1506
UNIVERSITÀ
DEGLI STUDI
DI URBINO
CARLO BO

UNIVERSITÀ DEGLI STUDI DI URBINO CARLO BO

Department of Pure and Applied Sciences

Ph.D. PROGRAMME IN:

RESEARCH METHODS IN SCIENCE AND TECHNOLOGY

CYCLE XXXVII

A PROCESS ALGEBRAIC THEORY OF REVERSIBLE CONCURRENT SYSTEMS WITH APPLICATIONS TO NONINTERFERENCE ANALYSIS

SSD: INFO-01/A

Coordinator: Ch.mo Prof. Luca Lanci

Supervisor: Ch.mo Prof. Marco Bernardo

Ph.D. student: Andrea Esposito

Academic Year 2023/2024

Abstract

This thesis explores reversibility in process algebra along with behavioral-equivalence-based noninterference analysis applied to reversible systems, thus presenting advances in theoretical foundations as well as practical applications. Reversibility is the capability of a system of undoing its own actions starting from the last performed one, in such a way that a consistent state is reached. This is not trivial to achieve in the case of concurrent systems, as the last performed action may not be uniquely identifiable and causality should be respected while going backward. Noninterference analysis supports the execution of secure computations in multi-level security systems by avoiding information leakage. This guarantees that low-level agents cannot infer, from their observations or through covert channels, the confidential behavior of high-level agents.

Building on previous works by De Nicola-Montanari-Vaandrager, Boudol-Castellani, Danos-Krivine, and Phillips-Ulidowski, in the first part of the thesis we introduce a lighter process algebraic language for reversible systems, which allows for both forward and backward computations without relying on communication keys or stack-based memories to support reversibility. The focus is on bisimulation semantics in the strong and weak cases, for which we define a forward version, which adheres to the interleaving style, as well as a reverse version and a forward-reverse version, which are truly concurrent instead. Key contributions include congruence results, modal logic characterizations, and sound and complete axiomatizations uniformly developed by following the proved trees approach of Degano-Priami. We also establish connections with other behavioral equivalences. Over sequential processes, reverse bisimilarities coincide with reverse trace equivalences while weak forward-reverse bisimilarity coincides with Van Glabbeek-Weijland's branching bisimilarity. Moreover, strong forward-reverse bisimilarity extended with backward ready multisets equality corresponds to Bednarczyk's hereditary history-preserving bisimilarity, thus providing for the latter a simpler alternative characterization valid also in the presence of autoconcurrency.

In the second part, we address Goguen-Meseguer's noninterference for reversible systems by relying on branching bisimilarity due to its connection with De Nicola-Montanari-Vaandrager's weak back-and-forth bisimilarity. We start by extending to the reversible setting Focardi-Gorrieri's classical taxonomy based on Milner's weak bisimilarity over nondeterministic processes, then we highlight the preservation and compositionality features of the resulting noninterference properties based on branching bisimilarity. We show the effectiveness in detecting covert channels arising in a reversible framework through some examples about database management system authentication. The same approach is subsequently applied to reversible processes exhibiting nondeterminism and probabilities expressed in the strictly alternating model of Hansson-Jonsson. We recast all the noninterference properties of interest by using weak and branching probabilistic bisimilarities, study their characteristics, establish a new taxonomy along with its relationships with the nondeterministic one, and illustrate their adequacy on a probabilistic smart contract lottery. Lastly, we consider reversible processes featuring nondeterminism and stochastic time expressed as Hermanns' interactive Markov chains. We define noninterference properties based on weak and branching stochastic bisimilarities, study their characteristics, further extend the aforementioned taxonomies, and provide some examples about obfuscation and permission mechanisms in database management systems.

Acknowledgments

First, I want to thank my supervisor, Prof. Marco Bernardo. He has been a truly extraordinary mentor, introducing me to process algebra, sparking my interest in theoretical computer science, and guiding me through the intricacies of the academic world. His rigor and precision have constantly motivated me to work hard and his guidance has been invaluable throughout these years. Most of the results contained in this thesis would not have been possible without his continuous support.

I am also grateful to Prof. Alessandro Aldini and Prof. Claudio A. Mezzina. They both provided me with priceless help in better understanding key concepts about noninterference and reversibility. Beyond their academic insights, they have always been generous with their time, engaging in stimulating discussions that often extended beyond those topics.

Special thanks go to Prof. Pierluigi Graziani, who immensely helped and supported me during the course of my PhD, especially at the start, and was always there for me. Whether offering a word of encouragement, providing comfort, or sharing a good laugh, I knew I could always rely on him.

I would like to extend my thanks to Prof. Robert J. van Glabbeek, who supervised my work as a visiting PhD student for a brief yet impactful period at the University of Edinburgh. The discussions we had about my work significantly enriched my understanding of the subtle nuances that distinguish various behavioral equivalences.

I am deeply grateful to the reviewers of this thesis, Prof. Ilaria Castellani (INRIA, Université Côte d'Azur) and Prof. Iain Phillips (Imperial College London), for their insightful comments and suggestions, which have significantly improved this manuscript.

I am also thankful to the Italian Ministry of University and Research, for the three-year PhD scholarship that funded my doctoral path, the PRIN 2020 project NiRvAna – Noninterference and Reversibility Analysis in Private Blockchains led by Prof. Marco Bernardo, which provided me with financial support for participating in many international conferences and summer schools and funded my current research grant, and the PhD Office of the University of Urbino, for the kind willingness to help with administration matters.

A very special thank to my PhD colleague and friend Christel, whose company always brought me fun times and lightheartedness, regardless of how hard or long of a day at the office it was.

A needed thank you to all of my friends, who supported me during this journey, cared about me, and were always there to help me in my time of need, whether for online calls or in person whenever I went back home. I hope not to overlook anyone as I express my gratitude to: Sabino, Michela, Dario, Ciro, Valentina, Flavio, Gaetano, Lorenzo, Luca, Martina, Francesco, Niki, and Ludovico. You gave me the strength to endure during these years.

Lastly, my deepest thanks go to my family, who always supported and encouraged me to follow my path regardless of how incomprehensible it was for them.
I love you. This thesis is dedicated to you.

Contents

List of Figures

List of Tables

Chapter 1

Introduction

Reversibility [101, 17] and noninterference [82] are fundamental concepts in computer science. The former refers to the capability of undoing computations in a causally consistent manner and brings with it the promise of lower energy consumption. The latter deals with the absence of unintended information leaks that may take place along covert channels, thus safeguarding the integrity of multi-level security systems.

Both concepts will be studied from a process algebraic perspective. The reason is that process calculi, which include examples such as CCS [112], CSP [45], ACP [18], and LOTOS [38] along with the tool support provided by CADP [72] and mCRL2 [84], constitute a foundational theory for concurrent and distributed systems. They comprise observable and unobservable actions as well as operators like sequential, alternative, and parallel compositions whereby building complex system descriptions from simpler ones. A central role is played by behavioral equivalences [20], which identify syntactically different process terms that exhibit the same observable behavior.

1.1 Reversible Computing

Reversibility is a well established concept in mathematics, physics, chemistry, and biology, where we find notions such as inverse operations, formulas, laws, and reactions. Formally speaking, given a function from an input set to an output set, reversibility has to do with the capability of each output to uniquely define the corresponding input, i.e., the invertibility of the function. As a consequence, irreversibility can be described via non-invertible functions; for example, conjunctions and disjunctions computed inside circuits are not reversible, while negation is reversible. In computing, especially in the case of concurrent and distributed systems, a dual phenomenon is nondeterminism, where it is the input that does not uniquely define the corresponding output.

Reversibility started to receive attention in computing only a few decades ago with the seminal work of Landauer [101] and Bennett [17]. It was observed that irreversible computations cause heat dissipation into circuits. More precisely, Landauer's principle states that any logically irreversible manipulation of information, such as the erasure of bits or the merging of computation paths, must be accompanied by a corresponding entropy increase in non-information-bearing degrees of freedom of the information processing apparatus or its environment. In particular, there is a minimal heat generation due to extra work for standardizing signals and making them independent of their history, so that it becomes impossible to determine input signals from output ones. According to this principle – which has been later verified in [36] and given a physical foundation in [70] – any logically reversible computation, in which no information is lost, may be potentially carried out without releasing any heat. In other words, the logical irreversibility of a function implies the physical irreversibility of computing that function and the consequent dissipative effects.

In addition to low energy consumption, reversible computing has applications in many areas nowadays, among which we mention the following:

- Robotics [108], wireless communications [137], and fault-tolerant systems [54, 141, 102, 139], where reversibility supports backtrack or rollback operations when encountering obstacles or malfunctionings.
- Parallel discrete-event simulation [119, 132], where it is necessary to go back whenever an inconsistent state is reached by the optimistic approach followed to speed up the simulation itself.
- Distributed algorithms [143, 31], where it is vital for individual participants to be able to escape from situations in which resources cannot be acquired or consensus cannot be achieved.
- Program debugging [73, 105], where reversibility helps avoiding to reproduce situations in which errors occurred, especially in the presence of concurrency as nondeterminism hinders reproducibility.
- Biochemical system modeling [125, 126], for a faithful representation of phenomena that are reversible in nature.

A reversible computing system features two directions of computation. The forward one coincides with the normal way of computing. The backward one undoes the effects of the forward one so as to return to a consistent state, i.e., a state that can be encountered while moving in the forward direction. Returning to a consistent state is not an easy task to accomplish in a concurrent system, because the undo procedure necessarily starts from the last performed action and this may not be uniquely identifiable due to concurrency. The strategy to adopt should respect causality, i.e., an action can be undone provided that all the actions it subsequently caused, if any, have been undone beforehand [53].

1.1.1 Reversible Process Calculi

In this thesis we address reversibility in a process algebraic framework, for which we refer the reader to [112, 45, 18, 38, 20, 72, 84] and the references therein. Process calculi were not natively equipped with inverse operators, hence do not directly support reversibility. To make them reversible, two approaches have been developed that keep track of executed actions and are able to revert computations in a causally consistent manner. The two approaches have been shown to be equivalent in [103] and the common properties they exploit to ensure causal reversibility have been systematically classified in [107].

The dynamic approach of [53, 100] is represented by RCCS (R for reversible) and its mobile variants [104, 52]. RCCS is an extension of CCS [112] that uses stack-based memories attached to processes so as to store all executed actions and all subprocesses discarded upon choices. A single transition relation is defined, while actions are divided into forward and backward thereby resulting in forward and backward transitions respectively. This approach is adequate in the case of very expressive calculi as well as programming languages.

The static approach of [121] proposes instead a general method to reverse calculi, of which CCSK (K for keys) and its quantitative variants [32, 37, 33, 34] are a result. The idea is to make all process algebraic operators static – in particular action prefix and choice – so that executed actions and discarded alternative subprocesses are kept within the syntax. A forward transition relation and a backward transition relation are defined separately. Their labels are actions extended with communication keys so as to know, upon generating backward transitions, which actions synchronized with each other in the forward direction. This approach is very handy when dealing with basic process calculi.

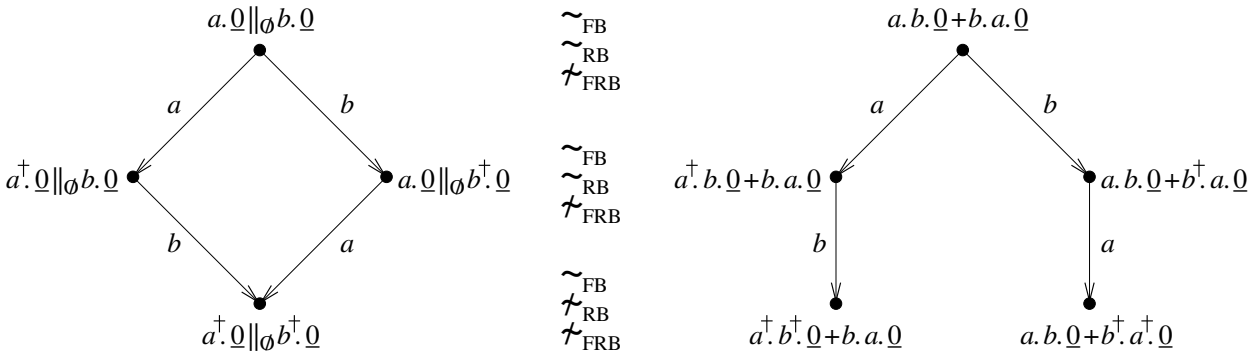


Figure 1.1: Comparing forward, reverse, and forward-reverse bisimilarities: interleaving vs. true concurrency

1.1.2 Bisimulation Semantics for Reversible Processes

Syntactically different process terms that denote the same behavior can be identified by means of behavioral equivalences. Among the many relations proposed in the literature [76], bisimilarity [117, 112] plays a central role. It represents the capability of mimicking each other's behavior stepwise. Given two bisimilar processes, whenever either process can perform a certain action, then the other process can respond with the same action and after the execution of that action the two processes are still related, so that this game can go ahead endlessly. In [121] the definition of bisimilarity was adapted to reversible processes by matching forward transitions on the one hand and backward transitions on the other hand. In a reversible setting with a single transition relation, it can be further adapted by matching outgoing transitions when going forward and incoming transitions when going backward [57].

Let us denote by $\sim_{\rm FRB}$ the resulting forward-reverse bisimilarity and by $\sim_{\rm FB}$ and $\sim_{\rm RB}$ its two components, i.e., forward bisimilarity – which considers only outgoing transitions – and reverse bisimilarity – which considers only incoming transitions. Unlike $\sim_{\rm FB}$, which corresponds to classical bisimilarity [117, 112], as noted in [121] it turns out that $\sim_{\rm FRB}$ – and also $\sim_{\rm RB}$ – does not satisfy the expansion law of parallel composition into a nondeterministic choice among all possible action sequencings. In Figure 1.1 we depict two labeled transition systems respectively representing a process that can perform action a in parallel with action b – i.e., $a \,.\, \underline{0} \,\|_\emptyset\, b \,.\, \underline{0}$ using a CSP-like parallel composition [45] – and a process that can perform either a followed by b or b followed by a – i.e., $a \,.\, b \,.\, \underline{0} + b \,.\, a \,.\, \underline{0}$ with $+$ denoting a CCS-like nondeterministic choice [112] – where $a \neq b$ and $\dagger$ decorates executed actions.

The forward bisimulation game yields the usual interleaving setting by relating the two top states, the two left intermediate states, the two right intermediate states, and the three bottom states. However, the three bottom states are no longer related if we play the reverse bisimulation game, as the bottom state in the first system has two differently labeled incoming transitions while either bottom state in the second system has only one. The remaining pairs of states are related by reverse bisimilarity as they have identically labeled incoming transitions, whereas they are told apart by forward-reverse bisimilarity due to the failure of the interplay between outgoing and incoming transitions matching. More precisely, any two corresponding intermediate states are not forward-reverse bisimilar because their identically labeled outgoing transitions reach the aforementioned inequivalent bottom states. In turn, the two initial states are not forward-reverse bisimilar either, because their identically labeled outgoing transitions reach the aforementioned inequivalent intermediate states. In summary, reverse and forward-reverse bisimilarities are truly concurrent.

For the sake of completeness, we recall that an interleaving view of parallel composition can be restored under the forward-reverse bisimulation game by considering computation paths (instead of states) like in the back-and-forth bisimilarity of [57]. Besides causality, this approach additionally preserves history, in the sense that backward moves are constrained to take place along the path followed in the forward direction even in the presence of concurrency. For instance, in the labeled transition system on the left, after performing a and then b it is not possible to undo a before b – as the forward computation is $a\,b$ and we have to backtrack – although there are no causality constraints between actions a and b.

1.2 Noninterference in Multi-Level Security Systems

Noninterference was introduced by Goguen and Meseguer [82] to reason about the way in which illegitimate information flows can occur in multi-level security systems due to covert channels from high-level agents to low-level ones. Since the first definition, conceived for deterministic systems, a lot of work has been done leading to a variety of extensions to nondeterministic or quantitative domains, in multiple frameworks going from language-based security to concurrency theory; see, e.g., [67, 4, 110, 87, 140, 130, 15, 7, 5, 94] and the references therein. Analogously, to verify information-flow security properties based on noninterference, several different approaches have been proposed ranging from the application of type theory [144] and abstract interpretation [74] to control flow and equivalence or model checking [68, 111, 6].

Noninterference guarantees that low-level agents cannot infer from their observations what high-level ones are doing. Regardless of its specific definition, noninterference is closely tied to the notion of behavioral equivalence [76] because, given a multi-level security system, the idea is to compare the system behavior with high-level actions being prevented and the system behavior with the same actions being hidden. A natural framework in which to study system behavior is given by process algebra. In this setting, weak bisimilarity [112] has been employed in [67] to reason formally about covert channels and illegitimate information flows as well as to study a classification of noninterference properties for nondeterministic systems.

1.2.1 Noninterference Properties

One of the first and most intuitive proposals of noninterference property has been Bisimulation-based Strong Nondeterministic Non-Interference (BSNNI) [67]. Given a process P and denoting by $\mathcal{A}_\mathcal{H}$ the set of all possible high-level actions, the property is satisfied if P with its high-level actions being prevented – modeled by $P \setminus \mathcal{A}_\mathcal{H}$ where $\setminus$ is a CCS-like restriction operator [112] – behaves the same as P with its high-level actions being hidden – modeled by $P / \mathcal{A}_\mathcal{H}$ where $/$ is a CSP-like hiding operator [45]. The equivalence between these two low-level views of P means that a low-level agent cannot infer the high-level behavior of the system. For instance, in the process $l\,.\,\underline{0} + h\,.\,l\,.\,\underline{0}$, which can either perform the low-level action l alone or the high-level action h followed by the low-level action l, a low-level agent that observes the execution of l cannot infer anything about the execution of h. Indeed, $(l\,.\,\underline{0} + h\,.\,l\,.\,\underline{0}) \setminus \{h\}$ and $(l\,.\,\underline{0} + h\,.\,l\,.\,\underline{0}) / \{h\}$ are equivalent because the former process behaves as $l\,.\,\underline{0}$, the latter process behaves as $l\,.\,\underline{0} + \tau\,.\,l\,.\,\underline{0}$ with τ representing the unobservable action, and $l\,.\,\underline{0} \approx l\,.\,\underline{0} + \tau\,.\,l\,.\,\underline{0}$ with $\approx$ being any τ-abstracting equivalence in the bisimulation style.

BSNNI is not powerful enough to detect information leakages that derive from the behavior of a high-level agent interacting with the system. For instance, $l\,.\,\underline{0} + h_1\,.\,h_2\,.\,l\,.\,\underline{0}$ is BSNNI for the same reason discussed above. However, a high-level agent like $h_1\,.\,\underline{0}$ enables h_1 and then disables h_2, thus yielding the low-level view of the system $l\,.\,\underline{0} + \tau\,.\,\underline{0}$, which is clearly distinguishable from $l\,.\,\underline{0}$ as only in the former a low-level agent may not observe l. To avoid such a limitation, the most obvious solution consists of checking explicitly the interaction on any action

set included in $\mathcal{A}_{\mathcal{H}}$ between the system and every possible high-level agent Q. The resulting property is called Bisimulation-based Non-Deducibility on Composition (BNDC) [67].

To circumvent the verification problems related to the universal quantification over Q, several properties have been proposed that are stronger than BNDC. They all express some persistency conditions, stating that the security checks have to be extended to all the processes reachable from a secure one. Three of the most representative ones among such properties are the variant of BSNNI that requires every reachable process to satisfy BSNNI itself, called Strong BSNNI (SBSNNI) [67], the variant of BNDC that requires every reachable process to satisfy BNDC itself, called Persistent BNDC (P_BNDC) [69], and Strong BNDC (SBNDC) [67], which requires the low-level view of every reachable process to be the same before and after the execution of any high-level action, meaning that the execution of high-level actions must be completely transparent to low-level agents.

1.2.2 Nondeterministic Systems

The foundational work on noninterference for nondeterministic systems in a process algebraic framework has been carried out in [67] by employing weak bisimilarity [112]. The aforementioned properties have been studied in terms of their preservation under weak bisimilarity – meaning that, whenever a process is secure under any of such properties, then every other equivalent process is secure too according to the same property – as well as their compositionality with respect to typical process algebraic operators – the composition of processes enjoying the same persistent property possess that property too. Furthemore, a taxonomy of those properties has been developed that explicitly highlights the inclusion relationships.

1.2.3 Probabilistic Systems

Noninterference in probabilistic systems extends classical security analysis by accounting for scenarios where adversaries may exploit probabilistic behavior to infer confidential information. In this setting, security properties must ensure that high-level actions do not affect the probability distribution of observable behaviors, thus preventing probabilistic covert channels. Unlike purely nondeterministic models, probabilistic models require a more fine-grained analysis to capture leakages.

In [7] a combination of the generative and reactive probabilistic models of [79] is considered. On top of it, a probabilistic process calculus is built, where not only choice but also parallel composition and hiding are decorated with a probabilistic parameter, so that the selection among all the actions executable by a process is fully probabilistic. Using a behavioral equivalence akin to the weak probabilistic bisimilarity of [13], probabilistic variants of BSNNI, BNDC, and SBNDC are investigated with respect to preservation and compositionality features. Their taxonomy is also developed and compared with the nondeterministic one of [67].

1.2.4 Stochastically Timed Systems

Noninterference in stochastically timed systems further extends information flow analysis as time-related information can be exploited to infer high-level activities or alter the steady-state behavior of the system. Based on process algebraic frameworks inspired by [93] – where every action is enriched with a positive real number expressing the rate of the exponential distribution quantifying the duration of the action – together with stochastic variants of weak bisimilarity, in [5] stochastic variants of BSNNI and SBNDC are considered whilst in [94] a stochastic variant of P_BNDC is examined.

1.3 Contributions and Organization of the Thesis

In this thesis we present a fully fledged process algebraic theory of reversible concurrent systems (Part I) and we extend noninterference analysis to reversible multi-level security systems (Part II).

The first contribution of this thesis is a lighter approach to the definition of reversible process calculi, which avoids both stack-based memories [53, 100] and communication keys with the related infinite branching [121]. Like in [121], we keep in the process syntax all the information needed to support reversibility, in particular executed actions and discarded subprocesses. Similar to [53, 100], the operational semantics generates a labeled transition system based on a single transition relation. Following [57], we deem the transition relation to be symmetric: each transition is viewed as an outgoing transition of its source state when going forward or an incoming transition of its target state when going backward. Consequently, as in [42] we can mark all executed actions with the same symbol, which we choose to be † (Chapter 2).

The second contribution is a systematic study of the properties of $\sim_{\mathrm{FRB}}$ and its two components $\sim_{\mathrm{FB}}$ and $\sim_{\mathrm{RB}}$, of which we consider both the strong variants, treating all the actions in the same way, and the weak variants, capable of abstracting from unobservable actions (Chapter 3). In particular:

- We compare the discriminating power of the considered bisimilarities and investigate whether they are congruences with respect to the operators of our reversible process calculus to support compositional reasoning (Chapter 4).
- We provide modal logic characterizations of the considered bisimilarities, which illustrate what properties are preserved by each of them and offer diagnostic information to explain why two processes are not equivalent (Chapter 5).
- We exhibit sound and complete axiomatizations of the considered bisimilarities, which elucidate the fundamental equational laws behind those equivalences. Since forward bisimilarities are interleaving whereas reverse and forward-reverse bisimilarities are truly concurrent, to uniformly derive expansion laws of parallel composition for all of them we use encodings based on the proved trees approach of [59] (Chapter 6).
- We show alternative characterizations of reverse and forward-reverse bisimilarities, so as to establish connections with other behavioral equivalences such as trace equivalences [45], branching bisimilarity [80], and hereditary history-preserving bisimilarity [16] (Chapter 7).

The third contribution is recognizing that, while weak bisimilarity is appropriate for the noninterfence analysis of standard forward-only systems [67], to study information flow in reversible systems a more discriminating weak equivalence is needed, as witnessed by a number of examples. One possibility is to resort to weak forward-reverse bisimilarity. However, given its truly concurrent nature, it may turn out to be too discriminating. From this viewpoint a better option is branching bisimilarity [80], because it coincides with weak forward-reverse bisimilarity over sequential processes as well as weak back-and-forth bisimilarity [57], which works under the assumption that backward moves are constrained to stick to the same path undertaken in the forward direction.

The fourth contribution is recasting the noninterference properties of [67, 69] by using branching bisimilarity, investigating their preservation and compositionality features, and establishing a taxonomy for them to be compared with the one based on weak bisimilarity. This is done not only in the case of nondeterministic systems (Chapter 8), but also in the case of nondeterministic systems extended with probabilities according to the strictly alternating model of [86] (Chapter 9) as well as in the case of nondeterministic systems extended with stochastic time based on the interactive Markov chain model of [90] (Chapter 10).

The thesis concludes by summarizing our findings and indicating future work (Chapter 11).

Part I

Reversible Process Algebra without Memories and Keys

Chapter 2

A Lighter Calculus for Reversible Concurrent Systems

In this chapter, whose contents have appeared in [27, 29], we present the syntax (Section 2.1) and the semantics (Section 2.2) of a process algebraic language for expressing reversible concurrent systems in a compositional way. Although inspired by CCSK [121] and RCCS [53, 100], our calculus is lighter because there are neither communication keys nor stack-based memories.

2.1 Syntax of Reversible Concurrent Processes

In the representation of a system, we are used to describe only its future behavior. In order to support reversibility according to [121], we have to enrich the syntax with information about the past, in particular which actions have already been executed. Unlike [121], we do not need to add distinct communication keys to non-synchronizing executed actions because the operational semantics will be based on a single transition relation like in [53, 100]. Similar to [42], it thus suffices to mark all executed actions with the same symbol, which we choose to be †.

Given a countable set $\mathcal{A}$ of actions including an unobservable action that we denote by τ, our language PRPC (Proved Reversible Process Calculus) has the following syntax inspired by those of CCS [112] and CSP [45]:

$$P ::= \underline{0} \mid a \,.\, P \mid a^{\dagger} \,.\, P \mid P \llcorner \rho \urcorner \mid P + P \mid P \parallel_L P$$

where $a \in \mathcal{A}$, $\rho : \mathcal{A} \to \mathcal{A}$ such that $\rho(\tau) = \tau$, $L \subseteq \mathcal{A} \setminus \{\tau\}$, and:

- $\underline{0}$ is the terminated process.
- $a \,.\, P$ is a process that can execute action a and whose forward continuation is P (unexecuted action prefix).
- $a^{\dagger} \,.\, P$ is a process that executed action a and whose forward continuation is inside P, which can undo action a after all executed actions within P have been undone (executed action prefix).
- $P \llcorner \rho \urcorner$ is a process in which all actions executed by P are renamed according to function ρ – expressed for short as a set of elements of the form $a \mapsto b$ with $a \neq b$ – where τ is left unchanged whilst observable actions can be modified and even hidden, i.e., turned into τ (renaming).
- $P_1 + P_2$ expresses a nondeterministic choice between P_1 and P_2 as far as neither has executed any action yet, otherwise only the one that was selected in the past can move (past-sensitive alternative composition).
- $P_1 \parallel_L P_2$ expresses that P_1 and P_2 proceed independently of each other on actions in $\overline{L} = \mathcal{A} \setminus L$ while they have to synchronize on every action in L (parallel composition).

We can characterize two important classes of processes via as many predicates defined by induction on the syntactical structure of a process P. Firstly, we define *initial* processes, in which all actions are unexecuted and hence no † appears:

$$\begin{array}{rcl} \mathit{initial}(\underline{0}) & & \\ \mathit{initial}(a\,.\,P') & \text{iff} & \mathit{initial}(P') \\ \mathit{initial}(P'\llcorner\rho\urcorner) & \text{iff} & \mathit{initial}(P') \\ \mathit{initial}(P_1 + P_2) & \text{iff} & \mathit{initial}(P_1) \wedge \mathit{initial}(P_2) \\ \mathit{initial}(P_1 \parallel_L P_2) & \text{iff} & \mathit{initial}(P_1) \wedge \mathit{initial}(P_2) \end{array}$$

Secondly, we define *well-formed* processes, whose set we denote by P, in which both unexecuted and executed actions can occur in certain circumstances:

$$\begin{array}{rcl} \mathit{wf}(\underline{0}) & & \\ \mathit{wf}(a\,.\,P') & \text{iff} & \mathit{initial}(P') \\ \mathit{wf}(a^\dagger\,.\,P') & \text{iff} & \mathit{wf}(P') \\ \mathit{wf}(P'\llcorner\rho\urcorner) & \text{iff} & \mathit{wf}(P') \\ \mathit{wf}(P_1 + P_2) & \text{iff} & (\mathit{wf}(P_1) \wedge \mathit{initial}(P_2)) \vee (\mathit{initial}(P_1) \wedge \mathit{wf}(P_2)) \\ \mathit{wf}(P_1 \parallel_L P_2) & \text{iff} & \mathit{wf}(P_1) \wedge \mathit{wf}(P_2) \end{array}$$

Well formedness not only imposes that every unexecuted action is followed by an initial process, but also that in every alternative composition at least one subprocess is initial. Multiple paths arise in the presence of both alternative and parallel compositions. However, at each occurrence of the former, only the subprocess chosen for execution can move. Although not selected, the other subprocess is kept as an initial subprocess within the overall process in the same way as executed actions are kept inside the syntax [42, 121], so as to support reversibility. For example, in $a^\dagger\,.\,b\,.\,\underline{0} + c\,.\,d\,.\,\underline{0}$ the subprocess $c\,.\,d\,.\,\underline{0}$ cannot move as a was selected in the choice between a and c.

It is worth noting that:

- $\underline{0}$ is both initial and well-formed.
- Any initial process is well-formed too.
- P also contains processes that are not initial like, e.g., $a^\dagger\,.\,b\,.\,\underline{0}$, which can either do b or undo a.
- In P the relative positions of already executed actions and actions to be executed matter. More precisely, an action of the former kind can never occur after one of the latter kind. For instance, $a^\dagger\,.\,b\,.\,\underline{0} \in \mathsf{P}$ whereas $b\,.\,a^\dagger\,.\,\underline{0} \notin \mathsf{P}$.
- In P the subprocesses of an alternative composition can be both initial, but cannot be both non-initial. As an example, $a\,.\,\underline{0} + b\,.\,\underline{0} \in \mathsf{P}$ whilst $a^\dagger\,.\,\underline{0} + b^\dagger\,.\,\underline{0} \notin \mathsf{P}$.

2.2 Proved Structural Operational Semantics

According to [121], dynamic operators such as action prefix and alternative composition have to be made static in the operational semantic rules, so as to keep in the syntax all the information needed to support reversibility. Unlike [121], we do not generate a forward transition relation and a backward one, but a single transition relation that, like in [57], we deem to be symmetric in order to enforce the *loop property* [53]: every executed action can be undone and every undone action can be redone. In our setting a backward transition from P' to P is subsumed by the corresponding forward transition t from P to P'. As we will see in Chapter 3, following [57] we view t as an *outgoing* transition of P when going forward, while we view t as an *incoming* transition of P' when going backward.

$$(\text{Act}_\text{f})\ \frac{initial(P)}{a\,.\,P \xrightarrow{a} a^\dagger\,.\,P} \qquad (\text{Act}_\text{p})\ \frac{P \xrightarrow{\theta} P'}{a^\dagger\,.\,P \xrightarrow{\cdot_a\theta} a^\dagger\,.\,P'}$$

$$(\text{Ren})\ \frac{P \xrightarrow{\theta} P'}{P\llcorner\rho\lrcorner \xrightarrow{\llcorner\rho\lrcorner\theta} P'\llcorner\rho\lrcorner}$$

$$(\text{Cho}_\text{l})\ \frac{P_1 \xrightarrow{\theta} P_1' \quad initial(P_2)}{P_1 + P_2 \xrightarrow{+\theta} P_1' + P_2} \qquad (\text{Cho}_\text{r})\ \frac{P_2 \xrightarrow{\theta} P_2' \quad initial(P_1)}{P_1 + P_2 \xrightarrow{+\theta} P_1 + P_2'}$$

$$(\text{Par}_\text{l})\ \frac{P_1 \xrightarrow{\theta} P_1' \quad act(\theta) \notin L}{P_1 \parallel_L P_2 \xrightarrow{\lVert_L\theta} P_1' \parallel_L P_2} \qquad (\text{Par}_\text{r})\ \frac{P_2 \xrightarrow{\theta} P_2' \quad act(\theta) \notin L}{P_1 \parallel_L P_2 \xrightarrow{\lVert_L\theta} P_1 \parallel_L P_2'}$$

$$(\text{Syn})\ \frac{P_1 \xrightarrow{\theta_1} P_1' \quad P_2 \xrightarrow{\theta_2} P_2' \quad act(\theta_1) = act(\theta_2) \in L}{P_1 \parallel_L P_2 \xrightarrow{\langle\theta_1,\theta_2\rangle_L} P_1' \parallel_L P_2'}$$

Table 2.1: Proved operational semantic rules for reversible concurrent processes

To enable the uniform derivation of expansion laws for parallel composition (see Chapter 6) under the various bisimilarities that we will consider, we provide an operational semantics based on [59], which is very concrete as every transition is labeled with a *proof term* [41, 42]. This is an action preceded by the sequence of operator symbols in the scope of which the action occurs inside the source process of the transition. In the case of a binary operator, the corresponding symbol also specifies whether the action occurs to the left or to the right. The syntax that we adopt for the set Θ of proof terms is as follows:

$$\theta ::= a \mid \cdot_a\theta \mid \llcorner\rho\lrcorner\theta \mid +\theta \mid \dot{+}\theta \mid \lVert_L\theta \mid \rVert_L\theta \mid \langle\theta,\theta\rangle_L$$

where a, ρ, L are added as subscripts as they may turn out to be useful (see, e.g., the forthcoming function act).

The proved operational semantic rules are in Table 2.1 and generate the proved labeled transition system $(\mathsf{P}, \Theta, \longrightarrow)$ where $\longrightarrow \subseteq \mathsf{P} \times \Theta \times \mathsf{P}$ is the proved transition relation. We denote by $\mathbb{P} \subsetneq \mathsf{P}$ the set of processes that are *reachable* from an initial one via $\longrightarrow$. Not all well-formed processes are reachable; for example, $a^\dagger\,.\,\underline{0} \parallel_{\{a\}} \underline{0}$ is not reachable from $a\,.\,\underline{0} \parallel_{\{a\}} \underline{0}$ as action a on the left cannot synchronize with any action on the right. From now on we consider only $\mathbb{P}$ and denote by $\mathbb{P}_{\text{init}}$ the set of initial processes as they are all reachable.

The first rule for action prefix (Act_f where f stands for forward) applies only if P is initial and retains the executed action in the target process of the generated forward transition by decorating the action itself with $\dagger$. The second rule (Act_p where p stands for propagation) propagates actions of inner initial subprocesses by putting an a-dot before them in the transition label for each outer executed a-action prefix that is encountered.

In the only rule for renaming (Ren), the transition label is changed according to the τ-preserving renaming function ρ by placing a ρ-corner pair at the beginning of the proof term.

In both rules for alternative composition (Cho_l and Cho_r where l stands for left and r stands for right), the subprocess that has not been selected for execution is retained as an initial subprocess in the target process of the generated transition. When both subprocesses are initial, both rules for alternative composition are applicable, otherwise only one of them can be applied and in that case it is the non-initial subprocess that can move, because the other one has been discarded at the moment of the selection. The symbol $+$ or $\dot{+}$ is added at the beginning of

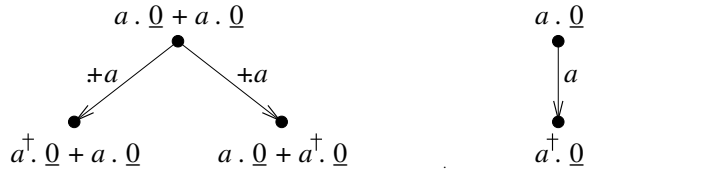
the proof term.

The three rules for parallel composition use partial function $act : \Theta \rightharpoonup \mathcal{A}$ to extract an action from a proof term θ. This function, which will be used throughout the first part of the thesis, is defined by induction on the syntactical structure of θ as follows:

$$\begin{aligned} act(a) &= a \\ act(.\!_a\,\theta') &= act(\theta') \\ act(\llcorner\!\!\urcorner_\rho\,\theta') &= \rho(act(\theta')) \\ act(\dot{+}\,\theta') = act(\dot{+}\,\theta') &= act(\theta') \\ act(\|_L\,\theta') = act(\|_L\,\theta') &= act(\theta') \\ act(\langle \theta_1, \theta_2 \rangle_L) &= \begin{cases} act(\theta_1) & \text{if } act(\theta_1) = act(\theta_2) \\ \text{undefined} & \text{otherwise} \end{cases} \end{aligned}$$

In the first two rules (PAR$_\text{l}$ and PAR$_\text{r}$), a single subprocess proceeds by performing an action not belonging to L, with $\|_L$ or $\|_L$ being placed at the beginning of the proof term. In the third rule (SYN), both subprocesses synchronize on an action in L and the resulting proof term contains both individual proof terms. If $L = \emptyset$ or $L = \mathcal{A} \setminus \{\tau\}$, then the two subprocesses are fully independent or fully synchronized, respectively, on observable actions.

Example 2.1. The proved labeled transition systems generated by the rules in Table 2.1 for the two initial processes $a\,.\,\underline{0} \,\|_\emptyset\, b\,.\,\underline{0}$ and $a\,.\,b\,.\,\underline{0} + b\,.\,a\,.\,\underline{0}$ are shown in Figure 1.1 even though each of their transitions is labeled with $act(\theta)$ instead of θ, e.g., on the left label a should be $\|_\emptyset a$ and label b should be $\|_\emptyset b$. As another example, the proved labeled transition systems for the two initial processes $a\,.\,\underline{0} + a\,.\,\underline{0}$ and $a\,.\,\underline{0}$ are depicted below:



In the case of a forward-only process calculus like CCS [112], a single a-transition would be generated from $a\,.\,\underline{0} + a\,.\,\underline{0}$ to $\underline{0}$ due to the absence of decorated actions within processes. ■

Every process may have several outgoing transitions and, if it is not initial, has at least one incoming transition. Let $\mathbb{P}_\text{seq}$ be the set of *sequential* processes of $\mathbb{P}$, in which there are no occurrences of parallel composition. Due to the decoration of executed actions inside the process syntax, over $\mathbb{P}_\text{seq}$ it holds that every non-initial process has exactly one incoming transition, the underlying labeled transition systems turn out to be trees, and well formedness coincides with reachability.

Proposition 2.1. *Let $P \in \mathbb{P}_\text{seq}$:*

1. *If P is not initial then it has exactly one incoming transition.*
2. *If P is initial then its underlying labeled transition system is a tree.*

Proof. For the first property we proceed by induction on the syntactical structure of $P \in \mathbb{P}_\text{seq}$ with $\neg \mathit{initial}(P)$:

- If P is $a^\dagger\,.\,P'$ there are two cases:
  - If $\mathit{initial}(P')$ then $a^\dagger\,.\,P'$ has exactly one incoming transition, which is labeled with a, by virtue of rule ACT$_\text{f}$ in Table 2.1.

  - If $\neg \mathit{initial}(P')$ then by the induction hypothesis P' has exactly one incoming transition and hence so does $a^{\dagger}.P'$ by virtue of rule $\textsc{Act}_{\mathrm{p}}$ in Table 2.1.

- If P is $P' \llcorner \rho \urcorner$ then by the induction hypothesis P' has exactly one incoming transition and hence so does $P' \llcorner \rho \urcorner$ by virtue of rule Ren in Table 2.1.

- If P is $P_1 + P_2$ there are two cases:

  - If $\neg \mathit{initial}(P_1)$ then by the induction hypothesis P_1 has exactly one incoming transition and hence so does $P_1 + P_2$ by virtue of rule $\textsc{Cho}_{\mathrm{l}}$ in Table 2.1 and the fact that, if the source process of the transition to $P_1 + P_2$ is initial, then its outgoing transitions have target processes that pairwise differ for the action that is decorated with $\dagger$ inside each of them.
  - If $\neg \mathit{initial}(P_2)$ then the proof is similar with $\textsc{Cho}_{\mathrm{r}}$ in lieu of $\textsc{Cho}_{\mathrm{l}}$.

The second property is a consequence of the first one. ■

Chapter 3

Forward, Reverse, and Forward-Reverse Bisimilarities

In this chapter, whose contents have appeared in [27, 25, 29], we define forward, reverse, and forward-reverse bisimilarities over the set $\mathbb{P}$ of reachable processes introduced in the previous chapter, both in the strong case (Section 3.1) and in the weak one (Section 3.2). They will allow us to identify syntactically different processes that exhibit the same behavior.

3.1 Strong Bisimilarities

When defining bisimilarity in a reversible setting, one can consider only the forward direction like in [117, 112], only the backward direction, or both directions like in [121]. In the specific reversible setting of PRPC, in which there is a single transition relation viewed as being symmetric [57], the bisimulation game compares only *outgoing* transitions in the first case, only *incoming* transitions in the second case, or both kinds of transitions in the third case. Below we present the *strong* versions of the three bisimilarities, i.e., the versions that treat τ-actions as if they were observable. In the definitions of bisimilarities we abstract from operator symbols inside transition labels by using function *act*.

Definition 3.1. *We say that $P_1, P_2 \in \mathbb{P}$ are* forward bisimilar*, written $P_1 \sim_{\rm FB} P_2$, iff $(P_1, P_2) \in \mathcal{B}$ for some forward bisimulation $\mathcal{B}$. A symmetric relation $\mathcal{B}$ over $\mathbb{P}$ is a* forward bisimulation *iff, whenever $(P_1, P_2) \in \mathcal{B}$, then:*

- *For each $P_1 \stackrel{\theta_1}{\longrightarrow} P_1'$ there exists $P_2 \stackrel{\theta_2}{\longrightarrow} P_2'$ such that $act(\theta_1) = act(\theta_2)$ and $(P_1', P_2') \in \mathcal{B}$.* ■

Definition 3.2. *We say that $P_1, P_2 \in \mathbb{P}$ are* reverse bisimilar*, written $P_1 \sim_{\rm RB} P_2$, iff $(P_1, P_2) \in \mathcal{B}$ for some reverse bisimulation $\mathcal{B}$. A symmetric relation $\mathcal{B}$ over $\mathbb{P}$ is a* reverse bisimulation *iff, whenever $(P_1, P_2) \in \mathcal{B}$, then:*

- *For each $P_1' \stackrel{\theta_1}{\longrightarrow} P_1$ there exists $P_2' \stackrel{\theta_2}{\longrightarrow} P_2$ such that $act(\theta_1) = act(\theta_2)$ and $(P_1', P_2') \in \mathcal{B}$.* ■

Definition 3.3. *We say that $P_1, P_2 \in \mathbb{P}$ are* forward-reverse bisimilar*, written $P_1 \sim_{\rm FRB} P_2$, iff $(P_1, P_2) \in \mathcal{B}$ for some forward-reverse bisimulation $\mathcal{B}$. A symmetric relation $\mathcal{B}$ over $\mathbb{P}$ is a* forward-reverse bisimulation *iff, whenever $(P_1, P_2) \in \mathcal{B}$, then:*

- *For each* $P_1 \xrightarrow{\theta_1} P_1'$ *there exists* $P_2 \xrightarrow{\theta_2} P_2'$ *such that* $act(\theta_1) = act(\theta_2)$ *and* $(P_1', P_2') \in \mathcal{B}$.
- *For each* $P_1' \xrightarrow{\theta_1} P_1$ *there exists* $P_2' \xrightarrow{\theta_2} P_2$ *such that* $act(\theta_1) = act(\theta_2)$ *and* $(P_1', P_2') \in \mathcal{B}$. ■

Proposition 3.1. *Let* $\sim \in \{\sim_{\mathrm{FB}}, \sim_{\mathrm{RB}}, \sim_{\mathrm{FRB}}\}$. *Then* $\sim$ *is an equivalence relation.*

Proof. $\sim$ is reflexive because the identity relation over $\mathbb{P}$, i.e., $\{(P, P) \mid P \in \mathbb{P}\}$ is a $\sim$-bisimulation. $\sim$ is symmetric because so is every $\sim$-bisimulation. $\sim$ is transitive because the composition of two $\sim$-bisimulations, i.e., $\mathcal{B}_1 \circ \mathcal{B}_2 = \{(P_1, P_2) \in \mathbb{P} \times \mathbb{P} \mid \exists P \in \mathbb{P}.\, (P_1, P) \in \mathcal{B}_1 \wedge (P, P_2) \in \mathcal{B}_2\}$ is still a $\sim$-bisimulation. ■

Example 3.1. The first two processes in Example 2.1 are identified only by $\sim_{\mathrm{FB}}$ and trivially $\sim_{\mathrm{RB}}$ as they are initial (see Figure 1.1), while the last two processes are identified by all the three equivalences as witnessed by any bisimulation that contains the pairs $(a\,.\,\underline{0} + a\,.\,\underline{0}, a\,.\,\underline{0})$, $(a^\dagger.\,\underline{0} + a\,.\,\underline{0}, a^\dagger.\,\underline{0})$, and $(a\,.\,\underline{0} + a^\dagger.\,\underline{0}, a^\dagger.\,\underline{0})$. ■

It is easy to establish two necessary conditions for the three bisimilarities considered so far. Following the terminology of [116, 19], the two conditions respectively make use of the forward ready set in the forward direction and the backward ready set in the backward direction; the latter condition will be exploited in Chapter 6 when developing the expansion laws for parallel composition under reverse and forward-reverse semantics.

We proceed by induction on the syntactical structure of $P \in \mathbb{P}$ to define its forward ready set $frs(P) \subseteq \mathcal{A}$, i.e., the set of actions that P can immediately execute (labels of its outgoing transitions), as well as its backward ready set $brs(P) \subseteq \mathcal{A}$, i.e., the set of actions whose execution led to P (labels of its incoming transitions), where we use $\rho(A)$ to denote $\{\rho(a) \mid a \in A\}$:

$$
\begin{array}{rcl@{\qquad}rcl}
frs(\underline{0}) & = & \emptyset & brs(\underline{0}) & = & \emptyset \\
frs(a\,.\,P') & = & \{a\} & brs(a\,.\,P') & = & \emptyset \\
frs(a^\dagger.\,P') & = & frs(P') & brs(a^\dagger.\,P') & = & \left\{ \begin{array}{ll} \{a\} & \text{if } initial(P') \\ brs(P') & \text{if } \neg initial(P') \end{array} \right. \\
frs(P' \llcorner \rho \lrcorner) & = & \rho(frs(P')) & brs(P' \llcorner \rho \lrcorner) & = & \rho(brs(P')) \\
frs(P_1 + P_2) & = & \left\{ \begin{array}{ll} frs(P_1) \cup frs(P_2) & \text{if } initial(P_1) \wedge initial(P_2) \\ frs(P_1) & \text{if } \neg initial(P_1) \wedge initial(P_2) \\ frs(P_2) & \text{if } initial(P_1) \wedge \neg initial(P_2) \end{array} \right. & & & \\
brs(P_1 + P_2) & = & \left\{ \begin{array}{ll} \emptyset & \text{if } initial(P_1) \wedge initial(P_2) \\ brs(P_1) & \text{if } \neg initial(P_1) \wedge initial(P_2) \\ brs(P_2) & \text{if } initial(P_1) \wedge \neg initial(P_2) \end{array} \right. & & & \\
frs(P_1 \parallel_L P_2) & = & (frs(P_1) \cap \overline{L}) \cup (frs(P_2) \cap \overline{L}) \cup (frs(P_1) \cap frs(P_2) \cap L) & & & \\
brs(P_1 \parallel_L P_2) & = & (brs(P_1) \cap \overline{L}) \cup (brs(P_2) \cap \overline{L}) \cup (brs(P_1) \cap brs(P_2) \cap L) & & &
\end{array}
$$

Proposition 3.2. *Let* $P_1, P_2 \in \mathbb{P}$. *Then:*

1. *If* $P_1 \sim P_2$ *for* $\sim \in \{\sim_{\mathrm{FB}}, \sim_{\mathrm{FRB}}\}$, *then* $frs(P_1) = frs(P_2)$.
2. *If* $P_1 \sim P_2$ *for* $\sim \in \{\sim_{\mathrm{RB}}, \sim_{\mathrm{FRB}}\}$, *then* $brs(P_1) = brs(P_2)$.

Proof. A straightforward consequence of the definitions of the considered equivalences. ■

3.2 Weak Bisimilarities

We now introduce *weak* variants [112] of forward, reverse, and forward-reverse bisimilarities, i.e., variants capable of abstracting from τ-actions. In the following definitions, $P \Longrightarrow P'$ means that $P' = P$ or there exists a nonempty sequence of finitely many τ-transitions such that the target of each of them coincides with the source of the subsequent one, with the source of the first one being P and the target of the last one being P'. Moreover, $\Longrightarrow \stackrel{\theta}{\longrightarrow} \Longrightarrow$ stands for an $act(\theta)$-transition possibly preceded and followed by finitely many τ-transitions. Following [112], for the three weak variants we also provide three alternative definitions, which will be exploited in the proofs of the forthcoming Theorem 5.2, Theorem 7.2, Lemma 7.1, Theorem 7.3, and Theorem 7.4.

Definition 3.4. *We say that $P_1, P_2 \in \mathbb{P}$ are* weakly forward bisimilar*, written $P_1 \approx_{\rm FB} P_2$, iff $(P_1, P_2) \in \mathcal{B}$ for some weak forward bisimulation $\mathcal{B}$. A symmetric relation $\mathcal{B}$ over $\mathbb{P}$ is a* weak forward bisimulation *iff, whenever $(P_1, P_2) \in \mathcal{B}$, then:*

- *For each $P_1 \stackrel{\theta_1}{\longrightarrow} P_1'$ with $act(\theta_1) = \tau$ there exists $P_2 \Longrightarrow P_2'$ such that $(P_1', P_2') \in \mathcal{B}$.*
- *For each $P_1 \stackrel{\theta_1}{\longrightarrow} P_1'$ with $act(\theta_1) \neq \tau$ there exists $P_2 \Longrightarrow \stackrel{\theta_2}{\longrightarrow} \Longrightarrow P_2'$ such that $act(\theta_1) = act(\theta_2)$ and $(P_1', P_2') \in \mathcal{B}$.* ■

Proposition 3.3. *A symmetric relation $\mathcal{B}$ over $\mathbb{P}$ is a weak forward bisimulation iff, whenever $(P_1, P_2) \in \mathcal{B}$, then:*

- *For each $P_1 \Longrightarrow P_1'$ there exists $P_2 \Longrightarrow P_2'$ such that $(P_1', P_2') \in \mathcal{B}$.*
- *For each $P_1 \Longrightarrow \stackrel{\theta_1}{\longrightarrow} \Longrightarrow P_1'$ with $act(\theta_1) \neq \tau$ there exists $P_2 \Longrightarrow \stackrel{\theta_2}{\longrightarrow} \Longrightarrow P_2'$ such that $act(\theta_1) = act(\theta_2)$ and $(P_1', P_2') \in \mathcal{B}$.*

Proof. The proof is divided into two parts:

- Assume that $\mathcal{B}$ is a weak forward bisimulation and consider $(P_1, P_2) \in \mathcal{B}$. There are three cases:
  - If $P_1 \Longrightarrow P_1'$ where the sequence of τ-transitions is empty, i.e., $P_1 \Longrightarrow P_1$, then P_2 stays idle, i.e., $P_2 \Longrightarrow P_2$, with the two target processes being related by $\mathcal{B}$.
  - If $P_1 \Longrightarrow P_1'$ where the sequence of τ-transitions is not empty, then each such transition is matched according to $\mathcal{B}$ on the side of P_2, hence there exists $P_2 \Longrightarrow P_2'$ such that $(P_1', P_2') \in \mathcal{B}$.
  - If $P_1 \Longrightarrow \stackrel{\theta_1}{\longrightarrow} \Longrightarrow P_1'$ with $act(\theta_1) \neq \tau$, then each transition in the sequence is matched according to $\mathcal{B}$ on the side of P_2, hence there exists $P_2 \Longrightarrow \stackrel{\theta_2}{\longrightarrow} \Longrightarrow P_2'$ such that $act(\theta_1) = act(\theta_2)$ and $(P_1', P_2') \in \mathcal{B}$.
- Assume that $\mathcal{B}$ satisfies the property stated in the proposition and consider $(P_1, P_2) \in \mathcal{B}$. There are two cases:
  - If $P_1 \stackrel{\theta_1}{\longrightarrow} P_1'$ with $act(\theta_1) = \tau$, which can be rewritten as $P_1 \Longrightarrow P_1'$, then there exists $P_2 \Longrightarrow P_2'$ such that $(P_1', P_2') \in \mathcal{B}$.
  - If $P_1 \stackrel{\theta_1}{\longrightarrow} P_1'$ with $act(\theta_1) \neq \tau$, which can be rewritten as $P_1 \Longrightarrow P_1 \stackrel{\theta_1}{\longrightarrow} P_1' \Longrightarrow P_1'$, then there exists $P_2 \Longrightarrow \stackrel{\theta_2}{\longrightarrow} \Longrightarrow P_2'$ such that $act(\theta_1) = act(\theta_2)$ and $(P_1', P_2') \in \mathcal{B}$. ■

Definition 3.5. *We say that* $P_1, P_2 \in \mathbb{P}$ *are* weakly reverse bisimilar*, written* $P_1 \approx_{\mathrm{RB}} P_2$*, iff* $(P_1, P_2) \in \mathcal{B}$ *for some weak reverse bisimulation* $\mathcal{B}$*. A symmetric relation* $\mathcal{B}$ *over* $\mathbb{P}$ *is a* weak reverse bisimulation *iff, whenever* $(P_1, P_2) \in \mathcal{B}$*, then:*

- *For each* $P_1' \xrightarrow{\theta_1} P_1$ *with* $act(\theta_1) = \tau$ *there exists* $P_2' \Longrightarrow P_2$ *such that* $(P_1', P_2') \in \mathcal{B}$*.*
- *For each* $P_1' \xrightarrow{\theta_1} P_1$ *with* $act(\theta_1) \neq \tau$ *there exists* $P_2' \Longrightarrow \xrightarrow{\theta_2} \Longrightarrow P_2$ *such that* $act(\theta_1) = act(\theta_2)$ *and* $(P_1', P_2') \in \mathcal{B}$*.* ■

Proposition 3.4. *A symmetric relation* $\mathcal{B}$ *over* $\mathbb{P}$ *is a weak reverse bisimulation iff, whenever* $(P_1, P_2) \in \mathcal{B}$*, then:*

- *For each* $P_1' \Longrightarrow P_1$ *there exists* $P_2' \Longrightarrow P_2$ *such that* $(P_1', P_2') \in \mathcal{B}$*.*
- *For each* $P_1' \Longrightarrow \xrightarrow{\theta_1} \Longrightarrow P_1$ *with* $act(\theta_1) \neq \tau$ *there exists* $P_2' \Longrightarrow \xrightarrow{\theta_2} \Longrightarrow P_2$ *such that* $act(\theta_1) = act(\theta_2)$ *and* $(P_1', P_2') \in \mathcal{B}$*.*

Proof. The proof is divided into two parts:

- Assume that $\mathcal{B}$ is a weak reverse bisimulation and consider $(P_1, P_2) \in \mathcal{B}$. There are three cases:
  - If $P_1' \Longrightarrow P_1$ where the sequence of τ-transitions is empty, i.e., $P_1 \Longrightarrow P_1$, then P_2 stays idle, i.e., $P_2 \Longrightarrow P_2$, with the two target processes being related by $\mathcal{B}$.
  - If $P_1' \Longrightarrow P_1$ where the sequence of τ-transitions is not empty, then each such transition is matched according to $\mathcal{B}$ on the side of P_2, hence there exists $P_2' \Longrightarrow P_2$ such that $(P_1', P_2') \in \mathcal{B}$.
  - If $P_1' \Longrightarrow \xrightarrow{\theta_1} \Longrightarrow P_1$ with $act(\theta_1) \neq \tau$, then each transition in the sequence is matched according to $\mathcal{B}$ on the side of P_2, hence there exists $P_2' \Longrightarrow \xrightarrow{\theta_2} \Longrightarrow P_2$ such that $act(\theta_1) = act(\theta_2)$ and $(P_1', P_2') \in \mathcal{B}$.
- Assume that $\mathcal{B}$ satisfies the property stated in the proposition and consider $(P_1, P_2) \in \mathcal{B}$. There are two cases:
  - If $P_1' \xrightarrow{\theta_1} P_1$ with $act(\theta_1) = \tau$, which can be rewritten as $P_1' \Longrightarrow P_1$, then there exists $P_2 \Longrightarrow P_2'$ such that $(P_1', P_2') \in \mathcal{B}$.
  - If $P_1' \xrightarrow{\theta_1} P_1$ with $act(\theta_1) \neq \tau$, which can be rewritten as $P_1' \Longrightarrow P_1' \xrightarrow{\theta_1} P_1 \Longrightarrow P_1$, then there exists $P_2' \Longrightarrow \xrightarrow{\theta_2} \Longrightarrow P_2$ such that $act(\theta_1) = act(\theta_2)$ and $(P_1', P_2') \in \mathcal{B}$. ■

Definition 3.6. *We say that* $P_1, P_2 \in \mathbb{P}$ *are* weakly forward-reverse bisimilar*, written* $P_1 \approx_{\mathrm{FRB}} P_2$*, iff* $(P_1, P_2) \in \mathcal{B}$ *for some weak forward-reverse bisimulation* $\mathcal{B}$*. A symmetric relation* $\mathcal{B}$ *over* $\mathbb{P}$ *is a* weak forward-reverse bisimulation *iff, whenever* $(P_1, P_2) \in \mathcal{B}$*, then:*

- *For each* $P_1 \xrightarrow{\theta_1} P_1'$ *with* $act(\theta_1) = \tau$ *there exists* $P_2 \Longrightarrow P_2'$ *such that* $(P_1', P_2') \in \mathcal{B}$*.*
- *For each* $P_1 \xrightarrow{\theta_1} P_1'$ *with* $act(\theta_1) \neq \tau$ *there exists* $P_2 \Longrightarrow \xrightarrow{\theta_2} \Longrightarrow P_2'$ *such that* $act(\theta_1) = act(\theta_2)$ *and* $(P_1', P_2') \in \mathcal{B}$*.*

- *For each* $P_1' \xrightarrow{\theta_1} P_1$ *with* $act(\theta_1) = \tau$ *there exists* $P_2' \Longrightarrow P_2$ *such that* $(P_1', P_2') \in \mathcal{B}$.
- *For each* $P_1' \xrightarrow{\theta_1} P_1$ *with* $act(\theta_1) \neq \tau$ *there exists* $P_2' \Longrightarrow \xrightarrow{\theta_2} \Longrightarrow P_2$ *such that* $act(\theta_1) = act(\theta_2)$ *and* $(P_1', P_2') \in \mathcal{B}$. ■

Proposition 3.5. *A symmetric relation* $\mathcal{B}$ *over* $\mathbb{P}$ *is a weak forward-reverse bisimulation iff, whenever* $(P_1, P_2) \in \mathcal{B}$, *then:*

- *For each* $P_1 \Longrightarrow P_1'$ *there exists* $P_2 \Longrightarrow P_2'$ *such that* $(P_1', P_2') \in \mathcal{B}$.
- *For each* $P_1 \Longrightarrow \xrightarrow{\theta_1} \Longrightarrow P_1'$ *with* $act(\theta_1) \neq \tau$ *there exists* $P_2 \Longrightarrow \xrightarrow{\theta_2} \Longrightarrow P_2'$ *such that* $act(\theta_1) = act(\theta_2)$ *and* $(P_1', P_2') \in \mathcal{B}$.
- *For each* $P_1' \Longrightarrow P_1$ *there exists* $P_2' \Longrightarrow P_2$ *such that* $(P_1', P_2') \in \mathcal{B}$.
- *For each* $P_1' \Longrightarrow \xrightarrow{\theta_1} \Longrightarrow P_1$ *with* $act(\theta_1) \neq \tau$ *there exists* $P_2' \Longrightarrow \xrightarrow{\theta_2} \Longrightarrow P_2$ *such that* $act(\theta_1) = act(\theta_2)$ *and* $(P_1', P_2') \in \mathcal{B}$.

Proof. It stems from the combination of all the cases in the proofs of Propositions 3.3 and 3.4. ■

Proposition 3.6. *Let* $\approx \in \{\approx_{\rm FB}, \approx_{\rm RB}, \approx_{\rm FRB}\}$. *Then* $\approx$ *is an equivalence relation.*

Proof. See the proof of Proposition 3.1, where Propositions 3.3, 3.4, and 3.5 are exploited to show transitivity via bisimulation composition. ■

Like in the strong case, it is easy to establish two necessary conditions for the three weak bisimilarities considered so far, which respectively make use of weak variants of the forward ready set and the backward ready set; the latter condition will be exploited in Chapter 6 when dealing with expansion laws for parallel composition under weak reverse and forward-reverse semantics. The two sets $frs_{\rm w}(P) \subseteq \mathcal{A} \setminus \{\tau\}$ and $brs_{\rm w}(P) \subseteq \mathcal{A} \setminus \{\tau\}$ are defined as follows for $P \in \mathbb{P}$:

$$\begin{aligned} frs_{\rm w}(P) &= \{a \in \mathcal{A} \setminus \{\tau\} \mid P \Longrightarrow \xrightarrow{\theta} \Longrightarrow P' \wedge act(\theta) = a\} \\ brs_{\rm w}(P) &= \{a \in \mathcal{A} \setminus \{\tau\} \mid P' \Longrightarrow \xrightarrow{\theta} \Longrightarrow P \wedge act(\theta) = a\} \end{aligned}$$

Note that $frs_{\rm w}(P) = frs(P)$ (resp. $brs_{\rm w}(P) = brs(P)$) when P has no unexecuted (resp. executed) actions named τ or changed to τ by some renaming function.

Proposition 3.7. *Let* $P_1, P_2 \in \mathbb{P}$. *Then:*

1. *If* $P_1 \approx P_2$ *for* $\approx \in \{\approx_{\rm FB}, \approx_{\rm FRB}\}$, *then* $frs_{\rm w}(P_1) = frs_{\rm w}(P_2)$.
2. *If* $P_1 \approx P_2$ *for* $\approx \in \{\approx_{\rm RB}, \approx_{\rm FRB}\}$, *then* $brs_{\rm w}(P_1) = brs_{\rm w}(P_2)$.

Proof. A straightforward consequence of the alternative characterizations of the considered equivalences. ■

We observe that $brs_{\rm w}(P)$ can be characterized syntactically. We start by defining over $\mathbb{P}$ a weak variant of predicate *initial* in which executed τ-actions are admitted at the beginning of a process:

$$\begin{array}{rl}
initial_{\rm w}(\underline{0}) & \\
initial_{\rm w}(a\,.\,P') & \text{iff } initial(P') \\
initial_{\rm w}(\tau^\dagger\,.\,P') & \text{iff } initial_{\rm w}(P') \\
initial_{\rm w}(P'\llcorner\rho^\urcorner) & \text{iff } initial_{\rm w}(\rho^\dagger_\tau(P')) \\
initial_{\rm w}(P_1 + P_2) & \text{iff } (initial_{\rm w}(P_1) \wedge initial(P_2)) \vee (initial(P_1) \wedge initial_{\rm w}(P_2)) \\
initial_{\rm w}(P_1 \parallel_L P_2) & \text{iff } initial_{\rm w}(P_1) \wedge initial_{\rm w}(P_2)
\end{array}$$

where $\rho^\dagger_\tau(P)$ is the process obtained from $P \in \mathbb{P}$ by changing to τ all of its executed actions renamed τ by ρ (below symbol $\circ$ denotes the composition of renaming functions):

$$\begin{array}{rcl}
\rho^\dagger_\tau(\underline{0}) & = & \underline{0} \\
\rho^\dagger_\tau(a\,.\,P') & = & a\,.\,\rho^\dagger_\tau(P') \\
\rho^\dagger_\tau(a^\dagger\,.\,P') & = & \left\{\begin{array}{ll} \tau^\dagger\,.\,\rho^\dagger_\tau(P') & \text{if } \rho(a) = \tau \\ a^\dagger\,.\,\rho^\dagger_\tau(P') & \text{if } \rho(a) \neq \tau \end{array}\right. \\
\rho^\dagger_\tau(P'\llcorner\rho'^\urcorner) & = & (\rho \circ \rho')^\dagger_\tau(P') \\
\rho^\dagger_\tau(P_1 + P_2) & = & \rho^\dagger_\tau(P_1) + \rho^\dagger_\tau(P_2) \\
\rho^\dagger_\tau(P_1 \parallel_L P_2) & = & \rho^\dagger_\tau(P_1) \parallel_L \rho^\dagger_\tau(P_2)
\end{array}$$

so that $initial_{\rm w}((a^\dagger\,.\,\underline{0})\llcorner a \mapsto \tau^\urcorner)$, i.e., $initial_{\rm w}(\tau^\dagger\,.\,\underline{0})$, and $initial_{\rm w}(((a_1^\dagger\,.\,\underline{0})\llcorner a_1 \mapsto a^\urcorner \parallel_{\{a\}} (a_2^\dagger\,.\,\underline{0})\llcorner a_2 \mapsto a^\urcorner)\llcorner a \mapsto \tau^\urcorner)$, i.e., $initial_{\rm w}(\tau^\dagger\,.\,\underline{0} \parallel_\emptyset \tau^\dagger\,.\,\underline{0})$, are true. Note that $initial(P)$ implies $initial_{\rm w}(P)$. Then $brs_{\rm w}(P) \subseteq \mathcal{A} \setminus \{\tau\}$ can be inductively characterized as follows:

$$\begin{array}{rcl}
brs_{\rm w}(\underline{0}) & = & \emptyset \\
brs_{\rm w}(a\,.\,P') & = & \emptyset \\
brs_{\rm w}(a^\dagger\,.\,P') & = & \left\{\begin{array}{ll} \{a\} & \text{if } a \neq \tau \wedge initial_{\rm w}(P') \\ brs_{\rm w}(P') & \text{if } a = \tau \vee \neg initial_{\rm w}(P') \end{array}\right. \\
brs_{\rm w}(P'\llcorner\rho^\urcorner) & = & \rho(brs_{\rm w}(\rho^\dagger_\tau(P'))) \\
brs_{\rm w}(P_1 + P_2) & = & \left\{\begin{array}{ll} \emptyset & \text{if } initial(P_1) \wedge initial(P_2) \\ brs_{\rm w}(P_1) & \text{if } \neg initial(P_1) \wedge initial(P_2) \\ brs_{\rm w}(P_2) & \text{if } initial(P_1) \wedge \neg initial(P_2) \end{array}\right. \\
brs_{\rm w}(P_1 \parallel_L P_2) & = & (brs_{\rm w}(P_1) \cap \overline{L}) \cup (brs_{\rm w}(P_2) \cap \overline{L}) \cup (brs_{\rm w}(P_1) \cap brs_{\rm w}(P_2) \cap L)
\end{array}$$

We point out that $initial_{\rm w}$ is used in place of *initial* only in the clause of $brs_{\rm w}$ for executed action prefix. In this way $brs_{\rm w}(a^\dagger\,.\,\tau^\dagger\,.\,\underline{0}) = \{a\}$ because $initial_{\rm w}(\tau^\dagger\,.\,\underline{0})$, otherwise we would have erroneously obtained $\emptyset$ as $\neg initial(\tau^\dagger\,.\,\underline{0})$. We also emphasize the use of $\rho^\dagger_\tau$ in the clause for renaming, thanks to which we derive $brs_{\rm w}((a^\dagger\,.\,b^\dagger\,.\,\underline{0})\llcorner b \mapsto \tau^\urcorner) = brs_{\rm w}(a^\dagger\,.\,\tau^\dagger\,.\,\underline{0}) = \{a\}$ as expected.

We finally observe that a similar characterization for $frs_{\rm w}(P)$ is not possible. For instance, if we defined $\rho_\tau(P)$ as the process obtained from P by changing to τ all of its unexecuted actions renamed τ by ρ, then the deadlocked process $(a\,.\,c \parallel_{\{a,b\}} b\,.\,d)\llcorner a \mapsto \tau, b \mapsto \tau^\urcorner$ would become $(\tau\,.\,c \parallel_{\{a,b\}} \tau\,.\,d)$, which can move instead.

Chapter 4

Discriminating Power and Congruence Property

In this chapter, whose contents have appeared in [27, 25, 29], we compare the discriminating power of the six bisimilarities defined in the previous chapter and investigate whether they are congruences with respect to the operators of PRPC so as to support compositional reasoning, both in the strong case (Section 4.1) and in the weak one (Section 4.2).

4.1 Strong Bisimilarities

It holds that $\sim_{\rm FRB} \subsetneq \sim_{\rm FB} \cap \sim_{\rm RB}$. The inclusion is strict because for example the two processes $a^\dagger . \underline{0}$ and $a^\dagger . \underline{0} + c . \underline{0}$ are identified by $\sim_{\rm FB}$ – as there are no outgoing transitions on both sides – and $\sim_{\rm RB}$ – as there is only one incoming a-transition on both sides – but distinguished by $\sim_{\rm FRB}$ – as in the latter process c is enabled again after undoing a and hence there is one outgoing c-transition in addition to one outgoing a-transition. Moreover, $\sim_{\rm FB}$ and $\sim_{\rm RB}$ are incomparable because for instance:

$$a^\dagger . \underline{0} \sim_{\rm FB} \underline{0} \quad \text{but} \quad a^\dagger . \underline{0} \not\sim_{\rm RB} \underline{0}$$
$$a . \underline{0} \sim_{\rm RB} \underline{0} \quad \text{but} \quad a . \underline{0} \not\sim_{\rm FB} \underline{0}$$

Note that that $\sim_{\rm FRB} = \sim_{\rm FB}$ over initial sequential processes, with $\sim_{\rm RB}$ being strictly coarser as it relates all initial processes, whilst $\sim_{\rm FRB} \neq \sim_{\rm RB}$ over processes with no outgoing transitions (which we may call final) because, after going backward, previously discarded subprocesses come into play again in the forward direction.

In principle, it makes sense that $\sim_{\rm FB}$ identifies processes with a different past and that $\sim_{\rm RB}$ identifies processes with a different future, in particular with $\underline{0}$ that has neither past nor future. However, for $\sim_{\rm FB}$ this results in a compositionality violation with respect to alternative composition. As an example:

$$a^\dagger . b . \underline{0} \sim_{\rm FB} b . \underline{0} \quad \text{but} \quad a^\dagger . b . \underline{0} + c . \underline{0} \not\sim_{\rm FB} b . \underline{0} + c . \underline{0}$$

because in $a^\dagger . b . \underline{0} + c . \underline{0}$ action c is disabled by virtue of the already executed action $a^\dagger$, while in $b . \underline{0} + c . \underline{0}$ action c is enabled as there are no past actions preventing it from occurring. Note that a similar phenomenon does not happen with $\sim_{\rm RB}$ as $a^\dagger . b . \underline{0} \not\sim_{\rm RB} b . \underline{0}$ due to the incoming a-transition of $a^\dagger . b . \underline{0}$. In other words, the insensitivity to the presence of the past breaks the compositionality of $\sim_{\rm FB}$, while the insensitivity to the presence of the future does not violate the compositionality of $\sim_{\rm RB}$.

This problem, which does not show up for $\sim_{\rm RB}$ and $\sim_{\rm FRB}$ because these two equivalences cannot identify an initial process with a non-initial one, leads to the following variant of $\sim_{\rm FB}$ that is sensitive to the presence of the past.

Definition 4.1. *We say that $P_1, P_2 \in \mathbb{P}$ are* past-sensitive forward bisimilar*, written $P_1 \sim_{\mathrm{FB:ps}} P_2$, iff $(P_1, P_2) \in \mathcal{B}$ for some past-sensitive forward bisimulation $\mathcal{B}$. A symmetric relation $\mathcal{B}$ over $\mathbb{P}$ is a* past-sensitive forward bisimulation *iff it is a forward bisimulation such that initial$(P_1) \iff$ initial(P_2) for all $(P_1, P_2) \in \mathcal{B}$.* ■

Proposition 4.1. *$\sim_{\mathrm{FB:ps}}$ is an equivalence relation.*

Proof. See the proof of Proposition 3.1, where the initiality constraint is trivially satisfied by the identity relation as well as bisimulation composition. ■

Since $\sim_{\mathrm{FB:ps}}$ is sensitive to the presence of the past, we have that $a^\dagger . b . \underline{0} \not\sim_{\mathrm{FB:ps}} b . \underline{0}$, but non-initial processes having a different past can still be identified as we will see in a moment. It holds that $\sim_{\mathrm{FRB}} \subsetneq \sim_{\mathrm{FB:ps}} \cap \sim_{\mathrm{RB}}$, with $\sim_{\mathrm{FRB}} = \sim_{\mathrm{FB:ps}}$ over initial sequential processes as well as $\sim_{\mathrm{FB:ps}}$ and $\sim_{\mathrm{RB}}$ being incomparable because, e.g., for $a_1 \neq a_2$:

$$a_1^\dagger . P \sim_{\mathrm{FB:ps}} a_2^\dagger . P \quad \text{but} \quad a_1^\dagger . P \not\sim_{\mathrm{RB}} a_2^\dagger . P$$
$$a_1 . P \sim_{\mathrm{RB}} a_2 . P \quad \text{but} \quad a_1 . P \not\sim_{\mathrm{FB:ps}} a_2 . P$$

We show that all the four strong bisimilarities are congruences with respect to action prefix, renaming, and parallel composition, while only $\sim_{\mathrm{FB:ps}}$, $\sim_{\mathrm{RB}}$, and $\sim_{\mathrm{FRB}}$ are congruences with respect to alternative composition too. Moreover, $\sim_{\mathrm{FB:ps}}$ turns out to be the coarsest congruence with respect to + contained in $\sim_{\mathrm{FB}}$.

Theorem 4.1. *Let $\sim \in \{\sim_{\mathrm{FB}}, \sim_{\mathrm{FB:ps}}, \sim_{\mathrm{RB}}, \sim_{\mathrm{FRB}}\}$, $\sim' \in \{\sim_{\mathrm{FB:ps}}, \sim_{\mathrm{RB}}, \sim_{\mathrm{FRB}}\}$, and $P_1, P_2 \in \mathbb{P}$:*

1. *If $P_1 \sim P_2$ then for all $a \in \mathcal{A}$:*
   - *$a . P_1 \sim a . P_2$ provided that initial$(P_1) \wedge$ initial(P_2).*
   - *$a^\dagger . P_1 \sim a^\dagger . P_2$.*
2. *If $P_1 \sim P_2$ then for all $\rho : \mathcal{A} \to \mathcal{A}$ such that $\rho(\tau) = \tau$:*
   - *$P_1 \llcorner \rho \urcorner \sim P_2 \llcorner \rho \urcorner$.*
3. *If $P_1 \sim' P_2$ then for all $P \in \mathbb{P}$:*
   - *$P_1 + P \sim' P_2 + P$ and $P + P_1 \sim' P + P_2$ provided that initial$(P) \vee$ (initial$(P_1) \wedge$ initial$(P_2))$.*
4. *$P_1 \sim_{\mathrm{FB:ps}} P_2$ iff $P_1 + P \sim_{\mathrm{FB}} P_2 + P$ for all $P \in \mathbb{P}$ such that initial$(P) \vee$ (initial$(P_1) \wedge$ initial$(P_2))$.*
5. *If $P_1 \sim P_2$ then for all $P \in \mathbb{P}$ and $L \subseteq \mathcal{A} \setminus \{\tau\}$:*
   - *$P_1 \parallel_L P \sim P_2 \parallel_L P$ and $P \parallel_L P_1 \sim P \parallel_L P_2$ provided that $P_1 \parallel_L P, P_2 \parallel_L P, P \parallel_L P_1, P \parallel_L P_2 \in \mathbb{P}$.*

Proof. Let $P_1, P_2 \in \mathbb{P}$:

1. Let $P_1 \sim P_2$ and $a \in \mathcal{A}$ and consider a $\sim$-bisimulation $\mathcal{B}$ containing the pair (P_1, P_2). Then:
   $$\mathcal{B}' = \{(a . Q_1, a . Q_2) \mid (Q_1, Q_2) \in \mathcal{B} \wedge \mathit{initial}(Q_1) \wedge \mathit{initial}(Q_2)\} \cup \{(a^\dagger . Q_1, a^\dagger . Q_2) \mid (Q_1, Q_2) \in \mathcal{B}\}$$
   is a $\sim$-bisimulation too (note that $\mathcal{B}$ does not need to be included in $\mathcal{B}'$ as action prefix is a static operator in our reversible setting) because:

- If $\sim$ considers moving forward, then both $a \,.\, Q_1$ and $a \,.\, Q_2$ with $\mathit{initial}(Q_1)$ and $\mathit{initial}(Q_2)$ turn out to have a single outgoing a-transition and these two a-transitions respectively reach $a^\dagger \,.\, Q_1$ and $a^\dagger \,.\, Q_2$, which form a pair of $\mathcal{B}'$.
- Moving backward is not allowed from $a \,.\, Q_1$ and $a \,.\, Q_2$ with $\mathit{initial}(Q_1)$ and $\mathit{initial}(Q_2)$ as they are both initial and hence have no incoming transitions.
- $a^\dagger \,.\, Q_1$ and $a^\dagger \,.\, Q_2$ have $\sim$-matching outgoing/incoming transitions – depending on whether $\sim$ considers moving forward/backward – respectively determined by the two $\sim$-equivalent processes Q_1 and Q_2. In particular, if Q_1 and Q_2 are initial and $\sim$ considers moving backward, then $a^\dagger \,.\, Q_1$ and $a^\dagger \,.\, Q_2$ turn out to have a single incoming a-transition and these two a-transitions respectively depart from $a \,.\, Q_1$ and $a \,.\, Q_2$, which form a pair of $\mathcal{B}'$.

Therefore $a \,.\, P_1 \sim a \,.\, P_2$, provided that $\mathit{initial}(P_1) \wedge \mathit{initial}(P_2)$, as well as $a^\dagger \,.\, P_1 \sim a^\dagger \,.\, P_2$.

2. Let $P_1 \sim P_2$ and $\rho : \mathcal{A} \to \mathcal{A}$ be such that $\rho(\tau) = \tau$ and consider a $\sim$-bisimulation $\mathcal{B}$ containing the pair (P_1, P_2). Then:
$$\mathcal{B}' \;=\; \{(Q_1 \llcorner \rho \lrcorner, Q_2 \llcorner \rho \lrcorner) \mid (Q_1, Q_2) \in \mathcal{B}\}$$
is a $\sim$-bisimulation too because the $\sim$-matching transitions of Q_1 and Q_2 are trivially preserved by ρ. Therefore $P_1 \llcorner \rho \lrcorner \sim P_2 \llcorner \rho \lrcorner$.

3. Let $P_1 \sim' P_2$ and $P \in \mathbb{P}$ and consider a $\sim'$-bisimulation $\mathcal{B}$ containing the pair (P_1, P_2). Then:
$$\mathcal{B}' \;=\; \{(Q_1 + Q, Q_2 + Q) \mid (Q_1, Q_2) \in \mathcal{B} \wedge (\mathit{initial}(Q) \vee (\mathit{initial}(Q_1) \wedge \mathit{initial}(Q_2)))\}$$
is a $\sim'$-bisimulation too (note that $\mathcal{B}$ does not need to be included in $\mathcal{B}'$ as alternative composition is a static operator in our reversible setting) because $Q_1 + Q$ and $Q_2 + Q$ have $\sim'$-matching outgoing/incoming transitions – depending on whether $\sim'$ considers moving forward/backward – determined by the two $\sim'$-equivalent processes Q_1 and Q_2 when $\mathit{initial}(Q)$ or by Q when $\mathit{initial}(Q_1) \wedge \mathit{initial}(Q_2)$. Note that in the forward case, since from $(Q_1, Q_2) \in \mathcal{B}$ it follows that $\mathit{initial}(Q_1) \iff \mathit{initial}(Q_2)$, when $\mathit{initial}(Q)$ all the initial actions of Q are enabled both in $Q_1 + Q$ and in $Q_2 + Q$ if $\mathit{initial}(Q_1) \wedge \mathit{initial}(Q_2)$ or in neither of them if $\neg\mathit{initial}(Q_1) \wedge \neg\mathit{initial}(Q_2)$.
Therefore $P_1 + P \sim' P_2 + P$ provided that $\mathit{initial}(P) \vee (\mathit{initial}(P_1) \wedge \mathit{initial}(P_2))$.
The proof that $P + P_1 \sim' P + P_2$ is similar because the two operational semantic rules for alternative composition in Table 2.1 are symmetric.

4. If $P_1 \sim_{\mathrm{FB:ps}} P_2$ then, based on what we have proved above, $P_1 + P \sim_{\mathrm{FB:ps}} P_2 + P$ for all $P \in \mathbb{P}$ such that $\mathit{initial}(P) \vee (\mathit{initial}(P_1) \wedge \mathit{initial}(P_2))$ – so that $\mathit{initial}(P_1 + P) \iff \mathit{initial}(P_2 + P)$ is satisfied – and hence $P_1 + P \sim_{\mathrm{FB}} P_2 + P$ because $\sim_{\mathrm{FB:ps}} \subsetneq \sim_{\mathrm{FB}}$.
As for the reverse implication, we reason on the contrapositive. If $P_1 \not\sim_{\mathrm{FB:ps}} P_2$ there are two cases:

- If P_1 and P_2 have no matching outgoing transitions, then $P_1 + \underline{0}$ and $P_2 + \underline{0}$, where $\mathit{initial}(\underline{0})$, have no matching outgoing transitions either, hence $P_1 + \underline{0} \not\sim_{\mathrm{FB}} P_2 + \underline{0}$.
- If $\mathit{initial}(P_1) \iff \mathit{initial}(P_2)$ does not hold, say $\neg\mathit{initial}(P_1)$ and $\mathit{initial}(P_2)$, then, even if P_1 and P_2 have matching outgoing transitions, it turns out that $P_1 + c \,.\, \underline{0} \not\sim_{\mathrm{FB}} P_2 + c \,.\, \underline{0}$, where $\mathit{initial}(c \,.\, \underline{0})$ and c is an action occurring neither in P_1 nor in P_2, because $P_2 + c \,.\, \underline{0}$ has an outgoing c-transition whilst $P_1 + c \,.\, \underline{0}$ has not.

5. Let $P_1 \sim P_2$, $P \in \mathbb{P}$, and $L \subseteq \mathcal{A} \setminus \{\tau\}$ and consider a $\sim$-bisimulation $\mathcal{B}$ containing the pair (P_1, P_2). Then:
$$\mathcal{B}' = \{(Q_1 \parallel_L Q, Q_2 \parallel_L Q) \mid (Q_1, Q_2) \in \mathcal{B} \wedge Q_1 \parallel_L Q, Q_2 \parallel_L Q \in \mathbb{P}\}$$
is a $\sim$-bisimulation too because $Q_1 \parallel_L Q$ and $Q_2 \parallel_L Q$ have $\sim$-matching outgoing/incoming transitions – depending on whether $\sim$ considers moving forward/backward – determined by the two $\sim$-equivalent processes Q_1 and Q_2 or by Q, both when moving independent of each other and when synchronizing on an action in L. Note that if $\mathit{initial}(Q_1) \iff \mathit{initial}(Q_2)$, then $\mathit{initial}(Q_1 \parallel_L Q) \iff \mathit{initial}(Q_2 \parallel_L Q)$.
Therefore $P_1 \parallel_L P \sim P_2 \parallel_L P$ provided that $P_1 \parallel_L P, P_2 \parallel_L P \in \mathbb{P}$.
The proof that $P \parallel_L P_1 \sim P \parallel_L P_2$ is similar because the three operational semantic rules for parallel composition in Table 2.1 are symmetric. ■

4.2 Weak Bisimilarities

Each of the three weak bisimilarities is strictly coarser than the corresponding strong one. Similar to the strong case, $\approx_{\mathrm{FRB}} \subsetneq \approx_{\mathrm{FB}} \cap \approx_{\mathrm{RB}}$ with $\approx_{\mathrm{FB}}$ and $\approx_{\mathrm{RB}}$ being incomparable. Unlike the strong case, $\approx_{\mathrm{FRB}} \neq \approx_{\mathrm{FB}}$ over initial sequential processes. For instance, $\tau.a.\underline{0} + a.\underline{0} + b.\underline{0}$ and $\tau.a.\underline{0} + b.\underline{0}$ are identified by $\approx_{\mathrm{FB}}$ but told apart by $\approx_{\mathrm{FRB}}$: if the former performs a, the latter responds with τ followed by a and if it subsequently undoes a thus becoming $\tau^\dagger.a.\underline{0} + b.\underline{0}$ in which only a is enabled, the latter can only respond by undoing a thus becoming $\tau.a.\underline{0} + a.\underline{0} + b.\underline{0}$ in which both a and b are enabled. An analogous counterexample with non-initial τ-actions is given by $c.(\tau.a.\underline{0} + a.\underline{0} + b.\underline{0})$ and $c.(\tau.a.\underline{0} + b.\underline{0})$.

As for compositionality, we observe that $\approx_{\mathrm{FB}}$ suffers from the same problem with respect to alternative composition as $\sim_{\mathrm{FB}}$. Moreover, $\approx_{\mathrm{FB}}$ and $\approx_{\mathrm{FRB}}$ feature the same problem as weak bisimilarity for forward-only processes [112], i.e., for $\approx \in \{\approx_{\mathrm{FB}}, \approx_{\mathrm{FRB}}\}$ it holds that:
$$\tau.a.\underline{0} \approx a.\underline{0} \quad \text{but} \quad \tau.a.\underline{0} + b.\underline{0} \not\approx a.\underline{0} + b.\underline{0}$$
because if $\tau.a.\underline{0} + b.\underline{0}$ performs τ thereby evolving to $\tau^\dagger.a.\underline{0} + b.\underline{0}$ where only a is enabled in the forward direction, then $a.\underline{0} + b.\underline{0}$ can neither idle nor move in the attempt to match $\tau^\dagger.a.\underline{0} + b.\underline{0}$.

To solve both problems it is sufficient to redefine the two equivalences by making them sensitive to the presence of the past, exactly like in the strong case for forward bisimilarity. By so doing, $\tau.a.\underline{0}$ is no longer identified with $a.\underline{0}$: if the former performs τ thereby evolving to $\tau^\dagger.a.\underline{0}$ and the latter idles, then $\tau^\dagger.a.\underline{0}$ and $a.\underline{0}$ are told apart because the latter is initial while the former is not.

Definition 4.2. *We say that $P_1, P_2 \in \mathbb{P}$ are* weakly past-sensitive forward bisimilar*, written $P_1 \approx_{\mathrm{FB:ps}} P_2$, iff $(P_1, P_2) \in \mathcal{B}$ for some weak past-sensitive forward bisimulation $\mathcal{B}$. A symmetric relation $\mathcal{B}$ over $\mathbb{P}$ is a* weak past-sensitive forward bisimulation *iff it is a weak forward bisimulation such that $\mathit{initial}(P_1) \iff \mathit{initial}(P_2)$ for all $(P_1, P_2) \in \mathcal{B}$.* ■

Definition 4.3. *We say that $P_1, P_2 \in \mathbb{P}$ are* weakly past-sensitive forward-reverse bisimilar*, written $P_1 \approx_{\mathrm{FRB:ps}} P_2$, iff $(P_1, P_2) \in \mathcal{B}$ for some weak past-sensitive forward-reverse bisimulation $\mathcal{B}$. A symmetric relation $\mathcal{B}$ over $\mathbb{P}$ is a* weak past-sensitive forward-reverse bisimulation *iff it is a weak forward-reverse bisimulation such that $\mathit{initial}(P_1) \iff \mathit{initial}(P_2)$ for all $(P_1, P_2) \in \mathcal{B}$.* ■

Proposition 4.2. *Let $\approx \in \{\approx_{\mathrm{FB:ps}}, \approx_{\mathrm{FRB:ps}}\}$. Then $\approx$ is an equivalence relation.*

Proof. See the proof of Propositions 3.6 and 4.1. ■

Note that $\sim_{\mathrm{FRB}} \subsetneq \approx_{\mathrm{FRB:ps}}$ as the former naturally satisfies the initiality condition, while $\sim_{\mathrm{FB}}$ and $\approx_{\mathrm{FB:ps}}$ are incomparable because $a^\dagger . \underline{0}$ and $\underline{0}$ are identified by $\sim_{\mathrm{FB}}$ and told apart by $\approx_{\mathrm{FB:ps}}$ but $a . \tau . \underline{0}$ and $a . \underline{0}$ are identified by $\approx_{\mathrm{FB:ps}}$ and told apart by $\sim_{\mathrm{FB}}$. Like in the non-past-sensitive case, $\approx_{\mathrm{FRB:ps}} \neq \approx_{\mathrm{FB:ps}}$ over initial sequential processes, as shown by $\tau . a . \underline{0} + a . \underline{0}$ and $\tau . a . \underline{0}$: if the former performs a, the latter responds with τ followed by a and if it subsequently undoes a thus becoming the non-initial process $\tau^\dagger . a . \underline{0}$, the latter can only respond by undoing a thus becoming the initial process $\tau . a . \underline{0} + a . \underline{0}$. An analogous counterexample with non-initial τ-actions is given again by $c . (\tau . a . \underline{0} + a . \underline{0} + b . \underline{0})$ and $c . (\tau . a . \underline{0} + b . \underline{0})$.

We show that all the five weak bisimilarities are congruences with respect to action prefix, renaming, and parallel composition, while only $\approx_{\mathrm{FB:ps}}$, $\approx_{\mathrm{RB}}$, and $\approx_{\mathrm{FRB:ps}}$ are congruences with respect to alternative composition too. Moreover, $\approx_{\mathrm{FB:ps}}$ and $\approx_{\mathrm{FRB:ps}}$ turn out to be the coarsest congruences with respect to $+$ respectively contained in $\approx_{\mathrm{FB}}$ and $\approx_{\mathrm{FRB}}$.

Theorem 4.2. *Let* $\approx \in \{\approx_{\mathrm{FB}}, \approx_{\mathrm{FB:ps}}, \approx_{\mathrm{RB}}, \approx_{\mathrm{FRB}}, \approx_{\mathrm{FRB:ps}}\}$, $\approx' \in \{\approx_{\mathrm{FB:ps}}, \approx_{\mathrm{RB}}, \approx_{\mathrm{FRB:ps}}\}$, *and* $P_1, P_2 \in \mathbb{P}$*:*

1. *If* $P_1 \approx P_2$ *then for all* $a \in \mathcal{A}$*:*
   - $a . P_1 \approx a . P_2$ *provided that* $\mathit{initial}(P_1) \wedge \mathit{initial}(P_2)$.
   - $a^\dagger . P_1 \approx a^\dagger . P_2$.
2. *If* $P_1 \approx P_2$ *then for all* $\rho : \mathcal{A} \to \mathcal{A}$ *such that* $\rho(\tau) = \tau$*:*
   - $P_1 \llcorner \rho \urcorner \approx P_2 \llcorner \rho \urcorner$.
3. *If* $P_1 \approx' P_2$ *then for all* $P \in \mathbb{P}$*:*
   - $P_1 + P \approx' P_2 + P$ *and* $P + P_1 \approx' P + P_2$ *provided that* $\mathit{initial}(P) \vee (\mathit{initial}(P_1) \wedge \mathit{initial}(P_2))$.
4. $P_1 \approx_{\mathrm{FB:ps}} P_2$ *iff* $P_1 + P \approx_{\mathrm{FB}} P_2 + P$ *for all* $P \in \mathbb{P}$ *such that* $\mathit{initial}(P) \vee (\mathit{initial}(P_1) \wedge \mathit{initial}(P_2))$.
5. $P_1 \approx_{\mathrm{FRB:ps}} P_2$ *iff* $P_1 + P \approx_{\mathrm{FRB}} P_2 + P$ *for all* $P \in \mathbb{P}$ *such that* $\mathit{initial}(P) \vee (\mathit{initial}(P_1) \wedge \mathit{initial}(P_2))$.
6. *If* $P_1 \approx P_2$ *then for all* $P \in \mathbb{P}$ *and* $L \subseteq \mathcal{A} \setminus \{\tau\}$*:*
   - $P_1 \parallel_L P \approx P_2 \parallel_L P$ *and* $P \parallel_L P_1 \approx P \parallel_L P_2$ *provided that* $P_1 \parallel_L P, P_2 \parallel_L P, P \parallel_L P_1, P \parallel_L P_2 \in \mathbb{P}$.

Proof. See the proof of Theorem 4.1, where:

- In the case of the renaming operator, $\approx$-matching transitions of Q_1 and Q_2 are preserved by ρ even when their labels are turned into τ.
- In the proof of the two coarsest congruence results, we take $c \neq \tau$. ∎

We conclude by noting that the aforementioned compositionality problems with respect to alternative composition may not be solved, in our reversible setting, by employing the construction of [112] for building a weak bisimulation congruence on top of weak bisimilarity over forward-only processes. In particular, if we introduced a variant $\approx'_{\rm FB}$ of $\approx_{\rm FB}$ such that, given two processes related by $\approx'_{\rm FB}$, a τ-transition on either side must be matched by a τ-transition on the other side with the two reached processes being related by $\approx_{\rm FB}$, then again $a^\dagger . b . \underline{0} \approx'_{\rm FB} b . \underline{0}$ but $a^\dagger . b . \underline{0} + c . \underline{0} \not\approx'_{\rm FB} b . \underline{0} + c . \underline{0}$. It is therefore essential to keep initial processes separate from non-initial ones to achieve compositionality.

However, the construction of [112] can be adapted to our reversible setting, a fact that will be exploited in the proof of the forthcoming Theorem 6.10. In the case of two initial processes, every transition of either process must be matched by a transition of the other process labeled with the same action, with the two reached non-initial processes being related by $\approx_B$ for $B \in \{\rm FB, FRB\}$. In the case of two non-initial processes, in addition to requiring them to be $\approx_B$-equivalent, we may have to make sure that their initial versions are equivalent in the sense above. Let us define function $to\_initial : \mathbb{P} \to \mathbb{P}_{\rm init}$ by induction on the syntactical structure of $P \in \mathbb{P}$ as follows:

$$\begin{array}{rcll} to\_initial(P) & = & P & \text{if } initial(P) \\ to\_initial(a^\dagger . P') & = & a . to\_initial(P') & \\ to\_initial(P' \llcorner \rho \urcorner) & = & to\_initial(P') \llcorner \rho \urcorner & \text{if } \neg initial(P') \\ to\_initial(P_1 + P_2) & = & to\_initial(P_1) + to\_initial(P_2) & \text{if } \neg initial(P_1) \vee \neg initial(P_2) \\ to\_initial(P_1 \parallel_L P_2) & = & to\_initial(P_1) \parallel_L to\_initial(P_2) & \text{if } \neg initial(P_1) \vee \neg initial(P_2) \end{array}$$

For instance, the two non-initial processes $\tau^\dagger . a^\dagger . \underline{0}$ and $a^\dagger . \underline{0}$ are identified by $\approx_{\rm FRB}$, but $to\_initial(\tau^\dagger . a^\dagger . \underline{0}) = \tau . a . \underline{0} \not\approx_{\rm FRB:ps} a . \underline{0} = to\_initial(a^\dagger . \underline{0})$, hence $\tau^\dagger . a^\dagger . \underline{0} \not\approx_{\rm FRB:ps} a^\dagger . \underline{0}$ either. On the other hand, it is not enough to guarantee that their initial versions are equivalent. For example, $to\_initial(a^\dagger . b . \underline{0}) = a . b . \underline{0} = to\_initial(a^\dagger . b^\dagger . \underline{0})$ but $a^\dagger . b . \underline{0} \not\approx_{\rm FRB} a^\dagger . b^\dagger . \underline{0}$.

Definition 4.4. *We say that $P_1, P_2 \in \mathbb{P}$ are* weakly forward (resp. forward-reverse) bisimulation congruent*, written $P_1 \approx_{B:\rm c} P_2$ for $B \in \{\rm FB, FRB\}$, iff one of the following two clauses holds:*

- *P_1 and P_2 are both initial and for all $P_1 \xrightarrow{\theta_1} P'_1$ there exists $P_2 \xrightarrow{\theta_2} P'_2$ such that $act(\theta_1) = act(\theta_2)$ and $P'_1 \approx_B P'_2$, and vice versa.*
- *P_1 and P_2 are both non-initial, $P_1 \approx_B P_2$, and – when $B = \rm FRB$ – $to\_initial(P_1) \approx_{B:\rm c} to\_initial(P_2)$.* ■

Theorem 4.3. *Let $P_1, P_2 \in \mathbb{P}$ and $B \in \{\rm FB, FRB\}$. Then $P_1 \approx_{B:\rm c} P_2$ iff $P_1 \approx_{B:\rm ps} P_2$.*

Proof. The proof is divided into two parts:

- Suppose that $P_1 \approx_{B:\rm c} P_2$. There are two cases:
  - If P_1 and P_2 are initial, then for all $P_1 \xrightarrow{\theta_1} P'_1$ there exists $P_2 \xrightarrow{\theta_2} P'_2$ such that $act(\theta_1) = act(\theta_2)$ and $P'_1 \approx_B P'_2$, and vice versa. For $B = \rm FB$ this is enough to conclude that $P_1 \approx_{B:\rm ps} P_2$, while for $B = \rm FRB$ it stems from all those P'_1 and P'_2 being $\approx_B$-equivalent non-initial processes whose only incoming transitions are labeled with the same action and respectively depart from the two initial processes P_1 and P_2 (hence $P'_1 \approx_{B:\rm ps} P'_2$ for all those pairs).
  - If P_1 and P_2 are not initial, then $P_1 \approx_B P_2$ and $to\_initial(P_1) \approx_{B:\rm c} to\_initial(P_2)$. While stepwise mimicking each other's behavior in the forward direction, P_1 and P_2 can only encounter pairs of non-initial processes related by $\approx_B$. For $B = \rm FRB$, by virtue of $to\_initial(P_1) \approx_{B:\rm c} to\_initial(P_2)$, while

stepwise mimicking each other's behavior in the backward direction, there is a way for P_1 and P_2 not to respectively end up in an initial process and a non-initial process. In conclusion, $P_1 \approx_{B:\mathrm{ps}} P_2$.

- Suppose that $P_1 \approx_{B:\mathrm{ps}} P_2$. There are two cases:
  - If P_1 and P_2 are initial, whenever P_1 has a τ-transition to a non-initial process that is $\approx_B$-equivalent to P_2, then P_2 must have a τ-transition to a non-initial process that is $\approx_B$-equivalent to P_1, and vice versa, otherwise $P_1 \approx_{B:\mathrm{ps}} P_2$ could not hold. Therefore, for all $P_1 \xrightarrow{\theta_1} P_1'$ there exists $P_2 \xrightarrow{\theta_2} P_2'$ such that $act(\theta_1) = act(\theta_2)$ and $P_1' \approx_B P_2'$, and vice versa, i.e., $P_1 \approx_{B:\mathrm{c}} P_2$.
  - Let P_1 and P_2 be not initial. On the one hand, we have that $P_1 \approx_{B:\mathrm{ps}} P_2$ implies $P_1 \approx_B P_2$. On the other hand, when $B = \mathrm{FRB}$, from $P_1 \approx_{B:\mathrm{ps}} P_2$ it follows that, while stepwise mimicking each other's behavior in the backward direction, there is a way for P_1 and P_2 not to respectively end up in an initial process and a non-initial process. Therefore $to\_initial(P_1) \approx_{B:\mathrm{ps}} to\_initial(P_2)$ and hence $to\_initial(P_1) \approx_{B:\mathrm{c}} to\_initial(P_2)$ due to what we have shown in the previous case. In conclusion, $P_1 \approx_{B:\mathrm{c}} P_2$. ■

Chapter 5

Modal Logic Characterizations

In this chapter, whose contents have appeared in [26, 29], after introducing a general modal logic with forward and backward modalities (Section 5.1), we exhibit fragments of that modal logic (see the forthcoming Table 5.1) that characterize the three strong bisimilarities $\sim_{\mathrm{FB}}$, $\sim_{\mathrm{RB}}$, $\sim_{\mathrm{FRB}}$, the three weak bisimilarities $\approx_{\mathrm{FB}}$, $\approx_{\mathrm{RB}}$, $\approx_{\mathrm{FRB}}$, and the three past-sensitive variants $\sim_{\mathrm{FB:ps}}$, $\approx_{\mathrm{FB:ps}}$, $\approx_{\mathrm{FRB:ps}}$ (Section 5.2). These characterizations show what properties are preserved by each bisimilarity and are useful to provide diagnostic information, in the form of distinguishing formulas, that explains why two processes are not bisimilar.

5.1 A Modal Logic with Forward and Backward Modalities

We start by presenting a general modal logic $\mathcal{L}$ from which we will take nine fragments to characterize the nine aforementioned bisimilarities. It consists of Hennessy-Milner logic [88] – which includes true, negation, conjunction, and modality $\langle a \rangle$ representing the possibility of performing a – extended with the proposition init, the strong backward modality $\langle a^\dagger \rangle$, the two weak forward modalities $\langle\!\langle \tau \rangle\!\rangle$ and $\langle\!\langle a \rangle\!\rangle$, and the two weak backward modalities $\langle\!\langle \tau^\dagger \rangle\!\rangle$ and $\langle\!\langle a^\dagger \rangle\!\rangle$, where $a \neq \tau$ within weak modalities. The syntax of its formulas is the following:

$$\phi ::= \mathsf{true} \mid \mathsf{init} \mid \neg\phi \mid \phi \wedge \phi \mid \langle a \rangle \phi \mid \langle a^\dagger \rangle \phi \mid \langle\!\langle \tau \rangle\!\rangle \phi \mid \langle\!\langle a \rangle\!\rangle \phi \mid \langle\!\langle \tau^\dagger \rangle\!\rangle \phi \mid \langle\!\langle a^\dagger \rangle\!\rangle \phi$$

The satisfaction relation $\models \subseteq \mathbb{P} \times \mathcal{L}$ is defined by induction on the syntactical structure of $\phi \in \mathcal{L}$ as follows:

$$\begin{array}{lll}
P \models \mathsf{true} & & \\
P \models \mathsf{init} & \text{iff} & \mathit{initial}(P) \\
P \models \neg\phi' & \text{iff} & P \not\models \phi' \\
P \models \phi_1 \wedge \phi_2 & \text{iff} & P \models \phi_1 \text{ and } P \models \phi_2 \\
P \models \langle a \rangle \phi' & \text{iff} & \text{there exists } P \xrightarrow{\theta} P' \text{ such that } \mathit{act}(\theta) = a \text{ and } P' \models \phi' \\
P \models \langle a^\dagger \rangle \phi' & \text{iff} & \text{there exists } P' \xrightarrow{\theta} P \text{ such that } \mathit{act}(\theta) = a \text{ and } P' \models \phi' \\
P \models \langle\!\langle \tau \rangle\!\rangle \phi' & \text{iff} & \text{there exists } P \Longrightarrow P' \text{ such that } P' \models \phi' \\
P \models \langle\!\langle a \rangle\!\rangle \phi' & \text{iff} & \text{there exists } P \Longrightarrow \xrightarrow{\theta} \Longrightarrow P' \text{ such that } \mathit{act}(\theta) = a \text{ and } P' \models \phi' \\
P \models \langle\!\langle \tau^\dagger \rangle\!\rangle \phi' & \text{iff} & \text{there exists } P' \Longrightarrow P \text{ such that } P' \models \phi' \\
P \models \langle\!\langle a^\dagger \rangle\!\rangle \phi' & \text{iff} & \text{there exists } P' \Longrightarrow \xrightarrow{\theta} \Longrightarrow P \text{ such that } \mathit{act}(\theta) = a \text{ and } P' \models \phi'
\end{array}$$

Derived operators can be considered too, like false defined as $\neg\mathsf{true}$, $\phi_1 \vee \phi_2$ defined as $\neg(\neg\phi_1 \wedge \neg\phi_2)$, $[a]\phi$ defined as $\neg\langle a \rangle \neg\phi$, and so on. Note that every $P \in \mathbb{P}$ is *image finite*, i.e., it has finitely many outgoing transitions labeled with proof terms containing the same action.

	true	init	$\neg$	$\wedge$	$\langle a \rangle$	$\langle a^\dagger \rangle$	$\langle\langle \tau \rangle\rangle$	$\langle\langle a \rangle\rangle$	$\langle\langle \tau^\dagger \rangle\rangle$	$\langle\langle a^\dagger \rangle\rangle$
$\mathcal{L}_{\mathrm{FB}}$	✓		✓	✓	✓					
$\mathcal{L}_{\mathrm{FB:ps}}$	✓	✓	✓	✓	✓					
$\mathcal{L}_{\mathrm{RB}}$	✓		✓	✓		✓				
$\mathcal{L}_{\mathrm{FRB}}$	✓		✓	✓	✓	✓				
$\mathcal{L}^{\tau}_{\mathrm{FB}}$	✓		✓	✓			✓	✓		
$\mathcal{L}^{\tau}_{\mathrm{FB:ps}}$	✓	✓	✓	✓			✓	✓		
$\mathcal{L}^{\tau}_{\mathrm{RB}}$	✓		✓	✓					✓	✓
$\mathcal{L}^{\tau}_{\mathrm{FRB}}$	✓		✓	✓			✓	✓	✓	✓
$\mathcal{L}^{\tau}_{\mathrm{FRB:ps}}$	✓	✓	✓	✓			✓	✓	✓	✓

Table 5.1: Fragments of $\mathcal{L}$ characterizing the nine bisimilarities

The use of backward operators is not new in the definition of properties of programs through temporal logics [109] or modal logics [89]. In particular, in the latter work a logic with a past operator was introduced to capture interesting properties of generalized labeled transition systems where only observable actions are considered. In that setting it was proven that the equivalence induced by the considered logic coincides with a generalization of the strong bisimilarity of [112]. This result was later confirmed in [58] by showing that the addition of a strong backward modality – interpreted over computation paths instead of states – provides no additional discriminating power with respect to Hennessy-Milner logic, i.e., the induced equivalence is again the strong bisimilarity of [112].

In contrast, we have seen that the strong forward bisimilarities $\sim_{\mathrm{FB}}$ and $\sim_{\mathrm{FB:ps}}$ do not coincide with the strong forward-reverse bisimilarity $\sim_{\mathrm{FRB}}$ and this extends to their weak counterparts. Therefore, in our context – in which all the equivalences are defined over states – the presence of backward modalities matters. It is worth noting that our two weak backward modalities are similar to the ones considered in [57, 58] to characterize weak back-and-forth bisimilarity defined over computation paths.

5.2 Fragments Characterizing the Nine Bisimilarities

We can characterize all the nine bisimilarities defined in the two previous chapters by taking suitable fragments of $\mathcal{L}$. For each of the four strong bisimilarities $\sim_B$, where $B \in \{\mathrm{FB}, \mathrm{FB{:}ps}, \mathrm{RB}, \mathrm{FRB}\}$, we denote the corresponding logic by $\mathcal{L}_B$. We proceed similarly for each of the five weak bisimilarities $\approx_B$, where $B \in \{\mathrm{FB}, \mathrm{FB{:}ps}, \mathrm{RB}, \mathrm{FRB}, \mathrm{FRB{:}ps}\}$, to obtain the corresponding logic $\mathcal{L}^{\tau}_B$. The nine fragments are listed in Table 5.1, which indicates that true, negation, and conjunction are common to all fragments, while the proposition init is needed only for the three past-sensitive bisimilarities. We now show that each such fragment induces the intended bisimilarity, in the sense that two processes are bisimilar iff they satisfy the same set of formulas in the corresponding fragment.

The proof technique that we use is inspired by the one employed in [2] to demonstrate that Hennessy-Milner logic characterizes the strong bisimilarity for forward-only processes of [112]. To prove that any two bisimilar processes P_1 and P_2 satisfy the same formulas of the considered fragment, we assume that $P_1 \models \phi$ for an arbitrary formula ϕ and then we show that $P_2 \models \phi$ too by induction on the depth of ϕ, where the depth of $\phi \in \mathcal{L}$ – intended as an upper bound to the depth of the syntax tree of the formula – is defined by induction on the syntactical structure of ϕ as follows:

$$\begin{aligned} depth(\mathsf{true}) = depth(\mathsf{init}) &= 0 \\ depth(\neg\phi') &= 1 + depth(\phi') \\ depth(\phi_1 \wedge \phi_2) &= 1 + \max(depth(\phi_1), depth(\phi_2)) \\ depth(\langle a \rangle \phi') = depth(\langle a^\dagger \rangle \phi') &= 1 + depth(\phi') \\ depth(\langle\!\langle \tau \rangle\!\rangle \phi') = depth(\langle\!\langle a \rangle\!\rangle \phi') = depth(\langle\!\langle \tau^\dagger \rangle\!\rangle \phi') = depth(\langle\!\langle a^\dagger \rangle\!\rangle \phi') &= 1 + depth(\phi') \end{aligned}$$

As for the reverse implication, we show that the relation $\mathcal{B}$ formed by all pairs of processes (P_1, P_2) that satisfy the same formulas of the considered fragment is a bisimulation. More specifically, starting from $(P_1, P_2) \in \mathcal{B}$ we assume by contradiction that, whenever P_1 has a strong/weak a-transition to/from P_1', then there is no P_2' such that P_2 has a strong/weak a-transition to/from P_2' with $(P_1', P_2') \in \mathcal{B}$, i.e., satisfying the same formulas as P_1'. This entails that, for every $P_{2,i}$ forward/backward reachable from P_2 via a strong/weak a-transition, by definition of $\mathcal{B}$ there exists some formula ϕ_i such that $P_1' \models \phi_i$ and $P_{2,i}' \not\models \phi_i$, which leads to a formula with a strong/weak forward/backward modality on a followed by $\bigwedge_i \phi_i$ that is satisfied by P_1 but not by P_2, thereby contradicting $(P_1, P_2) \in \mathcal{B}$.

Theorem 5.1. *Let $P_1, P_2 \in \mathbb{P}$ and $B \in \{\mathrm{FB}, \mathrm{FB{:}ps}, \mathrm{RB}, \mathrm{FRB}\}$. Then $P_1 \sim_B P_2$ iff $\forall \phi \in \mathcal{L}_B.\, P_1 \models \phi \iff P_2 \models \phi$.*

Proof. We consider each of the four strong bisimilarities in turn:

- Let $B = \mathrm{FB}$. The proof is divided into two parts:
  - Assuming that $P_1 \sim_{\mathrm{FB}} P_2$ and $P_1 \models \phi$ for an arbitrary formula $\phi \in \mathcal{L}_{\mathrm{FB}}$, we prove that $P_2 \models \phi$ too by proceeding by induction on $k = depth(\phi)$:
    - If $k = 0$ then ϕ must be true, which is trivially satisfied by P_2 too.
    - If $k \geq 1$ there are three cases:
      - If ϕ is $\neg\phi'$ then from $P_1 \models \neg\phi'$ we derive that $P_1 \not\models \phi'$. If it were $P_2 \models \phi'$ then by the induction hypothesis it would hold that $P_1 \models \phi'$, which is not the case. Therefore $P_2 \not\models \phi'$ and hence $P_2 \models \neg\phi'$ too.
      - If ϕ is $\phi_1 \wedge \phi_2$ then from $P_1 \models \phi_1 \wedge \phi_2$ we derive that $P_1 \models \phi_1$ and $P_1 \models \phi_2$. From the induction hypothesis it follows that $P_2 \models \phi_1$ and $P_2 \models \phi_2$ and hence $P_2 \models \phi_1 \wedge \phi_2$ too.
      - If ϕ is $\langle a \rangle \phi'$ then from $P_1 \models \langle a \rangle \phi'$ we derive that there exists $P_1 \xrightarrow{\theta_1} P_1'$ such that $act(\theta_1) = a$ and $P_1' \models \phi'$. From $P_1 \sim_{\mathrm{FB}} P_2$ it then follows that there exists $P_2 \xrightarrow{\theta_2} P_2'$ such that $act(\theta_2) = a$ and $P_1' \sim_{\mathrm{FB}} P_2'$. By applying the induction hypothesis we derive that $P_2' \models \phi'$ and hence $P_2 \models \langle a \rangle \phi'$ too.
  - Assuming that P_1 and P_2 satisfy the same formulas in $\mathcal{L}_{\mathrm{FB}}$, we prove that the symmetric relation $\mathcal{B} = \{(Q_1, Q_2) \in \mathbb{P} \times \mathbb{P} \mid Q_1 \text{ and } Q_2 \text{ satisfy the same formulas in } \mathcal{L}_{\mathrm{FB}}\}$ is a forward bisimulation.

    Given $(Q_1, Q_2) \in \mathcal{B}$ such that $Q_1 \xrightarrow{\theta_1} Q_1'$, suppose by contradiction that there is no Q_2' satisfying the same formulas as Q_1' such that $Q_2 \xrightarrow{\theta_2} Q_2'$ and $act(\theta_1) = act(\theta_2)$, i.e., $(Q_1', Q_2') \in \mathcal{B}$ for no Q_2' $act(\theta_1)$-reachable from Q_2. Since Q_2 has finitely many outgoing transitions, the set of processes that Q_2 can reach by performing an $act(\theta_1)$-transition is finite, say $\{Q_{2,1}', \ldots, Q_{2,n}'\}$ with $n \geq 0$. Since none of the processes in the set satisfies the same formulas as Q_1', for each $1 \leq i \leq n$ there exists $\phi_i \in \mathcal{L}_{\mathrm{FB}}$ such that $Q_1' \models \phi_i$ but $Q_{2,i}' \not\models \phi_i$.

    We can then construct the formula $\langle act(\theta_1) \rangle \bigwedge_{i=1}^{n} \phi_i$ that is satisfied by Q_1 but not by Q_2; if $n = 0$ then it

is sufficient to take $\langle act(\theta_1)\rangle\mathsf{true}$. This formula violates $(Q_1, Q_2) \in \mathcal{B}$, hence there must exist at least one Q_2' satisfying the same formulas as Q_1' such that $Q_2 \xrightarrow{\theta_2} Q_2'$ and $act(\theta_1) = act(\theta_2)$, so that $(Q_1', Q_2') \in \mathcal{B}$.

- Let B = FB:ps. The proof is divided into two parts:
  - Assuming that $P_1 \sim_{\mathrm{FB:ps}} P_2$ and $P_1 \models \phi$ for an arbitrary formula $\phi \in \mathcal{L}_{\mathrm{FB:ps}}$, we prove that $P_2 \models \phi$ too by proceeding by induction on $k = depth(\phi)$:
    - If $k = 0$ then either $\phi = \mathsf{true}$ or $\phi = \mathsf{init}$. In the former case, true is trivially satisfied by P_2 too. In the latter case, since from $P_1 \models \mathsf{init}$ it follows that $initial(P_1)$ and from $P_1 \sim_{\mathrm{FB:ps}} P_2$ it follows that $initial(P_1) \iff initial(P_2)$, we derive that $initial(P_2)$ and hence $P_2 \models \mathsf{init}$ too.
    - If $k \geq 1$ then we proceed like in the case B = FB.
  - Assuming that P_1 and P_2 satisfy the same formulas in $\mathcal{L}_{\mathrm{FB:ps}}$, we prove that the symmetric relation $\mathcal{B} = \{(Q_1, Q_2) \in \mathbb{P} \times \mathbb{P} \mid Q_1 \text{ and } Q_2 \text{ satisfy the same formulas in } \mathcal{L}_{\mathrm{FB:ps}}\}$ is a past-sensitive forward bisimulation.
    Given $(Q_1, Q_2) \in \mathcal{B}$, first of all we observe that $Q_1 \models \mathsf{init} \iff Q_2 \models \mathsf{init}$ and hence $initial(Q_1) \iff initial(Q_2)$. If $Q_1 \xrightarrow{\theta_1} Q_1'$ then we proceed like in the case B = FB.

- Let B = RB. The proof is divided into two parts:
  - Assuming that $P_1 \sim_{\mathrm{RB}} P_2$ and $P_1 \models \phi$ for an arbitrary formula $\phi \in \mathcal{L}_{\mathrm{RB}}$, we prove that $P_2 \models \phi$ too by proceeding by induction on $k = depth(\phi)$:
    - If $k = 0$ then we proceed like in the case B = FB.
    - If $k \geq 1$ there are three cases:
      - If ϕ is $\neg\phi'$ then we proceed like in the case B = FB.
      - If ϕ is $\phi_1 \wedge \phi_2$ then we proceed like in the case B = FB.
      - If ϕ is $\langle a^\dagger\rangle\phi'$ then from $P_1 \models \langle a^\dagger\rangle\phi'$ we derive that there exists $P_1' \xrightarrow{\theta_1} P_1$ such that $act(\theta_1) = a$ and $P_1' \models \phi'$. From $P_1 \sim_{\mathrm{RB}} P_2$ it then follows that there exists $P_2' \xrightarrow{\theta_2} P_2$ such that $act(\theta_2) = a$ and $P_1' \sim_{\mathrm{RB}} P_2'$. By applying the induction hypothesis we derive that $P_2' \models \phi'$ and hence $P_2 \models \langle a^\dagger\rangle\phi'$ too.
  - Assuming that P_1 and P_2 satisfy the same formulas in $\mathcal{L}_{\mathrm{RB}}$, we prove that the symmetric relation $\mathcal{B} = \{(Q_1, Q_2) \in \mathbb{P} \times \mathbb{P} \mid Q_1 \text{ and } Q_2 \text{ satisfy the same formulas in } \mathcal{L}_{\mathrm{RB}}\}$ is a reverse bisimulation.
    Given $(Q_1, Q_2) \in \mathcal{B}$ such that $Q_1' \xrightarrow{\theta_1} Q_1$, suppose by contradiction that there is no Q_2' satisfying the same formulas as Q_1' such that $Q_2' \xrightarrow{\theta_2} Q_2$ and $act(\theta_1) = act(\theta_2)$, i.e., $(Q_1', Q_2') \in \mathcal{B}$ for no Q_2' $act(\theta_1)$-reaching Q_2. Since Q_2 has finitely many incoming transitions, the set of processes that can reach Q_2 by performing an $act(\theta_1)$-transition is finite, say $\{Q_{2,1}', \ldots, Q_{2,n}'\}$ with $n \geq 0$. Since none of the processes in the set satisfies the same formulas as Q_1', for each $1 \leq i \leq n$ there exists $\phi_i \in \mathcal{L}_{\mathrm{RB}}$ such that $Q_1' \models \phi_i$ but $Q_{2,i}' \not\models \phi_i$.
    We can then construct the formula $\langle act(\theta_1)^\dagger\rangle \bigwedge_{i=1}^{n} \phi_i$ that is satisfied by Q_1 but not by Q_2; if $n = 0$ then it is sufficient to take $\langle act(\theta_1)^\dagger\rangle\mathsf{true}$. This formula violates $(Q_1, Q_2) \in \mathcal{B}$, hence there must exist at least one Q_2' satisfying the same formulas as Q_1' such that $Q_2' \xrightarrow{\theta_2} Q_2$ and $act(\theta_1) = act(\theta_2)$, so that $(Q_1', Q_2') \in \mathcal{B}$.

- Let $B = \text{FRB}$. The proof is divided into two parts:
  - Assuming that $P_1 \sim_{\text{FRB}} P_2$ and $P_1 \models \phi$ for an arbitrary formula $\phi \in \mathcal{L}_{\text{FRB}}$, we prove that $P_2 \models \phi$ too by proceeding by induction on $k = \mathit{depth}(\phi)$:
    - If $k = 0$ then we proceed like in the case $B = \text{FB}$.
    - If $k \geq 1$ there are four cases:
      - If ϕ is $\neg\phi'$ then we proceed like in the case $B = \text{FB}$.
      - If ϕ is $\phi_1 \wedge \phi_2$ then we proceed like in the case $B = \text{FB}$.
      - If ϕ is $\langle a \rangle \phi'$ then we proceed like in the case $B = \text{FB}$.
      - If ϕ is $\langle a^\dagger \rangle \phi'$ then we proceed like in the case $B = \text{RB}$.
  - Assuming that P_1 and P_2 satisfy the same formulas in $\mathcal{L}_{\text{FRB}}$, we prove that the symmetric relation $\mathcal{B} = \{(Q_1, Q_2) \in \mathbb{P} \times \mathbb{P} \mid Q_1 \text{ and } Q_2 \text{ satisfy the same formulas in } \mathcal{L}_{\text{FRB}}\}$ is a forward-reverse bisimulation. Given $(Q_1, Q_2) \in \mathcal{B}$:
    - If $Q_1 \xrightarrow{\theta_1} Q_1'$ then we proceed like in the case $B = \text{FB}$.
    - If $Q_1' \xrightarrow{\theta_1} Q_1$ then we proceed like in the case $B = \text{RB}$. ∎

Theorem 5.2. *Let $P_1, P_2 \in \mathbb{P}$ and $B \in \{\text{FB}, \text{FB:ps}, \text{RB}, \text{FRB}, \text{FRB:ps}\}$. Then $P_1 \approx_B P_2$ iff $\forall \phi \in \mathcal{L}_B^\tau . P_1 \models \phi \iff P_2 \models \phi$.*

Proof. We consider each of the five weak bisimilarities in turn:

- Let $B = \text{FB}$. The proof is divided into two parts:
  - Assuming that $P_1 \approx_{\text{FB}} P_2$ and $P_1 \models \phi$ for an arbitrary formula $\phi \in \mathcal{L}_{\text{FB}}^\tau$, we prove that $P_2 \models \phi$ too by proceeding by induction on $k = \mathit{depth}(\phi)$:
    - If $k = 0$ then ϕ must be true, which is trivially satisfied by P_2 too.
    - If $k \geq 1$ there are four cases:
      - If ϕ is $\neg\phi'$ then from $P_1 \models \neg\phi'$ we derive that $P_1 \not\models \phi'$. If it were $P_2 \models \phi'$ then by the induction hypothesis it would hold that $P_1 \models \phi'$, which is not the case. Therefore $P_2 \not\models \phi'$ and hence $P_2 \models \neg\phi'$ too.
      - If ϕ is $\phi_1 \wedge \phi_2$ then from $P_1 \models \phi_1 \wedge \phi_2$ we derive that $P_1 \models \phi_1$ and $P_1 \models \phi_2$. From the induction hypothesis it follows that $P_2 \models \phi_1$ and $P_2 \models \phi_2$ and hence $P_2 \models \phi_1 \wedge \phi_2$ too.
      - If ϕ is $\langle\!\langle \tau \rangle\!\rangle \phi'$ then from $P_1 \models \langle\!\langle \tau \rangle\!\rangle \phi'$ we derive that there exists $P_1 \Longrightarrow P_1'$ such that $P_1' \models \phi'$. From $P_1 \approx_{\text{FB}} P_2$ and Proposition 3.3 it then follows that there exists $P_2 \Longrightarrow P_2'$ such that $P_1' \approx_{\text{FB}} P_2'$. By applying the induction hypothesis we derive that $P_2' \models \phi'$ and hence $P_2 \models \langle\!\langle \tau \rangle\!\rangle \phi'$ too.
      - If ϕ is $\langle\!\langle a \rangle\!\rangle \phi'$ then from $P_1 \models \langle\!\langle a \rangle\!\rangle \phi'$ we derive that there exists $P_1 \Longrightarrow \xrightarrow{\theta_1} \Longrightarrow P_1'$ such that $\mathit{act}(\theta_1) = a$ and $P_1' \models \phi'$. From $P_1 \approx_{\text{FB}} P_2$ and Proposition 3.3 it then follows that there exists $P_2 \Longrightarrow \xrightarrow{\theta_2} \Longrightarrow P_2'$ such that $\mathit{act}(\theta_2) = a$ and $P_1' \approx_{\text{FB}} P_2'$. By applying the induction hypothesis we derive that $P_2' \models \phi'$ and hence $P_2 \models \langle\!\langle a \rangle\!\rangle \phi'$ too.

- Assuming that P_1 and P_2 satisfy the same formulas in $\mathcal{L}^{\tau}_{\mathrm{FB}}$, we prove that the symmetric relation $\mathcal{B} = \{(Q_1, Q_2) \in \mathbb{P} \times \mathbb{P} \mid Q_1 \text{ and } Q_2 \text{ satisfy the same formulas in } \mathcal{L}^{\tau}_{\mathrm{FB}}\}$ is a weak forward bisimulation.
  Given $(Q_1, Q_2) \in \mathcal{B}$ such that $Q_1 \xrightarrow{\theta_1} Q'_1$, there are two cases:
  - If $act(\theta_1) = \tau$ suppose by contradiction that there is no Q'_2 satisfying the same formulas as Q'_1 such that $Q_2 \Longrightarrow Q'_2$, i.e., $(Q'_1, Q'_2) \in \mathcal{B}$ for no Q'_2 τ^*-reachable from Q_2. Since Q_2 and the finitely many processes τ^*-reachable from it have finitely many outgoing transitions, the set of processes that Q_2 can reach by performing a possibly empty sequence of finitely many τ-transitions is finite, say $\{Q'_{2,1}, \ldots, Q'_{2,n}\}$ with $n \geq 0$. Since none of the processes in the set satisfies the same formulas as Q'_1, for each $1 \leq i \leq n$ there exists $\phi_i \in \mathcal{L}^{\tau}_{\mathrm{FB}}$ such that $Q'_1 \models \phi_i$ but $Q'_{2,i} \not\models \phi_i$.
    We can then construct the formula $\langle\langle\tau\rangle\rangle \bigwedge_{i=1}^{n} \phi_i$ that is satisfied by Q_1 but not by Q_2; if $n = 0$ then it is sufficient to take $\langle\langle\tau\rangle\rangle\mathsf{true}$. This formula violates $(Q_1, Q_2) \in \mathcal{B}$, hence there must exist at least one Q'_2 satisfying the same formulas as Q'_1 such that $Q_2 \Longrightarrow Q'_2$, so that $(Q'_1, Q'_2) \in \mathcal{B}$.
  - If $act(\theta_1) \neq \tau$ suppose by contradiction that there is no Q'_2 satisfying the same formulas as Q'_1 such that $Q_2 \Longrightarrow \xrightarrow{\theta_2} \Longrightarrow Q'_2$ and $act(\theta_1) = act(\theta_2)$, i.e., $(Q'_1, Q'_2) \in \mathcal{B}$ for no Q'_2 $\tau^* act(\theta_1)\tau^*$-reachable from Q_2. Since Q_2 and the finitely many processes $\tau^* act(\theta_1)\tau^*$-reachable from it have finitely many outgoing transitions, the set of processes that Q_2 can reach by performing an $act(\theta_1)$-transition preceded and followed by a possibly empty sequence of finitely many τ-transitions is finite, say $\{Q'_{2,1}, \ldots, Q'_{2,n}\}$ with $n \geq 0$. Since none of the processes in the set satisfies the same formulas as Q'_1, for each $1 \leq i \leq n$ there exists $\phi_i \in \mathcal{L}^{\tau}_{\mathrm{FB}}$ such that $Q'_1 \models \phi_i$ but $Q'_{2,i} \not\models \phi_i$.
    We can then construct the formula $\langle\langle act(\theta_1)\rangle\rangle \bigwedge_{i=1}^{n} \phi_i$ that is satisfied by Q_1 but not by Q_2; if $n = 0$ then it is sufficient to take $\langle\langle act(\theta_1)\rangle\rangle\mathsf{true}$. This formula violates $(Q_1, Q_2) \in \mathcal{B}$, hence there must exist at least one Q'_2 satisfying the same formulas as Q'_1 such that $Q_2 \Longrightarrow \xrightarrow{\theta_2} \Longrightarrow Q'_2$ and $act(\theta_1) = act(\theta_2)$, so that $(Q'_1, Q'_2) \in \mathcal{B}$.

- Let $B =$ FB:ps. The proof is divided into two parts:
  - Assuming that $P_1 \approx_{\mathrm{FB:ps}} P_2$ and $P_1 \models \phi$ for an arbitrary formula $\phi \in \mathcal{L}^{\tau}_{\mathrm{FB:ps}}$, we prove that $P_2 \models \phi$ too by proceeding by induction on $k = depth(\phi)$:
    - If $k = 0$ then either $\phi = \mathsf{true}$ or $\phi = \mathsf{init}$. In the former case, true is trivially satisfied by P_2 too. In the latter case, since from $P_1 \models \mathsf{init}$ it follows that $initial(P_1)$ and from $P_1 \approx_{\mathrm{FB:ps}} P_2$ it follows that $initial(P_1) \Longleftrightarrow initial(P_2)$, we derive that $initial(P_2)$ and hence $P_2 \models \mathsf{init}$ too.
    - If $k \geq 1$ then we proceed like in the case $B =$ FB.
  - Assuming that P_1 and P_2 satisfy the same formulas in $\mathcal{L}^{\tau}_{\mathrm{FB:ps}}$, we prove that the symmetric relation $\mathcal{B} = \{(Q_1, Q_2) \in \mathbb{P}\times\mathbb{P} \mid Q_1 \text{ and } Q_2 \text{ satisfy the same formulas in } \mathcal{L}^{\tau}_{\mathrm{FB:ps}}\}$ is a weak past-sensitive forward bisimulation.
    Given $(Q_1, Q_2) \in \mathcal{B}$, first of all we observe that $Q_1 \models \mathsf{init} \Longleftrightarrow Q_2 \models \mathsf{init}$ and hence $initial(Q_1) \Longleftrightarrow initial(Q_2)$. If $Q_1 \xrightarrow{\theta_1} Q'_1$ then we proceed like in the case $B =$ FB.

- Let B = RB. The proof is divided into two parts:
  - Assuming that $P_1 \approx_{\mathrm{RB}} P_2$ and $P_1 \models \phi$ for an arbitrary formula $\phi \in \mathcal{L}^{\tau}_{\mathrm{RB}}$, we prove that $P_2 \models \phi$ too by proceeding by induction on $k = \mathit{depth}(\phi)$:
    - If $k = 0$ then we proceed like in the case B = FB.
    - If $k \geq 1$ there are four cases:
      - If ϕ is $\neg\phi'$ then we proceed like in the case B = FB.
      - If ϕ is $\phi_1 \wedge \phi_2$ then we proceed like in the case B = FB.
      - If ϕ is $\langle\!\langle \tau^\dagger \rangle\!\rangle \phi'$ then from $P_1 \models \langle\!\langle \tau^\dagger \rangle\!\rangle \phi'$ we derive that there exists $P'_1 \Longrightarrow P_1$ such that $P'_1 \models \phi'$. From $P_1 \approx_{\mathrm{RB}} P_2$ and Proposition 3.4 it then follows that there exists $P'_2 \Longrightarrow P_2$ such that $P'_1 \approx_{\mathrm{RB}} P'_2$. By applying the induction hypothesis we derive that $P'_2 \models \phi'$ and hence $P_2 \models \langle\!\langle \tau^\dagger \rangle\!\rangle \phi'$ too.
      - If ϕ is $\langle\!\langle a^\dagger \rangle\!\rangle \phi'$ then from $P_1 \models \langle\!\langle a^\dagger \rangle\!\rangle \phi'$ we derive that there exists $P'_1 \Longrightarrow \xrightarrow{\theta_1} \Longrightarrow P_1$ such that $\mathit{act}(\theta_1) = a$ and $P'_1 \models \phi'$. From $P_1 \approx_{\mathrm{RB}} P_2$ and Proposition 3.4 it then follows that there exists $P'_2 \Longrightarrow \xrightarrow{\theta_2} \Longrightarrow P_2$ such that $\mathit{act}(\theta_1) = \mathit{act}(\theta_2)$ and $P'_1 \approx_{\mathrm{RB}} P'_2$. By applying the induction hypothesis we derive that $P'_2 \models \phi'$ and hence $P_2 \models \langle\!\langle a^\dagger \rangle\!\rangle \phi'$ too.
  - Assuming that P_1 and P_2 satisfy the same formulas in $\mathcal{L}^{\tau}_{\mathrm{RB}}$, we prove that the symmetric relation $\mathcal{B} = \{(Q_1, Q_2) \in \mathbb{P} \times \mathbb{P} \mid Q_1 \text{ and } Q_2 \text{ satisfy the same formulas in } \mathcal{L}^{\tau}_{\mathrm{RB}}\}$ is a weak reverse bisimulation.

    Given $(Q_1, Q_2) \in \mathcal{B}$ such that $Q'_1 \xrightarrow{\theta_1} Q_1$, there are two cases:
    - If $\mathit{act}(\theta_1) = \tau$ suppose by contradiction that there is no Q'_2 satisfying the same formulas as Q'_1 such that $Q'_2 \Longrightarrow Q_2$, i.e., $(Q'_1, Q'_2) \in \mathcal{B}$ for no Q'_2 τ^*-reaching Q_2. Since Q_2 and the finitely many processes τ^*-reaching it have finitely many incoming transitions, the set of processes that can reach Q_2 by performing a possibly empty sequence of finitely many τ-transitions is finite, say $\{Q'_{2,1}, \ldots, Q'_{2,n}\}$ with $n \geq 0$. Since none of the processes in the set satisfies the same formulas as Q'_1, for each $1 \leq i \leq n$ there exists $\phi_i \in \mathcal{L}^{\tau}_{\mathrm{RB}}$ such that $Q'_1 \models \phi_i$ but $Q'_{2,i} \not\models \phi_i$.

      We can then construct the formula $\langle\!\langle \tau^\dagger \rangle\!\rangle \bigwedge_{i=1}^{n} \phi_i$ that is satisfied by Q_1 but not by Q_2; if $n = 0$ then it is sufficient to take $\langle\!\langle \tau^\dagger \rangle\!\rangle \mathsf{true}$. This formula violates $(Q_1, Q_2) \in \mathcal{B}$, hence there must exist at least one Q'_2 satisfying the same formulas as Q'_1 such that $Q'_2 \Longrightarrow Q_2$, so that $(Q'_1, Q'_2) \in \mathcal{B}$.
    - If $\mathit{act}(\theta_1) \neq \tau$ suppose by contradiction that there is no Q'_2 satisfying the same formulas as Q'_1 such that $Q'_2 \Longrightarrow \xrightarrow{\theta_2} \Longrightarrow Q_2$ and $\mathit{act}(\theta_1) = \mathit{act}(\theta_2)$, i.e., $(Q'_1, Q'_2) \in \mathcal{B}$ for no Q'_2 $\tau^* \mathit{act}(\theta_1) \tau^*$-reaching Q_2. Since Q_2 and the finitely many processes $\tau^* \mathit{act}(\theta_1) \tau^*$-reaching it have finitely many incoming transitions, the set of processes that can reach Q_2 by performing an $\mathit{act}(\theta_1)$-transition preceded and followed by a possibly empty sequence of finitely many τ-transitions is finite, say $\{Q'_{2,1}, \ldots, Q'_{2,n}\}$ with $n \geq 0$. Since none of the processes in the set satisfies the same formulas as Q'_1, for each $1 \leq i \leq n$ there exists $\phi_i \in \mathcal{L}^{\tau}_{\mathrm{RB}}$ such that $Q'_1 \models \phi_i$ but $Q'_{2,i} \not\models \phi_i$.

      We can then construct the formula $\langle\!\langle \mathit{act}(\theta_1)^\dagger \rangle\!\rangle \bigwedge_{i=1}^{n} \phi_i$ that is satisfied by Q_1 but not by Q_2; if $n = 0$ then it is sufficient to take $\langle\!\langle \mathit{act}(\theta_1)^\dagger \rangle\!\rangle \mathsf{true}$. This formula violates $(Q_1, Q_2) \in \mathcal{B}$, hence there must exist at least one Q'_2 satisfying the same formulas as Q'_1 such that $Q'_2 \Longrightarrow \xrightarrow{\theta_2} \Longrightarrow Q_2$ and $\mathit{act}(\theta_1) = \mathit{act}(\theta_2)$, so that $(Q'_1, Q'_2) \in \mathcal{B}$.

- Let B = FRB. The proof is divided into two parts:
  - Assuming that $P_1 \approx_{\mathrm{FRB}} P_2$ and $P_1 \models \phi$ for an arbitrary formula $\phi \in \mathcal{L}^{\tau}_{\mathrm{FRB}}$, we prove that $P_2 \models \phi$ too by proceeding by induction on $k = \mathit{depth}(\phi)$:
    - If $k = 0$ then we proceed like in the case B = FB.
    - If $k \geq 1$ there are six cases:
      - If ϕ is $\neg\phi'$ then we proceed like in the case B = FB.
      - If ϕ is $\phi_1 \wedge \phi_2$ then we proceed like in the case B = FB.
      - If ϕ is $\langle\!\langle\tau\rangle\!\rangle\phi'$ then we proceed like in the case B = FB by using Proposition 3.5.
      - If ϕ is $\langle\!\langle a\rangle\!\rangle\phi'$ then we proceed like in the case B = FB by using Proposition 3.5.
      - If ϕ is $\langle\!\langle\tau^{\dagger}\rangle\!\rangle\phi'$ then we proceed like in the case B = RB by using Proposition 3.5.
      - If ϕ is $\langle\!\langle a^{\dagger}\rangle\!\rangle\phi'$ then we proceed like in the case B = RB by using Proposition 3.5.
  - Assuming that P_1 and P_2 satisfy the same formulas in $\mathcal{L}^{\tau}_{\mathrm{FRB}}$, we prove that the symmetric relation $\mathcal{B} = \{(Q_1, Q_2) \in \mathbb{P} \times \mathbb{P} \mid Q_1 \text{ and } Q_2 \text{ satisfy the same formulas in } \mathcal{L}^{\tau}_{\mathrm{FRB}}\}$ is a weak forward-reverse bisimulation.
    Given $(Q_1, Q_2) \in \mathcal{B}$:
    - If $Q_1 \xrightarrow{\theta_1} Q_1'$ then we proceed like in the case B = FB.
    - If $Q_1' \xrightarrow{\theta_1} Q_1$ then we proceed like in the case B = RB.
- Let B = FRB:ps. The proof is divided into two parts:
  - Assuming that $P_1 \approx_{\mathrm{FRB:ps}} P_2$ and $P_1 \models \phi$ for an arbitrary formula $\phi \in \mathcal{L}^{\tau}_{\mathrm{FRB:ps}}$, we prove that $P_2 \models \phi$ too by proceeding by induction on $k = \mathit{depth}(\phi)$:
    - If $k = 0$ then we proceed like in the case B = FB:ps.
    - If $k \geq 1$ then we proceed like in the case B = FRB.
  - Assuming that P_1 and P_2 satisfy the same formulas in $\mathcal{L}^{\tau}_{\mathrm{FRB:ps}}$, we prove that the symmetric relation $\mathcal{B} = \{(Q_1, Q_2) \in \mathbb{P} \times \mathbb{P} \mid Q_1 \text{ and } Q_2 \text{ satisfy the same formulas in } \mathcal{L}^{\tau}_{\mathrm{FRB:ps}}\}$ is a weak past-sensitive forward-reverse bisimulation.
    Given $(Q_1, Q_2) \in \mathcal{B}$, first of all we observe that $Q_1 \models \mathsf{init} \iff Q_2 \models \mathsf{init}$ and hence $\mathit{initial}(Q_1) \iff \mathit{initial}(Q_2)$. Then we proceed like in the case B = FRB. ■

We conclude with the following remarks:

- The fragments that characterize the four forward bisimilarities $\sim_{\rm FB}$, $\sim_{\rm FB:ps}$, $\approx_{\rm FB}$, $\approx_{\rm FB:ps}$ are essentially identical to the Hennessy-Milner logic – first two bisimilarities – and its weak variant – last two bisimilarities. The only difference is the possible presence of proposition init, which is necessary to distinguish between initial and non-initial processes in the past-sensitive cases.

- The fragments that characterize the two reverse bisimilarities $\sim_{\rm RB}$ and $\approx_{\rm RB}$ over sequential processes need only true and the backward modalities $\langle a^\dagger\rangle$ – first bisimilarity – or $\langle\!\langle \tau^\dagger\rangle\!\rangle$ and $\langle\!\langle a^\dagger\rangle\!\rangle$ – second bisimilarity – due to the forthcoming Theorems 7.1 and 7.2 showing that reverse bisimulation semantics coincides with reverse trace semantics over those processes. As for the counterexample about concurrent processes preceding those two theorems, a distinguishing formula with respect to $\sim_{\rm RB}$ is $\langle c^\dagger\rangle\neg(\langle a^\dagger\rangle\mathsf{true}\wedge\langle b^\dagger\rangle\mathsf{true}\wedge\langle c^\dagger\rangle\mathsf{true})$.

- The fragments that characterize the three forward-reverse bisimilarities $\sim_{\rm FRB}$, $\approx_{\rm FRB}$, $\approx_{\rm FRB:ps}$ are akin to the logic $\mathcal{L}_{\rm BF}$ introduced in [57] to characterize weak back-and-forth bisimilarity and branching bisimilarity. A crucial distinction between our three fragments and $\mathcal{L}_{\rm BF}$ is that the former are interpreted over states while $\mathcal{L}_{\rm BF}$ is interpreted over computation paths. Moreover, as already mentioned, defining a strong variant of $\mathcal{L}_{\rm BF}$ would yield a logic that characterizes the strong bisimilarity of [112], whereas in our setting forward-only bisimilarities are different from forward-reverse ones and hence different logics are needed.

- According to the logical characterizations of branching bisimilarity in [58], the forthcoming Theorem 7.3, which shows that branching bisimilarity and weak forward-reverse bisimilarity coincide over initial sequential processes, opens the way to two further logical characterizations of $\approx_{\rm FRB}$ over those processes:

  - The first additional characterization replaces the two backward modalities with an until operator $\phi_1\langle\!\langle a\rangle\!\rangle\phi_2$. This is satisfied by a process P iff either $a = \tau$ and P satisfies ϕ_2, or there exists $P \Longrightarrow \bar{P} \stackrel{\theta}{\longrightarrow} P'$ such that every process along $P \Longrightarrow \bar{P}$ satisfies ϕ_1, $act(\theta) = a$, and P' satisfies ϕ_2.
  - The second additional characterization is given by the temporal logic CTL* without the next operator, thanks to a revisitation of the stuttering equivalence of [46] and the bridge between Kripke structures (in which states are decorated with propositions) and labeled transition systems (in which transitions are decorated with actions) established in [58].

  As for the first counterexample about concurrent processes preceding the forthcoming Theorem 7.3, a distinguishing formula with respect to $\approx_{\rm FRB}$ is $\langle\!\langle a\rangle\!\rangle\langle\!\langle b\rangle\!\rangle(\langle\!\langle a^\dagger\rangle\!\rangle\mathsf{true}\wedge\langle\!\langle b^\dagger\rangle\!\rangle\mathsf{true})$.

Chapter 6

Sound and Complete Axiomatizations

In this chapter, whose contents have appeared in [27, 25, 29], we start by recalling some notions about deduction systems (Section 6.1) as well as observation functions and process encodings for deriving expansion laws of parallel composition (Section 6.2). Then we develop sound and complete axiomatizations for the two forward bisimulation congruences $\sim_{\mathrm{FB:ps}}$ and $\approx_{\mathrm{FB:ps}}$ (Section 6.3) and, after providing process encodings based on backward ready sets (Section 6.4), for the two reverse bisimulation congruences $\sim_{\mathrm{RB}}$ and $\approx_{\mathrm{RB}}$ (Section 6.5) and the two forward-reverse bisimulation congruences $\sim_{\mathrm{FRB}}$ and $\approx_{\mathrm{FRB:ps}}$ (Section 6.6). These axiomatizations (see the forthcoming Tables 6.1, 6.2, 6.4, 6.5, 6.6, 6.7) elucidate the fundamental equational laws characterizing the aforementioned bisimilarities and can also be exploited as bisimilarity-preserving rewriting rules for manipulating processes.

6.1 Deduction Systems

The deduction systems that we will consider are sets comprising the general axioms and inference rules below for $=$ on $\mathbb{P}$, each enriched with a set A of additional bisimilarity-specific axioms. They correspond to the fact that $\sim_{\mathrm{FB:ps}}$, $\approx_{\mathrm{FB:ps}}$, $\sim_{\mathrm{RB}}$, $\approx_{\mathrm{RB}}$, $\sim_{\mathrm{FRB}}$, $\approx_{\mathrm{FRB:ps}}$ are equivalence relations (Propositions 3.1, 4.1, 3.6, 4.2) as well as congruences with respect to all PRPC operators (Theorems 4.1 and 4.2):

- Reflexivity: $P = P$.
- Symmetry: $\dfrac{P_1 = P_2}{P_2 = P_1}$.
- Transitivity: $\dfrac{P_1 = P_2 \quad P_2 = P_3}{P_1 = P_3}$.
- .-substitutivity: $\dfrac{P_1 = P_2 \quad \mathit{initial}(P_1) \wedge \mathit{initial}(P_2)}{a\,.\,P_1 = a\,.\,P_2}$, $\dfrac{P_1 = P_2}{a^\dagger.\,P_1 = a^\dagger.\,P_2}$.
- $\llcorner\urcorner$-substitutivity: $\dfrac{P_1 = P_2}{P_1 \llcorner \rho \urcorner = P_2 \llcorner \rho \urcorner}$.
- $+$-substitutivity: $\dfrac{P_1 = P_2 \quad \mathit{initial}(P) \vee (\mathit{initial}(P_1) \wedge \mathit{initial}(P_2))}{P_1 + P = P_2 + P \quad P + P_1 = P + P_2}$.

- $\|$-substitutivity: $\dfrac{P_1 = P_2 \quad P_1 \,\|_L\, P, P_2 \,\|_L\, P, P \,\|_L\, P_1, P \,\|_L\, P_2 \in \mathbb{P}}{P_1 \,\|_L\, P = P_2 \,\|_L\, P \quad P \,\|_L\, P_1 = P \,\|_L\, P_2}$.

The deducibility relation will be denoted by $\vdash$. Given $\simeq \in \{\sim_{\text{FB:ps}}, \approx_{\text{FB:ps}}, \sim_{\text{RB}}, \approx_{\text{RB}}, \sim_{\text{FRB}}, \approx_{\text{FRB:ps}}\}$, the deduction system enriched with $\mathsf{A}_{\simeq}$ is *sound* (resp. *complete*) for $\simeq$ iff for all $P_1, P_2 \in \mathbb{P}$ it holds that if $\mathsf{A}_{\simeq} \vdash P_1 = P_2$ then $P_1 \simeq P_2$ (resp. if $P_1 \simeq P_2$ then $\mathsf{A}_{\simeq} \vdash P_1 = P_2$). To be precise, we should say ground complete due to the absence of variables within processes.

Some of the proofs related to completeness will proceed by induction on the size of a process, intended as an upper bound to the depth of the proved labeled transition system starting from the initial process obtained from the original one by eliminating all action decorations. It is defined by induction on the syntactical structure of $P \in \mathbb{P}$ as follows:

$$\begin{aligned} size(\underline{0}) &= 0 \\ size(a\,.\,P') = size(a^\dagger\,.\,P') &= 1 + size(P') \\ size(P' \llcorner \rho \urcorner) &= size(P') \\ size(P_1 + P_2) &= \max(size(P_1), size(P_2)) \\ size(P_1 \,\|_L\, P_2) &= size(P_1) + size(P_2) \end{aligned}$$

6.2 Expansion Laws via Observation Functions and Process Encodings

Expansion laws are among the most important bisimilarity-specific axioms. They are useful to relate sequential specifications of systems with their concurrent implementations [112]. In the interleaving setting they can be obtained quite naturally, whereas this is not the case under true concurrency.

More precisely, the usual technique for axiomatizing bisimilarity consists of introducing normal forms, in which only action prefix and alternative composition occur, along with expansion laws, through which occurrences of parallel composition are progressively eliminated. Although this originated in the interleaving setting for forward-only calculi [88] to *identify* processes such as $a\,.\,\underline{0} \,\|_\emptyset\, b\,.\,\underline{0}$ and $a\,.\,b\,.\,\underline{0} + b\,.\,a\,.\,\underline{0}$, it was later exploited also in the truly concurrent spectrum [77, 66] to *distinguish* processes like the aforementioned two. This requires an extension of the process calculus syntax to add suitable discriminating information within action prefixes. For example:

- Causal bisimilarity [55, 56] (corresponding to history-preserving bisimilarity [129]): every action is enriched with the set of its causing actions, each of which is expressed as a numeric backward pointer, so that the former process is expanded to $<a, \emptyset>\,.\,<b, \emptyset>\,.\,\underline{0} + <b, \emptyset>\,.\,<a, \emptyset>\,.\,\underline{0}$ while the latter process becomes $<a, \emptyset>\,.\,<b, \{1\}>\,.\,\underline{0} + <b, \emptyset>\,.\,<a, \{1\}>\,.\,\underline{0}$.
- Location bisimilarity [43] (corresponding to local history-preserving bisimilarity [48]): every action is enriched with the name of the location in which it is executed, so that the former process is expanded to $<a, l_a>\,.\,<b, l_b>\,.\,\underline{0} + <b, l_b>\,.\,<a, l_a>\,.\,\underline{0}$ while the latter process becomes $<a, l_a>\,.\,<b, l_a l_b>\,.\,\underline{0} + <b, l_b>\,.\,<a, l_b l_a>\,.\,\underline{0}$.
- Pomset bisimilarity [40]: instead of a single action, a prefix may contain a partially ordered multiset of actions that are either independent of each other or causally related, so that the former process is expanded to $a\,.\,b\,.\,\underline{0} + b\,.\,a\,.\,\underline{0} + (a \parallel b)\,.\,\underline{0}$ while the latter process is left unchanged.

Thanks to the proved operational semantics in Table 2.1, by following the proved trees approach of [59] we can *uniformly* derive expansion laws for the two interleaving bisimulation congruences $\sim_{\text{FB:ps}}$ and $\approx_{\text{FB:ps}}$

and the four truly concurrent bisimulation congruences $\sim_{\mathrm{RB}}$, $\approx_{\mathrm{RB}}$, $\sim_{\mathrm{FRB}}$, $\approx_{\mathrm{FRB:ps}}$. The first step consists of introducing six *observation functions* ℓ_{F}, $\ell_{\mathrm{F,w}}$, ℓ_{R}, $\ell_{\mathrm{R,w}}$, ℓ_{FR}, $\ell_{\mathrm{FR,w}}$ that respectively transform the proof terms labeling proved transitions into suitable observations according to $\sim_{\mathrm{FB:ps}}$, $\approx_{\mathrm{FB:ps}}$, $\sim_{\mathrm{RB}}$, $\approx_{\mathrm{RB}}$, $\sim_{\mathrm{FRB}}$, $\approx_{\mathrm{FRB:ps}}$. In the interleaving case proof terms are simply reduced to the actions they contain, while in the truly concurrent case they are transformed into actions extended with discriminating information as exemplified above.

In addition to a specific proof term θ, as shown in [59] each such function, say ℓ, may depend on other possible parameters in the proved labeled transition system generated by the semantic rules in Table 2.1. Moreover, it must preserve actions, i.e., if $\ell(\theta_1) = \ell(\theta_2)$ then $act(\theta_1) = act(\theta_2)$. Based on the corresponding ℓ, from each of the six aforementioned congruences we can thus derive a bisimilarity in which, whenever $(P_1, P_2) \in \mathcal{B}$, the strong forward clause requires that:

$$\text{for each } P_1 \xrightarrow{\ell(\theta_1)} P_1' \text{ there exists } P_2 \xrightarrow{\ell(\theta_2)} P_2' \text{ such that } \ell(\theta_1) = \ell(\theta_2) \text{ and } (P_1', P_2') \in \mathcal{B}$$

while the strong backward clause requires that:

$$\text{for each } P_1' \xrightarrow{\ell(\theta_1)} P_1 \text{ there exists } P_2' \xrightarrow{\ell(\theta_2)} P_2 \text{ such that } \ell(\theta_1) = \ell(\theta_2) \text{ and } (P_1', P_2') \in \mathcal{B}$$

and similarly for the weak clauses. We indicate with $\sim_{\mathrm{FB:ps}:\ell_{\mathrm{F}}}$, $\approx_{\mathrm{FB:ps}:\ell_{\mathrm{F,w}}}$, $\sim_{\mathrm{RB}:\ell_{\mathrm{R}}}$, $\approx_{\mathrm{RB}:\ell_{\mathrm{R,w}}}$, $\sim_{\mathrm{FRB}:\ell_{\mathrm{FR}}}$, $\approx_{\mathrm{FRB:ps}:\ell_{\mathrm{FR,w}}}$ the six resulting bisimilarities.

The second step – left implicit in [59] – consists of lifting ℓ to processes so as to encode observations within action prefixes of new processes in which only action prefix and alternative composition occur. For $P \in \mathbb{P}_{\mathrm{seq}}$ the idea is to proceed inductively as follows where $\sigma \in \Theta_{\mathrm{seq}}^*$ for $\Theta_{\mathrm{seq}} = \{.a, \llcorner\rho\urcorner, \dot{+}, \dot{+} \mid a \in \mathcal{A}, \rho : \mathcal{A} \to \mathcal{A} \text{ such that } \rho(\tau) = \tau\}$:

$$\begin{aligned}
\ell^{\sigma}(\underline{0}) &= \underline{0}\\
\ell^{\sigma}(a \,.\, P') &= \ell(\sigma a) \,.\, \ell^{\sigma .a}(P')\\
\ell^{\sigma}(a^{\dagger} \,.\, P') &= \ell(\sigma a)^{\dagger} \,.\, \ell^{\sigma .a}(P')\\
\ell^{\sigma}(P' \llcorner\rho\urcorner) &= \ell^{\sigma \llcorner\rho\urcorner}(P')\\
\ell^{\sigma}(P_1 + P_2) &= \ell^{\sigma \dot{+}}(P_1) + \ell^{\sigma \dot{+}}(P_2)
\end{aligned}$$

Every sequential process P will thus be encoded as $\ell^{\varepsilon}(P)$, so for example $a \,.\, b \,.\, \underline{0} + b \,.\, a \,.\, \underline{0}$ will become:

$$\ell^{\dot{+}}(a \,.\, b \,.\, \underline{0}) + \ell^{\dot{+}}(b \,.\, a \,.\, \underline{0}) = \ell(\dot{+}a) \,.\, \ell^{\dot{+} .a}(b \,.\, \underline{0}) + \ell(\dot{+}b) \,.\, \ell^{\dot{+} .b}(a \,.\, \underline{0}) = \ell(\dot{+}a) \,.\, \ell(\dot{+}_{.a} b) \,.\, \underline{0} + \ell(\dot{+}b) \,.\, \ell(\dot{+}_{.b} a) \,.\, \underline{0}$$

Then, given two initial sequential processes encoded as follows due to the commutativity and associativity of alternative composition (where any summation over an empty index set is $\underline{0}$ and every θ_i is of the form $\sigma_i a_i$):

$$P_1 = \sum_{i \in I_1} \ell(\theta_{1,i}) \,.\, P_{1,i} \quad \text{and} \quad P_2 = \sum_{i \in I_2} \ell(\theta_{2,i}) \,.\, P_{2,i}$$

the idea is to encode their parallel composition through the following expansion law (where $\underline{0} \parallel_L \underline{0}$ yields $\underline{0}$):

$$\begin{aligned}
P_1 \parallel_L P_2 = &\sum_{i \in I_1, act(\theta_{1,i}) \notin L} \ell(\lfloor\!\lfloor_L \theta_{1,i}) \,.\, (P_{1,i} \parallel_L P_2) + \sum_{i \in I_2, act(\theta_{2,i}) \notin L} \ell(\lfloor\!\lfloor_L \theta_{2,i}) \,.\, (P_1 \parallel_L P_{2,i}) +\\
&\sum_{i \in I_1, act(\theta_{1,i}) \in L} \; \sum_{j \in I_2, act(\theta_{2,j}) = act(\theta_{1,i})} \ell(\langle \theta_{1,i}, \theta_{2,j} \rangle_L) \,.\, (P_{1,i} \parallel_L P_{2,j})
\end{aligned}$$

For instance, $a \,.\, \underline{0} \parallel_{\emptyset} b \,.\, \underline{0}$, represented as $\ell(a) \,.\, \underline{0} \parallel_{\emptyset} \ell(b) \,.\, \underline{0}$, will be expanded as follows:

$$\ell(a) \,.\, \underline{0} \parallel_{\emptyset} \ell(b) \,.\, \underline{0} = \ell(\lfloor\!\lfloor_{\emptyset} a) \,.\, (\underline{0} \parallel_{\emptyset} \ell(b) \,.\, \underline{0}) + \ell(\lfloor\!\lfloor_{\emptyset} b) \,.\, (\ell(a) \,.\, \underline{0} \parallel_{\emptyset} \underline{0}) = \ell(\lfloor\!\lfloor_{\emptyset} a) \,.\, \ell(\lfloor\!\lfloor_{\emptyset} b) \,.\, \underline{0} + \ell(\lfloor\!\lfloor_{\emptyset} b) \,.\, \ell(\lfloor\!\lfloor_{\emptyset} a) \,.\, \underline{0}$$

where, compared to the encoding of $a \,.\, b \,.\, \underline{0} + b \,.\, a \,.\, \underline{0}$, in general $\ell(\dot{+}a) \neq \ell(\lfloor\!\lfloor_{\emptyset} a) \neq \ell(\dot{+}_{.b} a)$ and $\ell(\dot{+}_{.a} b) \neq \ell(\lfloor\!\lfloor_{\emptyset} b) \neq \ell(\dot{+}b)$. The expansion laws for the cases in which the two sequential processes are not both initial – which are specific to reversible processes and hence not addressed in [59] – can be derived similarly. We will see that care must be taken when both processes are non-initial because for example $a^{\dagger} \,.\, \underline{0} \parallel_{\emptyset} b^{\dagger} \,.\, \underline{0}$ cannot be expanded to $\ell(\lfloor\!\lfloor_{\emptyset} a)^{\dagger} \,.\, \ell(\lfloor\!\lfloor_{\emptyset} b)^{\dagger} \,.\, \underline{0} + \ell(\lfloor\!\lfloor_{\emptyset} b)^{\dagger} \,.\, \ell(\lfloor\!\lfloor_{\emptyset} a)^{\dagger} \,.\, \underline{0}$ as the latter is not even well-formed due to the presence of executed actions on both sides of $+$.

In the subsequent sections we will investigate how to define the six observation functions in such a way that the six bisimilarities $\sim_{\mathrm{FB:ps}:\ell_{\mathrm{F}}}$, $\approx_{\mathrm{FB:ps}:\ell_{\mathrm{F,w}}}$, $\sim_{\mathrm{RB}:\ell_{\mathrm{R}}}$, $\approx_{\mathrm{RB}:\ell_{\mathrm{R,w}}}$, $\sim_{\mathrm{FRB}:\ell_{\mathrm{FR}}}$, $\approx_{\mathrm{FRB:ps}:\ell_{\mathrm{FR,w}}}$ respectively coincide with

the six congruences $\sim_{\text{FB:ps}}$, $\approx_{\text{FB:ps}}$, $\sim_{\text{RB}}$, $\approx_{\text{RB}}$, $\sim_{\text{FRB}}$, $\approx_{\text{FRB:ps}}$. As far as true concurrency is concerned, we point out that the observation functions developed in [59] for causal semantics and location semantics were inspired by additional information already present in the labels of the original semantics, i.e., backward pointers sets [55] and localities [43] respectively. In our case, instead, the original semantics in Table 2.1 features labels that contain only actions (and localities in the case of parallel composition), hence for reverse and forward-reverse congruences we have to find out the additional information necessary to discriminate, e.g., the processes associated with the three bottom states in Figure 1.1.

6.3 Axiomatizations of Forward Bisimulation Congruences

Strong and weak forward bisimilarities respectively coincide with the strong and weak bisimilarities over forward-only processes of [112] and hence comply with the interleaving view of concurrency. Therefore, we can exploit the same observation function for interleaving semantics used in [59], which we express as $\ell_{\text{F}}(\theta) = \ell_{\text{F,w}}(\theta) = act(\theta)$ and immediately implies that $\sim_{\text{FB:ps:}\ell_{\text{F}}}$ and $\approx_{\text{FB:ps:}\ell_{\text{F,w}}}$ respectively coincide with $\sim_{\text{FB:ps}}$ and $\approx_{\text{FB:ps}}$. Moreover, no additional information has to be inserted into action prefixes, i.e., the lifting to processes of the observation function is the identity over processes.

The axioms for $\sim_{\text{FB:ps}}$ are presented in Section 6.3.1, while the additional ones for $\approx_{\text{FB:ps}}$ are discussed in Section 6.3.2.

6.3.1 Axiomatization of $\sim_{\text{FB:ps}}$

The set A_{F} of axioms for $\sim_{\text{FB:ps}}$ is shown in Table 6.1 (where-clauses ensure $\mathbb{P}$-membership). Axioms $\mathsf{A}_{\text{F},1}$ to $\mathsf{A}_{\text{F},4}$ express associativity, commutativity, neutral element, and idempotency of alternative composition, while axioms $\mathsf{A}_{\text{F},5}$ to $\mathsf{A}_{\text{F},8}$ represent the application of renaming and its distributivity with respect to alternative composition. These axioms basically coincide with those for forward-only processes [88].

The subsequent axioms are specific to our reversible setting. Axioms $\mathsf{A}_{\text{F},9}$ and $\mathsf{A}_{\text{F},10}$ together establish that the presence of the past cannot be ignored, but the specific past can be neglected when moving only forward. Likewise, axiom $\mathsf{A}_{\text{F},11}$ states that a previously non-selected alternative process can be discarded when moving only forward; note that it does not subsume axioms $\mathsf{A}_{\text{F},3}$ and $\mathsf{A}_{\text{F},4}$ because P has to be non-initial in $\mathsf{A}_{\text{F},11}$.

Since due to axioms $\mathsf{A}_{\text{F},9}$ and $\mathsf{A}_{\text{F},10}$ we only need to remember whether some action has been executed in the past, axiom $\mathsf{A}_{\text{F},12}$ is the only expansion law needed for $\sim_{\text{FB:ps}}$. Notation $[a^\dagger.]$ stands for the possible presence of an executed action prefix, with $a^\dagger$ being present at the beginning of the expansion iff at least one of $a_1^\dagger$ and $a_2^\dagger$ is present at the beginning of P_1 and P_2 respectively. In P_1 and P_2, as well as on the righthand side of the expansion, summations are allowed by axioms $\mathsf{A}_{\text{F},1}$ and $\mathsf{A}_{\text{F},2}$ and represent $\underline{0}$ when their index sets are empty (so that $\mathsf{A}_{\text{F}} \vdash \underline{0} \parallel_L \underline{0} = \underline{0} + \underline{0} + \underline{0} = \underline{0}$ due to axiom $\mathsf{A}_{\text{F},3}$, substitutivity with respect to alternative composition, and transitivity).

Following [88], to show the soundness and ground completeness of A_{F} for $\sim_{\text{FB:ps}}$ we introduce a suitable normal form to which every process can be reduced. The only operators that can occur in such a normal form are action prefix and alternative composition, hence all processes in normal form are sequential and renaming free.

Definition 6.1. *We say that $P \in \mathbb{P}$ is in* forward normal form*, written* F-nf*, iff it is equal to $[a^\dagger.] \sum_{i \in I} a_i \,.\, P_i$ where the executed action prefix $a^\dagger.\_$ is optional, I is a finite index set (with the summation being $\underline{0}$ when $I = \emptyset$), and each P_i is initial and in F-nf.* ■

Lemma 6.1. *For all (initial) $P \in \mathbb{P}$ there exists (an initial) $Q \in \mathbb{P}$ in F-nf such that $\mathsf{A}_{\text{F}} \vdash P = Q$.*

$$
\begin{array}{lrcll}
(\mathsf{A}_{\mathrm{F},1}) & (P + Q) + R & = & P + (Q + R) & \text{where at least two among } P,\ Q,\ R \text{ are initial} \\
(\mathsf{A}_{\mathrm{F},2}) & P + Q & = & Q + P & \text{where } \mathit{initial}(P) \vee \mathit{initial}(Q) \\
(\mathsf{A}_{\mathrm{F},3}) & P + \underline{0} & = & P & \\
(\mathsf{A}_{\mathrm{F},4}) & P + P & = & P & \text{where } \mathit{initial}(P) \\
(\mathsf{A}_{\mathrm{F},5}) & \underline{0} \llcorner \rho \urcorner & = & \underline{0} & \\
(\mathsf{A}_{\mathrm{F},6}) & (a \,.\, P) \llcorner \rho \urcorner & = & \rho(a) \,.\, (P \llcorner \rho \urcorner) & \text{where } \mathit{initial}(P) \\
(\mathsf{A}_{\mathrm{F},7}) & (a^\dagger \,.\, P) \llcorner \rho \urcorner & = & \rho(a)^\dagger \,.\, (P \llcorner \rho \urcorner) & \\
(\mathsf{A}_{\mathrm{F},8}) & (P + Q) \llcorner \rho \urcorner & = & (P \llcorner \rho \urcorner) + (Q \llcorner \rho \urcorner) & \text{where } \mathit{initial}(P) \vee \mathit{initial}(Q) \\
(\mathsf{A}_{\mathrm{F},9}) & a^\dagger \,.\, P & = & b^\dagger \,.\, P & \text{if } \mathit{initial}(P) \\
(\mathsf{A}_{\mathrm{F},10}) & a^\dagger \,.\, P & = & P & \text{if } \neg \mathit{initial}(P) \\
(\mathsf{A}_{\mathrm{F},11}) & P + Q & = & P & \text{if } \neg \mathit{initial}(P), \text{ where } \mathit{initial}(Q)
\end{array}
$$

$$
\begin{array}{lrcl}
(\mathsf{A}_{\mathrm{F},12}) & P_1 \parallel_L P_2 & = & [a^\dagger.] \Bigg(\displaystyle\sum_{i \in I_1, a_{1,i} \notin L} a_{1,i} \,.\, (P_{1,i} \parallel_L P'_2) + \\
& & & \displaystyle\sum_{i \in I_2, a_{2,i} \notin L} a_{2,i} \,.\, (P'_1 \parallel_L P_{2,i}) + \\
& & & \displaystyle\sum_{i \in I_1, a_{1,i} \in L} \sum_{j \in I_2, a_{2,j} = a_{1,i}} a_{1,i} \,.\, (P_{1,i} \parallel_L P_{2,j}) \Bigg)
\end{array}
$$

with $P_k = [a_k^\dagger.]P'_k$, $P'_k = \sum_{i \in I_k} a_{k,i} \,.\, P_{k,i}$, in F-nf for $k \in \{1, 2\}$ and $a^\dagger$ being present iff so is $a_1^\dagger$ or $a_2^\dagger$

Table 6.1: Axioms characterizing $\sim_{\mathrm{FB:ps}}$

Proof. We proceed by induction on the syntactical structure of $P \in \mathbb{P}$:

- If P is $\underline{0}$ then the result follows by taking Q equal to $\underline{0}$ due to reflexivity.
- If P is $a \,.\, P'$ where P' is initial, then by the induction hypothesis there exists Q' initial and in F-nf such that $\mathsf{A}_{\mathrm{F}} \vdash P' = Q'$. The result follows by taking Q equal to $a \,.\, Q'$ – which is in F-nf because Q' is initial and in F-nf – due to substitutivity with respect to action prefix.
- If P is $a^\dagger \,.\, P'$ then by the induction hypothesis there exists Q' in F-nf such that $\mathsf{A}_{\mathrm{F}} \vdash P' = Q'$. There are two cases:
  - If P' and Q' are both initial, then the result follows by taking Q equal to $a^\dagger \,.\, Q'$ – which is in F-nf because Q' is initial and in F-nf – due to substitutivity with respect to executed action prefix.
  - Let P' and Q' be both non-initial. Since Q' is in F-nf and hence features a single executed action prefix at the beginning, i.e., Q' is $b^\dagger \,.\, Q''$ with Q'' initial and in F-nf, the result follows by taking Q equal to Q' by virtue of $\mathsf{A}_{\mathrm{F}} \vdash a^\dagger \,.\, P' = a^\dagger \,.\, Q'$ due to substitutivity with respect to executed action prefix, $\mathsf{A}_{\mathrm{F}} \vdash a^\dagger \,.\, Q' = Q'$ due to axiom $\mathsf{A}_{\mathrm{F},10}$, and transitivity.
- If P is $P' \llcorner \rho \urcorner$ then by the induction hypothesis there exists Q' in F-nf – say $Q' = [a^\dagger.] \sum_{i \in I} a_i \,.\, Q_i$ – such that $\mathsf{A}_{\mathrm{F}} \vdash P' = Q'$, hence $\mathsf{A}_{\mathrm{F}} \vdash P' \llcorner \rho \urcorner = Q' \llcorner \rho \urcorner$ due to substitutivity with respect to renaming. The result follows after possibly repeated applications of axioms $\mathsf{A}_{\mathrm{F},5}$ to $\mathsf{A}_{\mathrm{F},8}$ to $Q' \llcorner \rho \urcorner$ due to transitivity.

- If P is $P_1 + P_2$ then by the induction hypothesis there exist Q_1 and Q_2 in F-nf such that $\mathsf{A}_{\mathrm{F}} \vdash P_1 = Q_1$ and $\mathsf{A}_{\mathrm{F}} \vdash P_2 = Q_2$, hence $\mathsf{A}_{\mathrm{F}} \vdash P_1 + P_2 = Q_1 + Q_2$ due to substitutivity with respect to alternative composition. There are three cases:
  - If P_1 and P_2 are both initial, then Q_1 and Q_2 are both initial too and hence the result follows by taking Q equal to $Q_1 + Q_2$, up to an application of axiom $\mathsf{A}_{\mathrm{F},3}$ in the case that $Q_1 + Q_2$ is not in F-nf because Q_1 and Q_2 are not different from $\underline{0}$ (possibly preceded by an application of axiom $\mathsf{A}_{\mathrm{F},2}$ to move the $\underline{0}$ subprocess to the right of $+$) and transitivity.
  - If only P_2 is initial, then only Q_2 is initial too and hence the result follows by taking Q equal to Q_1 by virtue of $\mathsf{A}_{\mathrm{F}} \vdash Q_1 + Q_2 = Q_1$ due to axiom $\mathsf{A}_{\mathrm{F},11}$ and transitivity.
  - If only P_1 is initial, then only Q_1 is initial too and hence the result follows by taking Q equal to Q_2 by virtue of $\mathsf{A}_{\mathrm{F}} \vdash Q_1 + Q_2 = Q_2 + Q_1$ due to axiom $\mathsf{A}_{\mathrm{F},2}$, $\mathsf{A}_{\mathrm{F}} \vdash Q_2 + Q_1 = Q_2$ due to axiom $\mathsf{A}_{\mathrm{F},11}$, and transitivity.

- If P is $P_1 \parallel_L P_2$ then by the induction hypothesis there exist Q_1 and Q_2 in F-nf – say $Q_1 = [a_1^\dagger.]Q_1'$ with $Q_1' = \sum_{i \in I_1} a_{1,i} \,.\, Q_{1,i}$ and $Q_2 = [a_2^\dagger.]Q_2'$ with $Q_2' = \sum_{i \in I_2} a_{2,i} \,.\, Q_{2,i}$ – such that $\mathsf{A}_{\mathrm{F}} \vdash P_1 = Q_1$ and $\mathsf{A}_{\mathrm{F}} \vdash P_2 = Q_2$, hence $\mathsf{A}_{\mathrm{F}} \vdash P_1 \parallel_L P_2 = Q_1 \parallel_L Q_2$ due to substitutivity with respect to parallel composition. As a consequence $\mathsf{A}_{\mathrm{F}} \vdash P_1 \parallel_L P_2 = [a^\dagger.](\sum_{i \in I_1, a_{1,i} \notin L} a_{1,i} \,.\, (Q_{1,i} \parallel_L Q_2') + \sum_{i \in I_2, a_{2,i} \notin L} a_{2,i} \,.\, (Q_1' \parallel_L Q_{2,i}) + \sum_{i \in I_1, a_{1,i} \in L} \sum_{j \in I_2, a_{2,j} = a_{1,i}} a_{1,i} \,.\, (Q_{1,i} \parallel_L Q_{2,j}))$ due to axiom $\mathsf{A}_{\mathrm{F},12}$ and transitivity. We recall that Q_1', Q_2', and every $Q_{1,i}$ and $Q_{2,i}$ are all initial and in F-nf. Moreover, thanks to axiom $\mathsf{A}_{\mathrm{F},9}$ we can assume that either $a_1, a_2 \notin L$ or $a_1 = a_2 \in L$ so as to ensure that $Q_1 \parallel_L Q_2 \in \mathbb{P}$.
  We now prove that, if $O_1, O_2 \in \mathbb{P}$ are (initial and) in F-nf and such that $O_1 \parallel_L O_2 \in \mathbb{P}$, then there exists $O \in \mathbb{P}$ (initial and) in F-nf such that $\mathsf{A}_{\mathrm{F}} \vdash O_1 \parallel_L O_2 = O$, from which the result will follow due to substitutivity with respect to action prefix, alternative composition, and executed action prefix if any. Since the parallel processes that we will encounter are not subprocesses of $O_1 \parallel_L O_2$, we proceed by induction on $\mathit{size}(O_1 \parallel_L O_2)$:
  - If $\mathit{size}(O_1 \parallel_L O_2) = 0$ then $O_1 \parallel_L O_2$ is $\underline{0} \parallel_L \underline{0}$ where $\mathsf{A}_{\mathrm{F}} \vdash \underline{0} \parallel_L \underline{0} = \underline{0} + \underline{0} + \underline{0}$ due to axiom $\mathsf{A}_{\mathrm{F},12}$. The result follows by taking O equal to $\underline{0}$ due to axiom $\mathsf{A}_{\mathrm{F},3}$ applied twice, substitutivity with respect to alternative composition, and transitivity.
  - If $\mathit{size}(O_1 \parallel_L O_2) > 0$ then $O_1 = [b_1^\dagger.]O_1'$ with $O_1' = \sum_{i \in J_1} b_{1,i} \,.\, O_{1,i}$ and $O_2 = [b_2^\dagger.]O_2'$ with $O_2' = \sum_{i \in J_2} b_{2,i} \,.\, O_{2,i}$, where at least one of the following holds: $b_1^\dagger$ present, $J_1 \neq \emptyset$, $b_2^\dagger$ present, $J_2 \neq \emptyset$. Thus $\mathsf{A}_{\mathrm{F}} \vdash O_1 \parallel_L O_2 = [b^\dagger.] \sum_{i \in J_1, b_{1,i} \notin L} b_{1,i} \,.\, (O_{1,i} \parallel_L O_2') + \sum_{i \in J_2, b_{2,i} \notin L} b_{2,i} \,.\, (O_1' \parallel_L O_{2,i}) + \sum_{i \in J_1, b_{1,i} \in L} \sum_{j \in J_2, b_{2,j} = b_{1,i}} b_{1,i} \,.\, (O_{1,i} \parallel_L O_{2,j})$ due to axiom $\mathsf{A}_{\mathrm{F},12}$. The result follows by applying the induction hypothesis to every $O_{1,i} \parallel_L O_2'$, $O_1' \parallel_L O_{2,i}$, $O_{1,i} \parallel_L O_{2,j}$ due to substitutivity with respect to action prefix, alternative composition, and executed action prefix if any, with possible applications of axiom $\mathsf{A}_{\mathrm{F},3}$ (each possibly preceded by an application of axiom $\mathsf{A}_{\mathrm{F},2}$ to move the $\underline{0}$ subprocess to the right of $+$). ∎

Theorem 6.1. *Let $P_1, P_2 \in \mathbb{P}$. Then $P_1 \sim_{\mathrm{FB:ps}} P_2$ iff $\mathsf{A}_{\mathrm{F}} \vdash P_1 = P_2$.*

Proof. Soundness, i.e., $\mathsf{A}_{\mathrm{F}} \vdash P_1 = P_2 \implies P_1 \sim_{\mathrm{FB:ps}} P_2$, is a straightforward consequence of the general axioms and inference rules behind $\vdash$ (see Section 6.1) together with $\sim_{\mathrm{FB:ps}}$ being an equivalence relation (see Proposition 4.1)

and a congruence (see Theorem 4.1), plus the fact that the lefthand side process of each additional axiom in Table 6.1 is $\sim_{\rm FB:ps}$-equivalent to the righthand side process of the same axiom.
Let us address ground completeness, i.e., $P_1 \sim_{\rm FB:ps} P_2 \implies \mathsf{A_F} \vdash P_1 = P_2$. We suppose that P_1 and P_2 are both in F-nf and proceed by induction on the syntactical structure of P_1:

- If P_1 is $\underline{0}$ then from $P_1 \sim_{\rm FB:ps} P_2$ and P_2 in F-nf we derive that P_2 can only be $\underline{0}$, from which the result follows by reflexivity.
- If P_1 is $[a_1^\dagger.] \sum_{i \in I_1} a_{1,i} \,.\, P_{1,i}$ with $a_1^\dagger$ present or $I_1 \neq \emptyset$, then from $P_1 \sim_{\rm FB:ps} P_2$ and P_2 in F-nf we derive that P_2 can only be $[a_2^\dagger.] \sum_{i \in I_2} a_{2,i} \,.\, P_{2,i}$ with $a_2^\dagger$ present iff $a_1^\dagger$ present and $I_2 \neq \emptyset$ iff $I_1 \neq \emptyset$. We recall that every $P_{1,i}$ and every $P_{2,i}$ is initial and in F-nf.
  Since $P_1 \sim_{\rm FB:ps} P_2$, for each $i_1 \in I_1$ there exists $i_2 \in I_2$ such that $a_{1,i_1} = a_{2,i_2}$ and $P_{1,i_1} \sim_{\rm FB:ps} P_{2,i_2}$, and vice versa. From the induction hypothesis we obtain that $\mathsf{A_F} \vdash P_{1,i_1} = P_{2,i_2}$. It then follows that:
  - $\mathsf{A_F} \vdash a_{1,i_1} \,.\, P_{1,i_1} = a_{2,i_2} \,.\, P_{2,i_2}$ due to substitutivity with respect to action prefix.
  - $\mathsf{A_F} \vdash \sum_{i \in I_1} a_{1,i} \,.\, P_{1,i} = \sum_{i \in I_2} a_{2,i} \,.\, P_{2,i}$ due to substitutivity with respect to alternative composition as well as axiom $\mathsf{A}_{\mathrm{F},4}$ and transitivity in the presence of identical summands on the same side that are absent on the other side (possibly preceded by applications of axioms $\mathsf{A}_{\mathrm{F},1}$ and $\mathsf{A}_{\mathrm{F},2}$ to move identical summands next to each other).
  - $\mathsf{A_F} \vdash [a_1^\dagger.] \sum_{i \in I_1} a_{1,i} \,.\, P_{1,i} = [a_1^\dagger.] \sum_{i \in I_2} a_{2,i} \,.\, P_{2,i}$ due to substitutivity with respect to executed action prefix.
  - $\mathsf{A_F} \vdash [a_1^\dagger.] \sum_{i \in I_1} a_{1,i} \,.\, P_{1,i} = [a_2^\dagger.] \sum_{i \in I_2} a_{2,i} \,.\, P_{2,i}$ due to axiom $\mathsf{A}_{\mathrm{F},9}$ and transitivity if $a_2 \neq a_1$.

If P_1 and P_2 are not both in F-nf, thanks to Lemma 6.1 we can find Q_1 and Q_2 in F-nf, each of which is initial iff so is its corresponding original process, such that $\mathsf{A_F} \vdash P_1 = Q_1$ and $\mathsf{A_F} \vdash P_2 = Q_2$, hence $\mathsf{A_F} \vdash Q_2 = P_2$ by symmetry. Due to soundness, we get $P_1 \sim_{\rm FB:ps} Q_1$, hence $Q_1 \sim_{\rm FB:ps} P_1$ as $\sim_{\rm FB:ps}$ is symmetric, and $P_2 \sim_{\rm FB:ps} Q_2$. Since $P_1 \sim_{\rm FB:ps} P_2$, we also get $Q_1 \sim_{\rm FB:ps} Q_2$ as $\sim_{\rm FB:ps}$ is transitive. By virtue of what has been shown above, from $Q_1 \sim_{\rm FB:ps} Q_2$ with Q_1 and Q_2 in F-nf it follows that $\mathsf{A_F} \vdash Q_1 = Q_2$ and hence $\mathsf{A_F} \vdash P_1 = P_2$ by transitivity. ■

6.3.2 Axiomatization of $\approx_{\rm FB:ps}$

To equationally characterize $\approx_{\rm FB:ps}$, in addition to the axioms in Table 6.1 we have to consider the τ-laws in Table 6.2. Axioms $\mathsf{A}^\tau_{\mathrm{F},1}$ to $\mathsf{A}^\tau_{\mathrm{F},3}$ coincide with those for the weak bisimulation congruence over forward-only processes of [112]. A variant of $\mathsf{A}^\tau_{\mathrm{F},1}$ with a being decorated on both sides, i.e., axiom $\mathsf{A}^\tau_{\mathrm{F},4}$, is also needed for achieving ground completeness in our reversible setting. We denote by $\mathsf{A}^\tau_{\mathrm{F}}$ the set of axioms in Tables 6.1 and 6.2.

Note that $a^\dagger \,.\, \tau^\dagger \,.\, P = a^\dagger \,.\, P$ can instead be derived from axiom $\mathsf{A}_{\mathrm{F},9}$ or $\mathsf{A}_{\mathrm{F},10}$ depending on whether P is initial or not ($\tau^\dagger \,.\, P = a^\dagger \,.\, P$) and axiom $\mathsf{A}_{\mathrm{F},10}$ applied only to the lefthand side, along with transitivity. Likewise, $P' + \tau \,.\, P = \tau^\dagger \,.\, P'$ where P' is not initial and $P + \tau^\dagger \,.\, P' = \tau^\dagger \,.\, P'$ where P' may not be initial, as well as $a^\dagger \,.\, (P' + \tau \,.\, Q) + a \,.\, Q = a^\dagger \,.\, (P' + \tau \,.\, Q)$, $a^\dagger \,.\, (P + \tau^\dagger \,.\, Q') + a \,.\, Q = a^\dagger \,.\, (P + \tau^\dagger \,.\, Q')$, and $a \,.\, (P + \tau \,.\, Q) + a^\dagger \,.\, Q' = a^\dagger \,.\, (P + \tau^\dagger \,.\, Q')$, where P' and Q' may not be initial, can be derived by exploiting axiom $\mathsf{A}_{\mathrm{F},11}$ too.

$(\mathsf{A}^{\tau}_{\mathrm{F},1})$	$a\,.\,\tau\,.\,P$	$=$	$a\,.\,P$	where $\mathit{initial}(P)$
$(\mathsf{A}^{\tau}_{\mathrm{F},2})$	$P + \tau\,.\,P$	$=$	$\tau\,.\,P$	where $\mathit{initial}(P)$
$(\mathsf{A}^{\tau}_{\mathrm{F},3})$	$a\,.\,(P + \tau\,.\,Q) + a\,.\,Q$	$=$	$a\,.\,(P + \tau\,.\,Q)$	where $\mathit{initial}(P) \wedge \mathit{initial}(Q)$
$(\mathsf{A}^{\tau}_{\mathrm{F},4})$	$a^{\dagger}\,.\,\tau\,.\,P$	$=$	$a^{\dagger}\,.\,P$	where $\mathit{initial}(P)$

Table 6.2: Additional τ-axioms for $\approx_{\mathrm{FB:ps}}$

Lemma 6.2. *For all (initial) $P \in \mathbb{P}$ there exists (an initial) $Q \in \mathbb{P}$ in F-nf such that $\mathsf{A}^{\tau}_{\mathrm{F}} \vdash P = Q$.*

Proof. See the proof of Lemma 6.1, as in the considered normal form τ-actions do not play a role different from the one of observable actions. In particular, unexecuted τ-actions are not abstracted away unless they are inside non-selected alternative subprocesses. ∎

In addition to the forward normal form of Definition 6.1, we use a function that extracts the forward behavior from a process by eliminating executed actions and non-selected alternative subprocesses. Function $\mathit{to\_forward} : \mathbb{P} \to \mathbb{P}_{\mathrm{init}}$ is defined by induction on the syntactical structure of $P \in \mathbb{P}$ as follows:

$$\begin{array}{rcll}
\mathit{to_forward}(P) & = & P & \text{if } \mathit{initial}(P) \\
\mathit{to_forward}(a^{\dagger}\,.\,P') & = & \mathit{to_forward}(P') & \\
\mathit{to_forward}(P' \llcorner \rho \urcorner) & = & \mathit{to_forward}(P') \llcorner \rho \urcorner & \text{if } \neg\mathit{initial}(P') \\
\mathit{to_forward}(P_1 + P_2) & = & \mathit{to_forward}(P_1) & \text{if } \neg\mathit{initial}(P_1) \wedge \mathit{initial}(P_2) \\
\mathit{to_forward}(P_1 + P_2) & = & \mathit{to_forward}(P_2) & \text{if } \neg\mathit{initial}(P_2) \wedge \mathit{initial}(P_1) \\
\mathit{to_forward}(P_1 \parallel_L P_2) & = & \mathit{to_forward}(P_1) \parallel_L \mathit{to_forward}(P_2) & \text{if } \neg\mathit{initial}(P_1) \vee \neg\mathit{initial}(P_2)
\end{array}$$

The resulting initial process preserves the forward behavior of the original process in the following sense.

Proposition 6.1. *Let $P, P', P'', Q \in \mathbb{P}$ and $\theta', \theta'' \in \Theta$. Then:*

1. *$\mathit{to\_forward}(P) = P$ when $\mathit{initial}(P)$ while $\mathit{to\_forward}(P) \sim_{\mathrm{FB}} P$ when $\neg\mathit{initial}(P)$.*
2. *$\mathit{to\_forward}(P) \xrightarrow{\theta'} P'$ iff $P \xrightarrow{\theta''} P''$ with $\mathit{act}(\theta') = \mathit{act}(\theta'')$ and $P' \sim_{\mathrm{FB:ps}} P''$.*
3. *If $P \approx_{\mathrm{FB:ps}} Q$ then $\mathit{to\_forward}(P) \approx_{\mathrm{FB:ps}} \mathit{to\_forward}(Q)$ when P and Q are initial or cannot execute τ-actions, otherwise $\mathit{to\_forward}(P) \approx_{\mathrm{FB}} \mathit{to\_forward}(Q)$.*

Proof. The first property is a straightforward consequence of the definition of *to_forward* and the fact that $\sim_{\mathrm{FB}}$ considers only the forward behavior of processes, as $\mathit{to\_forward}(P)$ is obtained from P by removing all decorated (i.e., executed) actions as well as all non-selected alternative subprocesses, which are all the parts of P from which an outgoing transition cannot be generated. Note that $\mathit{to\_forward}(P) \sim_{\mathrm{FB:ps}} P$ does not hold when P is not initial because $\mathit{to\_forward}(P)$ is initial.
The second property is a consequence of the first one, with P' (resp. θ') not coinciding with P'' (resp. θ'') when P is not initial because in that case P'' contains decorated actions along with possible non-selected alternative subprocesses that cannot be present in P'. However $P' \sim_{\mathrm{FB:ps}} P''$ (in lieu of $P' \sim_{\mathrm{FB}} P''$ only) because both P' and P'' are not initial.

As for the third property, we consider the following two cases:

- If both P and Q are initial, then $to\_forward(P) = P \approx_{\rm FB:ps} Q = to\_forward(Q)$.
- If both P and Q are not initial, then $to\_forward(P) \neq P$ and $to\_forward(Q) \neq Q$.
  Suppose that $to\_forward(P) \xrightarrow{\theta'} P'$. Then, due to the second property, $P \xrightarrow{\theta''} P''$ with $act(\theta') = act(\theta'')$ and $P' \sim_{\rm FB:ps} P''$, hence $P' \approx_{\rm FB:ps} P''$ because $\sim_{\rm FB:ps}$ is contained in $\approx_{\rm FB:ps}$. There are two subcases:
  - If $act(\theta'') = \tau$ then from $P \approx_{\rm FB:ps} Q$ it follows that $Q \Longrightarrow Q''$ with $P'' \approx_{\rm FB:ps} Q''$. By repeatedly applying the second property along $Q \Longrightarrow Q''$ we get $to\_forward(Q) \Longrightarrow Q'$ with $Q' \approx_{\rm FB} Q''$ (instead of $Q' \approx_{\rm FB:ps} Q''$) as Q'' is not initial while Q' may be initial (this is the case when no τ is performed by $to\_forward(Q)$). Since $\approx_{\rm FB:ps}$ is contained in $\approx_{\rm FB}$, the result stems from $P' \approx_{\rm FB} P'' \approx_{\rm FB} Q'' \approx_{\rm FB} Q'$ as $\approx_{\rm FB}$ is symmetric and transitive.
  - If $act(\theta'') \neq \tau$ then from $P \approx_{\rm FB:ps} Q$ it follows that $Q \Longrightarrow \xrightarrow{\theta} \Longrightarrow Q''$ with $act(\theta'') = act(\theta)$ and $P'' \approx_{\rm FB:ps} Q''$. By repeatedly applying the second property along $Q \Longrightarrow \xrightarrow{\theta} \Longrightarrow Q''$ we get $to\_forward(Q) \Longrightarrow \xrightarrow{\theta'''} \Longrightarrow Q'$ with $act(\theta''') = act(\theta)$ and $Q' \approx_{\rm FB:ps} Q''$ (as neither Q' nor Q'' is initial). The result stems from $P' \approx_{\rm FB:ps} P'' \approx_{\rm FB:ps} Q'' \approx_{\rm FB:ps} Q'$ as $\approx_{\rm FB:ps}$ is symmetric and transitive. ∎

Furthermore, following the approach used for the weak bisimulation congruence over forward-only processes of [112], we introduce a *saturated* forward normal form where, for every transition sequence in which a transition labeled with a certain action is preceded or followed by finitely many τ-transitions, a direct transition labeled with that action is present too. Unlike [112], where both the transition sequence and the direct transition have the same target process, here two distinct $\approx_{\rm FB:ps}$-equivalent target processes P' (for the transition sequence) and P'' (for the direct transition) come into play due to the presence of decorated actions within processes.

Definition 6.2. *We say that $P \in \mathbb{P}$ is in* saturated forward normal form*, written* sat-F-nf*, iff it is equal to $[b^\dagger.]\sum_{i\in I} a_i \,.\, P_i$ where the executed action prefix $b^\dagger.\_$ is optional, I is a finite index set (with the summation being $\underline{0}$ when $I = \emptyset$), each P_i is initial and in sat-F-nf, and if $P \Longrightarrow \xrightarrow{\theta'} \Longrightarrow P'$ then $P \xrightarrow{\theta''} P''$ with $act(\theta') = act(\theta'')$ and $P' \approx_{\rm FB:ps} P''$.* ∎

This leads to the so-called *saturation lemma* below, which is instrumental to reduce in sat-F-nf every process in F-nf. Unlike [112], it features $to\_forward(P')$ in place of P' in the final part of its statement otherwise we would have the unexecuted action $act(\theta)$ followed by the non-initial process P', which does not yield a well-formed process.

Lemma 6.3. *Let $P, P' \in \mathbb{P}$ and $\theta \in \Theta$. If P is initial and $P \Longrightarrow \xrightarrow{\theta} \Longrightarrow P'$, then $\mathsf{A}^\tau_{\rm F} \vdash P = P + act(\theta) \,.\, to\_forward(P')$.*

Proof. Suppose that the initial process $P \in \mathbb{P}$ is in F-nf. Should this not be the case, thanks to Lemma 6.2 we could find Q initial and in F-nf such that $\mathsf{A}^\tau_{\rm F} \vdash P = Q$, hence proving the result for Q would entail the validity of the result for P by substitutivity. In particular:

- If $P \Longrightarrow \xrightarrow{\theta} \Longrightarrow P'$ then $Q \Longrightarrow \xrightarrow{\theta'} \Longrightarrow Q'$ with $act(\theta) = act(\theta')$ and $P' \approx_{\rm FB:ps} Q'$ due to $\mathsf{A}^\tau_{\rm F} \vdash P = Q$ implying $P \approx_{\rm FB:ps} Q$ by soundness (forthcoming Theorem 6.2) and the fact that Q cannot idle when $act(\theta) = \tau$ because P and Q are both initial and hence P' and Q' must be both non-initial as $P' \approx_{\rm FB:ps} Q'$.

- $\mathsf{A}_{\mathrm{F}}^{\tau} \vdash \mathit{to\_forward}(P') = \mathit{to\_forward}(Q')$ because, observing that $\mathit{to\_forward}(Q')$ is in F-nf given that so is Q, $\underline{0}$-summands and replicated summands possibly occurring in $\mathit{to\_forward}(P')$ can be eliminated via axioms $\mathsf{A}_{\mathrm{F},3}$ and $\mathsf{A}_{\mathrm{F},4}$, respectively, as well as renamings and parallel compositions possibly occurring in $\mathit{to\_forward}(P')$ can be eliminated via axioms $\mathsf{A}_{\mathrm{F},5}$ to $\mathsf{A}_{\mathrm{F},8}$ and $\mathsf{A}_{\mathrm{F},12}$, respectively, and Q is a F-nf for P so that Q' cannot abstract from unexecuted τ-actions unless they are inside non-selected alternative subprocesses (which by the way can occur neither in $\mathit{to\_forward}(P')$ nor in $\mathit{to\_forward}(Q')$ as they are both initial).

We thus proceed by induction on the syntactical structure of the initial process P in F-nf such that $P \Longrightarrow \xrightarrow{\theta} \Longrightarrow P'$ (note that P cannot be $\underline{0}$ and cannot feature any executed action at the beginning), where in the following any summation is meant to disappear when the corresponding finite index set I is empty:

- If P is $\sum_{i \in I} a_i \,.\, P_i + \mathit{act}(\theta) \,.\, \bar{P}$ and P' is $\sum_{i \in I} a_i \,.\, P_i + \mathit{act}(\theta)^{\dagger} \,.\, \bar{P}$ – i.e., there are no τ-transitions preceding or following the $\mathit{act}(\theta)$-transition in $P \Longrightarrow \xrightarrow{\theta} \Longrightarrow P'$ – where we note that $\bar{P}$ is initial and in F-nf because so is P, then $\mathsf{A}_{\mathrm{F}}^{\tau} \vdash P = P + \mathit{act}(\theta) \,.\, \bar{P}$ by axiom $\mathsf{A}_{\mathrm{F},4}$ applied to $\mathit{act}(\theta) \,.\, \bar{P}$ and substitutivity inside P, with $\bar{P} = \mathit{to\_forward}(P')$.

- If P is $\sum_{i \in I} a_i \,.\, P_i + \mathit{act}(\theta) \,.\, Q$ and $\sum_{i \in I} a_i \,.\, P_i + \mathit{act}(\theta)^{\dagger} \,.\, Q \Longrightarrow \xrightarrow{\theta'} \Longrightarrow P'$ with $\mathit{act}(\theta') = \tau$ – i.e., no τ-transition precedes but at least one τ-transition follows the $\mathit{act}(\theta)$-transition in $P \Longrightarrow \xrightarrow{\theta} \Longrightarrow P'$ – then:

  - Since $\sum_{i \in I} a_i \,.\, P_i + \mathit{act}(\theta)^{\dagger} \,.\, Q \Longrightarrow \xrightarrow{\theta'} \Longrightarrow P'$ comes from $Q \Longrightarrow \xrightarrow{\theta''} \Longrightarrow Q'$ with $\mathit{act}(\theta'') = \tau$, $\mathit{to\_forward}(P') = \mathit{to\_forward}(Q')$, and Q initial and in F-nf, by the induction hypothesis $\mathsf{A}_{\mathrm{F}}^{\tau} \vdash Q = Q + \tau \,.\, \mathit{to\_forward}(P')$.
  - $\mathsf{A}_{\mathrm{F}}^{\tau} \vdash P = P + \mathit{act}(\theta) \,.\, \mathit{to\_forward}(P')$ because:
    * $\mathsf{A}_{\mathrm{F}}^{\tau} \vdash P = P + \mathit{act}(\theta) \,.\, Q$ by axiom $\mathsf{A}_{\mathrm{F},4}$ applied to $\mathit{act}(\theta) \,.\, Q$ and substitutivity inside P.
    * $\mathsf{A}_{\mathrm{F}}^{\tau} \vdash P = P + \mathit{act}(\theta) \,.\, (Q + \tau \,.\, \mathit{to\_forward}(P'))$ by substitutivity and transitivity.
    * $\mathsf{A}_{\mathrm{F}}^{\tau} \vdash P = P + \mathit{act}(\theta) \,.\, (Q + \tau \,.\, \mathit{to\_forward}(P')) + \mathit{act}(\theta) \,.\, \mathit{to\_forward}(P')$ by axiom $\mathsf{A}_{\mathrm{F},3}^{\tau}$, substitutivity, and transitivity.
    * $\mathsf{A}_{\mathrm{F}}^{\tau} \vdash P = P + \mathit{act}(\theta) \,.\, Q + \mathit{act}(\theta) \,.\, \mathit{to\_forward}(P')$ by substitutivity and transitivity.
    * $\mathsf{A}_{\mathrm{F}}^{\tau} \vdash P = P + \mathit{act}(\theta) \,.\, \mathit{to\_forward}(P')$ by axiom $\mathsf{A}_{\mathrm{F},4}$ as P contains $\mathit{act}(\theta) \,.\, Q$ as summand, substitutivity, and transitivity.

- If P is $\sum_{i \in I} a_i \,.\, P_i + \tau \,.\, Q$ and $\sum_{i \in I} a_i \,.\, P_i + \tau^{\dagger} \,.\, Q \Longrightarrow \xrightarrow{\theta} \Longrightarrow P'$ – i.e., at least one τ-transition precedes the $\mathit{act}(\theta)$-transition in $P \Longrightarrow \xrightarrow{\theta} \Longrightarrow P'$ – then:

  - Since $\sum_{i \in I} a_i \,.\, P_i + \tau^{\dagger} \,.\, Q \Longrightarrow \xrightarrow{\theta} \Longrightarrow P'$ comes from $Q \Longrightarrow \xrightarrow{\theta'} \Longrightarrow Q'$ with $\mathit{act}(\theta) = \mathit{act}(\theta')$, $\mathit{to\_forward}(P') = \mathit{to\_forward}(Q')$, and Q initial and in F-nf, by the induction hypothesis $\mathsf{A}_{\mathrm{F}}^{\tau} \vdash Q = Q + \mathit{act}(\theta) \,.\, \mathit{to\_forward}(P')$.
  - $\mathsf{A}_{\mathrm{F}}^{\tau} \vdash P = P + \mathit{act}(\theta) \,.\, \mathit{to\_forward}(P')$ because:
    * $\mathsf{A}_{\mathrm{F}}^{\tau} \vdash P = P + \tau \,.\, Q$ by axiom $\mathsf{A}_{\mathrm{F},4}$ applied to $\tau \,.\, Q$ and substitutivity inside P.
    * $\mathsf{A}_{\mathrm{F}}^{\tau} \vdash P = P + \tau \,.\, Q + Q$ by axiom $\mathsf{A}_{\mathrm{F},2}^{\tau}$, symmetry, substitutivity, and transitivity.
    * $\mathsf{A}_{\mathrm{F}}^{\tau} \vdash P = P + \tau \,.\, Q + Q + \mathit{act}(\theta) \,.\, \mathit{to\_forward}(P')$ by substitutivity and transitivity.

- $\mathsf{A}^\tau_{\mathrm{F}} \vdash P = P + \tau \,.\, Q + act(\theta) \,.\, to\_forward(P')$ by symmetry, axiom $\mathsf{A}^\tau_{\mathrm{F},2}$, substitutivity, and transitivity.
- $\mathsf{A}^\tau_{\mathrm{F}} \vdash P = P + act(\theta) \,.\, to\_forward(P')$ by axiom $\mathsf{A}_{\mathrm{F},4}$ as P contains $\tau \,.\, Q$ as summand, substitutivity, and transitivity. ∎

Lemma 6.4. *For all (initial) $P \in \mathbb{P}$ in F-nf there exists (an initial) $Q \in \mathbb{P}$ in sat-F-nf such that $\mathsf{A}^\tau_{\mathrm{F}} \vdash P = Q$.*

Proof. We proceed by induction on the syntactical structure of $P \in \mathbb{P}$ in F-nf:

- If P is $\underline{0}$ then the result follows by taking Q equal to $\underline{0}$ due to reflexivity.
- If P is $\sum_{i \in I} a_i \,.\, P_i$ with $I \neq \emptyset$, then from the induction hypothesis it follows that for all $i \in I$ there exists Q_i in sat-F-nf such that $\mathsf{A}^\tau_{\mathrm{F}} \vdash P_i = Q_i$, hence $\mathsf{A}^\tau_{\mathrm{F}} \vdash P = \sum_{i \in I} a_i \,.\, Q_i$ by substitutivity with respect to action prefix and alternative composition.
  Suppose that $\sum_{i \in I} a_i \,.\, Q_i \Longrightarrow \xrightarrow{\theta'} \Longrightarrow Q'$ and – to avoid trivial cases – there is no Q'' such that $\sum_{i \in I} a_i \,.\, Q_i \xrightarrow{\theta''} Q''$ with $act(\theta') = act(\theta'')$ and $Q' \approx_{\mathrm{FB:ps}} Q''$. Since $\sum_{i \in I} a_i \,.\, Q_i$ is initial, from Lemma 6.3 we get $\mathsf{A}^\tau_{\mathrm{F}} \vdash \sum_{i \in I} a_i \,.\, Q_i = \sum_{i \in I} a_i \,.\, Q_i + act(\theta') \,.\, to\_forward(Q')$, hence $\mathsf{A}^\tau_{\mathrm{F}} \vdash P = \sum_{i \in I} a_i \,.\, Q_i + act(\theta') \,.\, to\_forward(Q')$ by transitivity, where each Q_i and $to\_forward(Q')$ are initial and in sat-F-nf.
  From $\sum_{i \in I} a_i \,.\, Q_i \Longrightarrow \xrightarrow{\theta'} \Longrightarrow Q'$ it follows that $\sum_{i \in I} a_i \,.\, Q_i + act(\theta') \,.\, to\_forward(Q') \Longrightarrow \xrightarrow{\theta'''} \Longrightarrow Q'''$ with $act(\theta''') = act(\theta')$ and $Q''' \approx_{\mathrm{FB:ps}} Q'$. Moreover $\sum_{i \in I} a_i \,.\, Q_i + act(\theta') \,.\, to\_forward(Q') \xrightarrow{\theta''''} \sum_{i \in I} a_i \,.\, Q_i + act(\theta')^\dagger \,.\, to\_forward(Q')$ with $act(\theta'''') = act(\theta')$, hence $act(\theta''') = act(\theta'''')$. From the fact that Q' and $act(\theta')^\dagger \,.\, to\_forward(Q')$ are both non-initial and Proposition 6.1 we get $Q' \approx_{\mathrm{FB:ps}} act(\theta')^\dagger \,.\, to\_forward(Q')$, at which point we exploit the soundness of axiom $\mathsf{A}_{\mathrm{F},11}$ (forthcoming Theorem 6.2) on the righthand side and the fact that $\approx_{\mathrm{FB:ps}}$ is transitive to obtain that $Q''' \approx_{\mathrm{FB:ps}} \sum_{i \in I} a_i \,.\, Q_i + act(\theta')^\dagger \,.\, to\_forward(Q')$.
- If P is $b^\dagger \,.\, \hat{P}$ then from the induction hypothesis it follows that there exists $\hat{Q}$ in sat-F-nf such that $\mathsf{A}^\tau_{\mathrm{F}} \vdash \hat{P} = \hat{Q}$, hence $\mathsf{A}^\tau_{\mathrm{F}} \vdash P = b^\dagger \,.\, \hat{Q}$ by substitutivity with respect to executed action prefix.
  Suppose that $b^\dagger \,.\, \hat{Q} \Longrightarrow \xrightarrow{\theta'} \Longrightarrow Q'$ and – to avoid trivial cases – there is no Q'' such that $b^\dagger \,.\, \hat{Q} \xrightarrow{\theta''} Q''$ with $act(\theta') = act(\theta'')$ and $Q' \approx_{\mathrm{FB:ps}} Q''$. Since $\hat{Q}$ is initial, from Lemma 6.3 and substitutivity with respect to executed action prefix we get $\mathsf{A}^\tau_{\mathrm{F}} \vdash b^\dagger \,.\, \hat{Q} = b^\dagger \,.\, (\hat{Q} + act(\theta') \,.\, to\_forward(Q'))$, hence $\mathsf{A}^\tau_{\mathrm{F}} \vdash P = b^\dagger \,.\, (\hat{Q} + act(\theta') \,.\, to\_forward(Q'))$ by transitivity, where $\hat{Q}$ and $to\_forward(Q')$ are initial and in sat-F-nf.
  From $b^\dagger \,.\, \hat{Q} \Longrightarrow \xrightarrow{\theta'} \Longrightarrow Q'$ it follows that $b^\dagger \,.\, (\hat{Q} + act(\theta') \,.\, to\_forward(Q')) \Longrightarrow \xrightarrow{\theta'''} \Longrightarrow Q'''$ with $act(\theta''') = act(\theta')$ and $Q''' \approx_{\mathrm{FB:ps}} Q'$. Moreover $b^\dagger \,.\, (\hat{Q} + act(\theta') \,.\, to\_forward(Q')) \xrightarrow{\theta''''} b^\dagger \,.\, (\hat{Q} + act(\theta')^\dagger \,.\, to\_forward(Q'))$ with $act(\theta'''') = act(\theta')$, hence $act(\theta''') = act(\theta'''')$. From the fact that Q' and $act(\theta')^\dagger \,.\, to\_forward(Q')$ are both non-initial and Proposition 6.1 we get $Q' \approx_{\mathrm{FB:ps}} act(\theta')^\dagger \,.\, to\_forward(Q')$, at which point we exploit the soundness of axioms $\mathsf{A}_{\mathrm{F},11}$ and $\mathsf{A}_{\mathrm{F},10}$ (forthcoming Theorem 6.2) on the righthand side and the fact that $\approx_{\mathrm{FB:ps}}$ is transitive to obtain that $Q''' \approx_{\mathrm{FB:ps}} b^\dagger \,.\, (\hat{Q} + act(\theta')^\dagger \,.\, to\_forward(Q'))$. ∎

Theorem 6.2. *Let $P_1, P_2 \in \mathbb{P}$. Then $P_1 \approx_{\mathrm{FB:ps}} P_2$ iff $\mathsf{A}^{\tau}_{\mathrm{F}} \vdash P_1 = P_2$.*

Proof. Soundness, i.e., $\mathsf{A}^{\tau}_{\mathrm{F}} \vdash P_1 = P_2 \Longrightarrow P_1 \approx_{\mathrm{FB:ps}} P_2$, is a straightforward consequence of the general axioms and inference rules behind $\vdash$ (see Section 6.1) together with $\approx_{\mathrm{FB:ps}}$ being an equivalence relation (see Proposition 4.2) and a congruence (see Theorem 4.2), plus the fact that the lefthand side process of each additional axiom in Tables 6.1 (recall that $\sim_{\mathrm{FB:ps}}$ is included in $\approx_{\mathrm{FB:ps}}$) and 6.2 is $\approx_{\mathrm{FB:ps}}$-equivalent to the righthand side process of the same axiom.
Let us address ground completeness, i.e., $P_1 \approx_{\mathrm{FB:ps}} P_2 \Longrightarrow \mathsf{A}^{\tau}_{\mathrm{F}} \vdash P_1 = P_2$. We suppose that P_1 and P_2 are both in sat-F-nf. Given that some of the processes that we will encounter are not subprocesses of P_1 or P_2 due to the application of axiom $\mathsf{A}^{\tau}_{\mathrm{F},1}$ or $\mathsf{A}^{\tau}_{\mathrm{F},4}$, we proceed by induction on $k = \mathit{size}(P_1) + \mathit{size}(P_2)$:

- If $k = 0$ then from $P_1 \approx_{\mathrm{FB:ps}} P_2$ and P_1 and P_2 in sat-F-nf we derive that P_1 and P_2 are both equal to $\underline{0}$, from which the result follows by reflexivity.
- Let $k \geq 2$ with P_1 being $\sum_{i \in I_1} a_{1,i} \,.\, P_{1,i}$ and P_2 being $\sum_{i \in I_2} a_{2,i} \,.\, P_{2,i}$, where $I_1 \neq \emptyset \neq I_2$ and every $P_{1,i}$ and every $P_{2,i}$ is initial and in sat-F-nf. Since $P_1 \approx_{\mathrm{FB:ps}} P_2$, whenever for some $a_{1,i_1} = a$ we have $P_1 \xrightarrow{\theta_1} a^{\dagger} \,.\, P_{1,i_1} + \sum_{i \in I_1 \setminus \{i_1\}} a_{1,i} \,.\, P_{1,i}$ with $\mathit{act}(\theta_1) = a$, then for some $a_{2,i_2} = a$ we have $P_2 \xrightarrow{\theta_2} a^{\dagger} \,.\, P_{2,i_2} + \sum_{i \in I_2 \setminus \{i_2\}} a_{2,i} \,.\, P_{2,i}$ with $\mathit{act}(\theta_2) = a$ as P_2 is in sat-F-nf, where $a^{\dagger} \,.\, P_{1,i_1} + \sum_{i \in I_1 \setminus \{i_1\}} a_{1,i} \,.\, P_{1,i} \approx_{\mathrm{FB:ps}} a^{\dagger} \,.\, P_{2,i_2} + \sum_{i \in I_2 \setminus \{i_2\}} a_{2,i} \,.\, P_{2,i}$, and vice versa. Since $\mathit{to\_forward}(a^{\dagger} \,.\, P_{1,i_1} + \sum_{i \in I_1 \setminus \{i_1\}} a_{1,i} \,.\, P_{1,i}) = P_{1,i_1}$ and $\mathit{to\_forward}(a^{\dagger} \,.\, P_{2,i_2} + \sum_{i \in I_2 \setminus \{i_2\}} a_{2,i} \,.\, P_{2,i}) = P_{2,i_2}$, from $a^{\dagger} \,.\, P_{1,i_1} + \sum_{i \in I_1 \setminus \{i_1\}} a_{1,i} \,.\, P_{1,i} \approx_{\mathrm{FB:ps}} a^{\dagger} \,.\, P_{2,i_2} + \sum_{i \in I_2 \setminus \{i_2\}} a_{2,i} \,.\, P_{2,i}$ and Proposition 6.1(3) two cases arise:
  - If $P_{1,i_1} \approx_{\mathrm{FB:ps}} P_{2,i_2}$ then from the induction hypothesis we obtain $\mathsf{A}^{\tau}_{\mathrm{F}} \vdash P_{1,i_1} = P_{2,i_2}$, hence $\mathsf{A}^{\tau}_{\mathrm{F}} \vdash a_{1,i_1} \,.\, P_{1,i_1} = a_{2,i_2} \,.\, P_{2,i_2}$ by substitutivity with respect to action prefix.
  - If $P_{1,i_1} \approx_{\mathrm{FB}} P_{2,i_2}$ but $P_{1,i_1} \not\approx_{\mathrm{FB:ps}} P_{2,i_2}$ – as is the case, e.g., when $a_{1,i_1} \,.\, P_{1,i_1}$ is $a \,.\, \tau \,.\, \underline{0}$ and $a_{2,i_2} \,.\, P_{2,i_2}$ is $a \,.\, \underline{0}$ – then P_{1,i_1} can execute τ-actions (thus reaching non-initial processes) to which P_{2,i_2} can respond only by idling (thus remaining in an initial process), or vice versa. If the considered summand of P_1 is $a_{1,i_1} \,.\, \tau \,.\, P'_{1,i_1}$, we exploit the soundness of axiom $\mathsf{A}^{\tau}_{\mathrm{F},1}$ to obtain $a_{1,i_1} \,.\, \tau \,.\, P'_{1,i_1} \approx_{\mathrm{FB:ps}} a_{1,i_1} \,.\, P''_{1,i_1}$ where P''_{1,i_1} is a subprocess of P'_{1,i_1} that is initial, in sat-F-nf, and not executing τ-actions, so that $P''_{1,i_1} \approx_{\mathrm{FB:ps}} P_{2,i_2}$ and we can then proceed like in the previous case by additionally applying axiom $\mathsf{A}^{\tau}_{\mathrm{F},1}$.
    More generally, the considered summand of P_1 may be of the form $a_{1,i_1} \,.\, (\tau \,.\, P'_{1,i_1} + \ldots)$, but then P'_{1,i_1}, after executing possible τ-actions, must offer all the alternative observable actions enabled by P_{2,i_2} and only those actions, otherwise $P_{1,i_1} \approx_{\mathrm{FB}} P_{2,i_2}$ cannot hold given that P_{2,i_2} can only idle whenever P_{1,i_1} executes a τ-action. As a consequence, for every subprocess alternative to $\tau \,.\, P'_{1,i_1}$:
    - If it starts with a τ-action, then for the same reason it must offer all the alternative observable actions enabled by P_{2,i_2} and only those actions, hence it must be $\approx_{\mathrm{FB:ps}}$-equivalent to $\tau \,.\, P'_{1,i_1}$ and can be absorbed by $\tau \,.\, P'_{1,i_1}$ by exploiting the soundness of axiom $\mathsf{A}_{\mathrm{F},4}$.
    - If it starts with an observable action, then that action must be enabled by P_{2,i_2} in order for $P_{1,i_1} \approx_{\mathrm{FB}} P_{2,i_2}$ to hold and the considered subprocess can be absorbed within $\tau \,.\, P'_{1,i_1}$ as follows by exploiting the soundness of axioms $\mathsf{A}_{\mathrm{F},4}$ and $\mathsf{A}^{\tau}_{\mathrm{F},2}$:
      - $\tau \,.\, P'_{1,i_1}$ is expanded to $P'_{1,i_1} + \tau \,.\, P'_{1,i_1}$ via axiom $\mathsf{A}^{\tau}_{\mathrm{F},2}$, with its application being repeated in the case that P'_{1,i_1} starts with a τ-action and so on, until the considered subprocess appears in the expansion.

· The original occurrence of the considered subprocess and the new one inside the expansion are merged into a single one via axiom $\mathsf{A}_{\mathrm{F},4}$.
· The resulting process is contracted back to $\tau\,.\,P'_{1,i_1}$ via as many applications of axiom $\mathsf{A}^{\tau}_{\mathrm{F},2}$.

The result finally follows by substitutivity with respect to alternative composition and, in the presence of identical summands on the same side, axiom $\mathsf{A}_{\mathrm{F},4}$ possibly preceded by applications of axioms $\mathsf{A}_{\mathrm{F},1}$ and $\mathsf{A}_{\mathrm{F},2}$ to move identical summands next to each other.

- Let $k \geq 2$ with P_1 being $a_1^\dagger.\,P'_1$ and P_2 being $a_2^\dagger.\,P'_2$, where P'_1 and P'_2 are both initial and in sat-F-nf. Since $\mathit{to\_forward}(P_1) = P'_1$ and $\mathit{to\_forward}(P_2) = P'_2$, from $P_1 \approx_{\mathrm{FB:ps}} P_2$ and Proposition 6.1(3) two cases arise:
  - If $P'_1 \approx_{\mathrm{FB:ps}} P'_2$ then from the induction hypothesis we obtain $\mathsf{A}^{\tau}_{\mathrm{F}} \vdash P'_1 = P'_2$, hence $\mathsf{A}^{\tau}_{\mathrm{F}} \vdash a^\dagger.\,P'_1 = a^\dagger.\,P'_2$ by substitutivity with respect to executed action prefix. Thanks to axiom $\mathsf{A}_{\mathrm{F},9}$ we derive $\mathsf{A}^{\tau}_{\mathrm{F}} \vdash a_1^\dagger.\,P'_1 = a^\dagger.\,P'_1$ and $\mathsf{A}^{\tau}_{\mathrm{F}} \vdash a^\dagger.\,P'_2 = a_2^\dagger.\,P'_2$, from which $\mathsf{A}^{\tau}_{\mathrm{F}} \vdash a_1^\dagger.\,P'_1 = a_2^\dagger.\,P'_2$ follows by transitivity.
  - If $P'_1 \approx_{\mathrm{FB}} P'_2$ but $P'_1 \not\approx_{\mathrm{FB:ps}} P'_2$ – as is the case, e.g., when $a_1^\dagger.\,P'_1$ is $a_1^\dagger.\,\tau\,.\,\underline{0}$ and $a_2^\dagger.\,P'_2$ is $a_2^\dagger.\,\underline{0}$ – then P'_1 can execute τ-actions (thus reaching non-initial processes) to which P'_2 can respond only by idling (thus remaining in an initial process), or vice versa. If P_1 is $a_1^\dagger.\,\tau\,.\,P''_1$, we exploit the soundness of axiom $\mathsf{A}^{\tau}_{\mathrm{F},4}$ to obtain $P_1 \approx_{\mathrm{FB:ps}} a_1^\dagger.\,P'''_1$ where P'''_1 is a subprocess of P''_1 that is initial, in sat-F-nf, and not executing τ-actions, so that $P'''_1 \approx_{\mathrm{FB:ps}} P'_2$ and we can then proceed like in the previous case by additionally applying axiom $\mathsf{A}^{\tau}_{\mathrm{F},4}$.

    More generally, the considered summand of P_1 may be of the form $a^\dagger_{1,i_1}\,.\,(\tau\,.\,P'_{1,i_1} + \ldots)$, but then every subprocess alternative to $\tau\,.\,P'_{1,i_1}$ can be suitably absorbed as shown earlier.

- Note that the case in which P_1 is $\sum_{i \in I_1} a_{1,i}\,.\,P_{1,i}$ with I_1 possibly empty and P_2 is $a_2^\dagger.\,P'_2$, or vice versa, cannot occur because the former is initial while the latter is not. Likewise, the case in which P_1 is $\sum_{i \in I_1} a_{1,i}\,.\,P_{1,i}$ with $I_1 \neq \emptyset$ and P_2 is $\underline{0}$, or vice versa, cannot occur either because the former has at least one outgoing transition while the latter has not (should the former process be able to execute only sequences of τ-transitions, after which non-initial processes are reached, the latter process could respond only by idling thus remaining in an initial process). In other words, both cases would contradict $P_1 \approx_{\mathrm{FB:ps}} P_2$.

If P_1 and P_2 are not both in sat-F-nf, thanks to Lemmas 6.2 and 6.4 we can find Q_1 and Q_2 in sat-F-nf, each of which is initial iff so is its corresponding original process, such that $\mathsf{A}^{\tau}_{\mathrm{F}} \vdash P_1 = Q_1$ and $\mathsf{A}^{\tau}_{\mathrm{F}} \vdash P_2 = Q_2$, hence $\mathsf{A}^{\tau}_{\mathrm{F}} \vdash Q_2 = P_2$ by symmetry. Due to soundness, we get $P_1 \approx_{\mathrm{FB:ps}} Q_1$, hence $Q_1 \approx_{\mathrm{FB:ps}} P_1$ as $\approx_{\mathrm{FB:ps}}$ is symmetric, and $P_2 \approx_{\mathrm{FB:ps}} Q_2$. Since $P_1 \approx_{\mathrm{FB:ps}} P_2$, we also get $Q_1 \approx_{\mathrm{FB:ps}} Q_2$ as $\approx_{\mathrm{FB:ps}}$ is transitive. By virtue of what has been shown above, from $Q_1 \approx_{\mathrm{FB:ps}} Q_2$ with Q_1 and Q_2 in sat-F-nf it follows that $\mathsf{A}^{\tau}_{\mathrm{F}} \vdash Q_1 = Q_2$ and hence $\mathsf{A}^{\tau}_{\mathrm{F}} \vdash P_1 = P_2$ by transitivity. ∎

$$(\text{ACT}_{\text{brs,f}})\ \frac{initial(U)}{<a,\beth>.U \xrightarrow{a,\beth}_{\text{brs}} <a^\dagger,\beth>.U} \qquad (\text{ACT}_{\text{brs,p}})\ \frac{U \xrightarrow{\theta,\daleth}_{\text{brs}} U'}{<a^\dagger,\beth>.U \xrightarrow{\cdot a\theta,\daleth}_{\text{brs}} <a^\dagger,\beth>.U'}$$

$$(\text{CHO}_{\text{brs,l}})\ \frac{U_1 \xrightarrow{\theta,\beth}_{\text{brs}} U_1' \quad initial(U_2)}{U_1 + U_2 \xrightarrow{\dot{+}\theta,\beth}_{\text{brs}} U_1' + U_2} \qquad (\text{CHO}_{\text{brs,r}})\ \frac{U_2 \xrightarrow{\theta,\beth}_{\text{brs}} U_2' \quad initial(U_1)}{U_1 + U_2 \xrightarrow{\dot{+}\theta,\beth}_{\text{brs}} U_1 + U_2'}$$

Table 6.3: Proved operational semantic rules for $\mathbb{P}_{\text{brs}}$ ($\beth, \daleth \in 2^{\mathcal{A}}$)

6.4 Process Encodings Based on Backward Ready Sets

Since reverse and forward-reverse bisimilarities are truly concurrent, before developing their axiomatizations – in particular their expansion laws – we have to provide process encodings that insert suitable additional discriminating information into action prefixes. We show that this information is the same for both semantics and is constituted by backward ready sets. Precisely, for every proved transition $P \xrightarrow{\theta} P'$ we let $\ell_{\text{R}}(\theta)_{P'} = \ell_{\text{FR}}(\theta)_{P'} = <act(\theta), brs(P')> \triangleq \ell_{\text{brs}}(\theta)_{P'}$ and $\ell_{\text{R,w}}(\theta)_{P'} = \ell_{\text{FR,w}}(\theta)_{P'} = <act(\theta), brs_{\text{w}}(P')> \triangleq \ell_{\text{brs,w}}(\theta)_{P'}$, where in the aforementioned observation functions we have indicated their primary argument θ in parentheses and their secondary argument P' as a subscript. The intuition behind resorting to backward ready sets comes from Figure 1.1, where the reverse- and forward-reverse-inequivalent processes associated with the three bottom states have three different backward ready sets: $\{b,a\}, \{b\}, \{a\}$.

By virtue of Proposition 3.2(2), the distinguishing power of $\sim_{\text{RB}}$ and $\sim_{\text{FRB}}$ does not change if, in the related definitions of bisimulation, we additionally require that $brs(P_1) = brs(P_2)$ for all $(P_1, P_2) \in \mathcal{B}$. Likewise, thanks to Proposition 3.7(2), the discriminating power of $\approx_{\text{RB}}$ and $\approx_{\text{FRB:ps}}$ does not vary if, in the related definitions of bisimulation, we additionally require that $brs_{\text{w}}(P_1) = brs_{\text{w}}(P_2)$ for all $(P_1, P_2) \in \mathcal{B}$. Thus, it is immediate to realize that $\sim_{\text{RB}:\ell_{\text{brs}}}$, $\sim_{\text{FRB}:\ell_{\text{brs}}}$, $\approx_{\text{RB}:\ell_{\text{brs,w}}}$, $\approx_{\text{FRB:ps}:\ell_{\text{brs,w}}}$ (see page 41) respectively coincide with $\sim_{\text{RB}}$, $\sim_{\text{FRB}}$, $\approx_{\text{RB}}$, $\approx_{\text{FRB:ps}}$.

The former four bisimilarities also apply to the encoding target $\mathbb{P}_{\text{brs}}$, i.e., the set of renaming-free processes obtained from $\mathbb{P}_{\text{seq}}$ by extending every action prefix with a subset of $\mathcal{A}$. The syntax of $\mathbb{P}_{\text{brs}}$ is defined as follows where $\beth \in 2^{\mathcal{A}}$:

$$U ::= \underline{0} \mid <a,\beth>.U \mid <a^\dagger,\beth>.U \mid U + U$$

The proved operational semantic rules for $\mathbb{P}_{\text{brs}}$ shown in Table 6.3 generate the proved labeled transition system $(\mathbb{P}_{\text{brs}}, \Theta_{\text{brs}} \times 2^{\mathcal{A}}, \longrightarrow_{\text{brs}})$ where Θ_{brs} is a variant of Θ in which only the operators of $\mathbb{P}_{\text{brs}}$ are considered. With respect to those in Table 2.1, the rules in Table 6.3 additionally label the produced transitions with the action sets occurring in the action prefixes inside the source processes. Given a symmetric relation $\mathcal{B}$ over $\mathbb{P}_{\text{brs}}$ and $(U_1, U_2) \in \mathcal{B}$, the forward clause of $\sim_{\text{FRB}:\ell_{\text{brs}}}$ can be rephrased as:

for each $U_1 \xrightarrow{\theta_1,\beth}_{\text{brs}} U_1'$ there exists $U_2 \xrightarrow{\theta_2,\beth}_{\text{brs}} U_2'$ such that $act(\theta_1) = act(\theta_2)$ and $(U_1', U_2') \in \mathcal{B}$

while the backward clauses of $\sim_{\text{RB}:\ell_{\text{brs}}}$ and $\sim_{\text{FRB}:\ell_{\text{brs}}}$ can be rephrased as:

for each $U_1' \xrightarrow{\theta_1,\beth}_{\text{brs}} U_1$ there exists $U_2' \xrightarrow{\theta_2,\beth}_{\text{brs}} U_2$ such that $act(\theta_1) = act(\theta_2)$ and $(U_1', U_2') \in \mathcal{B}$

and similarly for the weak clauses of $\approx_{\text{RB}:\ell_{\text{brs,w}}}$ and $\approx_{\text{FRB:ps}:\ell_{\text{brs,w}}}$ in which $\Longrightarrow_{\text{brs}}$ is used to represent a possibly empty sequence of finitely many τ-brs-transitions.

Following the proved trees approach described in Section 6.2, we have to lift $\ell_{\text{brs}}/\ell_{\text{brs,w}}$ so as to encode $\mathbb{P}$ into $\mathbb{P}_{\text{brs}}$. The objective is to extend each action prefix with the strong/weak backward ready set of the reached process. For processes in $\mathbb{P}_{\text{seq}}$ it is just a matter of extending any action prefix with a singleton containing the action itself

or, in the weak case, the action itself if different from τ, the closest preceding observable action otherwise. In contrast, backward ready sets may contain several actions when handling processes not in $\mathbb{P}_{\mathrm{seq}}$. To account for this, the lifting of $\ell_{\mathrm{brs}}/\ell_{\mathrm{brs,w}}$ has to make use of a secondary argument, which we call environment process and will be written as a subscript of the lifting function by analogy with the secondary argument of the observation function.

The environment process is progressively updated as prefixes are turned into pairs so as to represent the process reached so far, i.e., the process yielding the backward ready set. The environment process E for P embodies P, in the sense that it is initially P and then its forward behavior is updated upon each action prefix extension by decorating the action as executed, where the action is located within E by a proof term. To correctly handle the extension of prefixes containing already executed actions like $a^\dagger.P'$, (part of) E has to be brought back by replacing $a^\dagger.P'$ inside E with the process $to\_initial(a^\dagger.P')$ obtained from $a^\dagger.P'$ by removing all †-decorations (see page 26 for the definition of function $to\_initial : \mathbb{P} \to \mathbb{P}_{\mathrm{init}}$).

In Sections 6.4.1 and 6.4.2 we respectively provide the liftings of ℓ_{brs} and $\ell_{\mathrm{brs,w}}$.

6.4.1 Process Encoding Based on Strong Backward Ready Sets for $\sim_{\mathbf{RB}}$ and $\sim_{\mathbf{FRB}}$

In Definitions 6.3 and 6.4 we develop the lifting of ℓ_{brs} and denote by $\widetilde{P}$ the result of its application to P. We recall that $\ell_{\mathrm{brs}}(\theta)_{P'} = <act(\theta), brs(P')>$ for $P \xrightarrow{\theta} P'$ and we let $\ell_{\mathrm{brs}}(\theta)^\dagger_{P'} = <act(\theta)^\dagger, brs(P')>$. We further recall that $\Theta_{\mathrm{seq}} = \{.a, \llcorner\rho, +, \dot{+} \mid a \in \mathcal{A}, \rho : \mathcal{A} \to \mathcal{A} \text{ such that } \rho(\tau) = \tau\}$.

Definition 6.3. *The ℓ_{brs}-encoding of $P \in \mathbb{P}$ is $\widetilde{P} = \ell^\varepsilon_{\mathrm{brs}}(P)_P$ where $\ell^\sigma_{\mathrm{brs}} : \mathbb{P} \times \mathbb{P} \to \mathbb{P}_{\mathrm{brs}}$ for $\sigma \in \Theta^*_{\mathrm{seq}}$ is defined by induction on the syntactical structure of its primary argument P which is a subprocess of its secondary argument E:*

$$\begin{array}{rcl}
\ell^\sigma_{\mathrm{brs}}(\underline{0})_E & = & \underline{0} \\
\ell^\sigma_{\mathrm{brs}}(a\,.\,P')_E & = & \ell_{\mathrm{brs}}(\sigma a)_{upd(E,\sigma a)}\,.\,\ell^{\sigma.a}_{\mathrm{brs}}(P')_{upd(E,\sigma a)} \\
\ell^\sigma_{\mathrm{brs}}(a^\dagger.\,P')_E & = & \ell_{\mathrm{brs}}(\sigma a)^\dagger_{upd(\ddot{E},\sigma a)}\,.\,\ell^{\sigma.a}_{\mathrm{brs}}(P')_E \\
\ell^\sigma_{\mathrm{brs}}(P' \llcorner\rho\urcorner)_E & = & \ell^{\sigma\llcorner\rho}_{\mathrm{brs}}(P')_E \\
\ell^\sigma_{\mathrm{brs}}(P_1 + P_2)_E & = & \ell^{\sigma+}_{\mathrm{brs}}(P_1)_E + \ell^{\sigma\dot{+}}_{\mathrm{brs}}(P_2)_E \\
\ell^\sigma_{\mathrm{brs}}(P_1 \parallel_L P_2)_E & = & e\ell^\sigma_{\mathrm{brs}}(\widetilde{P}_1, \widetilde{P}_2, L)_E
\end{array}$$

with function $e\ell^\sigma_{\mathrm{brs}}$ being defined later on, $\ddot{E}$ being obtained from E by replacing $a^\dagger.P'$ with $to\_initial(a^\dagger.P')$, and function $upd : \mathbb{P} \times \Theta \to \mathbb{P}$ being defined by induction on the syntactical structure of its first argument E as follows:

$$\begin{array}{rcl}
upd(\underline{0}, \theta) & = & \underline{0} \\
upd(a\,.\,E', \theta) & = & \left\{ \begin{array}{ll} a^\dagger.\,E' & \text{if } \theta = a \\ a\,.\,E' & \text{otherwise} \end{array} \right. \\
upd(a^\dagger.\,E', \theta) & = & \left\{ \begin{array}{ll} a^\dagger.\,upd(E', \theta') & \text{if } \theta = .a\theta' \\ a^\dagger.\,E' & \text{otherwise} \end{array} \right. \\
upd(E' \llcorner\rho\urcorner, \theta) & = & \left\{ \begin{array}{ll} upd(E', \theta') \llcorner\rho\urcorner & \text{if } \theta = \llcorner\rho\urcorner\theta' \\ E' \llcorner\rho\urcorner & \text{otherwise} \end{array} \right. \\
upd(E_1 + E_2, \theta) & = & \left\{ \begin{array}{ll} upd(E_1, \theta') + E_2 & \text{if } \theta = +\theta' \\ E_1 + upd(E_2, \theta') & \text{if } \theta = \dot{+}\theta' \\ E_1 + E_2 & \text{otherwise} \end{array} \right. \\
upd(E_1 \parallel_L E_2, \theta) & = & \left\{ \begin{array}{ll} upd(E_1, \theta') \parallel_L E_2 & \text{if } \theta = \lfloor\!\lfloor_L\theta' \\ E_1 \parallel_L upd(E_2, \theta') & \text{if } \theta = \lfloor\!\rfloor_L\theta' \\ upd(E_1, \theta_1) \parallel_L upd(E_2, \theta_2) & \text{if } \theta = \langle\theta_1, \theta_2\rangle_L \\ E_1 \parallel_L E_2 & \text{otherwise} \end{array} \right.
\end{array}$$

■

Example 6.1. Let us encode some sequential processes (for them function $e\ell^{\sigma}_{\mathrm{brs}}$ does not come into play):

- Let P be the initial sequential process $a\,.\,b\,.\,\underline{0} + b\,.\,a\,.\,\underline{0}$. Then:
$$\begin{aligned}\widetilde{P} \;=\; \ell^{\varepsilon}_{\mathrm{brs}}(P)_P \;&=\; \ell^{+}_{\mathrm{brs}}(a\,.\,b\,.\,\underline{0})_{a\,.\,b\,.\,\underline{0}+b\,.\,a\,.\,\underline{0}} + \ell^{+}_{\mathrm{brs}}(b\,.\,a\,.\,\underline{0})_{a\,.\,b\,.\,\underline{0}+b\,.\,a\,.\,\underline{0}}\\ &=\; \ell_{\mathrm{brs}}(\dot{+}a)_{a^\dagger\,.\,b\,.\,\underline{0}+b\,.\,a\,.\,\underline{0}} \cdot \ell^{\dot{+}\cdot a}_{\mathrm{brs}}(b\,.\,\underline{0})_{a^\dagger\,.\,b\,.\,\underline{0}+b\,.\,a\,.\,\underline{0}} +\\ &\quad\; \ell_{\mathrm{brs}}(\dot{+}b)_{a\,.\,b\,.\,\underline{0}+b^\dagger\,.\,a\,.\,\underline{0}} \cdot \ell^{\dot{+}\cdot b}_{\mathrm{brs}}(a\,.\,\underline{0})_{a\,.\,b\,.\,\underline{0}+b^\dagger\,.\,a\,.\,\underline{0}}\\ &=\; <a,\{a\}>\,.\,\ell_{\mathrm{brs}}(\dot{+}\cdot_a b)_{a^\dagger\,.\,b^\dagger\,.\,\underline{0}+b\,.\,a\,.\,\underline{0}} \cdot \ell^{\dot{+}\cdot a\cdot b}_{\mathrm{brs}}(\underline{0})_{a^\dagger\,.\,b^\dagger\,.\,\underline{0}+b\,.\,a\,.\,\underline{0}} +\\ &\quad\; <b,\{b\}>\,.\,\ell_{\mathrm{brs}}(\dot{+}\cdot_b a)_{a\,.\,b\,.\,\underline{0}+b^\dagger\,.\,a^\dagger\,.\,\underline{0}} \cdot \ell^{\dot{+}\cdot b\cdot a}_{\mathrm{brs}}(\underline{0})_{a\,.\,b\,.\,\underline{0}+b^\dagger\,.\,a^\dagger\,.\,\underline{0}}\\ &=\; <a,\{a\}>\,.\,<b,\{b\}>\,.\,\underline{0} + <b,\{b\}>\,.\,<a,\{a\}>\,.\,\underline{0}\end{aligned}$$

- Let Q be the non-initial sequential process $a^\dagger\,.\,b^\dagger\,.\,\underline{0}$. Then:
$$\begin{aligned}\widetilde{Q} \;=\; \ell^{\varepsilon}_{\mathrm{brs}}(Q)_Q \;&=\; \ell_{\mathrm{brs}}(a)^{\dagger}_{a^\dagger\,.\,b\,.\,\underline{0}} \cdot \ell^{\cdot a}_{\mathrm{brs}}(b^\dagger\,.\,\underline{0})_{a^\dagger\,.\,b^\dagger\,.\,\underline{0}}\\ &=\; <a^\dagger,\{a\}>\,.\,\ell_{\mathrm{brs}}(\cdot_a b)^{\dagger}_{a^\dagger\,.\,b^\dagger\,.\,\underline{0}} \cdot \ell^{\cdot a\cdot b}_{\mathrm{brs}}(\underline{0})_{a^\dagger\,.\,b^\dagger\,.\,\underline{0}}\\ &=\; <a^\dagger,\{a\}>\,.\,<b^\dagger,\{b\}>\,.\,\underline{0}\end{aligned}$$
Note that Definition 6.3 yields $a\,.\,b\,.\,\underline{0}$ as $\ddot{Q}$ after the second $=$ (before it, Q is a subprocess of the environment Q) and $a^\dagger\,.\,b\,.\,\underline{0}$ as $\ddot{Q}$ after the third $=$ (before it, $b^\dagger\,.\,\underline{0}$ is a subprocess of the environment Q).

- Let R be the sequential process with renaming $(a\,.\,b\,.\,\underline{0})\llcorner\rho\urcorner$ where $\llcorner\rho\urcorner = \llcorner a \mapsto c, b \mapsto d\urcorner$. Then:
$$\begin{aligned}\widetilde{R} \;=\; \ell^{\varepsilon}_{\mathrm{brs}}(R)_R \;&=\; \ell^{\llcorner\rho\urcorner}_{\mathrm{brs}}(a\,.\,b\,.\,\underline{0})_R\\ &=\; \ell_{\mathrm{brs}}(\llcorner\rho\urcorner a)_{(a^\dagger\,.\,b\,.\,\underline{0})\,\llcorner\rho\urcorner} \cdot \ell^{\llcorner\rho\urcorner\cdot a}_{\mathrm{brs}}(b\,.\,\underline{0})_{(a^\dagger\,.\,b\,.\,\underline{0})\,\llcorner\rho\urcorner}\\ &=\; <c,\{c\}>\,.\,\ell_{\mathrm{brs}}(\llcorner\rho\urcorner\cdot a\, b)_{(a^\dagger\,.\,b^\dagger\,.\,\underline{0})\,\llcorner\rho\urcorner} \cdot \ell^{\llcorner\rho\urcorner\cdot a\cdot b}_{\mathrm{brs}}(\underline{0})_{(a^\dagger\,.\,b^\dagger\,.\,\underline{0})\,\llcorner\rho\urcorner}\\ &=\; <c,\{c\}>\,.\,<d,\{d\}>\,.\,\underline{0}\end{aligned}$$
Note that the presence of $\llcorner\rho\urcorner$ inside the primary argument of the occurrences of ℓ_{brs} – i.e., the argument of *act* – and the presence of $\llcorner\rho\urcorner$ inside the secondary argument of the occurrences of ℓ_{brs} – i.e., the argument of *brs* – determine the renaming of all actions in both components of both extended prefixes. ■

While for sequential processes the backward ready set added to every action prefix is a singleton containing the action itself, this is no longer the case when dealing with processes of the form $P_1 \,\|_L\, P_2$. We thus complete the encoding by providing the definition of $e\ell^{\sigma}_{\mathrm{brs}}$. When P_1 and P_2 are not both initial, in the expansion we have to reconstruct all possible alternative action sequencings that have not been undertaken – which yield as many initial subprocesses – because under the forward-reverse semantics each of them could be selected after a rollback. In the subcase in which both P_1 and P_2 are non-initial and their executed actions are not in L – e.g., $a^\dagger\,.\,\underline{0} \,\|_\emptyset\, b^\dagger\,.\,\underline{0}$ – care must be taken because executed actions cannot appear on both sides of an alternative composition – e.g., the expansion cannot be of the form $a^\dagger\,.\,b^\dagger\,.\,\underline{0} + b^\dagger\,.\,a^\dagger\,.\,\underline{0}$ in that not well-formed. To overcome this, based on a total order $\leq_\dagger$ over Θ induced by the trace of actions executed so far, the expansion builds the corresponding sequencing of already executed actions plus all the aforementioned unexecuted action sequencings – e.g., something of the form $a^\dagger\,.\,b^\dagger\,.\,\underline{0} + b\,.\,a\,.\,\underline{0}$ or $b^\dagger\,.\,a^\dagger\,.\,\underline{0} + a\,.\,b\,.\,\underline{0}$ depending on whether $\|_\emptyset a \leq_\dagger \|_\emptyset b$ or $\|_\emptyset b \leq_\dagger \|_\emptyset a$ respectively.

Definition 6.4. *Let $P_1, P_2 \in \mathbb{P}$, $L \subseteq \mathcal{A}\setminus\{\tau\}$, $E_1, E_2, E \in \mathbb{P}$ be such that $P_1 \,\|_L\, P_2, E_1 \,\|_L\, E_2 \in \mathbb{P}$, P_1 is a subprocess of E_1, P_2 is a subprocess of E_2, and $E_1 \,\|_L\, E_2$ is a subprocess of E. Then $e\ell^{\sigma}_{\mathrm{brs}} : \mathbb{P}_{\mathrm{brs}} \times \mathbb{P}_{\mathrm{brs}} \times 2^{\mathcal{A}\setminus\{\tau\}} \times \mathbb{P} \to \mathbb{P}_{\mathrm{brs}}$ for $\sigma \in \Theta^*_{\mathrm{seq}}$ is inductively defined as follows, where square brackets enclose optional subprocesses as already done in Section 6.3 and every summation over an empty index set is taken to be $\underline{0}$ (and for simplicity is omitted within a choice unless all alternative subprocesses inside that choice are $\underline{0}$, in which case the whole choice boils down to $\underline{0}$):*

- *If* $\widetilde{P}_1$ *and* $\widetilde{P}_2$ *are both initial, say* $\widetilde{P}_k = \sum_{i\in I_k} \ell_{\mathrm{brs}}(\theta_{k,i})_{upd(P_k,\theta_{k,i})} \,.\, \widetilde{P}_{k,i}$ *for* $k \in \{1,2\}$*, let* $e\ell^{\sigma}_{\mathrm{brs}}(\widetilde{P}_1,\widetilde{P}_2,L)_E =$
$$\sum_{i\in I_1, act(\theta_{1,i})\notin L} \ell_{\mathrm{brs}}(\sigma\!\parallel_L\!\theta_{1,i})_{upd(E,\sigma\parallel_L\theta_{1,i})} \,.\, e\ell^{\sigma}_{\mathrm{brs}}(\widetilde{P}_{1,i},\widetilde{P}_2,L)_{upd(E,\sigma\parallel_L\theta_{1,i})} +$$
$$\sum_{i\in I_2, act(\theta_{2,i})\notin L} \ell_{\mathrm{brs}}(\sigma\!\parallel_L\!\theta_{2,i})_{upd(E,\sigma\parallel_L\theta_{2,i})} \,.\, e\ell^{\sigma}_{\mathrm{brs}}(\widetilde{P}_1,\widetilde{P}_{2,i},L)_{upd(E,\sigma\parallel_L\theta_{2,i})} +$$
$$\sum_{i\in I_1, act(\theta_{1,i})\in L} \sum_{j\in I_2, act(\theta_{2,j})=act(\theta_{1,i})} \ell_{\mathrm{brs}}(\sigma\langle\theta_{1,i},\theta_{2,j}\rangle_L)_{upd(E,\sigma\langle\theta_{1,i},\theta_{2,j}\rangle_L)} \,.\, e\ell^{\sigma}_{\mathrm{brs}}(\widetilde{P}_{1,i},\widetilde{P}_{2,j},L))_{upd(E,\sigma\langle\theta_{1,i},\theta_{2,j}\rangle_L)}$$
where each of the three summation-shaped subprocesses to the right of $=$ *is an initial process.*

- *If* $\widetilde{P}_1$ *is not initial while* $\widetilde{P}_2$ *is initial, say* $\widetilde{P}_1 = \ell_{\mathrm{brs}}(\theta_1)^{\dagger}_{upd(to\_\,initial(P_1),\theta_1)} \,.\, \widetilde{P}'_1\,[+\,\widetilde{P}''_1]$ *where* $act(\theta_1) \notin L$ *and the optional* $\widetilde{P}''_1$ *is initial, say* $\widetilde{P}''_1 = \sum_{i\in I_1} \ell_{\mathrm{brs}}(\theta_{1,i})_{upd(P''_1,\theta_{1,i})} \,.\, \widetilde{P}''_{1,i}$*, and* $\widetilde{P}_2 = \sum_{i\in I_2} \ell_{\mathrm{brs}}(\theta_{2,i})_{upd(P_2,\theta_{2,i})} \,.\, \widetilde{P}_{2,i}$*, for* $\ddot{E}$ *obtained from* E *by replacing* P_1 *with* $to\_\,initial(P_1)$ *let* $e\ell^{\sigma}_{\mathrm{brs}}(\widetilde{P}_1,\widetilde{P}_2,L)_E =$
$$\ell_{\mathrm{brs}}(\sigma\!\parallel_L\!\theta_1)^{\dagger}_{upd(\ddot{E},\sigma\parallel_L\theta_1)} \,.\, e\ell^{\sigma}_{\mathrm{brs}}(\widetilde{P}'_1,\widetilde{P}_2,L)_E +$$
$$[\sum_{i\in I_1, act(\theta_{1,i})\notin L} \ell_{\mathrm{brs}}(\sigma\!\parallel_L\!\theta_{1,i})_{upd(\ddot{E},\sigma\parallel_L\theta_{1,i})} \,.\, e\ell^{\sigma}_{\mathrm{brs}}(\widetilde{P}''_{1,i},\widetilde{P}_2,L)_{upd(\ddot{E},\sigma\parallel\theta_{1,i})} +]$$
$$\sum_{i\in I_2, act(\theta_{2,i})\notin L} \ell_{\mathrm{brs}}(\sigma\!\parallel_L\!\theta_{2,i})_{upd(\ddot{E},\sigma\parallel_L\theta_{2,i})} \,.\, e\ell^{\sigma}_{\mathrm{brs}}(to\_\,initial(\widetilde{P}_1),\widetilde{P}_{2,i},L)_{upd(\ddot{E},\sigma\parallel_L\theta_{2,i})} +$$
$$[\sum_{i\in I_1, act(\theta_{1,i})\in L} \sum_{j\in I_2, act(\theta_{2,j})=act(\theta_{1,i})} \ell_{\mathrm{brs}}(\sigma\langle\theta_{1,i},\theta_{2,j}\rangle_L)_{upd(\ddot{E},\sigma\langle\theta_{1,i},\theta_{2,j}\rangle_L)} \,.\, e\ell^{\sigma}_{\mathrm{brs}}(\widetilde{P}''_{1,i},\widetilde{P}_{2,j},L))_{upd(\ddot{E},\sigma\langle\theta_{1,i},\theta_{2,j}\rangle_L)}]$$
where each of the last three summation-shaped subprocesses on the right is an initial process needed by the forward-reverse semantics, with the presence of the first one and the third one depending on the presence of $\widetilde{P}''_1$*.*

- *The case in which* $\widetilde{P}_1$ *is initial while* $\widetilde{P}_2$ *is not initial is like the previous one.*

- *If* $\widetilde{P}_1$ *and* $\widetilde{P}_2$ *are both non-initial, say* $\widetilde{P}_k = \ell_{\mathrm{brs}}(\theta_k)^{\dagger}_{upd(to\_\,initial(P_k),\theta_k)} \,.\, \widetilde{P}'_k\,[+\,\widetilde{P}''_k]$ *where the optional* $\widetilde{P}''_k$ *is initial, say* $\widetilde{P}''_k = \sum_{i\in I_k} \ell_{\mathrm{brs}}(\theta_{k,i})_{upd(P''_k,\theta_{k,i})} \,.\, \widetilde{P}''_{k,i}$*, for* $k \in \{1,2\}$*, for* $\ddot{E}$ *obtained from* E *by replacing each* P_k *with* $to\_\,initial(P_k)$ *there are three subcases:*

  - *If* $act(\theta_1) \notin L \wedge (act(\theta_2) \in L \vee \sigma\!\parallel_L\!\theta_1 \leq_{\dagger} \sigma\!\parallel_L\!\theta_2)$*, let* $e\ell^{\sigma}_{\mathrm{brs}}(\widetilde{P}_1,\widetilde{P}_2,L)_E =$
$$\ell_{\mathrm{brs}}(\sigma\!\parallel_L\!\theta_1)^{\dagger}_{upd(\ddot{E},\sigma\parallel_L\theta_1)} \,.\, e\ell^{\sigma}_{\mathrm{brs}}(\widetilde{P}'_1,\widetilde{P}_2,L)_E +$$
$$[\ell_{\mathrm{brs}}(\sigma\!\parallel_L\!\theta_2)_{upd(\ddot{E},\sigma\parallel_L\theta_2)} \,.\, e\ell^{\sigma}_{\mathrm{brs}}(to\_\,initial(\widetilde{P}_1),to\_\,initial(\widetilde{P}'_2),L)_{upd(\ddot{E},\sigma\parallel_L\theta_2)} +]$$
$$[\sum_{i\in I_1, act(\theta_{1,i})\notin L} \ell_{\mathrm{brs}}(\sigma\!\parallel_L\!\theta_{1,i})_{upd(\ddot{E},\sigma\parallel_L\theta_{1,i})} \,.\, e\ell^{\sigma}_{\mathrm{brs}}(\widetilde{P}''_{1,i},to\_\,initial(\widetilde{P}_2),L)_{upd(\ddot{E},\sigma\parallel_L\theta_{1,i})} +]$$
$$[\sum_{i\in I_2, act(\theta_{2,i})\notin L} \ell_{\mathrm{brs}}(\sigma\!\parallel_L\!\theta_{2,i})_{upd(\ddot{E},\sigma\parallel_L\theta_{2,i})} \,.\, e\ell^{\sigma}_{\mathrm{brs}}(to\_\,initial(\widetilde{P}_1),\widetilde{P}''_{2,i},L)_{upd(\ddot{E},\sigma\parallel_L\theta_{2,i})} +]$$
$$[\sum_{i\in I_1, act(\theta_{1,i})\in L} \sum_{j\in I_2, act(\theta_{2,j})=act(\theta_{1,i})} \ell_{\mathrm{brs}}(\sigma\langle\theta_{1,i},\theta_{2,j}\rangle_L)_{upd(\ddot{E},\sigma\langle\theta_{1,i},\theta_{2,j}\rangle_L)} \,.\, e\ell^{\sigma}_{\mathrm{brs}}(\widetilde{P}''_{1,i},\widetilde{P}''_{2,j},L))_{upd(\ddot{E},\sigma\langle\theta_{1,i},\theta_{2,j}\rangle_L)}]$$
    where each of the last four subprocesses on the right is an initial process needed by the forward-reverse semantics, with the first one being present only if $act(\theta_2) \notin L$ *and the presence of the subsequent three respectively depending on the presence of* $\widetilde{P}''_1$*,* $\widetilde{P}''_2$*, or both.*
  - *The subcase* $act(\theta_2) \notin L \wedge (act(\theta_1) \in L \vee \sigma\!\parallel_L\!\theta_2 \leq_{\dagger} \sigma\!\parallel_L\!\theta_1)$ *is like the previous one.*

– *If* $act(\theta_1) = act(\theta_2) \in L$, *let* $e\ell^{\sigma}_{\mathrm{brs}}(\widetilde{P}_1, \widetilde{P}_2, L)_E =$
$\ell_{\mathrm{brs}}(\sigma\langle\theta_1,\theta_2\rangle_L)^{\dagger}{}_{upd(\ddot{E},\sigma\langle\theta_1,\theta_2\rangle_L)} \cdot e\ell^{\sigma}_{\mathrm{brs}}(\widetilde{P}'_1, \widetilde{P}'_2, L)_E +$
$[\sum_{i\in I_1, act(\theta_{1,i})\notin L} \ell_{\mathrm{brs}}(\sigma\|_L\theta_{1,i})_{upd(\ddot{E},\sigma\|_L\theta_{1,i})} \cdot e\ell^{\sigma}_{\mathrm{brs}}(\widetilde{P}''_{1,i}, to\_initial(\widetilde{P}_2), L)_{upd(\ddot{E},\sigma\|_L\theta_{1,i})} +]$
$[\sum_{i\in I_2, act(\theta_{2,i})\notin L} \ell_{\mathrm{brs}}(\sigma\|_L\theta_{2,i})_{upd(\ddot{E},\sigma\|_L\theta_{2,i})} \cdot e\ell^{\sigma}_{\mathrm{brs}}(to\_initial(\widetilde{P}_1), \widetilde{P}''_{2,i}, L)_{upd(\ddot{E},\sigma\|_L\theta_{2,i})} +]$
$[\sum_{i\in I_1, act(\theta_{1,i})\in L} \sum_{j\in I_2, act(\theta_{2,j})=act(\theta_{1,i})} \ell_{\mathrm{brs}}(\sigma\langle\theta_{1,i},\theta_{2,j}\rangle_L)_{upd(\ddot{E},\sigma\langle\theta_{1,i},\theta_{2,j}\rangle_L)} \cdot e\ell^{\sigma}_{\mathrm{brs}}(\widetilde{P}''_{1,i}, \widetilde{P}''_{2,j}, L))_{upd(\ddot{E},\sigma\langle\theta_{1,i},\theta_{2,j}\rangle_L)}]$
where each of the last three summation-shaped subprocesses on the right is an initial process needed by the forward-reverse semantics, with their presence respectively depending on the presence of $\widetilde{P}''_1$, $\widetilde{P}''_2$, *or both.* ■

Example 6.2. Let P be $P_1 \|_\emptyset P_2$, where P_1 and P_2 are the initial sequential processes $a\,.\,\underline{0}$ and $b\,.\,\underline{0}$ respectively, so that $\widetilde{P}_1 = \ell_{\mathrm{brs}}(a)_{a^\dagger.\underline{0}}\,.\,\widetilde{\underline{0}}$ and $\widetilde{P}_2 = \ell_{\mathrm{brs}}(b)_{b^\dagger.\underline{0}}\,.\,\widetilde{\underline{0}}$. Then:

$$\begin{aligned}
\widetilde{P} \;=\; \ell^{\varepsilon}_{\mathrm{brs}}(P)_P \;&=\; e\ell^{\varepsilon}_{\mathrm{brs}}(\widetilde{P}_1, \widetilde{P}_2, \emptyset)_P \\
&=\; \ell_{\mathrm{brs}}(\|_\emptyset a)_{a^\dagger.\underline{0}\,\|_\emptyset\, b\,.\,\underline{0}} \cdot e\ell^{\varepsilon}_{\mathrm{brs}}(\widetilde{\underline{0}}, \widetilde{P}_2, \emptyset)_{a^\dagger.\underline{0}\,\|_\emptyset\, b\,.\,\underline{0}} + \\
&\quad\; \ell_{\mathrm{brs}}(\|_\emptyset b)_{a\,.\,\underline{0}\,\|_\emptyset\, b^\dagger.\underline{0}} \cdot e\ell^{\varepsilon}_{\mathrm{brs}}(\widetilde{P}_1, \widetilde{\underline{0}}, \emptyset)_{a\,.\,\underline{0}\,\|_\emptyset\, b^\dagger.\underline{0}} \\
&=\; <a,\{a\}>\,.\,\ell_{\mathrm{brs}}(\|_\emptyset b)_{a^\dagger.\underline{0}\,\|_\emptyset\, b^\dagger.\underline{0}} \cdot e\ell^{\varepsilon}_{\mathrm{brs}}(\widetilde{\underline{0}}, \widetilde{\underline{0}}, \emptyset)_{a^\dagger.\underline{0}\,\|_\emptyset\, b^\dagger.\underline{0}} + \\
&\quad\; <b,\{b\}>\,.\,\ell_{\mathrm{brs}}(\|_\emptyset a)_{a^\dagger.\underline{0}\,\|_\emptyset\, b^\dagger.\underline{0}} \cdot e\ell^{\varepsilon}_{\mathrm{brs}}(\widetilde{\underline{0}}, \widetilde{\underline{0}}, \emptyset)_{a^\dagger.\underline{0}\,\|_\emptyset\, b^\dagger.\underline{0}} \\
&=\; <a,\{a\}>\,.\,<b,\{a,b\}>\,.\,\underline{0} + <b,\{b\}>\,.\,<a,\{a,b\}>\,.\,\underline{0}
\end{aligned}$$

which is different from the encoding of $a\,.\,b\,.\,\underline{0} + b\,.\,a\,.\,\underline{0}$ shown in Example 6.1, unless $a = b$ as in that case the backward ready set $\{a, b\}$ collapses to a singleton (indeed $a\,.\,\underline{0} \|_\emptyset a\,.\,\underline{0} \sim_{\mathrm{FRB}} a\,.\,a\,.\,\underline{0} + a\,.\,a\,.\,\underline{0} \sim_{\mathrm{FRB}} a\,.\,a\,.\,\underline{0}$).
If instead P_1 is the non-initial sequential process $a^\dagger.\,\underline{0}$ while P_2 is the initial sequential process $b\,.\,\underline{0}$, so that $\widetilde{P}_1 = \ell_{\mathrm{brs}}(a)^\dagger_{a^\dagger.\underline{0}}\,.\,\widetilde{\underline{0}}$ and $\widetilde{P}_2 = \ell_{\mathrm{brs}}(b)_{b^\dagger.\underline{0}}\,.\,\widetilde{\underline{0}}$, then:

$$\begin{aligned}
\widetilde{P} \;=\; \ell^{\varepsilon}_{\mathrm{brs}}(P)_P \;&=\; e\ell^{\varepsilon}_{\mathrm{brs}}(\widetilde{P}_1, \widetilde{P}_2, \emptyset)_P \\
&=\; \ell_{\mathrm{brs}}(\|_\emptyset a)^\dagger_{a^\dagger.\underline{0}\,\|_\emptyset\, b\,.\,\underline{0}} \cdot e\ell^{\varepsilon}_{\mathrm{brs}}(\widetilde{\underline{0}}, \widetilde{P}_2, \emptyset)_P + \\
&\quad\; \ell_{\mathrm{brs}}(\|_\emptyset b)_{a\,.\,\underline{0}\,\|_\emptyset\, b^\dagger.\underline{0}} \cdot e\ell^{\varepsilon}_{\mathrm{brs}}(\ell_{\mathrm{brs}}(a)_{a^\dagger.\underline{0}} \cdot \widetilde{\underline{0}}, \widetilde{\underline{0}}, \emptyset)_{a\,.\,\underline{0}\,\|_\emptyset\, b^\dagger.\underline{0}} \\
&=\; <a^\dagger,\{a\}>\,.\,\ell_{\mathrm{brs}}(\|_\emptyset b)_{a^\dagger.\underline{0}\,\|_\emptyset\, b^\dagger.\underline{0}} \cdot e\ell^{\varepsilon}_{\mathrm{brs}}(\widetilde{\underline{0}}, \widetilde{\underline{0}}, \emptyset)_{a^\dagger.\underline{0}\,\|_\emptyset\, b^\dagger.\underline{0}} + \\
&\quad\; <b,\{b\}>\,.\,\ell_{\mathrm{brs}}(\|_\emptyset a)_{a^\dagger.\underline{0}\,\|_\emptyset\, b^\dagger.\underline{0}} \cdot e\ell^{\varepsilon}_{\mathrm{brs}}(\widetilde{\underline{0}}, \widetilde{\underline{0}}, \emptyset)_{a^\dagger.\underline{0}\,\|_\emptyset\, b^\dagger.\underline{0}} \\
&=\; <a^\dagger,\{a\}>\,.\,<b,\{a,b\}>\,.\,\underline{0} + <b,\{b\}>\,.\,<a,\{a,b\}>\,.\,\underline{0}
\end{aligned}$$

which is different from the encoding of $a^\dagger.\,b\,.\,\underline{0} + b\,.\,a\,.\,\underline{0}$ unless $a = b$.
If finally P_1 is the non-initial sequential process $a^\dagger.\,\underline{0}$ and P_2 is the non-initial sequential process $b^\dagger.\,\underline{0}$, so that $\widetilde{P}_1 = \ell_{\mathrm{brs}}(a)^\dagger_{a^\dagger.\underline{0}}\,.\,\widetilde{\underline{0}}$ and $\widetilde{P}_2 = \ell_{\mathrm{brs}}(b)^\dagger_{b^\dagger.\underline{0}}\,.\,\widetilde{\underline{0}}$, then for $\|_\emptyset a \leq_\dagger \|_\emptyset b$:

$$\begin{aligned}
\widetilde{P} \;=\; \ell^{\varepsilon}_{\mathrm{brs}}(P)_P \;&=\; e\ell^{\varepsilon}_{\mathrm{brs}}(\widetilde{P}_1, \widetilde{P}_2, \emptyset)_P \\
&=\; \ell_{\mathrm{brs}}(\|_\emptyset a)^\dagger_{a^\dagger.\underline{0}\,\|_\emptyset\, b\,.\,\underline{0}} \cdot e\ell^{\varepsilon}_{\mathrm{brs}}(\widetilde{\underline{0}}, \widetilde{P}_2, \emptyset)_P + \\
&\quad\; \ell_{\mathrm{brs}}(\|_\emptyset b)_{a\,.\,\underline{0}\,\|_\emptyset\, b^\dagger.\underline{0}} \cdot e\ell^{\varepsilon}_{\mathrm{brs}}(\ell_{\mathrm{brs}}(a)_{a^\dagger.\underline{0}} \cdot \widetilde{\underline{0}}, \widetilde{\underline{0}}, \emptyset)_{a\,.\,\underline{0}\,\|_\emptyset\, b^\dagger.\underline{0}} \\
&=\; <a^\dagger,\{a\}>\,.\,\ell_{\mathrm{brs}}(\|_\emptyset b)^\dagger_{a^\dagger.\underline{0}\,\|_\emptyset\, b^\dagger.\underline{0}} \cdot e\ell^{\varepsilon}_{\mathrm{brs}}(\widetilde{\underline{0}}, \widetilde{\underline{0}}, \emptyset)_{a^\dagger.\underline{0}\,\|_\emptyset\, b^\dagger.\underline{0}} + \\
&\quad\; <b,\{b\}>\,.\,\ell_{\mathrm{brs}}(\|_\emptyset a)_{a^\dagger.\underline{0}\,\|_\emptyset\, b^\dagger.\underline{0}} \cdot e\ell^{\varepsilon}_{\mathrm{brs}}(\widetilde{\underline{0}}, \widetilde{\underline{0}}, \emptyset)_{a^\dagger.\underline{0}\,\|_\emptyset\, b^\dagger.\underline{0}} \\
&=\; <a^\dagger,\{a\}>\,.\,<b^\dagger,\{a,b\}>\,.\,\underline{0} + <b,\{b\}>\,.\,<a,\{a,b\}>\,.\,\underline{0}
\end{aligned}$$

which is different from the encoding of $a^\dagger.\,b^\dagger.\,\underline{0} + b\,.\,a\,.\,\underline{0}$ unless $a = b$. ■

We now investigate the correctness of the ℓ_{brs}-encoding. We start by showing that the encoding is compositional with respect to all the operators of $\mathbb{P}_{\mathrm{brs}}$ and preserves initiality and – to a large extent – backward ready sets.

Lemma 6.5. *Let $a \in \mathcal{A}$ and $P, P_1, P_2 \in \mathbb{P}$ be such that $a\,.\,P, P_1 + P_2 \in \mathbb{P}$. Then:*

1. $\widetilde{a\,.\,P} = <a, \{a\}>\,.\,\widetilde{P}$.
2. $\widetilde{a^\dagger.\,P} = <a^\dagger, \{a\}>\,.\,\widetilde{P}$.
3. $\widetilde{P_1 + P_2} = \widetilde{P}_1 + \widetilde{P}_2$.

Proof. From Definition 6.3 it follows that:

1. $\widetilde{a\,.\,P} = \ell_{\mathrm{brs}}(a)_{a^\dagger.\,P}\,.\,\ell^{\cdot a}_{\mathrm{brs}}(P)_{a^\dagger.\,P} = <a, brs(a^\dagger.\,P)>\,.\,\ell^{\varepsilon}_{\mathrm{brs}}(P)_P = <a, \{a\}>\,.\,\widetilde{P}$ because P is the immediate subprocess of $a\,.\,P$ and, once the environment $a^\dagger.\,P$ reduces to P, the symbol $\cdot_a$ is no longer necessary in the superscript. The fact that $brs(a^\dagger.\,P) = \{a\}$ stems from the initiality of P (otherwise $a\,.\,P \notin \mathbb{P}$).
2. $\widetilde{a^\dagger.\,P} = \ell_{\mathrm{brs}}(a)^\dagger_{a^\dagger.\,to\_\,initial(P)}\,.\,\ell^{\cdot a}_{\mathrm{brs}}(P)_{a^\dagger.\,P} = <a^\dagger, brs(a^\dagger.\,to\_\,initial(P))>\,.\,\ell^{\varepsilon}_{\mathrm{brs}}(P)_P = <a^\dagger, \{a\}>\,.\,\widetilde{P}$ because P is the immediate subprocess of $a^\dagger.\,P$ and, once the environment $a^\dagger.\,P$ reduces to P, the symbol $\cdot_a$ is no longer necessary in the superscript. The fact that $brs(a^\dagger.\,to\_\,initial(P)) = \{a\}$ stems from the initiality of $to\_\,initial(P)$.
3. $\widetilde{P_1 + P_2} = \ell^{+}_{\mathrm{brs}}(P_1)_{P_1+P_2} + \ell^{+}_{\mathrm{brs}}(P_2)_{P_1+P_2} = \ell^{\varepsilon}_{\mathrm{brs}}(P_1)_{P_1} + \ell^{\varepsilon}_{\mathrm{brs}}(P_2)_{P_2} = \widetilde{P_1} + \widetilde{P_2}$ because P_1 and P_2 are the immediate subprocesses of $P_1 + P_2$ and, once the environment $P_1 + P_2$ reduces to P_1 (resp. P_2), the symbol $+$ (resp. $+$) is no longer necessary in the superscript. ∎

Proposition 6.2. *Let $P \in \mathbb{P}$. Then:*

1. *initial*$(\widetilde{P})$ *iff* *initial*(P).
2. $brs(\widetilde{P}) = brs(P)$ *if P has no subprocesses of the form $Q_1 \parallel_{L'} Q_2$ such that: Q_1 and Q_2 are non-initial, the last executed action $b_1^\dagger$ in $\widetilde{Q}_1$ is different from the last executed action $b_2^\dagger$ in $\widetilde{Q}_2$, and $b_1, b_2 \notin L'$.*

Proof. After recalling that for non-initial sequential processes like $\widetilde{Q}_1$ and $\widetilde{Q}_2$ it makes sense to talk about their last executed action, we proceed by induction on the syntactical structure of $P \in \mathbb{P}$ to prove both properties simultaneously:

- If P is $\underline{0}$ then $\widetilde{P} = \underline{0}$ by Definition 6.3. They are both initial and $brs(\widetilde{P}) = brs(P) = \emptyset$.
- If P is $a\,.\,P'$ then $\widetilde{P} = <a, \{a\}>\,.\,\widetilde{P'}$ by Lemma 6.5(1). They are both initial and $brs(\widetilde{P}) = brs(P) = \emptyset$.
- If P is $a^\dagger.\,P'$ then $\widetilde{P} = <a^\dagger, \{a\}>\,.\,\widetilde{P'}$ by Lemma 6.5(2), where *initial*$(\widetilde{P'})$ iff *initial*(P') and $brs(\widetilde{P'}) = brs(P')$ by the induction hypothesis. P and $\widetilde{P}$ are both non-initial. Moreover $brs(\widetilde{P}) = brs(P)$ because the two sets are equal to $\{a\}$ when P' and $\widetilde{P'}$ are both initial, while they are equal to $brs(P')$ when P' and $\widetilde{P'}$ are both non-initial.

- If P is $P' \llcorner \rho \urcorner$ then $\widetilde{P}$ is obtained from $\widetilde{P'}$ by renaming all of its actions and backward ready sets according to ρ, where *initial*$(\widetilde{P'})$ iff *initial*(P') and $brs(\widetilde{P'}) = brs(P')$ by the induction hypothesis. Then *initial*$(\widetilde{P})$ iff *initial*(P) and $brs(\widetilde{P}) = \rho(brs(\widetilde{P'})) = \rho(brs(P')) = brs(P)$.
- If P is $P_1 + P_2$ then $\widetilde{P} = \widetilde{P_1} + \widetilde{P_2}$ by Lemma 6.5(3), where *initial*$(\widetilde{P_k})$ iff *initial*(P_k) and $brs(\widetilde{P_k}) = brs(P_k)$ for $k \in \{1,2\}$ by the induction hypothesis. Then *initial*$(\widetilde{P})$ iff *initial*(P). Moreover $brs(\widetilde{P}) = brs(P)$ because the two sets are equal to $\emptyset$ when P_1, P_2, $\widetilde{P_1}$, $\widetilde{P_2}$ are all initial, $brs(P_1)$ when P_1 and $\widetilde{P_1}$ are non-initial while P_2 and $\widetilde{P_2}$ are initial, or $brs(P_2)$ when P_1 and $\widetilde{P_1}$ are initial while P_2 and $\widetilde{P_2}$ are non-initial.
- If P is $P_1 \parallel_L P_2$ then $\widetilde{P} = e\ell^{\varepsilon}_{\rm brs}(\widetilde{P_1}, \widetilde{P_2}, L)_P$ by Definition 6.3, where *initial*$(\widetilde{P_k})$ iff *initial*(P_k) and $brs(\widetilde{P_k}) = brs(P_k)$ for $k \in \{1,2\}$ by the induction hypothesis. There are two cases:
  - If P_1 and P_2 are both initial – hence P is initial – then so are $\widetilde{P_1}$ and $\widetilde{P_2}$ – hence $\widetilde{P}$ is initial by Definition 6.4 – and vice versa. In this case $brs(\widetilde{P}) = brs(P) = \emptyset$.
  - If P_1 and P_2 are not both initial – hence P is non-initial – then so are $\widetilde{P_1}$ and $\widetilde{P_2}$ – hence $\widetilde{P}$ is non-initial by Definition 6.4 – and vice versa. As far as backward ready set preservation is concerned, there are three subcases:
    - If only P_1 and $\widetilde{P_1}$ are non-initial, say $\widetilde{P_1} = <a_1^\dagger, \{a_1\}> . \widetilde{P_1'} [+ \widetilde{P_1''}]$ where $a_1 \notin L$ and the optional $\widetilde{P_1''}$ is initial, then $brs(\widetilde{P_1}) = brs(P_1) = brs(a_1^\dagger . P_1')$ and $brs(\widetilde{P_2}) = brs(P_2) = \emptyset$. Therefore $brs(\widetilde{P}) = brs(\widetilde{P_1}) = brs(P_1) = brs(P)$ as P_2 and $\widetilde{P_2}$ are initial.
    - The subcase in which only P_2 and $\widetilde{P_2}$ are non-initial is like the previous one.
    - Let P_1, P_2, $\widetilde{P_1}$, $\widetilde{P_2}$ be all non-initial, say $\widetilde{P_k} = <a_k^\dagger, \{a_k\}> . \widetilde{P_k'} [+ \widetilde{P_k''}]$, where the optional $\widetilde{P_k''}$ is initial, for $k \in \{1,2\}$. Since by hypothesis it is not the case that the last executed action $b_1^\dagger$ in $\widetilde{P_1}$ is different from the last executed action $b_2^\dagger$ in $\widetilde{P_2}$ and $b_1, b_2 \notin L$ – and the same is true for all possible subprocesses of P_1 and P_2 of the form $Q_1 \parallel_{L'} Q_2$ with Q_1 and Q_2 non-initial – it holds that $brs(\widetilde{P_k}) = brs(P_k) = \{b_k\}$ for $k \in \{1,2\}$. Recalling that $brs(P_1 \parallel_L P_2) = (brs(P_1) \cap \overline{L}) \cup (brs(P_2) \cap \overline{L}) \cup (brs(P_1) \cap brs(P_2) \cap L)$, there are four further subcases (for the last two think, e.g., of $a^\dagger . b_1^\dagger . \underline{0} \parallel_{\{b_1\}} b_1^\dagger . b_2^\dagger . \underline{0}$):
      - If $b_1, b_2 \notin L$ then from the aforementioned hypothesis it follows that $b_1 = b_2 \triangleq b$ and hence $brs(\widetilde{P}) = brs(P) = (brs(P_1) \cap \overline{L}) \cup (brs(P_2) \cap \overline{L}) \cup \emptyset = \{b\}$.
      - If $b_1, b_2 \in L$ then from $P \in \mathbb{P}$ it follows that $b_1 = b_2 \triangleq b$ and hence $brs(\widetilde{P}) = brs(P) = \emptyset \cup \emptyset \cup (brs(P_1) \cap brs(P_2) \cap L) = \{b\}$.
      - If $b_1 \in L$ and $b_2 \notin L$, then from $P \in \mathbb{P}$ it follows that $brs(\widetilde{P}) = brs(P) = \emptyset \cup (brs(P_2) \cap \overline{L}) \cup \emptyset = \{b_2\}$.
      - If $b_1 \notin L$ and $b_2 \in L$, then from $P \in \mathbb{P}$ it follows that $brs(\widetilde{P}) = brs(P) = (brs(P_1) \cap \overline{L}) \cup \emptyset \cup \emptyset = \{b_1\}$. ■

As an example, for P given by $a^\dagger . \underline{0} \parallel_\emptyset b^\dagger . \underline{0}$ we have that $\widetilde{P} = <a^\dagger, \{a\}> . <b^\dagger, \{a,b\}> . \underline{0} + <b, \{b\}> . <a, \{a,b\}> . \underline{0}$ when the last executed actions satisfy $\Vert_\emptyset a \leq_\dagger \Vert_\emptyset b$ (see the final part of Example 6.2), hence $brs(P) = \{a,b\} \neq \{b\} = brs(\widetilde{P})$ for $a \neq b$. However, in $\widetilde{P}$ the backward ready set $\{a,b\}$ occurs next to the last executed action $b^\dagger$, hence it will label the related transition in $\longrightarrow_{\rm brs}$ (see Table 6.3). Indeed, the $\ell_{\rm brs}$-encoding is correct in the following sense.

Theorem 6.3. *Let $P, P' \in \mathbb{P}$, $\theta \in \Theta$, and $\bar{\theta} \in \Theta_{\rm brs}$. Then $P \xrightarrow{\theta} P'$ iff $\widetilde{P} \xrightarrow{\bar{\theta}, brs(P')}_{\rm brs} \widetilde{P}'$ with $act(\theta) = act(\bar{\theta})$.*

Proof. We proceed by induction on the number $n \in \mathbb{N}_{\geq 1}$ of applications of operational semantic rules that are necessary to derive the considered transitions:

- If $n = 1$ then P is $a\,.\,Q$, with *initial*(Q), and $\widetilde{P} = <a, \{a\}>\,.\,\widetilde{Q}$ by Lemma 6.5(1). According to the rules $\text{ACT}_{\rm f}$ in Table 2.1 and $\text{ACT}_{\rm brs,f}$ in Table 6.3, their only outgoing transitions are respectively $P \xrightarrow{a} a^\dagger\,.\,Q$ and $\widetilde{P} \xrightarrow{a,\{a\}}_{\rm brs} <a^\dagger, \{a\}>\,.\,\widetilde{Q}$, with $\{a\} = brs(a^\dagger\,.\,Q)$ as *initial*(Q) and $<a^\dagger, \{a\}>\,.\,\widetilde{Q} = \widetilde{a^\dagger\,.\,Q}$ by Lemma 6.5(2).
- If $n > 1$ there are four cases:
  - Let P be $a^\dagger\,.\,Q$. If $P \xrightarrow{\cdot_a \theta'} a^\dagger\,.\,Q'$ then $Q \xrightarrow{\theta'} Q'$ by rule $\text{ACT}_{\rm p}$ in Table 2.1. By the induction hypothesis this is equivalent to $\widetilde{Q} \xrightarrow{\bar{\theta}', brs(Q')}_{\rm brs} \widetilde{Q}'$ with $act(\theta') = act(\bar{\theta}')$, which implies $<a^\dagger, \{a\}>\,.\,\widetilde{Q} \xrightarrow{\cdot_a \bar{\theta}', brs(a^\dagger\,.\,Q')}_{\rm brs} <a^\dagger, \{a\}>\,.\,\widetilde{Q}'$ by rule $\text{ACT}_{\rm brs,p}$ in Table 6.3 – as $brs(a^\dagger\,.\,Q') = brs(Q')$ due to $\neg$*initial*(Q') – with $<a^\dagger, \{a\}>\,.\,\widetilde{Q} = \widetilde{P}$ and $<a^\dagger, \{a\}>\,.\,\widetilde{Q}' = \widetilde{a^\dagger\,.\,Q'}$ by Lemma 6.5(2).
    The proof starting from $\widetilde{P} \xrightarrow{\cdot_a \bar{\theta}', brs(a^\dagger\,.\,Q')}_{\rm brs} \widetilde{a^\dagger\,.\,Q'}$ is similar.
  - Let P be $Q \llcorner \rho \urcorner$. If $P \xrightarrow{\llcorner_\rho \theta'} Q' \llcorner \rho \urcorner$ then $Q \xrightarrow{\theta'} Q'$ by rule REN in Table 2.1. By the induction hypothesis this is equivalent to $\widetilde{Q} \xrightarrow{\bar{\theta}', brs(Q')}_{\rm brs} \widetilde{Q}'$ with $act(\theta') = act(\bar{\theta}')$, which implies $\widetilde{P} \xrightarrow{\bar{\bar{\theta}}', brs(Q' \llcorner \rho \urcorner)}_{\rm brs} \widetilde{Q' \llcorner \rho \urcorner}$ with $\bar{\bar{\theta}}'$ obtained from $\bar{\theta}'$ by changing the action at its end according to ρ so that $act(\llcorner_\rho \theta') = act(\bar{\bar{\theta}}')$, because $\widetilde{P}$ (resp. $\widetilde{Q' \llcorner \rho \urcorner}$) is obtained from $\widetilde{Q}$ (resp. $\widetilde{Q}'$) by renaming all of its actions and backward ready sets according to ρ and $brs(Q' \llcorner \rho \urcorner) = \rho(brs(Q'))$.
    The proof starting from $\widetilde{P} \xrightarrow{\bar{\bar{\theta}}', brs(Q' \llcorner \rho \urcorner)}_{\rm brs} \widetilde{Q' \llcorner \rho \urcorner}$ is similar.
  - Let P be $P_1 + P_2$. There are two subcases:
    - If $P \xrightarrow{+\theta'} P_1' + P_2$ with *initial*(P_2), then $P_1 \xrightarrow{\theta'} P_1'$ by rule $\text{CHO}_{\rm l}$ in Table 2.1. By the induction hypothesis this is equivalent to $\widetilde{P}_1 \xrightarrow{\bar{\theta}', brs(P_1')}_{\rm brs} \widetilde{P}_1'$ with $act(\theta') = act(\bar{\theta}')$, which implies $\widetilde{P}_1 + \widetilde{P}_2 \xrightarrow{+\bar{\theta}', brs(P_1' + P_2)}_{\rm brs} \widetilde{P}_1' + \widetilde{P}_2$ by rule $\text{CHO}_{\rm brs,l}$ in Table 6.3 – as $brs(P_1' + P_2) = brs(P_1')$ due to *initial*(P_2) – with $\widetilde{P}_1 + \widetilde{P}_2 = \widetilde{P}$ and $\widetilde{P}_1' + \widetilde{P}_2 = \widetilde{P_1' + P_2}$ by Lemma 6.5(3).
      The proof starting from $\widetilde{P} \xrightarrow{+\bar{\theta}', brs(P_1' + P_2)}_{\rm brs} \widetilde{P_1' + P_2}$ is similar.
    - The subcase in which $P \xrightarrow{+\theta'} P_1 + P_2'$ with *initial*(P_1) is like the previous one.
  - Let P be $P_1 \parallel_L P_2$. There are three subcases:
    - If $P \xrightarrow{\parallel_L \theta'} P_1' \parallel_L P_2$ with $act(\theta') \notin L$, then $P_1 \xrightarrow{\theta'} P_1'$ by rule $\text{PAR}_{\rm l}$ in Table 2.1. By the induction hypothesis this is equivalent to $\widetilde{P}_1 \xrightarrow{\bar{\theta}', brs(P_1')}_{\rm brs} \widetilde{P}_1'$ with $act(\theta') = act(\bar{\theta}')$. By Definition 6.4 this implies that $\widetilde{P}$, after a possible sequence of executed actions, has a maximal initial subprocess with a summand of the form $<act(\parallel_L \bar{\theta}'), brs(P_1' \parallel_L P_2)>\,.\,\widetilde{P_1' \parallel_L P_2}$, hence $\widetilde{P} \xrightarrow{\bar{\bar{\theta}}', brs(P_1' \parallel_L P_2)}_{\rm brs} \widetilde{P_1' \parallel_L P_2}$ for a suitable $\bar{\bar{\theta}}' \in \Theta_{\rm brs}$ such that $act(\bar{\theta}') = act(\bar{\bar{\theta}}')$.
      The proof starting from $\widetilde{P} \xrightarrow{\bar{\bar{\theta}}', brs(P_1' \parallel_L P_2)}_{\rm brs} \widetilde{P_1' \parallel_L P_2}$ is similar.

* The subcase in which $P \xrightarrow{\mathbb{L}_L \theta'} P_1 \parallel_L P_2'$ with $act(\theta') \notin L$ is like the previous one.
* If $P \xrightarrow{\langle \theta_1, \theta_2 \rangle_L} P_1' \parallel_L P_2'$ with $act(\theta_1) = act(\theta_2) \in L$, then $P_k \xrightarrow{\theta_k} P_k'$ for $k \in \{1,2\}$ by rule SYN in Table 2.1. By the induction hypothesis this is equivalent to $\widetilde{P}_k \xrightarrow{\bar{\theta}_k, brs(P_k')}_{\rm brs} \widetilde{P}_k'$ with $act(\theta_k) = act(\bar{\theta}_k)$. By Definition 6.4 this implies that $\widetilde{P}$, after a possible sequence of executed actions, has a maximal initial subprocess with a summand of the form $<act(\langle \bar{\theta}_1, \bar{\theta}_2 \rangle_L), brs(P_1' \parallel_L P_2')> . \widetilde{P_1' \parallel_L P_2'}$, hence $\widetilde{P} \xrightarrow{\bar{\bar{\theta}}, brs(P_1' \parallel_L P_2')}_{\rm brs} \widetilde{P_1' \parallel_L P_2'}$ for a suitable $\bar{\bar{\theta}} \in \Theta_{\rm brs}$ such that $act(\bar{\theta}_k) = act(\bar{\bar{\theta}})$ for $k \in \{1,2\}$. The proof starting from $\widetilde{P} \xrightarrow{\bar{\bar{\theta}}, brs(P_1' \parallel_L P_2')}_{\rm brs} \widetilde{P_1' \parallel_L P_2'}$ is similar. ∎

Corollary 6.1. *Let $P_1, P_2 \in \mathbb{P}$ and $B \in \{\rm RB, FRB\}$. Then $P_1 \sim_B P_2$ iff $\widetilde{P}_1 \sim_{B:\ell_{\rm brs}} \widetilde{P}_2$.*

Proof. The proof is divided into two parts:

- Suppose that $P_1 \sim_B P_2$ and let $\mathcal{B}$ be a $\sim_B$-bisimulation containing the pair (P_1, P_2). The result follows by proving that $\mathcal{B}' = \{(\widetilde{Q}_1, \widetilde{Q}_2) \mid (Q_1, Q_2) \in \mathcal{B}\}$ is a $\sim_{B:\ell_{\rm brs}}$-bisimulation. Let $(\widetilde{Q}_1, \widetilde{Q}_2) \in \mathcal{B}'$ so that $(Q_1, Q_2) \in \mathcal{B}$:
  - If $B = \rm FRB$ and $\widetilde{Q}_1 \xrightarrow{\bar{\theta}_1, brs(Q_1')}_{\rm brs} \widetilde{Q}_1'$, then $Q_1 \xrightarrow{\theta_1} Q_1'$ with $act(\bar{\theta}_1) = act(\theta_1)$ due to Theorem 6.3. From $(Q_1, Q_2) \in \mathcal{B}$ it follows that there exists $Q_2 \xrightarrow{\theta_2} Q_2'$ such that $act(\theta_1) = act(\theta_2)$ and $(Q_1', Q_2') \in \mathcal{B}$. Thus $\widetilde{Q}_2 \xrightarrow{\bar{\theta}_2, brs(Q_2')}_{\rm brs} \widetilde{Q}_2'$ with $act(\theta_2) = act(\bar{\theta}_2)$ due to Theorem 6.3 – so $act(\bar{\theta}_1) = act(\bar{\theta}_2)$ – and $(Q_1', Q_2') \in \mathcal{B}$ implying $brs(Q_1') = brs(Q_2')$ due to Proposition 3.2(2) and $(\widetilde{Q}_1', \widetilde{Q}_2') \in \mathcal{B}'$.
  - If $\widetilde{Q}_1' \xrightarrow{\bar{\theta}_1, brs(Q_1)}_{\rm brs} \widetilde{Q}_1$ the proof is like the previous one where Proposition 3.2(2) yields $brs(Q_1) = brs(Q_2)$.
- Suppose that $\widetilde{P}_1 \sim_{B:\ell_{\rm brs}} \widetilde{P}_2$ and let $\mathcal{B}$ be a $\sim_{B:\ell_{\rm brs}}$-bisimulation containing the pair $(\widetilde{P}_1, \widetilde{P}_2)$. The result follows by proving that $\mathcal{B}' = \{(Q_1, Q_2) \mid (\widetilde{Q}_1, \widetilde{Q}_2) \in \mathcal{B}\}$ is a $\sim_B$-bisimulation. Let $(Q_1, Q_2) \in \mathcal{B}'$ so that $(\widetilde{Q}_1, \widetilde{Q}_2) \in \mathcal{B}$:
  - If $B = \rm FRB$ and $Q_1 \xrightarrow{\theta_1} Q_1'$, then $\widetilde{Q}_1 \xrightarrow{\bar{\theta}_1, brs(Q_1')}_{\rm brs} \widetilde{Q}_1'$ with $act(\theta_1) = act(\bar{\theta}_1)$ due to Theorem 6.3. From $(\widetilde{Q}_1, \widetilde{Q}_2) \in \mathcal{B}$ it follows that there exists $\widetilde{Q}_2 \xrightarrow{\bar{\theta}_2, brs(Q_2')}_{\rm brs} \widetilde{Q}_2'$ such that $act(\bar{\theta}_1) = act(\bar{\theta}_2)$, $brs(Q_1') = brs(Q_2')$, and $(\widetilde{Q}_1', \widetilde{Q}_2') \in \mathcal{B}$. Thus $Q_2 \xrightarrow{\theta_2} Q_2'$ with $act(\bar{\theta}_2) = act(\theta_2)$ due to Theorem 6.3 – so $act(\theta_1) = act(\theta_2)$ – and $(\widetilde{Q}_1', \widetilde{Q}_2') \in \mathcal{B}$ implying $(Q_1', Q_2') \in \mathcal{B}'$.
  - If $Q_1' \xrightarrow{\theta_1} Q_1$ the proof is like the previous one. ∎

We conclude by showing a form of compositionality of $\sim_{\rm RB:\ell_{brs}}$ and $\sim_{\rm FRB:\ell_{brs}}$ with respect to all the operators of $\mathbb{P}$.

Theorem 6.4. *Let* $\sim \in \{\sim_{\mathrm{RB}:\ell_{\mathrm{brs}}}, \sim_{\mathrm{FRB}:\ell_{\mathrm{brs}}}\}$ *and* $P_1, P_2 \in \mathbb{P}$. *If* $\widetilde{P_1} \sim \widetilde{P_2}$ *then:*

- *For all* $a \in \mathcal{A}$*:*
  - $\widetilde{a\,.\,P_1} \sim \widetilde{a\,.\,P_2}$ *provided that* $\mathit{initial}(P_1) \wedge \mathit{initial}(P_2)$.
  - $\widetilde{a^\dagger\,.\,P_1} \sim \widetilde{a^\dagger\,.\,P_2}$.
- *For all* $\rho : \mathcal{A} \to \mathcal{A}$ *such that* $\rho(\tau) = \tau$*:*
  - $\widetilde{P_1 \llcorner \rho \urcorner} \sim \widetilde{P_2 \llcorner \rho \urcorner}$.
- *For all* $P \in \mathbb{P}$*:*
  - $\widetilde{P_1 + P} \sim \widetilde{P_2 + P}$ *and* $\widetilde{P + P_1} \sim \widetilde{P + P_2}$ *provided that* $\mathit{initial}(P) \vee (\mathit{initial}(P_1) \wedge \mathit{initial}(P_2))$.
- *For all* $P \in \mathbb{P}$ *and* $L \subseteq \mathcal{A} \setminus \{\tau\}$*:*
  - $\widetilde{P_1 \parallel_L P} \sim \widetilde{P_2 \parallel_L P}$ *and* $\widetilde{P \parallel_L P_1} \sim \widetilde{P \parallel_L P_2}$ *provided that* $P_1 \parallel_L P, P_2 \parallel_L P, P \parallel_L P_1, P \parallel_L P_2 \in \mathbb{P}$.

Proof. Similar to the proof of Theorem 4.1 by exploiting Lemma 6.5. ∎

6.4.2 Process Encoding Based on Weak Backward Ready Sets for $\approx_{\mathbf{RB}}$ and $\approx_{\mathbf{FRB:ps}}$

Definitions 6.3 and 6.4 have precisely the same structure in the case of $\ell_{\mathrm{brs,w}}$, whose lifting applied to P we denote by $\widehat{P}$. We recall that $\ell_{\mathrm{brs,w}}(\theta)_{P'} = <\mathit{act}(\theta), \mathit{brs}_{\mathrm{w}}(P')>$ for $P \xrightarrow{\theta} P'$ and we let $\ell_{\mathrm{brs,w}}(\theta)^\dagger_{P'} = <\mathit{act}(\theta)^\dagger, \mathit{brs}_{\mathrm{w}}(P')>$. Due to the use of $\mathit{brs}_{\mathrm{w}}(P')$ in place of $\mathit{brs}(P')$, the main difference between $\widehat{P}$ and $\widetilde{P}$ has to do with action sets accompanying unobservable actions inside extended prefixes.

Example 6.3. Let $a \neq \tau \neq b$:

- $\widetilde{\tau\,.\,\underline{0}} = \ell_{\mathrm{brs}}(\tau)_{\tau^\dagger\,.\,\underline{0}}\,.\,\underline{0} = <\tau, \{\tau\}>\,.\,\underline{0}$
  $\widehat{\tau\,.\,\underline{0}} = \ell_{\mathrm{brs,w}}(\tau)_{\tau^\dagger\,.\,\underline{0}}\,.\,\underline{0} = <\tau, \emptyset>\,.\,\underline{0}$
- $\widetilde{\tau\,.\,\tau\,.\,\underline{0}} = \ell_{\mathrm{brs}}(\tau)_{\tau^\dagger\,.\,\tau\,.\,\underline{0}}\,.\,\ell_{\mathrm{brs}}(\tau)_{\tau^\dagger\,.\,\tau^\dagger\,.\,\underline{0}}\,.\,\underline{0} = <\tau, \{\tau\}>\,.\,<\tau, \{\tau\}>\,.\,\underline{0}$
  $\widehat{\tau\,.\,\tau\,.\,\underline{0}} = \ell_{\mathrm{brs,w}}(\tau)_{\tau^\dagger\,.\,\tau\,.\,\underline{0}}\,.\,\ell_{\mathrm{brs,w}}(\tau)_{\tau^\dagger\,.\,\tau^\dagger\,.\,\underline{0}}\,.\,\underline{0} = <\tau, \emptyset>\,.\,<\tau, \emptyset>\,.\,\underline{0}$ — equal to $<\tau, \emptyset>\,.\,\widehat{\tau\,.\,\underline{0}}$
- $\widetilde{a\,.\,\tau\,.\,\underline{0}} = \ell_{\mathrm{brs}}(a)_{a^\dagger\,.\,\tau\,.\,\underline{0}}\,.\,\ell_{\mathrm{brs}}(\tau)_{a^\dagger\,.\,\tau^\dagger\,.\,\underline{0}}\,.\,\underline{0} = <a, \{a\}>\,.\,<\tau, \{\tau\}>\,.\,\underline{0}$
  $\widehat{a\,.\,\tau\,.\,\underline{0}} = \ell_{\mathrm{brs,w}}(a)_{a^\dagger\,.\,\tau\,.\,\underline{0}}\,.\,\ell_{\mathrm{brs,w}}(\tau)_{a^\dagger\,.\,\tau^\dagger\,.\,\underline{0}}\,.\,\underline{0} = <a, \{a\}>\,.\,<\tau, \{a\}>\,.\,\underline{0}$
- $\widetilde{\tau^\dagger\,.\,\tau\,.\,\underline{0}} = \ell_{\mathrm{brs}}(\tau)^\dagger_{\tau^\dagger\,.\,\tau\,.\,\underline{0}}\,.\,\ell_{\mathrm{brs}}(\tau)_{\tau^\dagger\,.\,\tau^\dagger\,.\,\underline{0}}\,.\,\underline{0} = <\tau^\dagger, \{\tau\}>\,.\,<\tau, \{\tau\}>\,.\,\underline{0}$
  $\widehat{\tau^\dagger\,.\,\tau\,.\,\underline{0}} = \ell_{\mathrm{brs,w}}(\tau)^\dagger_{\tau^\dagger\,.\,\tau\,.\,\underline{0}}\,.\,\ell_{\mathrm{brs,w}}(\tau)_{\tau^\dagger\,.\,\tau^\dagger\,.\,\underline{0}}\,.\,\underline{0} = <\tau^\dagger, \emptyset>\,.\,<\tau, \emptyset>\,.\,\underline{0}$ — equal to $<\tau^\dagger, \emptyset>\,.\,\widehat{\tau\,.\,\underline{0}}$
- $\widetilde{a^\dagger\,.\,\tau^\dagger\,.\,\tau\,.\,\underline{0}} = \ell_{\mathrm{brs}}(a)^\dagger_{a^\dagger\,.\,\tau\,.\,\tau\,.\,\underline{0}}\,.\,\ell_{\mathrm{brs}}(\tau)^\dagger_{a^\dagger\,.\,\tau^\dagger\,.\,\tau\,.\,\underline{0}}\,.\,\ell_{\mathrm{brs}}(\tau)_{a^\dagger\,.\,\tau^\dagger\,.\,\tau^\dagger\,.\,\underline{0}}\,.\,\underline{0} = <a^\dagger, \{a\}>\,.\,<\tau^\dagger, \{\tau\}>\,.\,<\tau, \{\tau\}>\,.\,\underline{0}$
  $\widehat{a^\dagger\,.\,\tau^\dagger\,.\,\tau\,.\,\underline{0}} = \ell_{\mathrm{brs,w}}(a)^\dagger_{a^\dagger\,.\,\tau\,.\,\tau\,.\,\underline{0}}\,.\,\ell_{\mathrm{brs,w}}(\tau)^\dagger_{a^\dagger\,.\,\tau^\dagger\,.\,\tau\,.\,\underline{0}}\,.\,\ell_{\mathrm{brs,w}}(\tau)_{a^\dagger\,.\,\tau^\dagger\,.\,\tau^\dagger\,.\,\underline{0}}\,.\,\underline{0} = <a^\dagger, \{a\}>\,.\,<\tau^\dagger, \{a\}>\,.\,<\tau, \{a\}>\,.\,\underline{0}$
- $\widetilde{(a^\dagger\,.\,b^\dagger\,.\,b\,.\,\underline{0}) \llcorner b \mapsto \tau \urcorner} = \ell^{\llcorner b \mapsto \tau \urcorner}_{\mathrm{brs}}(a^\dagger\,.\,b^\dagger\,.\,b\,.\,\underline{0})_{(a^\dagger\,.\,b^\dagger\,.\,b\,.\,\underline{0}) \llcorner b \mapsto \tau \urcorner} = <a^\dagger, \{a\}>\,.\,<\tau^\dagger, \{\tau\}>\,.\,<\tau, \{\tau\}>\,.\,\underline{0}$
  $\widehat{(a^\dagger\,.\,b^\dagger\,.\,b\,.\,\underline{0}) \llcorner b \mapsto \tau \urcorner} = \ell^{\llcorner b \mapsto \tau \urcorner}_{\mathrm{brs,w}}(a^\dagger\,.\,b^\dagger\,.\,b\,.\,\underline{0})_{(a^\dagger\,.\,b^\dagger\,.\,b\,.\,\underline{0}) \llcorner b \mapsto \tau \urcorner} = <a^\dagger, \{a\}>\,.\,<\tau^\dagger, \{a\}>\,.\,<\tau, \{a\}>\,.\,\underline{0}$ ∎

The properties of the $\ell_{\mathrm{brs,w}}$-encoding are similar to those of the ℓ_{brs}-encoding apart from its compositionality with respect to action prefix in $\mathbb{P}_{\mathrm{brs}}$, which gets looser as illustrated by the previous examples.

Lemma 6.6. *Let $a \in \mathcal{A}$ and $P, P_1, P_2 \in \mathbb{P}$ be such that $a\,.\,P, P_1 + P_2 \in \mathbb{P}$. Then:*

1. *$\widehat{a\,.\,P} = <a, \emptyset>\,.\,\widehat{P}$ if $a = \tau$, while $\widehat{a\,.\,P} = <a, \{a\}>\,.\,U_P$ with U_P being obtained from $\widehat{P}$ by adding a to the second component of each possible extended τ-prefix at the beginning of $\widehat{P}$ if $a \neq \tau$.*
2. *$\widehat{a^\dagger.\,P} = <a^\dagger, \emptyset>\,.\,\widehat{P}$ if $a = \tau$, while $\widehat{a^\dagger.\,P} = <a^\dagger, \{a\}>\,.\,U_P$ with U_P being obtained from $\widehat{P}$ by adding a to the second component of each possible extended $\tau^\dagger$- and τ-prefix at the beginning of $\widehat{P}$ if $a \neq \tau$.*
3. *$\widehat{P_1 + P_2} = \widehat{P}_1 + \widehat{P}_2$.*

Proof. From the version of Definition 6.3 for $\ell_{\mathrm{brs,w}}$ it follows that:

1. $\widehat{a\,.\,P} = \ell_{\mathrm{brs,w}}(a)_{a^\dagger.\,P}\,.\,\ell^{\cdot a}_{\mathrm{brs,w}}(P)_{a^\dagger.\,P} = <a, brs_{\mathrm{w}}(a^\dagger.\,P)>\,.\,\ell^{\cdot a}_{\mathrm{brs,w}}(P)_{a^\dagger.\,P}$. There are two cases:
   - If $a = \tau$ then $brs_{\mathrm{w}}(a^\dagger.\,P) = \emptyset$ due to the initiality of P (otherwise $a\,.\,P \notin \mathbb{P}$). Moreover $\ell^{\cdot a}_{\mathrm{brs,w}}(P)_{a^\dagger.\,P}$ coincides with $\ell^{\varepsilon}_{\mathrm{brs,w}}(P)_P$ – where the symbol $\cdot_a$ is no longer necessary in the superscript once the environment $a^\dagger.\,P$ reduces to P – i.e., $\widehat{P}$, because $brs_{\mathrm{w}}(a^\dagger.\,P) = \emptyset$.
   - If $a \neq \tau$ then $brs_{\mathrm{w}}(a^\dagger.\,P) = \{a\}$ due to the initiality of P (otherwise $a\,.\,P \notin \mathbb{P}$). Moreover $\ell^{\cdot a}_{\mathrm{brs,w}}(P)_{a^\dagger.\,P}$ is obtained from $\ell^{\varepsilon}_{\mathrm{brs,w}}(P)_P$ – where the symbol $\cdot_a$ is no longer necessary in the superscript once the environment $a^\dagger.\,P$ reduces to P – i.e., $\widehat{P}$, provided that a is added to the second component of each possible extended τ-prefix at the beginning of $\widehat{P}$.
2. $\widehat{a^\dagger.\,P} = \ell_{\mathrm{brs,w}}(a)^\dagger_{a^\dagger.\,to\_\,initial(P)}\,.\,\ell^{\cdot a}_{\mathrm{brs,w}}(P)_{a^\dagger.\,P} = <a^\dagger, brs_{\mathrm{w}}(a^\dagger.\,to\_\,initial(P))>\,.\,\ell^{\cdot a}_{\mathrm{brs,w}}(P)_{a^\dagger.\,P}$. There are two cases:
   - If $a = \tau$ then $brs_{\mathrm{w}}(a^\dagger.\,to\_\,initial(P)) = \emptyset$ due to the initiality of $to\_\,initial(P)$. Moreover $\ell^{\cdot a}_{\mathrm{brs,w}}(P)_{a^\dagger.\,P}$ coincides with $\ell^{\varepsilon}_{\mathrm{brs,w}}(P)_P$ – where the symbol $\cdot_a$ is no longer necessary in the superscript once the environment $a^\dagger.\,P$ reduces to P – i.e., $\widehat{P}$, because $brs_{\mathrm{w}}(a^\dagger.\,to\_\,initial(P)) = \emptyset$.
   - If $a \neq \tau$ then $brs_{\mathrm{w}}(a^\dagger.\,to\_\,initial(P)) = \{a\}$ due to the initiality of $to\_\,initial(P)$. Moreover $\ell^{\cdot a}_{\mathrm{brs,w}}(P)_{a^\dagger.\,P}$ is obtained from $\ell^{\varepsilon}_{\mathrm{brs,w}}(P)_P$ – where the symbol $\cdot_a$ is no longer necessary in the superscript once the environment $a^\dagger.\,P$ reduces to P – i.e., $\widehat{P}$, provided that a is added to the second component of each possible extended $\tau^\dagger$- and τ-prefix at the beginning of $\widehat{P}$.
3. $\widehat{P_1 + P_2} = \ell^{+}_{\mathrm{brs,w}}(P_1)_{P_1+P_2} + \ell^{+}_{\mathrm{brs,w}}(P_2)_{P_1+P_2} = \ell^{\varepsilon}_{\mathrm{brs,w}}(P_1)_{P_1} + \ell^{\varepsilon}_{\mathrm{brs,w}}(P_2)_{P_2} = \widehat{P_1} + \widehat{P_2}$ because P_1 and P_2 are the immediate subprocesses of $P_1 + P_2$ and, once the environment $P_1 + P_2$ reduces to P_1 (resp. P_2), the symbol $+$ (resp. $+$) is no longer necessary in the superscript. ∎

Proposition 6.3. *Let $P \in \mathbb{P}$. Then:*

1. *initial*$(\widehat{P})$ *iff* *initial*(P).
2. $brs_{\mathrm{w}}(\widehat{P}) = brs_{\mathrm{w}}(P)$ *if P has no subprocesses of the form $Q_1 \parallel_{L'} Q_2$ such that: Q_1 and Q_2 are non-initial, the last executed observable action $b_1^\dagger$ in $\widehat{Q}_1$ is different from the last executed observable action $b_2^\dagger$ in $\widehat{Q}_2$, and $b_1, b_2 \notin L'$.*

Proof. After recalling that for non-initial sequential processes like $\widehat{Q}_1$ and $\widehat{Q}_2$ it makes sense to talk about their last executed observable action (if any, i.e, if it is not the case that all executed actions are $\tau^\dagger$), we proceed by induction on the syntactical structure of $P \in \mathbb{P}$ to prove both properties simultaneously:

- If P is $\underline{0}$ then $\widehat{P} = \underline{0}$ by the version of Definition 6.3 for $\ell_{\mathrm{brs,w}}$. They are both initial and $brs_{\mathrm{w}}(\widehat{P}) = brs_{\mathrm{w}}(P) = \emptyset$.
- If P is $a\,.\,P'$ then $\widehat{P}$ is of the form established by Lemma 6.6(1). They are both initial and $brs_{\mathrm{w}}(\widehat{P}) = brs_{\mathrm{w}}(P) = \emptyset$.
- If P is $a^\dagger.\,P'$ then $\widehat{P}$ is of the form established by Lemma 6.6(2), where *initial*$(\widehat{P'})$ iff *initial*(P') and $brs_{\mathrm{w}}(\widehat{P'}) = brs_{\mathrm{w}}(P')$ by the induction hypothesis. P and $\widehat{P}$ are both non-initial. Moreover $brs_{\mathrm{w}}(\widehat{P}) = brs_{\mathrm{w}}(P)$ because the two sets are equal to $\emptyset$ – if $a = \tau$ – or $\{a\}$ – if $a \neq \tau$ – when P' and $\widehat{P}'$ are both initial, while they are equal to $brs_{\mathrm{w}}(P')$ when P' and $\widehat{P}'$ are both non-initial.
- If P is $P'{\llcorner}\rho{\urcorner}$ then $\widehat{P}$ is obtained from $\widehat{P'}$ by renaming all of its actions and backward ready sets according to ρ, provided that the second component of each possible extended prefix whose first component is observable and renamed τ by ρ, as well as the second component of each possible subsequent extended prefix whose first component is named τ, is changed to the second component of the closest preceding extended prefix whose first component is an action neither named τ nor renamed τ by ρ (or $\emptyset$ if there is no such a preceding prefix), where *initial*$(\widehat{P'})$ iff *initial*(P') and $brs_{\mathrm{w}}(\widehat{P'}) = brs_{\mathrm{w}}(P')$ by the induction hypothesis. Then *initial*$(\widehat{P})$ iff *initial*(P). Moreover $brs_{\mathrm{w}}(\widehat{P}) = \rho(brs_{\mathrm{w}}(\rho_\tau^\dagger(\widehat{P'}))) = \rho(brs_{\mathrm{w}}(\rho_\tau^\dagger(P'))) = brs_{\mathrm{w}}(P)$.
- If P is $P_1 + P_2$ then $\widehat{P} = \widehat{P}_1 + \widehat{P}_2$ by Lemma 6.6(3), where *initial*$(\widehat{P}_k)$ iff *initial*(P_k) and $brs_{\mathrm{w}}(\widehat{P}_k) = brs_{\mathrm{w}}(P_k)$ for $k \in \{1,2\}$ by the induction hypothesis. Then *initial*$(\widehat{P})$ iff *initial*(P). Moreover $brs_{\mathrm{w}}(\widehat{P}) = brs_{\mathrm{w}}(P)$ because the two sets are equal to $\emptyset$ when P_1, P_2, $\widehat{P}_1$, $\widehat{P}_2$ are all initial, $brs_{\mathrm{w}}(P_1)$ when P_1 and $\widehat{P}_1$ are non-initial while P_2 and $\widehat{P}_2$ are initial, or $brs_{\mathrm{w}}(P_2)$ when P_1 and $\widehat{P}_1$ are initial while P_2 and $\widehat{P}_2$ are non-initial.
- If P is $P_1 \parallel_L P_2$ then $\widehat{P} = e\ell^{\varepsilon}_{\mathrm{brs,w}}(\widehat{P}_1, \widehat{P}_2, L)_P$ by the version of Definition 6.3 for $\ell_{\mathrm{brs,w}}$, where *initial*$(\widehat{P}_k)$ iff *initial*(P_k) and $brs_{\mathrm{w}}(\widehat{P}_k) = brs_{\mathrm{w}}(P_k)$ for $k \in \{1,2\}$ by the induction hypothesis. There are two cases:
  - If P_1 and P_2 are both initial – hence P is initial – then so are $\widehat{P}_1$ and $\widehat{P}_2$ – hence $\widehat{P}$ is initial by the version of Definition 6.4 for $\ell_{\mathrm{brs,w}}$ – and vice versa. In this case $brs_{\mathrm{w}}(\widehat{P}) = brs_{\mathrm{w}}(P) = \emptyset$.
  - If P_1 and P_2 are not both initial – hence P is non-initial – then so are $\widehat{P}_1$ and $\widehat{P}_2$ – hence $\widehat{P}$ is non-initial by the version of Definition 6.4 for $\ell_{\mathrm{brs,w}}$ – and vice versa. As far as weak backward ready set preservation is concerned, there are three subcases:

- If only P_1 and $\widehat{P}_1$ are non-initial, say $\widehat{P}_1 = <a_1^\dagger, \beth_1> . \widehat{P}_1' [+ \widehat{P}_1'']$ where $a_1 \notin L$, $\beth_1$ is $\emptyset$ or $\{a_1\}$ depending on whether $a_1 = \tau$ or not, and the optional $\widehat{P}_1''$ is initial, then $brs_{\rm w}(\widehat{P}_1) = brs_{\rm w}(P_1) = brs_{\rm w}(a_1^\dagger . P_1')$ and $brs_{\rm w}(\widehat{P}_2) = brs_{\rm w}(P_2) = \emptyset$. Therefore $brs_{\rm w}(\widehat{P}) = brs_{\rm w}(\widehat{P}_1) = brs_{\rm w}(P_1) = brs_{\rm w}(P)$ as P_2 and $\widehat{P}_2$ are initial.
- The subcase in which only P_2 and $\widehat{P}_2$ are non-initial is like the previous one.
- Let P_1, P_2, $\widehat{P}_1$, $\widehat{P}_2$ be all non-initial, say $\widehat{P}_k = <a_k^\dagger, \beth_k> . \widehat{P}_k' [+ \widehat{P}_k'']$, where $\beth_k$ is $\emptyset$ or $\{a_k\}$ depending on whether $a_k = \tau$ or not and the optional $\widehat{P}_k''$ is initial, for $k \in \{1,2\}$. There are four further subcases:
  - If all executed actions in $\widehat{P}_1$ and in $\widehat{P}_2$ are $\tau^\dagger$, then $brs_{\rm w}(\widehat{P}) = brs_{\rm w}(P) = \emptyset$.
  - If all executed actions in $\widehat{P}_1$ are $\tau^\dagger$ while this is not the case for $\widehat{P}_2$, whose last executed observable action is $b_2^\dagger$, then $brs_{\rm w}(\widehat{P}) = brs_{\rm w}(P) = \{b_2\}$.
  - If all executed actions in $\widehat{P}_2$ are $\tau^\dagger$ while this is not the case for $\widehat{P}_1$, whose last executed observable action is $b_1^\dagger$, then $brs_{\rm w}(\widehat{P}) = brs_{\rm w}(P) = \{b_1\}$.
  - Assume that not all executed actions in $\widehat{P}_1$ and in $\widehat{P}_2$ are $\tau^\dagger$. Since by hypothesis it is not the case that the last executed observable action $b_1^\dagger$ in $\widehat{P}_1$ is different from the last executed observable action $b_2^\dagger$ in $\widehat{P}_2$ and $b_1, b_2 \notin L$ – and the same is true for all possible subprocesses of P_1 and P_2 of the form $Q_1 \parallel_{L'} Q_2$ with Q_1 and Q_2 non-initial – it holds that $brs_{\rm w}(\widehat{P}_k) = brs_{\rm w}(P_k) = \{b_k\}$ for $k \in \{1,2\}$. Recalling that $brs_{\rm w}(P_1 \parallel_L P_2) = (brs_{\rm w}(P_1) \cap \overline{L}) \cup (brs_{\rm w}(P_2) \cap \overline{L}) \cup (brs_{\rm w}(P_1) \cap brs_{\rm w}(P_2) \cap L)$, there are four more subcases (for the last two think, e.g., of $\tau^\dagger . a^\dagger . \tau^\dagger . b_1^\dagger . \tau^\dagger . \underline{0} \parallel_{\{b_1\}} \tau^\dagger . b_1^\dagger . \tau^\dagger . b_2^\dagger . \tau^\dagger . \underline{0}$):
    - If $b_1, b_2 \notin L$ then from the aforementioned hypothesis it follows that $b_1 = b_2 \triangleq b$ and hence $brs_{\rm w}(\widehat{P}) = brs_{\rm w}(P) = (brs_{\rm w}(P_1) \cap \overline{L}) \cup (brs_{\rm w}(P_2) \cap \overline{L}) \cup \emptyset = \{b\}$.
    - If $b_1, b_2 \in L$ then from $P \in \mathbb{P}$ it follows that $b_1 = b_2 \triangleq b$ and hence $brs_{\rm w}(\widehat{P}) = brs_{\rm w}(P) = \emptyset \cup \emptyset \cup (brs_{\rm w}(P_1) \cap brs_{\rm w}(P_2) \cap L) = \{b\}$.
    - If $b_1 \in L$ and $b_2 \notin L$, then from $P \in \mathbb{P}$ it follows that $brs_{\rm w}(\widehat{P}) = brs_{\rm w}(P) = \emptyset \cup (brs_{\rm w}(P_2) \cap \overline{L}) \cup \emptyset = \{b_2\}$.
    - If $b_1 \notin L$ and $b_2 \in L$, then from $P \in \mathbb{P}$ it follows that $brs_{\rm w}(\widehat{P}) = brs_{\rm w}(P) = (brs_{\rm w}(P_1) \cap \overline{L}) \cup \emptyset \cup \emptyset = \{b_1\}$. ■

Theorem 6.5. *Let $P, P' \in \mathbb{P}$, $\theta \in \Theta$, and $\bar{\theta} \in \Theta_{\rm brs}$. Then $P \xrightarrow{\theta} P'$ iff $\widehat{P} \xrightarrow{\bar{\theta}, brs_{\rm w}(P')}_{\rm brs} \widehat{P}'$ with $act(\theta) = act(\bar{\theta})$.*

Proof. We proceed by induction on the number $n \in \mathbb{N}_{\geq 1}$ of applications of operational semantic rules that are necessary to derive the considered transitions:

- If $n = 1$ then P is $a . Q$, with *initial*(Q), and $\widehat{P} = <a, \beth> . U_Q$ by Lemma 6.6(1), with $\beth = \emptyset$ and $U_Q = \widehat{Q}$ or $\beth = \{a\}$ and U_Q being obtained from $\widehat{Q}$ by adding a to the second component of each possible extended τ-prefix at the beginning of $\widehat{Q}$ depending on whether $a = \tau$ or not. According to the rules $\text{ACT}_{\rm f}$ in Table 2.1 and $\text{ACT}_{\rm brs,f}$ in Table 6.3, their only outgoing transitions are respectively $P \xrightarrow{a} a^\dagger . Q$ and $\widehat{P} \xrightarrow{a, \beth}_{\rm brs} <a^\dagger, \beth> . U_Q$, with $\beth = brs_{\rm w}(a^\dagger . Q)$ as *initial*(Q) and $<a^\dagger, \beth> . U_Q = \widehat{a^\dagger . Q}$ by Lemma 6.6(2) where – in the case that $a \neq \tau$ – there cannot be extended $\tau^\dagger$-prefixes at the beginning of $\widehat{Q}$ due to *initial*(Q).

- If $n > 1$ there are four cases:
  - Let P be $a^\dagger . Q$. If $P \xrightarrow{\cdot a\theta'} a^\dagger . Q'$ then $Q \xrightarrow{\theta'} Q'$ by rule ACT_p in Table 2.1. By the induction hypothesis this is equivalent to $\widehat{Q} \xrightarrow{\bar\theta', brs_\text{w}(Q')}_\text{brs} \widehat{Q'}$ with $act(\theta') = act(\bar\theta')$, which implies $U_Q \xrightarrow{\bar\theta', \urcorner}_\text{brs} U_{Q'}$ with $\urcorner = brs_\text{w}(Q')$ and $U_Q = \widehat{Q}$ (resp. $U_{Q'} = \widehat{Q'}$) or $\urcorner = \{a\}$ and U_Q (resp. $U_{Q'}$) being obtained from $\widehat{Q}$ (resp. $\widehat{Q'}$) by adding a to the second component of each possible extended $\tau^\dagger$- and τ-prefix at the beginning of $\widehat{Q}$ (resp. $\widehat{Q'}$) depending on whether $act(\bar\theta') \neq \tau \vee brs_\text{w}(Q') \neq \emptyset \vee a = \tau$ or not. This in turn implies $<a^\dagger, \sqsupset> . U_Q \xrightarrow{\cdot a\bar\theta', brs_\text{w}(a^\dagger . Q')}_\text{brs} <a^\dagger, \sqsupset> . U_{Q'}$ by rule $\text{ACT}_\text{brs,p}$ in Table 6.3 – as $brs_\text{w}(a^\dagger . Q') = \urcorner$ – with $\sqsupset = \emptyset$ or $\sqsupset = \{a\}$ depending on whether $a = \tau$ or not, hence $<a^\dagger, \sqsupset> . U_Q = \widehat{P}$ and $<a^\dagger, \sqsupset> . U_{Q'} = \widehat{a^\dagger . Q'}$ by Lemma 6.6(2).

    The proof starting from $\widehat{P} \xrightarrow{\cdot a\bar\theta', brs_\text{w}(a^\dagger . Q')}_\text{brs} \widehat{a^\dagger . Q'}$ is similar.
  - Let P be $Q \llcorner \rho \urcorner$. If $P \xrightarrow{\llcorner \rho\theta'} Q' \llcorner \rho \urcorner$ then $Q \xrightarrow{\theta'} Q'$ by rule REN in Table 2.1. By the induction hypothesis this is equivalent to $\widehat{Q} \xrightarrow{\bar\theta', brs_\text{w}(Q')}_\text{brs} \widehat{Q'}$ with $act(\theta') = act(\bar\theta')$, which implies $\widehat{P} \xrightarrow{\bar{\bar\theta}', brs(Q' \llcorner \rho \urcorner)}_\text{brs} \widehat{Q' \llcorner \rho \urcorner}$ with $\bar{\bar\theta}'$ obtained from $\bar\theta'$ by changing the action at its end according to ρ so that $act(\llcorner \rho\theta') = act(\bar{\bar\theta}')$, because $\widehat{P}$ (resp. $\widehat{Q' \llcorner \rho \urcorner}$) is obtained from $\widehat{Q}$ (resp. $\widehat{Q'}$) by renaming all of its actions and backward ready sets according to ρ, provided that the second component of each possible extended prefix whose first component is observable and renamed τ by ρ, as well as the second component of each possible subsequent extended prefix whose first component is named τ, is changed to the second component of the closest preceding extended prefix whose first component is an action neither named τ nor renamed τ by ρ (or $\emptyset$ if there is no such a preceding prefix), and $brs_\text{w}(Q' \llcorner \rho \urcorner) = \rho(brs_\text{w}(\rho^\dagger_\tau(Q')))$.

    The proof starting from $\widehat{P} \xrightarrow{\bar{\bar\theta}', brs_\text{w}(Q' \llcorner \rho \urcorner)}_\text{brs} \widehat{Q' \llcorner \rho \urcorner}$ is similar.
  - Let P be $P_1 + P_2$. There are two subcases:
    - If $P \xrightarrow{+\theta'} P_1' + P_2$ with $initial(P_2)$, then $P_1 \xrightarrow{\theta'} P_1'$ by rule CHO_l in Table 2.1. By the induction hypothesis this is equivalent to $\widehat{P_1} \xrightarrow{\bar\theta', brs_\text{w}(P_1')}_\text{brs} \widehat{P_1'}$ with $act(\theta') = act(\bar\theta')$, which implies $\widehat{P_1} + \widehat{P_2} \xrightarrow{+\bar\theta', brs_\text{w}(P_1' + P_2)}_\text{brs} \widehat{P_1'} + \widehat{P_2}$ by rule $\text{CHO}_\text{brs,l}$ in Table 6.3 – as $brs_\text{w}(P_1' + P_2) = brs_\text{w}(P_1')$ due to $initial(P_2)$ – with $\widehat{P_1} + \widehat{P_2} = \widehat{P}$ and $\widehat{P_1'} + \widehat{P_2} = \widehat{P_1' + P_2}$ by Lemma 6.6(3).

      The proof starting from $\widehat{P} \xrightarrow{+\bar\theta', brs_\text{w}(P_1' + P_2)}_\text{brs} \widehat{P_1' + P_2}$ is similar.
    - The subcase in which $P \xrightarrow{+\theta'} P_1 + P_2'$ with $initial(P_1)$ is like the previous one.
  - Let P be $P_1 \parallel_L P_2$. There are three subcases:
    - If $P \xrightarrow{\parallel_L \theta'} P_1' \parallel_L P_2$ with $act(\theta') \notin L$, then $P_1 \xrightarrow{\theta'} P_1'$ by rule PAR_l in Table 2.1. By the induction hypothesis this is equivalent to $\widehat{P_1} \xrightarrow{\bar\theta', brs_\text{w}(P_1')}_\text{brs} \widehat{P_1'}$ with $act(\theta') = act(\bar\theta')$. By the version of Definition 6.4 for $\ell_\text{brs,w}$ this implies that $\widehat{P}$, after a possible sequence of executed actions, has a maximal initial subprocess with a summand of the form $<act(\parallel_L \bar\theta'), brs_\text{w}(P_1' \parallel_L P_2)> . \widehat{P_1' \parallel_L P_2}$, hence $\widehat{P} \xrightarrow{\bar{\bar\theta}', brs_\text{w}(P_1' \parallel_L P_2)}_\text{brs} \widehat{P_1' \parallel_L P_2}$ for a suitable $\bar{\bar\theta}' \in \Theta_\text{brs}$ such that $act(\bar\theta') = act(\bar{\bar\theta}')$.

      The proof starting from $\widehat{P} \xrightarrow{\bar{\bar\theta}', brs_\text{w}(P_1' \parallel_L P_2)}_\text{brs} \widehat{P_1' \parallel_L P_2}$ is similar.

* The subcase in which $P \xrightarrow{\mathbb{L}_L \theta'} P_1 \parallel_L P_2'$ with $act(\theta') \notin L$ is like the previous one.
* If $P \xrightarrow{\langle \theta_1, \theta_2 \rangle_L} P_1' \parallel_L P_2'$ with $act(\theta_1) = act(\theta_2) \in L$, then $P_k \xrightarrow{\theta_k} P_k'$ for $k \in \{1,2\}$ by rule SYN in Table 2.1. By the induction hypothesis this is equivalent to $\widehat{P}_k \xrightarrow{\bar{\theta}_k, brs_{\rm w}(P_k')}_{\rm brs} \widehat{P}_k'$ with $act(\theta_k) = act(\bar{\theta}_k)$. By the version of Definition 6.4 for $\ell_{\rm brs,w}$ this implies that $\widehat{P}$, after a possible sequence of executed actions, has a maximal initial subprocess with a summand of the form $< act(\langle \bar{\theta}_1, \bar{\theta}_2 \rangle_L), brs_{\rm w}(P_1' \parallel_L P_2') > . \widehat{P_1' \parallel_L P_2'}$, hence $\widehat{P} \xrightarrow{\bar{\bar{\theta}}, brs_{\rm w}(P_1' \parallel_L P_2')}_{\rm brs} \widehat{P_1' \parallel_L P_2'}$ for a suitable $\bar{\bar{\theta}} \in \Theta_{\rm brs}$ such that $act(\bar{\theta}_k) = act(\bar{\bar{\theta}})$ for $k \in \{1,2\}$.
  The proof starting from $\widehat{P} \xrightarrow{\bar{\bar{\theta}}, brs_{\rm w}(P_1' \parallel_L P_2')}_{\rm brs} \widehat{P_1' \parallel_L P_2'}$ is similar. ∎

Corollary 6.2. *Let $P_1, P_2 \in \mathbb{P}$ and $B \in \{\text{RB}, \text{FRB:ps}\}$. Then $P_1 \approx_B P_2$ iff $\widehat{P}_1 \approx_{B:\ell_{\rm brs,w}} \widehat{P}_2$.*

Proof. The proof is divided into two parts:

- Suppose that $P_1 \approx_B P_2$ and let $\mathcal{B}$ be a $\approx_B$-bisimulation containing the pair (P_1, P_2). The result follows by proving that $\mathcal{B}' = \{(\widehat{Q}_1, \widehat{Q}_2) \mid (Q_1, Q_2) \in \mathcal{B}\}$ is a $\approx_{B:\ell_{\rm brs,w}}$-bisimulation. Let $(\widehat{Q}_1, \widehat{Q}_2) \in \mathcal{B}'$ so that $(Q_1, Q_2) \in \mathcal{B}$:
  - If $B = \text{FRB:ps}$ and $\widehat{Q}_1 \xrightarrow{\bar{\theta}_1, brs_{\rm w}(Q_1')}_{\rm brs} \widehat{Q}_1'$, then $Q_1 \xrightarrow{\theta_1} Q_1'$ with $act(\bar{\theta}_1) = act(\theta_1)$ due to Theorem 6.5. There are two cases:
    * If $act(\theta_1) = \tau$ then from $(Q_1, Q_2) \in \mathcal{B}$ it follows that there exists $Q_2 \Longrightarrow Q_2'$ such that $(Q_1', Q_2') \in \mathcal{B}$. Thus $\widehat{Q}_2 \Longrightarrow_{\rm brs} \widehat{Q}_2'$ due to Theorem 6.5 with $(Q_1', Q_2') \in \mathcal{B}$ implying $(\widehat{Q}_1', \widehat{Q}_2') \in \mathcal{B}'$.
    * If $act(\theta_1) \neq \tau$ then from $(Q_1, Q_2) \in \mathcal{B}$ it follows that there exists $Q_2 \Longrightarrow \bar{Q}_2 \xrightarrow{\theta_2} \bar{Q}_2' \Longrightarrow Q_2'$ such that $act(\theta_1) = act(\theta_2)$ and $(Q_1', Q_2') \in \mathcal{B}$. Thus $\widehat{Q}_2 \Longrightarrow_{\rm brs} \widehat{\bar{Q}}_2 \xrightarrow{\bar{\theta}_2, brs_{\rm w}(\bar{Q}_2')}_{\rm brs} \widehat{\bar{Q}_2'} \Longrightarrow_{\rm brs} \widehat{Q}_2'$ with $act(\theta_2) = act(\bar{\theta}_2)$ due to Theorem 6.5 – so $act(\bar{\theta}_1) = act(\bar{\theta}_2)$ – $brs_{\rm w}(\bar{Q}_2') = brs_{\rm w}(Q_2')$ as $\bar{Q}_2' \Longrightarrow Q_2'$, and $(Q_1', Q_2') \in \mathcal{B}$ implying $brs_{\rm w}(Q_1') = brs_{\rm w}(Q_2')$ due to Proposition 3.7(2) and $(\widehat{Q}_1', \widehat{Q}_2') \in \mathcal{B}'$.
  - If $\widehat{Q}_1' \xrightarrow{\bar{\theta}_1, brs_{\rm w}(Q_1)}_{\rm brs} \widehat{Q}_1$ the proof is like the previous one where Proposition 3.7(2) yields $brs_{\rm w}(Q_1) = brs_{\rm w}(Q_2)$.
- Suppose that $\widehat{P}_1 \approx_{B:\ell_{\rm brs,w}} \widehat{P}_2$ and let $\mathcal{B}$ be a $\approx_{B:\ell_{\rm brs,w}}$-bisimulation containing the pair $(\widehat{P}_1, \widehat{P}_2)$. The result follows by proving that $\mathcal{B}' = \{(Q_1, Q_2) \mid (\widehat{Q}_1, \widehat{Q}_2) \in \mathcal{B}\}$ is a $\approx_B$-bisimulation. Let $(Q_1, Q_2) \in \mathcal{B}'$ so that $(\widehat{Q}_1, \widehat{Q}_2) \in \mathcal{B}$:
  - If $B = \text{FRB:ps}$ and $Q_1 \xrightarrow{\theta_1} Q_1'$, then $\widehat{Q}_1 \xrightarrow{\bar{\theta}_1, brs_{\rm w}(Q_1')}_{\rm brs} \widehat{Q}_1'$ with $act(\theta_1) = act(\bar{\theta}_1)$ due to Theorem 6.5. There are two cases:
    * If $act(\bar{\theta}_1) = \tau$ then from $(\widehat{Q}_1, \widehat{Q}_2) \in \mathcal{B}$ it follows that there exists $\widehat{Q}_2 \Longrightarrow_{\rm brs} \widehat{Q}_2'$ such that $(\widehat{Q}_1', \widehat{Q}_2') \in \mathcal{B}$. Thus $Q_2 \Longrightarrow Q_2'$ due to Theorem 6.5 with $(\widehat{Q}_1', \widehat{Q}_2') \in \mathcal{B}$ implying $(Q_1', Q_2') \in \mathcal{B}'$.

* If $act(\bar{\theta}_1) \neq \tau$ then from $(\widehat{Q}_1, \widehat{Q}_2) \in \mathcal{B}$ it follows that there exists $\widehat{Q}_2 \Longrightarrow_{\mathrm{brs}} \widehat{\bar{Q}}_2 \xrightarrow{\bar{\theta}_2, brs_{\mathrm{w}}(\bar{Q}'_2)}_{\mathrm{brs}} \widehat{\bar{Q}'_2} \Longrightarrow_{\mathrm{brs}} \widehat{Q}'_2$ such that $act(\bar{\theta}_1) = act(\bar{\theta}_2)$, $brs_{\mathrm{w}}(Q'_1) = brs_{\mathrm{w}}(\bar{Q}'_2)$ – so $brs_{\mathrm{w}}(Q'_1) = brs_{\mathrm{w}}(Q'_2)$ as $\widehat{\bar{Q}'_2} \Longrightarrow_{\mathrm{brs}} \widehat{Q}'_2$ – and $(\widehat{Q}'_1, \widehat{Q}'_2) \in \mathcal{B}$. Thus $Q_2 \Longrightarrow \bar{Q}_2 \xrightarrow{\theta_2} \bar{Q}'_2 \Longrightarrow Q'_2$ with $act(\bar{\theta}_2) = act(\theta_2)$ due to Theorem 6.5 – so $act(\theta_1) = act(\theta_2)$ – and $(\widehat{Q}'_1, \widehat{Q}'_2) \in \mathcal{B}$ implying $(Q'_1, Q'_2) \in \mathcal{B}'$.

– If $Q'_1 \xrightarrow{\theta_1} Q_1$ the proof is like the previous one. ∎

Theorem 6.6. *Let* $\approx \in \{\approx_{\mathrm{RB:}\ell_{\mathrm{brs,w}}}, \approx_{\mathrm{FRB:ps:}\ell_{\mathrm{brs,w}}}\}$ *and* $P_1, P_2 \in \mathbb{P}$. *If* $\widehat{P}_1 \approx \widehat{P}_2$ *then:*

- *For all* $a \in \mathcal{A}$*:*
  - $\widehat{a \,.\, P_1} \approx \widehat{a \,.\, P_2}$ *provided that* $initial(P_1) \wedge initial(P_2)$.
  - $\widehat{a^\dagger \,.\, P_1} \approx \widehat{a^\dagger \,.\, P_2}$.
- *For all* $\rho : \mathcal{A} \to \mathcal{A}$ *such that* $\rho(\tau) = \tau$*:*
  - $\widehat{P_1 \llcorner \rho \urcorner} \approx \widehat{P_2 \llcorner \rho \urcorner}$.
- *For all* $P \in \mathbb{P}$*:*
  - $\widehat{P_1 + P} \approx \widehat{P_2 + P}$ *and* $\widehat{P + P_1} \approx \widehat{P + P_2}$ *provided that* $initial(P) \vee (initial(P_1) \wedge initial(P_2))$.
- *For all* $P \in \mathbb{P}$ *and* $L \subseteq \mathcal{A} \setminus \{\tau\}$*:*
  - $\widehat{P_1 \parallel_L P} \approx \widehat{P_2 \parallel_L P}$ *and* $\widehat{P \parallel_L P_1} \approx \widehat{P \parallel_L P_2}$ *provided that* $P_1 \parallel_L P, P_2 \parallel_L P, P \parallel_L P_1, P \parallel_L P_2 \in \mathbb{P}$.

Proof. Similar to the proof of Theorem 4.2 by exploiting Lemma 6.6. ∎

6.5 Axiomatizations of Reverse Bisimulation Congruences

The axioms via $\mathbb{P}_{\mathrm{brs}}$ for $\sim_{\mathrm{RB}}$ are presented in Section 6.5.1, while those for $\approx_{\mathrm{RB}}$ are discussed in Section 6.5.2.

6.5.1 Axiomatization of $\sim_{\mathrm{RB}}$

The set A_{R} of ℓ_{brs}-based axioms for $\sim_{\mathrm{RB}}$ is shown in Table 6.4 (remember that where-clauses ensure $\mathbb{P}$-membership). Axioms $\mathsf{A}_{\mathrm{R},1}$ to $\mathsf{A}_{\mathrm{R},4}$, already encountered in Table 6.1 without encoding, express associativity and commutativity of alternative composition as well as the application of renaming to the terminated process and executed actions.

The subsequent axioms are specific to our reversible setting. Axiom $\mathsf{A}_{\mathrm{R},5}$ establishes that the future can be completely canceled when moving only backward; note that this axiom implies $\widetilde{(a \,.\, P) \llcorner \rho \urcorner} = \widetilde{P \llcorner \rho \urcorner}$ thus making $\widetilde{(a \,.\, P) \llcorner \rho \urcorner} = \widetilde{\rho(a) \,.\, (P \llcorner \rho \urcorner)}$ unnecessary. Likewise, axiom $\mathsf{A}_{\mathrm{R},6}$ states that a previously non-selected alternative process can be discarded when moving only backward; note that this axiom subsumes both $\widetilde{P + \underline{0}} = \widetilde{P}$ and

$(\mathsf{A}_{\mathrm{R},1})$	$\widetilde{(P+Q)}+R$	$=$	$\widetilde{P+(Q+R)}$	where at least two among P, Q, R are initial
$(\mathsf{A}_{\mathrm{R},2})$	$\widetilde{P+Q}$	$=$	$\widetilde{Q+P}$	where $initial(P) \vee initial(Q)$
$(\mathsf{A}_{\mathrm{R},3})$	$\widetilde{\underline{0}\llcorner\rho\urcorner}$	$=$	$\widetilde{\underline{0}}$	
$(\mathsf{A}_{\mathrm{R},4})$	$\widetilde{(a^\dagger.P)\llcorner\rho\urcorner}$	$=$	$\rho(a)^\dagger.\widetilde{(P\llcorner\rho\urcorner)}$	
$(\mathsf{A}_{\mathrm{R},5})$	$\widetilde{a.P}$	$=$	$\widetilde{P}$	where $initial(P)$
$(\mathsf{A}_{\mathrm{R},6})$	$\widetilde{P+Q}$	$=$	$\widetilde{P}$	if $initial(Q)$
$(\mathsf{A}_{\mathrm{R},7})$	$\widetilde{P_1 \parallel_L P_2}$	$=$	$e\ell^{\varepsilon}_{\mathrm{brs,R}}(\widetilde{P_1},\widetilde{P_2},L)_{P_1 \parallel_L P_2}$	with P_k in R-nf for $k \in \{1,2\}$

Table 6.4: Axioms characterizing $\sim_{\mathrm{RB}}$ via the ℓ_{brs}-encoding into $\mathbb{P}_{\mathrm{brs}}$ processes

$\widetilde{P+P} = \widetilde{P}$, i.e., neutral element and idempotency of alternative composition, and implies $\widetilde{(P+Q)\llcorner\rho\urcorner} = \widetilde{P\llcorner\rho\urcorner}$ thus making $\widetilde{(P+Q)\llcorner\rho\urcorner} = \widetilde{(P\llcorner\rho\urcorner)+(Q\llcorner\rho\urcorner)}$ unnecessary. Axiom $\mathsf{A}_{\mathrm{R},7}$ concisely expresses via $e\ell_{\mathrm{brs,R}}$ – a variant of $e\ell_{\mathrm{brs}}$ that will be introduced shortly – the expansion laws for $\sim_{\mathrm{RB}}$ where, for $k \in \{1,2\}$, P_k is a $+$-free and renaming-free sequential process possibly featuring only executed actions (see the forthcoming Theorem 7.1).

Definition 6.5. *We say that $P \in \mathbb{P}$ is in* reverse normal form*, written* R-nf*, iff it is equal to $\underline{0}$ or $a^\dagger.P'$ where P' is in R-nf. This extends to $\mathbb{P}_{\mathrm{brs}}$ in the expected way.* ■

In order for R-nf to effectively support the proof of ground completeness of the axiomatization, we need to introduce a simplification of the ℓ_{brs}-encoding of parallel composition. For example, the ℓ_{brs}-encoding of $a^\dagger.\underline{0} \parallel_\emptyset b^\dagger.\underline{0}$ is $<a^\dagger,\{a\}>.<b^\dagger,\{a,b\}>.\underline{0} + <b,\{b\}>.<a,\{a,b\}>.\underline{0}$ under $\lVert_\emptyset a \leq_\dagger \rVert_\emptyset b$. This can be turned into R-nf by considering its subprocess $<a^\dagger,\{a\}>.<b^\dagger,\{a,b\}>.\underline{0}$, which however would not be the ℓ_{brs}-encoding of any process in $\mathbb{P}$ if $a \neq b$. When moving only backward we can adapt Definition 6.4 by letting $e\ell^{\sigma}_{\mathrm{brs,R}}(\widetilde{P_1},\widetilde{P_2},L)_E$ be equal to the only summand of $e\ell^{\sigma}_{\mathrm{brs}}(\widetilde{P_1},\widetilde{P_2},L)_E$ that contains executed actions (or $\underline{0}$ when there is no such summand), i.e.:

- $\underline{0}$ if $\widetilde{P_1}$ and $\widetilde{P_2}$ are both initial.
- $\ell_{\mathrm{brs}}(\sigma\lVert_L\theta_1)^\dagger_{upd(\ddot{E},\sigma\lVert_L\theta_1)}.e\ell^{\sigma}_{\mathrm{brs,R}}(\widetilde{P_1'},\widetilde{P_2},L)_E$ if $\widetilde{P_1}$ is not initial while $\widetilde{P_2}$ is initial, or $\widetilde{P_1}$ and $\widetilde{P_2}$ are both non-initial and $act(\theta_1) \notin L \wedge (act(\theta_2) \in L \vee \sigma\lVert_L\theta_1 \leq_\dagger \sigma\rVert_L\theta_2)$.
- $\ell_{\mathrm{brs}}(\sigma\rVert_L\theta_2)^\dagger_{upd(\ddot{E},\sigma\rVert_L\theta_2)}.e\ell^{\sigma}_{\mathrm{brs,R}}(\widetilde{P_1},\widetilde{P_2'},L)_E$ if $\widetilde{P_1}$ is initial while $\widetilde{P_2}$ is not initial, or $\widetilde{P_1}$ and $\widetilde{P_2}$ are both non-initial and $act(\theta_2) \notin L \wedge (act(\theta_1) \in L \vee \sigma\rVert_L\theta_2 \leq_\dagger \sigma\lVert_L\theta_1)$.
- $\ell_{\mathrm{brs}}(\sigma\langle\theta_1,\theta_2\rangle_L)^\dagger_{upd(\ddot{E},\sigma\langle\theta_1,\theta_2\rangle_L)}.e\ell^{\sigma}_{\mathrm{brs,R}}(\widetilde{P_1'},\widetilde{P_2'},L)_E$ if $\widetilde{P_1}$ and $\widetilde{P_2}$ are both non-initial and $act(\theta_1) = act(\theta_2) \in L$.

Let $\mathbb{P}_{\mathrm{no}\urcorner}$ be the set of renaming-free processes of $\mathbb{P}$. Moreover, let $\vdash_{\mathrm{brs}}$ be the ℓ_{brs}-version of $\vdash$ for $\mathbb{P}_{\mathrm{brs}}$, in which for every equation in the general axioms and inference rules of Section 6.1 the ℓ_{brs}-encoding of the processes on both sides is considered instead of the plain processes in $\mathbb{P}$. The following lemma, which guarantees transformability into R-nf, would not hold if "$\widetilde{Q}$ in R-nf" were replaced by "Q in R-nf". This can be seen by taking P equal to $a^\dagger.\underline{0} \parallel_\emptyset b^\dagger.\underline{0}$ with $a \neq b$, as the ℓ_{brs}-encoding of no process Q in R-nf (hence sequential) would contain in one of its extended prefixes a backward ready set like $\{a,b\}$ that is not a singleton.

Lemma 6.7. *For all (initial) $P \in \mathbb{P}$ there exists (an initial) $Q \in \mathbb{P}_{\mathrm{no}\llcorner\urcorner}$ such that $\mathsf{A}_{\mathrm{R}} \vdash_{\mathrm{brs}} \widetilde{P} = \widetilde{Q}$ with $\widetilde{Q}$ in R-nf $(= \widetilde{\underline{0}})$.*

Proof. We proceed by induction on the syntactical structure of $P \in \mathbb{P}$:

- If P is $\underline{0}$ then the result follows by taking Q equal to $\underline{0}$ due to $\mathsf{A}_{\mathrm{R}} \vdash_{\mathrm{brs}} \widetilde{\underline{0}} = \widetilde{\underline{0}}$ by reflexivity.
- If P is $a\,.\,P'$ where P' is initial, then by the induction hypothesis there exists $Q' \in \mathbb{P}_{\mathrm{no}\llcorner\urcorner}$ initial and with $\widetilde{Q'}$ in R-nf such that $\mathsf{A}_{\mathrm{R}} \vdash_{\mathrm{brs}} \widetilde{P'} = \widetilde{Q'}$. The result follows by taking Q equal to Q' due to $\mathsf{A}_{\mathrm{R}} \vdash_{\mathrm{brs}} \widetilde{a\,.\,P'} = \widetilde{a\,.\,Q'}$ by substitutivity with respect to action prefix, $\mathsf{A}_{\mathrm{R}} \vdash_{\mathrm{brs}} \widetilde{a\,.\,Q'} = \widetilde{Q'}$ by axiom $\mathsf{A}_{\mathrm{R},5}$, and transitivity.
- If P is $a^{\dagger}\,.\,P'$ then by the induction hypothesis there exists $Q' \in \mathbb{P}_{\mathrm{no}\llcorner\urcorner}$ with $\widetilde{Q'}$ in R-nf such that $\mathsf{A}_{\mathrm{R}} \vdash_{\mathrm{brs}} \widetilde{P'} = \widetilde{Q'}$. The result follows by taking Q equal to $a^{\dagger}\,.\,Q'$ – where $\widetilde{a^{\dagger}\,.\,Q'}$ is in R-nf because so is $\widetilde{Q'}$ – due to $\mathsf{A}_{\mathrm{R}} \vdash_{\mathrm{brs}} \widetilde{a^{\dagger}\,.\,P'} = \widetilde{a^{\dagger}\,.\,Q'}$ by substitutivity with respect to executed action prefix.
- If P is $P' \llcorner \rho \urcorner$ then by the induction hypothesis there exists $Q' \in \mathbb{P}_{\mathrm{no}\llcorner\urcorner}$ with $\widetilde{Q'}$ in R-nf – which is a possibly empty sequence of executed extended prefixes terminated by $\underline{0}$ – such that $\mathsf{A}_{\mathrm{R}} \vdash_{\mathrm{brs}} \widetilde{P'} = \widetilde{Q'}$, hence $\mathsf{A}_{\mathrm{R}} \vdash_{\mathrm{brs}} \widetilde{P' \llcorner \rho \urcorner} = \widetilde{Q' \llcorner \rho \urcorner}$ by substitutivity with respect to renaming, where $\widetilde{Q' \llcorner \rho \urcorner}$ is in R-nf because it is obtained from $\widetilde{Q'}$ by renaming all of its actions and backward ready sets according to ρ. The result follows by substitutivity with respect to executed action prefix and transitivity after possibly repeated applications of axiom $\mathsf{A}_{\mathrm{R},4}$ and a final application of axiom $\mathsf{A}_{\mathrm{R},3}$ to $\widetilde{Q' \llcorner \rho \urcorner}$ aimed at achieving $\mathsf{A}_{\mathrm{R}} \vdash_{\mathrm{brs}} \widetilde{P' \llcorner \rho \urcorner} = \widetilde{Q}$ with $Q \in \mathbb{P}_{\mathrm{no}\llcorner\urcorner}$ in addition to $\widetilde{Q}$ in R-nf.
- If P is $P_1 + P_2$ then by the induction hypothesis there exist $Q_1, Q_2 \in \mathbb{P}_{\mathrm{no}\llcorner\urcorner}$ with $\widetilde{Q}_1$ and $\widetilde{Q}_2$ in R-nf such that $\mathsf{A}_{\mathrm{R}} \vdash_{\mathrm{brs}} \widetilde{P}_1 = \widetilde{Q}_1$ and $\mathsf{A}_{\mathrm{R}} \vdash_{\mathrm{brs}} \widetilde{P}_2 = \widetilde{Q}_2$, hence $\mathsf{A}_{\mathrm{R}} \vdash_{\mathrm{brs}} \widetilde{P_1 + P_2} = \widetilde{Q_1 + Q_2}$ by substitutivity with respect to alternative composition. There are three cases:
  - If P_1 and P_2 are both initial, then Q_1 and Q_2 are both initial too and hence the result follows by taking Q equal to Q_1 due to $\mathsf{A}_{\mathrm{R}} \vdash_{\mathrm{brs}} \widetilde{Q_1 + Q_2} = \widetilde{Q}_1$ – by axiom $\mathsf{A}_{\mathrm{R},6}$ – and transitivity.
  - If only P_2 is initial, then only Q_2 is initial too and hence the result follows by taking Q equal to Q_1 for the same reason as the previous case.
  - If only P_1 is initial, then only Q_1 is initial too and hence the result follows by taking Q equal to Q_2 due to $\mathsf{A}_{\mathrm{R}} \vdash_{\mathrm{brs}} \widetilde{Q_1 + Q_2} = \widetilde{Q_2 + Q_1}$ by axiom $\mathsf{A}_{\mathrm{R},2}$, $\mathsf{A}_{\mathrm{R}} \vdash_{\mathrm{brs}} \widetilde{Q_2 + Q_1} = \widetilde{Q}_2$ by axiom $\mathsf{A}_{\mathrm{R},6}$, and transitivity.
- If P is $P_1 \parallel_L P_2$ then by the induction hypothesis there exist $Q_1, Q_2 \in \mathbb{P}_{\mathrm{no}\llcorner\urcorner}$ with $\widetilde{Q}_1$ and $\widetilde{Q}_2$ in R-nf such that $\mathsf{A}_{\mathrm{R}} \vdash_{\mathrm{brs}} \widetilde{P}_1 = \widetilde{Q}_1$ and $\mathsf{A}_{\mathrm{R}} \vdash_{\mathrm{brs}} \widetilde{P}_2 = \widetilde{Q}_2$, hence $\mathsf{A}_{\mathrm{R}} \vdash_{\mathrm{brs}} \widetilde{P_1 \parallel_L P_2} = \widetilde{Q_1 \parallel_L Q_2}$ by substitutivity with respect to parallel composition. As a consequence $\mathsf{A}_{\mathrm{R}} \vdash_{\mathrm{brs}} \widetilde{P_1 \parallel_L P_2} = e\ell^{\varepsilon}_{\mathrm{brs,R}}(\widetilde{Q}_1, \widetilde{Q}_2, L)_{Q_1 \parallel_L Q_2}$ by axiom $\mathsf{A}_{\mathrm{R},7}$ and transitivity. Note that $Q_1 \parallel_L Q_2 \in \mathbb{P}_{\mathrm{no}\llcorner\urcorner}$ because so are Q_1 and Q_2 and $\widetilde{Q_1 \parallel_L Q_2}$, i.e., $e\ell^{\varepsilon}_{\mathrm{brs,R}}(\widetilde{Q}_1, \widetilde{Q}_2, L)_{Q_1 \parallel_L Q_2}$, is in R-nf by the simplified version of Definition 6.4. ∎

Theorem 6.7. *Let $P_1, P_2 \in \mathbb{P}$. Then $\widetilde{P}_1 \sim_{\mathrm{RB}:\ell_{\mathrm{brs}}} \widetilde{P}_2$ iff $\mathsf{A}_{\mathrm{R}} \vdash_{\mathrm{brs}} \widetilde{P}_1 = \widetilde{P}_2$.*

Proof. Soundness, i.e., $\mathsf{A}_{\mathrm{R}} \vdash_{\mathrm{brs}} \widetilde{P}_1 = \widetilde{P}_2 \implies \widetilde{P}_1 \sim_{\mathrm{RB}:\ell_{\mathrm{brs}}} \widetilde{P}_2$, is a straightforward consequence of the axioms and inference rules behind $\vdash_{\mathrm{brs}}$ (see Section 6.1 where for each equation side its ℓ_{brs}-encoding is considered) together with $\sim_{\mathrm{RB}:\ell_{\mathrm{brs}}}$ being an equivalence relation and a congruence (see Theorem 6.4), plus the fact that the lefthand side process of each additional axiom in Table 6.4 is $\sim_{\mathrm{RB}:\ell_{\mathrm{brs}}}$-equivalent to the righthand side process of the same axiom. Let us address ground completeness, i.e., $\widetilde{P}_1 \sim_{\mathrm{RB}:\ell_{\mathrm{brs}}} \widetilde{P}_2 \implies \mathsf{A}_{\mathrm{R}} \vdash_{\mathrm{brs}} \widetilde{P}_1 = \widetilde{P}_2$. We suppose that $\widetilde{P}_1$ and $\widetilde{P}_2$ are both in R-nf and proceed by induction on the syntactical structure of $\widetilde{P}_1$:

- If $\widetilde{P}_1$ is $\widetilde{\underline{0}}$ then from $\widetilde{P}_1 \sim_{\mathrm{RB}:\ell_{\mathrm{brs}}} \widetilde{P}_2$ and $\widetilde{P}_2$ in R-nf we derive that $\widetilde{P}_2$ can only be $\widetilde{\underline{0}}$, from which the result follows by reflexivity.
- If $\widetilde{P}_1$ is $\widetilde{a_1^\dagger.\, P_1'}$ then from $\widetilde{P}_1 \sim_{\mathrm{RB}:\ell_{\mathrm{brs}}} \widetilde{P}_2$ and $\widetilde{P}_2$ in R-nf we derive that $\widetilde{P}_2$ can only be $\widetilde{a_2^\dagger.\, P_2'}$. We recall that $\widetilde{P}_1'$ and $\widetilde{P}_1'$ are both in R-nf.
  From $\widetilde{P}_1 \sim_{\mathrm{RB}:\ell_{\mathrm{brs}}} \widetilde{P}_2$ and $\widetilde{P}_1$ and $\widetilde{P}_2$ both in R-nf and different from $\widetilde{\underline{0}}$ it follows that $\widetilde{P}_1$ and $\widetilde{P}_2$ consist of the same sequence of executed actions, hence in particular $a_1 = a_2$ and $\widetilde{P_1'} \sim_{\mathrm{RB}:\ell_{\mathrm{brs}}} \widetilde{P_2'}$. From the induction hypothesis we obtain $\mathsf{A}_{\mathrm{R}} \vdash_{\mathrm{brs}} \widetilde{P_1'} = \widetilde{P_2'}$, hence $\mathsf{A}_{\mathrm{R}} \vdash_{\mathrm{brs}} \widetilde{a_1^\dagger.\, P_1'} = \widetilde{a_2^\dagger.\, P_2'}$ by substitutivity with respect to executed action prefix.

If $\widetilde{P}_1$ and $\widetilde{P}_2$ are not both in R-nf, thanks to Lemma 6.7 we can find $Q_1, Q_2 \in \mathbb{P}_{\mathrm{no}\lrcorner}$, each of which is initial iff so is its corresponding process, with $\widetilde{Q}_1$ and $\widetilde{Q}_2$ in R-nf such that $\mathsf{A}_{\mathrm{R}} \vdash_{\mathrm{brs}} \widetilde{P}_1 = \widetilde{Q}_1$ and $\mathsf{A}_{\mathrm{R}} \vdash_{\mathrm{brs}} \widetilde{P}_2 = \widetilde{Q}_2$, hence $\mathsf{A}_{\mathrm{R}} \vdash_{\mathrm{brs}} \widetilde{Q}_2 = \widetilde{P}_2$ by symmetry. Due to soundness, we get $\widetilde{P}_1 \sim_{\mathrm{RB}:\ell_{\mathrm{brs}}} \widetilde{Q}_1$, hence $\widetilde{Q}_1 \sim_{\mathrm{RB}:\ell_{\mathrm{brs}}} \widetilde{P}_1$ as $\sim_{\mathrm{RB}:\ell_{\mathrm{brs}}}$ is symmetric, and $\widetilde{P}_2 \sim_{\mathrm{RB}:\ell_{\mathrm{brs}}} \widetilde{Q}_2$. Since $\widetilde{P}_1 \sim_{\mathrm{RB}:\ell_{\mathrm{brs}}} \widetilde{P}_2$, we also get $\widetilde{Q}_1 \sim_{\mathrm{RB}:\ell_{\mathrm{brs}}} \widetilde{Q}_2$ as $\sim_{\mathrm{RB}:\ell_{\mathrm{brs}}}$ is transitive. By virtue of what has been shown above, from $\widetilde{Q}_1 \sim_{\mathrm{RB}:\ell_{\mathrm{brs}}} \widetilde{Q}_2$ with $\widetilde{Q}_1$ and $\widetilde{Q}_2$ in R-nf it follows that $\mathsf{A}_{\mathrm{R}} \vdash_{\mathrm{brs}} \widetilde{Q}_1 = \widetilde{Q}_2$ and hence $\mathsf{A}_{\mathrm{R}} \vdash_{\mathrm{brs}} \widetilde{P}_1 = \widetilde{P}_2$ by transitivity. ∎

Corollary 6.3. *Let $P_1, P_2 \in \mathbb{P}$. Then $P_1 \sim_{\mathrm{RB}} P_2$ iff $\mathsf{A}_{\mathrm{R}} \vdash_{\mathrm{brs}} \widetilde{P}_1 = \widetilde{P}_2$.*

Proof. It stems from $P_1 \sim_{\mathrm{RB}} P_2$ iff $\widetilde{P}_1 \sim_{\mathrm{RB}:\ell_{\mathrm{brs}}} \widetilde{P}_2$ as established by Corollary 6.1. ∎

6.5.2 Axiomatization of $\approx_{\mathrm{RB}}$

The set $\mathsf{A}_{\mathrm{R}}^{\tau}$ of $\ell_{\mathrm{brs,w}}$-based axioms for $\approx_{\mathrm{RB}}$ is shown in Table 6.5. The first seven axioms have the same shape as those in Table 6.4, with the difference that the $\ell_{\mathrm{brs,w}}$-encoding is considered in lieu of the one based on ℓ_{brs} (again in the simplified form for parallel composition motivated after Definition 6.5).

The additional axiom, i.e., axiom $\mathsf{A}_{\mathrm{R},8}^{\tau}$, which is specific to our reversible setting, expresses the abstraction capability of $\approx_{\mathrm{RB}}$. It is worth noting that it represents the reverse counterpart of the only τ-law that, over forward-only processes, is valid for weak bisimilarity but not for weak bisimulation congruence [112].

Let $\vdash_{\mathrm{brs,w}}$ be the $\ell_{\mathrm{brs,w}}$-version of $\vdash$ for $\mathbb{P}_{\mathrm{brs}}$, in which for every equation in the general axioms and inference rules of Section 6.1 the $\ell_{\mathrm{brs,w}}$-encoding of the processes on both sides is considered instead of the plain processes in $\mathbb{P}$. We point out that transformability into R-nf is enough to prove ground completeness, i.e., resorting to saturation like in Section 6.3.2 is not needed, because no choice occurs when moving only backward.

$(\mathsf{A}^\tau_{\mathrm{R},1})$	$\widehat{(P + Q)} + R$	$=$	$P + \widehat{(Q + R)}$	where at least two among P, Q, R are initial
$(\mathsf{A}^\tau_{\mathrm{R},2})$	$\widehat{P + Q}$	$=$	$\widehat{Q + P}$	where $initial(P) \vee initial(Q)$
$(\mathsf{A}^\tau_{\mathrm{R},3})$	$\widehat{\underline{0}\llcorner\rho\urcorner}$	$=$	$\widehat{\underline{0}}$	
$(\mathsf{A}^\tau_{\mathrm{R},4})$	$\widehat{(a^\dagger.P)\llcorner\rho\urcorner}$	$=$	$\rho(a)^\dagger.\widehat{(P\llcorner\rho\urcorner)}$	
$(\mathsf{A}^\tau_{\mathrm{R},5})$	$\widehat{a.P}$	$=$	$\widehat{P}$	where $initial(P)$
$(\mathsf{A}^\tau_{\mathrm{R},6})$	$\widehat{P + Q}$	$=$	$\widehat{P}$	if $initial(Q)$
$(\mathsf{A}^\tau_{\mathrm{R},7})$	$\widehat{P_1 \parallel_L P_2}$	$=$	$e\ell^{\varepsilon}_{\mathrm{brs,w,R}}(\widehat{P}_1, \widehat{P}_2, L)_{P_1 \parallel_L P_2}$	with P_k in R-nf for $k \in \{1,2\}$
$(\mathsf{A}^\tau_{\mathrm{R},8})$	$\widehat{\tau^\dagger.P}$	$=$	$\widehat{P}$	

Table 6.5: Axioms characterizing $\approx_{\mathrm{RB}}$ via the $\ell_{\mathrm{brs,w}}$-encoding into $\mathbb{P}_{\mathrm{brs}}$ processes

Lemma 6.8. *For all (initial) $P \in \mathbb{P}$ there exists (an initial) $Q \in \mathbb{P}_{\mathrm{no}\urcorner}$ such that $\mathsf{A}^\tau_{\mathrm{R}} \vdash_{\mathrm{brs,w}} \widehat{P} = \widehat{Q}$ with $\widehat{Q}$ in R-nf ($= \widehat{\underline{0}}$).*

Proof. Since in the considered normal form τ-actions do not play a role different from the one of observable actions, we proceed like in the proof of Lemma 6.7 apart from the renaming case in which, when obtaining $\widehat{Q'\llcorner\rho\urcorner}$ from $\widehat{Q'}$ by renaming all of its actions and backward ready sets according to ρ, the second component of each possible extended prefix whose first component is observable and renamed τ by ρ, as well as the second component of each possible subsequent extended prefix whose first component is named τ, is changed to the second component of the closest preceding extended prefix whose first component is an action neither named τ nor renamed τ by ρ (or $\emptyset$ if there is no such a preceding prefix). ∎

Theorem 6.8. *Let $P_1, P_2 \in \mathbb{P}$. Then $\widehat{P}_1 \approx_{\mathrm{RB}:\ell_{\mathrm{brs,w}}} \widehat{P}_2$ iff $\mathsf{A}^\tau_{\mathrm{R}} \vdash_{\mathrm{brs,w}} \widehat{P}_1 = \widehat{P}_2$.*

Proof. Soundness, i.e., $\mathsf{A}^\tau_{\mathrm{R}} \vdash_{\mathrm{brs,w}} \widehat{P}_1 = \widehat{P}_2 \implies \widehat{P}_1 \approx_{\mathrm{RB}:\ell_{\mathrm{brs,w}}} \widehat{P}_2$, is a straightforward consequence of the axioms and inference rules behind $\vdash_{\mathrm{brs,w}}$ (see Section 6.1 where for each equation side its $\ell_{\mathrm{brs,w}}$-encoding is considered) together with $\approx_{\mathrm{RB}:\ell_{\mathrm{brs,w}}}$ being an equivalence relation and a congruence (see Theorem 6.6), plus the fact that the lefthand side process of each additional axiom in Table 6.5 is $\approx_{\mathrm{RB}:\ell_{\mathrm{brs,w}}}$-equivalent to the righthand side process of the same axiom.
Let us address ground completeness, i.e., $\widehat{P}_1 \approx_{\mathrm{RB}:\ell_{\mathrm{brs,w}}} \widehat{P}_2 \implies \mathsf{A}^\tau_{\mathrm{R}} \vdash_{\mathrm{brs,w}} \widehat{P}_1 = \widehat{P}_2$. We suppose that $\widehat{P}_1$ and $\widehat{P}_2$ are both in R-nf. Given that we cannot proceed by induction on the syntactical structure of $\widehat{P}_1$ or $size(\widehat{P}_1)$ alone because, in the case that $\widehat{P}_1$ is $\widehat{\underline{0}}$ or equivalently $size(\widehat{P}_1) = 0$, from $\widehat{P}_1 \approx_{\mathrm{RB}:\ell_{\mathrm{brs,w}}} \widehat{P}_2$ and $\widehat{P}_1$ and $\widehat{P}_2$ in R-nf we cannot conclude that $\widehat{P}_2$ is $\widehat{\underline{0}}$ or equivalently $size(\widehat{P}_2) = 0$ too, we proceed by induction on $k = size(\widehat{P}_1) + size(\widehat{P}_2)$:

- If $k = 0$ then from $\widehat{P}_1 \approx_{\mathrm{RB}:\ell_{\mathrm{brs,w}}} \widehat{P}_2$ and $\widehat{P}_1$ and $\widehat{P}_2$ in R-nf we derive that both $\widehat{P}_1$ and $\widehat{P}_2$ can only be $\widehat{\underline{0}}$, from which the result follows by reflexivity.
- If $k > 0$ there are three cases:
  - If $\widehat{P}_1$ is $\widehat{a_1^\dagger.P_1'}$ and $\widehat{P}_2$ is $\widehat{\underline{0}}$, then $a_1 = \tau$ and $\widehat{P}_1' \approx_{\mathrm{RB}:\ell_{\mathrm{brs,w}}} \widehat{P}_2$ otherwise $\widehat{P}_1 \approx_{\mathrm{RB}:\ell_{\mathrm{brs,w}}} \widehat{P}_2$ could not hold. From the induction hypothesis we obtain $\mathsf{A}^\tau_{\mathrm{RB}} \vdash_{\mathrm{brs,w}} \widehat{P}_1' = \widehat{P}_2$, hence $\mathsf{A}^\tau_{\mathrm{RB}} \vdash_{\mathrm{brs,w}} \widehat{a_1^\dagger.P_1'} = \widehat{P}_2$ due to

$\mathsf{A}^{\tau}_{\mathrm{RB}} \vdash_{\mathrm{brs,w}} \widehat{a_1^\dagger \,.\, P_1'} = \widehat{a_1^\dagger \,.\, P_2}$ by substitutivity with respect to executed action prefix, $\mathsf{A}^{\tau}_{\mathrm{RB}} \vdash_{\mathrm{brs,w}} \widehat{a_1^\dagger \,.\, P_2} = \widehat{P}_2$ by axiom $\mathsf{A}^{\tau}_{\mathrm{R},8}$, and transitivity.

- If $\widehat{P}_1$ is $\widehat{\underline{0}}$ and $\widehat{P}_2$ is $\widehat{a_2^\dagger \,.\, P_2'}$, then we proceed like in the previous case.
- If $\widehat{P}_1$ is $\widehat{a_1^\dagger \,.\, P_1'}$ and $\widehat{P}_2$ is $\widehat{a_2^\dagger \,.\, P_2'}$, there are three subcases:
  - If $a_1 \neq \tau \neq a_2$ then $a_1 = a_2$ and $\widehat{P}_1' \approx_{\mathrm{RB}:\ell_{\mathrm{brs,w}}} \widehat{P}_2'$ otherwise $\widehat{P}_1 \approx_{\mathrm{RB}:\ell_{\mathrm{brs,w}}} \widehat{P}_2$ could not hold. From the induction hypothesis we obtain $\mathsf{A}^{\tau}_{\mathrm{RB}} \vdash_{\mathrm{brs,w}} \widehat{P}_1' = \widehat{P}_2'$, hence $\mathsf{A}^{\tau}_{\mathrm{RB}} \vdash_{\mathrm{brs,w}} \widehat{a_1^\dagger \,.\, P_1'} = \widehat{a_2^\dagger \,.\, P_2'}$ by substitutivity with respect to executed action prefix.
  - If $a_1 = \tau$ then $\mathsf{A}^{\tau}_{\mathrm{RB}} \vdash_{\mathrm{brs,w}} \widehat{a_1^\dagger \,.\, P_1'} = \widehat{P}_1'$ by axiom $\mathsf{A}^{\tau}_{\mathrm{R},8}$, hence $\widehat{a_1^\dagger \,.\, P_1'} \approx_{\mathrm{RB}:\ell_{\mathrm{brs,w}}} \widehat{P}_1'$ by soundness, which implies $\widehat{P}_1' \approx_{\mathrm{RB}:\ell_{\mathrm{brs,w}}} \widehat{a_1^\dagger \,.\, P_1'}$ as $\approx_{\mathrm{RB}:\ell_{\mathrm{brs,w}}}$ is symmetric and then $\widehat{P}_1' \approx_{\mathrm{RB}:\ell_{\mathrm{brs,w}}} \widehat{a_2^\dagger . P_2'}$ as $\widehat{a_1^\dagger \,.\, P_1'} \approx_{\mathrm{RB}:\ell_{\mathrm{brs,w}}} \widehat{a_2^\dagger . P_2'}$ and $\approx_{\mathrm{RB}:\ell_{\mathrm{brs,w}}}$ is transitive. From the induction hypothesis we obtain $\mathsf{A}^{\tau}_{\mathrm{RB}} \vdash_{\mathrm{brs,w}} \widehat{P}_1' = \widehat{a_2^\dagger \,.\, P_2'}$, hence $\mathsf{A}^{\tau}_{\mathrm{RB}} \vdash_{\mathrm{brs,w}} \widehat{a_1^\dagger \,.\, P_1'} = \widehat{a_2^\dagger \,.\, P_2'}$ due to $\mathsf{A}^{\tau}_{\mathrm{RB}} \vdash_{\mathrm{brs,w}} \widehat{a_1^\dagger \,.\, P_1'} = \widehat{a_1^\dagger \,.\, a_2^\dagger \,.\, P_2'}$ by substitutivity with respect to executed action prefix, $\mathsf{A}^{\tau}_{\mathrm{RB}} \vdash_{\mathrm{brs,w}} \widehat{a_1^\dagger \,.\, a_2^\dagger \,.\, P_2'} = \widehat{a_2^\dagger \,.\, P_2'}$ by axiom $\mathsf{A}^{\tau}_{\mathrm{R},8}$, and transitivity.
  - If $a_2 = \tau$ then we proceed like in the previous subcase.

If $\widehat{P}_1$ and $\widehat{P}_2$ are not both in R-nf, thanks to Lemma 6.8 we can find $Q_1, Q_2 \in \mathbb{P}_{\mathrm{no}\Box}$, each of which is initial iff so is its corresponding process, with $\widehat{Q}_1$ and $\widehat{Q}_2$ in R-nf such that $\mathsf{A}^{\tau}_{\mathrm{R}} \vdash_{\mathrm{brs,w}} \widehat{P}_1 = \widehat{Q}_1$ and $\mathsf{A}^{\tau}_{\mathrm{R}} \vdash_{\mathrm{brs,w}} \widehat{P}_2 = \widehat{Q}_2$, hence $\mathsf{A}^{\tau}_{\mathrm{R}} \vdash_{\mathrm{brs,w}} \widehat{Q}_2 = \widehat{P}_2$ by symmetry. Due to soundness, we get $\widehat{P}_1 \approx_{\mathrm{RB}:\ell_{\mathrm{brs,w}}} \widehat{Q}_1$, hence $\widehat{Q}_1 \approx_{\mathrm{RB}:\ell_{\mathrm{brs,w}}} \widehat{P}_1$ as $\approx_{\mathrm{RB}:\ell_{\mathrm{brs,w}}}$ is symmetric, and $\widehat{P}_2 \approx_{\mathrm{RB}:\ell_{\mathrm{brs,w}}} \widehat{Q}_2$. Since $\widehat{P}_1 \approx_{\mathrm{RB}:\ell_{\mathrm{brs,w}}} \widehat{P}_2$, we also get $\widehat{Q}_1 \approx_{\mathrm{RB}:\ell_{\mathrm{brs,w}}} \widehat{Q}_2$ as $\approx_{\mathrm{RB}:\ell_{\mathrm{brs,w}}}$ is transitive. By virtue of what has been shown above, from $\widehat{Q}_1 \approx_{\mathrm{RB}:\ell_{\mathrm{brs,w}}} \widehat{Q}_2$ with $\widehat{Q}_1$ and $\widehat{Q}_2$ in R-nf it follows that $\mathsf{A}^{\tau}_{\mathrm{R}} \vdash_{\mathrm{brs,w}} \widehat{Q}_1 = \widehat{Q}_2$ and hence $\mathsf{A}_{\mathrm{R}} \vdash_{\mathrm{brs,w}} \widehat{P}_1 = \widehat{P}_2$ by transitivity. ∎

Corollary 6.4. *Let $P_1, P_2 \in \mathbb{P}$. Then $P_1 \approx_{\mathrm{RB}} P_2$ iff $\mathsf{A}^{\tau}_{\mathrm{R}} \vdash_{\mathrm{brs,w}} \widehat{P}_1 = \widehat{P}_2$.*

Proof. It stems from $P_1 \approx_{\mathrm{RB}} P_2$ iff $\widehat{P}_1 \approx_{\mathrm{RB}:\ell_{\mathrm{brs,w}}} \widehat{P}_2$ as established by Corollary 6.2. ∎

6.6 Axiomatizations of Forward-Reverse Bisimulation Congruences

The axioms via $\mathbb{P}_{\mathrm{brs}}$ for $\sim_{\mathrm{FRB}}$ are presented in Section 6.6.1, while those for $\approx_{\mathrm{FRB:ps}}$ are discussed in Section 6.6.2.

6.6.1 Axiomatization of $\sim_{\mathrm{FRB}}$

The set A_{FR} of ℓ_{brs}-based axioms for $\sim_{\mathrm{FRB}}$ is shown in Table 6.6. Axioms $\mathsf{A}_{\mathrm{FR},1}$ to $\mathsf{A}_{\mathrm{FR},3}$ and axioms $\mathsf{A}_{\mathrm{FR},5}$ to $\mathsf{A}_{\mathrm{FR},8}$, already encountered in Table 6.1 without encoding, express associativity, commutativity, and neutral element of alternative composition as well as the application of renaming and its distributivity with respect to alternative composition.

$(\mathsf{A}_{\mathrm{FR},1})$	$\widetilde{(P + Q)} + R$	$=$	$\widetilde{P + (Q + R)}$	where at least two among P, Q, R are initial
$(\mathsf{A}_{\mathrm{FR},2})$	$\widetilde{P + Q}$	$=$	$\widetilde{Q + P}$	where $\mathit{initial}(P) \vee \mathit{initial}(Q)$
$(\mathsf{A}_{\mathrm{FR},3})$	$\widetilde{P + \underline{0}}$	$=$	$\widetilde{P}$	
$(\mathsf{A}_{\mathrm{FR},4})$	$\widetilde{P + Q}$	$=$	$\widetilde{P}$	if $\mathit{initial}(Q) \wedge \mathit{to\_initial}(P) = Q$
$(\mathsf{A}_{\mathrm{FR},5})$	$\widetilde{\underline{0} \llcorner \rho^{\urcorner}}$	$=$	$\widetilde{\underline{0}}$	
$(\mathsf{A}_{\mathrm{FR},6})$	$\widetilde{(a \,.\, P) \llcorner \rho^{\urcorner}}$	$=$	$\widetilde{\rho(a) \,.\, (P \llcorner \rho^{\urcorner})}$	where $\mathit{initial}(P)$
$(\mathsf{A}_{\mathrm{FR},7})$	$\widetilde{(a^{\dagger} \,.\, P) \llcorner \rho^{\urcorner}}$	$=$	$\widetilde{\rho(a)^{\dagger} \,.\, (P \llcorner \rho^{\urcorner})}$	
$(\mathsf{A}_{\mathrm{FR},8})$	$\widetilde{(P + Q) \llcorner \rho^{\urcorner}}$	$=$	$\widetilde{(P \llcorner \rho^{\urcorner}) + (Q \llcorner \rho^{\urcorner})}$	where $\mathit{initial}(P) \vee \mathit{initial}(Q)$
$(\mathsf{A}_{\mathrm{FR},9})$	$\widetilde{P_1 \parallel_L P_2}$	$=$	$e\ell^{\varepsilon}_{\mathrm{brs}}(\widetilde{P}_1, \widetilde{P}_2, L)_{P_1 \parallel_L P_2}$	with P_k in FR-nf for $k \in \{1, 2\}$

Table 6.6: Axioms characterizing $\sim_{\mathrm{FRB}}$ via the ℓ_{brs}-encoding into $\mathbb{P}_{\mathrm{brs}}$ processes

The other axioms are specific to our reversible setting. Axiom $\mathsf{A}_{\mathrm{FR},4}$ is an extended variant of idempotency appeared for the first time in [106] – with P and Q coinciding like in axiom $\mathsf{A}_{\mathrm{F},4}$ of Table 6.1 when they are both initial – where function *to_initial* (see page 26) brings a process back to its initial version by removing † from all executed actions. Note that, unlike Tables 6.1 and 6.4, there are no axioms allowing to abstract from the past (i.e., executed actions), the future (i.e., unexecuted actions), or previously non-selected alternative processes. Axiom $\mathsf{A}_{\mathrm{FR},9}$ concisely expresses via $e\ell_{\mathrm{brs}}$ the expansion laws for $\sim_{\mathrm{FRB}}$ where, for $k \in \{1, 2\}$, P_k is the renaming-free sequential process $[a_k^{\dagger} \,.\, P'_k +] \sum_{i \in I_k} a_{k,i} \,.\, P_{k,i}$.

Definition 6.6. *We say that $P \in \mathbb{P}$ is in* forward-reverse normal form, *written* FR-nf, *iff it is equal to $[a^{\dagger} \,.\, P' +] \sum_{i \in I} a_i \,.\, P_i$ where $a^{\dagger} \,.\, P'$ is optional, P' is in FR-nf, I is a finite index set (with the summation being $\underline{0}$ – or disappearing in the presence of $a^{\dagger} \,.\, P'$ – when $I = \emptyset$), and each P_i is initial and in FR-nf. This extends to $\mathbb{P}_{\mathrm{brs}}$ in the expected way.* ■

Lemma 6.9. *For all (initial) $P \in \mathbb{P}$ there exists (an initial) $Q \in \mathbb{P}_{\mathrm{no}\llcorner}$ such that $\mathsf{A}_{\mathrm{FR}} \vdash_{\mathrm{brs}} \widetilde{P} = \widetilde{Q}$ with $\widetilde{Q}$ in FR-nf.*

Proof. We proceed by induction on the syntactical structure of $P \in \mathbb{P}$:

- If P is $\underline{0}$ then the result follows by taking Q equal to $\underline{0}$ due to $\mathsf{A}_{\mathrm{FR}} \vdash_{\mathrm{brs}} \widetilde{\underline{0}} = \widetilde{\underline{0}}$ by reflexivity.
- If P is $a \,.\, P'$ where P' is initial, then by the induction hypothesis there exists $Q' \in \mathbb{P}_{\mathrm{no}\llcorner}$ initial and with $\widetilde{Q}'$ in FR-nf such that $\mathsf{A}_{\mathrm{FR}} \vdash_{\mathrm{brs}} \widetilde{P'} = \widetilde{Q}'$. The result follows by taking Q equal to $a \,.\, Q'$ – which is initial because so is Q' and such that $\widetilde{a \,.\, Q'}$ is in FR-nf because so is the initial $\widetilde{Q}'$ – due to $\mathsf{A}_{\mathrm{FR}} \vdash_{\mathrm{brs}} \widetilde{a \,.\, P'} = \widetilde{a \,.\, Q'}$ by substitutivity with respect to action prefix.
- If P is $a^{\dagger} \,.\, P'$ then by the induction hypothesis there exists $Q' \in \mathbb{P}_{\mathrm{no}\llcorner}$ with $\widetilde{Q}'$ in FR-nf such that $\mathsf{A}_{\mathrm{FR}} \vdash_{\mathrm{brs}} \widetilde{P'} = \widetilde{Q}'$. The result follows by taking Q equal to $a^{\dagger} \,.\, Q'$ – where $\widetilde{a^{\dagger} \,.\, Q'}$ is in FR-nf because so is $\widetilde{Q}'$ – due to $\mathsf{A}_{\mathrm{FR}} \vdash_{\mathrm{brs}} \widetilde{a^{\dagger} \,.\, P'} = \widetilde{a^{\dagger} \,.\, Q'}$ by substitutivity with respect to executed action prefix.
- If P is $P' \llcorner \rho^{\urcorner}$ then by the induction hypothesis there exists $Q' \in \mathbb{P}_{\mathrm{no}\llcorner}$ with $\widetilde{Q}'$ in FR-nf – say $[<a^{\dagger}, \{a\}> \,.\, U +] \sum_{i \in I} <a_i, \{a_i\}> \,.\, U_i$ – such that $\mathsf{A}_{\mathrm{FR}} \vdash_{\mathrm{brs}} \widetilde{P'} = \widetilde{Q}'$, hence $\mathsf{A}_{\mathrm{FR}} \vdash_{\mathrm{brs}} \widetilde{P' \llcorner \rho^{\urcorner}} = \widetilde{Q' \llcorner \rho^{\urcorner}}$ by

substitutivity with respect to renaming, where $\widetilde{Q' \llcorner \rho \urcorner}$ is in FR-nf because it is obtained from $\widetilde{Q'}$ by renaming all of its actions and backward ready sets according to ρ. The result follows by substitutivity with respect to action prefix and alternative composition as well as transitivity after possibly repeated applications of axioms $\mathsf{A}_{\mathrm{FR},5}$ to $\mathsf{A}_{\mathrm{FR},8}$ to $\widetilde{Q' \llcorner \rho \urcorner}$ aimed at achieving $\mathsf{A}_{\mathrm{FR}} \vdash_{\mathrm{brs}} \widetilde{P' \llcorner \rho \urcorner} = \widetilde{Q}$ with $Q \in \mathbb{P}_{\mathrm{no}\llcorner\urcorner}$ in addition to $\widetilde{Q}$ in FR-nf.

- If P is $P_1 + P_2$ then by the induction hypothesis there exist $Q_1, Q_2 \in \mathbb{P}_{\mathrm{no}\llcorner\urcorner}$ with $\widetilde{Q}_1$ and $\widetilde{Q}_2$ in FR-nf such that $\mathsf{A}_{\mathrm{FR}} \vdash_{\mathrm{brs}} \widetilde{P}_1 = \widetilde{Q}_1$ and $\mathsf{A}_{\mathrm{FR}} \vdash_{\mathrm{brs}} \widetilde{P}_2 = \widetilde{Q}_2$, hence $\mathsf{A}_{\mathrm{FR}} \vdash_{\mathrm{brs}} \widetilde{P_1 + P_2} = \widetilde{Q_1 + Q_2}$ by substitutivity with respect to alternative composition. There are three cases:

  - If P_1 and P_2 are both initial, then Q_1 and Q_2 are both initial too and hence the result follows by taking Q equal to $Q_1 + Q_2$ – which is in $\mathbb{P}_{\mathrm{no}\llcorner\urcorner}$ because so are Q_1 and Q_2 – up to an application of axiom $\mathsf{A}_{\mathrm{FR},3}$ in the case that $\widetilde{Q_1 + Q_2}$ is not in FR-nf because Q_1 and Q_2 are not different from $\underline{0}$ (possibly preceded by an application of axiom $\mathsf{A}_{\mathrm{FR},2}$ to move the $\underline{0}$ subprocess to the right of $+$) and transitivity.
  - If only P_2 is initial, then only Q_2 is initial too and hence the result follows by taking Q equal to $Q_1 + Q_2$ – which is in $\mathbb{P}_{\mathrm{no}\llcorner\urcorner}$ because so are Q_1 and Q_2 – up to an application of axiom $\mathsf{A}_{\mathrm{FR},3}$ in the case that $\widetilde{Q_1 + Q_2}$ is not in FR-nf (because Q_2 is not different from $\underline{0}$) and transitivity.
  - If only P_1 is initial, then only Q_1 is initial too and hence the result follows by taking Q equal to $Q_2 + Q_1$ – which is in $\mathbb{P}_{\mathrm{no}\llcorner\urcorner}$ because so are Q_2 and Q_1 – due to $\mathsf{A}_{\mathrm{FR}} \vdash_{\mathrm{brs}} \widetilde{Q_1 + Q_2} = \widetilde{Q_2 + Q_1}$ – by axiom $\mathsf{A}_{\mathrm{FR},2}$ – and transitivity, up to an application of axiom $\mathsf{A}_{\mathrm{FR},3}$ in the case that $Q_2 + Q_1$ is not in FR-nf (because Q_1 is not different from $\underline{0}$) and transitivity.

- If P is $P_1 \parallel_L P_2$ then by the induction hypothesis there exist $Q_1, Q_2 \in \mathbb{P}_{\mathrm{no}\llcorner\urcorner}$ with $\widetilde{Q}_1$ and $\widetilde{Q}_2$ in FR-nf such that $\mathsf{A}_{\mathrm{FR}} \vdash_{\mathrm{brs}} \widetilde{P}_1 = \widetilde{Q}_1$ and $\mathsf{A}_{\mathrm{FR}} \vdash_{\mathrm{brs}} \widetilde{P}_2 = \widetilde{Q}_2$, hence $\mathsf{A}_{\mathrm{FR}} \vdash_{\mathrm{brs}} \widetilde{P_1 \parallel_L P_2} = \widetilde{Q_1 \parallel_L Q_2}$ by substitutivity with respect to parallel composition. As a consequence $\mathsf{A}_{\mathrm{FR}} \vdash_{\mathrm{brs}} \widetilde{P_1 \parallel_L P_2} = e\ell^{\varepsilon}_{\mathrm{brs}}(\widetilde{Q}_1, \widetilde{Q}_2, L)_{Q_1 \parallel_L Q_2}$ by axiom $\mathsf{A}_{\mathrm{FR},9}$ and transitivity. Note that $Q_1 \parallel_L Q_2 \in \mathbb{P}_{\mathrm{no}\llcorner\urcorner}$ because so are Q_1 and Q_2 and $\widetilde{Q_1 \parallel_L Q_2}$, i.e., $e\ell^{\varepsilon}_{\mathrm{brs}}(\widetilde{Q}_1, \widetilde{Q}_2, L)_{Q_1 \parallel_L Q_2}$, is in FR-nf by Definition 6.4. ∎

Theorem 6.9. *Let $P_1, P_2 \in \mathbb{P}$. Then $\widetilde{P}_1 \sim_{\mathrm{FRB}:\ell_{\mathrm{brs}}} \widetilde{P}_2$ iff $\mathsf{A}_{\mathrm{FR}} \vdash_{\mathrm{brs}} \widetilde{P}_1 = \widetilde{P}_2$.*

Proof. Soundness, i.e., $\mathsf{A}_{\mathrm{FR}} \vdash_{\mathrm{brs}} \widetilde{P}_1 = \widetilde{P}_2 \implies \widetilde{P}_1 \sim_{\mathrm{FRB}:\ell_{\mathrm{brs}}} \widetilde{P}_2$, is a straightforward consequence of the axioms and inference rules behind $\vdash_{\mathrm{brs}}$ (see Section 6.1 where for each equation side its ℓ_{brs}-encoding is considered) together with $\sim_{\mathrm{FRB}:\ell_{\mathrm{brs}}}$ being an equivalence relation and a congruence (see Theorem 6.4), plus the fact that the lefthand side process of each additional axiom in Table 6.6 is $\sim_{\mathrm{FRB}:\ell_{\mathrm{brs}}}$-equivalent to the righthand side process of the same axiom.
Let us address ground completeness, i.e., $\widetilde{P}_1 \sim_{\mathrm{FRB}:\ell_{\mathrm{brs}}} \widetilde{P}_2 \implies \mathsf{A}_{\mathrm{FR}} \vdash_{\mathrm{brs}} \widetilde{P}_1 = \widetilde{P}_2$. We suppose that $\widetilde{P}_1$ and $\widetilde{P}_2$ are both in FR-nf and proceed by induction on the syntactical structure of $\widetilde{P}_1$:

- If $\widetilde{P}_1$ is $\widetilde{\underline{0}}$ then from $\widetilde{P}_1 \sim_{\mathrm{FRB}:\ell_{\mathrm{brs}}} \widetilde{P}_2$ and $\widetilde{P}_2$ in FR-nf we derive that $\widetilde{P}_2$ can only be $\widetilde{\underline{0}}$, from which the result follows by reflexivity.

- If $\widetilde{P}_1$ is $[\widetilde{a_1^\dagger \,.\, P_1'} +] \sum_{i \in I_1} \widetilde{a_{1,i} \,.\, P_{1,i}}$ with $\widetilde{a_1^\dagger \,.\, P_1'}$ present or $I_1 \neq \emptyset$, then from $\widetilde{P}_1 \sim_{\text{FRB}:\ell_{\text{brs}}} \widetilde{P}_2$ and $\widetilde{P}_2$ in FR-nf we derive that $\widetilde{P}_2$ can only be $[\widetilde{a_2^\dagger \,.\, P_2'} +] \sum_{i \in I_2} \widetilde{a_{2,i} \,.\, P_{2,i}}$ with $\widetilde{a_2^\dagger \,.\, P_2'}$ present iff $\widetilde{a_1^\dagger \,.\, P_1'}$ present and – if they are absent – $I_2 \neq \emptyset \neq I_1$. We recall that $\widetilde{P}_1'$, $\widetilde{P}_2'$, every $\widetilde{P}_{1,i}$, and every $\widetilde{P}_{2,i}$ are all in FR-nf.
  In the presence of $\widetilde{a_1^\dagger \,.\, P_1'}$ and $\widetilde{a_2^\dagger \,.\, P_2'}$, it is not necessarily the case that $I_2 \neq \emptyset$ iff $I_1 \neq \emptyset$. However, if for example $I_1 = \emptyset$ and $I_2 \neq \emptyset$, then in order for $\widetilde{P}_1 \sim_{\text{FRB}:\ell_{\text{brs}}} \widetilde{P}_2$ it must be the case that $\mathit{to\_initial}(\widetilde{a_2^\dagger \,.\, P_2'}) = \sum_{i \in I_2} \widetilde{a_{2,i} \,.\, P_{2,i}}$, in which case $\mathsf{A}_{\text{FR}} \vdash_{\text{brs}} \widetilde{P}_2 = \widetilde{a_2^\dagger \,.\, P_2'}$ by axiom $\mathsf{A}_{\text{FR},4}$. Therefore we can suppose that $I_2 \neq \emptyset$ iff $I_1 \neq \emptyset$ when examining the two main summands of $\widetilde{P}_1$ and $\widetilde{P}_2$.
  If $\widetilde{a_1^\dagger \,.\, P_1'}$ and $\widetilde{a_2^\dagger \,.\, P_2'}$ are present, from the fact that they are the only summands in $\widetilde{P}_1$ and $\widetilde{P}_2$ that can move it follows that $a_1 = a_2$ and $\widetilde{P}_1' \sim_{\text{FRB}:\ell_{\text{brs}}} \widetilde{P}_2'$, otherwise $\widetilde{P}_1 \sim_{\text{FRB}:\ell_{\text{brs}}} \widetilde{P}_2$ could not hold. From the induction hypothesis we obtain $\mathsf{A}_{\text{FR}} \vdash_{\text{brs}} \widetilde{P}_1' = \widetilde{P}_2'$ and hence $\mathsf{A}_{\text{FR}} \vdash_{\text{brs}} \widetilde{a_1^\dagger \,.\, P_1'} = \widetilde{a_2^\dagger \,.\, P_2'}$ by substitutivity with respect to executed action prefix.
  If $I_1 \neq \emptyset \neq I_2$, when going back to $\mathit{to\_initial}(\widetilde{P}_1)$ and $\mathit{to\_initial}(\widetilde{P}_2)$ also $\sum_{i \in I_1} \widetilde{a_{1,i} \,.\, P_{1,i}}$ and $\sum_{i \in I_2} \widetilde{a_{2,i} \,.\, P_{2,i}}$ can move. Suppose that $\mathit{to\_initial}(\widetilde{a_1^\dagger \,.\, P_1'}) \neq \sum_{i \in I_1} \widetilde{a_{1,i} \,.\, P_{1,i}}$ and $\mathit{to\_initial}(\widetilde{a_2^\dagger \,.\, P_2'}) \neq \sum_{i \in I_2} \widetilde{a_{2,i} \,.\, P_{2,i}}$ so as not to fall back into the previous case. Since $\widetilde{P}_1 \sim_{\text{FRB}:\ell_{\text{brs}}} \widetilde{P}_2$, for each $i_1 \in I_1$ there exists $i_2 \in I_2$ such that $a_{1,i_1} = a_{2,i_2}$ and $\widetilde{P}_{1,i_1} \sim_{\text{FRB}:\ell_{\text{brs}}} \widetilde{P}_{2,i_2}$, and vice versa. From the induction hypothesis we obtain $\mathsf{A}_{\text{FR}} \vdash_{\text{brs}} \widetilde{P}_{1,i_1} = \widetilde{P}_{2,i_2}$. It then follows that $\mathsf{A}_{\text{FR}} \vdash_{\text{brs}} \widetilde{a_{1,i_1} \,.\, P_{1,i_1}} = \widetilde{a_{2,i_2} \,.\, P_{2,i_2}}$ by substitutivity with respect to action prefix, hence $\mathsf{A}_{\text{FR}} \vdash_{\text{brs}} \sum_{i \in I_1} \widetilde{a_{1,i} \,.\, P_{1,i}} = \sum_{i \in I_2} \widetilde{a_{2,i} \,.\, P_{2,i}}$ by substitutivity with respect to alternative composition and, in the presence of identical summands on the same side that are absent on the other side, axiom $\mathsf{A}_{\text{FR},4}$ (possibly preceded by applications of axioms $\mathsf{A}_{\text{FR},1}$ and $\mathsf{A}_{\text{FR},2}$ to move identical summands next to each other) and transitivity.
  When $\widetilde{a_1^\dagger \,.\, P_1'}$ and $\widetilde{a_2^\dagger \,.\, P_2'}$ are present and $I_1 \neq \emptyset \neq I_2$, the result stems from substitutivity with respect to alternative composition.

If $\widetilde{P}_1$ and $\widetilde{P}_2$ are not both in FR-nf, thanks to Lemma 6.9 we can find $Q_1, Q_2 \in \mathbb{P}_{\text{no}\Box}$, each of which is initial iff so is its corresponding process, with $\widetilde{Q}_1$ and $\widetilde{Q}_2$ in FR-nf such that $\mathsf{A}_{\text{FR}} \vdash_{\text{brs}} \widetilde{P}_1 = \widetilde{Q}_1$ and $\mathsf{A}_{\text{FR}} \vdash_{\text{brs}} \widetilde{P}_2 = \widetilde{Q}_2$, hence $\mathsf{A}_{\text{FR}} \vdash_{\text{brs}} \widetilde{Q}_2 = \widetilde{P}_2$ by symmetry. Due to soundness, we get $\widetilde{P}_1 \sim_{\text{FRB}:\ell_{\text{brs}}} \widetilde{Q}_1$, hence $\widetilde{Q}_1 \sim_{\text{FRB}:\ell_{\text{brs}}} \widetilde{P}_1$ as $\sim_{\text{FRB}:\ell_{\text{brs}}}$ is symmetric, and $\widetilde{P}_2 \sim_{\text{FRB}:\ell_{\text{brs}}} \widetilde{Q}_2$. Since $\widetilde{P}_1 \sim_{\text{FRB}:\ell_{\text{brs}}} \widetilde{P}_2$, we also get $\widetilde{Q}_1 \sim_{\text{FRB}:\ell_{\text{brs}}} \widetilde{Q}_2$ as $\sim_{\text{FRB}:\ell_{\text{brs}}}$ is transitive. By virtue of what has been shown above, from $\widetilde{Q}_1 \sim_{\text{FRB}:\ell_{\text{brs}}} \widetilde{Q}_2$ with $\widetilde{Q}_1$ and $\widetilde{Q}_2$ in FR-nf it follows that $\mathsf{A}_{\text{FR}} \vdash_{\text{brs}} \widetilde{Q}_1 = \widetilde{Q}_2$ and hence $\mathsf{A}_{\text{FR}} \vdash_{\text{brs}} \widetilde{P}_1 = \widetilde{P}_2$ by transitivity. ∎

Corollary 6.5. *Let $P_1, P_2 \in \mathbb{P}$. Then $P_1 \sim_{\text{FRB}} P_2$ iff $\mathsf{A}_{\text{FR}} \vdash_{\text{brs}} \widetilde{P}_1 = \widetilde{P}_2$.*

Proof. It stems from $P_1 \sim_{\text{FRB}} P_2$ iff $\widetilde{P}_1 \sim_{\text{FRB}:\ell_{\text{brs}}} \widetilde{P}_2$ as established by Corollary 6.1. ∎

$(\mathsf{A}^{\tau}_{\mathrm{FR},1})$	$\widehat{(P+Q)}+R$	$=$	$P+\widehat{(Q+R)}$	where at least two among P, Q, R are initial
$(\mathsf{A}^{\tau}_{\mathrm{FR},2})$	$\widehat{P+Q}$	$=$	$\widehat{Q+P}$	where $initial(P) \vee initial(Q)$
$(\mathsf{A}^{\tau}_{\mathrm{FR},3})$	$\widehat{P+\underline{0}}$	$=$	$\widehat{P}$	
$(\mathsf{A}^{\tau}_{\mathrm{FR},4})$	$\widehat{P+Q}$	$=$	$\widehat{P}$	if $initial(Q) \wedge to\_initial(P) = Q$
$(\mathsf{A}^{\tau}_{\mathrm{FR},5})$	$\widehat{\underline{0}\llcorner\rho\urcorner}$	$=$	$\widehat{\underline{0}}$	
$(\mathsf{A}^{\tau}_{\mathrm{FR},6})$	$\widehat{(a\,.\,P)\llcorner\rho\urcorner}$	$=$	$\rho(a)\,.\,\widehat{(P\llcorner\rho\urcorner)}$	where $initial(P)$
$(\mathsf{A}^{\tau}_{\mathrm{FR},7})$	$\widehat{(a^{\dagger}\,.\,P)\llcorner\rho\urcorner}$	$=$	$\rho(a)^{\dagger}\,.\,\widehat{(P\llcorner\rho\urcorner)}$	
$(\mathsf{A}^{\tau}_{\mathrm{FR},8})$	$\widehat{(P+Q)\llcorner\rho\urcorner}$	$=$	$\widehat{(P\llcorner\rho\urcorner)+(Q\llcorner\rho\urcorner)}$	where $initial(P) \vee initial(Q)$
$(\mathsf{A}^{\tau}_{\mathrm{FR},9})$	$\widehat{P_1 \parallel_L P_2}$	$=$	$e\ell^{\varepsilon}_{\mathrm{brs,w}}(\widehat{P}_1,\widehat{P}_2,L)_{P_1 \parallel_L P_2}$	with P_k in FR-nf for $k \in \{1,2\}$
$(\mathsf{A}^{\tau}_{\mathrm{FR},10})$	$a\,.\,\widehat{(\tau\,.\,(P+Q)+P)}$	$=$	$a\,.\,\widehat{(P+Q)}$	where $initial(P) \wedge initial(Q)$
$(\mathsf{A}^{\tau}_{\mathrm{FR},11})$	$a^{\dagger}\,.\,\widehat{(\tau\,.\,(P+Q)+P')}$	$=$	$a^{\dagger}\,.\,\widehat{(P'+Q)}$	if $to\_initial(P') = P$, where $initial(P) \wedge initial(Q)$
$(\mathsf{A}^{\tau}_{\mathrm{FR},12})$	$a^{\dagger}\,.\,\widehat{(\tau^{\dagger}\,.\,(P'+Q)+P)}$	$=$	$a^{\dagger}\,.\,\widehat{(P'+Q)}$	if $to\_initial(P') = P$, where $initial(P)$

Table 6.7: Axioms characterizing $\approx_{\mathrm{FRB:ps}}$ via the $\ell_{\mathrm{brs,w}}$-encoding into $\mathbb{P}_{\mathrm{brs}}$ processes

6.6.2 Axiomatization of $\approx_{\mathrm{FRB:ps}}$

The set $\mathsf{A}^{\tau}_{\mathrm{FR}}$ of $\ell_{\mathrm{brs,w}}$-based axioms for $\approx_{\mathrm{FRB:ps}}$ is shown in Table 6.7. The first nine axioms have the same shape as those in Table 6.6, with the difference that the $\ell_{\mathrm{brs,w}}$-encoding is considered in lieu of the one based on ℓ_{brs}.

The three additional axioms, i.e., axioms $\mathsf{A}^{\tau}_{\mathrm{FR},10}$ to $\mathsf{A}^{\tau}_{\mathrm{FR},12}$, which are specific to our reversible setting, expresses the abstraction capability of $\approx_{\mathrm{FRB}}$. The first one is the only τ-law of branching bisimilarity over forward-only processes [80] (see the forthcoming Theorem 7.3), while the other two are necessary in our setting to achieve ground completeness.

Lemma 6.10. *For all (initial) $P \in \mathbb{P}$ there exists (an initial) $Q \in \mathbb{P}_{\mathrm{no}\llcorner\urcorner}$ such that $\mathsf{A}^{\tau}_{\mathrm{FR}} \vdash_{\mathrm{brs,w}} \widehat{P} = \widehat{Q}$ with $\widehat{Q}$ in FR-nf.*

Proof. Since in the considered normal form τ-actions do not play a role different from the one of observable actions, we proceed like in the proof of Lemma 6.9 apart from the renaming case in which, when obtaining $\widehat{Q'\llcorner\rho\urcorner}$ from $\widehat{Q'}$ by renaming all of its actions and backward ready sets according to ρ, the second component of each possible extended prefix whose first component is observable and renamed τ by ρ, as well as the second component of each possible subsequent extended prefix whose first component is named τ, is changed to the second component of the closest preceding extended prefix whose first component is an action neither named τ nor renamed τ by ρ (or $\emptyset$ if there is no such a preceding prefix). ∎

The saturation technique used in Section 6.3.2 to prove ground completeness for $\approx_{\mathrm{FB:ps}}$ turns out to be unsound for $\approx_{\mathrm{FRB:ps}}$ like in the case of branching bisimilarity over forward-only processes [75]. In particular, a normal form based on saturation cannot be set up for $\approx_{\mathrm{FRB:ps}}$. On the one hand, the backward version of:

$$\text{if } P \Longrightarrow \xrightarrow{\theta'} \Longrightarrow P' \text{ then } P \xrightarrow{\theta''} P'' \text{ with } act(\theta') = act(\theta'') \text{ and } P' \approx_{\mathrm{FRB:ps}} P''$$

which is:

$$\text{if } P' \Longrightarrow \xrightarrow{\theta'} \Longrightarrow P \text{ then } P'' \xrightarrow{\theta''} P \text{ with } act(\theta') = act(\theta'') \text{ and } P' \approx_{\mathrm{FRB:ps}} P''$$

can be satisfied only when P' and P'' coincide in the case that P has only one incoming transition, e.g., $P \in \mathbb{P}_{\rm seq}$. On the other hand, not even the forward version of saturation works for $\approx_{\rm FRB:ps}$ because it preserves neither past sensitivity in a forward-reverse framework nor forward-reverse semantics in general:

- Consider P given by $\tau \,.\, (a \,.\, \tau \,.\, \underline{0} + b \,.\, \underline{0}) + a \,.\, \underline{0} + b \,.\, \underline{0}$ along with its two transitions:
$$\begin{array}{lcl} P & \Longrightarrow \xrightarrow{\dotplus\dotplus.\tau\dotplus a} \Longrightarrow & \tau^\dagger \,.\, (a^\dagger \,.\, \tau^\dagger \,.\, \underline{0} + b \,.\, \underline{0}) + a \,.\, \underline{0} + b \,.\, \underline{0} \triangleq P' \\ P & \xrightarrow{\dotplus\dotplus a} & \tau \,.\, (a \,.\, \tau \,.\, \underline{0} + b \,.\, \underline{0}) + a^\dagger \,.\, \underline{0} + b \,.\, \underline{0} \triangleq P'' \end{array}$$
Then $P' \not\approx_{\rm FRB:ps} P''$. Indeed, if P' undoes τ with P'' idling and then undoes a thus reaching the non-initial process $\tau^\dagger \,.\, (a \,.\, \tau \,.\, \underline{0} + b \,.\, \underline{0}) + a \,.\, \underline{0} + b \,.\, \underline{0}$, then P'' can only respond by undoing a thus reaching the initial process P.

- Consider Q given by $\tau \,.\, a \,.\, (\tau \,.\, \underline{0} + b \,.\, \underline{0}) + a \,.\, \underline{0} + b \,.\, \underline{0}$ along with its two transitions:
$$\begin{array}{lcl} Q & \Longrightarrow \xrightarrow{\dotplus\dotplus.\tau a} \Longrightarrow & \tau^\dagger \,.\, a^\dagger \,.\, (\tau^\dagger \,.\, \underline{0} + b \,.\, \underline{0}) + a \,.\, \underline{0} + b \,.\, \underline{0} \triangleq Q' \\ Q & \xrightarrow{\dotplus\dotplus a} & \tau \,.\, a \,.\, (\tau \,.\, \underline{0} + b \,.\, \underline{0}) + a^\dagger \,.\, \underline{0} + b \,.\, \underline{0} \triangleq Q'' \end{array}$$
Then $Q' \not\approx_{\rm FRB:ps} Q''$. Indeed, if Q' undoes τ thus reaching $\tau^\dagger \,.\, a^\dagger \,.\, (\tau \,.\, \underline{0} + b \,.\, \underline{0}) + a \,.\, \underline{0} + b \,.\, \underline{0}$ with Q'' staying idle, then in the forward direction the newly reached process can perform b whereas Q'' cannot.

We thus proceed by recasting in our reversible setting a preliminary result for the completeness of the axiomatization of branching bisimulation congruence over forward-only processes provided in [1]. This yields two lemmas, where the former is about equivalent initial processes that are then proven to be equal when prefixed by an unexecuted action, while the latter has to do with equivalent arbitrary processes that are then proven to be equal when prefixed by an executed action. The proof of the former lemma and part of the latter lemma is inspired by the proof of the aforementioned result. In addition to these two lemmas, in the proof of ground completeness we exploit $\approx_{\rm FRB:c:\ell_{brs,w}}$, which is an alternative characterization of $\approx_{\rm FRB:ps:\ell_{brs,w}}$ inspired by Definition 4.4 and Theorem 4.3.

Lemma 6.11. *Let $P_1, P_2 \in \mathbb{P}$ be initial and $a \in \mathcal{A}$. If $\widehat{P_1} \approx_{\rm FRB:\ell_{brs,w}} \widehat{P_2}$ then $\mathsf{A}^\tau_{\rm FR} \vdash_{\rm brs,w} \widehat{a \,.\, P_1} = \widehat{a \,.\, P_2}$.*

Proof. We suppose that $\widehat{P_1}$ and $\widehat{P_2}$ are both in FR-nf. Given that we cannot proceed by induction on the syntactical structure of $\widehat{P_1}$ or $size(\widehat{P_1})$ alone because (i) in the case that $\widehat{P_1}$ is $\widehat{\underline{0}}$ or equivalently $size(\widehat{P_1}) = 0$ from $\widehat{P_1} \approx_{\rm FRB:\ell_{brs,w}} \widehat{P_2}$ and $\widehat{P_1}$ and $\widehat{P_2}$ in FR-nf we cannot conclude that $\widehat{P_2}$ is $\widehat{\underline{0}}$ or equivalently $size(\widehat{P_2}) = 0$ too and (ii) in other cases we work with $\widehat{P_1}$ itself instead of one of its subprocesses, we proceed by induction on $k = size(\widehat{P_1}) + size(\widehat{P_2})$:

- If $k = 0$ then from $\widehat{P_1} \approx_{\rm FRB:\ell_{brs,w}} \widehat{P_2}$ and $\widehat{P_1}$ and $\widehat{P_2}$ in FR-nf we derive that $\widehat{P_1}$ and $\widehat{P_2}$ are both equal to $\widehat{\underline{0}}$, from which the result follows by reflexivity and substitutivity with respect to action prefix.

- If $k > 0$ then $\widehat{P_1}$ is $\sum_{i \in I_1} \widehat{a_{1,i} \,.\, P_{1,i}}$ and $\widehat{P_2}$ is $\sum_{i \in I_2} \widehat{a_{2,i} \,.\, P_{2,i}}$, where every $\widehat{P_{1,i}}$ and every $\widehat{P_{2,i}}$ is initial and in FR-nf (from $\widehat{P_1} \approx_{\rm FRB:\ell_{brs,w}} \widehat{P_2}$ it follows that when either index set is empty, i.e., either process is $\widehat{\underline{0}}$, all the actions of the other process – whose index set cannot be empty – must be τ). Let us consider the following two conditions:

  1. There exists $i \in I_1$ such that $a_{1,i} = \tau$ and $\widehat{P_{1,i}} \approx_{\rm FRB:\ell_{brs,w}} \widehat{P_2}$.
  2. There exists $i \in I_2$ such that $a_{2,i} = \tau$ and $\widehat{P_{2,i}} \approx_{\rm FRB:\ell_{brs,w}} \widehat{P_1}$.

There are three cases:

- Suppose that neither condition 1 nor condition 2 holds. From $\widehat{P}_1 \approx_{\mathrm{FRB}:\ell_{\mathrm{brs,w}}} \widehat{P}_2$ it follows that, whenever $P_1 \xrightarrow{\theta_1,\sqsupset}_{\mathrm{brs}} \widehat{b^\dagger . P_{1,i_1}} + \sum_{i \in I_1 \setminus \{i_1\}} \widehat{a_{1,i} . P_{1,i}}$ with $act(\theta_1) = a_{1,i_1} = b$, then $\widehat{P}_2 \xrightarrow{\theta_2,\sqsupset}_{\mathrm{brs}} \widehat{b^\dagger . P_{2,i_2}} + \sum_{i \in I_2 \setminus \{i_2\}} \widehat{a_{2,i} . P_{2,i}}$ with $act(\theta_2) = a_{2,i_2} = b$, where $\widehat{b^\dagger . P_{1,i_1}} + \sum_{i \in I_1 \setminus \{i_1\}} \widehat{a_{1,i} . P_{1,i}} \approx_{\mathrm{FRB}:\ell_{\mathrm{brs,w}}} \widehat{b^\dagger . P_{2,i_2}} + \sum_{i \in I_2 \setminus \{i_2\}} \widehat{a_{2,i} . P_{2,i}}$, and vice versa. Note that P_2 (resp. P_1) cannot idle when $b = \tau$ because condition 1 (resp. 2) does not hold.
  Every pair of $\approx_{\mathrm{FRB}:\ell_{\mathrm{brs,w}}}$-equivalent reached processes is composed of two non-initial processes whose only incoming transitions are identically labeled and respectively depart from the two $\approx_{\mathrm{FRB}:\ell_{\mathrm{brs,w}}}$-equivalent initial processes $\widehat{P}_1$ and $\widehat{P}_2$, hence $\widehat{P}_{1,i_1} = \mathit{to\_forward}(\widehat{b^\dagger . P_{1,i_1}} + \sum_{i \in I_1 \setminus \{i_1\}} \widehat{a_{1,i} . P_{1,i}}) \approx_{\mathrm{FRB}:\ell_{\mathrm{brs,w}}} \mathit{to\_forward}(\widehat{b^\dagger . P_{2,i_2}} + \sum_{i \in I_2 \setminus \{i_2\}} \widehat{a_{2,i} . P_{2,i}}) = \widehat{P}_{2,i_2}$. From the induction hypothesis it follows that $\mathsf{A}^\tau_{\mathrm{FR}} \vdash_{\mathrm{brs,w}} \widehat{a_{1,i_1} . P_{1,i_1}} = \widehat{a_{2,i_2} . P_{2,i_2}}$, hence $\mathsf{A}^\tau_{\mathrm{FR}} \vdash_{\mathrm{brs,w}} \widehat{P}_1 = \widehat{P}_2$ by substitutivity with respect to alternative composition and, in the presence of identical summands on the same side that are absent on the other side, axiom $\mathsf{A}^\tau_{\mathrm{FR},4}$ (possibly preceded by applications of axioms $\mathsf{A}^\tau_{\mathrm{FR},1}$ and $\mathsf{A}^\tau_{\mathrm{FR},2}$ to move identical summands next to each other) and transitivity. Therefore $\mathsf{A}^\tau_{\mathrm{FR}} \vdash_{\mathrm{brs,w}} \widehat{a . P_1} = \widehat{a . P_2}$ by substitutivity with respect to action prefix.
- Suppose that both condition 1 and condition 2 hold. Then there exist $i_1 \in I_1$ and $i_2 \in I_2$ such that $a_{1,i_1} = \tau = a_{2,i_2}$ and $\widehat{P}_{1,i_1} \approx_{\mathrm{FRB}:\ell_{\mathrm{brs,w}}} \widehat{P}_2 \approx_{\mathrm{FRB}:\ell_{\mathrm{brs,w}}} \widehat{P}_1 \approx_{\mathrm{FRB}:\ell_{\mathrm{brs,w}}} \widehat{P}_{2,i_2}$, hence $\widehat{P}_{1,i_1} \approx_{\mathrm{FRB}:\ell_{\mathrm{brs,w}}} \widehat{P}_{2,i_2}$, where we have exploited the fact that $\approx_{\mathrm{FRB}:\ell_{\mathrm{brs,w}}}$ is symmetric and transitive. Since the considered chain of equalities can be rewritten as $\widehat{P}_1 \approx_{\mathrm{FRB}:\ell_{\mathrm{brs,w}}} \widehat{P}_{2,i_2} \approx_{\mathrm{FRB}:\ell_{\mathrm{brs,w}}} \widehat{P}_{1,i_1} \approx_{\mathrm{FRB}:\ell_{\mathrm{brs,w}}} \widehat{P}_2$ by virtue of the same two properties of $\approx_{\mathrm{FRB}:\ell_{\mathrm{brs,w}}}$, from the induction hypothesis it follows that $\mathsf{A}^\tau_{\mathrm{FR}} \vdash_{\mathrm{brs,w}} \widehat{a . P_1} = \widehat{a . P_{2,i_2}}$, $\mathsf{A}^\tau_{\mathrm{FR}} \vdash_{\mathrm{brs,w}} \widehat{a . P_{2,i_2}} = \widehat{a . P_{1,i_1}}$, and $\mathsf{A}^\tau_{\mathrm{FR}} \vdash_{\mathrm{brs,w}} \widehat{a . P_{1,i_1}} = \widehat{a . P_2}$, hence $\mathsf{A}^\tau_{\mathrm{FR}} \vdash_{\mathrm{brs,w}} \widehat{a . P_1} = \widehat{a . P_2}$ by transitivity.
- Suppose that only one of the two conditions holds, say condition 1. For every summand $\widehat{\tau . P_{1,i}}$ of $\widehat{P}_1$ such that $\widehat{P}_{1,i} \approx_{\mathrm{FRB}:\ell_{\mathrm{brs,w}}} \widehat{P}_2$ it holds that $\mathsf{A}^\tau_{\mathrm{FR}} \vdash_{\mathrm{brs,w}} \widehat{\tau . P_{1,i}} = \widehat{\tau . P_2}$ by the induction hypothesis, hence $\mathsf{A}^\tau_{\mathrm{FR}} \vdash_{\mathrm{brs,w}} \widehat{P}_{1_2} = \widehat{\tau . P_2}$, where $\widehat{P}_{1_2}$ is the summation of all those summands of $\widehat{P}_1$, by substitutivity with respect to alternative composition and, in the presence of identical summands on the righthand side that are absent on the lefthand side, axiom $\mathsf{A}^\tau_{\mathrm{FR},4}$ (possibly preceded by applications of axioms $\mathsf{A}^\tau_{\mathrm{FR},1}$ and $\mathsf{A}^\tau_{\mathrm{FR},2}$ to move identical summands next to each other) and transitivity. Indicating with $\widehat{P}'_1$ the summation of all the other summands of $\widehat{P}_1$ – for each of which $a_{1,i} \neq \tau$ or $\widehat{P}_{1,i} \not\approx_{\mathrm{FRB}:\ell_{\mathrm{brs,w}}} \widehat{P}_2$ – we obtain $\mathsf{A}^\tau_{\mathrm{FR}} \vdash_{\mathrm{brs,w}} \widehat{P}_1 = \widehat{\tau . P_2 + P'_1}$ by substitutivity with respect to alternative composition as $\widehat{P}_1$ is given by $\widehat{P_{1_2} + P'_1}$.
  Since $\widehat{P}_1 \approx_{\mathrm{FRB}:\ell_{\mathrm{brs,w}}} \widehat{P}_2$, condition 1 does not hold over $\widehat{P}'_1$, and condition 2 does not hold (over $\widehat{P}_2$), similar to the first case for each summand $\widehat{a_{1,i_1} . P_{1,i_1}}$ of $\widehat{P}'_1$ there must exist a summand $\widehat{a_{2,i_2} . P_{2,i_2}}$ of $\widehat{P}_2$ such that $a_{1,i_1} = a_{2,i_2}$ and $\widehat{P}_{1,i_1} \approx_{\mathrm{FRB}:\ell_{\mathrm{brs,w}}} \widehat{P}_{2,i_2}$, and vice versa, hence $\mathsf{A}^\tau_{\mathrm{FR}} \vdash_{\mathrm{brs,w}} \widehat{a_{1,i_1} . P_{1,i_1}} = \widehat{a_{2,i_2} . P_{2,i_2}}$ by the induction hypothesis, from which it follows that $\mathsf{A}^\tau_{\mathrm{FR}} \vdash_{\mathrm{brs,w}} \widehat{P}'_1 = \widehat{P}_{2_1}$, where $\widehat{P}_{2_1}$ is the summation of all the summands of $\widehat{P}_2$ matching a summand of $\widehat{P}'_1$, by substitutivity with respect to alternative composition and, in the presence of identical summands on the same side that are absent on the other side,

axiom $\mathsf{A}^\tau_{\mathrm{FR},4}$ (possibly preceded by applications of axioms $\mathsf{A}^\tau_{\mathrm{FR},1}$ and $\mathsf{A}^\tau_{\mathrm{FR},2}$ to move identical summands next to each other) and transitivity. Indicating with $\widehat{P}_2'$ the summation of all the other summands of $\widehat{P}_2$ – none of which $\approx_{\mathrm{FRB}:\ell_{\mathrm{brs,w}}}$-matches a summand of $\widehat{P}_1'$ – we obtain $\mathsf{A}^\tau_{\mathrm{FR}} \vdash_{\mathrm{brs,w}} \widehat{P}_2 = \widehat{P_1' + P_2'}$ by substitutivity with respect to alternative composition as $\widehat{P}_2$ is given by $\widehat{P_{2_1} + P_2'}$.
In conclusion $\mathsf{A}^\tau_{\mathrm{FR}} \vdash_{\mathrm{brs,w}} \widehat{a\,.\,P_1} = a\,.\,\widehat{(\tau\,.\,P_2 + P_1')}$ by substitutivity with respect to action prefix, $\mathsf{A}^\tau_{\mathrm{FR}} \vdash_{\mathrm{brs,w}} a\,.\,\widehat{(\tau\,.\,P_2 + P_1')} = a\,.\,(\tau\,.\,\widehat{(P_1' + P_2')} + P_1')$ by substitutivity with respect to action prefix and alternative composition, $\mathsf{A}^\tau_{\mathrm{FR}} \vdash_{\mathrm{brs,w}} a\,.\,(\tau\,.\,\widehat{(P_1' + P_2')} + P_1') = a\,.\,\widehat{(P_1' + P_2')}$ by axiom $\mathsf{A}^\tau_{\mathrm{FR},10}$, and $\mathsf{A}^\tau_{\mathrm{FR}} \vdash_{\mathrm{brs,w}} a\,.\,\widehat{(P_1' + P_2')} = \widehat{a\,.\,P_2}$ by substitutivity with respect to action prefix, hence $\mathsf{A}^\tau_{\mathrm{FR}} \vdash_{\mathrm{brs,w}} \widehat{a\,.\,P_1} = \widehat{a\,.\,P_2}$ by transitivity.
[Example: $P_1 \triangleq \tau\,.\,(b\,.\,\underline{0} + c\,.\,\underline{0} + d\,.\,\underline{0}) + d\,.\,\underline{0}$ and $P_2 \triangleq b\,.\,\underline{0} + c\,.\,\underline{0} + d\,.\,\underline{0}$.]

If $\widehat{P}_1$ and $\widehat{P}_2$ are not both in FR-nf, thanks to Lemma 6.10 we can find $Q_1, Q_2 \in \mathbb{P}_{\mathrm{no}\llcorner\urcorner}$ with $\widehat{Q}_1$ and $\widehat{Q}_2$ initial and in FR-nf such that $\mathsf{A}^\tau_{\mathrm{FR}} \vdash_{\mathrm{brs,w}} \widehat{P}_1 = \widehat{Q}_1$ and $\mathsf{A}^\tau_{\mathrm{FR}} \vdash_{\mathrm{brs,w}} \widehat{P}_2 = \widehat{Q}_2$, hence $\mathsf{A}^\tau_{\mathrm{FR}} \vdash_{\mathrm{brs,w}} \widehat{Q}_2 = \widehat{P}_2$ by symmetry, from which we obtain $\mathsf{A}^\tau_{\mathrm{FR}} \vdash_{\mathrm{brs,w}} \widehat{a\,.\,P_1} = \widehat{a\,.\,Q_1}$ and $\mathsf{A}^\tau_{\mathrm{FR}} \vdash_{\mathrm{brs,w}} \widehat{a\,.\,Q_2} = \widehat{a\,.\,P_2}$ by substitutivity with respect to action prefix. Due to the soundness of $\mathsf{A}^\tau_{\mathrm{FR}}$ (which will be demonstrated at the beginning of the proof of Theorem 6.10 in a way that is independent from this lemma), we get $\widehat{P}_1 \approx_{\mathrm{FRB}:\ell_{\mathrm{brs,w}}} \widehat{Q}_1$, hence $\widehat{Q}_1 \approx_{\mathrm{FRB}:\ell_{\mathrm{brs,w}}} \widehat{P}_1$ as $\approx_{\mathrm{FRB}:\ell_{\mathrm{brs,w}}}$ is symmetric, and $\widehat{P}_2 \approx_{\mathrm{FRB}:\ell_{\mathrm{brs,w}}} \widehat{Q}_2$. Since $\widehat{P}_1 \approx_{\mathrm{FRB}:\ell_{\mathrm{brs,w}}} \widehat{P}_2$, we also get $\widehat{Q}_1 \approx_{\mathrm{FRB}:\ell_{\mathrm{brs,w}}} \widehat{Q}_2$ as $\approx_{\mathrm{FRB}:\ell_{\mathrm{brs,w}}}$ is transitive. By virtue of what has been shown above, from $\widehat{Q}_1 \approx_{\mathrm{FRB}:\ell_{\mathrm{brs,w}}} \widehat{Q}_2$ with $\widehat{Q}_1$ and $\widehat{Q}_2$ initial and in FR-nf it follows that $\mathsf{A}^\tau_{\mathrm{FR}} \vdash_{\mathrm{brs,w}} \widehat{a\,.\,Q_1} = \widehat{a\,.\,Q_2}$ and hence $\mathsf{A}^\tau_{\mathrm{FR}} \vdash_{\mathrm{brs,w}} \widehat{a\,.\,P_1} = \widehat{a\,.\,P_2}$ by transitivity. ∎

Lemma 6.12. *Let $P_1, P_2 \in \mathbb{P}$ and $a \in \mathcal{A}$. If $\widehat{P}_1 \approx_{\mathrm{FRB}:\ell_{\mathrm{brs,w}}} \widehat{P}_2$ then $\mathsf{A}^\tau_{\mathrm{FR}} \vdash_{\mathrm{brs,w}} \widehat{a^\dagger\,.\,P_1} = \widehat{a^\dagger\,.\,P_2}$.*

Proof. We suppose that $\widehat{P}_1$ and $\widehat{P}_2$ are both in FR-nf. Given that we cannot proceed by induction on the syntactical structure of $\widehat{P}_1$ or $\mathit{size}(\widehat{P}_1)$ alone because (i) in the case that $\widehat{P}_1$ is $\widehat{\underline{0}}$ or equivalently $\mathit{size}(\widehat{P}_1) = 0$ from $\widehat{P}_1 \approx_{\mathrm{FRB}:\ell_{\mathrm{brs,w}}} \widehat{P}_2$ and $\widehat{P}_1$ and $\widehat{P}_2$ in FR-nf we cannot conclude that $\widehat{P}_2$ is $\widehat{\underline{0}}$ or equivalently $\mathit{size}(\widehat{P}_2) = 0$ too and (ii) in other cases we work with $\widehat{P}_1$ itself instead of one of its subprocesses, we proceed by induction on $k = \mathit{size}(\widehat{P}_1) + \mathit{size}(\widehat{P}_2)$:

- If $k = 0$ then from $\widehat{P}_1 \approx_{\mathrm{FRB}:\ell_{\mathrm{brs,w}}} \widehat{P}_2$ and $\widehat{P}_1$ and $\widehat{P}_2$ in FR-nf we derive that $\widehat{P}_1$ and $\widehat{P}_2$ are both equal to $\widehat{\underline{0}}$, from which the result follows by reflexivity and substitutivity with respect to executed action prefix.
- Let $k > 0$ with $\widehat{P}_1$ being $\sum_{i \in I_1} \widehat{a_{1,i}\,.\,P_{1,i}}$ and $\widehat{P}_2$ being $\sum_{i \in I_2} \widehat{a_{2,i}\,.\,P_{2,i}}$, where every $\widehat{P}_{1,i}$ and every $\widehat{P}_{2,i}$ is initial and in FR-nf. The proof is similar to the one of the corresponding case in the proof of Lemma 6.11, with the use of $a^\dagger$ in place of a and the final application of axiom $\mathsf{A}^\tau_{\mathrm{FR},11}$ in lieu of axiom $\mathsf{A}^\tau_{\mathrm{FR},10}$.
- Let $k > 0$ with $\widehat{P}_1$ being $\widehat{a_1^\dagger\,.\,P_1'} + \sum_{i \in I_1} \widehat{a_{1,i}\,.\,P_{1,i}}$ and $\widehat{P}_2$ being $\widehat{a_2^\dagger\,.\,P_2'} + \sum_{i \in I_2} \widehat{a_{2,i}\,.\,P_{2,i}}$, where $\widehat{P}_1'$ and $\widehat{P}_2'$ are in FR-nf and every $\widehat{P}_{1,i}$ and every $\widehat{P}_{2,i}$ is initial and in FR-nf. There are two cases:
  - Suppose that for $k \in \{1, 2\}$ either $I_k = \emptyset$, or $\mathit{to\_initial}(\widehat{a_k^\dagger\,.\,P_k'}) = \sum_{i \in I_k} \widehat{a_{k,i}\,.\,P_{k,i}}$ so that $\widehat{P}_k \approx_{\mathrm{FRB}:\ell_{\mathrm{brs,w}}} \widehat{a_k^\dagger\,.\,P_k'}$. There are two subcases:

* If $a_1 = a_2$ then from $\widehat{P}_1 \approx_{\mathrm{FRB}:\ell_{\mathrm{brs,w}}} \widehat{P}_2$ it follows that $\widehat{P}'_1 \approx_{\mathrm{FRB}:\ell_{\mathrm{brs,w}}} \widehat{P}'_2$. Therefore $\mathsf{A}^{\tau}_{\mathrm{FR}} \vdash_{\mathrm{brs,w}} \widehat{a^{\dagger}_1 . P'_1} = \widehat{a^{\dagger}_2 . P'_2}$ by the induction hypothesis, hence $\mathsf{A}^{\tau}_{\mathrm{FR}} \vdash_{\mathrm{brs,w}} \widehat{P}_1 = \widehat{P}_2$ if $I_1 = \emptyset = I_2$ or by axiom $\mathsf{A}^{\tau}_{\mathrm{FR},4}$ and transitivity in the case that $I_1 \neq \emptyset$ or $I_2 \neq \emptyset$. As a consequence $\mathsf{A}^{\tau}_{\mathrm{FR}} \vdash_{\mathrm{brs,w}} \widehat{a^{\dagger} . P_1} = \widehat{a^{\dagger} . P_2}$ by substitutivity with respect to executed action prefix.
* If $a_1 \neq a_2$ then from $\widehat{P}_1 \approx_{\mathrm{FRB}:\ell_{\mathrm{brs,w}}} \widehat{P}_2$ it follows that either action is τ, say a_1, while the other action is observable, as well as $\widehat{P}'_1 \approx_{\mathrm{FRB}:\ell_{\mathrm{brs,w}}} \widehat{P}_2$. Therefore $\mathsf{A}^{\tau}_{\mathrm{FR}} \vdash_{\mathrm{brs,w}} \widehat{\tau^{\dagger} . P'_1} = \widehat{\tau^{\dagger} . P_2}$ by the induction hypothesis, hence $\mathsf{A}^{\tau}_{\mathrm{FR}} \vdash_{\mathrm{brs,w}} \widehat{P}_1 = \widehat{\tau^{\dagger} . P_2}$ if $I_1 = \emptyset$ or by axiom $\mathsf{A}^{\tau}_{\mathrm{FR},4}$ and transitivity in the case that $I_1 \neq \emptyset$. As a consequence $\mathsf{A}^{\tau}_{\mathrm{FR}} \vdash_{\mathrm{brs,w}} \widehat{a^{\dagger} . P_1} = a^{\dagger} . \widehat{\tau^{\dagger} . P_2}$ by substitutivity with respect to executed action prefix, hence $\mathsf{A}^{\tau}_{\mathrm{FR}} \vdash_{\mathrm{brs,w}} \widehat{a^{\dagger} . P_1} = \widehat{a^{\dagger} . P_2}$ by axiom $\mathsf{A}^{\tau}_{\mathrm{FR},12}$ and transitivity.

– Suppose that for $k \in \{1, 2\}$ it holds that $I_k \neq \emptyset$ and $\mathit{to\_initial}(\widehat{a^{\dagger}_k . P'_k}) \neq \sum_{i \in I_k} \widehat{a_{k,i} . P_{k,i}}$. Observing that only $\widehat{a^{\dagger}_1 . P'_1}$ and $\widehat{a^{\dagger}_2 . P'_2}$ can move and, after going back to $\mathit{to\_initial}(\widehat{P}_1)$ and $\mathit{to\_initial}(\widehat{P}_2)$, also $\sum_{i \in I_1} \widehat{a_{1,i} . P_{1,i}}$ and $\sum_{i \in I_2} \widehat{a_{2,i} . P_{2,i}}$ can move, there are two subcases:
  * If every τ-summand of $\mathit{to\_initial}(\widehat{P}_1)$ has a $\approx_{\mathrm{FRB}:\ell_{\mathrm{brs,w}}}$-matching τ-summand of $\mathit{to\_initial}(\widehat{P}_2)$ and vice versa, then from $\widehat{P}_1 \approx_{\mathrm{FRB}:\ell_{\mathrm{brs,w}}} \widehat{P}_2$ it follows that $a_1 = a_2$, $\widehat{P}'_1 \approx_{\mathrm{FRB:ps}:\ell_{\mathrm{brs,w}}} \widehat{P}'_2$, and $\sum_{i \in I_1} \widehat{a_{1,i} . P_{1,i}} \approx_{\mathrm{FRB:ps}:\ell_{\mathrm{brs,w}}} \sum_{i \in I_2} \widehat{a_{2,i} . P_{2,i}}$. Thus $\mathsf{A}^{\tau}_{\mathrm{FR}} \vdash_{\mathrm{brs,w}} \widehat{a^{\dagger}_1 . P'_1} = \widehat{a^{\dagger}_2 . P'_2}$ by the induction hypothesis and $\mathsf{A}^{\tau}_{\mathrm{FR}} \vdash_{\mathrm{brs,w}} \sum_{i \in I_1} \widehat{a_{1,i} . P_{1,i}} = \sum_{i \in I_2} \widehat{a_{2,i} . P_{2,i}}$ by the ground completeness of $\mathsf{A}^{\tau}_{\mathrm{FR}}$ over initial processes (which will be demonstrated in the proof of Theorem 6.10 in a way that is independent from this lemma). As a consequence $\mathsf{A}^{\tau}_{\mathrm{FR}} \vdash_{\mathrm{brs,w}} \widehat{P}_1 = \widehat{P}_2$ by substitutivity with respect to alternative composition, hence $\mathsf{A}^{\tau}_{\mathrm{FR}} \vdash_{\mathrm{brs,w}} \widehat{a^{\dagger} . P_1} = \widehat{a^{\dagger} . P_2}$ by substitutivity with respect to executed action prefix.
  * Otherwise any other τ-summand of $\mathit{to\_initial}(\widehat{P}_1)$ must be such that its continuation is $\approx_{\mathrm{FRB}:\ell_{\mathrm{brs,w}}}$-equivalent to $\mathit{to\_initial}(\widehat{P}_2)$ and vice versa, where the summation of all such τ-summands is $\approx_{\mathrm{FRB}:\ell_{\mathrm{brs,w}}}$-equivalent to a single one. Such a single τ-summand can occur in either process and each of the other summands in that process must be $\approx_{\mathrm{FRB:ps}:\ell_{\mathrm{brs,w}}}$-equivalent to one of the summands of the other process. There are two further subcases:
    · If $a_1 = \tau$ and $a_2 \neq \tau$, so that $\widehat{P}'_1 \approx_{\mathrm{FRB}:\ell_{\mathrm{brs,w}}} \widehat{P}_2$, then $\mathsf{A}^{\tau}_{\mathrm{FR}} \vdash_{\mathrm{brs,w}} \widehat{\tau^{\dagger} . P'_1} = \widehat{\tau^{\dagger} . P_2}$ by the induction hypothesis. Therefore $\mathsf{A}^{\tau}_{\mathrm{FR}} \vdash_{\mathrm{brs,w}} \widehat{\tau^{\dagger} . P'_1} + \sum_{i \in I_1} \widehat{a_{1,i} . P_{1,i}} = \widehat{\tau^{\dagger} . P_2} + \sum_{i \in I_1} \widehat{a_{1,i} . P_{1,i}}$, i.e., $\mathsf{A}^{\tau}_{\mathrm{FR}} \vdash_{\mathrm{brs,w}} \widehat{P}_1 = \widehat{\tau^{\dagger} . P_2} + \sum_{i \in I_1} \widehat{a_{1,i} . P_{1,i}}$, by substitutivity with respect to alternative composition, hence $\mathsf{A}^{\tau}_{\mathrm{FR}} \vdash_{\mathrm{brs,w}} \widehat{a^{\dagger} . P_1} = a^{\dagger} . (\tau^{\dagger} . P_2 + \widehat{\sum_{i \in I_1} a_{1,i} . P_{1,i}})$ by substitutivity with respect to executed action prefix.
    Indicating with $\widehat{P}''_2$ the summation of the initial summands of $\widehat{P}_2$ that are not $\approx_{\mathrm{FRB:ps}:\ell_{\mathrm{brs,w}}}$-equivalent to any of the initial summands of $\widehat{P}_1$, we have that $\mathsf{A}^{\tau}_{\mathrm{FR}} \vdash_{\mathrm{brs,w}} \widehat{P}_2 = \widehat{a^{\dagger}_2 . P'_2} + \widehat{P}''_2 + \sum_{i \in I_1} \widehat{a_{1,i} . P_{1,i}}$ by substitutivity with respect to alternative composition and the ground completeness of $\mathsf{A}^{\tau}_{\mathrm{FR}}$ over initial processes (which will be demonstrated in the proof of Theorem 6.10 in a way that is independent from this lemma). Therefore $\mathsf{A}^{\tau}_{\mathrm{FR}} \vdash_{\mathrm{brs,w}} \widehat{a^{\dagger} . P_1} = a^{\dagger} . (\tau^{\dagger} . (a^{\dagger}_2 . P'_2 + P''_2 + \widehat{\sum_{i \in I_1} a_{1,i} . P_{1,i}}) + \sum_{i \in I_1} a_{1,i} . P_{1,i})$ by substitutivity with

respect to executed action prefix and alternative composition, hence $\mathsf{A}^\tau_{\rm FR} \vdash_{\rm brs,w} \widehat{a^\dagger.P_1} = a^\dagger.(a_2^\dagger.P_2' + \widehat{P_2'' + \sum_{i\in I_1} a_{1,i}.P_{1,i}})$, i.e., $\mathsf{A}^\tau_{\rm FR} \vdash_{\rm brs,w} \widehat{a^\dagger.P_1} = \widehat{a^\dagger.P_2}$, by axiom $\mathsf{A}^\tau_{\rm FR,12}$ and transitivity.
If $a_1 \neq \tau$ and $a_2 = \tau$, then we proceed similarly.
[Example: $P_1 \triangleq \tau^\dagger.(b^\dagger.\underline{0} + c.\underline{0} + d.\underline{0}) + d.\underline{0}$ and $P_2 \triangleq b^\dagger.\underline{0} + c.\underline{0} + d.\underline{0}$.]

- If $a_1 = a_2$, so that $\widehat{P}_1' \approx_{\rm FRB:\ell_{brs,w}} \widehat{P}_2'$, and the aforementioned single τ-summand occurs in $to\_initial(\widehat{P}_1)$, then $\mathsf{A}^\tau_{\rm FR} \vdash_{\rm brs,w} \widehat{a_1^\dagger.P_1'} = \widehat{a_2^\dagger.P_2'}$ by the induction hypothesis. Since the occurrence of that τ-summand in $\sum_{i\in I_1} \widehat{a_{1,i}.P_{1,i}}$ implies $\sum_{i\in I_1} \widehat{a_{1,i}.P_{1,i}} \approx_{\rm FRB:ps:\ell_{brs,w}} \tau.(to\_initial(\widehat{a_2^\dagger.P_2'}) + \sum_{i\in I_2} a_{2,i}.P_{2,i})$, we have that $\mathsf{A}^\tau_{\rm FR} \vdash_{\rm brs,w} \sum_{i\in I_1} \widehat{a_{1,i}.P_{1,i}} = \tau.(to\_initial(\widehat{a_2^\dagger.P_2'}) + \sum_{i\in I_2} a_{2,i}.P_{2,i})$ by the ground completeness of $\mathsf{A}^\tau_{\rm FR}$ over initial processes (which will be demonstrated in the proof of Theorem 6.10 in a way that is independent from this lemma). Thus $\mathsf{A}^\tau_{\rm FR} \vdash_{\rm brs,w} \widehat{a_1^\dagger.P_1'} + \sum_{i\in I_1} \widehat{a_{1,i}.P_{1,i}} = \widehat{a_2^\dagger.P_2'} + \tau.(to\_initial(\widehat{a_2^\dagger.P_2'}) + \sum_{i\in I_2} a_{2,i}.P_{2,i})$, i.e., $\mathsf{A}^\tau_{\rm FR} \vdash_{\rm brs,w} \widehat{P}_1 = \widehat{a_2^\dagger.P_2'} + \tau.(to\_initial(\widehat{a_2^\dagger.P_2'}) + \sum_{i\in I_2} a_{2,i}.P_{2,i})$, by substitutivity with respect to alternative composition, hence $\mathsf{A}^\tau_{\rm FR} \vdash_{\rm brs,w} \widehat{a^\dagger.P_1} = a^\dagger.(a_2^\dagger.P_2' + \tau.(to\_initial(\widehat{a_2^\dagger.P_2'}) + \sum_{i\in I_2} a_{2,i}.P_{2,i}))$ by substitutivity with respect to executed action prefix. As a consequence $\mathsf{A}^\tau_{\rm FR} \vdash_{\rm brs,w} \widehat{a^\dagger.P_1} = a^\dagger.(a_2^\dagger.P_2' + \widehat{\sum_{i\in I_2} a_{2,i}.P_{2,i}})$, i.e., $\mathsf{A}^\tau_{\rm FR} \vdash_{\rm brs,w} \widehat{a^\dagger.P_1} = \widehat{a^\dagger.P_2}$, by axiom $\mathsf{A}^\tau_{\rm FR,11}$ and transitivity.
If the aforementioned single τ-summand occurs in $to\_initial(\widehat{P}_2)$, then we proceed similarly.
[Example: $P_1 \triangleq d^\dagger.\underline{0} + \tau.(d.\underline{0} + b.\underline{0} + c.\underline{0})$ and $P_2 \triangleq d^\dagger.\underline{0} + b.\underline{0} + c.\underline{0}$.]

- Let $k > 0$ with $\widehat{P}_1$ being $\widehat{a_1^\dagger.P_1'} + \sum_{i\in I_1} \widehat{a_{1,i}.P_{1,i}}$ and $\widehat{P}_2$ being $\sum_{i\in I_2} \widehat{a_{2,i}.P_{2,i}}$, where $\widehat{P}_1'$ is in FR-nf and every $\widehat{P}_{1,i}$ and every $\widehat{P}_{2,i}$ is initial and in FR-nf. From $\widehat{P}_1 \approx_{\rm FRB:\ell_{brs,w}} \widehat{P}_2$ it follows that $a_1 = \tau$, $\widehat{P}_1' \approx_{\rm FRB:\ell_{brs,w}} \widehat{P}_2$, and each of the initial summands of $\widehat{P}_1$ must be $\approx_{\rm FRB:ps:\ell_{brs,w}}$-equivalent to one of the initial summands of $\widehat{P}_2$. Therefore $\mathsf{A}^\tau_{\rm FR} \vdash_{\rm brs,w} \widehat{\tau^\dagger.P_1'} = \widehat{\tau^\dagger.P_2}$ by the induction hypothesis, hence $\mathsf{A}^\tau_{\rm FR} \vdash_{\rm brs,w} \widehat{\tau^\dagger.P_1'} + \sum_{i\in I_1} \widehat{a_{1,i}.P_{1,i}} = \widehat{\tau^\dagger.P_2} + \sum_{i\in I_1} \widehat{a_{1,i}.P_{1,i}}$, i.e., $\mathsf{A}^\tau_{\rm FR} \vdash_{\rm brs,w} \widehat{P}_1 = \widehat{\tau^\dagger.P_2} + \sum_{i\in I_1} \widehat{a_{1,i}.P_{1,i}}$, by substitutivity with respect to alternative composition, from which it follows that $\mathsf{A}^\tau_{\rm FR} \vdash_{\rm brs,w} \widehat{a^\dagger.P_1} = a^\dagger.(\tau^\dagger.P_2 + \widehat{\sum_{i\in I_1} a_{1,i}.P_{1,i}})$ by substitutivity with respect to executed action prefix.
Indicating with $\widehat{P}_2''$ the summation of the initial summands of $\widehat{P}_2$ that are not $\approx_{\rm FRB:ps:\ell_{brs,w}}$-equivalent to any of the initial summands of $\widehat{P}_1$, we have that $\mathsf{A}^\tau_{\rm FR} \vdash_{\rm brs,w} \widehat{P}_2 = \widehat{P}_2'' + \sum_{i\in I_1} \widehat{a_{1,i}.P_{1,i}}$ by substitutivity with respect to alternative composition and the ground completeness of $\mathsf{A}^\tau_{\rm FR}$ over initial processes (which will be demonstrated in the proof of Theorem 6.10 in a way that is independent from this lemma). Therefore $\mathsf{A}^\tau_{\rm FR} \vdash_{\rm brs,w} \widehat{a^\dagger.P_1} = a^\dagger.(\tau^\dagger.(P_2'' + \sum_{i\in I_1} \widehat{a_{1,i}.P_{1,i}}) + \sum_{i\in I_1} a_{1,i}.P_{1,i})$ by substitutivity with respect to executed action prefix and alternative composition, hence $\mathsf{A}^\tau_{\rm FR} \vdash_{\rm brs,w} \widehat{a^\dagger.P_1} = a^\dagger.(P_2'' + \widehat{\sum_{i\in I_1} a_{1,i}.P_{1,i}})$, i.e., $\mathsf{A}^\tau_{\rm FR} \vdash_{\rm brs,w} \widehat{a^\dagger.P_1} = \widehat{a^\dagger.P_2}$, by axiom $\mathsf{A}^\tau_{\rm FR,12}$ and transitivity.
If $\widehat{P}_1$ is $\sum_{i\in I_1} \widehat{a_{1,i}.P_{1,i}}$ and $\widehat{P}_2$ is $\widehat{a_2^\dagger.P_2'} + \sum_{i\in I_2} \widehat{a_{2,i}.P_{2,i}}$, then we proceed similarly.

[Example: $P_1 \triangleq \tau^\dagger.(b\,.\,\underline{0} + c\,.\,\underline{0} + d\,.\,\underline{0}) + d\,.\,\underline{0}$ and $P_2 \triangleq b\,.\,\underline{0} + c\,.\,\underline{0} + d\,.\,\underline{0}$.]

If $\widehat{P_1}$ and $\widehat{P_2}$ are not both in FR-nf, thanks to Lemma 6.10 we can find $Q_1, Q_2 \in \mathbb{P}_{\mathrm{no}\sqsupset}$, each of which is initial iff so is its corresponding process, with $\widehat{Q_1}$ and $\widehat{Q_2}$ in FR-nf such that $\mathsf{A}^\tau_{\mathrm{FR}} \vdash_{\mathrm{brs,w}} \widehat{P_1} = \widehat{Q_1}$ and $\mathsf{A}^\tau_{\mathrm{FR}} \vdash_{\mathrm{brs,w}} \widehat{P_2} = \widehat{Q_2}$, hence $\mathsf{A}^\tau_{\mathrm{FR}} \vdash_{\mathrm{brs,w}} \widehat{Q_2} = \widehat{P_2}$ by symmetry, from which we obtain $\mathsf{A}^\tau_{\mathrm{FR}} \vdash_{\mathrm{brs,w}} \widehat{a^\dagger.P_1} = \widehat{a^\dagger.Q_1}$ and $\mathsf{A}^\tau_{\mathrm{FR}} \vdash_{\mathrm{brs,w}} \widehat{a^\dagger.Q_2} = \widehat{a^\dagger.P_2}$ by substitutivity with respect to executed action prefix. Due to the soundness of $\mathsf{A}^\tau_{\mathrm{FR}}$ (which will be demonstrated at the beginning of the proof of Theorem 6.10 in a way that is independent from this lemma), we get $\widehat{P_1} \approx_{\mathrm{FRB}:\ell_{\mathrm{brs,w}}} \widehat{Q_1}$, hence $\widehat{Q_1} \approx_{\mathrm{FRB}:\ell_{\mathrm{brs,w}}} \widehat{P_1}$ as $\approx_{\mathrm{FRB}:\ell_{\mathrm{brs,w}}}$ is symmetric, and $\widehat{P_2} \approx_{\mathrm{FRB}:\ell_{\mathrm{brs,w}}} \widehat{Q_2}$. Since $\widehat{P_1} \approx_{\mathrm{FRB}:\ell_{\mathrm{brs,w}}} \widehat{P_2}$, we also get $\widehat{Q_1} \approx_{\mathrm{FRB}:\ell_{\mathrm{brs,w}}} \widehat{Q_2}$ as $\approx_{\mathrm{FRB}:\ell_{\mathrm{brs,w}}}$ is transitive. By virtue of what has been shown above, from $\widehat{Q_1} \approx_{\mathrm{FRB}:\ell_{\mathrm{brs,w}}} \widehat{Q_2}$ with $\widehat{Q_1}$ and $\widehat{Q_2}$ in FR-nf it follows that $\mathsf{A}^\tau_{\mathrm{FR}} \vdash_{\mathrm{brs,w}} \widehat{a^\dagger.Q_1} = \widehat{a^\dagger.Q_2}$ and hence $\mathsf{A}^\tau_{\mathrm{FR}} \vdash_{\mathrm{brs,w}} \widehat{a^\dagger.P_1} = \widehat{a^\dagger.P_2}$ by transitivity. ∎

Theorem 6.10. *Let $P_1, P_2 \in \mathbb{P}$. Then $\widehat{P_1} \approx_{\mathrm{FRB:ps}:\ell_{\mathrm{brs,w}}} \widehat{P_2}$ iff $\mathsf{A}^\tau_{\mathrm{FR}} \vdash_{\mathrm{brs,w}} \widehat{P_1} = \widehat{P_2}$.*

Proof. Soundness, i.e., $\mathsf{A}^\tau_{\mathrm{FR}} \vdash_{\mathrm{brs,w}} \widehat{P_1} = \widehat{P_2} \Longrightarrow \widehat{P_1} \approx_{\mathrm{FRB:ps}:\ell_{\mathrm{brs,w}}} \widehat{P_2}$, is a straightforward consequence of the axioms and inference rules behind $\vdash_{\mathrm{brs,w}}$ (see Section 6.1 where for each equation side its $\ell_{\mathrm{brs,w}}$-encoding is considered) together with $\approx_{\mathrm{FRB:ps}:\ell_{\mathrm{brs,w}}}$ being an equivalence relation and a congruence (see Theorem 6.6), plus the fact that the lefthand side process of each additional axiom in Table 6.7 is $\approx_{\mathrm{FRB:ps}:\ell_{\mathrm{brs,w}}}$-equivalent to the righthand side process of the same axiom.
Let us address ground completeness, i.e., $\widehat{P_1} \approx_{\mathrm{FRB:ps}:\ell_{\mathrm{brs,w}}} \widehat{P_2} \Longrightarrow \mathsf{A}^\tau_{\mathrm{FR}} \vdash_{\mathrm{brs,w}} \widehat{P_1} = \widehat{P_2}$. We suppose that $\widehat{P_1}$ and $\widehat{P_2}$ are both in FR-nf and recall that $\mathit{initial}(\widehat{P_1}) \Longleftrightarrow \mathit{initial}(\widehat{P_2})$. There are three cases based on $\widehat{P_1}$:

- If $\widehat{P_1}$ is $\underline{\widehat{0}}$ then from $\widehat{P_1} \approx_{\mathrm{FRB:ps}:\ell_{\mathrm{brs,w}}} \widehat{P_2}$ and $\widehat{P_2}$ in FR-nf we derive that $\widehat{P_2}$ can only be $\underline{\widehat{0}}$, from which the result follows by reflexivity.
- If $\widehat{P_1}$ is $\sum_{i \in I_1} \widehat{a_{1,i}\,.\,P_{1,i}}$ with $I_1 \neq \emptyset$, then from $\widehat{P_1} \approx_{\mathrm{FRB:ps}:\ell_{\mathrm{brs,w}}} \widehat{P_2}$ and $\widehat{P_2}$ in FR-nf we derive that $\widehat{P_2}$ is $\sum_{i \in I_2} \widehat{a_{2,i}\,.\,P_{2,i}}$ with $I_2 \neq \emptyset$. We recall that every $\widehat{P_{1,i}}$ and every $\widehat{P_{2,i}}$ is initial and in FR-nf.
  Since $\widehat{P_1} \approx_{\mathrm{FRB:ps}:\ell_{\mathrm{brs,w}}} \widehat{P_2}$ iff $\widehat{P_1} \approx_{\mathrm{FRB:c}:\ell_{\mathrm{brs,w}}} \widehat{P_2}$ (see Definition 4.4 and Theorem 4.3), from the fact that $\widehat{P_1}$ and $\widehat{P_2}$ are initial it follows that, whenever $\widehat{P_1} \xrightarrow{\theta_1,\sqsupset}_{\mathrm{brs}} \widehat{a^\dagger.P_{1,i_1}} + \sum_{i \in I_1 \setminus \{i_1\}} \widehat{a_{1,i}\,.\,P_{1,i}}$ with $\mathit{act}(\theta_1) = a_{1,i_1} = a$, then $\widehat{P_2} \xrightarrow{\theta_2,\sqsupset}_{\mathrm{brs}} \widehat{a^\dagger.P_{2,i_2}} + \sum_{i \in I_2 \setminus \{i_2\}} \widehat{a_{2,i}\,.\,P_{2,i}}$ with $\mathit{act}(\theta_2) = a_{2,i_2} = a$, where $\widehat{a^\dagger.P_{1,i_1}} + \sum_{i \in I_1 \setminus \{i_1\}} \widehat{a_{1,i}\,.\,P_{1,i}} \approx_{\mathrm{FRB}:\ell_{\mathrm{brs,w}}} \widehat{a^\dagger.P_{2,i_2}} + \sum_{i \in I_2 \setminus \{i_2\}} \widehat{a_{2,i}\,.\,P_{2,i}}$, and vice versa. Every pair of $\approx_{\mathrm{FRB}:\ell_{\mathrm{brs,w}}}$-equivalent reached processes is composed of two non-initial processes whose only incoming transitions are identically labeled and respectively depart from the two $\approx_{\mathrm{FRB:ps}:\ell_{\mathrm{brs,w}}}$-equivalent initial processes $\widehat{P_1}$ and $\widehat{P_2}$, hence $\widehat{P_{1,i_1}} = \mathit{to\_forward}(\widehat{a^\dagger.P_{1,i_1}} + \sum_{i \in I_1 \setminus \{i_1\}} \widehat{a_{1,i}\,.\,P_{1,i}}) \approx_{\mathrm{FRB}:\ell_{\mathrm{brs,w}}} \mathit{to\_forward}(\widehat{a^\dagger.P_{2,i_2}} + \sum_{i \in I_2 \setminus \{i_2\}} \widehat{a_{2,i}\,.\,P_{2,i}}) = \widehat{P_{2,i_2}}$. Since $\widehat{P_{1,i_1}}$ and $\widehat{P_{2,i_2}}$ are initial, $\mathsf{A}^\tau_{\mathrm{FR}} \vdash_{\mathrm{brs,w}} \widehat{a_{1,i_1}\,.\,P_{1,i_1}} = \widehat{a_{2,i_2}\,.\,P_{2,i_2}}$ by Lemma 6.11. Therefore $\mathsf{A}^\tau_{\mathrm{FR}} \vdash_{\mathrm{brs,w}} \widehat{P_1} = \widehat{P_2}$ by substitutivity with respect to alternative composition and, in the presence of identical summands on the same side that are absent on the other side, axiom $\mathsf{A}^\tau_{\mathrm{FR},4}$ (possibly preceded by applications of axioms $\mathsf{A}^\tau_{\mathrm{FR},1}$ and $\mathsf{A}^\tau_{\mathrm{FR},2}$ to move identical summands next to each other) and transitivity.

- If $\widehat{P_1}$ is $\widehat{a_1^\dagger.\,P_1'} + \sum_{i\in I_1} \widehat{a_{1,i}\,.\,P_{1,i}}$ then from $\widehat{P_1} \approx_{\text{FRB:ps:}\ell_{\text{brs,w}}} \widehat{P_2}$ and $\widehat{P_2}$ in FR-nf we derive that $\widehat{P_2}$ is $\widehat{a_2^\dagger.\,P_2'} + \sum_{i\in I_2} \widehat{a_{2,i}\,.\,P_{2,i}}$. We recall that $\widehat{P_1'}$, $\widehat{P_2'}$, every $\widehat{P_{1,i}}$, and every $\widehat{P_{2,i}}$ are all in FR-nf. There are two subcases:

  - Suppose that either $I_1 = \emptyset$, or $to\_initial(\widehat{a_1^\dagger.\,P_1'}) = \sum_{i\in I_1} \widehat{a_{1,i}\,.\,P_{1,i}}$ so that $\widehat{P_1} \approx_{\text{FRB:ps:}\ell_{\text{brs,w}}} \widehat{a_1^\dagger.\,P_1'}$. Then either $I_2 = \emptyset$, or $to\_initial(\widehat{a_2^\dagger.\,P_2'}) = \sum_{i\in I_2} \widehat{a_{2,i}\,.\,P_{2,i}}$ so that $\widehat{P_2} \approx_{\text{FRB:ps:}\ell_{\text{brs,w}}} \widehat{a_2^\dagger.\,P_2'}$, otherwise $\widehat{P_1} \approx_{\text{FRB:ps:}\ell_{\text{brs,w}}} \widehat{P_2}$ could not hold. Since $\widehat{P_1} \approx_{\text{FRB:ps:}\ell_{\text{brs,w}}} \widehat{P_2}$ iff $\widehat{P_1} \approx_{\text{FRB:c:}\ell_{\text{brs,w}}} \widehat{P_2}$ (see Definition 4.4 and Theorem 4.3), from the fact that $\widehat{P_1}$ and $\widehat{P_2}$ are not initial it follows that $to\_initial(\widehat{P_1}) \approx_{\text{FRB:c:}\ell_{\text{brs,w}}} to\_initial(\widehat{P_2})$, i.e., $to\_initial(\widehat{a_1^\dagger.\,P_1'}) \approx_{\text{FRB:ps:}\ell_{\text{brs,w}}} to\_initial(\widehat{a_2^\dagger.\,P_2'})$. Thus $a_1 = a_2$ and $to\_initial(\widehat{P_1'}) \approx_{\text{FRB:ps:}\ell_{\text{brs,w}}} to\_initial(\widehat{P_2'})$, so that $\widehat{P_1'} \approx_{\text{FRB:}\ell_{\text{brs,w}}} \widehat{P_2'}$, otherwise $\widehat{P_1} \approx_{\text{FRB:ps:}\ell_{\text{brs,w}}} \widehat{P_2}$ could not hold. As a consequence $\mathsf{A}^\tau_{\text{FR}} \vdash_{\text{brs,w}} \widehat{a_1^\dagger.\,P_1'} = \widehat{a_2^\dagger.\,P_2'}$ by Lemma 6.12, hence $\mathsf{A}^\tau_{\text{FR}} \vdash_{\text{brs,w}} \widehat{P_1} = \widehat{P_2}$ if $I_1 = \emptyset = I_2$ or by axiom $\mathsf{A}^\tau_{\text{FR},4}$ and transitivity in the case that $I_1 \neq \emptyset$ or $I_2 \neq \emptyset$.
  - Let $I_1 \neq \emptyset$ and $to\_initial(\widehat{a_1^\dagger.\,P_1'}) \neq \sum_{i\in I_1} \widehat{a_{1,i}\,.\,P_{1,i}}$. Then $I_2 \neq \emptyset$ and $to\_initial(\widehat{a_2^\dagger.\,P_2'}) \neq \sum_{i\in I_2} \widehat{a_{2,i}\,.\,P_{2,i}}$, otherwise $\widehat{P_1} \approx_{\text{FRB:ps:}\ell_{\text{brs,w}}} \widehat{P_2}$ could not hold. Observing that only $\widehat{a_1^\dagger.\,P_1'}$ and $\widehat{a_2^\dagger.\,P_2'}$ can move and, after going back to $to\_initial(\widehat{P_1})$ and $to\_initial(\widehat{P_2})$, also $\sum_{i\in I_1} \widehat{a_{1,i}\,.\,P_{1,i}}$ and $\sum_{i\in I_2} \widehat{a_{2,i}\,.\,P_{2,i}}$ can move but it holds that $to\_initial(\widehat{a_1^\dagger.\,P_1'}) \neq \sum_{i\in I_1} \widehat{a_{1,i}\,.\,P_{1,i}}$ and $to\_initial(\widehat{a_2^\dagger.\,P_2'}) \neq \sum_{i\in I_2} \widehat{a_{2,i}\,.\,P_{2,i}}$, from $\widehat{P_1} \approx_{\text{FRB:ps:}\ell_{\text{brs,w}}} \widehat{P_2}$ it follows that $a_1 = a_2$, $\widehat{P_1'} \approx_{\text{FRB:ps:}\ell_{\text{brs,w}}} \widehat{P_2'}$, and $\sum_{i\in I_1} \widehat{a_{1,i}\,.\,P_{1,i}} \approx_{\text{FRB:ps:}\ell_{\text{brs,w}}} \sum_{i\in I_2} \widehat{a_{2,i}\,.\,P_{2,i}}$. Therefore $\mathsf{A}^\tau_{\text{FR}} \vdash_{\text{brs,w}} \widehat{a_1^\dagger.\,P_1'} = \widehat{a_2^\dagger.\,P_2'}$ by Lemma 6.12 and $\mathsf{A}^\tau_{\text{FR}} \vdash_{\text{brs,w}} \sum_{i\in I_1} \widehat{a_{1,i}\,.\,P_{1,i}} = \sum_{i\in I_2} \widehat{a_{2,i}\,.\,P_{2,i}}$ by completeness over initial processes (already proven in the previous two cases), hence $\mathsf{A}^\tau_{\text{FR}} \vdash_{\text{brs,w}} \widehat{a_1^\dagger.\,P_1'} + \sum_{i\in I_1} \widehat{a_{1,i}\,.\,P_{1,i}} = \widehat{a_2^\dagger.\,P_2'} + \sum_{i\in I_2} \widehat{a_{2,i}\,.\,P_{2,i}}$, i.e., $\mathsf{A}^\tau_{\text{FR}} \vdash_{\text{brs,w}} \widehat{P_1} = \widehat{P_2}$, by substitutivity with respect to alternative composition.

If $\widehat{P_1}$ and $\widehat{P_2}$ are not both in FR-nf, thanks to Lemma 6.10 we can find $Q_1, Q_2 \in \mathbb{P}_{\text{no}\langle\rangle}$, each of which is initial iff so is its corresponding process, with $\widehat{Q_1}$ and $\widehat{Q_2}$ in FR-nf such that $\mathsf{A}^\tau_{\text{FR}} \vdash_{\text{brs,w}} \widehat{P_1} = \widehat{Q_1}$ and $\mathsf{A}^\tau_{\text{FR}} \vdash_{\text{brs,w}} \widehat{P_2} = \widehat{Q_2}$, hence $\mathsf{A}^\tau_{\text{FR}} \vdash_{\text{brs,w}} \widehat{Q_2} = \widehat{P_2}$ by symmetry. Due to soundness, we get $\widehat{P_1} \approx_{\text{FRB:ps:}\ell_{\text{brs,w}}} \widehat{Q_1}$, hence $\widehat{Q_1} \approx_{\text{FRB:ps:}\ell_{\text{brs,w}}} \widehat{P_1}$ as $\approx_{\text{FRB:ps:}\ell_{\text{brs,w}}}$ is symmetric, and $\widehat{P_2} \approx_{\text{FRB:ps:}\ell_{\text{brs,w}}} \widehat{Q_2}$. Since $\widehat{P_1} \approx_{\text{FRB:ps:}\ell_{\text{brs,w}}} \widehat{P_2}$, we also get $\widehat{Q_1} \approx_{\text{FRB:ps:}\ell_{\text{brs,w}}} \widehat{Q_2}$ as $\approx_{\text{FRB:ps:}\ell_{\text{brs,w}}}$ is transitive. By virtue of what has been shown above, from $\widehat{Q_1} \approx_{\text{FRB:ps:}\ell_{\text{brs,w}}} \widehat{Q_2}$ with $\widehat{Q_1}$ and $\widehat{Q_2}$ in FR-nf it follows that $\mathsf{A}^\tau_{\text{FR}} \vdash_{\text{brs,w}} \widehat{Q_1} = \widehat{Q_2}$ and hence $\mathsf{A}_{\text{FR}} \vdash_{\text{brs,w}} \widehat{P_1} = \widehat{P_2}$ by transitivity. ∎

Corollary 6.6. *Let $P_1, P_2 \in \mathbb{P}$. Then $P_1 \approx_{\text{FRB:ps}} P_2$ iff $\mathsf{A}^\tau_{\text{FR}} \vdash_{\text{brs,w}} \widehat{P_1} = \widehat{P_2}$.*

Proof. It stems from $P_1 \approx_{\text{FRB:ps}} P_2$ iff $\widehat{P_1} \approx_{\text{FRB:ps:}\ell_{\text{brs,w}}} \widehat{P_2}$ as established by Corollary 6.2. ∎

Chapter 7

Relationships with Other Equivalences

In this chapter, whose contents have appeared in [26, 28, 29], we study the relationships of the previously defined bisimilarities with other equivalences so as to find alternative characterizations. We first address sequential processes, for which strong and weak reverse bisimilarities coincide with strong and weak reverse trace equivalences [45] and weak forward-reverse bisimilarity coincides with branching bisimilarity [80] (Section 7.1). Then we focus on concurrent processes, for which we establish a connection between strong forward-reverse bisimilarity and hereditary history-preserving bisimilarity [16] (Section 7.2).

7.1 Sequential Processes

On the one hand, it is easy to see that strong and weak forward bisimilarities coincide with the strong and weak bisimilarities of [112], because all these equivalences consider only the standard direction of computation and, as witnessed by Examples 2.1 and 3.1, no observable distinctions are introduced along that direction by decorated actions inside processes. On the other hand, we show that, over sequential processes, strong and weak reverse bisimilarities coincide with reverse variants of strong and weak trace equivalences [45] (Section 7.1.1), while weak forward-reverse bisimilarity coincides with branching bisimilarity [80] and its forward-reverse variant (Section 7.1.2).

7.1.1 Reverse Bisimilarities and Reverse Trace Equivalences

Two processes are related by trace equivalence if both perform the same sequences of actions [45]. This is a linear-time semantics because it completely abstracts from branching points as opposed to bisimilarity. Strong and weak reverse bisimilarities can be characterized in terms of reverse variants of strong and weak trace equivalences, which are obtained by defining for each $P \in \mathbb{P}$ its strong and weak reverse trace sets as follows:

$$trace_{\rm r}(P) \;=\; \{a_n \ldots a_1 \in \mathcal{A}^* \mid n \in \mathbb{N}, \forall i = 1, \ldots, n-1.\, (P_i \stackrel{\theta_i}{\longrightarrow} P_{i+1} \wedge act(\theta_i) = a_i), P_n = P\}$$

$$trace_{\rm r,w}(P) \;=\; \{a_n \ldots a_1 \in (\mathcal{A} \setminus \{\tau\})^* \mid n \in \mathbb{N}, \forall i = 1, \ldots, n-1.\, (P_i \Longrightarrow \stackrel{\theta_i}{\longrightarrow} \Longrightarrow P_{i+1} \wedge act(\theta_i) = a_i), P_n = P\}$$

where * applied to a set denotes the set of all finite sequences of elements of that set, including the empty sequence ε.

Definition 7.1. *We say that* $P_1, P_2 \in \mathbb{P}$ *are* reverse trace equivalent*, written* $P_1 \sim_{\rm RT} P_2$*, iff* $trace_{\rm r}(P_1) = trace_{\rm r}(P_2)$. ■

Definition 7.2. *We say that* $P_1, P_2 \in \mathbb{P}$ *are* weakly reverse trace equivalent*, written* $P_1 \approx_{\rm RT} P_2$*, iff* $trace_{\rm r,w}(P_1) = trace_{\rm r,w}(P_2)$. ■

Reverse bisimilarities coincide with reverse trace equivalences only over sequential processes. For example, $(a^\dagger.c^\dagger.\underline{0} \parallel_\emptyset c^\dagger.\underline{0}) \parallel_{\{c\}} (b^\dagger.c^\dagger.\underline{0} \parallel_\emptyset c^\dagger.\underline{0}) \sim_{\mathrm{RT}} (a^\dagger.d^\dagger.\underline{0} \parallel_{\{d\}} b^\dagger.d^\dagger.\underline{0} \parallel_{\{d\}} c^\dagger.d^\dagger.\underline{0}) \llcorner d \mapsto c^\urcorner$ because both processes possess the same reverse trace set $\{\varepsilon, c, ca, cb, cc, cab, cac, cba, cbc, cca, ccb, cabc, cacb, cbac, cbca, ccab, ccba\}$ with the first c in every reverse trace of the second process stemming from the renaming of d. In contrast, $(a^\dagger.c^\dagger.\underline{0} \parallel_\emptyset c^\dagger.\underline{0}) \parallel_{\{c\}} (b^\dagger.c^\dagger.\underline{0} \parallel_\emptyset c^\dagger.\underline{0}) \not\sim_{\mathrm{RB}} (a^\dagger.d^\dagger.\underline{0} \parallel_{\{d\}} b^\dagger.d^\dagger.\underline{0} \parallel_{\{d\}} c^\dagger.d^\dagger.\underline{0}) \llcorner d \mapsto c^\urcorner$ when the involved actions are pairwise different. The reason is that $(a^\dagger.d^\dagger.\underline{0} \parallel_{\{d\}} b^\dagger.d^\dagger.\underline{0} \parallel_{\{d\}} c^\dagger.d^\dagger.\underline{0}) \llcorner d \mapsto c^\urcorner$ has a single incoming transition – labeled with c stemming from the renaming of the three-way synchronization on d – whose source process $(a^\dagger.d.\underline{0} \parallel_{\{d\}} b^\dagger.d.\underline{0} \parallel_{\{d\}} c^\dagger.d.\underline{0}) \llcorner d \mapsto c^\urcorner$ in turn has three incoming transitions respectively labeled with a, b, and c, whereas $(a^\dagger.c^\dagger.\underline{0} \parallel_\emptyset c^\dagger.\underline{0}) \parallel_{\{c\}} (b^\dagger.c^\dagger.\underline{0} \parallel_\emptyset c^\dagger.\underline{0})$ has four incoming transitions – corresponding to the four two-way synchronizations on c – such that only the source process $(a^\dagger.c.\underline{0} \parallel_\emptyset c^\dagger.\underline{0}) \parallel_{\{c\}} (b^\dagger.c.\underline{0} \parallel_\emptyset c^\dagger.\underline{0})$ in turn has three incoming transitions respectively labeled with a, b, and c, whilst the source process $(a^\dagger.c^\dagger.\underline{0} \parallel_\emptyset c.\underline{0}) \parallel_{\{c\}} (b^\dagger.c^\dagger.\underline{0} \parallel_\emptyset c.\underline{0})$ has only one incoming transition – labeled with c – and the two source processes $(a^\dagger.c.\underline{0} \parallel_\emptyset c^\dagger.\underline{0}) \parallel_{\{c\}} (b^\dagger.c^\dagger.\underline{0} \parallel_\emptyset c.\underline{0})$ and $(a^\dagger.c^\dagger.\underline{0} \parallel_\emptyset c.\underline{0}) \parallel_{\{c\}} (b^\dagger.c.\underline{0} \parallel_\emptyset c^\dagger.\underline{0})$ have only two incoming transitions each – respectively labeled with a and c and with b and c. Once it has been reached after undoing the last performed c, which corresponds to the first c in every nonempty reverse trace, none of the last three processes can thus match $(a^\dagger.d.\underline{0} \parallel_{\{d\}} b^\dagger.d.\underline{0} \parallel_{\{d\}} c^\dagger.d.\underline{0}) \llcorner d \mapsto c^\urcorner$ in the reverse bisimulation game.

Theorem 7.1. *Let $P_1, P_2 \in \mathbb{P}_{\mathrm{seq}}$. Then $P_1 \sim_{\mathrm{RB}} P_2$ iff $P_1 \sim_{\mathrm{RT}} P_2$.*

Proof. The proof is divided into two parts:

- Assuming that $P_1 \sim_{\mathrm{RB}} P_2$, which implies that the length n of the longest reverse traces of P_1 and P_2 must be the same, we prove that $\mathit{trace}_{\mathrm{r}}(P_1) = \mathit{trace}_{\mathrm{r}}(P_2)$ by proceeding by induction on $n \in \mathbb{N}$ (due to Proposition 2.1(1) the longest reverse trace is unique in both sets; it must be the same because $P_1 \sim_{\mathrm{RB}} P_2$):
  - If $n = 0$ then P_1 and P_2 are initial and their longest reverse trace is ε. Therefore $\mathit{trace}_{\mathrm{r}}(P_1) = \{\varepsilon\} = \mathit{trace}_{\mathrm{r}}(P_2)$.
  - Let $n > 0$ with the longest reverse trace being $a_n \ldots a_1 \in \mathcal{A}^*$. From $P_1 \sim_{\mathrm{RB}} P_2$ and Proposition 2.1(1) it follows that there exist $P_1' \xrightarrow{\theta_1} P_1$ and $P_2' \xrightarrow{\theta_2} P_2$, with P_1' and P_2' unique, such that $\mathit{act}(\theta_1) = \mathit{act}(\theta_2) = a_n$ and $P_1' \sim_{\mathrm{RB}} P_2'$, hence $\mathit{trace}_{\mathrm{r}}(P_1') = \mathit{trace}_{\mathrm{r}}(P_2')$ by the induction hypothesis with $a_{n-1} \ldots a_1$ being the longest reverse trace in both sets. Therefore $\mathit{trace}_{\mathrm{r}}(P_1) = \mathit{trace}_{\mathrm{r}}(P_1') \cup \{a_n \ldots a_1\} = \mathit{trace}_{\mathrm{r}}(P_2') \cup \{a_n \ldots a_1\} = \mathit{trace}_{\mathrm{r}}(P_2)$.
- Assuming that $P_1 \sim_{\mathrm{RT}} P_2$, we prove that the symmetric relation $\mathcal{B} = \{(Q_1, Q_2) \in \mathbb{P}_{\mathrm{seq}} \times \mathbb{P}_{\mathrm{seq}} \mid \mathit{trace}_{\mathrm{r}}(Q_1) = \mathit{trace}_{\mathrm{r}}(Q_2)\}$ is a reverse bisimulation.
  Given $(Q_1, Q_2) \in \mathcal{B}$ such that $\mathit{trace}_{\mathrm{r}}(Q_1) \neq \{\varepsilon\} \neq \mathit{trace}_{\mathrm{r}}(Q_2)$, from $\mathit{trace}_{\mathrm{r}}(Q_1) = \mathit{trace}_{\mathrm{r}}(Q_2)$ and Proposition 2.1(1) it follows that there exist $Q_1' \xrightarrow{\theta_1} Q_1$ and $Q_2' \xrightarrow{\theta_2} Q_2$ with Q_1' and Q_2' unique and $\mathit{act}(\theta_1) = \mathit{act}(\theta_2)$, where Q_1 and Q_2 have the same unique longest reverse trace σ starting with $\mathit{act}(\theta_1)$ and $\mathit{act}(\theta_2)$ respectively. Therefore $\mathit{trace}_{\mathrm{r}}(Q_1') = \mathit{trace}_{\mathrm{r}}(Q_1) \setminus \{\sigma\} = \mathit{trace}_{\mathrm{r}}(Q_2) \setminus \{\sigma\} = \mathit{trace}_{\mathrm{r}}(Q_2')$ so that $(Q_1', Q_2') \in \mathcal{B}$. ∎

Corollary 7.1. *Let $P_1, P_2 \in \mathbb{P}$. If $P_1 \sim_{\mathrm{RB}} P_2$ then $P_1 \sim_{\mathrm{RT}} P_2$.*

Proof. See the first part of the proof of Theorem 7.1, where:

- The longest reverse traces of P_1 and P_2 may be more than one as P_1 and P_2 are not necessarily sequential.
- When $n > 0$, from $P_1 \sim_{\mathrm{RB}} P_2$ it follows that, for each of the longest reverse traces $a_n \ldots a_1 \in \mathcal{A}^*$ of P_1 and P_2, there exist $P_1' \xrightarrow{\theta_1} P_1$ and $P_2' \xrightarrow{\theta_2} P_2$ such that $act(\theta_1) = act(\theta_2) = a_n$ and $P_1' \sim_{\mathrm{RB}} P_2'$, hence $trace_{\mathrm{r}}(P_1') = trace_{\mathrm{r}}(P_2')$ by the induction hypothesis with $a_{n-1} \ldots a_1$ being one of the longest reverse traces in both sets. Therefore $trace_{\mathrm{r}}(P_1) \supseteq trace_{\mathrm{r}}(P_1') \cup \{a_n \ldots a_1\} = trace_{\mathrm{r}}(P_2') \cup \{a_n \ldots a_1\} \subseteq trace_{\mathrm{r}}(P_2)$. ∎

Theorem 7.2. *Let $P_1, P_2 \in \mathbb{P}_{\mathrm{seq}}$. Then $P_1 \approx_{\mathrm{RB}} P_2$ iff $P_1 \approx_{\mathrm{RT}} P_2$.*

Proof. The proof is divided into two parts:

- Assuming that $P_1 \approx_{\mathrm{RB}} P_2$, which implies that the length n of the longest weak reverse traces of P_1 and P_2 must be the same, we prove that $trace_{\mathrm{r,w}}(P_1) = trace_{\mathrm{r,w}}(P_2)$ by proceeding by induction on $n \in \mathbb{N}$ (due to Proposition 2.1(1) the longest weak reverse trace is unique in both sets; it must be the same because $P_1 \approx_{\mathrm{RB}} P_2$):
  - If $n = 0$ then either P_1 and P_2 are initial, or due to Proposition 3.4 and Proposition 2.1(1) there exist $P_1' \Longrightarrow P_1$ and $P_2' \Longrightarrow P_2$, with P_1' and P_2' unique and initial (at most one of P_1 and P_2 stays idle and thus coincides with P_1' or P_2' respectively), such that $P_1' \approx_{\mathrm{RB}} P_2'$. In both cases $trace_{\mathrm{r,w}}(P_1) = \{\varepsilon\} = trace_{\mathrm{r,w}}(P_2)$.
  - Let $n > 0$ with the longest weak reverse trace being $a_n \ldots a_1 \in (\mathcal{A} \setminus \{\tau\})^*$. From $P_1 \approx_{\mathrm{RB}} P_2$, Proposition 3.4, and Proposition 2.1(1) it follows that there exist $P_1' \Longrightarrow \xrightarrow{\theta_1} \Longrightarrow P_1$ and $P_2' \Longrightarrow \xrightarrow{\theta_2} \Longrightarrow P_2$, with P_1' and P_2' unique, such that $act(\theta_1) = act(\theta_2) = a_n$ and $P_1' \approx_{\mathrm{RB}} P_2'$, hence $trace_{\mathrm{r,w}}(P_1') = trace_{\mathrm{r,w}}(P_2')$ by the induction hypothesis with $a_{n-1} \ldots a_1$ being the longest weak reverse trace in both sets. Therefore $trace_{\mathrm{r,w}}(P_1) = trace_{\mathrm{r,w}}(P_1') \cup \{a_n \ldots a_1\} = trace_{\mathrm{r,w}}(P_2') \cup \{a_n \ldots a_1\} = trace_{\mathrm{r,w}}(P_2)$.
- Assuming that $P_1 \approx_{\mathrm{RT}} P_2$, we prove that the symmetric relation $\mathcal{B} = \{(Q_1, Q_2) \in \mathbb{P}_{\mathrm{seq}} \times \mathbb{P}_{\mathrm{seq}} \mid trace_{\mathrm{r,w}}(Q_1) = trace_{\mathrm{r,w}}(Q_2)\}$ is a weak reverse bisimulation.
  Given $(Q_1, Q_2) \in \mathcal{B}$, there are two cases:
  - If $trace_{\mathrm{r,w}}(Q_1) = \{\varepsilon\} = trace_{\mathrm{r,w}}(Q_2)$ then from Proposition 3.4 and Proposition 2.1(1) it follows that there exist $Q_1' \Longrightarrow Q_1$ and $Q_2' \Longrightarrow Q_2$ with Q_1' and Q_2' unique. Therefore $trace_{\mathrm{r,w}}(Q_1') = trace_{\mathrm{r,w}}(Q_1) = trace_{\mathrm{r,w}}(Q_2) = trace_{\mathrm{r,w}}(Q_2')$ so that $(Q_1', Q_2') \in \mathcal{B}$.
  - If $trace_{\mathrm{r,w}}(Q_1) \neq \{\varepsilon\} \neq trace_{\mathrm{r,w}}(Q_2)$ then from $trace_{\mathrm{r,w}}(Q_1) = trace_{\mathrm{r,w}}(Q_2)$, Proposition 3.4, and Proposition 2.1(1) it follows that there exist $Q_1' \Longrightarrow \xrightarrow{\theta_1} \Longrightarrow Q_1$ and $Q_2' \Longrightarrow \xrightarrow{\theta_2} \Longrightarrow Q_2$ with Q_1' and Q_2' unique and $act(\theta_1) = act(\theta_2)$, where Q_1 and Q_2 have the same unique longest weak reverse trace σ starting with $act(\theta_1)$ and $act(\theta_2)$ respectively. Therefore $trace_{\mathrm{r,w}}(Q_1') = trace_{\mathrm{r,w}}(Q_1) \setminus \{\sigma\} = trace_{\mathrm{r,w}}(Q_2) \setminus \{\sigma\} = trace_{\mathrm{r,w}}(Q_2')$ so that $(Q_1', Q_2') \in \mathcal{B}$. ∎

Corollary 7.2. *Let $P_1, P_2 \in \mathbb{P}$. If $P_1 \approx_{\rm RB} P_2$ then $P_1 \approx_{\rm RT} P_2$.*

Proof. See the first part of the proof of Theorem 7.2, where:

- The longest weak reverse traces of P_1 and P_2 may be more than one as P_1 and P_2 are not necessarily sequential.
- When $n > 0$, from $P_1 \approx_{\rm RB} P_2$ it follows that, for each of the longest weak reverse traces $a_n \ldots a_1 \in (\mathcal{A} \setminus \{\tau\})^*$ of P_1 and P_2, there exist $P_1' \Longrightarrow \xrightarrow{\theta_1} \Longrightarrow P_1$ and $P_2' \Longrightarrow \xrightarrow{\theta_2} \Longrightarrow P_2$ such that $act(\theta_1) = act(\theta_2) = a_n$ and $P_1' \approx_{\rm RB} P_2'$, hence $trace_{\rm r,w}(P_1') = trace_{\rm r,w}(P_2')$ by the induction hypothesis with $a_{n-1} \ldots a_1$ being one of the longest weak reverse traces in both sets. Therefore $trace_{\rm r,w}(P_1) \supseteq trace_{\rm r,w}(P_1') \cup \{a_n \ldots a_1\} = trace_{\rm r,w}(P_2') \cup \{a_n \ldots a_1\} \subseteq trace_{\rm r,w}(P_2)$. ∎

7.1.2 Weak Forward-Reverse Bisimilarity and Branching Bisimilarity

Weak forward-reverse bisimilarity can be characterized in terms of branching bisimilarity [80]. Unlike the weak bisimilarity of [112], branching bisimilarity preserves the branching structure of processes even when abstracting from τ-actions, as can be seen from condition $(P_1, \bar{P}_2) \in \mathcal{B}$ in the definition below.

Definition 7.3. *We say that $P_1, P_2 \in \mathbb{P}$ are* branching bisimilar*, written $P_1 \approx_{\rm BB} P_2$, iff $(P_1, P_2) \in \mathcal{B}$ for some branching bisimulation $\mathcal{B}$. A symmetric relation $\mathcal{B}$ over $\mathbb{P}$ is a* branching bisimulation *iff, whenever $(P_1, P_2) \in \mathcal{B}$, then for each $P_1 \xrightarrow{\theta_1} P_1'$ it holds that:*

- *either $act(\theta_1) = \tau$ and $(P_1', P_2) \in \mathcal{B}$;*
- *or there exists $P_2 \Longrightarrow \bar{P}_2 \xrightarrow{\theta_2} P_2'$ such that $act(\theta_1) = act(\theta_2)$, $(P_1, \bar{P}_2) \in \mathcal{B}$, and $(P_1', P_2') \in \mathcal{B}$.* ∎

Branching bisimilarity is already known to have some relationships with reversibility. More precisely, in [57] strong and weak back-and-forth bisimilarities have been introduced over labeled transition systems and respectively shown to coincide with the strong bisimilarity of [112] and branching bisimilarity. However, in [57] strong and weak back-and-forth bisimilarities have been defined *over computation paths* rather than states, so that any backward computation is constrained to follow the same path as the corresponding forward computation even in the presence of concurrency, which is consistent with an interleaving view of parallel composition. This is quite different from our forward-reverse bisimilarity *over states* inspired by [121], which accounts for the fact that when going backward the order in which independent actions are undone may be different from the order in which they were executed in the forward direction, thus leading to a truly concurrent view of parallel composition.

To show the relationship between our weak forward-reverse bisimilarity and branching bisimilarity, we follow the same proof strategy adopted in [57] for weak back-and-forth bisimilarity. Thus, we need first of all an alternative definition of our weak forward-reverse bisimulation that is closer to the way in which weak back-and-forth bisimulation is defined, i.e., finite transition sequences have to be employed on both sides of the weak bisimulation game. This is provided by Proposition 3.5.

Secondly, as a sanity check we prove that, like branching bisimilarity, our weak forward-reverse bisimilarity satisfies the *stuttering property* [80]. This means that, given a sequence of finitely many τ-transitions, if the source process of the first transition and the target process of the last transition are equivalent to each other, then all the intermediate processes are equivalent to them too – see $P_2 \Longrightarrow \bar{P}_2$ in Definition 7.3 when P_1 and P_2 as well as P_1 and $\bar{P}_2$ are related by the maximal branching bisimulation $\approx_{\rm BB}$ and hence so are P_2 and $\bar{P}_2$. In other words, while traversing the considered sequence of τ-transitions, we remain in the same equivalence class of processes, not only in the forward direction but also in the backward direction as we are talking about weak forward-reverse bisimilarity.

Proposition 7.1. *Let $n \in \mathbb{N}_{>0}$, $P_i \in \mathbb{P}$ for all $0 \leq i \leq n$, and $P_i \xrightarrow{\theta_i} P_{i+1}$ with $act(\theta_i) = \tau$ for all $0 \leq i \leq n-1$. If $P_0 \approx_{\rm FRB} P_n$ then $P_i \approx_{\rm FRB} P_0$ for all $0 \leq i \leq n$.*

Proof. Consider the reflexive and symmetric relation $\mathcal{B} = \cup_{i \in \mathbb{N}} \mathcal{B}_i$ over $\mathbb{P}$ where:

- $\mathcal{B}_0 = \approx_{\rm FRB}$.
- $\mathcal{B}_i = \mathcal{B}_{i-1} \cup \{(P, P'), (P', P) \in \mathbb{P} \times \mathbb{P} \mid \exists P'' \in \mathbb{P}.\, (P, P'') \in \mathcal{B}_{i-1} \wedge P \Longrightarrow P' \xrightarrow{\theta} P'' \wedge act(\theta) = \tau\}$ for all $i \in \mathbb{N}_{>0}$.

We start by proving that $\mathcal{B}$ satisfies the stuttering property, i.e., given $n \in \mathbb{N}_{>0}$, $P_i \in \mathbb{P}$ for all $0 \leq i \leq n$, and $P_i \xrightarrow{\theta_i} P_{i+1}$ with $act(\theta_i) = \tau$ for all $0 \leq i \leq n-1$, if $(P_0, P_n) \in \mathcal{B}$ then $(P_i, P_0) \in \mathcal{B}$ for all $0 \leq i \leq n$. We proceed by induction on n:

- If $n = 1$ then the considered computation is simply $P_0 \xrightarrow{\theta_0} P_1$ with $act(\theta_0) = \tau$ and $(P_0, P_1) \in \mathcal{B}$, hence trivially $(P_i, P_0) \in \mathcal{B}$ for all $0 \leq i \leq 1$ as $\mathcal{B}$ is reflexive – so that $(P_0, P_0) \in \mathcal{B}$ – and symmetric – so that $(P_1, P_0) \in \mathcal{B}$.
- Let $n > 1$. Since $(P_0, P_n) \in \mathcal{B}$, there must exist $m \in \mathbb{N}$ such that $(P_0, P_n) \in \mathcal{B}_m$. Let us consider the smallest such m. Then $(P_0, P_{n-1}) \in \mathcal{B}_{m+1}$ by definition of $\mathcal{B}_{m+1}$, hence $(P_0, P_{n-1}) \in \mathcal{B}$. From the induction hypothesis it follows that $(P_i, P_0) \in \mathcal{B}$ for all $0 \leq i \leq n-1$, hence $(P_i, P_0) \in \mathcal{B}$ for all $0 \leq i \leq n$ because $(P_0, P_n) \in \mathcal{B}$ and $\mathcal{B}$ is symmetric – so that $(P_n, P_0) \in \mathcal{B}$.

We now prove that every symmetric relation $\mathcal{B}_i$ is a weak forward-reverse bisimulation. We proceed by induction on $i \in \mathbb{N}$:

- If $i = 0$ then $\mathcal{B}_i$ is the maximal weak forward-reverse bisimulation.
- Let $i \geq 1$ and suppose that $\mathcal{B}_{i-1}$ is a weak forward-reverse bisimulation. Given $(P, P') \in \mathcal{B}_i$, assume that $P \xrightarrow{\theta} Q$ (resp. $Q \xrightarrow{\theta} P$). There are two cases:
  - If $(P, P') \in \mathcal{B}_{i-1}$ then by the induction hypothesis there exists $P' \Longrightarrow Q'$ (resp. $Q' \Longrightarrow P'$) if $act(\theta) = \tau$ or $P' \Longrightarrow \xrightarrow{\theta'} \Longrightarrow Q'$ (resp. $Q' \Longrightarrow \xrightarrow{\theta'} \Longrightarrow P'$) with $act(\theta) = act(\theta')$ if $act(\theta) \neq \tau$, such that $(Q, Q') \in \mathcal{B}_{i-1}$ and hence $(Q, Q') \in \mathcal{B}_i$ as $\mathcal{B}_{i-1} \subseteq \mathcal{B}_i$ by definition of $\mathcal{B}_i$.
  - If instead $(P, P') \notin \mathcal{B}_{i-1}$ then from $(P, P') \in \mathcal{B}_i$ it follows that there exists $P'' \in \mathbb{P}$ such that $(P, P'') \in \mathcal{B}_{i-1}$, $P \Longrightarrow P' \xrightarrow{\theta''} P''$, and $act(\theta'') = \tau$. There are two subcases:

- In the forward subcase, i.e., $P \xrightarrow{\theta} Q$, there are two further subcases:
  - If $(Q, P'') \in \mathcal{B}_{i-1}$ and $act(\theta) = \tau$, then from $P' \xrightarrow{\theta''} P''$ with $act(\theta'') = \tau$ it follows that $P' \Longrightarrow P''$ with $(Q, P'') \in \mathcal{B}_{i-1}$ and hence $(Q, P'') \in \mathcal{B}_i$ as $\mathcal{B}_{i-1} \subseteq \mathcal{B}_i$.
  - Otherwise from $(P, P'') \in \mathcal{B}_{i-1}$ and the induction hypothesis it follows that there exists $P'' \Longrightarrow \xrightarrow{\theta'''} \Longrightarrow P'''$ such that $act(\theta) = act(\theta''')$ and $(Q, P''') \in \mathcal{B}_{i-1}$, so that $P' \Longrightarrow \xrightarrow{\theta'''} \Longrightarrow P'''$ with $(Q, P''') \in \mathcal{B}_{i-1}$ and hence $(Q, P''') \in \mathcal{B}_i$ as $\mathcal{B}_{i-1} \subseteq \mathcal{B}_i$.
- In the backward subcase, i.e., $Q \xrightarrow{\theta} P$, it suffices to note that from $P \Longrightarrow P'$ it follows that $Q \xrightarrow{\theta} \Longrightarrow P'$.

Since $\mathcal{B}$ is the union of countably many weak forward-reverse bisimulations among which there is $\approx_{\rm FRB}$, it holds that $\mathcal{B} \subseteq \approx_{\rm FRB}$. On the other hand, $\approx_{\rm FRB} \subseteq \mathcal{B}$ by definition of $\mathcal{B}_0$. In conclusion $\mathcal{B} = \approx_{\rm FRB}$ – i.e., no relation $\mathcal{B}_i$ for $i \in \mathbb{N}_{>0}$ adds further pairs with respect to $\mathcal{B}_0$ – and hence $\approx_{\rm FRB}$ satisfies the stuttering property because so does $\mathcal{B}$. ∎

The stuttering property does not hold for $\approx_{\rm FRB:ps}$ when P_0 is initial, because in that case a τ-action would be decorated inside P_1 and hence $P_1 \not\approx_{\rm FRB:ps} P_0$. Therefore $\approx_{\rm FRB:ps}$ satisfies the stuttering property only over non-initial processes.

Thirdly, we prove that $\approx_{\rm FRB}$ satisfies the *cross property* [57]. This means that, whenever two processes can perform a sequence of finitely many τ-transitions such that each of the two target processes is $\approx_{\rm FRB}$-equivalent to the source process of the other sequence, then the two target processes are $\approx_{\rm FRB}$-equivalent to each other as well. Unlike [57], we do not require the two source processes to be reachable from two $\approx_{\rm FRB}$-equivalent processes.

Lemma 7.1. *For all $P_1', P_1'' \in \mathbb{P}$ such that $P_1' \Longrightarrow P_1''$ and for all $P_2', P_2'' \in \mathbb{P}$ such that $P_2' \Longrightarrow P_2''$, if $P_1' \approx_{\rm FRB} P_2''$ and $P_1'' \approx_{\rm FRB} P_2'$ then $P_1'' \approx_{\rm FRB} P_2''$.*

Proof. Consider the symmetric relation $\mathcal{B} = \approx_{\rm FRB} \cup \{(P_1'', P_2''), (P_2'', P_1'') \in \mathbb{P} \times \mathbb{P} \mid \exists P_1', P_2' \in \mathbb{P}.\ P_1' \Longrightarrow P_1'' \wedge P_2' \Longrightarrow P_2'' \wedge P_1' \approx_{\rm FRB} P_2'' \wedge P_1'' \approx_{\rm FRB} P_2'\}$. The result follows by proving that $\mathcal{B}$ is a weak forward-reverse bisimulation, because this implies that $P_1'' \approx_{\rm FRB} P_2''$ for every additional pair – i.e., $\mathcal{B}$ satisfies the cross property – as well as $\mathcal{B} = \approx_{\rm FRB}$ – hence $\approx_{\rm FRB}$ satisfies the cross property too.
Let $(P_1'', P_2'') \in \mathcal{B} \setminus \approx_{\rm FRB}$ to avoid trivial cases. Then there exist $P_1', P_2' \in \mathbb{P}$ such that $P_1' \Longrightarrow P_1''$, $P_2' \Longrightarrow P_2''$, $P_1' \approx_{\rm FRB} P_2''$, and $P_1'' \approx_{\rm FRB} P_2'$. There are two cases:

- In the forward case, assume that $P_1'' \xrightarrow{\theta_1} P_1'''$, from which we derive $P_1' \Longrightarrow P_1'' \xrightarrow{\theta_1} P_1'''$. Since $P_1' \approx_{\rm FRB} P_2''$, from Proposition 3.5 it follows that there exists $P_2'' \Longrightarrow P_2'''$ if $act(\theta_1) = \tau$ or $P_2'' \Longrightarrow \xrightarrow{\theta_2} \Longrightarrow P_2'''$ with $act(\theta_1) = act(\theta_2)$ if $act(\theta_1) \neq \tau$, such that $P_1''' \approx_{\rm FRB} P_2'''$ and hence $(P_1''', P_2''') \in \mathcal{B}$.
  When starting from $P_2'' \xrightarrow{\theta_2} P_2'''$, we exploit $P_2' \Longrightarrow P_2''$ and $P_1'' \approx_{\rm FRB} P_2'$ instead.
- In the backward case, assume that $P_1''' \xrightarrow{\theta_1} P_1''$. From $P_1'' \approx_{\rm FRB} P_2'$ it follows that there exists $P_2''' \Longrightarrow P_2'$ if $act(\theta_1) = \tau$, so that $P_2''' \Longrightarrow P_2''$ as $P_2' \Longrightarrow P_2''$, or $P_2''' \Longrightarrow \xrightarrow{\theta_2} \Longrightarrow P_2'$ with $act(\theta_1) = act(\theta_2)$ if $act(\theta_1) \neq \tau$, so that $P_2''' \Longrightarrow \xrightarrow{\theta_2} \Longrightarrow P_2''$ as $P_2' \Longrightarrow P_2''$, such that $P_1''' \approx_{\rm FRB} P_2'''$ and hence $(P_1''', P_2''') \in \mathcal{B}$.
  When starting from $P_2''' \xrightarrow{\theta_2} P_2''$, we exploit $P_1' \approx_{\rm FRB} P_2''$ and $P_1' \Longrightarrow P_1''$ instead. ∎

We are now in a position of proving that $\approx_{\rm FRB}$ coincides with $\approx_{\rm BB}$. This holds only over initial processes though. For instance, $a_1^\dagger . b . P \approx_{\rm BB} a_2^\dagger . b . P$ but $a_1^\dagger . b . P \not\approx_{\rm FRB} a_2^\dagger . b . P$ when $a_1 \neq a_2$. Moreover, consistent with the aforementioned interleaving view under which weak back-and-forth bisimilarity has been shown to coincide with branching bisimilarity in [57], our result holds only over sequential processes. As an example, $a . \underline{0} \parallel_\emptyset b . \underline{0} \approx_{\rm BB} a . b . \underline{0} + b . a . \underline{0}$ as shown by the branching bisimilarity arising from the symmetric closure of relation $\{(a . \underline{0} \parallel_\emptyset b . \underline{0}, a . b . \underline{0} + b . a . \underline{0}), (a^\dagger . \underline{0} \parallel_\emptyset b . \underline{0}, a^\dagger . b . \underline{0} + b . a . \underline{0}), (a . \underline{0} \parallel_\emptyset b^\dagger . \underline{0}, a . b . \underline{0} + b^\dagger . a . \underline{0}), (a^\dagger . \underline{0} \parallel_\emptyset b^\dagger . \underline{0}, a^\dagger . b^\dagger . \underline{0} + b . a . \underline{0}), (a^\dagger . \underline{0} \parallel_\emptyset b^\dagger . \underline{0}, a . b . \underline{0} + b^\dagger . a^\dagger . \underline{0})\}$. In contrast, $a . \underline{0} \parallel_\emptyset b . \underline{0} \not\approx_{\rm FRB} a . b . \underline{0} + b . a . \underline{0}$ when $a \neq b$. The reason is that $a^\dagger . \underline{0} \parallel_\emptyset b^\dagger . \underline{0}$ has two differently labeled incoming transitions while $a^\dagger . b^\dagger . \underline{0} + b . a . \underline{0}$ and $a . b . \underline{0} + b^\dagger . a^\dagger . \underline{0}$ have only one incoming transition each, hence $a^\dagger . \underline{0} \parallel_\emptyset b . \underline{0} \not\approx_{\rm FRB} a^\dagger . b . \underline{0} + b . a . \underline{0}$ and $a . \underline{0} \parallel_\emptyset b^\dagger . \underline{0} \not\approx_{\rm FRB} a . b . \underline{0} + b^\dagger . a . \underline{0}$ as their identically labeled outgoing transitions reach inequivalent processes, which in turn implies that $a . \underline{0} \parallel_\emptyset b . \underline{0} \not\approx_{\rm FRB} a . b . \underline{0} + b . a . \underline{0}$ as their identically labeled outgoing transitions reach inequivalent processes (see Figure 1.1).

As another example, $a . (\tau . \underline{0} + b . \underline{0}) \approx_{\rm FRB} ((a . (\tau . \underline{0} + b . \underline{0}) + a . c . \underline{0}) \parallel_{\{c\}} (\tau . \underline{0} + c . \underline{0})) \llcorner c \mapsto b \urcorner$. This can be seen by playing the weak forward-reverse bisimulation game with the subprocesses of the latter process that do not occur in the former. If the latter process performs the rightmost a thus evolving to $((a . (\tau . \underline{0} + b . \underline{0}) + a^\dagger . c . \underline{0}) \parallel_{\{c\}} (\tau . \underline{0} + c . \underline{0})) \llcorner c \mapsto b \urcorner$, where only either τ or the synchronization on c then changed to b can be performed, the former responds with a thus becoming $a^\dagger . (\tau . \underline{0} + b . \underline{0})$, with the two reached processes being $\approx_{\rm FRB}$-equivalent. If instead the latter process performs τ and then the rightmost a thus evolving to $((a . (\tau . \underline{0} + b . \underline{0}) + a^\dagger . c . \underline{0}) \parallel_{\{c\}} (\tau^\dagger . \underline{0} + c . \underline{0})) \llcorner c \mapsto b \urcorner$, where no further action can be performed, the former responds by staying idle and then with a followed by τ thus becoming $a^\dagger . (\tau^\dagger . \underline{0} + b . \underline{0})$, with the two reached processes being $\approx_{\rm FRB}$-equivalent even if the former can undo a and τ in any order whereas the latter can undo a only after undoing τ. In contrast, $a . (\tau . \underline{0} + b . \underline{0}) \not\approx_{\rm BB} ((a . (\tau . \underline{0} + b . \underline{0}) + a . c . \underline{0}) \parallel_{\{c\}} (\tau . \underline{0} + c . \underline{0})) \llcorner c \mapsto b \urcorner$. The reason is that $((a . (\tau . \underline{0} + b . \underline{0}) + a^\dagger . c . \underline{0}) \parallel_{\{c\}} (\tau^\dagger . \underline{0} + c . \underline{0})) \llcorner c \mapsto b \urcorner$, reached after performing τ and then the rightmost a, cannot be matched by $a^\dagger . (\tau . \underline{0} + b . \underline{0})$, reached after staying idle and then performing a (recall that in the $\approx_{\rm BB}$-response a cannot be followed by τ – it could be if the equivalence class did not change [80]), because the latter can perform b whereas the former cannot. Summing up, $\approx_{\rm FRB}$ and $\approx_{\rm BB}$ turn out to be incomparable over non-sequential processes.

Theorem 7.3. *Let* $P_1, P_2 \in \mathbb{P}_{\rm seq} \cap \mathbb{P}_{\rm init}$. *Then* $P_1 \approx_{\rm FRB} P_2$ *iff* $P_1 \approx_{\rm BB} P_2$.

Proof. The proof is divided into two parts:

- Suppose that $P_1 \approx_{\rm FRB} P_2$ and let $\mathcal{B}$ be a weak forward-reverse bisimulation such that $(P_1, P_2) \in \mathcal{B}$. Assume that $\mathcal{B}$ only contains all the pairs of $\approx_{\rm FRB}$-equivalent processes reachable from P_1 and P_2, so that Lemma 7.1 is applicable to $\mathcal{B}$. We show that $\mathcal{B}$ is a branching bisimulation too, from which $P_1 \approx_{\rm BB} P_2$ will follow.
  Given $(Q_1, Q_2) \in \mathcal{B}$, with Q_1 and Q_2 respectively reachable from P_1 and P_2, suppose that $Q_1 \xrightarrow{\theta_1} Q_1'$. There are two cases:
  - If $act(\theta_1) = \tau$ then from $(Q_1, Q_2) \in \mathcal{B}$ it follows that there exists $Q_2 \Longrightarrow Q_2'$ such that $(Q_1', Q_2') \in \mathcal{B}$. This means that we have a sequence of $n \geq 0$ transitions of the form $Q_{2,i} \xrightarrow{\theta_{2,i}} Q_{2,i+1}$ with $act(\theta_{2,i}) = \tau$ for all $0 \leq i \leq n-1$, where $Q_{2,0}$ is Q_2 while $Q_{2,n}$ is Q_2' so that $(Q_1', Q_{2,n}) \in \mathcal{B}$ as $(Q_1', Q_2') \in \mathcal{B}$.
    If $n = 0$ then we are done because Q_2' is Q_2 and hence $(Q_1', Q_2) \in \mathcal{B}$ as $(Q_1', Q_2') \in \mathcal{B}$, otherwise from $Q_{2,n}$ we go back to $Q_{2,n-1}$ via $Q_{2,n-1} \xrightarrow{\theta_{2,n-1}} Q_{2,n}$ with $act(\theta_{2,n-1}) = \tau$. Recalling that $(Q_1', Q_{2,n}) \in \mathcal{B}$,

if Q'_1 can respond by staying idle, so that $(Q'_1, Q_{2,n-1}) \in \mathcal{B}$, and $n = 1$, then we are done because $Q_{2,n-1}$ is Q_2 and hence $(Q'_1, Q_2) \in \mathcal{B}$ as $(Q'_1, Q_{2,n-1}) \in \mathcal{B}$, otherwise we go further back to $Q_{2,n-2}$ via $Q_{2,n-2} \xrightarrow{\theta_{2,n-2}} Q_{2,n-1}$ with $act(\theta_{2,n-2}) = \tau$ and consider $Q_{2,n-2} \Longrightarrow Q_{2,n}$. If Q'_1 can respond by staying idle, so that $(Q'_1, Q_{2,n-2}) \in \mathcal{B}$, and $n = 2$, then by virtue of Proposition 3.5 we are done because $Q_{2,n-2}$ is Q_2 and hence $(Q'_1, Q_2) \in \mathcal{B}$ as $(Q'_1, Q_{2,n-2}) \in \mathcal{B}$, otherwise we keep going backward.
By repeating this procedure, since $(Q'_1, Q_{2,n}) \in \mathcal{B}$ either we get to $(Q'_1, Q_{2,n-n}) \in \mathcal{B}$ and we are done because this implies that $(Q'_1, Q_2) \in \mathcal{B}$, or for some $0 < m \leq n$ such that $(Q'_1, Q_{2,m}) \in \mathcal{B}$ the incoming transition $Q_{2,m-1} \xrightarrow{\theta_{2,m-1}} Q_{2,m}$ with $act(\theta_{2,m-1}) = \tau$ is matched by $\bar{Q}_1 \Longrightarrow Q_1 \xrightarrow{\theta_1} Q'_1$ with $(\bar{Q}_1, Q_{2,m-1}) \in \mathcal{B}$, where by virtue of Proposition 2.1(1) $Q_1 \xrightarrow{\theta_1} Q'_1$ is the only incoming transition of Q'_1 as we are considering sequential processes. In the latter case, since $\bar{Q}_1 \Longrightarrow Q_1$, $Q_2 \Longrightarrow Q_{2,m-1}$, $(\bar{Q}_1, Q_{2,m-1}) \in \mathcal{B}$, $(Q_1, Q_2) \in \mathcal{B}$, all these processes are reachable from P_1 and P_2, and $\mathcal{B}$ is the restriction of $\approx_{\rm FRB}$ to the set of processes reachable from P_1 and P_2, from Lemma 7.1 we derive that $(Q_1, Q_{2,m-1}) \in \mathcal{B}$. Consequently $Q_2 \Longrightarrow Q_{2,m-1} \xrightarrow{\theta_{2,m-1}} Q_{2,m}$ with $act(\theta_1) = act(\theta_{2,m-1})$, $(Q_1, Q_{2,m-1}) \in \mathcal{B}$, and $(Q'_1, Q_{2,m}) \in \mathcal{B}$.

- If $act(\theta_1) \neq \tau$ then from $(Q_1, Q_2) \in \mathcal{B}$ it follows that there exists $Q_2 \Longrightarrow \bar{Q}_2 \xrightarrow{\theta_2} \bar{Q}'_2 \Longrightarrow Q'_2$ such that $act(\theta_1) = act(\theta_2)$ and $(Q'_1, Q'_2) \in \mathcal{B}$.
From $(Q'_1, Q'_2) \in \mathcal{B}$, $\bar{Q}'_2 \Longrightarrow Q'_2$, and Proposition 3.5 it follows that there exists $\bar{Q}'_1 \Longrightarrow Q'_1$ such that $(\bar{Q}'_1, \bar{Q}'_2) \in \mathcal{B}$. Since Q'_1 already has an incoming $act(\theta_1)$-transition from Q_1 and every non-initial sequential process has exactly one incoming transition due to Proposition 2.1(1), we derive that $\bar{Q}'_1$ is Q'_1 due to $act(\theta_1) \neq \tau$ and hence $(Q'_1, \bar{Q}'_2) \in \mathcal{B}$.
From $(Q'_1, \bar{Q}'_2) \in \mathcal{B}$ and $\bar{Q}_2 \xrightarrow{\theta_2} \bar{Q}'_2$ it follows that there exists $\bar{Q}_1 \Longrightarrow Q_1 \xrightarrow{\theta_1} Q'_1$ such that $(\bar{Q}_1, \bar{Q}_2) \in \mathcal{B}$. Since $\bar{Q}_1 \Longrightarrow Q_1$, $Q_2 \Longrightarrow \bar{Q}_2$, $(\bar{Q}_1, \bar{Q}_2) \in \mathcal{B}$, $(Q_1, Q_2) \in \mathcal{B}$, all these processes are reachable from P_1 and P_2, and $\mathcal{B}$ is the restriction of $\approx_{\rm FRB}$ to the set of processes reachable from P_1 and P_2, from Lemma 7.1 we derive that $(Q_1, \bar{Q}_2) \in \mathcal{B}$.
Consequently $Q_2 \Longrightarrow \bar{Q}_2 \xrightarrow{\theta_2} \bar{Q}'_2$ with $act(\theta_1) = act(\theta_2)$, $(Q_1, \bar{Q}_2) \in \mathcal{B}$, and $(Q'_1, \bar{Q}'_2) \in \mathcal{B}$.

- Suppose that $P_1 \approx_{\rm BB} P_2$ and let $\mathcal{B}$ be a branching bisimulation such that $(P_1, P_2) \in \mathcal{B}$. Assume that $\mathcal{B}$ only contains all the pairs of $\approx_{\rm BB}$-equivalent processes reachable from P_1 and P_2. We show that $\mathcal{B}$ is a weak forward-reverse bisimulation too, from which $P_1 \approx_{\rm FRB} P_2$ will follow.
Given $(Q_1, Q_2) \in \mathcal{B}$, with Q_1 and Q_2 respectively reachable from P_1 and P_2, there are two cases:

  - In the forward case, assume that $Q_1 \xrightarrow{\theta_1} Q'_1$. From $(Q_1, Q_2) \in \mathcal{B}$ it follows that either $act(\theta_1) = \tau$ and $(Q'_1, Q_2) \in \mathcal{B}$, hence $Q_2 \Longrightarrow Q_2$ with $(Q'_1, Q_2) \in \mathcal{B}$, or there exists $Q_2 \Longrightarrow \bar{Q}_2 \xrightarrow{\theta_2} Q'_2$ such that $act(\theta_1) = act(\theta_2)$, $(Q_1, \bar{Q}_2) \in \mathcal{B}$, and $(Q'_1, Q'_2) \in \mathcal{B}$, hence $Q_2 \Longrightarrow Q'_2$ if $act(\theta_1) = \tau$ or $Q_2 \Longrightarrow \xrightarrow{\theta_2} \Longrightarrow Q'_2$ with $act(\theta_1) = act(\theta_2)$ if $act(\theta_1) \neq \tau$, where $(Q'_1, Q'_2) \in \mathcal{B}$.
  - In the backward case – in which $(Q_1, Q_2) \neq (P_1, P_2)$ as P_1 and P_2 are both initial – assume that $Q'_1 \xrightarrow{\theta_1} Q_1$. There are two subcases:
    * If Q'_1 is P_1 then from $(Q_1, Q_2) \in \mathcal{B}$ it follows that either $act(\theta_1) = \tau$ and $(Q'_1, Q_2) \in \mathcal{B}$, where Q_2 is P_2 and $Q_2 \Longrightarrow Q_2$, or there exists $Q'_2 \Longrightarrow \bar{Q}_2 \xrightarrow{\theta_2} Q_2$ such that $act(\theta_1) = act(\theta_2)$, $(Q'_1, \bar{Q}_2) \in \mathcal{B}$, and $(Q'_1, Q'_2) \in \mathcal{B}$, where Q'_2 is P_2 – due to Proposition 2.1(1) – and $Q'_2 \Longrightarrow Q_2$ if $act(\theta_1) = \tau$ or $Q'_2 \Longrightarrow \xrightarrow{\theta_2} \Longrightarrow Q_2$ if $act(\theta_1) \neq \tau$.

∗ If Q_1' is not P_1 then from $(Q_1, Q_2) \in \mathcal{B}$ it follows that P_1 reaches Q_1' with a sequence of transitions that are $\mathcal{B}$-compatible with those with which P_2 reaches some Q_2' such that $(Q_1', Q_2') \in \mathcal{B}$ as the pairs in $\mathcal{B}$ contains all the processes reachable from P_1 and P_2. Therefore either $act(\theta_1) = \tau$ and $(Q_1, Q_2') \in \mathcal{B}$, where Q_2' is Q_2 and $Q_2 \Longrightarrow Q_2$, or there exists $Q_2' \Longrightarrow \bar{Q}_2 \xrightarrow{\theta_2} Q_2$ such that $act(\theta_1) = act(\theta_2)$ and $(Q_1', \bar{Q}_2) \in \mathcal{B}$ in addition to $(Q_1', Q_2') \in \mathcal{B}$ and $(Q_1, Q_2) \in \mathcal{B}$, where $Q_2' \Longrightarrow Q_2$ if $act(\theta_1) = \tau$ or $Q_2' \Longrightarrow \xrightarrow{\theta_2} \Longrightarrow Q_2$ if $act(\theta_1) \neq \tau$. ■

We conclude by studying the relationship between $\approx_{\rm FRB}$ and the following forward-reverse variant of branching bisimilarity, which is inspired by the back-and-forth branching bisimilarity mentioned in [57].

Definition 7.4. *We say that $P_1, P_2 \in \mathbb{P}$ are* forward-reverse branching bisimilar*, written $P_1 \approx_{\rm FRBB} P_2$, iff $(P_1, P_2) \in \mathcal{B}$ for some forward-reverse branching bisimulation $\mathcal{B}$. A symmetric relation $\mathcal{B}$ over $\mathbb{P}$ is a* forward-reverse branching bisimulation *iff, whenever $(P_1, P_2) \in \mathcal{B}$, then:*

- *For each $P_1 \xrightarrow{\theta_1} P_1'$ it holds that:*
  - *either $act(\theta_1) = \tau$ and $(P_1', P_2) \in \mathcal{B}$;*
  - *or there exists $P_2 \Longrightarrow \bar{P}_2 \xrightarrow{\theta_2} P_2'$ such that $act(\theta_1) = act(\theta_2)$, $(P_1, \bar{P}_2) \in \mathcal{B}$, and $(P_1', P_2') \in \mathcal{B}$.*
- *For each $P_1' \xrightarrow{\theta_1} P_1$ it holds that:*
  - *either $act(\theta_1) = \tau$ and $(P_1', P_2) \in \mathcal{B}$;*
  - *or there exists $P_2' \xrightarrow{\theta_2} \bar{P}_2 \Longrightarrow P_2$ such that $act(\theta_1) = act(\theta_2)$, $(P_1, \bar{P}_2) \in \mathcal{B}$, and $(P_1', P_2') \in \mathcal{B}$.* ■

Similar to [57], where branching bisimilarity has been shown to coincide with back-and-forth branching bisimilarity defined over computation paths, here we prove that $\approx_{\rm FRB}$ coincides with $\approx_{\rm FRBB}$. Our result holds only over sequential processes. For example, $a \,.\, (\tau \,.\, \underline{0} + b \,.\, \underline{0})$ and $((a \,.\, (\tau \,.\, \underline{0} + b \,.\, \underline{0}) + a \,.\, c \,.\, \underline{0}) \parallel_{\{c\}} (\tau \,.\, \underline{0} + c \,.\, \underline{0})) \llcorner c \mapsto b \urcorner$, which we have already examined right before Theorem 7.3, are identified by $\approx_{\rm FRB}$ but told apart by $\approx_{\rm FRBB}$. Unlike Theorem 7.3, there is no limitation to initial processes though.

Theorem 7.4. *Let $P_1, P_2 \in \mathbb{P}_{\rm seq}$. Then $P_1 \approx_{\rm FRB} P_2$ iff $P_1 \approx_{\rm FRBB} P_2$.*

Proof. The proof is divided into two parts:

- Suppose that $P_1 \approx_{\rm FRB} P_2$ and let $\mathcal{B}$ be a weak forward-reverse bisimulation such that $(P_1, P_2) \in \mathcal{B}$. Assume that $\mathcal{B}$ only contains all the pairs of $\approx_{\rm FRB}$-equivalent processes reachable from P_1 and P_2 or reaching them, so that Lemma 7.1 is applicable to $\mathcal{B}$. We show that $\mathcal{B}$ is a forward-reverse branching bisimulation too, from which $P_1 \approx_{\rm FRBB} P_2$ will follow.
  Given $(Q_1, Q_2) \in \mathcal{B}$, with Q_1 and Q_2 respectively reachable from P_1 and P_2 or reaching them, suppose that $Q_1 \xrightarrow{\theta_1} Q_1'$. There are two cases:
  - If $Q_1 \xrightarrow{\theta_1} Q_1'$ then we proceed like in the first part of the proof of Theorem 7.3, where $\mathcal{B}$ is the restriction of $\approx_{\rm FRB}$ to the set of processes reachable from P_1 and P_2 or reaching them.

– If $Q_1' \xrightarrow{\theta_1} Q_1$ there are two cases:

∗ If $act(\theta_1) = \tau$ then from $(Q_1, Q_2) \in \mathcal{B}$ it follows that there exists $Q_2' \Longrightarrow Q_2$ such that $(Q_1', Q_2') \in \mathcal{B}$.
This means that we have a sequence of $n \geq 0$ transitions of the form $Q_{2,i} \xrightarrow{\theta_{2,i}} Q_{2,i+1}$ with $act(\theta_{2,i}) = \tau$ for all $0 \leq i \leq n-1$, where $Q_{2,0}$ is Q_2' while $Q_{2,n}$ is Q_2 so that $(Q_1, Q_{2,n}) \in \mathcal{B}$ as $(Q_1, Q_2) \in \mathcal{B}$.
If $n = 0$ then we are done because Q_2' is Q_2 and hence $(Q_1', Q_2) \in \mathcal{B}$ as $(Q_1', Q_2') \in \mathcal{B}$, otherwise from $Q_{2,n}$ we go back to $Q_{2,n-1}$ via $Q_{2,n-1} \xrightarrow{\theta_{2,n-1}} Q_{2,n}$ with $act(\theta_{2,n-1}) = \tau$. Recalling that $(Q_1, Q_{2,n}) \in \mathcal{B}$, if Q_1 can respond by staying idle, so that $(Q_1, Q_{2,n-1}) \in \mathcal{B}$, and $n = 1$, then we are done because $Q_{2,n-1}$ is Q_2' so that $(Q_1, Q_2') \in \mathcal{B}$ as $(Q_1, Q_{2,n-1}) \in \mathcal{B}$ and hence $(Q_1', Q_2) \in \mathcal{B}$ as $(Q_1', Q_2') \in \mathcal{B}$, $(Q_2', Q_1) \in \mathcal{B}$, $(Q_1, Q_2) \in \mathcal{B}$, and $\mathcal{B}$ is transitive due to the pairs it contains, otherwise we go further back to $Q_{2,n-2}$ via $Q_{2,n-2} \xrightarrow{\theta_{2,n-2}} Q_{2,n-1}$ with $act(\theta_{2,n-2}) = \tau$ and consider $Q_{2,n-2} \Longrightarrow Q_{2,n}$. If Q_1 can respond by staying idle, so that $(Q_1, Q_{2,n-2}) \in \mathcal{B}$, and $n = 2$, then by virtue of Proposition 3.5 we are done because $Q_{2,n-2}$ is Q_2' so that $(Q_1, Q_2') \in \mathcal{B}$ as $(Q_1, Q_{2,n-2}) \in \mathcal{B}$ and hence $(Q_1', Q_2) \in \mathcal{B}$ as $(Q_1', Q_2') \in \mathcal{B}$, $(Q_2', Q_1) \in \mathcal{B}$, $(Q_1, Q_2) \in \mathcal{B}$, and $\mathcal{B}$ is transitive due to the pairs it contains, otherwise we keep going backward.
By repeating this procedure, since $(Q_1, Q_{2,n}) \in \mathcal{B}$ either we get to $(Q_1, Q_{2,n-n}) \in \mathcal{B}$ and we are done because this implies that $(Q_1', Q_2) \in \mathcal{B}$, or for some $0 < m \leq n$ such that $(Q_1, Q_{2,m}) \in \mathcal{B}$ the incoming transition $Q_{2,m-1} \xrightarrow{\theta_{2,m-1}} Q_{2,m}$ with $act(\theta_{2,m-1}) = \tau$ is matched by $\bar{Q}_1 \Longrightarrow Q_1' \xrightarrow{\theta_1} Q_1$ with $(\bar{Q}_1, Q_{2,m-1}) \in \mathcal{B}$, where by virtue of Proposition 2.1(1) $Q_1' \xrightarrow{\theta_1} Q_1$ is the only incoming transition of Q_1 as we are considering sequential processes. In the latter case, since $\bar{Q}_1 \Longrightarrow Q_1'$, $Q_2' \Longrightarrow Q_{2,m-1}$, $(\bar{Q}_1, Q_{2,m-1}) \in \mathcal{B}$, $(Q_1', Q_2') \in \mathcal{B}$, all these processes are reachable from P_1 and P_2 or reach them, and $\mathcal{B}$ is the restriction of $\approx_{\rm FRB}$ to the set of processes reachable from P_1 and P_2 or reaching them, from Lemma 7.1 we derive that $(Q_1', Q_{2,m-1}) \in \mathcal{B}$. Consequently $Q_{2,m-1} \xrightarrow{\theta_{2,m-1}} Q_{2,m} \Longrightarrow Q_2$ with $act(\theta_1) = act(\theta_{2,m-1})$, $(Q_1, Q_{2,m}) \in \mathcal{B}$, and $(Q_1', Q_{2,m-1}) \in \mathcal{B}$.

∗ If $act(\theta_1) \neq \tau$ then from $(Q_1, Q_2) \in \mathcal{B}$ it follows that there exists $Q_2' \Longrightarrow \bar{Q}_2' \xrightarrow{\theta_2} \bar{Q}_2 \Longrightarrow Q_2$ such that $act(\theta_1) = act(\theta_2)$ and $(Q_1', Q_2') \in \mathcal{B}$.
From $(Q_1, Q_2) \in \mathcal{B}$, $\bar{Q}_2 \Longrightarrow Q_2$, and Proposition 3.5 it follows that there exists $\bar{Q}_1 \Longrightarrow Q_1$ such that $(\bar{Q}_1, \bar{Q}_2) \in \mathcal{B}$. Since Q_1 already has an incoming $act(\theta_1)$-transition from Q_1' and every non-initial sequential process has exactly one incoming transition due to Proposition 2.1(1), we derive that $\bar{Q}_1$ is Q_1 due to $act(\theta_1) \neq \tau$ and hence $(Q_1, \bar{Q}_2) \in \mathcal{B}$.
From $(Q_1, \bar{Q}_2) \in \mathcal{B}$ and $\bar{Q}_2' \xrightarrow{\theta_2} \bar{Q}_2$ it follows that there exists $\bar{Q}_1' \Longrightarrow Q_1' \xrightarrow{\theta_1} Q_1$ such that $(\bar{Q}_1', \bar{Q}_2') \in \mathcal{B}$.
Since $\bar{Q}_1' \Longrightarrow Q_1'$, $Q_2' \Longrightarrow \bar{Q}_2'$, $(\bar{Q}_1', \bar{Q}_2') \in \mathcal{B}$, $(Q_1', Q_2') \in \mathcal{B}$, all these processes are reachable from P_1 and P_2 or reach them, and $\mathcal{B}$ is the restriction of $\approx_{\rm FRB}$ to the set of processes reachable from P_1 and P_2 or reaching them, from Lemma 7.1 we derive that $(Q_1', \bar{Q}_2') \in \mathcal{B}$.
Consequently $\bar{Q}_2' \xrightarrow{\theta_2} \bar{Q}_2 \Longrightarrow Q_2$ with $act(\theta_1) = act(\theta_2)$, $(Q_1, \bar{Q}_2) \in \mathcal{B}$, and $(Q_1', \bar{Q}_2') \in \mathcal{B}$.

- Suppose that $P_1 \approx_{\rm FRBB} P_2$ and let $\mathcal{B}$ be a forward-reverse branching bisimulation such that $(P_1, P_2) \in \mathcal{B}$. We show that $\mathcal{B}$ is a weak forward-reverse bisimulation too, from which $P_1 \approx_{\rm FRB} P_2$ will follow.
Given $(Q_1, Q_2) \in \mathcal{B}$, there are two cases:

– If $Q_1 \xrightarrow{\theta_1} Q_1'$ there are two subcases:
  * If $act(\theta_1) = \tau$ and $(Q_1', Q_2) \in \mathcal{B}$, then $Q_2 \Longrightarrow Q_2$ with $(Q_1', Q_2) \in \mathcal{B}$.
  * If there exists $Q_2 \Longrightarrow \bar{Q}_2 \xrightarrow{\theta_2} Q_2'$ such that $act(\theta_1) = act(\theta_2)$, $(Q_1, \bar{Q}_2) \in \mathcal{B}$, and $(Q_1', Q_2') \in \mathcal{B}$, then $Q_2 \Longrightarrow Q_2'$ if $act(\theta_1) = \tau$ or $Q_2 \Longrightarrow \xrightarrow{\theta_2} \Longrightarrow Q_2'$ with $act(\theta_1) = act(\theta_2)$ if $act(\theta_1) \neq \tau$, where $(Q_1', Q_2') \in \mathcal{B}$.

– If $Q_1' \xrightarrow{\theta_1} Q_1$ there are two subcases:
  * If $act(\theta_1) = \tau$ and $(Q_1', Q_2) \in \mathcal{B}$, then $Q_2 \Longrightarrow Q_2$ with $(Q_1', Q_2) \in \mathcal{B}$.
  * If there exists $Q_2' \xrightarrow{\theta_2} \bar{Q}_2 \Longrightarrow Q_2$ such that $act(\theta_1) = act(\theta_2)$, $(Q_1, \bar{Q}_2) \in \mathcal{B}$, and $(Q_1', Q_2') \in \mathcal{B}$, then $Q_2' \Longrightarrow Q_2$ if $act(\theta_1) = \tau$ or $Q_2' \Longrightarrow \xrightarrow{\theta_2} \Longrightarrow Q_2$ with $act(\theta_1) = act(\theta_2)$ if $act(\theta_1) \neq \tau$, where $(Q_1', Q_2') \in \mathcal{B}$. ■

Corollary 7.3. *Let $P_1, P_2 \in \mathbb{P}$. If $P_1 \approx_{\mathrm{FRBB}} P_2$ then $P_1 \approx_{\mathrm{FRB}} P_2$.*

Proof. See the second part of the proof of Theorem 7.4. ■

7.2 True Concurrency

In the spectrum of truly concurrent bisimilarities [77, 66, 123], there are two equivalences that are particularly important: history-preserving bisimilarity [129] and hereditary history-preserving bisimilarity [16]. They are the coarsest equivalence and the finest equivalence, respectively, that are preserved under action refinement and are capable of respecting causality, branching, and their interplay while abstracting from choices between identical alternatives [77]. Moreover, hereditary history-preserving bisimilarity can be obtained as a special case of a categorical definition of bisimilarity over concurrency models [96]. Logical characterizations of both equivalences have been provided in [124, 14], whereas an axiomatization for hereditary history-preserving bisimilarity has been developed over forward-only processes in [71]. Furthermore, history-preserving bisimilarity is known to coincide with causal bisimilarity [55, 56], hence the latter offers a characterization and an axiomatization [59] for the former.

Several characterizations have been provided also for hereditary history-preserving bisimilarity, all of which rely on forward-reverse bisimilarity. Those in [16, 122, 123, 9] hold under assumptions that essentially revolve around the absence of autoconcurrency, i.e., identically labeled transitions not in conflict with each other that depart from the same process – e.g., $a \,.\, \underline{0} \parallel_\emptyset a \,.\, \underline{0}$ – or arrive at the same process – e.g., $a^\dagger . \underline{0} \parallel_\emptyset a^\dagger . \underline{0}$. In contrast, the one in [10] does not make any restrictive assumption, but introduces a complex identification mechanism. We show that hereditary history-preserving bisimilarity corresponds to forward-reverse bisimilarity extended with a simple clause that checks backward ready multisets for equality (Section 7.2.1). In this way, the former equivalence inherits a variant of the sound and complete axiomatization in Table 6.6, where backward ready sets are replaced by backward ready multisets, whilst the latter inherits the logical characterizations of the former.

7.2.1 Strong Forward-Reverse Bisimilarity and Hereditary History-Preserving Bisimilarity

Let us recall hereditary history-preserving bisimilarity over stable configuration structures [78]. These are truly concurrent models originated from event structures [142] that resemble labeled transition systems; a configuration is a finite set of non-conflicting events that is downward-closed with respect to a causality relation over events. The bisimulation game compares configuration transitions, both outgoing and incoming. The equivalence relies on ternary bisimulation relations, where the third component is a labeling- and causality-preserving bijection from the set of events executed so far in the first structure to the set of events executed so far in the second structure. In the following two definitions taken from [77], $\mathscr{P}_{\text{fin}}(\mathcal{E})$ denotes the set of finite subsets of set $\mathcal{E}$ while $f \upharpoonright X$ denotes the restriction of function f to set X.

Definition 7.5. *A* configuration structure *is a quadruple* $\mathsf{C} = (\mathcal{E}, \mathcal{C}, \mathcal{A}, l)$ *where:*

- $\mathcal{E}$ *is a set of* events.
- $\mathcal{C} \subseteq \mathscr{P}_{\text{fin}}(\mathcal{E})$ *is a set of* configurations.
- $l : \bigcup_{X \in \mathcal{C}} X \to \mathcal{A}$ *is a* labeling function.

C *is said to be* stable *iff it is:*

- *Rooted:* $\emptyset \in \mathcal{C}$.
- *Connected:* $\forall X \in \mathcal{C} \setminus \{\emptyset\}. \exists e \in X. X \setminus \{e\} \in \mathcal{C}$.
- *Closed under bounded unions and intersections:* $\forall X, Y, Z \in \mathcal{C}. X \cup Y \subseteq Z \Longrightarrow X \cup Y, X \cap Y \in \mathcal{C}$.

The causality relation *over* $X \in \mathcal{C}$ *is defined by letting* $e_1 \leq_X e_2$ *for* $e_1, e_2 \in X$ *iff* $e_2 \in Y$ *implies* $e_1 \in Y$ *for all* $Y \in \mathcal{C}$ *such that* $Y \subseteq X$*; we write* $e_1 <_X e_2$ *when* $e_1 \leq_X e_2$ *and* $e_1 \neq e_2$*. Two events* $e_1, e_2 \in X$ *are* concurrent *in* X *iff* $e_1 \not<_X e_2$ *and* $e_2 \not<_X e_1$*. We write* $X \xrightarrow{a}_{\mathsf{C}} X'$ *for* $X, X' \in \mathcal{C}$ *and* $a \in \mathcal{A}$ *iff* $X \subseteq X'$, $X' \setminus X = \{e\}$, *and* $l(e) = a$. ■

Definition 7.6. *We say that two stable configuration structures* $\mathsf{C}_i = (\mathcal{E}_i, \mathcal{C}_i, \mathcal{A}, l_i)$, $i \in \{1, 2\}$, *are* hereditary history-preserving bisimilar*, written* $\mathsf{C}_1 \sim_{\text{HHPB}} \mathsf{C}_2$*, iff there exists a hereditary history-preserving bisimulation between* C_1 *and* C_2*, i.e., a relation* $\mathcal{B} \subseteq \mathcal{C}_1 \times \mathcal{C}_2 \times \mathscr{P}(\mathcal{E}_1 \times \mathcal{E}_2)$ *such that:*

- $(\emptyset, \emptyset, \emptyset) \in \mathcal{B}$.
- *Whenever* $(X_1, X_2, f) \in \mathcal{B}$*, then:*
  - $f \subseteq \mathcal{E}_1 \times \mathcal{E}_2$ *is a bijection from* X_1 *to* X_2 *that preserves:*
    - *Labeling:* $l_1(e) = l_2(f(e))$ *for all* $e \in X_1$.
    - *Causality:* $e \leq_{X_1} e' \Longleftrightarrow f(e) \leq_{X_2} f(e')$ *for all* $e, e' \in X_1$.
  - *For each* $X_1 \xrightarrow{a}_{\mathsf{C}_1} X_1'$ *there exist* $X_2 \xrightarrow{a}_{\mathsf{C}_2} X_2'$ *and* $f' \subseteq \mathcal{E}_1 \times \mathcal{E}_2$ *such that* $(X_1', X_2', f') \in \mathcal{B}$ *and* $f' \upharpoonright X_1 = f$*, and vice versa.*
  - *For each* $X_1' \xrightarrow{a}_{\mathsf{C}_1} X_1$ *there exist* $X_2' \xrightarrow{a}_{\mathsf{C}_2} X_2$ *and* $f' \subseteq \mathcal{E}_1 \times \mathcal{E}_2$ *such that* $(X_1', X_2', f') \in \mathcal{B}$ *and* $f \upharpoonright X_1' = f'$*, and vice versa.* ■

Given a configuration X, its *backward ready multiset* is defined as $brm(X) = \{\!|\, a \in \mathcal{A} \mid X' \xrightarrow{a}_{\mathcal{C}} X \,|\!\}$ where $\{\!|$ and $|\!\}$ are multiset delimiters.

Definition 7.7. *We say that two stable configuration structures $\mathcal{C}_i = (\mathcal{E}_i, \mathcal{C}_i, \mathcal{A}, l_i)$, $i \in \{1,2\}$, are* brm-forward-reverse bisimilar*, written $\mathcal{C}_1 \sim_{\text{FRB:brm}} \mathcal{C}_2$, iff there exists a brm-forward-reverse bisimulation between $\mathcal{C}_1$ and $\mathcal{C}_2$, i.e., a relation $\mathcal{B} \subseteq \mathcal{C}_1 \times \mathcal{C}_2$ such that:*

- $(\emptyset, \emptyset) \in \mathcal{B}$.
- *Whenever $(X_1, X_2) \in \mathcal{B}$, then:*
  - *For each $X_1 \xrightarrow{a}_{\mathcal{C}_1} X_1'$ there exists $X_2 \xrightarrow{a}_{\mathcal{C}_2} X_2'$ such that $(X_1', X_2') \in \mathcal{B}$, and vice versa.*
  - *For each $X_1' \xrightarrow{a}_{\mathcal{C}_1} X_1$ there exists $X_2' \xrightarrow{a}_{\mathcal{C}_2} X_2$ such that $(X_1', X_2') \in \mathcal{B}$, and vice versa.*
  - *$brm(X_1) = brm(X_2)$.* ■

Suppose that $a = b$ in Figure 1.1. Then the labeled transition system on the left is an example of autoconcurrency and can be viewed as the graph underlying a stable configuration structure in which the initial state is configuration $\emptyset$, the two intermediate states are respectively configurations $\{\|_\emptyset a\}$ and $\{\|_\emptyset a\}$, and the final state is configuration $\{\|_\emptyset a, \|_\emptyset a\}$, where we have used proof terms to denote events. In contrast, the labeled transition system on the right is an example of autoconflict in which each of the two branches is an example of autocausation. It can be viewed as the graph underlying a stable configuration structure in which the initial state is configuration $\emptyset$, the two intermediate states are respectively configurations $\{\dot{+}a\}$ and $\{\dot{+}a\}$, and the two final states are respectively configurations $\{\dot{+}a, \dot{+}_{\cdot a} a\}$ and $\{\dot{+}a, \dot{+}_{\cdot a} a\}$.

These two configuration structures are told apart by $\sim_{\text{HHPB}}$ because $\dot{+}a$ (resp. $\dot{+}a$) causally precedes $\dot{+}_{\cdot a} a$ (resp. $\dot{+}_{\cdot a} a$) while $\|_\emptyset a$ and $\|_\emptyset a$ are concurrent, hence in the final configurations no causality-preserving bijection would relate the former two events to the latter two events. The two structures are identified by $\sim_{\text{FRB}}$, but $\sim_{\text{FRB:brm}}$ distinguishes them because $brm(\{\|_\emptyset a, \|_\emptyset a\}) = \{\!|\, a, a \,|\!\}$ whereas $brm(\{\dot{+}a, \dot{+}_{\cdot a} a\}) = brm(\{\dot{+}a, \dot{+}_{\cdot a} a\}) = \{\!|\, a \,|\!\}$.

The theorem below holds under the assumption that the considered configuration structures come from processes each in the form of a net of automata – i.e., parallel composition of several sequential subprocesses – in which every conflict is local – i.e., its effect is local to one sequential subprocess.

Theorem 7.5. *Let $\mathcal{C}_i = (\mathcal{E}_i, \mathcal{C}_i, \mathcal{A}, l_i)$, $i \in \{1,2\}$, be two stable configuration structures. Then $\mathcal{C}_1 \sim_{\text{HHPB}} \mathcal{C}_2$ iff $\mathcal{C}_1 \sim_{\text{FRB:brm}} \mathcal{C}_2$.*

Proof. The proof is divided into two parts:

- Suppose that $\mathcal{C}_1 \sim_{\text{HHPB}} \mathcal{C}_2$ due to some hereditary history-preserving bisimulation $\mathcal{B}$. Then $\mathcal{C}_1 \sim_{\text{FRB:brm}} \mathcal{C}_2$ follows by proving that $\mathcal{B}' = \{(X_1, X_2) \mid (X_1, X_2, f) \in \mathcal{B}\}$ is a brm-forward-reverse bisimulation. Observing that the starting clause and the clauses for outgoing and incoming transitions matching of $\sim_{\text{FRB:brm}}$ (see Definition 7.7) are a simplification of those of $\sim_{\text{HHPB}}$ (see Definition 7.6), given $(X_1, X_2) \in \mathcal{B}'$, i.e., $(X_1, X_2, f) \in \mathcal{B}$, we just have to show that $brm(X_1) = brm(X_2)$.
  Suppose that this is not the case, say X_1 has fewer incoming a-transitions than X_2. Without loss of generality, we can assume that X_1 has one incoming a-transition while X_2 has two. Then there is a diamond closing into X_2, i.e., there exist three configurations Y_2, X_2', and X_2'' and two a-labeled events e_2' and e_2'' such that $Y_2 \xrightarrow{l_2(e_2')}_{\mathcal{C}_2} X_2'$, $Y_2 \xrightarrow{l_2(e_2'')}_{\mathcal{C}_2} X_2''$, $X_2' \xrightarrow{l_2(e_2'')}_{\mathcal{C}_2} X_2$, and $X_2'' \xrightarrow{l_2(e_2')}_{\mathcal{C}_2} X_2$, where e_2' and e_2'' are concurrent in X_2, i.e., $e_2' \not<_{X_2} e_2''$ and $e_2'' \not<_{X_2} e_2'$.

Due to $(X_1, X_2, f) \in \mathcal{B}$, on X_1 side there exist two configurations Y_1 and X_1' and two a-labeled events e_1' and e_1'' such that $Y_1 \xrightarrow{l_1(e_1')}_{\mathcal{C}_1} X_1' \xrightarrow{l_1(e_1'')}_{\mathcal{C}_1} X_1$ where $e_1' \leq_{X_1} e_1''$. Since $\mathcal{B}$ is a hereditary history-preserving bisimulation, f should relate e_1' and e_1'' with e_2' and e_2'' in a causality-preserving way, but this is not possible because $f(e_1') \not\leq_{X_2} f(e_1'')$.

- Suppose that $\mathcal{C}_1 \sim_{\text{FRB:brm}} \mathcal{C}_2$ due to some brm-forward-reverse bisimulation $\mathcal{B}$. Then, given $(X_1, X_2) \in \mathcal{B}$, the existence in $\mathcal{C}_1$ of a sequence of transitions $X_{1,n} \xrightarrow{l_1(e_{1,n})}_{\mathcal{C}_1} X_{1,n-1} \ldots X_{1,1} \xrightarrow{l_1(e_{1,1})}_{\mathcal{C}_1} X_1$ implies the existence in $\mathcal{C}_2$ of a sequence of transitions $X_{2,n} \xrightarrow{l_2(e_{2,n})}_{\mathcal{C}_2} X_{2,n-1} \ldots X_{2,1} \xrightarrow{l_2(e_{2,1})}_{\mathcal{C}_2} X_2$ such that $l_1(e_{1,h}) = l_2(e_{2,h})$ and $(X_{1,h}, X_{2,h}) \in \mathcal{B}$ for all $h = 1, \ldots, n$, and vice versa. Note that $n = 0$ when X_1 and X_2 are both empty; moreover $e_{1,h} \neq e_{1,k}$ and $e_{2,h} \neq e_{2,k}$ for all $h \neq k$ because in each transition the source configuration and the target configuration differ by one event, which is the executed event (see Definition 7.5).
  Thus $\mathcal{C}_1 \sim_{\text{HHPB}} \mathcal{C}_2$ follows by proving that $\mathcal{B}' = \{(X_1, X_2, \{(e_{1,h}, e_{2,h}) \mid h \in H\}) \mid (X_1, X_2) \in \mathcal{B} \wedge X_{i,|H|} \xrightarrow{l_i(e_{i,|H|})}_{\mathcal{C}_i} X_{i,|H|-1} \ldots X_{i,1} \xrightarrow{l_i(e_{i,1})}_{\mathcal{C}_i} X_i$ for $i \in \{1,2\} \wedge l_1(e_{1,h}) = l_2(e_{2,h})$ for all $h \in H \wedge (X_{1,h}, X_{2,h}) \in \mathcal{B}$ for all $h \in H \wedge X_{1,|H|} = X_{2,|H|} = \emptyset\}$ is a hereditary history-preserving bisimulation.
  Let $(X_1, X_2, \{(e_{1,h}, e_{2,h}) \mid h \in H\}) \in \mathcal{B}'$, so that $(X_1, X_2) \in \mathcal{B}$:
  - $(\emptyset, \emptyset, \emptyset) \in \mathcal{B}'$ because $(\emptyset, \emptyset) \in \mathcal{B}$.
  - Let us show that $f = \{(e_{1,h}, e_{2,h}) \mid h \in H\}$ is a bijection from X_1 to X_2 that preserves labeling and causality. Since we already know that in the domain (resp. codomain) of f the events are all different from each other, the domain of f and its codomain have the same cardinality, and events corresponding via f have the same label, we focus on causality by assuming that $|H| \geq 2$ so as to avoid trivial cases. We proceed by contradiction, so we suppose that there exist $e, e' \in X_1$ such that $e \leq_{X_1} e'$ but $f(e) \not\leq_{X_2} f(e')$. From $e \leq_{X_1} e'$ it follows that there exist $Y_1, Y_1' \in \mathcal{C}_1$ such that $Y_1, Y_1' \subseteq X_1$, $e \in Y_1$, $e, e' \in Y_1'$, and $Y_1 \xrightarrow{l_1(e')}_{\mathcal{C}_1} Y_1'$. Since $\mathcal{C}_1 \sim_{\text{FRB:brm}} \mathcal{C}_2$ with $\mathcal{C}_1$ and $\mathcal{C}_2$ enjoying connectedness, there exists a pair $(Y_1, Y_2) \in \mathcal{B}$ such that $Y_2 \xrightarrow{l_2(f(e'))}_{\mathcal{C}_2} Y_2'$ and $(Y_1', Y_2') \in \mathcal{B}$, where $Y_2, Y_2' \subseteq X_2$. From $f(e) \not\leq_{X_2} f(e')$ it follows that there are two cases:
    * If $f(e') \leq_{X_2} f(e)$ then there exists $Y_2' \xrightarrow{l_2(f(e))}_{\mathcal{C}_2} \hat{Y}_2$, but this transition cannot be mimicked by Y_1' because e is already in Y_1', thereby contradicting $(Y_1', Y_2') \in \mathcal{B}$.
    * If $f(e)$ and $f(e')$ are concurrent in X_2, then there exists $\hat{Y}_2 \xrightarrow{l_2(f(e))}_{\mathcal{C}_2} Y_2'$. Since $(Y_1', Y_2') \in \mathcal{B}$, their backward ready multisets must coincide, hence there should be $\hat{Y}_1 \xrightarrow{l_1(e)}_{\mathcal{C}_1} Y_1'$, but this is not possible because $e \leq_{X_1} e'$.
  - If $X_1 \xrightarrow{a}_{\mathcal{C}_1} X_1'$ where a is the label of some event e_1, then $X_2 \xrightarrow{a}_{\mathcal{C}_2} X_2'$ where a is the label of some event e_2 and $(X_1', X_2') \in \mathcal{B}$; note that $e_1 \notin X_1$ and $e_2 \notin X_2$. Therefore $(X_1', X_2', \{(e_{1,h}, e_{2,h}) \mid h \in H\} \cup \{(e_1, e_2)\}) \in \mathcal{B}'$.
    If we start from $X_2 \xrightarrow{a}_{\mathcal{C}_2} X_2'$, then we reason in the same way.
  - If $X_1' \xrightarrow{a}_{\mathcal{C}_1} X_1$ where a is the label of some event e_1, then $X_2' \xrightarrow{a}_{\mathcal{C}_2} X_2$ where a is the label of some event e_2 and $(X_1', X_2') \in \mathcal{B}$; note that $e_1 \notin X_1'$ and $e_2 \notin X_2'$. Therefore $\{(e_{1,h}, e_{2,h}) \mid h \in H\} \upharpoonright X_1' = \{(e_{1,h}, e_{2,h}) \mid h \in H\} \setminus \{(e_1, e_2)\}$ and hence $(X_1', X_2', \{(e_{1,h}, e_{2,h}) \mid h \in H\} \setminus \{(e_1, e_2)\}) \in \mathcal{B}'$.
    If we start from $X_2' \xrightarrow{a}_{\mathcal{C}_2} X_2$, then we reason in the same way. ■

Part II

Noninterference Analysis of Reversible Concurrent Systems

Chapter 8

Noninterference Analysis of Nondeterministic Reversible Systems

In this chapter, whose contents have appeared in [61, 65], we start addressing information flow analysis of reversible systems by using some of the notions and results of the first part of the thesis. Noninterference was introduced in [82] to reason about the way in which illegitimate information flows can occur in multi-level security systems due to covert channels from high-level agents to low-level ones. Noninterference guarantees that low-level agents cannot infer from their observations what high-level ones are doing. Regardless of its specific definition, noninterference is closely tied to the notion of behavioral equivalence [76], because the idea is to compare the system behavior with high-level actions being prevented and the system behavior with the same actions being hidden.

After the classification of noninterference security properties in a process algebraic framework proposed in [67], the literature concentrated on weak bisimilarity [112] given its abstraction capability and polynomial-time decidability. Here we claim that it is worth studying noninterference by making use of branching bisimilarity [80], which by the way can be decided more efficiently [85, 95]. A clear motivation for switching from weak to branching bisimilarity is provided by reversible systems. As demonstrated in Section 7.1.2, branching bisimilarity coincides with weak forward-reverse bisimilarity over sequential processes. Moreover, in the reversible framework of [57], in which backward moves are constrained to take place along the same path followed in the forward direction even in the presence of concurrency – thus preserving not only causality but also history – branching bisimilarity was shown to coincide with weak back-and-forth bisimilarity. These results allow us to search for covert channels in reversible systems via a standard process calculus, in which there is no need of decorations for executed actions, along with an efficiently verifiable equivalence, at the price of losing the truly concurrent nature of forward-reverse bisimilarity.

This chapter is organized as follows. In Section 8.1 we recall background definitions and results for several bisimulation equivalences as well as a selection of information-flow security properties based on weak bisimilarity that we formalize through a suitable process calculus. In Section 8.2 we introduce a database management system authentication example. In Section 8.3, after recasting the same information-flow security properties in terms of branching bisimilarity, we present some results about the preservation of those properties under branching bisimilarity and their compositionality with respect to the operators of the considered language, then we study the relationships among all the previously discussed properties and summarize them in a new taxonomy. In Section 8.4 we recall the notion of back-and-forth bisimilarity and its relationship in the weak case with branching bisimilarity, which allows us to apply our taxonomy to reversible systems. In Section 8.5 we add reversibility to the database management system authentication example to illustrate the need of branching-bisimilarity-based noninterference.

8.1 Background Definitions and Results

In this section we recall the labeled transition system model of [97] (Section 8.1.1) together with strong and weak bisimilarities [112] and branching bisimilarity [80] (Section 8.1.2). Then we introduce a basic process language inspired by [112, 45] (Section 8.1.3) through which we recall the definitions of weak-bisimulation-based information-flow security properties of [67, 69] (Section 8.1.4).

8.1.1 Labeled Transition Systems

To represent the behavior of a nondeterministic process, we use a labeled transition system [97]. This is a state-transition graph whose transitions are labeled with actions taken from a set $\mathcal{A}$ including the unobservable action τ.

Definition 8.1. *A* labeled transition system (LTS) *is a triple* $(\mathcal{S}, \mathcal{A}, \longrightarrow)$ *where* $\mathcal{S}$ *is an at most countable set of states,* $\mathcal{A}$ *is a countable set of actions, and* $\longrightarrow \subseteq \mathcal{S} \times \mathcal{A} \times \mathcal{S}$ *is the transition relation.* ■

A transition (s, a, s') is written $s \xrightarrow{a} s'$, where s is the source state, a is the transition label, and s' is the target state, in which case we say that s' is reachable from s via that a-transition. We say that s' is reachable from s, written $s' \in \mathit{reach}(s)$, iff $s' = s$ or there exists a sequence of finitely many transitions such that the target state of each of them coincides with the source state of the subsequent one, with the source of the first one being s and the target of the last one being s'.

8.1.2 Nondeterministic Bisimulation Equivalences

Bisimilarity [117, 112] identifies processes that are able to mimic each other's behavior stepwise, i.e., having the same branching structure. In the strong case, τ is treated like all the other actions.

Definition 8.2. *Let* $(\mathcal{S}, \mathcal{A}, \longrightarrow)$ *be an LTS. We say that* $s_1, s_2 \in \mathcal{S}$ *are* strongly bisimilar*, written* $s_1 \sim s_2$*, iff* $(s_1, s_2) \in \mathcal{B}$ *for some strong bisimulation* $\mathcal{B}$*. A symmetric relation* $\mathcal{B}$ *over* $\mathcal{S}$ *is a* strong bisimulation *iff, whenever* $(s_1, s_2) \in \mathcal{B}$*, then:*

- *For each* $s_1 \xrightarrow{a} s_1'$ *there exists* $s_2 \xrightarrow{a} s_2'$ *such that* $(s_1', s_2') \in \mathcal{B}$. ■

Weak bisimilarity [112] is additionally capable of abstracting from unobservable actions. Let $s \stackrel{\tau^*}{\Longrightarrow} s'$ mean that $s' \in \mathit{reach}(s)$ and, when $s' \neq s$, there exists a finite sequence of transitions from s to s' each of which is labeled with τ. Moreover let $\stackrel{\hat{a}}{\Longrightarrow}$ stand for $\stackrel{\tau^*}{\Longrightarrow}$ if $a = \tau$ or $\stackrel{\tau^*}{\Longrightarrow} \xrightarrow{a} \stackrel{\tau^*}{\Longrightarrow}$ if $a \neq \tau$.

Definition 8.3. *Let* $(\mathcal{S}, \mathcal{A}, \longrightarrow)$ *be an LTS. We say that* $s_1, s_2 \in \mathcal{S}$ *are* weakly bisimilar*, written* $s_1 \approx_{\mathrm{w}} s_2$*, iff* $(s_1, s_2) \in \mathcal{B}$ *for some weak bisimulation* $\mathcal{B}$*. A symmetric relation* $\mathcal{B}$ *over* $\mathcal{S}$ *is a* weak bisimulation *iff, whenever* $(s_1, s_2) \in \mathcal{B}$*, then:*

- *For each* $s_1 \xrightarrow{a}_{\mathrm{a}} s_1'$ *there exists* $s_2 \stackrel{\hat{a}}{\Longrightarrow} s_2'$ *such that* $(s_1', s_2') \in \mathcal{B}$. ■

Branching bisimilarity [80] is finer than weak bisimilarity as it preserves the branching structure of processes even when abstracting from τ-actions – see condition $(s_1, \bar{s}_2) \in \mathcal{B}$ in the definition below.

Definition 8.4. *Let* $(\mathcal{S}, \mathcal{A}, \longrightarrow)$ *be an LTS. We say that* $s_1, s_2 \in \mathcal{S}$ *are* branching bisimilar*, written* $s_1 \approx_{\mathrm{b}} s_2$*, iff* $(s_1, s_2) \in \mathcal{B}$ *for some branching bisimulation* $\mathcal{B}$*. A symmetric relation* $\mathcal{B}$ *over* $\mathcal{S}$ *is a* branching bisimulation *iff, whenever* $(s_1, s_2) \in \mathcal{B}$*, then:*

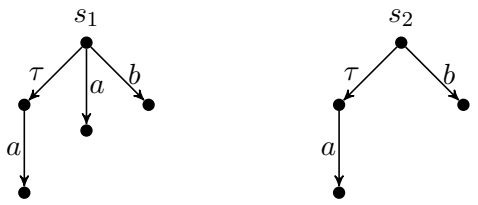


Figure 8.1: States related by $\approx_{\mathrm{w}}$ but distinguished by $\approx_{\mathrm{b}}$

- *For each* $s_1 \xrightarrow{a} s_1'$*:*
  - *either* $a = \tau$ *and* $(s_1', s_2) \in \mathcal{B}$*;*
  - *or there exists* $s_2 \stackrel{\tau^*}{\Longrightarrow} \bar{s}_2 \xrightarrow{a} s_2'$ *such that* $(s_1, \bar{s}_2) \in \mathcal{B}$ *and* $(s_1', s_2') \in \mathcal{B}$*.* ■

An example that highlights the higher distinguishing power of branching bisimilarity is given in Figure 8.1, where every LTS is depicted as a directed graph in which vertices represent states and action-labeled edges represent transitions. The initial states s_1 and s_2 of the two LTSs are weakly bisimilar but not branching bisimilar. The only transition that distinguishes s_1 from s_2 is the a-transition of s_1, which can be mimicked by s_2 according to weak bisimilarity by performing its τ-transition followed by its a-transition. However, s_2 cannot respond in the same way according to branching bisimilarity because the state reached after the τ-transition should be branching bisimilar to s_1, which is not the case due to the b-transition departing from s_1.

8.1.3 A Nondeterministic Process Calculus with High and Low Actions

We now introduce a basic process calculus to formalize the security properties of interest. To address two security levels, we partition the set $\mathcal{A} \setminus \{\tau\}$ of observable actions into $\mathcal{A}_{\mathcal{H}} \cup \mathcal{A}_{\mathcal{L}}$, with $\mathcal{A}_{\mathcal{H}} \cap \mathcal{A}_{\mathcal{L}} = \emptyset$, where $\mathcal{A}_{\mathcal{H}}$ is the set of high-level actions, ranged over by h, and $\mathcal{A}_{\mathcal{L}}$ is the set of low-level actions, ranged over by l. Note that $\tau \notin \mathcal{A}_{\mathcal{H}} \cup \mathcal{A}_{\mathcal{L}}$.

The set $\mathbb{P}_{\mathrm{nd}}$ of process terms is obtained by considering typical operators from CCS [112] and CSP [45]. In addition to action prefix, nondeterministic choice, and parallel composition – taken from CSP so as not to turn synchronizations among high-level actions into τ as would happen with the CCS parallel composition – we include restriction and hiding, as they are necessary to formalize noninterference properties, and recursion. The syntax for $\mathbb{P}_{\mathrm{nd}}$ is:

$$P ::= \underline{0} \mid a \,.\, P \mid P + P \mid P \parallel_L P \mid P \setminus L \mid P \,/\, L \mid K$$

where:

- $\underline{0}$ is the terminated process.
- $a \,.\, \_$, for $a \in \mathcal{A}$, is the action prefix operator describing a process that can initially perform action a.
- $\_ + \_$ is the alternative composition operator expressing a nondeterministic choice between two processes based on their initially executable actions.
- $\_ \parallel_L \_$, for $L \subseteq \mathcal{A} \setminus \{\tau\}$, is the parallel composition operator allowing two processes to proceed independently on any action not in L and forcing them to synchronize on every action in L.

Prefix	$a \,.\, P \xrightarrow{a} P$
Choice	$\dfrac{P_1 \xrightarrow{a} P_1'}{P_1 + P_2 \xrightarrow{a} P_1'} \qquad \dfrac{P_2 \xrightarrow{a} P_2'}{P_1 + P_2 \xrightarrow{a} P_2'}$
Parallel	$\dfrac{P_1 \xrightarrow{a} P_1' \quad a \notin L}{P_1 \parallel_L P_2 \xrightarrow{a} P_1' \parallel_L P_2} \qquad \dfrac{P_2 \xrightarrow{a} P_2' \quad a \notin L}{P_1 \parallel_L P_2 \xrightarrow{a} P_1 \parallel_L P_2'}$
Synch	$\dfrac{P_1 \xrightarrow{a} P_1' \quad P_2 \xrightarrow{a} P_2' \quad a \in L}{P_1 \parallel_L P_2 \xrightarrow{a} P_1' \parallel_L P_2'}$
Restriction	$\dfrac{P \xrightarrow{a} P' \quad a \notin L}{P \setminus L \xrightarrow{a} P' \setminus L}$
Hiding	$\dfrac{P \xrightarrow{a} P' \quad a \in L}{P \,/\, L \xrightarrow{\tau} P' \,/\, L} \qquad \dfrac{P \xrightarrow{a} P' \quad a \notin L}{P \,/\, L \xrightarrow{a} P' \,/\, L}$
Constant	$\dfrac{K \triangleq P \quad P \xrightarrow{a} P'}{K \xrightarrow{a} P'}$

Table 8.1: Operational semantic rules for purely nondeterministic processes

- $\_ \setminus L$, for $L \subseteq \mathcal{A} \setminus \{\tau\}$, is the restriction operator, which prevents the execution of all actions belonging to L.
- $\_ \,/\, L$, for $L \subseteq \mathcal{A} \setminus \{\tau\}$, is the hiding operator, which turns all the executed actions belonging to L into the unobservable action τ.
- K is a process constant equipped with a defining equation of the form $K \triangleq P$, where every constant possibly occurring in P – including K itself thus allowing for recursion – must be in the scope of an action prefix.

The operational semantic rules for the process language are shown in Table 8.1 and produce the LTS $(\mathbb{P}_{\mathrm{nd}}, \mathcal{A}, \longrightarrow)$ where $\longrightarrow \subseteq \mathbb{P}_{\mathrm{nd}} \times \mathcal{A} \times \mathbb{P}_{\mathrm{nd}}$, to which the bisimulation equivalences defined in Section 8.1.2 are applicable.

8.1.4 Nondeterministic Information-Flow Security Properties Based on Weak Bisimilarity

The intuition behind noninterference in a two-level security system is that, whenever a group of agents at the high security level performs some actions, the effect of those actions should not be visible by any agent at the low security level. Below is a representative selection of weak-bisimulation-based noninterference properties – *Nondeterministic Non-Interference* (NNI) and *Non-Deducibility on Composition* (NDC) – whose definitions and relationships are recalled from [67] and, as far as P_BNDC is concerned, from [69].

Definition 8.5. *Let* $P \in \mathbb{P}_{\mathrm{nd}}$*:*

- $P \in \mathrm{BSNNI}_{\approx_{\mathrm{w}}} \iff P \setminus \mathcal{A}_{\mathcal{H}} \approx_{\mathrm{w}} P \,/\, \mathcal{A}_{\mathcal{H}}$.
- $P \in \mathrm{BNDC}_{\approx_{\mathrm{w}}} \iff$ *for all* $Q \in \mathbb{P}_{\mathrm{nd}}$ *such that each of its actions belongs to* $\mathcal{A}_{\mathcal{H}}$ *and for all* $L \subseteq \mathcal{A}_{\mathcal{H}}$, $P \setminus \mathcal{A}_{\mathcal{H}} \approx_{\mathrm{w}} ((P \parallel_L Q) \,/\, L) \setminus \mathcal{A}_{\mathcal{H}}$.

- $P \in \text{SBSNNI}_{\approx_w} \iff$ *for all* $P' \in \mathit{reach}(P)$, $P' \in \text{BSNNI}_{\approx_w}$.
- $P \in \text{P\_BNDC}_{\approx_w} \iff$ *for all* $P' \in \mathit{reach}(P)$, $P' \in \text{BNDC}_{\approx_w}$.
- $P \in \text{SBNDC}_{\approx_w} \iff$ *for all* $P', P'' \in \mathit{reach}(P)$ *such that* $P' \xrightarrow{h} P''$, $P' \setminus \mathcal{A}_{\mathcal{H}} \approx_w P'' \setminus \mathcal{A}_{\mathcal{H}}$. ■

Theorem 8.1. $\text{SBNDC}_{\approx_w} \subsetneq \text{SBSNNI}_{\approx_w} = \text{P\_BNDC}_{\approx_w} \subsetneq \text{BNDC}_{\approx_w} \subsetneq \text{BSNNI}_{\approx_w}$. ■

Bisimulation-based Strong Nondeterministic Non-Interference (BSNNI) has been one of the first and most intuitive proposals. Basically, it is satisfied by any process P that behaves the same when its high-level actions are prevented (as modeled by $P \setminus \mathcal{A}_{\mathcal{H}}$) or when they are considered as hidden, unobservable actions (as modeled by $P / \mathcal{A}_{\mathcal{H}}$). The equivalence between these two low-level views of P states that a low-level agent cannot infer the high-level behavior of the system. For instance, a low-level agent that observes the execution of l in $l.\underline{0} + h.l.\underline{0}$ cannot infer anything about the execution of h. Indeed, $(l.\underline{0} + h.l.\underline{0}) \setminus \{h\} \approx_w (l.\underline{0} + h.l.\underline{0}) / \{h\}$ because the former process behaves as $l.\underline{0}$, the latter process behaves as $l.\underline{0} + \tau.l.\underline{0}$, and $l.\underline{0} \approx_w l.\underline{0} + \tau.l.\underline{0}$.

BSNNI is not powerful enough to detect information leakages that derive from the behavior of a high-level agent interacting with the system. For instance, $l.\underline{0} + h_1.h_2.l.\underline{0}$ is BSNNI for the same reason discussed above. However, a high-level agent like $h_1.\underline{0}$ enables h_1 and then disables h_2, thus yielding the low-level view of the system $l.\underline{0} + \tau.\underline{0}$, which is clearly distinguishable from $l.\underline{0}$ as only in the former a low-level agent may not observe l. To avoid such a limitation, the most obvious solution consists of checking explicitly the interaction on any action set $L \subseteq \mathcal{A}_{\mathcal{H}}$ between the system and every possible high-level agent Q. The resulting property is *Bisimulation-based Non-Deducibility on Composition* (BNDC), which features a universal quantification over Q containing only high-level actions.

To circumvent the verification problems related to such a quantifier, several properties have been proposed that are stronger than BNDC. They all express some persistency conditions, stating that the security checks have to be extended to all the processes reachable from a secure one. Three of the most representative ones among such properties are the variant of BSNNI that requires every reachable process to satisfy BSNNI itself, called *Strong* BSNNI (SBSNNI), the variant of BNDC that requires every reachable process to satisfy BNDC itself, called *Persistent* BNDC (P_BNDC), and *Strong* BNDC (SBNDC), which requires the low-level view of every reachable process to be the same before and after the execution of any high-level action, meaning that the execution of high-level actions must be completely transparent to low-level agents.

8.2 Use Case: DBMS Authentication – Weak Bisimilarity

Consider a multi-threaded system supporting the execution of concurrent transactions operating on a healthcare database, where only authorized users can write their data. Depending on a policy governed by the database management system (DBMS), such data can be shared with a dedicated module feeding the training set of a machine learning (ML) facility, which is responsible for building a trained model for data analysis purposes.

On the one hand, different authentication mechanisms can be employed to identify users and ensure data authenticity for each transaction. We address a simple password-based mechanism (pwd), a more sophisticated two-factor authentication system (2fa), and a scheme based on single sign on (sso) [39].

On the other hand, for security reasons related to sharing sensitive data with the ML module [3], only data transmitted through highly secure mechanisms, i.e., 2fa and sso, can be used to feed the training set. In any case, for privacy issues, users must not be aware of whether their data are actually chosen to train the ML model

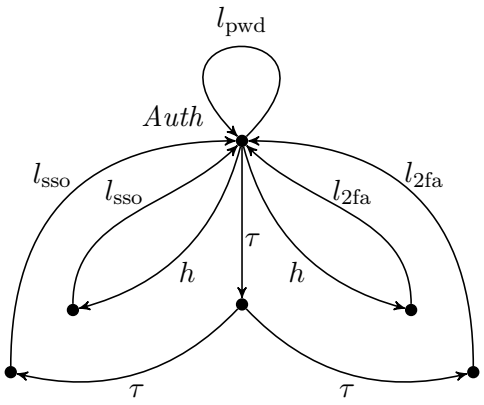


Figure 8.2: LTS underlying the DBMS authentication mechanism $Auth$

or not [12]. Hence, to avoid that the use of highly secure authentication implicitly reveals the involvement of the ML module, the DBMS internally decides not to consider certain transactions for the training set.

For the sake of simplicity, we concentrate on the authentication policy followed by the DBMS whenever handling a write transaction. Therefore, we abstract away from the description of the ML module and of the database access operations. In particular, we consider the following process, whose LTS is depicted in Figure 8.2:

$$\begin{aligned} Auth \triangleq\ & l_{\text{pwd}} \,.\, Auth + \\ & (h \,.\, l_{\text{sso}} \,.\, Auth + h \,.\, l_{\text{2fa}} \,.\, Auth) + \\ & \tau \,.\, (\tau \,.\, l_{\text{sso}} \,.\, Auth + \tau \,.\, l_{\text{2fa}} \,.\, Auth) \end{aligned}$$

Actions $l_\star$ express that the transaction is conducted under the authentication method represented by $\star$. We treat them as low-level actions because they represent interactions between the users and the DBMS. Action h represents an interaction between the DBMS and the ML module, which is deemed to be high level as the activities of the ML module must be transparent to the users.

The first summand of $Auth$ specifies that the DBMS is ready to offer the password-based mechanism, in which case the transaction data will not be passed to the ML module. The second summand models the communication with the ML module so that the transaction data – which must be protected through one of the two highly secure authentication mechanisms – will be included in the training set. Note that in this case the choice of the specific authentication method offered by the DBMS is nondeterministic and does not include the password-based mechanism. The third summand specifies that the DBMS decides internally, through the first τ-action, that the transaction data will not be passed to the ML module, even if the authentication method (chosen nondeterministically) is highly secure. Hence, in this case no interaction with the ML module is needed. The aim of this summand is to mimic the behavior of the second summand, thus acting as an obfuscation mechanism that shall not allow any user to detect the potential involvement of the ML module by simply observing the used authentication method.

Formally, the success of this obfuscation is guaranteed if the interaction with the ML module does not interfere with the low-level view of the system observed by any user, which can be verified as a noninterference property. More specifically, the ML module represents the high-level portion of the system that is expected not to interfere with the low-level behavior of any user interacting with the DBMS, thus justifying the use of the high-level action h modeling the interaction between such a module and the DBMS.

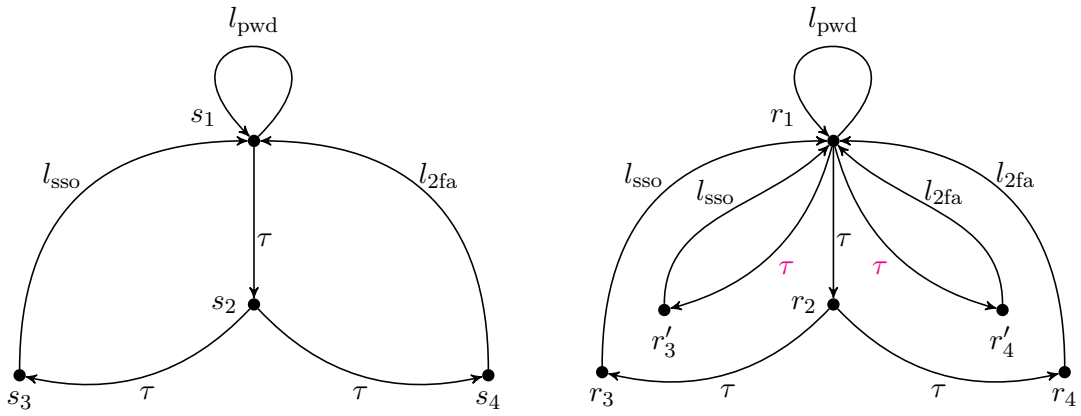


Figure 8.3: LTSs of the low-level views $Auth \setminus \mathcal{A}_{\mathcal{H}}$ (left) and $Auth \,/\, \mathcal{A}_{\mathcal{H}}$ (right)

As far as $\approx_{\text{w}}$-based noninterference is concerned, *Auth* does not leak any information from the high level to the low level. More precisely, the system is SBSNNI$_{\approx_{\text{w}}}$, and hence also BNDC$_{\approx_{\text{w}}}$ and BSNNI$_{\approx_{\text{w}}}$ by virtue of Theorem 8.1. Indeed, by observing Figure 8.3 – where the h-actions are forbidden on the left while they are transformed into the colored τ-actions on the right – it is easy to see that *Auth* is BSNNI$_{\approx_{\text{w}}}$, i.e., $Auth \setminus \mathcal{A}_{\mathcal{H}} \approx_{\text{w}} Auth \,/\, \mathcal{A}_{\mathcal{H}}$. The weak bisimulation relating the two low-level views of *Auth* is given by the following partition of the disjoint union of the two state spaces: $\{\{s_1, r_1\}, \{s_2, r_2\}, \{s_3, r_3, r'_3\}, \{s_4, r_4, r'_4\}\}$. Since the only high-level action is enabled at the initial state of *Auth*, it follows that *Auth* is SBSNNI$_{\approx_{\text{w}}}$ as well.

8.3 Nondeterministic Information-Flow Security Properties Based on Branching Bisimilarity

While the literature on behavioral-equivalence-based noninterference mainly concentrates on weak bisimulation semantics, here we address information-flow security properties relying on branching bisimilarity.

Definition 8.6. BSNNI$_{\approx_{\text{b}}}$, BNDC$_{\approx_{\text{b}}}$, SBSNNI$_{\approx_{\text{b}}}$, P_BNDC$_{\approx_{\text{b}}}$, SBNDC$_{\approx_{\text{b}}}$ *are obtained from the corresponding properties in Definition 8.5 by replacing the weak bisimilarity check ($\approx_{\text{w}}$) with the branching bisimilarity one ($\approx_{\text{b}}$).* ■

In this section we first study their preservation and compositionality characteristics so as to assess their usefulness (Section 8.3.1) and then we investigate the inclusion relationships among them and with the corresponding properties based on weak bisimilarity (Section 8.3.2).

8.3.1 Preservation and Compositionality

Similar to the weak bisimilarity case [67], all the $\approx_{\text{b}}$-based noninterference properties turn out to be preserved by $\approx_{\text{b}}$. This means that, whenever a process P_1 is secure under any of such properties, then every other branching bisimilar process P_2 is secure too according to the same property. This is very useful for automated property verification, as it allows one to work with the process with the smallest state space among the equivalent ones.

The preservation result of Theorem 8.2 immediately follows from the lemma below, which ensures that $\approx_{\rm b}$ is a congruence with respect to all the operators occurring in the aforementioned noninterference properties. These operators were not considered in the congruence results of [80, 75].

Lemma 8.1. *Let $P_1, P_2 \in \mathbb{P}_{\rm nd}$. If $P_1 \approx_{\rm b} P_2$ then:*

1. *$P_1 \parallel_L P \approx_{\rm b} P_2 \parallel_L P$ and $P \parallel_L P_1 \approx_{\rm b} P \parallel_L P_2$ for all $L \subseteq \mathcal{A} \setminus \{\tau\}$ and $P \in \mathbb{P}_{\rm nd}$.*
2. *$P_1 \setminus L \approx_{\rm b} P_2 \setminus L$ for all $L \subseteq \mathcal{A} \setminus \{\tau\}$.*
3. *$P_1 / L \approx_{\rm b} P_2 / L$ for all $L \subseteq \mathcal{A} \setminus \{\tau\}$.*

Proof. Let $\mathcal{B}$ be a branching bisimulation witnessing $P_1 \approx_{\rm b} P_2$:

1. The symmetric relation $\mathcal{B}' = \{(Q_1 \parallel_L Q, Q_2 \parallel_L Q) \mid (Q_1, Q_2) \in \mathcal{B} \wedge Q \in \mathbb{P}_{\rm nd}\}$ and its variant $\mathcal{B}''$ in which Q occurs to the left of parallel composition in each pair are branching bisimulations too. Let us focus on $\mathcal{B}'$. Given $(Q_1 \parallel_L Q, Q_2 \parallel_L Q) \in \mathcal{B}'$, so that $(Q_1, Q_2) \in \mathcal{B}$, there are three cases based on the operational semantic rules in Table 8.1:
   - If $Q_1 \parallel_L Q \xrightarrow{a} Q_1' \parallel_L Q$ with $Q_1 \xrightarrow{a} Q_1'$ and $a \notin L$, then either $a = \tau$ and $(Q_1', Q_2) \in \mathcal{B}$, or there exists $Q_2 \stackrel{\tau^*}{\Longrightarrow} \bar{Q}_2 \xrightarrow{a} Q_2'$ such that $(Q_1, \bar{Q}_2) \in \mathcal{B}$ and $(Q_1', Q_2') \in \mathcal{B}$. Since synchronization does not apply to τ and $a \notin L$, in the former subcase $Q_2 \parallel_L Q$ is allowed to stay idle with $(Q_1' \parallel_L Q, Q_2 \parallel_L Q) \in \mathcal{B}'$, while in the latter subcase $Q_2 \parallel_L Q \stackrel{\tau^*}{\Longrightarrow} \bar{Q}_2 \parallel_L Q \xrightarrow{a} Q_2' \parallel_L Q$ with $(Q_1 \parallel_L Q, \bar{Q}_2 \parallel_L Q) \in \mathcal{B}'$ and $(Q_1' \parallel_L Q, Q_2' \parallel_L Q) \in \mathcal{B}'$.
   - The case $Q_1 \parallel_L Q \xrightarrow{a} Q_1 \parallel_L Q'$ with $Q \xrightarrow{a} Q'$ and $a \notin L$ is trivial.
   - If $Q_1 \parallel_L Q \xrightarrow{a} Q_1' \parallel_L Q'$ with $Q_1 \xrightarrow{a} Q_1'$, $Q \xrightarrow{a} Q'$, and $a \in L$, then there exists $Q_2 \stackrel{\tau^*}{\Longrightarrow} \bar{Q}_2 \xrightarrow{a} Q_2'$ such that $(Q_1, \bar{Q}_2) \in \mathcal{B}$ and $(Q_1', Q_2') \in \mathcal{B}$. Since synchronization does not apply to τ and $a \in L$, we have that $Q_2 \parallel_L Q \stackrel{\tau^*}{\Longrightarrow} \bar{Q}_2 \parallel_L Q \xrightarrow{a} Q_2' \parallel_L Q'$ with $(Q_1 \parallel_L Q, \bar{Q}_2 \parallel_L Q) \in \mathcal{B}'$ and $(Q_1' \parallel_L Q', Q_2' \parallel_L Q') \in \mathcal{B}'$.
2. The symmetric relation $\mathcal{B}' = \{(Q_1 \setminus L, Q_2 \setminus L) \mid (Q_1, Q_2) \in \mathcal{B}\}$ is a branching bisimulation too. Given $(Q_1 \setminus L, Q_2 \setminus L) \in \mathcal{B}'$, so that $(Q_1, Q_2) \in \mathcal{B}$, there are two cases based on the operational semantic rules in Table 8.1:
   - If $Q_1 \setminus L \xrightarrow{\tau} Q_1' \setminus L$ with $Q_1 \xrightarrow{\tau} Q_1'$, then either $(Q_1', Q_2) \in \mathcal{B}$, or there exists $Q_2 \stackrel{\tau^*}{\Longrightarrow} \bar{Q}_2 \xrightarrow{\tau} Q_2'$ such that $(Q_1, \bar{Q}_2) \in \mathcal{B}$ and $(Q_1', Q_2') \in \mathcal{B}$. Since the restriction operator does not apply to τ, in the former subcase $Q_2 \setminus L$ is allowed to stay idle with $(Q_1' \setminus L, Q_2 \setminus L) \in \mathcal{B}'$, while in the latter subcase $Q_2 \setminus L \stackrel{\tau^*}{\Longrightarrow} \bar{Q}_2 \setminus L \xrightarrow{\tau} Q_2' \setminus L$ with $(Q_1 \setminus L, \bar{Q}_2 \setminus L) \in \mathcal{B}'$ and $(Q_1' \setminus L, Q_2' \setminus L) \in \mathcal{B}'$.
   - If $Q_1 \setminus L \xrightarrow{a} Q_1' \setminus L$ with $Q_1 \xrightarrow{a} Q_1'$ and $a \notin L \cup \{\tau\}$, then there exists $Q_2 \stackrel{\tau^*}{\Longrightarrow} \bar{Q}_2 \xrightarrow{a} Q_2'$ such that $(Q_1, \bar{Q}_2) \in \mathcal{B}$ and $(Q_1', Q_2') \in \mathcal{B}$. Since the restriction operator does not apply to τ and $a \notin L$, we have that $Q_2 \setminus L \stackrel{\tau^*}{\Longrightarrow} \bar{Q}_2 \setminus L \xrightarrow{a} Q_2' \setminus L$ with $(Q_1 \setminus L, \bar{Q}_2 \setminus L) \in \mathcal{B}'$ and $(Q_1' \setminus L, Q_2' \setminus L) \in \mathcal{B}'$.
3. The symmetric relation $\mathcal{B}' = \{(Q_1 / L, Q_2 / L) \mid (Q_1, Q_2) \in \mathcal{B}\}$ is a branching bisimulation too. Given $(Q_1 / L, Q_2 / L) \in \mathcal{B}'$, so that $(Q_1, Q_2) \in \mathcal{B}$, there are two cases based on the operational semantic rules in Table 8.1:

- If $Q_1 \,/\, L \xrightarrow{\tau} Q_1' \,/\, L$ with $Q_1 \xrightarrow{\tau} Q_1'$, then either $(Q_1', Q_2) \in \mathcal{B}$, or there exists $Q_2 \stackrel{\tau^*}{\Longrightarrow} \bar{Q}_2 \xrightarrow{\tau} Q_2'$ such that $(Q_1, \bar{Q}_2) \in \mathcal{B}$ and $(Q_1', Q_2') \in \mathcal{B}$. Since the hiding operator does not apply to τ, in the former subcase $Q_2 \,/\, L$ is allowed to stay idle with $(Q_1' \,/\, L, Q_2 \,/\, L) \in \mathcal{B}'$, while in the latter subcase $Q_2 \,/\, L \stackrel{\tau^*}{\Longrightarrow} \bar{Q}_2 \,/\, L \xrightarrow{\tau} Q_2' \,/\, L$ with $(Q_1 \,/\, L, \bar{Q}_2 \,/\, L) \in \mathcal{B}'$ and $(Q_1' \,/\, L, Q_2' \,/\, L) \in \mathcal{B}'$.
- If $Q_1 \,/\, L \xrightarrow{a} Q_1' \,/\, L$ with $Q_1 \xrightarrow{b} Q_1'$ and $b \in L \wedge a = \tau$ or $b \notin L \cup \{\tau\} \wedge a = b$, then there exists $Q_2 \stackrel{\tau^*}{\Longrightarrow} \bar{Q}_2 \xrightarrow{b} Q_2'$ such that $(Q_1, \bar{Q}_2) \in \mathcal{B}$ and $(Q_1', Q_2') \in \mathcal{B}$. Since the hiding operator does not apply to τ, we have that $Q_2 \,/\, L \stackrel{\tau^*}{\Longrightarrow} \bar{Q}_2 \,/\, L \xrightarrow{a} Q_2' \,/\, L$ with $(Q_1 \,/\, L, \bar{Q}_2 \,/\, L) \in \mathcal{B}'$ and $(Q_1' \,/\, L, Q_2' \,/\, L) \in \mathcal{B}'$. ■

Theorem 8.2. *Let* $P_1, P_2 \in \mathbb{P}_{\rm nd}$ *and* $\mathcal{P} \in \{\mathrm{BSNNI}_{\approx_{\rm b}}, \mathrm{BNDC}_{\approx_{\rm b}}, \mathrm{SBSNNI}_{\approx_{\rm b}}, \mathrm{P\_BNDC}_{\approx_{\rm b}}, \mathrm{SBNDC}_{\approx_{\rm b}}\}$. *If* $P_1 \approx_{\rm b} P_2$ *then* $P_1 \in \mathcal{P} \iff P_2 \in \mathcal{P}$.

Proof. A straightforward consequence of the definition of the various properties, i.e., Definition 8.6, and Lemma 8.1. ■

As far as modular verification is concerned, like in the weak bisimilarity case [67] only the local properties $\mathrm{SBSNNI}_{\approx_{\rm b}}$, $\mathrm{P\_BNDC}_{\approx_{\rm b}}$, and $\mathrm{SBNDC}_{\approx_{\rm b}}$ are compositional, i.e., are preserved by some operators of the calculus in certain circumstances. Unlike the compositionality results presented in [67], ours are related not only to parallel composition and restriction, but also to action prefix and hiding. Moreover, compositionality with respect to parallel composition is limited, for $\mathrm{SBSNNI}_{\approx_{\rm b}}$ and $\mathrm{P\_BNDC}_{\approx_{\rm b}}$, to the case in which synchronization can take place only among low-level actions, i.e., $L \subseteq \mathcal{A}_{\mathcal{L}}$, while in the case of $\mathrm{SBSNNI}_{\approx_{\rm w}}$ it holds for every $L \subseteq \mathcal{A} \setminus \{\tau\}$. A limitation to low-level actions applies to action prefix and hiding as well, whilst this is not the case for restriction. Another analogy with the weak bisimilarity case [67] is that none of the considered noninterference properties is compositional with respect to alternative composition. For instance, let us consider processes $P_1 = l \,.\, \underline{0}$ and $P_2 = h \,.\, \underline{0}$. Both processes are $\mathrm{BSNNI}_{\approx_{\rm b}}$, as $l \,.\, \underline{0} \setminus \{h\} \approx_{\rm b} l \,.\, \underline{0} \,/\, \{h\}$ and $h \,.\, \underline{0} \setminus \{h\} \approx_{\rm b} h \,.\, \underline{0} \,/\, \{h\}$, but $P_1 + P_2 \notin \mathrm{BSNNI}_{\approx_{\rm b}}$, because $(l \,.\, \underline{0} + h \,.\, \underline{0}) \setminus \{h\} \approx_{\rm b} l \,.\, \underline{0} \not\approx_{\rm b} l \,.\, \underline{0} + \tau \,.\, \underline{0} \approx_{\rm b} (l \,.\, \underline{0} + h \,.\, \underline{0}) \,/\, \{h\}$. It is easy to check that $P_1 + P_2 \notin \mathcal{P}$ also for $\mathcal{P} \in \{\mathrm{BNDC}_{\approx_{\rm b}}, \mathrm{SBSNNI}_{\approx_{\rm b}}, \mathrm{P\_BNDC}_{\approx_{\rm b}}, \mathrm{SBNDC}_{\approx_{\rm b}}\}$.

To establish compositionality, we first prove some ancillary results about parallel composition, restriction, and hiding under $\mathrm{SBSNNI}_{\approx_{\rm b}}$ and $\mathrm{SBNDC}_{\approx_{\rm b}}$.

Lemma 8.2. *Let* $P_1, P_2, P \in \mathbb{P}_{\rm nd}$. *Then:*

1. *If* $P_1, P_2 \in \mathrm{SBSNNI}_{\approx_{\rm b}}$ *and* $L \subseteq \mathcal{A}_{\mathcal{L}}$, *then* $(Q_1 \parallel_L Q_2) \setminus \mathcal{A}_{\mathcal{H}} \approx_{\rm b} (R_1 \parallel_L R_2) \,/\, \mathcal{A}_{\mathcal{H}}$ *for all* $Q_1, R_1 \in \mathit{reach}(P_1)$ *and* $Q_2, R_2 \in \mathit{reach}(P_2)$ *such that* $Q_1 \parallel_L Q_2, R_1 \parallel_L R_2 \in \mathit{reach}(P_1 \parallel_L P_2)$, $Q_1 \setminus \mathcal{A}_{\mathcal{H}} \approx_{\rm b} R_1 \,/\, \mathcal{A}_{\mathcal{H}}$, *and* $Q_2 \setminus \mathcal{A}_{\mathcal{H}} \approx_{\rm b} R_2 \,/\, \mathcal{A}_{\mathcal{H}}$.
2. *If* $P \in \mathrm{SBSNNI}_{\approx_{\rm b}}$ *and* $L \subseteq \mathcal{A} \setminus \{\tau\}$, *then* $(Q \,/\, \mathcal{A}_{\mathcal{H}}) \setminus L \approx_{\rm b} (R \setminus L) \,/\, \mathcal{A}_{\mathcal{H}}$ *for all* $Q, R \in \mathit{reach}(P)$ *such that* $Q \,/\, \mathcal{A}_{\mathcal{H}} \approx_{\rm b} R \setminus \mathcal{A}_{\mathcal{H}}$.
3. *If* $P_1, P_2 \in \mathrm{SBNDC}_{\approx_{\rm b}}$ *and* $L \subseteq \mathcal{A} \setminus \{\tau\}$, *then* $(Q_1 \parallel_L Q_2) \setminus \mathcal{A}_{\mathcal{H}} \approx_{\rm b} (R_1 \parallel_L R_2) \setminus \mathcal{A}_{\mathcal{H}}$ *for all* $Q_1, R_1 \in \mathit{reach}(P_1)$ *and* $Q_2, R_2 \in \mathit{reach}(P_2)$ *such that* $Q_1 \parallel_L Q_2, R_1 \parallel_L R_2 \in \mathit{reach}(P_1 \parallel_L P_2)$, $Q_1 \setminus \mathcal{A}_{\mathcal{H}} \approx_{\rm b} R_1 \setminus \mathcal{A}_{\mathcal{H}}$ *and* $Q_2 \setminus \mathcal{A}_{\mathcal{H}} \approx_{\rm b} R_2 \setminus \mathcal{A}_{\mathcal{H}}$.

Proof. Let $\mathcal{B}$ be a symmetric relation containing all the pairs of processes that have to be shown to be $\approx_{\mathrm{b}}$-equivalent according to the considered result:

1. Starting from $(Q_1 \parallel_L Q_2) \setminus \mathcal{A}_{\mathcal{H}}$ and $(R_1 \parallel_L R_2) \,/\, \mathcal{A}_{\mathcal{H}}$ related by $\mathcal{B}$, so that $Q_1 \setminus \mathcal{A}_{\mathcal{H}} \approx_{\mathrm{b}} R_1 \,/\, \mathcal{A}_{\mathcal{H}}$ and $Q_2 \setminus \mathcal{A}_{\mathcal{H}} \approx_{\mathrm{b}} R_2 \,/\, \mathcal{A}_{\mathcal{H}}$, there are twelve cases based on the operational semantic rules in Table 8.1. In the first five cases, it is $(Q_1 \parallel_L Q_2) \setminus \mathcal{A}_{\mathcal{H}}$ to move first:

   - If $(Q_1 \parallel_L Q_2) \setminus \mathcal{A}_{\mathcal{H}} \xrightarrow{l} (Q_1' \parallel_L Q_2) \setminus \mathcal{A}_{\mathcal{H}}$ with $Q_1 \xrightarrow{l} Q_1'$ and $l \notin L$, then $Q_1 \setminus \mathcal{A}_{\mathcal{H}} \xrightarrow{l} Q_1' \setminus \mathcal{A}_{\mathcal{H}}$ as $l \notin \mathcal{A}_{\mathcal{H}}$. From $Q_1 \setminus \mathcal{A}_{\mathcal{H}} \approx_{\mathrm{b}} R_1 \,/\, \mathcal{A}_{\mathcal{H}}$ it follows that there exists $R_1 \,/\, \mathcal{A}_{\mathcal{H}} \stackrel{\tau^*}{\Longrightarrow} \bar{R}_1 \,/\, \mathcal{A}_{\mathcal{H}} \xrightarrow{l} R_1' \,/\, \mathcal{A}_{\mathcal{H}}$ such that $Q_1 \setminus \mathcal{A}_{\mathcal{H}} \approx_{\mathrm{b}} \bar{R}_1 \,/\, \mathcal{A}_{\mathcal{H}}$ and $Q_1' \setminus \mathcal{A}_{\mathcal{H}} \approx_{\mathrm{b}} R_1' \,/\, \mathcal{A}_{\mathcal{H}}$. Since synchronization does not apply to τ and $l \notin L$, we have that $(R_1 \parallel_L R_2) \,/\, \mathcal{A}_{\mathcal{H}} \stackrel{\tau^*}{\Longrightarrow} (\bar{R}_1 \parallel_L R_2) \,/\, \mathcal{A}_{\mathcal{H}} \xrightarrow{l} (R_1' \parallel_L R_2) \,/\, \mathcal{A}_{\mathcal{H}}$ with $((Q_1 \parallel_L Q_2) \setminus \mathcal{A}_{\mathcal{H}}, (\bar{R}_1 \parallel_L R_2) \,/\, \mathcal{A}_{\mathcal{H}}) \in \mathcal{B}$ and $((Q_1' \parallel_L Q_2) \setminus \mathcal{A}_{\mathcal{H}}, (R_1' \parallel_L R_2) \,/\, \mathcal{A}_{\mathcal{H}}) \in \mathcal{B}$.
   - If $(Q_1 \parallel_L Q_2) \setminus \mathcal{A}_{\mathcal{H}} \xrightarrow{l} (Q_1 \parallel_L Q_2') \setminus \mathcal{A}_{\mathcal{H}}$ with $Q_2 \xrightarrow{l} Q_2'$ and $l \notin L$, then the proof is similar to the one of the previous case.
   - If $(Q_1 \parallel_L Q_2) \setminus \mathcal{A}_{\mathcal{H}} \xrightarrow{l} (Q_1' \parallel_L Q_2') \setminus \mathcal{A}_{\mathcal{H}}$ with $Q_i \xrightarrow{l} Q_i'$ for $i \in \{1, 2\}$ and $l \in L$, then $Q_i \setminus \mathcal{A}_{\mathcal{H}} \xrightarrow{l} Q_i' \setminus \mathcal{A}_{\mathcal{H}}$ as $l \notin \mathcal{A}_{\mathcal{H}}$. From $Q_i \setminus \mathcal{A}_{\mathcal{H}} \approx_{\mathrm{b}} R_i \,/\, \mathcal{A}_{\mathcal{H}}$ it follows that there exists $R_i \,/\, \mathcal{A}_{\mathcal{H}} \stackrel{\tau^*}{\Longrightarrow} \bar{R}_i \,/\, \mathcal{A}_{\mathcal{H}} \xrightarrow{l} R_i' \,/\, \mathcal{A}_{\mathcal{H}}$ such that $Q_i \setminus \mathcal{A}_{\mathcal{H}} \approx_{\mathrm{b}} \bar{R}_i \,/\, \mathcal{A}_{\mathcal{H}}$ and $Q_i' \setminus \mathcal{A}_{\mathcal{H}} \approx_{\mathrm{b}} R_i' \,/\, \mathcal{A}_{\mathcal{H}}$. Since synchronization does not apply to τ and $l \in L$, we have that $(R_1 \parallel_L R_2) \,/\, \mathcal{A}_{\mathcal{H}} \stackrel{\tau^*}{\Longrightarrow} (\bar{R}_1 \parallel_L \bar{R}_2) \,/\, \mathcal{A}_{\mathcal{H}} \xrightarrow{l} (R_1' \parallel_L R_2') \,/\, \mathcal{A}_{\mathcal{H}}$ with $((Q_1 \parallel_L Q_2) \setminus \mathcal{A}_{\mathcal{H}}, (\bar{R}_1 \parallel_L \bar{R}_2) \,/\, \mathcal{A}_{\mathcal{H}}) \in \mathcal{B}$ and $((Q_1' \parallel_L Q_2') \setminus \mathcal{A}_{\mathcal{H}}, (R_1' \parallel_L R_2') \,/\, \mathcal{A}_{\mathcal{H}}) \in \mathcal{B}$.
   - If $(Q_1 \parallel_L Q_2) \setminus \mathcal{A}_{\mathcal{H}} \xrightarrow{\tau} (Q_1' \parallel_L Q_2) \setminus \mathcal{A}_{\mathcal{H}}$ with $Q_1 \xrightarrow{\tau} Q_1'$, then $Q_1 \setminus \mathcal{A}_{\mathcal{H}} \xrightarrow{\tau} Q_1' \setminus \mathcal{A}_{\mathcal{H}}$ as $\tau \notin \mathcal{A}_{\mathcal{H}}$. From $Q_1 \setminus \mathcal{A}_{\mathcal{H}} \approx_{\mathrm{b}} R_1 \,/\, \mathcal{A}_{\mathcal{H}}$ it follows that either $Q_1' \setminus \mathcal{A}_{\mathcal{H}} \approx_{\mathrm{b}} R_1 \,/\, \mathcal{A}_{\mathcal{H}}$, or there exists $R_1 \,/\, \mathcal{A}_{\mathcal{H}} \stackrel{\tau^*}{\Longrightarrow} \bar{R}_1 \,/\, \mathcal{A}_{\mathcal{H}} \xrightarrow{\tau} R_1' \,/\, \mathcal{A}_{\mathcal{H}}$ such that $Q_1 \setminus \mathcal{A}_{\mathcal{H}} \approx_{\mathrm{b}} \bar{R}_1 \,/\, \mathcal{A}_{\mathcal{H}}$ and $Q_1' \setminus \mathcal{A}_{\mathcal{H}} \approx_{\mathrm{b}} R_1' \,/\, \mathcal{A}_{\mathcal{H}}$. Since synchronization does not apply to τ, in the former subcase $(R_1 \parallel_L R_2) \,/\, \mathcal{A}_{\mathcal{H}}$ is allowed to stay idle with $((Q_1' \parallel_L Q_2) \setminus \mathcal{A}_{\mathcal{H}}, (R_1 \parallel_L R_2) \,/\, \mathcal{A}_{\mathcal{H}}) \in \mathcal{B}$, while in the latter subcase $(R_1 \parallel_L R_2) \,/\, \mathcal{A}_{\mathcal{H}} \stackrel{\tau^*}{\Longrightarrow} (\bar{R}_1 \parallel_L R_2) \,/\, \mathcal{A}_{\mathcal{H}} \xrightarrow{\tau} (R_1' \parallel_L R_2) \,/\, \mathcal{A}_{\mathcal{H}}$ with $((Q_1 \parallel_L Q_2) \setminus \mathcal{A}_{\mathcal{H}}, (\bar{R}_1 \parallel_L R_2) \,/\, \mathcal{A}_{\mathcal{H}}) \in \mathcal{B}$ and $((Q_1' \parallel_L Q_2) \setminus \mathcal{A}_{\mathcal{H}}, (R_1' \parallel_L R_2) \,/\, \mathcal{A}_{\mathcal{H}}) \in \mathcal{B}$.
   - If $(Q_1 \parallel_L Q_2) \setminus \mathcal{A}_{\mathcal{H}} \xrightarrow{\tau} (Q_1 \parallel_L Q_2') \setminus \mathcal{A}_{\mathcal{H}}$ with $Q_2 \xrightarrow{\tau} Q_2'$, then the proof is similar to the one of the previous case.

   In the other seven cases, instead, it is $(R_1 \parallel_L R_2) \,/\, \mathcal{A}_{\mathcal{H}}$ to move first:

   - If $(R_1 \parallel_L R_2) \,/\, \mathcal{A}_{\mathcal{H}} \xrightarrow{l} (R_1' \parallel_L R_2) \,/\, \mathcal{A}_{\mathcal{H}}$ with $R_1 \xrightarrow{l} R_1'$ and $l \notin L$, then $R_1 \,/\, \mathcal{A}_{\mathcal{H}} \xrightarrow{l} R_1' \,/\, \mathcal{A}_{\mathcal{H}}$ as $l \notin \mathcal{A}_{\mathcal{H}}$. From $R_1 \,/\, \mathcal{A}_{\mathcal{H}} \approx_{\mathrm{b}} Q_1 \setminus \mathcal{A}_{\mathcal{H}}$ it follows that there exists $Q_1 \setminus \mathcal{A}_{\mathcal{H}} \stackrel{\tau^*}{\Longrightarrow} \bar{Q}_1 \setminus \mathcal{A}_{\mathcal{H}} \xrightarrow{l} Q_1' \setminus \mathcal{A}_{\mathcal{H}}$ such that $R_1 \,/\, \mathcal{A}_{\mathcal{H}} \approx_{\mathrm{b}} \bar{Q}_1 \setminus \mathcal{A}_{\mathcal{H}}$ and $R_1' \,/\, \mathcal{A}_{\mathcal{H}} \approx_{\mathrm{b}} Q_1' \setminus \mathcal{A}_{\mathcal{H}}$. Since synchronization does not apply to τ and $l \notin L$, we have that $(Q_1 \parallel_L Q_2) \setminus \mathcal{A}_{\mathcal{H}} \stackrel{\tau^*}{\Longrightarrow} (\bar{Q}_1 \parallel_L Q_2) \setminus \mathcal{A}_{\mathcal{H}} \xrightarrow{l} (Q_1' \parallel_L Q_2) \setminus \mathcal{A}_{\mathcal{H}}$ with $((R_1 \parallel_L R_2)/\mathcal{A}_{\mathcal{H}}, (\bar{Q}_1 \parallel_L Q_2) \setminus \mathcal{A}_{\mathcal{H}}) \in \mathcal{B}$ and $((R_1' \parallel_L R_2)/\mathcal{A}_{\mathcal{H}}, (Q_1' \parallel_L Q_2) \setminus \mathcal{A}_{\mathcal{H}}) \in \mathcal{B}$.
   - If $(R_1 \parallel_L R_2) \,/\, \mathcal{A}_{\mathcal{H}} \xrightarrow{l} (R_1 \parallel_L R_2') \,/\, \mathcal{A}_{\mathcal{H}}$ with $R_2 \xrightarrow{l} R_2'$ and $l \notin L$, then the proof is similar to the one of the previous case.

- If $(R_1 \parallel_L R_2) / \mathcal{A}_\mathcal{H} \xrightarrow{l} (R_1' \parallel_L R_2') / \mathcal{A}_\mathcal{H}$ with $R_i \xrightarrow{l} R_i'$ for $i \in \{1,2\}$ and $l \in L$, then $R_i / \mathcal{A}_\mathcal{H} \xrightarrow{l} R_i' / \mathcal{A}_\mathcal{H}$ as $l \notin \mathcal{A}_\mathcal{H}$. From $R_i / \mathcal{A}_\mathcal{H} \approx_\mathrm{b} Q_i \setminus \mathcal{A}_\mathcal{H}$ it follows that there exists $Q_i \setminus \mathcal{A}_\mathcal{H} \stackrel{\tau^*}{\Longrightarrow} \bar{Q}_i \setminus \mathcal{A}_\mathcal{H} \xrightarrow{l} Q_i' \setminus \mathcal{A}_\mathcal{H}$ with $R_i / \mathcal{A}_\mathcal{H} \approx_\mathrm{b} \bar{Q}_i \setminus \mathcal{A}_\mathcal{H}$ and $R_i' / \mathcal{A}_\mathcal{H} \approx_\mathrm{b} Q_i' \setminus \mathcal{A}_\mathcal{H}$. Since synchronization does not apply to τ and $l \in L$, we have that $(Q_1 \parallel_L Q_2) \setminus \mathcal{A}_\mathcal{H} \stackrel{\tau^*}{\Longrightarrow} (\bar{Q}_1 \parallel_L \bar{Q}_2) \setminus \mathcal{A}_\mathcal{H} \xrightarrow{l} (Q_1' \parallel_L Q_2') \setminus \mathcal{A}_\mathcal{H}$ with $((R_1 \parallel_L R_2)/\mathcal{A}_\mathcal{H}, (\bar{Q}_1 \parallel_L \bar{Q}_2) \setminus \mathcal{A}_\mathcal{H}) \in \mathcal{B}$ and $((R_1' \parallel_L R_2')/\mathcal{A}_\mathcal{H}, (Q_1' \parallel_L Q_2') \setminus \mathcal{A}_\mathcal{H}) \in \mathcal{B}$.
- If $(R_1 \parallel_L R_2) / \mathcal{A}_\mathcal{H} \xrightarrow{\tau} (R_1' \parallel_L R_2) / \mathcal{A}_\mathcal{H}$ with $R_1 \xrightarrow{\tau} R_1'$, then $R_1 / \mathcal{A}_\mathcal{H} \xrightarrow{\tau} R_1' / \mathcal{A}_\mathcal{H}$ as $\tau \notin \mathcal{A}_\mathcal{H}$. From $R_1 / \mathcal{A}_\mathcal{H} \approx_\mathrm{b} Q_1 \setminus \mathcal{A}_\mathcal{H}$ it follows that either $R_1' / \mathcal{A}_\mathcal{H} \approx_\mathrm{b} Q_1 \setminus \mathcal{A}_\mathcal{H}$, or there exists $Q_1 \setminus \mathcal{A}_\mathcal{H} \stackrel{\tau^*}{\Longrightarrow} \bar{Q}_1 \setminus \mathcal{A}_\mathcal{H} \xrightarrow{\tau} Q_1' \setminus \mathcal{A}_\mathcal{H}$ such that $R_1 / \mathcal{A}_\mathcal{H} \approx_\mathrm{b} \bar{Q}_1 \setminus \mathcal{A}_\mathcal{H}$ and $R_1' / \mathcal{A}_\mathcal{H} \approx_\mathrm{b} Q_1' \setminus \mathcal{A}_\mathcal{H}$. Since synchronization does not apply to τ, in the former subcase $(Q_1 \parallel_L Q_2) \setminus \mathcal{A}_\mathcal{H}$ is allowed to stay idle with $((R_1' \parallel_L R_2)/\mathcal{A}_\mathcal{H}, (Q_1 \parallel_L Q_2)\setminus\mathcal{A}_\mathcal{H}) \in \mathcal{B}$, while in the latter subcase $(Q_1 \parallel_L Q_2)\setminus\mathcal{A}_\mathcal{H} \stackrel{\tau^*}{\Longrightarrow} (\bar{Q}_1 \parallel_L Q_2)\setminus\mathcal{A}_\mathcal{H} \xrightarrow{\tau} (Q_1' \parallel_L Q_2)\setminus\mathcal{A}_\mathcal{H}$ with $((R_1 \parallel_L R_2)/\mathcal{A}_\mathcal{H}, (\bar{Q}_1 \parallel_L Q_2) \setminus \mathcal{A}_\mathcal{H}) \in \mathcal{B}$ and $((R_1' \parallel_L R_2)/\mathcal{A}_\mathcal{H}, (Q_1' \parallel_L Q_2) \setminus \mathcal{A}_\mathcal{H}) \in \mathcal{B}$.
- If $(R_1 \parallel_L R_2) / \mathcal{A}_\mathcal{H} \xrightarrow{\tau} (R_1 \parallel_L R_2') / \mathcal{A}_\mathcal{H}$ with $R_2 \xrightarrow{\tau} R_2'$, then the proof is similar to the one of the previous case.
- If $(R_1 \parallel_L R_2) / \mathcal{A}_\mathcal{H} \xrightarrow{\tau} (R_1' \parallel_L R_2) / \mathcal{A}_\mathcal{H}$ with $R_1 \xrightarrow{h} R_1'$ and $h \notin L$, then $R_1 / \mathcal{A}_\mathcal{H} \xrightarrow{\tau} R_1' / \mathcal{A}_\mathcal{H}$ as $h \in \mathcal{A}_\mathcal{H}$. The rest of the proof is like the one of the fourth case.
- If $(R_1 \parallel_L R_2) / \mathcal{A}_\mathcal{H} \xrightarrow{\tau} (R_1 \parallel_L R_2') / \mathcal{A}_\mathcal{H}$ with $R_2 \xrightarrow{h} R_2'$ and $h \notin L$, then the proof is similar to the one of the previous case.

2. Starting from $(Q / \mathcal{A}_\mathcal{H}) \setminus L$ and $(R \setminus L) / \mathcal{A}_\mathcal{H}$ related by $\mathcal{B}$, so that $Q / \mathcal{A}_\mathcal{H} \approx_\mathrm{b} R \setminus \mathcal{A}_\mathcal{H}$, there are six cases based on the operational semantic rules in Table 8.1. In the first three cases, it is $(Q / \mathcal{A}_\mathcal{H}) \setminus L$ to move first:

   - If $(Q / \mathcal{A}_\mathcal{H}) \setminus L \xrightarrow{l} (Q' / \mathcal{A}_\mathcal{H}) \setminus L$ with $Q \xrightarrow{l} Q'$ and $l \notin L$, then $Q / \mathcal{A}_\mathcal{H} \xrightarrow{l} Q' / \mathcal{A}_\mathcal{H}$ as $l \notin \mathcal{A}_\mathcal{H}$. From $Q / \mathcal{A}_\mathcal{H} \approx_\mathrm{b} R \setminus \mathcal{A}_\mathcal{H}$ it follows that there exists $R \setminus \mathcal{A}_\mathcal{H} \stackrel{\tau^*}{\Longrightarrow} \bar{R} \setminus \mathcal{A}_\mathcal{H} \xrightarrow{l} R' \setminus \mathcal{A}_\mathcal{H}$ such that $Q / \mathcal{A}_\mathcal{H} \approx_\mathrm{b} \bar{R} \setminus \mathcal{A}_\mathcal{H}$ and $Q' / \mathcal{A}_\mathcal{H} \approx_\mathrm{b} R' \setminus \mathcal{A}_\mathcal{H}$. Since the restriction and hiding operators do not apply to τ and l, we have that $(R \setminus L) / \mathcal{A}_\mathcal{H} \stackrel{\tau^*}{\Longrightarrow} (\bar{R} \setminus L) / \mathcal{A}_\mathcal{H} \xrightarrow{l} (R' \setminus L) / \mathcal{A}_\mathcal{H}$ with $((Q / \mathcal{A}_\mathcal{H}) \setminus L, (\bar{R} \setminus L) / \mathcal{A}_\mathcal{H}) \in \mathcal{B}$ and $((Q' / \mathcal{A}_\mathcal{H}) \setminus L, (R' \setminus L) / \mathcal{A}_\mathcal{H}) \in \mathcal{B}$.
   - If $(Q / \mathcal{A}_\mathcal{H}) \setminus L \xrightarrow{\tau} (Q' / \mathcal{A}_\mathcal{H}) \setminus L$ with $Q \xrightarrow{\tau} Q'$, then $Q / \mathcal{A}_\mathcal{H} \xrightarrow{\tau} Q' / \mathcal{A}_\mathcal{H}$ as $\tau \notin \mathcal{A}_\mathcal{H}$. From $Q / \mathcal{A}_\mathcal{H} \approx_\mathrm{b} R \setminus \mathcal{A}_\mathcal{H}$ it follows that either $Q' / \mathcal{A}_\mathcal{H} \approx_\mathrm{b} R \setminus \mathcal{A}_\mathcal{H}$, or there exists $R \setminus \mathcal{A}_\mathcal{H} \stackrel{\tau^*}{\Longrightarrow} \bar{R} \setminus \mathcal{A}_\mathcal{H} \xrightarrow{\tau} R' \setminus \mathcal{A}_\mathcal{H}$ such that $Q / \mathcal{A}_\mathcal{H} \approx_\mathrm{b} \bar{R} \setminus \mathcal{A}_\mathcal{H}$ and $Q' / \mathcal{A}_\mathcal{H} \approx_\mathrm{b} R' \setminus \mathcal{A}_\mathcal{H}$. Since the restriction and hiding operators do not apply to τ, in the former subcase $(R \setminus L) / \mathcal{A}_\mathcal{H}$ is allowed to stay idle with $((Q' / \mathcal{A}_\mathcal{H}) \setminus L, (R \setminus L) / \mathcal{A}_\mathcal{H}) \in \mathcal{B}$, while in the latter subcase $(R \setminus L) / \mathcal{A}_\mathcal{H} \stackrel{\tau^*}{\Longrightarrow} (\bar{R} \setminus L) / \mathcal{A}_\mathcal{H} \xrightarrow{\tau} (R' \setminus L) / \mathcal{A}_\mathcal{H}$ with $((Q / \mathcal{A}_\mathcal{H}) \setminus L, (\bar{R} \setminus L) / \mathcal{A}_\mathcal{H}) \in \mathcal{B}$ and $((Q' / \mathcal{A}_\mathcal{H}) \setminus L, (R' \setminus L) / \mathcal{A}_\mathcal{H}) \in \mathcal{B}$.
   - If $(Q / \mathcal{A}_\mathcal{H}) \setminus L \xrightarrow{\tau} (Q' / \mathcal{A}_\mathcal{H}) \setminus L$ with $Q \xrightarrow{h} Q'$, then $Q / \mathcal{A}_\mathcal{H} \xrightarrow{\tau} Q' / \mathcal{A}_\mathcal{H}$ as $h \in \mathcal{A}_\mathcal{H}$. The rest of the proof is similar to the one of the previous case.

   In the other three cases, instead, it is $(R \setminus L) / \mathcal{A}_\mathcal{H}$ to move first:

   - If $(R \setminus L) / \mathcal{A}_\mathcal{H} \xrightarrow{l} (R' \setminus L) / \mathcal{A}_\mathcal{H}$ with $R \xrightarrow{l} R'$ and $l \notin L$, then $R \setminus \mathcal{A}_\mathcal{H} \xrightarrow{l} R' \setminus \mathcal{A}_\mathcal{H}$ as $l \notin \mathcal{A}_\mathcal{H}$. From $R \setminus \mathcal{A}_\mathcal{H} \approx_\mathrm{b} Q / \mathcal{A}_\mathcal{H}$ it follows that there exists $Q / \mathcal{A}_\mathcal{H} \stackrel{\tau^*}{\Longrightarrow} \bar{Q} / \mathcal{A}_\mathcal{H} \xrightarrow{l} Q' / \mathcal{A}_\mathcal{H}$ such that $R \setminus \mathcal{A}_\mathcal{H}$

$\approx_{\mathrm{b}} \bar{Q} / \mathcal{A}_{\mathcal{H}}$ and $R' \setminus \mathcal{A}_{\mathcal{H}} \approx_{\mathrm{b}} Q' / \mathcal{A}_{\mathcal{H}}$. Since the restriction operator does not apply to τ and l, we have that $(Q / \mathcal{A}_{\mathcal{H}}) \setminus L \stackrel{\tau^*}{\Longrightarrow} (\bar{Q} / \mathcal{A}_{\mathcal{H}}) \setminus L \stackrel{l}{\longrightarrow} (Q' / \mathcal{A}_{\mathcal{H}}) \setminus L$ with $((R \setminus L) / \mathcal{A}_{\mathcal{H}}, (\bar{Q} / \mathcal{A}_{\mathcal{H}}) \setminus L) \in \mathcal{B}$ and $((R' \setminus L) / \mathcal{A}_{\mathcal{H}}, (Q' / \mathcal{A}_{\mathcal{H}}) \setminus L) \in \mathcal{B}$.

- If $(R \setminus L) / \mathcal{A}_{\mathcal{H}} \stackrel{\tau}{\longrightarrow} (R' \setminus L) / \mathcal{A}_{\mathcal{H}}$ with $R \stackrel{\tau}{\longrightarrow} R'$, then $R \setminus \mathcal{A}_{\mathcal{H}} \stackrel{\tau}{\longrightarrow} R' \setminus \mathcal{A}_{\mathcal{H}}$ as $\tau \notin \mathcal{A}_{\mathcal{H}}$. From $R \setminus \mathcal{A}_{\mathcal{H}} \approx_{\mathrm{b}} Q / \mathcal{A}_{\mathcal{H}}$ it follows that either $R' \setminus \mathcal{A}_{\mathcal{H}} \approx_{\mathrm{b}} Q / \mathcal{A}_{\mathcal{H}}$, or there exists $Q / \mathcal{A}_{\mathcal{H}} \stackrel{\tau^*}{\Longrightarrow} \bar{Q} / \mathcal{A}_{\mathcal{H}} \stackrel{\tau}{\longrightarrow} Q' / \mathcal{A}_{\mathcal{H}}$ such that $R \setminus \mathcal{A}_{\mathcal{H}} \approx_{\mathrm{b}} \bar{Q} / \mathcal{A}_{\mathcal{H}}$ and $R' \setminus \mathcal{A}_{\mathcal{H}} \approx_{\mathrm{b}} Q' / \mathcal{A}_{\mathcal{H}}$. Since the restriction operator does not apply to τ, in the former subcase $(Q / \mathcal{A}_{\mathcal{H}}) \setminus L$ is allowed to stay idle with $((R' \setminus L) / \mathcal{A}_{\mathcal{H}}, (Q / \mathcal{A}_{\mathcal{H}}) \setminus L) \in \mathcal{B}$, while in the latter subcase $(Q / \mathcal{A}_{\mathcal{H}}) \setminus L \stackrel{\tau^*}{\Longrightarrow} (\bar{Q} / \mathcal{A}_{\mathcal{H}}) \setminus L \stackrel{\tau}{\longrightarrow} (Q' / \mathcal{A}_{\mathcal{H}}) \setminus L$ with $((R \setminus L) / \mathcal{A}_{\mathcal{H}}, (\bar{Q} / \mathcal{A}_{\mathcal{H}}) \setminus L) \in \mathcal{B}$ and $((R' \setminus L) / \mathcal{A}_{\mathcal{H}}, (Q' / \mathcal{A}_{\mathcal{H}}) \setminus L) \in \mathcal{B}$.
- If $(R \setminus L) / \mathcal{A}_{\mathcal{H}} \stackrel{\tau}{\longrightarrow} (R' \setminus L) / \mathcal{A}_{\mathcal{H}}$ with $R \stackrel{h}{\longrightarrow} R'$ and $h \notin L$, then $R / \mathcal{A}_{\mathcal{H}} \stackrel{\tau}{\longrightarrow} R' / \mathcal{A}_{\mathcal{H}}$ as $h \in \mathcal{A}_{\mathcal{H}}$ (note that $R \setminus \mathcal{A}_{\mathcal{H}}$ cannot perform h). From $R / \mathcal{A}_{\mathcal{H}} \approx_{\mathrm{b}} R \setminus \mathcal{A}_{\mathcal{H}}$ – as $P \in \mathrm{SBSNNI}_{\approx_{\mathrm{b}}}$ and $R \in \mathit{reach}(P)$ – and $R \setminus \mathcal{A}_{\mathcal{H}} \approx_{\mathrm{b}} Q / \mathcal{A}_{\mathcal{H}}$ it follows that either $R' / \mathcal{A}_{\mathcal{H}} \approx_{\mathrm{b}} Q / \mathcal{A}_{\mathcal{H}}$ and hence $R' \setminus \mathcal{A}_{\mathcal{H}} \approx_{\mathrm{b}} Q / \mathcal{A}_{\mathcal{H}}$ – as $R' / \mathcal{A}_{\mathcal{H}} \approx_{\mathrm{b}} R' \setminus \mathcal{A}_{\mathcal{H}}$ due to $P \in \mathrm{SBSNNI}_{\approx_{\mathrm{b}}}$ and $R' \in \mathit{reach}(P)$ – or there exists $Q / \mathcal{A}_{\mathcal{H}} \stackrel{\tau^*}{\Longrightarrow} \bar{Q} / \mathcal{A}_{\mathcal{H}} \stackrel{\tau}{\longrightarrow} Q' / \mathcal{A}_{\mathcal{H}}$ such that $R / \mathcal{A}_{\mathcal{H}} \approx_{\mathrm{b}} \bar{Q} / \mathcal{A}_{\mathcal{H}}$ and $R' / \mathcal{A}_{\mathcal{H}} \approx_{\mathrm{b}} Q' / \mathcal{A}_{\mathcal{H}}$ and hence $R \setminus \mathcal{A}_{\mathcal{H}} \approx_{\mathrm{b}} \bar{Q} / \mathcal{A}_{\mathcal{H}}$ and $R' \setminus \mathcal{A}_{\mathcal{H}} \approx_{\mathrm{b}} Q' / \mathcal{A}_{\mathcal{H}}$. Since the restriction operator does not apply to τ, in the former subcase $(Q / \mathcal{A}_{\mathcal{H}}) \setminus L$ is allowed to stay idle with $((R' \setminus L) / \mathcal{A}_{\mathcal{H}}, (Q / \mathcal{A}_{\mathcal{H}}) \setminus L) \in \mathcal{B}$, while in the latter subcase $(Q / \mathcal{A}_{\mathcal{H}}) \setminus L \stackrel{\tau^*}{\Longrightarrow} (\bar{Q} / \mathcal{A}_{\mathcal{H}}) \setminus L \stackrel{\tau}{\longrightarrow} (Q' / \mathcal{A}_{\mathcal{H}}) \setminus L$ with $((R \setminus L) / \mathcal{A}_{\mathcal{H}}, (\bar{Q} / \mathcal{A}_{\mathcal{H}}) \setminus L) \in \mathcal{B}$ and $((R' \setminus L) / \mathcal{A}_{\mathcal{H}}, (Q' / \mathcal{A}_{\mathcal{H}}) \setminus L) \in \mathcal{B}$.

3. Starting from $(Q_1 \parallel_L Q_2) \setminus \mathcal{A}_{\mathcal{H}}$ and $(R_1 \parallel_L R_2) \setminus \mathcal{A}_{\mathcal{H}}$ related by $\mathcal{B}$, so that $Q_1 \setminus \mathcal{A}_{\mathcal{H}} \approx_{\mathrm{b}} R_1 \setminus \mathcal{A}_{\mathcal{H}}$ and $Q_2 \setminus \mathcal{A}_{\mathcal{H}} \approx_{\mathrm{b}} R_2 \setminus \mathcal{A}_{\mathcal{H}}$, there are five cases based on the operational semantic rules in Table 8.1:

   - If $(Q_1 \parallel_L Q_2) \setminus \mathcal{A}_{\mathcal{H}} \stackrel{l}{\longrightarrow} (Q_1' \parallel_L Q_2) \setminus \mathcal{A}_{\mathcal{H}}$ with $Q_1 \stackrel{l}{\longrightarrow} Q_1'$ and $l \notin L$, then $Q_1 \setminus \mathcal{A}_{\mathcal{H}} \stackrel{l}{\longrightarrow} Q_1' \setminus \mathcal{A}_{\mathcal{H}}$ as $l \notin \mathcal{A}_{\mathcal{H}}$. From $Q_1 \setminus \mathcal{A}_{\mathcal{H}} \approx_{\mathrm{b}} R_1 \setminus \mathcal{A}_{\mathcal{H}}$ it follows that there exists $R_1 \setminus \mathcal{A}_{\mathcal{H}} \stackrel{\tau^*}{\Longrightarrow} \bar{R}_1 \setminus \mathcal{A}_{\mathcal{H}} \stackrel{l}{\longrightarrow} R_1' \setminus \mathcal{A}_{\mathcal{H}}$ such that $Q_1 \setminus \mathcal{A}_{\mathcal{H}} \approx_{\mathrm{b}} \bar{R}_1 \setminus \mathcal{A}_{\mathcal{H}}$ and $Q_1' \setminus \mathcal{A}_{\mathcal{H}} \approx_{\mathrm{b}} R_1' \setminus \mathcal{A}_{\mathcal{H}}$. Since synchronization does not apply to τ and $l \notin L$, we have that $(R_1 \parallel_L R_2) \setminus \mathcal{A}_{\mathcal{H}} \stackrel{\tau^*}{\Longrightarrow} (\bar{R}_1 \parallel_L R_2) \setminus \mathcal{A}_{\mathcal{H}} \stackrel{l}{\longrightarrow} (R_1' \parallel_L R_2) \setminus \mathcal{A}_{\mathcal{H}}$ with $((Q_1 \parallel_L Q_2) \setminus \mathcal{A}_{\mathcal{H}}, (\bar{R}_1 \parallel_L R_2) \setminus \mathcal{A}_{\mathcal{H}}) \in \mathcal{B}$ and $((Q_1' \parallel_L Q_2) \setminus \mathcal{A}_{\mathcal{H}}, (R_1' \parallel_L R_2) \setminus \mathcal{A}_{\mathcal{H}}) \in \mathcal{B}$.
   - If $(Q_1 \parallel_L Q_2) \setminus \mathcal{A}_{\mathcal{H}} \stackrel{l}{\longrightarrow} (Q_1 \parallel_L Q_2') \setminus \mathcal{A}_{\mathcal{H}}$ with $Q_2 \stackrel{l}{\longrightarrow} Q_2'$ and $l \notin L$, then the proof is similar to the one of the previous case.
   - If $(Q_1 \parallel_L Q_2) \setminus \mathcal{A}_{\mathcal{H}} \stackrel{l}{\longrightarrow} (Q_1' \parallel_L Q_2') \setminus \mathcal{A}_{\mathcal{H}}$ with $Q_i \stackrel{l}{\longrightarrow} Q_i'$ for $i \in \{1, 2\}$ and $l \in L$, then $Q_i \setminus \mathcal{A}_{\mathcal{H}} \stackrel{l}{\longrightarrow} Q_i' \setminus \mathcal{A}_{\mathcal{H}}$ as $l \notin \mathcal{A}_{\mathcal{H}}$. From $Q_i \setminus \mathcal{A}_{\mathcal{H}} \approx_{\mathrm{b}} R_i \setminus \mathcal{A}_{\mathcal{H}}$ it follows that there exists $R_i \setminus \mathcal{A}_{\mathcal{H}} \stackrel{\tau^*}{\Longrightarrow} \bar{R}_i \setminus \mathcal{A}_{\mathcal{H}} \stackrel{l}{\longrightarrow} R_i' \setminus \mathcal{A}_{\mathcal{H}}$ such that $Q_i \setminus \mathcal{A}_{\mathcal{H}} \approx_{\mathrm{b}} \bar{R}_i \setminus \mathcal{A}_{\mathcal{H}}$ and $Q_i' \setminus \mathcal{A}_{\mathcal{H}} \approx_{\mathrm{b}} R_i' \setminus \mathcal{A}_{\mathcal{H}}$. Since synchronization does not apply to τ and $l \in L$, we have that $(R_1 \parallel_L R_2) \setminus \mathcal{A}_{\mathcal{H}} \stackrel{\tau^*}{\Longrightarrow} (\bar{R}_1 \parallel_L \bar{R}_2) \setminus \mathcal{A}_{\mathcal{H}} \stackrel{l}{\longrightarrow} (R_1' \parallel_L R_2') \setminus \mathcal{A}_{\mathcal{H}}$ with $((Q_1 \parallel_L Q_2) \setminus \mathcal{A}_{\mathcal{H}}, (\bar{R}_1 \parallel_L \bar{R}_2) \setminus \mathcal{A}_{\mathcal{H}}) \in \mathcal{B}$ and $((Q_1' \parallel_L Q_2') \setminus \mathcal{A}_{\mathcal{H}}, (R_1' \parallel_L R_2') \setminus \mathcal{A}_{\mathcal{H}}) \in \mathcal{B}$.
   - If $(Q_1 \parallel_L Q_2) \setminus \mathcal{A}_{\mathcal{H}} \stackrel{\tau}{\longrightarrow} (Q_1' \parallel_L Q_2) \setminus \mathcal{A}_{\mathcal{H}}$ with $Q_1 \stackrel{\tau}{\longrightarrow} Q_1'$, then $Q_1 \setminus \mathcal{A}_{\mathcal{H}} \stackrel{\tau}{\longrightarrow} Q_1' \setminus \mathcal{A}_{\mathcal{H}}$ as $\tau \notin \mathcal{A}_{\mathcal{H}}$. From $Q_1 \setminus \mathcal{A}_{\mathcal{H}} \approx_{\mathrm{b}} R_1 \setminus \mathcal{A}_{\mathcal{H}}$ it follows that either $Q_1' \setminus \mathcal{A}_{\mathcal{H}} \approx_{\mathrm{b}} R_1 \setminus \mathcal{A}_{\mathcal{H}}$, or there exists $R_1 \setminus \mathcal{A}_{\mathcal{H}} \stackrel{\tau^*}{\Longrightarrow} \bar{R}_1 \setminus \mathcal{A}_{\mathcal{H}} \stackrel{\tau}{\longrightarrow} R_1' \setminus \mathcal{A}_{\mathcal{H}}$ such that $Q_1 \setminus \mathcal{A}_{\mathcal{H}} \approx_{\mathrm{b}} \bar{R}_1 \setminus \mathcal{A}_{\mathcal{H}}$ and $Q_1' \setminus \mathcal{A}_{\mathcal{H}} \approx_{\mathrm{b}} R_1' \setminus \mathcal{A}_{\mathcal{H}}$. Since synchronization does not apply to τ, in the former subcase $(R_1 \parallel_L R_2) \setminus \mathcal{A}_{\mathcal{H}}$ is allowed to stay idle with $((Q_1' \parallel_L Q_2) \setminus \mathcal{A}_{\mathcal{H}}, (R_1 \parallel_L R_2) \setminus \mathcal{A}_{\mathcal{H}}) \in \mathcal{B}$, while in the latter subcase $(R_1 \parallel_L R_2) \setminus \mathcal{A}_{\mathcal{H}} \stackrel{\tau^*}{\Longrightarrow} (\bar{R}_1 \parallel_L R_2) \setminus \mathcal{A}_{\mathcal{H}} \stackrel{\tau}{\longrightarrow} (R_1' \parallel_L R_2) \setminus \mathcal{A}_{\mathcal{H}}$ with $((Q_1 \parallel_L Q_2) \setminus \mathcal{A}_{\mathcal{H}}, (\bar{R}_1 \parallel_L R_2) \setminus \mathcal{A}_{\mathcal{H}}) \in \mathcal{B}$ and $((Q_1' \parallel_L Q_2) \setminus \mathcal{A}_{\mathcal{H}}, (R_1' \parallel_L R_2) \setminus \mathcal{A}_{\mathcal{H}}) \in \mathcal{B}$.

- If $(Q_1 \parallel_L Q_2) \setminus \mathcal{A}_\mathcal{H} \xrightarrow{\tau} (Q_1 \parallel_L Q_2') \setminus \mathcal{A}_\mathcal{H}$ with $Q_2 \xrightarrow{\tau} Q_2'$, then the proof is similar to the one of the previous case. ■

Theorem 8.3. *Let* $P, P_1, P_2 \in \mathbb{P}_{\mathrm{nd}}$ *and* $\mathcal{P} \in \{\mathrm{SBSNNI}_{\approx_\mathrm{b}}, \mathrm{P\_BNDC}_{\approx_\mathrm{b}}, \mathrm{SBNDC}_{\approx_\mathrm{b}}\}$. *Then:*

1. $P \in \mathcal{P} \Longrightarrow a \,.\, P \in \mathcal{P}$ *for all* $a \in \mathcal{A}_\mathcal{L} \cup \{\tau\}$.
2. $P_1, P_2 \in \mathcal{P} \Longrightarrow P_1 \parallel_L P_2 \in \mathcal{P}$ *for all* $L \subseteq \mathcal{A}_\mathcal{L}$ *if* $\mathcal{P} \in \{\mathrm{SBSNNI}_{\approx_\mathrm{b}}, \mathrm{P\_BNDC}_{\approx_\mathrm{b}}\}$ *or for all* $L \subseteq \mathcal{A} \setminus \{\tau\}$ *if* $\mathcal{P} = \mathrm{SBNDC}_{\approx_\mathrm{b}}$.
3. $P \in \mathcal{P} \Longrightarrow P \setminus L \in \mathcal{P}$ *for all* $L \subseteq \mathcal{A} \setminus \{\tau\}$.
4. $P \in \mathcal{P} \Longrightarrow P \,/\, L \in \mathcal{P}$ *for all* $L \subseteq \mathcal{A}_\mathcal{L}$.

Proof. We first prove the four results for $\mathrm{SBSNNI}_{\approx_\mathrm{b}}$, from which it will follow that they hold for $\mathrm{P\_BNDC}_{\approx_\mathrm{b}}$ too by virtue of the forthcoming Theorem 8.4:

1. Given an arbitrary $P \in \mathrm{SBSNNI}_{\approx_\mathrm{b}}$ and an arbitrary $a \in \mathcal{A}_\mathcal{L} \cup \{\tau\}$, from $P \setminus \mathcal{A}_\mathcal{H} \approx_\mathrm{b} P \,/\, \mathcal{A}_\mathcal{H}$ we derive that $a \,.\, (P \setminus \mathcal{A}_\mathcal{H}) \approx_\mathrm{b} a \,.\, (P \,/\, \mathcal{A}_\mathcal{H})$ because $\approx_\mathrm{b}$ is a congruence with respect to action prefix [80], from which it follows that $(a \,.\, P) \setminus \mathcal{A}_\mathcal{H} \approx_\mathrm{b} (a \,.\, P) \,/\, \mathcal{A}_\mathcal{H}$, i.e., $a \,.\, P \in \mathrm{BrSNNI}_{\approx_\mathrm{b}}$, because $a \notin \mathcal{A}_\mathcal{H}$. To conclude the proof, it suffices to observe that all the processes reachable from $a \,.\, P$ after performing a are processes reachable from P, which are known to be $\mathrm{BSNNI}_{\approx_\mathrm{b}}$.
2. Given two arbitrary $P_1, P_2 \in \mathrm{SBSNNI}_{\approx_\mathrm{b}}$ and an arbitrary $L \subseteq \mathcal{A}_\mathcal{L}$, the result follows from Lemma 8.2(1) by taking Q_1 identical to R_1 and Q_2 identical to R_2.
3. Given an arbitrary $P \in \mathrm{SBSNNI}_{\approx_\mathrm{b}}$ and an arbitrary $L \subseteq \mathcal{A} \setminus \{\tau\}$, the result follows from Lemma 8.2(2) by taking Q identical to R – which will be denoted by P' – because:
   - $(P' \setminus L) \setminus \mathcal{A}_\mathcal{H} \approx_\mathrm{b} (P' \setminus \mathcal{A}_\mathcal{H}) \setminus L$ as the order in which restriction sets are considered is unimportant.
   - $(P' \setminus \mathcal{A}_\mathcal{H}) \setminus L \approx_\mathrm{b} (P' \,/\, \mathcal{A}_\mathcal{H}) \setminus L$ because $P' \setminus \mathcal{A}_\mathcal{H} \approx_\mathrm{b} P' \,/\, \mathcal{A}_\mathcal{H}$ – as $P \in \mathrm{SBSNNI}_{\approx_\mathrm{b}}$ and $P' \in \mathit{reach}(P)$ – and $\approx_\mathrm{b}$ is a congruence with respect to the restriction operator due to Lemma 8.1(2).
   - $(P' \,/\, \mathcal{A}_\mathcal{H}) \setminus L \approx_\mathrm{b} (P' \setminus L) \,/\, \mathcal{A}_\mathcal{H}$ as shown in Lemma 8.2(2).
   - From the transitivity of $\approx_\mathrm{b}$ we obtain that $(P' \setminus L) \setminus \mathcal{A}_\mathcal{H} \approx_\mathrm{b} (P' \setminus L) \,/\, \mathcal{A}_\mathcal{H}$.
4. Given an arbitrary $P \in \mathrm{SBSNNI}_{\approx_\mathrm{b}}$ and an arbitrary $L \subseteq \mathcal{A}_\mathcal{L}$, for every $P' \in \mathit{reach}(P)$ it holds that $P' \setminus \mathcal{A}_\mathcal{H} \approx_\mathrm{b} P' \,/\, \mathcal{A}_\mathcal{H}$, from which we derive that $(P' \setminus \mathcal{A}_\mathcal{H}) \,/\, L \approx_\mathrm{b} (P' \,/\, \mathcal{A}_\mathcal{H}) \,/\, L$ because $\approx_\mathrm{b}$ is a congruence with respect to the hiding operator due to Lemma 8.1(3). Since $L \cap \mathcal{A}_\mathcal{H} = \emptyset$, we have that $(P' \setminus \mathcal{A}_\mathcal{H}) \,/\, L$ is isomorphic to $(P' \,/\, L) \setminus \mathcal{A}_\mathcal{H}$ and $(P' \,/\, \mathcal{A}_\mathcal{H}) \,/\, L$ is isomorphic to $(P' \,/\, L) \,/\, \mathcal{A}_\mathcal{H}$, hence $(P' \,/\, L) \setminus \mathcal{A}_\mathcal{H} \approx_\mathrm{b} (P' \,/\, L) \,/\, \mathcal{A}_\mathcal{H}$, i.e., $P' \,/\, L$ is $\mathrm{BSNNI}_{\approx_\mathrm{b}}$.

We then prove the four results for $\mathrm{SBNDC}_{\approx_\mathrm{b}}$:

1. Given an arbitrary $P \in \mathrm{SBNDC}_{\approx_\mathrm{b}}$ and an arbitrary $a \in \mathcal{A}_\mathcal{L} \cup \{\tau\}$, it trivially holds that $a\,.\,P \in \mathrm{SBNDC}_{\approx_\mathrm{b}}$ because a is not high and all the processes reachable from $a\,.\,P$ after performing a are processes reachable from P, which is known to be $\mathrm{SBNDC}_{\approx_\mathrm{b}}$.

2. Given two arbitrary $P_1, P_2 \in \mathrm{SBNDC}_{\approx_\mathrm{b}}$ and an arbitrary $L \subseteq \mathcal{A} \setminus \{\tau\}$, the result follows from Lemma 8.2(3) as can be seen by observing that whenever $P_1' \parallel_L P_2' \xrightarrow{h} P_1'' \parallel_L P_2''$ for $P_1' \parallel_L P_2' \in \mathit{reach}(P_1 \parallel_L P_2)$:

   - If $P_1' \xrightarrow{h} P_1''$, $P_2'' = P_2'$ (hence $P_2' \setminus \mathcal{A}_\mathcal{H} \approx_\mathrm{b} P_2'' \setminus \mathcal{A}_\mathcal{H}$), and $h \notin L$, then from $P_1 \in \mathrm{SBNDC}_{\approx_\mathrm{b}}$ it follows that $P_1' \setminus \mathcal{A}_\mathcal{H} \approx_\mathrm{b} P_1'' \setminus \mathcal{A}_\mathcal{H}$, which in turn entails that $(P_1' \parallel_L P_2') \setminus \mathcal{A}_\mathcal{H} \approx_\mathrm{b} (P_1'' \parallel_L P_2'') \setminus \mathcal{A}_\mathcal{H}$ because $\approx_\mathrm{b}$ is a congruence with respect to the parallel composition operator due to Lemma 8.1(1) and restriction distributes over parallel composition.
   - If $P_2' \xrightarrow{h} P_2''$, $P_1'' = P_1'$, and $h \notin L$, then we reason like in the previous case.
   - If $P_1' \xrightarrow{h} P_1''$, $P_2' \xrightarrow{h} P_2''$, and $h \in L$, then from $P_1, P_2 \in \mathrm{SBNDC}_{\approx_\mathrm{b}}$ it follows that $P_1' \setminus \mathcal{A}_\mathcal{H} \approx_\mathrm{b} P_1'' \setminus \mathcal{A}_\mathcal{H}$ and $P_2' \setminus \mathcal{A}_\mathcal{H} \approx_\mathrm{b} P_2'' \setminus \mathcal{A}_\mathcal{H}$, which in turn entail that $(P_1' \parallel_L P_2') \setminus \mathcal{A}_\mathcal{H} \approx_\mathrm{b} (P_1'' \parallel_L P_2'') \setminus \mathcal{A}_\mathcal{H}$ because $\approx_\mathrm{b}$ is a congruence with respect to the parallel composition operator due to Lemma 8.1(1) and restriction distributes over parallel composition.

3. Given an arbitrary $P \in \mathrm{SBNDC}_{\approx_\mathrm{b}}$ and an arbitrary $L \subseteq \mathcal{A} \setminus \{\tau\}$, for every $P' \in \mathit{reach}(P)$ and for every P'' such that $P' \xrightarrow{h} P''$ it holds that $P' \setminus \mathcal{A}_\mathcal{H} \approx_\mathrm{b} P'' \setminus \mathcal{A}_\mathcal{H}$, from which we derive that $(P' \setminus \mathcal{A}_\mathcal{H}) \setminus L \approx_\mathrm{b} (P'' \setminus \mathcal{A}_\mathcal{H}) \setminus L$ because $\approx_\mathrm{b}$ is a congruence with respect to the restriction operator due to Lemma 8.1(2). Since $(P' \setminus \mathcal{A}_\mathcal{H}) \setminus L$ is isomorphic to $(P' \setminus L) \setminus \mathcal{A}_\mathcal{H}$ and $(P'' \setminus \mathcal{A}_\mathcal{H}) \setminus L$ is isomorphic to $(P'' \setminus L) \setminus \mathcal{A}_\mathcal{H}$, we have that $(P' \setminus L) \setminus \mathcal{A}_\mathcal{H} \approx_\mathrm{b} (P'' \setminus L) \setminus \mathcal{A}_\mathcal{H}$.

4. Given an arbitrary $P \in \mathrm{SBNDC}_{\approx_\mathrm{b}}$ and an arbitrary $L \subseteq \mathcal{A}_\mathcal{L}$, for every $P' \in \mathit{reach}(P)$ and for every P'' such that $P' \xrightarrow{h} P''$ it holds that $P' \setminus \mathcal{A}_\mathcal{H} \approx_\mathrm{b} P'' \setminus \mathcal{A}_\mathcal{H}$, from which we derive that $(P' \setminus \mathcal{A}_\mathcal{H}) / L \approx_\mathrm{b} (P'' \setminus \mathcal{A}_\mathcal{H}) / L$ because $\approx_\mathrm{b}$ is a congruence with respect to the hiding operator due to Lemma 8.1(3). Since $L \cap \mathcal{A}_\mathcal{H} = \emptyset$, we have that $(P' \setminus \mathcal{A}_\mathcal{H}) / L$ is isomorphic to $(P' / L) \setminus \mathcal{A}_\mathcal{H}$ and $(P'' \setminus \mathcal{A}_\mathcal{H}) / L$ is isomorphic to $(P'' / L) \setminus \mathcal{A}_\mathcal{H}$, hence $(P' / L) \setminus \mathcal{A}_\mathcal{H} \approx_\mathrm{b} (P'' / L) \setminus \mathcal{A}_\mathcal{H}$. ■

As far as parallel composition is concerned, the compositionality of $\mathrm{SBSNNI}_{\approx_\mathrm{b}}$ holds only for all $L \subseteq \mathcal{A}_\mathcal{L}$. As an example, both $P_1 = h\,.\,\underline{0} + l_1\,.\,\underline{0} + \tau\,.\,\underline{0}$ and $P_2 = h\,.\,\underline{0} + l_2\,.\,\underline{0} + \tau\,.\,\underline{0}$ are $\mathrm{SBSNNI}_{\approx_\mathrm{b}}$, but $P_1 \parallel_{\{h\}} P_2$ is not because the transition $(P_1 \parallel_{\{h\}} P_2) / \mathcal{A}_\mathcal{H} \xrightarrow{\tau} (\underline{0} \parallel_{\{h\}} \underline{0}) / \mathcal{A}_\mathcal{H}$ arising from the synchronization between the two h-actions cannot be matched by $(P_1 \parallel_{\{h\}} P_2) \setminus \mathcal{A}_\mathcal{H}$ in the branching bisimulation game. Indeed, the only two possibilities are $(P_1 \parallel_{\{h\}} P_2) \setminus \mathcal{A}_\mathcal{H} \xRightarrow{\tau^*} (P_1 \parallel_{\{h\}} P_2) \setminus \mathcal{A}_\mathcal{H} \xrightarrow{\tau} (\underline{0} \parallel_{\{h\}} P_2) \setminus \mathcal{A}_\mathcal{H} \xrightarrow{\tau} (\underline{0} \parallel_{\{h\}} \underline{0}) \setminus \mathcal{A}_\mathcal{H}$ and $(P_1 \parallel_{\{h\}} P_2) \setminus \mathcal{A}_\mathcal{H} \xRightarrow{\tau^*} (P_1 \parallel_{\{h\}} P_2) \setminus \mathcal{A}_\mathcal{H} \xrightarrow{\tau} (P_1 \parallel_{\{h\}} \underline{0}) \setminus \mathcal{A}_\mathcal{H} \xrightarrow{\tau} (\underline{0} \parallel_{\{h\}} \underline{0}) \setminus \mathcal{A}_\mathcal{H}$ but neither $(\underline{0} \parallel_{\{h\}} P_2) \setminus \mathcal{A}_\mathcal{H}$ nor $(P_1 \parallel_{\{h\}} \underline{0}) \setminus \mathcal{A}_\mathcal{H}$ is $\approx_\mathrm{b}$-equivalent to $(P_1 \parallel_{\{h\}} P_2) \setminus \mathcal{A}_\mathcal{H}$ when $l_1 \neq l_2$. Note that $(P_1 \parallel_{\{h\}} P_2) / \mathcal{A}_\mathcal{H} \approx_\mathrm{w} (P_1 \parallel_{\{h\}} P_2) \setminus \mathcal{A}_\mathcal{H}$ because $(P_1 \parallel_{\{h\}} P_2) / \mathcal{A}_\mathcal{H} \xrightarrow{\tau} (\underline{0} \parallel_{\{h\}} \underline{0}) / \mathcal{A}_\mathcal{H}$ is matched by $(P_1 \parallel_{\{h\}} P_2) \setminus \mathcal{A}_\mathcal{H} \xRightarrow{\tau^*} (\underline{0} \parallel_{\{h\}} \underline{0}) \setminus \mathcal{A}_\mathcal{H}$. However, it is not only a matter of the higher discriminating power of $\approx_\mathrm{b}$ with respect to $\approx_\mathrm{w}$. If we used the CCS parallel composition

operator [112], which turns the synchronization of two actions into τ thus combining communication with hiding, then the parallel composition of P_1 and P_2 with restriction on $\mathcal{A}_\mathcal{H}$ would be able to respond, in the branching bisimulation game, with a single τ-transition reaching the parallel composition of $\underline{0}$ and $\underline{0}$ with restriction on $\mathcal{A}_\mathcal{H}$.

8.3.2 Taxonomy of Security Properties

The relationships among the various $\approx_{\rm b}$-based noninterference properties turn out to follow the same pattern as those relying on $\approx_{\rm w}$ shown in Theorem 8.1.

Part of the proof of the forthcoming Theorem 8.4 exploits the notion of branching bisimulation up to $\approx_{\rm b}$ of [75] that we recall below, where $\approx_{\rm b}\mathcal{B}\approx_{\rm b}$ stands for the composition of the three mentioned relations. Note that $\mathcal{B}$ is no longer required to be a symmetric relation thus avoiding redundant information in it.

Definition 8.7. *A relation $\mathcal{B}$ over $\mathbb{P}_{\rm nd}$ is a* branching bisimulation up to $\approx_{\rm b}$ *iff, whenever $(P_1, P_2) \in \mathcal{B}$, then:*

- *For each $P_1 \stackrel{\tau^*}{\Longrightarrow} \bar{P}_1 \stackrel{a}{\longrightarrow} P_1'$ with $P_1 \approx_{\rm b} \bar{P}_1$:*
  - *either $a = \tau$ and $\bar{P}_1 \approx_{\rm b} P_1'$;*
  - *or there exists $P_2 \stackrel{\tau^*}{\Longrightarrow} \bar{P}_2 \stackrel{a}{\longrightarrow} P_2'$ such that $\bar{P}_1 \approx_{\rm b}\mathcal{B}\approx_{\rm b} \bar{P}_2$ and $P_1' \approx_{\rm b}\mathcal{B}\approx_{\rm b} P_2'$;*

  and vice versa. ■

In the case that $a = \tau$ and $\bar{P}_1 \approx_{\rm b} P_1'$, it holds that $P_1' \approx_{\rm b} \bar{P}_1 \approx_{\rm b} P_1\ \mathcal{B}\ P_2 \approx_{\rm b} P_2$, i.e., $P_1' \approx_{\rm b}\mathcal{B}\approx_{\rm b} P_2$, because $\approx_{\rm b}$ is reflexive, symmetric, and transitive.

Proposition 8.1. *Let $P_1, P_2 \in \mathbb{P}_{\rm nd}$ and $\mathcal{B}$ be a branching bisimulation up to $\approx_{\rm b}$. If $(P_1, P_2) \in \mathcal{B}$ then $P_1 \approx_{\rm b} P_2$.* ■

Before presenting the taxonomy of the noninterference properties based on $\approx_{\rm b}$, we prove some further ancillary results about parallel composition, restriction, and hiding under $\mathrm{SBSNNI}_{\approx_{\rm b}}$ and $\mathrm{SBNDC}_{\approx_{\rm b}}$.

Lemma 8.3. *Let $P, P_1, P_2 \in \mathbb{P}_{\rm nd}$. Then:*

1. *If $P \in \mathrm{SBNDC}_{\approx_{\rm b}}$, $P' \in reach(P)$, and $P' / \mathcal{A}_\mathcal{H} \stackrel{\tau^*}{\Longrightarrow} P'' / \mathcal{A}_\mathcal{H}$, then $P' \setminus \mathcal{A}_\mathcal{H} \stackrel{\tau^*}{\Longrightarrow} \hat{P}'' \setminus \mathcal{A}_\mathcal{H}$ with $P'' \setminus \mathcal{A}_\mathcal{H} \approx_{\rm b} \hat{P}'' \setminus \mathcal{A}_\mathcal{H}$.*
2. *If $P_1, P_2 \in \mathrm{SBNDC}_{\approx_{\rm b}}$ and $P_1 \setminus \mathcal{A}_\mathcal{H} \approx_{\rm b} P_2 \setminus \mathcal{A}_\mathcal{H}$, then $P_1 / \mathcal{A}_\mathcal{H} \approx_{\rm b} P_2 / \mathcal{A}_\mathcal{H}$.*
3. *If $P_2 \in \mathrm{SBSNNI}_{\approx_{\rm b}}$ and $L \subseteq \mathcal{A}_\mathcal{H}$, then $P_1' \setminus \mathcal{A}_\mathcal{H} \approx_{\rm b} ((P_2' \parallel_L Q) / L) \setminus \mathcal{A}_\mathcal{H}$ for all $Q \in \mathbb{P}$ having only actions in $\mathcal{A}_\mathcal{H}$ and for all $P_1' \in reach(P_1)$ and $P_2' \in reach(P_2)$ such that $P_1' \setminus \mathcal{A}_\mathcal{H} \approx_{\rm b} P_2' / \mathcal{A}_\mathcal{H}$.*

Proof. Let us prove the three results:

1. We proceed by induction on the number $n \in \mathbb{N}$ of τ-transitions along $P' / \mathcal{A}_\mathcal{H} \stackrel{\tau^*}{\Longrightarrow} P'' / \mathcal{A}_\mathcal{H}$:
   - If $n = 0$ then $P' / \mathcal{A}_\mathcal{H}$ stays idle and $P'' / \mathcal{A}_\mathcal{H}$ is $P' / \mathcal{A}_\mathcal{H}$. Likewise, $P' \setminus \mathcal{A}_\mathcal{H}$ can stay idle, i.e., $P' \setminus \mathcal{A}_\mathcal{H} \stackrel{\tau^*}{\Longrightarrow} P' \setminus \mathcal{A}_\mathcal{H}$, with $P' \setminus \mathcal{A}_\mathcal{H} \approx_{\rm b} P' \setminus \mathcal{A}_\mathcal{H}$ as $\approx_{\rm b}$ is reflexive.

- Let $n > 0$ and $P'_0 / \mathcal{A}_\mathcal{H} \xrightarrow{\tau} P'_1 / \mathcal{A}_\mathcal{H} \xrightarrow{\tau} \ldots \xrightarrow{\tau} P'_{n-1} / \mathcal{A}_\mathcal{H} \xrightarrow{\tau} P'_n / \mathcal{A}_\mathcal{H}$ where P'_0 is P' and P'_n is P''. From the induction hypothesis it follows that $P' \setminus \mathcal{A}_\mathcal{H} \stackrel{\tau^*}{\Longrightarrow} \hat{P}'_{n-1} \setminus \mathcal{A}_\mathcal{H}$ with $P'_{n-1} \setminus \mathcal{A}_\mathcal{H} \approx_\mathrm{b} \hat{P}'_{n-1} \setminus \mathcal{A}_\mathcal{H}$. As far as the n-th τ-transition $P'_{n-1} / \mathcal{A}_\mathcal{H} \xrightarrow{\tau} P'_n / \mathcal{A}_\mathcal{H}$ is concerned, there are two cases depending on whether it is originated from $P'_{n-1} \xrightarrow{\tau} P'_n$ or $P'_{n-1} \xrightarrow{h} P'_n$:
  - If $P'_{n-1} \xrightarrow{\tau} P'_n$ then $P'_{n-1} \setminus \mathcal{A}_\mathcal{H} \xrightarrow{\tau} P'_n \setminus \mathcal{A}_\mathcal{H}$. Since $P'_{n-1} \setminus \mathcal{A}_\mathcal{H} \approx_\mathrm{b} \hat{P}'_{n-1} \setminus \mathcal{A}_\mathcal{H}$:
    - either $P'_n \setminus \mathcal{A}_\mathcal{H} \approx_\mathrm{b} \hat{P}'_{n-1} \setminus \mathcal{A}_\mathcal{H}$, in which case $\hat{P}'_{n-1} \setminus \mathcal{A}_\mathcal{H}$ stays idle and hence $P' \setminus \mathcal{A}_\mathcal{H} \stackrel{\tau^*}{\Longrightarrow} \hat{P}'_{n-1} \setminus \mathcal{A}_\mathcal{H}$ with $P'' \setminus \mathcal{A}_\mathcal{H} \approx_\mathrm{b} \hat{P}'_{n-1} \setminus \mathcal{A}_\mathcal{H}$;
    - or there exists $\hat{P}'_{n-1} \setminus \mathcal{A}_\mathcal{H} \stackrel{\tau^*}{\Longrightarrow} \bar{P}_{n-1} \setminus \mathcal{A}_\mathcal{H} \xrightarrow{\tau} \hat{P}'_n \setminus \mathcal{A}_\mathcal{H}$ such that $P'_{n-1} \setminus \mathcal{A}_\mathcal{H} \approx_\mathrm{b} \bar{P}_{n-1} \setminus \mathcal{A}_\mathcal{H}$ and $P'_n \setminus \mathcal{A}_\mathcal{H} \approx_\mathrm{b} \hat{P}'_n \setminus \mathcal{A}_\mathcal{H}$, hence $P' \setminus \mathcal{A}_\mathcal{H} \stackrel{\tau^*}{\Longrightarrow} \hat{P}'_n \setminus \mathcal{A}_\mathcal{H}$ with $P'' \setminus \mathcal{A}_\mathcal{H} \approx_\mathrm{b} \hat{P}'_n \setminus \mathcal{A}_\mathcal{H}$.
  - If $P'_{n-1} \xrightarrow{h} P'_n$ then from $P \in \mathrm{SBNDC}_{\approx_\mathrm{b}}$ it follows that $P'_{n-1} \setminus \mathcal{A}_\mathcal{H} \approx_\mathrm{b} P'_n \setminus \mathcal{A}_\mathcal{H}$. Since $P'_{n-1} \setminus \mathcal{A}_\mathcal{H} \approx_\mathrm{b} \hat{P}'_{n-1} \setminus \mathcal{A}_\mathcal{H}$ and $\approx_\mathrm{b}$ is symmetric and transitive, we obtain $P'_n \setminus \mathcal{A}_\mathcal{H} \approx_\mathrm{b} \hat{P}'_{n-1} \setminus \mathcal{A}_\mathcal{H}$ with $P' \setminus \mathcal{A}_\mathcal{H} \stackrel{\tau^*}{\Longrightarrow} \hat{P}'_{n-1} \setminus \mathcal{A}_\mathcal{H}$.

2. Let $\mathcal{B}$ be a symmetric relation containing all the pairs of processes that have to be shown to be $\approx_\mathrm{b}$-equivalent according to the considered result. Starting from $(P_1 / \mathcal{A}_\mathcal{H}, P_2 / \mathcal{A}_\mathcal{H}) \in \mathcal{B}$, so that $P_1 \setminus \mathcal{A}_\mathcal{H} \approx_\mathrm{b} P_2 \setminus \mathcal{A}_\mathcal{H}$, there are three cases based on the operational semantic rules in Table 8.1:

   - If $P_1 / \mathcal{A}_\mathcal{H} \xrightarrow{\tau} P'_1 / \mathcal{A}_\mathcal{H}$ with $P_1 \xrightarrow{h} P'_1$, then $P_1 \setminus \mathcal{A}_\mathcal{H} \approx_\mathrm{b} P'_1 \setminus \mathcal{A}_\mathcal{H}$ as $h \in \mathcal{A}_\mathcal{H}$ and $P_1 \in \mathrm{SBNDC}_{\approx_\mathrm{b}}$. Since $P'_1 \setminus \mathcal{A}_\mathcal{H} \approx_\mathrm{b} P_2 \setminus \mathcal{A}_\mathcal{H}$, as $P_1 \setminus \mathcal{A}_\mathcal{H} \approx_\mathrm{b} P_2 \setminus \mathcal{A}_\mathcal{H}$ and $\approx_\mathrm{b}$ is symmetric and transitive, with $P'_1, P_2 \in \mathrm{SBNDC}_{\approx_\mathrm{b}}$, we have that $P_2 / \mathcal{A}_\mathcal{H}$ is allowed to stay idle with $(P'_1 / \mathcal{A}_\mathcal{H}, P_2 / \mathcal{A}_\mathcal{H}) \in \mathcal{B}$.
   - If $P_1 / \mathcal{A}_\mathcal{H} \xrightarrow{l} P'_1 / \mathcal{A}_\mathcal{H}$ with $P_1 \xrightarrow{l} P'_1$, then $P_1 \setminus \mathcal{A}_\mathcal{H} \xrightarrow{l} P'_1 \setminus \mathcal{A}_\mathcal{H}$ as $l \notin \mathcal{A}_\mathcal{H}$. From $P_1 \setminus \mathcal{A}_\mathcal{H} \approx_\mathrm{b} P_2 \setminus \mathcal{A}_\mathcal{H}$ it follows that there exists $P_2 \setminus \mathcal{A}_\mathcal{H} \stackrel{\tau^*}{\Longrightarrow} \bar{P}_2 \setminus \mathcal{A}_\mathcal{H} \xrightarrow{l} P'_2 \setminus \mathcal{A}_\mathcal{H}$ such that $P_1 \setminus \mathcal{A}_\mathcal{H} \approx_\mathrm{b} \bar{P}_2 \setminus \mathcal{A}_\mathcal{H}$ and $P'_1 \setminus \mathcal{A}_\mathcal{H} \approx_\mathrm{b} P'_2 \setminus \mathcal{A}_\mathcal{H}$. Thus $P_2 / \mathcal{A}_\mathcal{H} \stackrel{\tau^*}{\Longrightarrow} \bar{P}_2 / \mathcal{A}_\mathcal{H} \xrightarrow{l} P'_2 / \mathcal{A}_\mathcal{H}$ as $l, \tau \notin \mathcal{A}_\mathcal{H}$. Since $P_1 \setminus \mathcal{A}_\mathcal{H} \approx_\mathrm{b} \bar{P}_2 \setminus \mathcal{A}_\mathcal{H}$ with $P_1, \bar{P}_2 \in \mathrm{SBNDC}_{\approx_\mathrm{b}}$ and $P'_1 \setminus \mathcal{A}_\mathcal{H} \approx_\mathrm{b} P'_2 \setminus \mathcal{A}_\mathcal{H}$ with $P'_1, P'_2 \in \mathrm{SBNDC}_{\approx_\mathrm{b}}$, we have that $(P_1 / \mathcal{A}_\mathcal{H}, \bar{P}_2 / \mathcal{A}_\mathcal{H}) \in \mathcal{B}$ and $(P'_1 / \mathcal{A}_\mathcal{H}, P'_2 / \mathcal{A}_\mathcal{H}) \in \mathcal{B}$.
   - If $P_1 / \mathcal{A}_\mathcal{H} \xrightarrow{\tau} P'_1 / \mathcal{A}_\mathcal{H}$ with $P_1 \xrightarrow{\tau} P'_1$, then $P_1 \setminus \mathcal{A}_\mathcal{H} \xrightarrow{\tau} P'_1 \setminus \mathcal{A}_\mathcal{H}$ as $\tau \notin \mathcal{A}_\mathcal{H}$. There are two subcases:
     - If $P'_1 \setminus \mathcal{A}_\mathcal{H} \approx_\mathrm{b} P_2 \setminus \mathcal{A}_\mathcal{H}$ then $P_2 \setminus \mathcal{A}_\mathcal{H}$ is allowed to stay idle with $(P'_1 / \mathcal{A}_\mathcal{H}, P_2 / \mathcal{A}_\mathcal{H}) \in \mathcal{B}$ because $P'_1 \setminus \mathcal{A}_\mathcal{H} \approx_\mathrm{b} P_2 \setminus \mathcal{A}_\mathcal{H}$ and $P'_1, P_2 \in \mathrm{SBNDC}_{\approx_\mathrm{b}}$.
     - If $P'_1 \setminus \mathcal{A}_\mathcal{H} \not\approx_\mathrm{b} P_2 \setminus \mathcal{A}_\mathcal{H}$ then the proof is like the one of the previous case with $\xrightarrow{\tau}$ used in place of $\xrightarrow{l}$.

3. Let $\mathcal{B}$ be a symmetric relation containing all the pairs of processes that have to be shown to be $\approx_\mathrm{b}$-equivalent according to the considered result. Starting from $P'_1 \setminus \mathcal{A}_\mathcal{H}$ and $((P'_2 \parallel_L Q) / L) \setminus \mathcal{A}_\mathcal{H}$ related by $\mathcal{B}$, so that $P'_1 \setminus \mathcal{A}_\mathcal{H} \approx_\mathrm{b} P'_2 / \mathcal{A}_\mathcal{H}$, there are six cases based on the operational semantic rules in Table 8.1. In the first two cases, it is $P'_1 \setminus \mathcal{A}_\mathcal{H}$ to move first:

   - Let $P'_1 \setminus \mathcal{A}_\mathcal{H} \xrightarrow{l} P''_1 \setminus \mathcal{A}_\mathcal{H}$. We observe that from $P'_2 \in \mathit{reach}(P_2)$ and $P_2 \in \mathrm{SBSNNI}_{\approx_\mathrm{b}}$ it follows that $P'_2 \setminus \mathcal{A}_\mathcal{H} \approx_\mathrm{b} P'_2 / \mathcal{A}_\mathcal{H}$, so that $P'_1 \setminus \mathcal{A}_\mathcal{H} \approx_\mathrm{b} P'_2 / \mathcal{A}_\mathcal{H} \approx_\mathrm{b} P'_2 \setminus \mathcal{A}_\mathcal{H}$, i.e., $P'_1 \setminus \mathcal{A}_\mathcal{H} \approx_\mathrm{b} P'_2 \setminus \mathcal{A}_\mathcal{H}$, as $\approx_\mathrm{b}$ is symmetric

and transitive. As a consequence, since $l \neq \tau$ there exists $P_2' \setminus \mathcal{A}_\mathcal{H} \stackrel{\tau^*}{\Longrightarrow} \bar{P}_2' \setminus \mathcal{A}_\mathcal{H} \stackrel{l}{\longrightarrow} P_2'' \setminus \mathcal{A}_\mathcal{H}$ such that $P_1' \setminus \mathcal{A}_\mathcal{H} \approx_\mathrm{b} \bar{P}_2' \setminus \mathcal{A}_\mathcal{H}$ and $P_1'' \setminus \mathcal{A}_\mathcal{H} \approx_\mathrm{b} P_2'' \setminus \mathcal{A}_\mathcal{H}$. Thus $((P_2' \parallel_L Q) / L) \setminus \mathcal{A}_\mathcal{H} \stackrel{\tau^*}{\Longrightarrow} ((\bar{P}_2' \parallel_L Q) / L) \setminus \mathcal{A}_\mathcal{H} \stackrel{l}{\longrightarrow} ((P_2'' \parallel_L Q) / L) \setminus \mathcal{A}_\mathcal{H}$ with $(P_1' \setminus \mathcal{A}_\mathcal{H}, ((\bar{P}_2' \parallel_L Q) / L) \setminus \mathcal{A}_\mathcal{H}) \in \mathcal{B}$ – because $P_1' \in \mathit{reach}(P_1)$, $\bar{P}_2' \in \mathit{reach}(P_2)$, and $P_1' \setminus \mathcal{A}_\mathcal{H} \approx_\mathrm{b} \bar{P}_2' / \mathcal{A}_\mathcal{H}$ as $P_2 \in \mathrm{SBSNNI}_{\approx_\mathrm{b}}$ – and $(P_1'' \setminus \mathcal{A}_\mathcal{H}, ((P_2'' \parallel_L Q) / L) \setminus \mathcal{A}_\mathcal{H}) \in \mathcal{B}$ – because $P_1'' \in \mathit{reach}(P_1)$, $P_2'' \in \mathit{reach}(P_2)$, and $P_1'' \setminus \mathcal{A}_\mathcal{H} \approx_\mathrm{b} P_2'' / \mathcal{A}_\mathcal{H}$ as $P_2 \in \mathrm{SBSNNI}_{\approx_\mathrm{b}}$.

- If $P_1' \setminus \mathcal{A}_\mathcal{H} \stackrel{\tau}{\longrightarrow} P_1'' \setminus \mathcal{A}_\mathcal{H}$ there are two subcases:
  - If $P_1'' \setminus \mathcal{A}_\mathcal{H} \approx_\mathrm{b} P_2' / \mathcal{A}_\mathcal{H}$ then $(P_2' \parallel_L Q) / L) \setminus \mathcal{A}_\mathcal{H}$ is allowed to stay idle with $(P_1'' \setminus \mathcal{A}_\mathcal{H}, ((P_2' \parallel_L Q) / L) \setminus \mathcal{A}_\mathcal{H}) \in \mathcal{B}$ because $P_1'' \in \mathit{reach}(P_1)$ and $P_2' \in \mathit{reach}(P_2)$.
  - If $P_1'' \setminus \mathcal{A}_\mathcal{H} \not\approx_\mathrm{b} P_2' / \mathcal{A}_\mathcal{H}$ then the proof is like the one of the previous case with $\stackrel{\tau}{\longrightarrow}$ used in place of $\stackrel{l}{\longrightarrow}$.

In the other four cases, instead, it is $((P_2' \parallel_L Q) / L) \setminus \mathcal{A}_\mathcal{H}$ to move first:

- Let $((P_2' \parallel_L Q) / L) \setminus \mathcal{A}_\mathcal{H} \stackrel{l}{\longrightarrow} ((P_2'' \parallel_L Q) / L) \setminus \mathcal{A}_\mathcal{H}$ with $P_2' \stackrel{l}{\longrightarrow} P_2''$ so that $P_2' \setminus \mathcal{A}_\mathcal{H} \stackrel{l}{\longrightarrow} P_2'' \setminus \mathcal{A}_\mathcal{H}$ as $l \notin \mathcal{A}_\mathcal{H}$. We observe that from $P_2' \in \mathit{reach}(P_2)$ and $P_2 \in \mathrm{SBSNNI}_{\approx_\mathrm{b}}$ it follows that $P_2' \setminus \mathcal{A}_\mathcal{H} \approx_\mathrm{b} P_2' / \mathcal{A}_\mathcal{H}$, so that $P_2' \setminus \mathcal{A}_\mathcal{H} \approx_\mathrm{b} P_2' / \mathcal{A}_\mathcal{H} \approx_\mathrm{b} P_1' \setminus \mathcal{A}_\mathcal{H}$, i.e., $P_2' \setminus \mathcal{A}_\mathcal{H} \approx_\mathrm{b} P_1' \setminus \mathcal{A}_\mathcal{H}$, as $\approx_\mathrm{b}$ is symmetric and transitive. As a consequence, since $l \neq \tau$ there exists $P_1' \setminus \mathcal{A}_\mathcal{H} \stackrel{\tau^*}{\Longrightarrow} \bar{P}_1' \setminus \mathcal{A}_\mathcal{H} \stackrel{l}{\longrightarrow} P_1'' \setminus \mathcal{A}_\mathcal{H}$ such that $P_2' \setminus \mathcal{A}_\mathcal{H} \approx_\mathrm{b} \bar{P}_1' \setminus \mathcal{A}_\mathcal{H}$ and $P_2'' \setminus \mathcal{A}_\mathcal{H} \approx_\mathrm{b} P_1'' \setminus \mathcal{A}_\mathcal{H}$. Thus $(((P_2' \parallel_L Q) / L) \setminus \mathcal{A}_\mathcal{H}, \bar{P}_1' \setminus \mathcal{A}_\mathcal{H}) \in \mathcal{B}$ – because $\bar{P}_1' \in \mathit{reach}(P_1)$, $P_2' \in \mathit{reach}(P_2)$, and $\bar{P}_1' \setminus \mathcal{A}_\mathcal{H} \approx_\mathrm{b} P_2' / \mathcal{A}_\mathcal{H}$ as $P_2 \in \mathrm{SBSNNI}_{\approx_\mathrm{b}}$ – and $(((P_2'' \parallel_L Q) / L) \setminus \mathcal{A}_\mathcal{H}, P_1'' \setminus \mathcal{A}_\mathcal{H}) \in \mathcal{B}$ – because $P_1'' \in \mathit{reach}(P_1)$, $P_2'' \in \mathit{reach}(P_2)$, and $P_1'' \setminus \mathcal{A}_\mathcal{H} \approx_\mathrm{b} P_2'' / \mathcal{A}_\mathcal{H}$ as $P_2 \in \mathrm{SBSNNI}_{\approx_\mathrm{b}}$.
- If $((P_2' \parallel_L Q) / L) \setminus \mathcal{A}_\mathcal{H} \stackrel{\tau}{\longrightarrow} ((P_2'' \parallel_L Q) / L) \setminus \mathcal{A}_\mathcal{H}$ with $P_2' \stackrel{\tau}{\longrightarrow} P_2''$ so that $P_2' \setminus \mathcal{A}_\mathcal{H} \stackrel{\tau}{\longrightarrow} P_2'' \setminus \mathcal{A}_\mathcal{H}$ as $\tau \notin \mathcal{A}_\mathcal{H}$, there are two subcases:
  - If $P_2'' \setminus \mathcal{A}_\mathcal{H} \approx_\mathrm{b} P_1' \setminus \mathcal{A}_\mathcal{H}$ then $P_1' \setminus \mathcal{A}_\mathcal{H}$ is allowed to stay idle with $(((P_2'' \parallel_L Q) / L) \setminus \mathcal{A}_\mathcal{H}, P_1' \setminus \mathcal{A}_\mathcal{H}) \in \mathcal{B}$ because $P_1' \in \mathit{reach}(P_1)$, $P_2'' \in \mathit{reach}(P_2)$, and $P_1' \setminus \mathcal{A}_\mathcal{H} \approx_\mathrm{b} P_2'' / \mathcal{A}_\mathcal{H}$ as $P_2 \in \mathrm{SBSNNI}_{\approx_\mathrm{b}}$.
  - If $P_2'' \setminus \mathcal{A}_\mathcal{H} \not\approx_\mathrm{b} P_1' \setminus \mathcal{A}_\mathcal{H}$ then the proof is like the one of the previous case with $\stackrel{\tau}{\longrightarrow}$ used in place of $\stackrel{l}{\longrightarrow}$.
- If $((P_2' \parallel_L Q) / L) \setminus \mathcal{A}_\mathcal{H} \stackrel{\tau}{\longrightarrow} ((P_2' \parallel_L Q') / L) \setminus \mathcal{A}_\mathcal{H}$ with $Q \stackrel{\tau}{\longrightarrow} Q'$, then trivially $(((P_2' \parallel_L Q') / L) \setminus \mathcal{A}_\mathcal{H}, P_1' \setminus \mathcal{A}_\mathcal{H}) \in \mathcal{B}$.
- Let $((P_2' \parallel_L Q) / L) \setminus \mathcal{A}_\mathcal{H} \stackrel{\tau}{\longrightarrow} ((P_2'' \parallel_L Q' / L) \setminus \mathcal{A}_\mathcal{H})$ with $P_2' \stackrel{h}{\longrightarrow} P_2''$ – so that $P_2' / \mathcal{A}_\mathcal{H} \stackrel{\tau}{\longrightarrow} P_2'' / \mathcal{A}_\mathcal{H}$ as $h \in \mathcal{A}_\mathcal{H}$ – and $Q \stackrel{h}{\longrightarrow} Q'$ for $h \in L$. We observe that from $P_2', P_2'' \in \mathit{reach}(P_2)$ and $P_2 \in \mathrm{SBSNNI}_{\approx_\mathrm{b}}$ it follows that $P_2' \setminus \mathcal{A}_\mathcal{H} \approx_\mathrm{b} P_2' / \mathcal{A}_\mathcal{H}$ and $P_2'' \setminus \mathcal{A}_\mathcal{H} \approx_\mathrm{b} P_2'' / \mathcal{A}_\mathcal{H}$, so that $P_2' \setminus \mathcal{A}_\mathcal{H} \stackrel{\tau}{\longrightarrow} P_2'' \setminus \mathcal{A}_\mathcal{H}$ and $P_2' \setminus \mathcal{A}_\mathcal{H} \approx_\mathrm{b} P_2' / \mathcal{A}_\mathcal{H} \approx_\mathrm{b} P_1' \setminus \mathcal{A}_\mathcal{H}$, i.e., $P_2' \setminus \mathcal{A}_\mathcal{H} \approx_\mathrm{b} P_1' \setminus \mathcal{A}_\mathcal{H}$, as $\approx_\mathrm{b}$ is symmetric and transitive. There are two subcases:
  - If $P_2'' \setminus \mathcal{A}_\mathcal{H} \approx_\mathrm{b} P_1' \setminus \mathcal{A}_\mathcal{H}$ then $P_1' \setminus \mathcal{A}_\mathcal{H}$ is allowed to stay idle with $(((P_2'' \parallel_L Q') / L) \setminus \mathcal{A}_\mathcal{H}, P_1' \setminus \mathcal{A}_\mathcal{H}) \in \mathcal{B}$ because $P_1' \in \mathit{reach}(P_1)$, $P_2'' \in \mathit{reach}(P_2)$, and $P_1' \setminus \mathcal{A}_\mathcal{H} \approx_\mathrm{b} P_2'' / \mathcal{A}_\mathcal{H}$ as $P_2 \in \mathrm{SBSNNI}_{\approx_\mathrm{b}}$.
  - If $P_2'' \setminus \mathcal{A}_\mathcal{H} \not\approx_\mathrm{b} P_1' \setminus \mathcal{A}_\mathcal{H}$ then there exists $P_1' \setminus \mathcal{A}_\mathcal{H} \stackrel{\tau^*}{\Longrightarrow} \bar{P}_1' \setminus \mathcal{A}_\mathcal{H} \stackrel{\tau}{\longrightarrow} P_1'' \setminus \mathcal{A}_\mathcal{H}$ such that $P_2' \setminus \mathcal{A}_\mathcal{H} \approx_\mathrm{b} \bar{P}_1' \setminus \mathcal{A}_\mathcal{H}$ and $P_2'' \setminus \mathcal{A}_\mathcal{H} \approx_\mathrm{b} P_1'' \setminus \mathcal{A}_\mathcal{H}$. Thus $(((P_2' \parallel_L Q) / L) \setminus \mathcal{A}_\mathcal{H}, \bar{P}_1' \setminus \mathcal{A}_\mathcal{H}) \in \mathcal{B}$ – because $\bar{P}_1' \in \mathit{reach}(P_1)$, $P_2' \in \mathit{reach}(P_2)$, and $\bar{P}_1' \setminus \mathcal{A}_\mathcal{H} \approx_\mathrm{b} P_2' / \mathcal{A}_\mathcal{H}$ as $P_2 \in \mathrm{SBSNNI}_{\approx_\mathrm{b}}$ – and $(((P_2'' \parallel_L Q') / L) \setminus \mathcal{A}_\mathcal{H}, P_1'' \setminus \mathcal{A}_\mathcal{H}) \in \mathcal{B}$ – because $P_1'' \in \mathit{reach}(P_1)$, $P_2'' \in \mathit{reach}(P_2)$, and $P_1'' \setminus \mathcal{A}_\mathcal{H} \approx_\mathrm{b} P_2'' / \mathcal{A}_\mathcal{H}$ as $P_2 \in \mathrm{SBSNNI}_{\approx_\mathrm{b}}$. ■

Theorem 8.4. $\text{SBNDC}_{\approx_b} \subsetneq \text{SBSNNI}_{\approx_b} = \text{P\_BNDC}_{\approx_b} \subsetneq \text{BNDC}_{\approx_b} \subsetneq \text{BSNNI}_{\approx_b}$.

Proof. Let us examine each relationship separately:

- $\text{SBNDC}_{\approx_b} \subsetneq \text{SBSNNI}_{\approx_b}$. Given $P \in \text{SBNDC}_{\approx_b}$, the result follows by proving that the relation $\mathcal{B} = \{(P' \setminus \mathcal{A}_\mathcal{H}, P' / \mathcal{A}_\mathcal{H}) \mid P' \in \mathit{reach}(P)\}$ is a branching bisimulation up to $\approx_b$. Starting from $(P' \setminus \mathcal{A}_\mathcal{H}, P' / \mathcal{A}_\mathcal{H}) \in \mathcal{B}$, there are three cases based on the operational semantic rules in Table 8.1. In the first case, it is $P' \setminus \mathcal{A}_\mathcal{H}$ to move first:

  - If $P' \setminus \mathcal{A}_\mathcal{H} \stackrel{\tau^*}{\Longrightarrow} \bar{P}' \setminus \mathcal{A}_\mathcal{H} \stackrel{a}{\longrightarrow} P'' \setminus \mathcal{A}_\mathcal{H}$ with $a \in \mathcal{A}_\mathcal{L} \cup \{\tau\}$, then $P' / \mathcal{A}_\mathcal{H} \stackrel{\tau^*}{\Longrightarrow} \bar{P}' / \mathcal{A}_\mathcal{H} \stackrel{a}{\longrightarrow} P'' / \mathcal{A}_\mathcal{H}$ as $a, \tau \notin \mathcal{A}_\mathcal{H}$, with $(\bar{P}' \setminus \mathcal{A}_\mathcal{H}, \bar{P}' / \mathcal{A}_\mathcal{H}) \in \mathcal{B}$ and $(P'' \setminus \mathcal{A}_\mathcal{H}, P'' / \mathcal{A}_\mathcal{H}) \in \mathcal{B}$ as $\bar{P}', P'' \in \mathit{reach}(P)$. Thus $\bar{P}' \setminus \mathcal{A}_\mathcal{H} \approx_b \bar{P}' \setminus \mathcal{A}_\mathcal{H}\ \mathcal{B}\ \bar{P}' / \mathcal{A}_\mathcal{H} \approx_b \bar{P}' / \mathcal{A}_\mathcal{H}$ and $P'' \setminus \mathcal{A}_\mathcal{H} \approx_b P'' \setminus \mathcal{A}_\mathcal{H}\ \mathcal{B}\ P'' / \mathcal{A}_\mathcal{H} \approx_b P'' / \mathcal{A}_\mathcal{H}$.

  In the other two cases, instead, it is $P' / \mathcal{A}_\mathcal{H}$ to move first (note that possible τ-transitions along $\stackrel{\tau^*}{\Longrightarrow}$ arising from high actions in P' can no longer be executed when responding from $P' \setminus \mathcal{A}_\mathcal{H}$, but for them we exploit $P \in \text{SBNDC}_{\approx_b}$ and Lemma 8.3(1)):

  - Let $P' / \mathcal{A}_\mathcal{H} \stackrel{\tau^*}{\Longrightarrow} \bar{P}' / \mathcal{A}_\mathcal{H} \stackrel{a}{\longrightarrow} P'' / \mathcal{A}_\mathcal{H}$ with $a \in \mathcal{A}_\mathcal{L} \cup \{\tau\}$. From $P' / \mathcal{A}_\mathcal{H} \stackrel{\tau^*}{\Longrightarrow} \bar{P}' / \mathcal{A}_\mathcal{H}$ and Lemma 8.3(1) it follows that $P' \setminus \mathcal{A}_\mathcal{H} \stackrel{\tau^*}{\Longrightarrow} \hat{P}' \setminus \mathcal{A}_\mathcal{H}$ with $\bar{P}' \setminus \mathcal{A}_\mathcal{H} \approx_b \hat{P}' \setminus \mathcal{A}_\mathcal{H}$. From $\bar{P}' / \mathcal{A}_\mathcal{H} \stackrel{a}{\longrightarrow} P'' / \mathcal{A}_\mathcal{H}$ it follows that $\bar{P}' \setminus \mathcal{A}_\mathcal{H} \stackrel{a}{\longrightarrow} P'' \setminus \mathcal{A}_\mathcal{H}$ as $a \notin \mathcal{A}_\mathcal{H}$. Since $\bar{P}' \setminus \mathcal{A}_\mathcal{H} \approx_b \hat{P}' \setminus \mathcal{A}_\mathcal{H}$ there are two cases:
    - If $a = \tau$ and $P'' \setminus \mathcal{A}_\mathcal{H} \approx_b \hat{P}' \setminus \mathcal{A}_\mathcal{H}$, then $\bar{P}' \setminus \mathcal{A}_\mathcal{H} \approx_b P'' \setminus \mathcal{A}_\mathcal{H}$ as $\approx_b$ is symmetric and transitive. From $\bar{P}', P'' \in \text{SBNDC}_{\approx_b}$ and Lemma 8.3(2) it follows that $\bar{P}' / \mathcal{A}_\mathcal{H} \approx_b P'' / \mathcal{A}_\mathcal{H}$. Thus $P' \setminus \mathcal{A}_\mathcal{H}$ is allowed to stay idle.
    - Otherwise there exists $\hat{P}' \setminus \mathcal{A}_\mathcal{H} \stackrel{\tau^*}{\Longrightarrow} \hat{P}'' \setminus \mathcal{A}_\mathcal{H} \stackrel{a}{\longrightarrow} \hat{P}''' \setminus \mathcal{A}_\mathcal{H}$ such that $\bar{P}' \setminus \mathcal{A}_\mathcal{H} \approx_b \hat{P}'' \setminus \mathcal{A}_\mathcal{H}$ and $P'' \setminus \mathcal{A}_\mathcal{H} \approx_b \hat{P}''' \setminus \mathcal{A}_\mathcal{H}$. From $P' \setminus \mathcal{A}_\mathcal{H} \stackrel{\tau^*}{\Longrightarrow} \hat{P}' \setminus \mathcal{A}_\mathcal{H}$ it follows that $P' \setminus \mathcal{A}_\mathcal{H} \stackrel{\tau^*}{\Longrightarrow} \hat{P}'' \setminus \mathcal{A}_\mathcal{H} \stackrel{a}{\longrightarrow} \hat{P}''' \setminus \mathcal{A}_\mathcal{H}$ with $\hat{P}'' \setminus \mathcal{A}_\mathcal{H} \approx_b \bar{P}' \setminus \mathcal{A}_\mathcal{H}\ \mathcal{B}\ \bar{P}' / \mathcal{A}_\mathcal{H} \approx_b \bar{P}' / \mathcal{A}_\mathcal{H}$ and $\hat{P}''' \setminus \mathcal{A}_\mathcal{H} \approx_b P'' \setminus \mathcal{A}_\mathcal{H}\ \mathcal{B}\ P'' / \mathcal{A}_\mathcal{H} \approx_b P'' / \mathcal{A}_\mathcal{H}$.
  - Let $P' / \mathcal{A}_\mathcal{H} \stackrel{\tau^*}{\Longrightarrow} \bar{P}' / \mathcal{A}_\mathcal{H} \stackrel{\tau}{\longrightarrow} P'' / \mathcal{A}_\mathcal{H}$ with $\bar{P}' \stackrel{h}{\longrightarrow} P''$. From $\bar{P}' \in \mathit{reach}(P)$ and $P \in \text{SBNDC}_{\approx_b}$ it follows that $\bar{P}' \setminus \mathcal{A}_\mathcal{H} \approx_b P'' \setminus \mathcal{A}_\mathcal{H}$, hence $\bar{P}' / \mathcal{A}_\mathcal{H} \approx_b P'' / \mathcal{A}_\mathcal{H}$ by virtue of Lemma 8.3(2) as $\bar{P}', P'' \in \text{SBNDC}_{\approx_b}$. Thus $P' \setminus \mathcal{A}_\mathcal{H}$ is allowed to stay idle.

- $\text{SBSNNI}_{\approx_b} = \text{P\_BNDC}_{\approx_b}$. $\text{SBSNNI}_{\approx_b} \subseteq \text{P\_BNDC}_{\approx_b}$ follows from Lemma 8.3(3) by taking P_1' identical to P_2' and both reachable from $P \in \text{SBSNNI}_{\approx_b}$.
  On the other hand, if $P \in \text{P\_BNDC}_{\approx_b}$ then $P' \in \text{BNDC}_{\approx_b}$ for every $P' \in \mathit{reach}(P)$. Since $\text{BNDC}_{\approx_b} \subsetneq \text{BSNNI}_{\approx_b}$ as will be shown in the last case of the proof of this theorem, $P' \in \text{BSNNI}_{\approx_b}$ for every $P' \in \mathit{reach}(P)$, i.e., $P \in \text{SBSNNI}_{\approx_b}$.

- $\text{SBSNNI}_{\approx_b} \subsetneq \text{BNDC}_{\approx_b}$. If $P \in \text{SBSNNI}_{\approx_b} = \text{P\_BNDC}_{\approx_b}$ then it immediately follows that $P \in \text{BNDC}_{\approx_b}$.

- $\text{BNDC}_{\approx_b} \subsetneq \text{BSNNI}_{\approx_b}$. If $P \in \text{BNDC}_{\approx_b}$, i.e., $P \setminus \mathcal{A}_\mathcal{H} \approx_b (P \parallel_L Q) / L) \setminus \mathcal{A}_\mathcal{H}$ for all $Q \in \mathbb{P}_{\text{nd}}$ such that each of its actions belongs to $\mathcal{A}_\mathcal{H}$ and for all $L \subseteq \mathcal{A}_\mathcal{H}$, then we can consider in particular $\hat{Q}$ capable of stepwise mimicking the high-level behavior of P, in the sense that $\hat{Q}$ is able to synchronize with all the high-level actions executed by P and its reachable processes, along with $\hat{L} = \mathcal{A}_\mathcal{H}$. As a consequence $(P \parallel_{\hat{L}} \hat{Q}) / \hat{L}) \setminus \mathcal{A}_\mathcal{H}$ is isomorphic to $P / \mathcal{A}_\mathcal{H}$, hence $P \setminus \mathcal{A}_\mathcal{H} \approx_b P / \mathcal{A}_\mathcal{H}$, i.e., $P \in \text{BSNNI}_{\approx_b}$, as $\approx_b$ is transitive. ∎

All the inclusions in the previous theorem are strict as shown by the following counterexamples:

- The process $\tau\,.\,l\,.\,\underline{0}+l\,.\,l\,.\,\underline{0}+h\,.\,l\,.\,\underline{0}$ is $\mathrm{SBSNNI}_{\approx_\mathrm{b}}$ (resp. $\mathrm{P\_BNDC}_{\approx_\mathrm{b}}$) because $(\tau\,.\,l\,.\,\underline{0}+l\,.\,l\,.\,\underline{0}+h\,.\,l\,.\,\underline{0})\setminus\{h\} \approx_\mathrm{b} (\tau\,.\,l\,.\,\underline{0}+l\,.\,l\,.\,\underline{0}+h\,.\,l\,.\,\underline{0})\,/\,\{h\}$ and action h is enabled only at the beginning so every reachable process is $\mathrm{BSNNI}_{\approx_\mathrm{b}}$ (resp. $\mathrm{BNDC}_{\approx_\mathrm{b}}$). It is not $\mathrm{SBNDC}_{\approx_\mathrm{b}}$ because the low-level view of the process reached after action h, i.e., $(l\,.\,\underline{0})\setminus\{h\}$, is not $\approx_\mathrm{b}$-equivalent to $(\tau\,.\,l\,.\,\underline{0}+l\,.\,l\,.\,\underline{0}+h\,.\,l\,.\,\underline{0})\setminus\{h\}$.
- The process $l\,.\,\underline{0}+l\,.\,l\,.\,\underline{0}+l\,.\,h\,.\,l\,.\,\underline{0}$ is $\mathrm{BNDC}_{\approx_\mathrm{b}}$ because, whether there are synchronizations with high-level actions or not, the overall process can always perform either an l-action or a sequence of two l-actions. It is not $\mathrm{SBSNNI}_{\approx_\mathrm{b}}$ (resp. $\mathrm{P\_BNDC}_{\approx_\mathrm{b}}$) because the reachable process $h\,.\,l\,.\,\underline{0}$ is not $\mathrm{BSNNI}_{\approx_\mathrm{b}}$ (resp. $\mathrm{BNDC}_{\approx_\mathrm{b}}$).
- The process $l\,.\,\underline{0}+h\,.\,h\,.\,l\,.\,\underline{0}$ is $\mathrm{BSNNI}_{\approx_\mathrm{b}}$ as $(l\,.\,\underline{0}+h\,.\,h\,.\,l\,.\,\underline{0})\setminus\{h\} \approx_\mathrm{b} (l\,.\,\underline{0}+h\,.\,h\,.\,l\,.\,\underline{0})\,/\,\{h\}$. It is not $\mathrm{BNDC}_{\approx_\mathrm{b}}$ due to $(((l\,.\,\underline{0}+h\,.\,h\,.\,l\,.\,\underline{0})\parallel_{\{h\}}(h\,.\,\underline{0}))\,/\,\{h\})\setminus\{h\} \not\approx_\mathrm{b} (l\,.\,\underline{0}+h\,.\,h\,.\,l\,.\,\underline{0})\setminus\{h\}$ because the former behaves as $l\,.\,\underline{0}+\tau\,.\,\underline{0}$ while the latter behaves as $l\,.\,\underline{0}$.

We further observe that each of the $\approx_\mathrm{b}$-based noninterference properties implies the corresponding $\approx_\mathrm{w}$-based one, due to the fact that $\approx_\mathrm{b}$ is finer than $\approx_\mathrm{w}$.

Theorem 8.5. *The following inclusions hold:*

1. $\mathrm{BSNNI}_{\approx_\mathrm{b}} \subsetneq \mathrm{BSNNI}_{\approx_\mathrm{w}}$.
2. $\mathrm{BNDC}_{\approx_\mathrm{b}} \subsetneq \mathrm{BNDC}_{\approx_\mathrm{w}}$.
3. $\mathrm{SBSNNI}_{\approx_\mathrm{b}} \subsetneq \mathrm{SBSNNI}_{\approx_\mathrm{w}}$.
4. $\mathrm{P\_BNDC}_{\approx_\mathrm{b}} \subsetneq \mathrm{P\_BNDC}_{\approx_\mathrm{w}}$.
5. $\mathrm{SBNDC}_{\approx_\mathrm{b}} \subsetneq \mathrm{SBNDC}_{\approx_\mathrm{w}}$. ∎

All the inclusions above are strict by virtue of the following result; for an example of P_1 and P_2 below, see Figure 8.1.

Theorem 8.6. *Let $P_1, P_2 \in \mathbb{P}_\mathrm{nd}$ be such that $P_1 \approx_\mathrm{w} P_2$ but $P_1 \not\approx_\mathrm{b} P_2$. If no high-level actions occur in P_1 and P_2, then $Q \in \{P_1 + h\,.\,P_2, P_2 + h\,.\,P_1\}$ is such that:*

1. $Q \in \mathrm{BSNNI}_{\approx_\mathrm{w}}$ *but* $Q \notin \mathrm{BSNNI}_{\approx_\mathrm{b}}$.
2. $Q \in \mathrm{BNDC}_{\approx_\mathrm{w}}$ *but* $Q \notin \mathrm{BNDC}_{\approx_\mathrm{b}}$.
3. $Q \in \mathrm{SBSNNI}_{\approx_\mathrm{w}}$ *but* $Q \notin \mathrm{SBSNNI}_{\approx_\mathrm{b}}$.
4. $Q \in \mathrm{P\_BNDC}_{\approx_\mathrm{w}}$ *but* $Q \notin \mathrm{P\_BNDC}_{\approx_\mathrm{b}}$.
5. $Q \in \mathrm{SBNDC}_{\approx_\mathrm{w}}$ *but* $Q \notin \mathrm{SBNDC}_{\approx_\mathrm{b}}$.

Proof. Let Q be $P_1 + h\,.\,P_2$ (the proof is similar for Q equal to $P_2 + h\,.\,P_1$) and observe that no high-level actions occur in every process reachable from Q except Q itself:

1. Since the only high-level action occurring in Q is h, in the proof of $Q \in \mathrm{BSNNI}_{\approx_\mathrm{w}}$ the only interesting case is the transition $Q \,/\, \mathcal{A}_\mathcal{H} \xrightarrow{\tau} P_2 \,/\, \mathcal{A}_\mathcal{H}$, to which $Q \setminus \mathcal{A}_\mathcal{H}$ responds by staying idle because $P_2 \,/\, \mathcal{A}_\mathcal{H} \approx_\mathrm{w} P_2 \approx_\mathrm{w} P_1 \approx_\mathrm{w} Q \setminus \mathcal{A}_\mathcal{H}$, i.e., $P_2 \,/\, \mathcal{A}_\mathcal{H} \approx_\mathrm{w} Q \setminus \mathcal{A}_\mathcal{H}$ as $\approx_\mathrm{w}$ is symmetric and transitive.
   On the other hand, $Q \notin \mathrm{BSNNI}_{\approx_\mathrm{b}}$ because $P_2 \not\approx_\mathrm{b} P_1$ in the same situation as before.

2. Since $Q \in \mathrm{BSNNI}_{\approx_\mathrm{w}}$ by the previous result and no high-level actions occur in every process reachable from Q other than Q, it holds that $Q \in \mathrm{SBSNNI}_{\approx_\mathrm{w}}$ and hence $Q \in \mathrm{BNDC}_{\approx_\mathrm{w}}$ by virtue of Theorem 8.1.
   On the other hand, from $Q \notin \mathrm{BSNNI}_{\approx_\mathrm{b}}$ by the previous result it follows that $Q \notin \mathrm{BNDC}_{\approx_\mathrm{b}}$ by virtue of Theorem 8.4.

3. We already know from the proof of the previous result that $Q \in \mathrm{SBSNNI}_{\approx_\mathrm{w}}$.
   On the other hand, from $Q \notin \mathrm{BSNNI}_{\approx_\mathrm{b}}$ by the first result it follows that $Q \notin \mathrm{SBSNNI}_{\approx_\mathrm{b}}$ by virtue of Theorem 8.4.

4. An immediate consequence of $\mathrm{P\_BNDC}_{\approx_\mathrm{w}} = \mathrm{SBSNNI}_{\approx_\mathrm{w}}$ (Theorem 8.1) and $\mathrm{P\_BNDC}_{\approx_\mathrm{b}} = \mathrm{SBSNNI}_{\approx_\mathrm{b}}$ (Theorem 8.4).

5. Since the only high-level action occurring in Q is h, in the proof of $Q \in \mathrm{SBNDC}_{\approx_\mathrm{w}}$ the only interesting case is the transition $Q \xrightarrow{h} P_2$, for which it holds that $Q \setminus \mathcal{A}_\mathcal{H} \approx_\mathrm{w} P_1 \approx_\mathrm{w} P_2 \approx_\mathrm{w} P_2 \setminus \mathcal{A}_\mathcal{H}$, i.e., $Q \setminus \mathcal{A}_\mathcal{H} \approx_\mathrm{w} P_2 \setminus \mathcal{A}_\mathcal{H}$ as $\approx_\mathrm{pw}$ is transitive.
   On the other hand, $Q \notin \mathrm{SBNDC}_{\approx_\mathrm{b}}$ because $P_1 \not\approx_\mathrm{b} P_2$ in the same situation as before. ∎

An alternative strategy to explore the differences between $\approx_\mathrm{w}$ and $\approx_\mathrm{b}$ with respect to $\mathrm{BSNNI}_{\approx_\mathrm{w}}/\mathrm{BSNNI}_{\approx_\mathrm{b}}$ and $\mathrm{SBSNNI}_{\approx_\mathrm{w}}/\mathrm{SBSNNI}_{\approx_\mathrm{b}}$ consists of considering the two τ-laws $P + \tau \,.\, P = \tau \,.\, P$ and $a \,.\, (P + \tau \,.\, Q) + a \,.\, Q = a \,.\, (P + \tau \,.\, Q)$ for $\approx_\mathrm{w}$ [112]. The strategy is inspired by the initial remarks in [80], where it is noted that the two aforementioned laws are responsible for the lack of distinguishing power of $\approx_\mathrm{w}$ over τ-branching processes. For each law the strategy is based on constructing a pair of new processes from the ones equated by the law, such that they are weakly bisimilar but not branching bisimilar. Then we build a new process R such that $R \setminus \mathcal{A}_\mathcal{H}$ and $R \,/\, \mathcal{A}_\mathcal{H}$ are isomorphic to the two constructed processes.

Proposition 8.2. *From $P + \tau \,.\, P = \tau \,.\, P$ it is possible to construct a process $R \in \mathbb{P}_\mathrm{nd}$ such that $R \in \mathrm{BSNNI}_{\approx_\mathrm{w}}$ but $P \notin \mathrm{BSNNI}_{\approx_\mathrm{b}}$ and $P \in \mathrm{SBSNNI}_{\approx_\mathrm{w}}$ but $P \notin \mathrm{SBSNNI}_{\approx_\mathrm{b}}$.*

Proof. In the considered τ-law let us instantiate P as $\tau \,.\, l_1 \,.\, \underline{0} + \tau \,.\, l_2 \,.\, \underline{0}$ and then add $+ l_3 \,.\, \underline{0}$ to both sides of the law thus obtaining $(\tau \,.\, l_1 \,.\, \underline{0} + \tau \,.\, l_2 \,.\, \underline{0}) + \tau \,.\, (\tau \,.\, l_1 \,.\, \underline{0} + \tau \,.\, l_2 \,.\, \underline{0}) + l_3 \,.\, \underline{0} = \tau \,.\, (\tau \,.\, l_1 \,.\, \underline{0} + \tau \,.\, l_2 \,.\, \underline{0}) + l_3 \,.\, \underline{0}$, which are related by weak bisimilarity but not by branching bisimilarity. Now let us define process R as $(h \,.\, l_1 \,.\, \underline{0} + h \,.\, l_2 \,.\, \underline{0}) + \tau \,.\, (\tau \,.\, l_1 \,.\, \underline{0} + \tau \,.\, l_2 \,.\, \underline{0}) + l_3 \,.\, \underline{0}$, for which it holds that $R \,/\, \mathcal{A}_\mathcal{H}$ and $R \setminus \mathcal{A}_\mathcal{H}$ are isomorphic to the two sides of the law, respectively. By construction it immediately follows that R is $\mathrm{BSNNI}_{\approx_\mathrm{w}}$ but not $\mathrm{BSNNI}_{\approx_\mathrm{b}}$.
Since the only high-level action is performed by R itself, which is $\mathrm{BSNNI}_{\approx_\mathrm{w}}$, for every other process R' reachable from R it holds that $R' \setminus \mathcal{A}_\mathcal{H}$ is isomorphic to $R' \,/\, \mathcal{A}_\mathcal{H}$, hence $R \in \mathrm{SBSNNI}_{\approx_\mathrm{w}}$ but $P \notin \mathrm{SBSNNI}_{\approx_\mathrm{b}}$. ∎

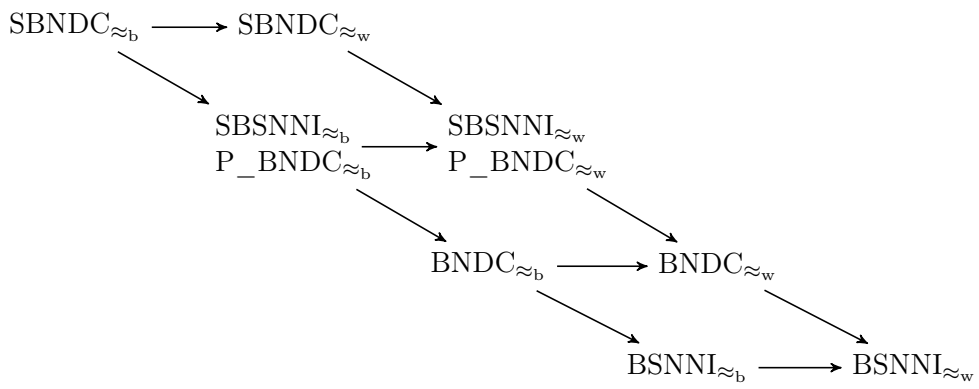


Figure 8.4: Taxonomy of security properties based on weak and branching bisimilarities

Proposition 8.3. *From* $a \,.\, (P + \tau \,.\, Q) + a \,.\, Q = a \,.\, (P + \tau \,.\, Q)$ *it is possible to construct a process* $R \in \mathbb{P}_{\mathrm{nd}}$ *such that* $R \in \mathrm{BSNNI}_{\approx_w}$ *but* $P \notin \mathrm{BSNNI}_{\approx_b}$ *and* $P \in \mathrm{SBSNNI}_{\approx_w}$ *but* $P \notin \mathrm{SBSNNI}_{\approx_b}$.

Proof. In the considered τ-law let us instantiate a as τ, P as $l_1 \,.\, \underline{0}$, and Q as $l_2 \,.\, \underline{0}$, then add $+ l_3 \,.\, \underline{0}$ to both sides of the law thus obtaining $\tau \,.\, (l_1 \,.\, \underline{0} + \tau \,.\, l_2 \,.\, \underline{0}) + \tau \,.\, l_2 \,.\, \underline{0} + l_3 \,.\, \underline{0} = \tau \,.\, (l_1 \,.\, \underline{0} + \tau \,.\, l_2 \,.\, \underline{0}) + l_3 \,.\, \underline{0}$, which are related by weak bisimilarity but not by branching bisimilarity. Now let us define process R as $\tau \,.\, (l_1 \,.\, \underline{0} + \tau \,.\, l_2 \,.\, \underline{0}) + h \,.\, l_2 \,.\, \underline{0} + l_3 \,.\, \underline{0}$, for which it holds that $R \,/\, \mathcal{A}_{\mathcal{H}}$ and $R \setminus \mathcal{A}_{\mathcal{H}}$ are isomorphic to the two sides of the law, respectively. By construction it immediately follows that R is $\mathrm{BSNNI}_{\approx_w}$ but not $\mathrm{BSNNI}_{\approx_b}$.
Since the only high-level action is performed by R itself, which is $\mathrm{BSNNI}_{\approx_w}$, for every other process R' reachable from R it holds that $R' \setminus \mathcal{A}_{\mathcal{H}}$ is isomorphic to $R' \,/\, \mathcal{A}_{\mathcal{H}}$, hence $R \in \mathrm{SBSNNI}_{\approx_w}$ but $R \notin \mathrm{SBSNNI}_{\approx_b}$. ∎

The diagram in Figure 8.4 summarizes the inclusions among the various noninterference properties based on the results in Theorems 8.1, 8.4, and 8.5, where $\mathcal{P} \to \mathcal{Q}$ means that $\mathcal{P}$ is strictly included in $\mathcal{Q}$. The arrows missing in the diagram, witnessing incomparability, are justified by the following counterexamples:

- $\mathrm{SBNDC}_{\approx_w}$ vs. $\mathrm{SBSNNI}_{\approx_b}$. The process $\tau \,.\, l \,.\, \underline{0} + l \,.\, l \,.\, \underline{0} + h \,.\, l \,.\, \underline{0}$ is $\mathrm{BSNNI}_{\approx_b}$ as $(\tau \,.\, l \,.\, \underline{0} + l \,.\, l \,.\, \underline{0} + h \,.\, l \,.\, \underline{0}) \setminus \{h\} \approx_b \tau \,.\, l \,.\, \underline{0} + l \,.\, l \,.\, \underline{0} \approx_b \tau \,.\, l \,.\, \underline{0} + l \,.\, l \,.\, \underline{0} + \tau \,.\, l \,.\, \underline{0} \approx_b (\tau \,.\, l \,.\, \underline{0} + l \,.\, l \,.\, \underline{0} + h \,.\, l \,.\, \underline{0}) \,/\, \{h\}$. It is also $\mathrm{SBSNNI}_{\approx_b}$ because every reachable process does not enable further high-level actions. However, it is not $\mathrm{SBNDC}_{\approx_w}$ because after executing the high-level action h it can perform a single l-action, while the original process with the restriction on high-level actions can go along a path where it can perform two l-actions. On the other hand, the process Q mentioned in Theorem 8.6 is $\mathrm{SBNDC}_{\approx_w}$ but neither $\mathrm{BSNNI}_{\approx_b}$ nor $\mathrm{SBSNNI}_{\approx_b}$.

- $\mathrm{SBSNNI}_{\approx_w}$ vs. $\mathrm{BNDC}_{\approx_b}$. The process $l \,.\, h \,.\, l \,.\, \underline{0} + l \,.\, \underline{0} + l \,.\, l \,.\, \underline{0}$ is $\mathrm{BSNNI}_{\approx_b}$ as $(l \,.\, h \,.\, l \,.\, \underline{0} + l \,.\, \underline{0} + l \,.\, l \,.\, \underline{0}) \setminus \{h\} \approx_b l \,.\, \underline{0} + l \,.\, \underline{0} + l \,.\, l \,.\, \underline{0} \approx_b l \,.\, \tau \,.\, l \,.\, \underline{0} + l \,.\, \underline{0} + l \,.\, l \,.\, \underline{0} \approx_b (l \,.\, h \,.\, l \,.\, \underline{0} + l \,.\, \underline{0} + l \,.\, l \,.\, \underline{0}) \,/\, \{h\}$. In particular, the subprocesses $l \,.\, l \,.\, \underline{0}$ and $l \,.\, \tau \,.\, l \,.\, \underline{0}$ are equated by virtue of the other τ-law of weak bisimilarity, i.e., $a \,.\, \tau \,.\, P = a \,.\, P$, which is a special case of the only τ-law of branching bisimilarity. The same process is $\mathrm{BNDC}_{\approx_b}$ too as it includes only one high-level action, hence the only possible high-level strategy coincides with the check conducted by $\mathrm{BSNNI}_{\approx_b}$. However, it is not $\mathrm{SBSNNI}_{\approx_w}$ because of the reachable process $h \,.\, l \,.\, \underline{0}$, which is not $\mathrm{BSNNI}_{\approx_w}$.

On the other hand, the process Q mentioned in Theorem 8.6 is $\text{SBSNNI}_{\approx_\text{w}}$ but not $\text{BSNNI}_{\approx_\text{b}}$ and, therefore, not even $\text{BNDC}_{\approx_\text{b}}$.

- $\text{BNDC}_{\approx_\text{w}}$ vs. $\text{BSNNI}_{\approx_\text{b}}$. The process $l.\underline{0} + h_1.h_2.l.\underline{0}$ is not $\text{BNDC}_{\approx_\text{w}}$ as discussed in Section 8.1.4, but it is $\text{BSNNI}_{\approx_\text{b}}$ as $(l.\underline{0} + h_1.h_2.l.\underline{0}) \setminus \{h_1, h_2\} \approx_\text{b} l.\underline{0} \approx_\text{b} l.\underline{0} + \tau.\tau.l.\underline{0} \approx_\text{b} (l.\underline{0} + h_1.h_2.l.\underline{0}) / \{h_1, h_2\}$. In contrast, the process Q mentioned in Theorem 8.6 is both $\text{BSNNI}_{\approx_\text{w}}$ and $\text{BNDC}_{\approx_\text{w}}$, but not $\text{BSNNI}_{\approx_\text{b}}$.

It is worth noting that the strongest property based on weak bisimilarity ($\text{SBNDC}_{\approx_\text{w}}$) and the weakest property based on branching bisimilarity ($\text{BSNNI}_{\approx_\text{b}}$) are incomparable too. The former is a very restrictive property because it requires a local check every time a high-level action is performed, while the latter requires a check only on the initial state. On the other hand, as shown in Theorem 8.6, it is very easy to construct processes that are secure under properties based on $\approx_\text{w}$ but not on $\approx$, due to the minimal number of high-level actions in Q.

8.4 Reversibility via Weak Back-and-Forth Bisimilarity

As done in the first part of the thesis, following [57] an LTS $(\mathcal{S}, \mathcal{A}, \longrightarrow)$ represents a reversible process if each of its transitions is seen as bidirectional. When going backward, it is of paramount importance to respect causality, i.e., the last performed transition must be the first one to be undone. In [57] a strong and a weak bisimulation equivalences were defined that enforce not only causality, but also history preservation. This means that, when going backward, a process can only backtrack, i.e., it can only move along the path representing the history that brought the process to the current state, even in the presence of concurrency. To accomplish this, the equivalences were defined over computations, not over states, and the notion of transition was suitably revised.

Definition 8.8. *A sequence* $\xi = s_0 \xrightarrow{a_1} s_1 \xrightarrow{a_2} s_2 \ldots s_{n-1} \xrightarrow{a_n} s_n$ *is a* path *of length* n *from state* s_0*. We let* $\mathit{first}(\xi) = s_0$ *and* $\mathit{last}(\xi) = s_n$*; the empty path is indicated with* ε*. We denote by* $\mathit{path}(s)$ *the set of paths from* s*.* ■

Definition 8.9. *A pair* $\rho = (s, \xi)$ *is called a* run *from state* s *iff* $\xi \in \mathit{path}(s)$*, in which case we let* $\mathit{path}(\rho) = \xi$*,* $\mathit{first}(\rho) = \mathit{first}(\xi) = s$*, and* $\mathit{last}(\rho) = \mathit{last}(\xi)$*, with* $\mathit{first}(\rho) = \mathit{last}(\rho) = s$ *when* $\xi = \varepsilon$*. We denote by* $\mathit{run}(s)$ *the set of runs from state* s*. Given* $\rho = (s, \xi) \in \mathit{run}(s)$ *and* $\rho' = (s', \xi') \in \mathit{run}(s')$*, their composition* $\rho\rho' = (s, \xi\xi') \in \mathit{run}(s)$ *is defined iff* $\mathit{last}(\rho) = \mathit{first}(\rho') = s'$*. We write* $\rho \xrightarrow{a} \rho'$ *iff there exists* $\bar\rho = (\bar s, \bar s \xrightarrow{a} s')$ *with* $\bar s = \mathit{last}(\rho)$ *such that* $\rho' = \rho\bar\rho$*; note that* $\mathit{first}(\rho) = \mathit{first}(\rho')$*.* ■

In the two bisimulation equivalences of [57], for the LTS at hand the set $\mathcal{U}$ of runs is considered in lieu of $\mathcal{S}$. Using runs instead of just paths is convenient in the case of an empty path so as to know the state under examination. Given a pair of runs (ρ_1, ρ_2), in the two definitions below recalled from [57] the forward clauses consider outgoing transitions whereas the backward clauses consider incoming transitions.

Definition 8.10. *Let* $(\mathcal{S}, \mathcal{A}, \longrightarrow)$ *be an LTS. We say that* $s_1, s_2 \in \mathcal{S}$ *are* strongly back-and-forth bisimilar*, written* $s_1 \sim_\text{bf} s_2$*, iff* $((s_1, \varepsilon), (s_2, \varepsilon)) \in \mathcal{B}$ *for some strong back-and-forth bisimulation* $\mathcal{B}$*. A symmetric relation* $\mathcal{B}$ *over* $\mathcal{U}$ *is a* strong back-and-forth bisimulation *iff, whenever* $(\rho_1, \rho_2) \in \mathcal{B}$*, then:*

- *For each* $\rho_1 \xrightarrow{a} \rho_1'$ *there exists* $\rho_2 \xrightarrow{a} \rho_2'$ *such that* $(\rho_1', \rho_2') \in \mathcal{B}$*.*
- *For each* $\rho_1' \xrightarrow{a} \rho_1$ *there exists* $\rho_2' \xrightarrow{a} \rho_2$ *such that* $(\rho_1', \rho_2') \in \mathcal{B}$*.* ■

Definition 8.11. *Let $(\mathcal{S}, \mathcal{A}, \longrightarrow)$ be an LTS. We say that $s_1, s_2 \in \mathcal{S}$ are* weakly back-and-forth bisimilar*, written $s_1 \approx_{\rm bf} s_2$, iff $((s_1, \varepsilon), (s_2, \varepsilon)) \in \mathcal{B}$ for some weak back-and-forth bisimulation $\mathcal{B}$. A symmetric relation $\mathcal{B}$ over $\mathcal{U}$ is a* weak back-and-forth bisimulation *iff, whenever $(\rho_1, \rho_2) \in \mathcal{B}$, then:*

- *For each $\rho_1 \stackrel{a}{\longrightarrow} \rho_1'$ there exists $\rho_2 \stackrel{\hat{a}}{\Longrightarrow} \rho_2'$ such that $(\rho_1', \rho_2') \in \mathcal{B}$.*
- *For each $\rho_1' \stackrel{a}{\longrightarrow} \rho_1$ there exists $\rho_2' \stackrel{\hat{a}}{\Longrightarrow} \rho_2$ such that $(\rho_1', \rho_2') \in \mathcal{B}$.* ■

In [57] it was shown that strong back-and-forth bisimilarity coincides with strong bisimilarity. Surprisingly, weak back-and-forth bisimilarity does not coincide with weak bisimilarity. Instead, it coincides with branching bisimilarity. For example, in Figure 8.1 it holds that $s_1 \not\approx_{\rm bf} s_2$ because in the forward direction $(s_1, \varepsilon) \stackrel{a}{\longrightarrow} (s_1, s_1 \stackrel{a}{\longrightarrow} s_1')$ is matched by $(s_2, \varepsilon) \stackrel{\tau}{\longrightarrow} (s_2, s_2 \stackrel{\tau}{\longrightarrow} s_2') \stackrel{a}{\longrightarrow} (s_2, s_2 \stackrel{\tau}{\longrightarrow} s_2' \stackrel{a}{\longrightarrow} s_2'')$, but then in the backward direction $(s_2, s_2 \stackrel{\tau}{\longrightarrow} s_2') \stackrel{a}{\longrightarrow} (s_2, s_2 \stackrel{\tau}{\longrightarrow} s_2' \stackrel{a}{\longrightarrow} s_2'')$ is not matched by $(s_1, \varepsilon) \stackrel{a}{\longrightarrow} (s_1, s_1 \stackrel{a}{\longrightarrow} s_1')$ because (s_1, ε) has an outgoing b-transition whilst $(s_2, s_2 \stackrel{\tau}{\longrightarrow} s_2')$ has not.

Theorem 8.7. *Let $(\mathcal{S}, \mathcal{A}, \longrightarrow)$ be an LTS and $s_1, s_2 \in \mathcal{S}$. Then:*

- *$s_1 \sim_{\rm bf} s_2$ iff $s_1 \sim s_2$.*
- *$s_1 \approx_{\rm bf} s_2$ iff $s_1 \approx_{\rm b} s_2$.* ■

Therefore the properties $\text{BSNNI}_{\approx_{\rm b}}$, $\text{BNDC}_{\approx_{\rm b}}$, $\text{SBSNNI}_{\approx_{\rm b}}$, $\text{P\_BNDC}_{\approx_{\rm b}}$, $\text{SBNDC}_{\approx_{\rm b}}$ do not change if $\approx_{\rm b}$ is replaced by $\approx_{\rm bf}$. This allows us to study noninterference properties for reversible systems by using the polynomial-time decidable $\approx_{\rm b}$ in a standard process calculus like the one of Section 8.1.3, without having to resort to truly concurrent equivalences such as the weak forward-reverse bisimilarity studied in the first part of the thesis or a weak variant of hereditary history-preserving bisimilarity (see Section 7.2.1) in a calculus relying on external memories like in [53] or executed action decorations like in [121, 35] or the first part of the thesis.

8.5 Use Case: DBMS Authentication – Branching Bisimilarity

The example provided in Section 8.2 is useful to illustrate the limitations of weak bisimilarity when investigating potential covert channels in reversible systems. In particular, it turns out that $Auth \setminus \mathcal{A}_{\mathcal{H}} \not\approx_{\rm b} Auth \,/\, \mathcal{A}_{\mathcal{H}}$, i.e., $Auth$ is not $\text{BSNNI}_{\approx_{\rm b}}$, and hence not even $\text{BNDC}_{\approx_{\rm b}}$, $\text{SBSNNI}_{\approx_{\rm b}}$, $\text{SBNDC}_{\approx_{\rm b}}$ by virtue of Theorem 8.4. As can be seen in Figure 8.3, the reason is that, if $Auth \,/\, \mathcal{A}_{\mathcal{H}}$ performs the leftmost τ-action and hence moves to state r_3', from which the only executable action is $l_{\rm sso}$, then according to the definition of branching bisimilarity $Auth \setminus \mathcal{A}_{\mathcal{H}}$ can:

- either stay idle, but from that state $Auth \setminus \mathcal{A}_{\mathcal{H}}$ can then perform actions other than $l_{\rm sso}$ that cannot be matched on the side of $Auth \,/\, \mathcal{A}_{\mathcal{H}}$;
- or perform two τ-actions thereby reaching state s_3, but the last traversed state, i.e., s_2, is not branching bisimilar to the initial state of $Auth \,/\, \mathcal{A}_{\mathcal{H}}$.

In a standard model of execution, where the computation can proceed only forward, the distinguishing power of branching bisimilarity may be considered too severe, as no practical covert channel actually occurs and the system can be deemed noninterfering as shown in Section 8.2. Indeed, a low-level user has no possibility of distinguishing

the internal move performed by $Auth \,/\, \mathcal{A}_{\mathcal{H}}$ that leads to $l_{\text{sso}} \,.\, Auth$ from the sequence of internal moves performed by $Auth \setminus \mathcal{A}_{\mathcal{H}}$ that lead to $l_{\text{sso}} \,.\, Auth$ as well. This motivates the fact that, historically, weak bisimilarity has been preferred in the setting of noninterference.

Now we know that, if we replace the branching bisimulation semantics with the weak back-and-forth bisimulation semantics, nothing changes about the outcome of noninterference verification. Assuming that the DBMS allows transactions to be reversed, it is instructive to discuss why $\text{BSNNI}_{\approx_{\text{b}}}$ is not satisfied by following the formalization of the weak back-and-forth bisimulation semantics provided in Section 8.4.

After $Auth \,/\, \mathcal{A}_{\mathcal{H}}$ performs the run $(r_1, (r_1 \xrightarrow{\tau} r_3' \xrightarrow{l_{\text{sso}}} r_1))$, process $Auth \setminus \mathcal{A}_{\mathcal{H}}$ can respond by performing the run $(s_1, (s_1 \xrightarrow{\tau} s_2 \xrightarrow{\tau} s_3 \xrightarrow{l_{\text{sso}}} s_1))$. If either process goes back by undoing l_{sso}, then the other one can undo l_{sso} as well and the states r_3' and s_3 are reached. However, if $Auth \setminus \mathcal{A}_{\mathcal{H}}$ goes further back by undoing $s_2 \xrightarrow{\tau} s_3$ too, then $Auth \,/\, \mathcal{A}_{\mathcal{H}}$ can:

- either undo $r_1 \xrightarrow{\tau} r_3'$, but in this case r_1 enables action l_{pwd} while s_2 does not;
- or stay idle, but in this case r_3' enables only l_{sso}, while s_2 can go along the path $s_2 \xrightarrow{\tau} s_4 \xrightarrow{l_{\text{2fa}}} s_1$ as well.

This line of reasoning immediately allows us to reveal a potential covert channel under reversible computing. In fact, let us assume that the transaction modeled by $Auth$ is not only executed forward, but also enables backward computations triggered, e.g., whenever debugging mode is activated [60]. This may happen in response to some user-level malfunctioning, which may be due, for instance, to the authentication operation or to the transaction execution. As formally shown above, if the action l_{sso} performed at r_3' after the high-level interaction is undone along with the latter, then the system enables again the execution of the action l_{pwd}. This is motivated in our example by the fact that, by virtue of the transaction rollback, any kind of authentication becomes admissible again. On the other hand, this is not possible after undoing the action l_{sso} performed at state s_3, because in such a case the internal decision of the DBMS of adopting a highly secure mechanism is not reversed. In other words, by reversing the computation the low-level user can become aware of the fact that the transaction data are feeding the training set or not.

In the literature, there are several reverse debuggers working in this way like, e.g., UndoDB [60], a Linux-based interactive time-travel debugger that can handle multiple threads and their backward execution. For instance, it is integrated within the DBMS SAP HANA (`https://undo.io/resources/type/case-studies/`) in order to reduce time-to-resolution of software failures. In our example, by virtue of the observations conducted above, if the system is executed backward just after performing l_{sso}, a low-level user can decide whether a high-level action had occurred before or not, thus revealing a covert channel. Such a covert channel is completely concealed during the forward execution of the system and is detected only when the system is executed backward. In general, this may happen when the reverse debugger is activated by virtue of some unexpected event (e.g., segmentation fault, stack overflow, memory corruption) caused intentionally or not, as a consequence of which some undesired information flow emerges toward low-level users.

Chapter 9

Noninterference Analysis of Probabilistic Reversible Systems

In this chapter, whose contents have appeared in [62, 64], we extend the approach of the previous chapter to address noninterference properties in a framework featuring nondeterminism, probabilities, and reversibility. The starting point for our study is given by the probabilistic variants of BSNNI, BNDC, and SBNDC developed in [7] over a probabilistic process calculus based on a combination of the generative and reactive probabilistic models of [79]. In addition to probabilistic choice, in [7] other operators such as parallel composition and hiding are decorated with a probabilistic parameter, so that the selection among all the actions executable by a process is fully probabilistic. Moreover, the behavioral equivalence considered in [7] is akin to the weak probabilistic bisimilarity of [13], which is known to coincide with probabilistic branching bisimilarity over fully probabilistic processes.

Here we move to a more expressive setting combining nondeterminism and probabilities through the strictly alternating model of [86]. In this model, states are divided into nondeterministic and probabilistic, while transitions are divided into action transitions – each labeled with an action and going from a nondeterministic state to a probabilistic one – and probabilistic transitions – each labeled with a probability and going from a probabilistic state to a nondeterministic one. A more flexible variant, called the non-strictly alternating model [120], allows for action transitions also between two nondeterministic states. An alternative model is the non-alternating one given by Segala simple probabilistic automata [133], where every transition is labeled with an action and goes from a state to a probability distribution over states. Both the alternating model and the non-alternating one – whose relationships have been studied in [135] – encompass nondeterministic models, generative models, and reactive models as special cases. Due to the fundamental role played by branching bisimulation semantics in reversible systems, we adopt the alternating model because of the probabilistic branching bisimulation congruence developed for it in [8] along with equational and logical characterizations and a polynomial-time decision procedure. In the non-alternating model, for which branching bisimilarity has been just defined in [134], weak variants of bisimulation semantics require – to achieve transitivity – that a single transition be matched by a convex combination of several transitions – corresponding to the use of randomized schedulers – which causes such equivalences to be less manageable although they can be decided in polynomial time [138].

Following [86] we build a process calculus that, unlike the one in [7], supports nondeterminism and decorates with probabilistic parameters only probabilistic choices. As for behavioral equivalences, we introduce a weak probabilistic bisimilarity inspired by the one in [120] and adapt the probabilistic branching bisimilarity of the non-strictly alternating model in [8]. By using these two equivalences we recast the noninterference properties

of [67, 69] for irreversible systems and the noninterference properties of the previous chapter for reversible systems, respectively, to study their preservation and compositionality aspects as well as to provide a taxonomy similar to the one in the previous chapter. Unlike [7], the resulting noninterference properties are lighter as they do not need additional universal quantifications over probabilistic parameters. Furthermore, reversibility comes into play by extending one of the results of [57] to the strictly alternating model; we show that a probabilistic variant of weak back-and-forth bisimilarity coincides with our adaptation of the probabilistic branching bisimilarity of [8]. Finally, we point out that for proving some results we have to resort to the bisimulation-up-to technique [131] and therefore introduce probabilistic variants of up-to weak [112] and branching [75] bisimulations.

This chapter is organized as follows. In Section 9.1 we recall the strictly alternating model of [86] along with various definitions of strong and weak bisimilarities for it – with weak ones inspired by [120, 8] – and a process calculus interpreted on it. In Section 9.2 we recast in this probabilistic framework the aforementioned selection of noninterference properties, study their preservation and compositionality characteristics, develop their taxonomy, and relate it to the nondeterministic taxonomy. In Section 9.3 we establish a connection with reversibility by introducing a weak probabilistic back-and-forth bisimilarity and proving that it coincides with probabilistic branching bisimilarity. Finally, in Section 9.4 we present an example of a lottery implemented through a probabilistic smart contract to show the adequacy of our approach when dealing with information flows in systems featuring nondeterminism and probabilities, both in the irreversible case and in the reversible one.

9.1 Background Definitions and Results

In this section we recall the strict alternating model of [86] (Section 9.1.1) along with strong and weak probabilistic bisimilarities [120] and probabilistic branching bisimilarity [8] (Section 9.1.2). Then we introduce a probabilistic process language inspired by [86] (Section 9.1.3) through which we will express bisimulation-based information-flow security properties accounting for nondeterminism and probabilities.

9.1.1 Probabilistic Labeled Transition Systems

To represent the behavior of a process featuring nondeterminism and probabilities, we use a probabilistic labeled transition system. This is a variant of a labeled transition system [97] whose transitions are labeled with actions or probabilities. Since we adopt the strictly alternating model of [86], we distinguish between nondeterministic and probabilistic states. The transitions of the former are labeled only with actions, while the transitions of the latter are labeled only with probabilities. Every action transition leads from a nondeterministic state to a probabilistic one, while every probabilistic transition leads from a probabilistic state to a nondeterministic one. In the following, we denote by $\mathcal{S}_{\rm n}$ (resp. $\mathcal{S}_{\rm p}$) the set of nondeterministic (resp. probabilistic) states. We recall that the action set $\mathcal{A}$ contains the unobservable action τ.

Definition 9.1. *A* probabilistic labeled transition system (PLTS) *is a triple* $(\mathcal{S}, \mathcal{A}, \longrightarrow)$ *where* $\mathcal{S} = \mathcal{S}_{\rm n} \cup \mathcal{S}_{\rm p}$ *with* $\mathcal{S}_{\rm n} \cap \mathcal{S}_{\rm p} = \emptyset$ *is an at most countable set of states,* $\mathcal{A}$ *is a countable set of actions, and* $\longrightarrow = \longrightarrow_{\rm a} \cup \longrightarrow_{\rm p}$ *is the transition relation, with* $\longrightarrow_{\rm a} \subseteq \mathcal{S}_{\rm n} \times \mathcal{A} \times \mathcal{S}_{\rm p}$ *being the action transition relation whilst* $\longrightarrow_{\rm p} \subseteq \mathcal{S}_{\rm p} \times \mathbb{R}_{]0,1]} \times \mathcal{S}_{\rm n}$ *being the probabilistic transition relation satisfying* $\sum_{(s,p,s') \in \longrightarrow_{\rm p}} p \in \{0, 1\}$ *for all* $s \in \mathcal{S}_{\rm p}$. ■

An action transition (s, a, s') is written $s \xrightarrow{a}_{\rm a} s'$ while a probabilistic transition (s, p, s') is written $s \xrightarrow{p}_{\rm p} s'$, where s is the source state and s' is the target state. We say that s' is reachable from s, written $s' \in \mathit{reach}(s)$, iff $s' = s$ or there exists a sequence of finitely many transitions such that the target state of each of them coincides

with the source state of the subsequent one, with the source of the first one being s and the target of the last one being s'.

9.1.2 Probabilistic Bisimulation Equivalences

Bisimilarity [117, 112] identifies processes that are able to mimic each other's behavior stepwise, i.e., having the same branching structure. In the strictly alternating model, this extends to probabilistic behavior [86]. Let $\pi(s, C) = \sum_{s \xrightarrow{p}_{\mathrm{p}} s', s' \in C} p$ be the cumulative probability with which state s reaches a state in C; note that $\pi(s, C) = 0$ when s is not a probabilistic state or C is not a set of nondeterministic states.

Definition 9.2. *Let $(\mathcal{S}, \mathcal{A}, \longrightarrow)$ be a PLTS. We say that $s_1, s_2 \in \mathcal{S}$ are* strongly probabilistic bisimilar*, written $s_1 \sim_{\mathrm{p}} s_2$, iff $(s_1, s_2) \in \mathcal{B}$ for some strong probabilistic bisimulation $\mathcal{B}$. An equivalence relation $\mathcal{B} \subseteq (\mathcal{S}_{\mathrm{n}} \times \mathcal{S}_{\mathrm{n}}) \cup (\mathcal{S}_{\mathrm{p}} \times \mathcal{S}_{\mathrm{p}})$ is a* strong probabilistic bisimulation *iff, whenever $(s_1, s_2) \in \mathcal{B}$, then:*

- *For each $s_1 \xrightarrow{a}_{\mathrm{a}} s_1'$ there exists $s_2 \xrightarrow{a}_{\mathrm{a}} s_2'$ such that $(s_1', s_2') \in \mathcal{B}$.*
- *$\pi(s_1, C) = \pi(s_2, C)$ for all equivalence classes $C \in \mathcal{S}_{\mathrm{n}}/\mathcal{B}$.* ■

In [120] a strong probabilistic bisimilarity more liberal than the one in [86] allows a nondeterministic state and a probabilistic state to be identified when the latter concentrates all of its probabilistic mass in reaching the former. Think, e.g., of a probabilistic state whose outgoing transitions all reach the same nondeterministic state. To this purpose the following function is introduced in [120]:

$$prob(s, s') = \begin{cases} p & \text{if } s \in \mathcal{S}_{\mathrm{p}} \wedge \sum_{s \xrightarrow{p'}_{\mathrm{p}} s'} p' = p > 0 \\ 1 & \text{if } s \in \mathcal{S}_{\mathrm{n}} \wedge s' = s \\ 0 & \text{otherwise} \end{cases}$$

and is then lifted to a set C of states by letting $prob(s, C) = \sum_{s' \in C} prob(s, s')$.

Definition 9.3. *Let $(\mathcal{S}, \mathcal{A}, \longrightarrow)$ be a PLTS. We say that $s_1, s_2 \in \mathcal{S}$ are* strongly mix-probabilistic bisimilar*, written $s_1 \sim_{\mathrm{pm}} s_2$, iff $(s_1, s_2) \in \mathcal{B}$ for some strong mix-probabilistic bisimulation $\mathcal{B}$. An equivalence relation $\mathcal{B}$ over $\mathcal{S}$ is a* strong mix-probabilistic bisimulation *iff, whenever $(s_1, s_2) \in \mathcal{B}$, then:*

- *If $s_1, s_2 \in \mathcal{S}_{\mathrm{n}}$, for each $s_1 \xrightarrow{a}_{\mathrm{a}} s_1'$ there exists $s_2 \xrightarrow{a}_{\mathrm{a}} s_2'$ such that $(s_1', s_2') \in \mathcal{B}$.*
- *$prob(s_1, C) = prob(s_2, C)$ for all equivalence classes $C \in \mathcal{S}/\mathcal{B}$.* ■

Weak bisimilarity [112] is additionally capable of abstracting from unobservable actions. In a probabilistic setting, it is also desirable to be able to abstract from probabilistic transitions in certain circumstances. Let $s \Longrightarrow s'$ mean that $s' \in reach(s)$ and, when $s' \neq s$, there exists a finite sequence of transitions from s to s' in which τ-transitions and probabilistic transitions alternate. Moreover let $\stackrel{a}{\Longrightarrow}$ stand for $\Longrightarrow \xrightarrow{a}_{\mathrm{a}} \Longrightarrow$ and $\stackrel{\hat{a}}{\Longrightarrow}$ stand for $\Longrightarrow$ if $a = \tau$ or $\stackrel{a}{\Longrightarrow}$ if $a \neq \tau$. The weak probabilistic bisimilarity below is inspired by the one in [120]. The constraint $s_1, s_2 \in \mathcal{S}_{\mathtt{n}}$ occurring in the first clause of Definition 9.3 is no longer necessary due to the use of $\Longrightarrow$.

Definition 9.4. *Let $(\mathcal{S}, \mathcal{A}, \longrightarrow)$ be a PLTS. We say that $s_1, s_2 \in \mathcal{S}$ are* weakly probabilistic bisimilar*, written $s_1 \approx_{\mathrm{pw}} s_2$, iff $(s_1, s_2) \in \mathcal{B}$ for some weak probabilistic bisimulation $\mathcal{B}$. An equivalence relation $\mathcal{B}$ over $\mathcal{S}$ is a* weak probabilistic bisimulation *iff, whenever $(s_1, s_2) \in \mathcal{B}$, then:*

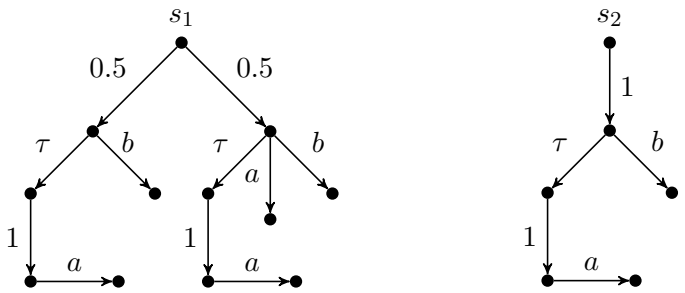


Figure 9.1: States related by $\approx_{\mathrm{pw}}$ but distinguished by $\approx_{\mathrm{pb}}$

- *For each* $s_1 \xrightarrow{a}_{\mathrm{a}} s_1'$ *there exists* $s_2 \stackrel{\hat{a}}{\Longrightarrow} s_2'$ *such that* $(s_1', s_2') \in \mathcal{B}$.
- $prob(s_1, C) = prob(s_2, C)$ *for all equivalence classes* $C \in \mathcal{S}/\mathcal{B}$. ■

Branching bisimilarity [80] is finer than weak bisimilarity as it preserves the branching structure of processes even when abstracting from τ-actions – see condition $(s_1, \bar{s}_2) \in \mathcal{B}$ in the definition below. The probabilistic branching bisimilarity that follows is inspired by the one in [8].

Definition 9.5. *Let* $(\mathcal{S}, \mathcal{A}, \longrightarrow)$ *be a PLTS. We say that* $s_1, s_2 \in \mathcal{S}$ *are* probabilistic branching bisimilar*, written* $s_1 \approx_{\mathrm{pb}} s_2$*, iff* $(s_1, s_2) \in \mathcal{B}$ *for some probabilistic branching bisimulation* $\mathcal{B}$*. An equivalence relation* $\mathcal{B}$ *over* $\mathcal{S}$ *is a* probabilistic branching bisimulation *iff, whenever* $(s_1, s_2) \in \mathcal{B}$*, then:*

- *For each* $s_1 \xrightarrow{a}_{\mathrm{a}} s_1'$*:*
  - *either* $a = \tau$ *and* $(s_1', s_2) \in \mathcal{B}$*;*
  - *or there exists* $s_2 \Longrightarrow \bar{s}_2 \xrightarrow{a}_{\mathrm{a}} s_2'$ *such that* $(s_1, \bar{s}_2) \in \mathcal{B}$ *and* $(s_1', s_2') \in \mathcal{B}$.
- $prob(s_1, C) = prob(s_2, C)$ *for all equivalence classes* $C \in \mathcal{S}/\mathcal{B}$. ■

An example that highlights the higher distinguishing power of probabilistic branching bisimilarity is given in Figure 9.1, where every PLTS is depicted as a directed graph in which vertices represent states and action- or probability-labeled edges represent transitions. The initial states s_1 and s_2 of the two PLTSs are weakly probabilistic bisimilar but not probabilistic branching bisimilar. On the one hand, each of the two states reachable from s_1 with probability 0.5 and the state reachable from s_2 with probability 1 are all weakly probabilistic bisimilar and hence the cumulative probability to reach them is the same from both initial states. On the other hand, the two states reachable from s_1 are not probabilistic branching bisimilar, because if the one on the right performs a then the one on the left cannot respond by performing τ, 1, and a because the state executing a no longer enables b. Thus, with respect to probabilistic branching bisimilarity, s_1 reaches with probability 0.5 two different equivalence classes, while s_2 reaches with probability 1 only one of them.

Prefix	$a \,.\, P \xrightarrow{a}_{\mathrm{a}} P$
Choice	$\dfrac{N_1 \xrightarrow{a}_{\mathrm{a}} P_1}{N_1 + N_2 \xrightarrow{a}_{\mathrm{a}} P_1} \qquad \dfrac{N_2 \xrightarrow{a}_{\mathrm{a}} P_2}{N_1 + N_2 \xrightarrow{a}_{\mathrm{a}} P_2}$
Parallel	$\dfrac{N_1 \xrightarrow{a}_{\mathrm{a}} P_1 \quad a \notin L}{N_1 \parallel_L N_2 \xrightarrow{a}_{\mathrm{a}} P_1 \parallel_L [1]N_2} \qquad \dfrac{N_2 \xrightarrow{a}_{\mathrm{a}} P_2 \quad a \notin L}{N_1 \parallel_L N_2 \xrightarrow{a}_{\mathrm{a}} [1]N_1 \parallel_L P_2}$
Synch	$\dfrac{N_1 \xrightarrow{a}_{\mathrm{a}} P_1 \quad N_2 \xrightarrow{a}_{\mathrm{a}} P_2 \quad a \in L}{N_1 \parallel_L N_2 \xrightarrow{a}_{\mathrm{a}} P_1 \parallel_L P_2}$
Restriction	$\dfrac{N \xrightarrow{a}_{\mathrm{a}} P \quad a \notin L}{N \setminus L \xrightarrow{a}_{\mathrm{a}} P \setminus L}$
Hiding	$\dfrac{N \xrightarrow{a}_{\mathrm{a}} P \quad a \in L}{N \,/\, L \xrightarrow{\tau}_{\mathrm{a}} P \,/\, L} \qquad \dfrac{N \xrightarrow{a}_{\mathrm{a}} P \quad a \notin L}{N \,/\, L \xrightarrow{a}_{\mathrm{a}} P \,/\, L}$
Constant	$\dfrac{NK \triangleq N \quad N \xrightarrow{a}_{\mathrm{a}} P}{NK \xrightarrow{a}_{\mathrm{a}} P}$

Table 9.1: Operational semantic rules for nondeterministic processes (action transitions)

9.1.3 A Probabilistic Process Calculus with High and Low Actions

We now introduce a probabilistic process calculus to formalize the security properties of interest. To address two security levels, like in the previous chapter we partition the set $\mathcal{A} \setminus \{\tau\}$ of observable actions into $\mathcal{A}_{\mathcal{H}} \cup \mathcal{A}_{\mathcal{L}}$, with $\mathcal{A}_{\mathcal{H}} \cap \mathcal{A}_{\mathcal{L}} = \emptyset$, where $\mathcal{A}_{\mathcal{H}}$ is the set of high-level actions, ranged over by h, and $\mathcal{A}_{\mathcal{L}}$ is the set of low-level actions, ranged over by l. Note that $\tau \notin \mathcal{A}_{\mathcal{H}} \cup \mathcal{A}_{\mathcal{L}}$.

The overall set of process terms is given by $\mathbb{P}_{\mathrm{pr}} = \mathbb{P}_{\mathrm{n}} \cup \mathbb{P}_{\mathrm{p}}$ and ranged over by E. The set $\mathbb{P}_{\mathrm{n}}$ of nondeterministic process terms, ranged over by N, is obtained by considering typical operators from CCS [112] and CSP [45]. The set $\mathbb{P}_{\mathrm{p}}$ of probabilistic process terms, ranged over by P, is obtained by taking a probabilistic choice operator similar to the one of [86]. In addition to action prefix, choice, and parallel composition – taken from CSP so as not to turn synchronizations among high-level actions into τ as would happen with the CCS parallel composition – we include restriction and hiding, as they are necessary to formalize noninterference properties, and recursion. The syntax for $\mathbb{P}_{\mathrm{pr}}$ is:

$$\begin{array}{rcl} N & ::= & \underline{0} \mid a \,.\, P \mid N + N \mid N \parallel_L N \mid N \setminus L \mid N \,/\, L \mid NK \\ P & ::= & \bigoplus_{i \in I} [p_i] N_i \mid P \parallel_L P \mid P \setminus L \mid P \,/\, L \mid PK \end{array}$$

where:

- $\underline{0}$ is the terminated process.
- $a \,.\, \_$, for $a \in \mathcal{A}$, is the action prefix operator describing a process that can initially perform action a.
- $\_ + \_$ is the alternative composition operator expressing a nondeterministic choice between two processes based on their initially executable actions.

ProbChoice	$\dfrac{j \in I}{\bigoplus_{i \in I}[p_i]N_i \xrightarrow{p_j}_{\mathrm{p}} N_j}$
ProbSync	$\dfrac{P_1 \xrightarrow{p_1}_{\mathrm{p}} N_1 \quad P_2 \xrightarrow{p_2}_{\mathrm{p}} N_2}{P_1 \parallel_L P_2 \xrightarrow{p_1 \cdot p_2}_{\mathrm{p}} N_1 \parallel_L N_2}$
ProbRestriction	$\dfrac{P \xrightarrow{p}_{\mathrm{p}} N}{P \setminus L \xrightarrow{p}_{\mathrm{p}} N \setminus L}$
ProbHiding	$\dfrac{P \xrightarrow{p}_{\mathrm{p}} N}{P / L \xrightarrow{p}_{\mathrm{p}} N / L}$
ProbConstant	$\dfrac{PK \triangleq P \quad P \xrightarrow{p}_{\mathrm{p}} N}{PK \xrightarrow{p}_{\mathrm{p}} N}$

Table 9.2: Operational semantic rules for probabilistic processes (probabilistic transitions)

- $\bigoplus_{i \in I}[p_i]\,\_$, for I finite and not empty, is the generalized probabilistic composition operator expressing a probabilistic choice among finitely many processes each with probability $p_i \in \mathbb{R}_{]0,1]}$ and such that $\sum_{i \in I} p_i = 1$. We will use $[p_1]N_1 \oplus [p_2]N_2$ as a shorthand for $\bigoplus_{i \in \{1,2\}}[p_i]N_i$ and $a\,.\,N$ as a shorthand for $a\,.\,[1]N$ especially when N is $\underline{0}$.

- $\_ \parallel_L \_$, for $L \subseteq \mathcal{A} \setminus \{\tau\}$, is the parallel composition operator allowing two processes to proceed independently on any action not in L and forcing them to synchronize on every action in L as well as on probabilities (which are multiplied) [86].

- $\_ \setminus L$, for $L \subseteq \mathcal{A} \setminus \{\tau\}$, is the restriction operator, which prevents the execution of all actions belonging to L.

- $\_ / L$, for $L \subseteq \mathcal{A} \setminus \{\tau\}$, is the hiding operator, which turns all the executed actions belonging to L into the unobservable action τ.

- NK (resp. PK) is a process constant equipped with a defining equation of the form $NK \triangleq N$ (resp. $PK \triangleq P$), where every constant possibly occurring in N (resp. P) – including NK (resp. PK) itself thus allowing for recursion – must be in the scope of an action prefix.

The operational semantic rules for the process language are shown in Tables 9.1 and 9.2 for nondeterministic and probabilistic processes respectively. Together they produce the PLTS $(\mathbb{P}_{\mathrm{pr}}, \mathcal{A}, \longrightarrow)$ where $\longrightarrow = \longrightarrow_{\mathrm{a}} \cup \longrightarrow_{\mathrm{p}}$, to which the bisimulation equivalences defined in Section 9.1.2 are applicable. While $\longrightarrow_{\mathrm{a}} \subseteq \mathbb{P}_{\mathrm{n}} \times \mathcal{A} \times \mathbb{P}_{\mathrm{p}}$ is a relation, $\longrightarrow_{\mathrm{p}} \subseteq \mathbb{P}_{\mathrm{p}} \times \mathbb{R}_{]0,1]} \times \mathbb{P}_{\mathrm{n}}$ is deemed to be a multirelation [86]; e.g., from $[p_1]N \oplus [p_2]N$ there must be two transitions to N even when $p_1 = p_2$ otherwise the probabilities labeling the transitions departing from the source process would not sum up to 1. Note that in the *Parallel* rules the nondeterministic subprocess that does not move has to be prefixed by [1] to make it probabilistic within the overall target process [86]; after all, $[1]N \sim_{\mathrm{pm}} N$. We let $[1]N \in \mathit{reach}(E)$ whenever $N \in \mathit{reach}(E)$.

9.2 Probabilistic Information-Flow Security Properties

In this section, after recasting the definitions of noninterference properties of the previous chapter by taking as behavioral equivalence the weak or branching bisimilarity of Section 9.1.2, we investigate their preservation and compositionality characteristics (Section 9.2.1), we show the inclusion relationships between the ones based on $\approx_{\rm pw}$ and the ones based on $\approx_{\rm pb}$ (Section 9.2.2), and we relate the resulting probabilistic taxonomy with the nondeterministic one (Section 9.2.3).

Definition 9.6. *Let $E \in \mathbb{P}_{\rm pr}$ and $\approx \in \{\approx_{\rm pw}, \approx_{\rm pb}\}$:*

- $E \in {\rm BSNNI}_\approx \iff E \setminus \mathcal{A}_\mathcal{H} \approx E / \mathcal{A}_\mathcal{H}$.
- $E \in {\rm BNDC}_\approx \iff$ *for all* $F \in \mathbb{P}_{\rm pr}$ *such that each of its actions belongs to* $\mathcal{A}_\mathcal{H}$ *and for all* $L \subseteq \mathcal{A}_\mathcal{H}$, $E \setminus \mathcal{A}_\mathcal{H} \approx ((E \parallel_L F) / L) \setminus \mathcal{A}_\mathcal{H}$ *when* $E, F \in \mathbb{P}_{\rm n}$ *or* $E, F \in \mathbb{P}_{\rm p}$.
- $E \in {\rm SBSNNI}_\approx \iff$ *for all* $E' \in reach(E)$, $E' \in {\rm BSNNI}_\approx$.
- $E \in {\rm P\_BNDC}_\approx \iff$ *for all* $E' \in reach(E)$, $E' \in {\rm BNDC}_\approx$.
- $E \in {\rm SBNDC}_\approx \iff$ *for all* $E', E'' \in reach(E)$ *such that* $E' \xrightarrow{h}_{\rm a} E''$, $E' \setminus \mathcal{A}_\mathcal{H} \approx E'' \setminus \mathcal{A}_\mathcal{H}$. ■

To see the different distinguishing power of these probabilistic noninterference properties, we can adapt the examples of Section 8.1.4. For instance, in this probabilistic setting, a low-level agent that observes the execution of l in $E = l\,.\,\underline{0} + l\,.\,([0.5]h\,.\,[1]l_1\,.\,\underline{0} \oplus [0.5]h\,.\,[1]l_2\,.\,\underline{0}) + l\,.\,([0.5]l_1\,.\,\underline{0} \oplus [0.5]l_2\,.\,\underline{0})$ cannot infer anything about the execution of h. Indeed, after the execution of l, what the low-level agent observes is either a terminal state, reached with probability 1, or the execution of either l_1 or l_2, both with probability 0.5. Formally, $E\setminus\{h\} \approx E\,/\,\{h\}$ because $l\,.\,\underline{0}+l\,.\,([0.5]\underline{0}\oplus[0.5]\underline{0})+l\,.\,([0.5]l_1\,.\,\underline{0}\oplus[0.5]l_2\,.\,\underline{0}) \approx l\,.\,\underline{0}+l\,.\,([0.5]\tau\,.\,[1]l_1\,.\,\underline{0}\oplus[0.5]\tau\,.\,[1]l_2\,.\,\underline{0})+l\,.\,([0.5]l_1\,.\,\underline{0}\oplus[0.5]l_2\,.\,\underline{0})$, hence E is ${\rm BSNNI}_\approx$.

On the other hand, in $F = l\,.\,\underline{0} + l\,.\,([0.5]h_1\,.\,[1]l_1\,.\,\underline{0} \oplus [0.5]h_2\,.\,[1]l_2\,.\,\underline{0}) + l\,.\,([0.5]l_1\,.\,\underline{0} \oplus [0.5]l_2\,.\,\underline{0})$, which is ${\rm BSNNI}_\approx$ for the same reason discussed above, a high-level agent could decide to enable only h_1, thus turning the low-level view of the system into $l\,.\,\underline{0} + l\,.\,([0.5]\tau\,.\,[1]l_1\,.\,\underline{0} \oplus [0.5]\underline{0}) + l\,.\,([0.5]l_1\,.\,\underline{0} \oplus [0.5]l_2\,.\,\underline{0})$, which is clearly distinguishable from $l\,.\,\underline{0} + l\,.\,([0.5]\underline{0} \oplus [0.5]\underline{0}) + l\,.\,([0.5]l_1\,.\,\underline{0} \oplus [0.5]l_2\,.\,\underline{0})$, as in the former there is a case in which the low-level agent can observe l_1 but not l_2 after the execution of l. In other words, F is not ${\rm BNDC}_\approx$.

9.2.1 Preservation and Compositionality

All the probabilistic noninterference properties of Definition 9.6 turn out to be preserved by the bisimilarity employed in their definition. This means that if a process E_1 is secure under any of such properties, then every other equivalent process E_2 is secure too according to the same property. This is very useful for automated property verification, as it allows us to work with the process with the smallest state space among the equivalent ones.

The preservation result of Theorem 9.1 immediately follows from Lemma 9.2 below, which ensures that $\approx_{\rm pw}$ and $\approx_{\rm pb}$ are congruences with respect to all the operators occurring in the aforementioned noninterference properties. Congruence with respect to action prefix is also addressed as it will be exploited in the proof of the compositionality result of Theorem 9.2. Similar congruence properties have been proven in [8] for $\approx_{\rm pb}$ in the non-strictly alternating model.

The congruence lemma is preceded by the following lemma about the relationship between parallel composition of processes and product of probabilities.

Lemma 9.1. *Let* $E_1 \parallel_L E_2, E'_1 \parallel_L E'_2 \in \mathbb{P}_{\rm pr}$. *Then* $prob(E_1 \parallel_L E_2, E'_1 \parallel_L E'_2) = prob(E_1, E'_1) \cdot prob(E_2, E'_2)$.

Proof. There are two cases:

- If G_1 and G_2 are both nondeterministic, then $prob(G_1, G'_1) \cdot prob(G_2, G'_2) = 1$ if $G_1 = G'_1$ and $G_2 = G'_2$ while $prob(G_1, G'_1) \cdot prob(G_2, G'_2) = 0$ otherwise. From this fact it follows that $prob(G_1 \parallel_L G_2, G'_1 \parallel_L G'_2) = 1$ if $G_1 \parallel_L G_2 = G'_1 \parallel_L G'_2$, i.e., $G_1 = G'_1$ and $G_2 = G'_2$, while $prob(G_1 \parallel_L G_2, G'_1 \parallel_L G'_2) = 0$ otherwise.
- If G_1 and G_2 are both probabilistic, then $prob(G_1, G'_1) = \sum_{G_1 \xrightarrow{p}_{\rm p} G'_1} p$ and $prob(G_2, G'_2) = \sum_{G_2 \xrightarrow{q}_{\rm p} G'_2} q$ and hence $prob(G_1, G'_1) \cdot prob(G_2, G'_2) = \sum_{G_1 \xrightarrow{p}_{\rm p} G'_1} p \cdot \sum_{G_2 \xrightarrow{q}_{\rm p} G'_2} q = \sum_{G_1 \xrightarrow{p}_{\rm p} G'_1} \sum_{G_2 \xrightarrow{q}_{\rm p} G'_2} p \cdot q$ by distributivity, which is equal to $prob(G_1 \parallel_L G_2, G'_1 \parallel_L G'_2)$ according to the operational semantic rules in Table 9.2. ■

Lemma 9.2. *Let* $E_1, E_2 \in \mathbb{P}_{\rm pr}$ *and* $\approx \in \{\approx_{\rm pw}, \approx_{\rm pb}\}$. *If* $E_1 \approx E_2$ *then:*

1. $a \,.\, E_1 \approx a \,.\, E_2$ *for all* $a \in \mathcal{A}$, *when* $E_1, E_2 \in \mathbb{P}_{\rm p}$.
2. $E_1 \parallel_L E \approx E_2 \parallel_L E$ *and* $E \parallel_L E_1 \approx E \parallel_L E_2$ *for all* $L \subseteq \mathcal{A} \setminus \{\tau\}$ *and* $E \in \mathbb{P}_{\rm pr}$, *when* $E_1, E_2, E \in \mathbb{P}_{\rm n}$ *or* $E_1, E_2, E \in \mathbb{P}_{\rm p}$.
3. $E_1 \setminus L \approx E_2 \setminus L$ *for all* $L \subseteq \mathcal{A} \setminus \{\tau\}$.
4. $E_1 \,/\, L \approx E_2 \,/\, L$ *for all* $L \subseteq \mathcal{A} \setminus \{\tau\}$.

Proof. We first prove the four results for the $\approx_{\rm pw}$-based properties. Let $\mathcal{B}$ be a weak probabilistic bisimulation witnessing $E_1 \approx_{\rm pw} E_2$:

1. The equivalence relation $\mathcal{B}' = (\mathcal{B} \cup \{(a \,.\, F_1, a \,.\, F_2) \mid (F_1, F_2) \in \mathcal{B} \wedge F_1, F_2 \in \mathbb{P}_{\rm p}\})^+$ is a weak probabilistic bisimulation too. The result immediately follows from the fact that, given $(a \,.\, F_1, a \,.\, F_2) \in \mathcal{B}'$ with $(F_1, F_2) \in \mathcal{B}$, $a \,.\, F_1 \xrightarrow{a}_{\rm a} F_1$ is matched by $a \,.\, F_2 \Longrightarrow a \,.\, F_2 \xrightarrow{a}_{\rm a} F_2 \Longrightarrow F_2$ with $(F_1, F_2) \in \mathcal{B}'$ as well as $prob(a \,.\, F_1, \bar{C}) = prob(a \,.\, F_2, \bar{C}) = 1$ for $\bar{C} = [a \,.\, F_1]_{\mathcal{B}'}$ while $prob(a \,.\, F_1, C') = prob(a \,.\, F_2, C') = 0$ for any other $C' \in \mathbb{P}_{\rm pr}/\mathcal{B}'$.
2. The equivalence relation $\mathcal{B}' = \mathcal{I}_{\mathbb{P}_{\rm pr}} \cup \{(F_1 \parallel_L F, F_2 \parallel_L F) \mid (F_1, F_2) \in \mathcal{B} \wedge (F_1 \parallel_L F, F_2 \parallel_L F \in \mathbb{P}_{\rm n} \vee F_1 \parallel_L F, F_2 \parallel_L F \in \mathbb{P}_{\rm p})\}$ $\cup \{(F_1 \parallel_L [1]F, F_2 \parallel_L F) \mid (F_1, F_2) \in \mathcal{B} \wedge F_1 \in \mathbb{P}_{\rm p} \wedge F_2 \parallel_L F \in \mathbb{P}_{\rm n}\} \cup \{(F_1 \parallel_L F, F_2 \parallel_L [1]F) \mid (F_1, F_2) \in \mathcal{B} \wedge F_2 \in \mathbb{P}_{\rm p} \wedge F_1 \parallel_L F \in \mathbb{P}_{\rm n}\}$ and its variant $\mathcal{B}''$ in which F occurs to the left of parallel composition in each pair are weak probabilistic bisimulations too. Let us focus on $\mathcal{B}'$. Given $(F_1 \parallel_L F, F_2 \parallel_L F) \in \mathcal{B}'$ with $(F_1, F_2) \in \mathcal{B}$, there are three cases for action transitions based on the operational semantic rules in Table 9.1:
   - If $F_1 \parallel_L F \xrightarrow{a}_{\rm a} F'_1 \parallel_L [1]F$ with $F_1 \xrightarrow{a}_{\rm a} F'_1$ and $a \notin L$, then there exists $F_2 \stackrel{\hat{a}}{\Longrightarrow} F'_2$ such that $(F'_1, F'_2) \in \mathcal{B}$. Note that the action transition from $F_1 \parallel_L F$ implies that $F_1 \parallel_L F \in \mathbb{P}_{\rm n}$, i.e., $F_1, F \in \mathbb{P}_{\rm n}$, hence $F_2 \parallel_L F \in \mathbb{P}_{\rm n}$ too. Since synchronization does not apply to τ and $a \notin L$, we have that $F_2 \parallel_L F \stackrel{\hat{a}}{\Longrightarrow} F'_2 \parallel_L F$ with $(F'_1 \parallel_L [1]F, F'_2 \parallel_L F) \in \mathcal{B}'$ if F_2 stays idle, while $F_2 \parallel_L F \stackrel{\hat{a}}{\Longrightarrow} F'_2 \parallel_L [1]F$ with $(F'_1 \parallel_L [1]F, F'_2 \parallel_L [1]F) \in \mathcal{B}'$ if F_2 moves, in which case the right subprocess alternates between F and $[1]F$ thus allowing the probabilistic transitions along $F_2 \stackrel{\hat{a}}{\Longrightarrow} F'_2$ to synchronize with the only one of $[1]F$.

- The case $F_1 \parallel_L F \xrightarrow{a}_{\rm a} [1]F_1 \parallel_L F'$ with $F \xrightarrow{a}_{\rm a} F'$ and $a \notin L$ is trivial.
- If $F_1 \parallel_L F \xrightarrow{a}_{\rm a} F_1' \parallel_L F'$ with $F_1 \xrightarrow{a}_{\rm a} F_1'$, $F \xrightarrow{a}_{\rm a} F'$, and $a \in L$, then there exists $F_2 \Longrightarrow \xrightarrow{a}_{\rm a} \Longrightarrow F_2'$ such that $(F_1', F_2') \in \mathcal{B}$. Since synchronization does not apply to τ and $a \in L$, we have that $F_2 \parallel_L F \Longrightarrow \xrightarrow{a}_{\rm a} \Longrightarrow F_2' \parallel_L F'$ with $(F_1' \parallel_L F', F_2' \parallel_L F') \in \mathcal{B}'$, where the right subprocess alternates between F and $[1]F$ before performing a or between F' and $[1]F'$ after performing a thus allowing the probabilistic transitions along $F_2 \Longrightarrow \xrightarrow{a}_{\rm a} \Longrightarrow F_2'$ to synchronize with the only one of $[1]F$ before performing a or the only one of $[1]F'$ after performing a.

As for probabilities, to avoid trivial cases let $F_1, F_2, F \in \mathbb{P}_{\rm p}$ and consider an equivalence class $C' = C \parallel_L F' = \{H \parallel_L F' \mid H \in C\}$ for some $C \in \mathbb{P}_{\rm pr}/\mathcal{B}$ with $F' \in \mathbb{P}_{\rm n}$. By virtue of Lemma 9.1 we obtain $prob(F_k \parallel_L F, C') = \sum_{H \parallel_L F' \in C'} prob(F_k \parallel_L F, H \parallel_L F') = \sum_{H \parallel_L F' \in C'} prob(F_k, H) \cdot prob(F, F') = \sum_{H \in C} prob(F_k, H) \cdot prob(F, F') = (\sum_{H \in C} prob(F_k, H)) \cdot prob(F, F') = prob(F_k, C) \cdot prob(F, F')$ for $k \in \{1, 2\}$. From $(F_1, F_2) \in \mathcal{B}$ it follows that $prob(F_1, C) = prob(F_2, C)$, hence $prob(F_1 \parallel_L F, C') = prob(F_2 \parallel_L F, C')$.

3. The equivalence relation $\mathcal{B}' = \mathcal{I}_{\mathbb{P}_{\rm pr}} \cup \{(F_1 \setminus L, F_2 \setminus L) \mid (F_1, F_2) \in \mathcal{B}\}$ is a weak probabilistic bisimulation too. Given $(F_1 \setminus L, F_2 \setminus L) \in \mathcal{B}'$ with $(F_1, F_2) \in \mathcal{B}$, there are two cases for action transitions based on the operational semantic rules in Table 9.1:

   - If $F_1 \setminus L \xrightarrow{\tau}_{\rm a} F_1' \setminus L$ with $F_1 \xrightarrow{\tau}_{\rm a} F_1'$, then there exists $F_2 \Longrightarrow F_2'$ such that $(F_1', F_2') \in \mathcal{B}$. Since the restriction operator does not apply to τ and probabilistic transitions, we have that $F_2 \setminus L \Longrightarrow F_2' \setminus L$ with $(F_1' \setminus L, F_2' \setminus L) \in \mathcal{B}'$.
   - If $F_1 \setminus L \xrightarrow{a}_{\rm a} F_1' \setminus L$ with $F_1 \xrightarrow{a}_{\rm a} F_1'$ and $a \notin L \cup \{\tau\}$, then there exists $F_2 \Longrightarrow \xrightarrow{a}_{\rm a} \Longrightarrow F_2'$ such that $(F_1', F_2') \in \mathcal{B}$. Since the restriction operator does not apply to τ and probabilistic transitions and $a \notin L$, we have that $F_2 \setminus L \Longrightarrow \xrightarrow{a}_{\rm a} \Longrightarrow F_2' \setminus L$ with $(F_1' \setminus L, F_2' \setminus L) \in \mathcal{B}'$.

   As for probabilities, to avoid trivial cases consider an equivalence class $C' = C \setminus L = \{F \setminus L \mid F \in C\}$ for some $C \in \mathbb{P}_{\rm pr}/\mathcal{B}$. From $(F_1, F_2) \in \mathcal{B}$ it follows that $prob(F_1, C) = prob(F_2, C)$. Since the restriction operator does not apply to probabilistic transitions, we have that $prob(F_1 \setminus L, C') = prob(F_1, C) = prob(F_2, C) = prob(F_2 \setminus L, C')$.

4. The equivalence relation $\mathcal{B}' = \mathcal{I}_{\mathbb{P}_{\rm pr}} \cup \{(F_1 / L, F_2 / L) \mid (F_1, F_2) \in \mathcal{B}\}$ is a weak probabilistic bisimulation too. Given $(F_1 / L, F_2 / L) \in \mathcal{B}'$ with $(F_1, F_2) \in \mathcal{B}$, there are two cases for action transitions based on the operational semantic rules in Table 9.1:

   - If $F_1 / L \xrightarrow{\tau}_{\rm a} F_1' / L$ with $F_1 \xrightarrow{\tau}_{\rm a} F_1'$, then there exists $F_2 \Longrightarrow F_2'$ such that $(F_1', F_2') \in \mathcal{B}$. Since the hiding operator does not apply to τ and probabilistic transitions, we have that $F_2 / L \Longrightarrow F_2' / L$ with $(F_1' / L, F_2' / L) \in \mathcal{B}'$.
   - If $F_1 / L \xrightarrow{a}_{\rm a} F_1' / L$ with $F_1 \xrightarrow{b}_{\rm a} F_1'$ and $b \in L \wedge a = \tau$ or $b \notin L \cup \{\tau\} \wedge a = b$, then there exists $F_2 \stackrel{\hat{b}}{\Longrightarrow} F_2'$ such that $(F_1', F_2') \in \mathcal{B}$. Since the hiding operator does not apply to τ and probabilistic transitions, we have that $F_2 / L \stackrel{\hat{a}}{\Longrightarrow} F_2' / L$ with $(F_1' / L, F_2' / L) \in \mathcal{B}'$.

   As for probabilities, to avoid trivial cases consider an equivalence class $C' = C / L = \{F / L \mid F \in C\}$ for some $C \in \mathbb{P}_{\rm pr}/\mathcal{B}$. From $(F_1, F_2) \in \mathcal{B}$ it follows that $prob(F_1, C) = prob(F_2, C)$. Since the hiding operator

does not apply to probabilistic transitions, we have that $prob(F_1 \,/\, L, C') = prob(F_1, C) = prob(F_2, C) = prob(F_2 \,/\, L, C')$.

We then prove the four results for the $\approx_{\rm pb}$-based properties. Let $\mathcal{B}$ be a probabilistic branching bisimulation witnessing $E_1 \approx_{\rm pb} E_2$. We show that the equivalence relations $\mathcal{B}'$ considered for the $\approx_{\rm pw}$-based properties are probabilistic branching bisimulations too:

1. The result immediately follows from the fact that, given $(a\,.\,F_1, a\,.\,F_2) \in \mathcal{B}'$ with $(F_1, F_2) \in \mathcal{B}$, $a\,.\,F_1 \stackrel{a}{\longrightarrow}_{\rm a} F_1$ is matched by $a\,.\,F_2 \Longrightarrow a\,.\,F_2 \stackrel{a}{\longrightarrow}_{\rm a} F_2$ with $(a\,.\,F_1, a\,.\,F_2) \in \mathcal{B}'$ and $(F_1, F_2) \in \mathcal{B}'$ as well as $prob(a\,.\,F_1, \bar{C}) = prob(a\,.\,F_2, \bar{C}) = 1$ for $\bar{C} = [a\,.\,F_1]_{\mathcal{B}'}$ while $prob(a\,.\,F_1, C') = prob(a\,.\,F_2, C') = 0$ for any other $C' \in \mathbb{P}_{\rm pr}/\mathcal{B}'$.

2. Given $(F_1 \parallel_L F, F_2 \parallel_L F) \in \mathcal{B}'$ with $(F_1, F_2) \in \mathcal{B}$, there are three cases for action transitions based on the operational semantic rules in Table 9.1:

   - If $F_1 \parallel_L F \stackrel{a}{\longrightarrow}_{\rm a} F_1' \parallel_L [1]F$ with $F_1 \stackrel{a}{\longrightarrow}_{\rm a} F_1'$ and $a \notin L$, then either $a = \tau$ and $(F_1', F_2) \in \mathcal{B}$, or there exists $F_2 \Longrightarrow \bar{F}_2 \stackrel{a}{\longrightarrow}_{\rm a} F_2'$ such that $(F_1, \bar{F}_2) \in \mathcal{B}$ and $(F_1', F_2') \in \mathcal{B}$. Note that the action transition from $F_1 \parallel_L F$ implies that $F_1 \parallel_L F \in \mathbb{P}_{\rm n}$, i.e., $F_1, F \in \mathbb{P}_{\rm n}$, hence $F_2 \parallel_L F \in \mathbb{P}_{\rm n}$ too. Since synchronization does not apply to τ and $a \notin L$, in the former subcase $F_2 \parallel_L F$ is allowed to stay idle with $(F_1' \parallel_L [1]F, F_2 \parallel_L F) \in \mathcal{B}'$, while in the latter subcase $F_2 \parallel_L F \Longrightarrow \bar{F}_2 \parallel_L F \stackrel{a}{\longrightarrow}_{\rm a} F_2' \parallel_L [1]F$ with $(F_1 \parallel_L F, \bar{F}_2 \parallel_L F) \in \mathcal{B}'$ and $(F_1' \parallel_L [1]F, F_2' \parallel_L [1]F) \in \mathcal{B}'$, in which subcase the right subprocess alternates between F and $[1]F$ before a is performed thus allowing the probabilistic transitions along $F_2 \Longrightarrow \bar{F}_2$ to synchronize with the only one of $[1]F$.
   - The case $F_1 \parallel_L F \stackrel{a}{\longrightarrow}_{\rm a} [1]F_1 \parallel_L F'$ with $F \stackrel{a}{\longrightarrow}_{\rm a} F'$ and $a \notin L$ is trivial.
   - If $F_1 \parallel_L F \stackrel{a}{\longrightarrow}_{\rm a} F_1' \parallel_L F'$ with $F_1 \stackrel{a}{\longrightarrow}_{\rm a} F_1'$, $F \stackrel{a}{\longrightarrow}_{\rm a} F'$, and $a \in L$, then there exists $F_2 \Longrightarrow \bar{F}_2 \stackrel{a}{\longrightarrow}_{\rm a} F_2'$ such that $(F_1, \bar{F}_2) \in \mathcal{B}$ and $(F_1', F_2') \in \mathcal{B}$. Since synchronization does not apply to τ and $a \in L$, we have that $F_2 \parallel_L F \Longrightarrow \bar{F}_2 \parallel_L F \stackrel{a}{\longrightarrow}_{\rm a} F_2' \parallel_L F'$ with $(F_1 \parallel_L F, \bar{F}_2 \parallel_L F) \in \mathcal{B}'$ and $(F_1' \parallel_L F', F_2' \parallel_L F') \in \mathcal{B}'$, where the right subprocess alternates between F and $[1]F$ before performing a thus allowing the probabilistic transitions along $F_2 \Longrightarrow \bar{F}_2$ to synchronize with the only one of $[1]F$.

   As for probabilities, we reason like in the proof of the corresponding result for $\approx_{\rm pw}$.

3. Given $(F_1 \setminus L, F_2 \setminus L) \in \mathcal{B}'$ with $(F_1, F_2) \in \mathcal{B}$, there are two cases for action transitions based on the operational semantic rules in Table 9.1:

   - If $F_1 \setminus L \stackrel{\tau}{\longrightarrow}_{\rm a} F_1' \setminus L$ with $F_1 \stackrel{\tau}{\longrightarrow}_{\rm a} F_1'$, then either $(F_1', F_2) \in \mathcal{B}$, or there exists $F_2 \Longrightarrow \bar{F}_2 \stackrel{\tau}{\longrightarrow}_{\rm a} F_2'$ such that $(F_1, \bar{F}_2) \in \mathcal{B}$ and $(F_1', F_2') \in \mathcal{B}$. Since the restriction operator does not apply to τ and probabilistic transitions, in the former subcase $F_2 \setminus L$ is allowed to stay idle with $(F_1' \setminus L, F_2 \setminus L) \in \mathcal{B}'$, while in the latter subcase $F_2 \setminus L \Longrightarrow \bar{F}_2 \setminus L \stackrel{\tau}{\longrightarrow}_{\rm a} F_2' \setminus L$ with $(F_1 \setminus L, \bar{F}_2 \setminus L) \in \mathcal{B}'$ and $(F_1' \setminus L, F_2' \setminus L) \in \mathcal{B}'$.
   - If $F_1 \setminus L \stackrel{a}{\longrightarrow}_{\rm a} F_1' \setminus L$ with $F_1 \stackrel{a}{\longrightarrow}_{\rm a} F_1'$ and $a \notin L \cup \{\tau\}$, then there exists $F_2 \Longrightarrow \bar{F}_2 \stackrel{a}{\longrightarrow}_{\rm a} F_2'$ such that $(F_1, \bar{F}_2) \in \mathcal{B}$ and $(F_1', F_2') \in \mathcal{B}$. Since the restriction operator does not apply to τ and probabilistic transitions and $a \notin L$, we have that $F_2 \setminus L \Longrightarrow \bar{F}_2 \setminus L \stackrel{a}{\longrightarrow}_{\rm a} F_2' \setminus L$ with $(F_1 \setminus L, \bar{F}_2 \setminus L) \in \mathcal{B}'$ and $(F_1' \setminus L, F_2' \setminus L) \in \mathcal{B}'$.

   As for probabilities, we reason like in the proof of the corresponding result for $\approx_{\rm pw}$.

4. Given $(F_1 \,/\, L, F_2 \,/\, L) \in \mathcal{B}'$ with $(F_1, F_2) \in \mathcal{B}$, there are two cases for action transitions based on the operational semantic rules in Table 9.1:

   - If $F_1 \,/\, L \xrightarrow{\tau}_{\mathrm{a}} F_1' \,/\, L$ with $F_1 \xrightarrow{\tau}_{\mathrm{a}} F_1'$, then either $(F_1', F_2) \in \mathcal{B}$, or there exists $F_2 \Longrightarrow \bar{F}_2 \xrightarrow{\tau}_{\mathrm{a}} F_2'$ such that $(F_1, \bar{F}_2) \in \mathcal{B}$ and $(F_1', F_2') \in \mathcal{B}$. Since the hiding operator does not apply to τ and probabilistic transitions, in the former subcase $F_2 \,/\, L$ is allowed to stay idle with $(F_1' \,/\, L, F_2 \,/\, L) \in \mathcal{B}'$, while in the latter subcase $F_2 \,/\, L \Longrightarrow \bar{F}_2 \,/\, L \xrightarrow{\tau}_{\mathrm{a}} F_2' \,/\, L$ with $(F_1 \,/\, L, \bar{F}_2 \,/\, L) \in \mathcal{B}'$ and $(F_1' \,/\, L, F_2' \,/\, L) \in \mathcal{B}'$.
   - If $F_1 \,/\, L \xrightarrow{a}_{\mathrm{a}} F_1' \,/\, L$ with $F_1 \xrightarrow{b}_{\mathrm{a}} F_1'$ and $b \in L \wedge a = \tau$ or $b \notin L \cup \{\tau\} \wedge a = b$, then there exists $F_2 \Longrightarrow \bar{F}_2 \xrightarrow{b}_{\mathrm{a}} F_2'$ such that $(F_1, \bar{F}_2) \in \mathcal{B}$ and $(F_1', F_2') \in \mathcal{B}$. Since the hiding operator does not apply to τ and probabilistic transitions, we have that $F_2 \,/\, L \Longrightarrow \bar{F}_2 \,/\, L \xrightarrow{a}_{\mathrm{a}} F_2' \,/\, L$ with $(F_1 \,/\, L, \bar{F}_2 \,/\, L) \in \mathcal{B}'$ and $(F_1' \,/\, L, F_2' \,/\, L) \in \mathcal{B}'$.

   As for probabilities, we reason like in the proof of the corresponding result for $\approx_{\mathrm{pw}}$. ∎

Theorem 9.1. *Let* $E_1, E_2 \in \mathbb{P}_{\mathrm{pr}}$, $\approx \in \{\approx_{\mathrm{pw}}, \approx_{\mathrm{pb}}\}$, *and* $\mathcal{P} \in \{\mathrm{BSNNI}_{\approx}, \mathrm{BNDC}_{\approx}, \mathrm{SBSNNI}_{\approx}, \mathrm{P\_BNDC}_{\approx}, \mathrm{SBNDC}_{\approx}\}$. *If* $E_1 \approx E_2$ *then* $E_1 \in \mathcal{P} \Longleftrightarrow E_2 \in \mathcal{P}$.

Proof. A straightforward consequence of the definition of the various properties, i.e., Definition 9.6, and Lemma 9.2. ∎

As far as modular verification is concerned, like in the nondeterministic setting of the previous chapter only the local properties $\mathrm{SBSNNI}_{\approx}$, $\mathrm{P\_BNDC}_{\approx}$, and $\mathrm{SBNDC}_{\approx}$ are compositional, i.e., are preserved by some operators of the calculus in certain circumstances. Moreover, similar to the previous chapter, compositionality with respect to parallel composition is limited, for $\mathrm{SBSNNI}_{\approx_{\mathrm{pb}}}$ and $\mathrm{P\_BNDC}_{\approx_{\mathrm{pb}}}$, to the case in which synchronizations can take place only among low-level actions, i.e., $L \subseteq \mathcal{A}_{\mathcal{L}}$. A limitation to low-level actions applies to action prefix and hiding as well, whilst this is not the case for restriction. Another analogy with the nondeterministic setting of the previous chapter is that none of the considered noninterference properties is compositional with respect to alternative composition, as can be noted by examining $E_1 + E_2$ where $E_1 = l\,.\,[1]\underline{0}$ and $E_2 = h\,.\,[1]\underline{0}$ (see after Theorem 8.2). Moreover, compositionality also fails for probabilistic composition, for which it is sufficient to consider $[p]E_1 \oplus [1-p]E_2$.

To establish compositionality, we first prove some ancillary results about parallel composition, restriction, and hiding under SBSNNI and SBNDC similar to those in the previous chapter.

Lemma 9.3. *Let* $E_1, E_2 \in \mathbb{P}_{\mathrm{n}}$ *or* $E_1, E_2 \in \mathbb{P}_{\mathrm{p}}$, $E \in \mathbb{P}_{\mathrm{pr}}$, *and* $\approx \in \{\approx_{\mathrm{pw}}, \approx_{\mathrm{pb}}\}$. *Then:*

1. *If* $E_1, E_2 \in \mathrm{SBSNNI}_{\approx}$ *and* $L \subseteq \mathcal{A} \setminus \{\tau\}$ *for* $\approx_{\mathrm{pw}}$ *or* $L \subseteq \mathcal{A}_{\mathcal{L}}$ *for* $\approx_{\mathrm{pb}}$, *then* $(F_1 \parallel_L F_2) \setminus \mathcal{A}_{\mathcal{H}} \approx (G_1 \parallel_L G_2) \,/\, \mathcal{A}_{\mathcal{H}}$ *for all* $F_1, G_1 \in \mathit{reach}(E_1)$ *and* $F_2, G_2 \in \mathit{reach}(E_2)$ *such that* $F_1 \parallel_L F_2, G_1 \parallel_L G_2 \in \mathit{reach}(E_1 \parallel_L E_2)$, $F_1 \setminus \mathcal{A}_{\mathcal{H}} \approx G_1 \,/\, \mathcal{A}_{\mathcal{H}}$, *and* $F_2 \setminus \mathcal{A}_{\mathcal{H}} \approx G_2 \,/\, \mathcal{A}_{\mathcal{H}}$.
2. *If* $E \in \mathrm{SBSNNI}_{\approx}$ *and* $L \subseteq \mathcal{A} \setminus \{\tau\}$, *then* $(F \,/\, \mathcal{A}_{\mathcal{H}}) \setminus L \approx (G \setminus L) \,/\, \mathcal{A}_{\mathcal{H}}$ *for all* $F, G \in \mathit{reach}(E)$ *such that* $F \,/\, \mathcal{A}_{\mathcal{H}} \approx G \setminus \mathcal{A}_{\mathcal{H}}$.
3. *If* $E_1, E_2 \in \mathrm{SBNDC}_{\approx}$ *and* $L \subseteq \mathcal{A} \setminus \{\tau\}$, *then* $(F_1 \parallel_L F_2) \setminus \mathcal{A}_{\mathcal{H}} \approx (G_1 \parallel_L G_2) \setminus \mathcal{A}_{\mathcal{H}}$ *for all* $F_1, G_1 \in \mathit{reach}(E_1)$ *and* $F_2, G_2 \in \mathit{reach}(E_2)$ *such that* $F_1 \parallel_L F_2, G_1 \parallel_L G_2 \in \mathit{reach}(E_1 \parallel_L E_2)$, $F_1 \setminus \mathcal{A}_{\mathcal{H}} \approx G_1 \setminus \mathcal{A}_{\mathcal{H}}$ *and* $F_2 \setminus \mathcal{A}_{\mathcal{H}} \approx G_2 \setminus \mathcal{A}_{\mathcal{H}}$.

Proof. We first prove the three results for the $\approx_{\rm pw}$-based properties. Let $\mathcal{B}$ be an equivalence relation containing all the pairs of processes that have to be shown to be $\approx_{\rm pw}$-equivalent according to the considered result:

1. Starting from $(F_1 \parallel_L F_2)\backslash\mathcal{A}_\mathcal{H}$ and $(G_1 \parallel_L G_2) / \mathcal{A}_\mathcal{H}$ related by $\mathcal{B}$, so that $F_1\backslash\mathcal{A}_\mathcal{H} \approx_{\rm pw} G_1 / \mathcal{A}_\mathcal{H}$ and $F_2\backslash\mathcal{A}_\mathcal{H} \approx_{\rm pw} G_2 / \mathcal{A}_\mathcal{H}$, there are thirteen cases for action transitions based on the operational semantic rules in Table 9.1. In the first five cases, it is $(F_1 \parallel_L F_2) \setminus \mathcal{A}_\mathcal{H}$ to move first:

   - If $(F_1 \parallel_L F_2) \setminus \mathcal{A}_\mathcal{H} \xrightarrow{l}_{\rm a} (F_1' \parallel_L [1]F_2) \setminus \mathcal{A}_\mathcal{H}$ with $F_1 \xrightarrow{l}_{\rm a} F_1'$ and $l \notin L$, then $F_1 \setminus \mathcal{A}_\mathcal{H} \xrightarrow{l}_{\rm a} F_1' \setminus \mathcal{A}_\mathcal{H}$ as $l \notin \mathcal{A}_\mathcal{H}$. From $F_1 \setminus \mathcal{A}_\mathcal{H} \approx_{\rm pw} G_1 / \mathcal{A}_\mathcal{H}$ it follows that there exists $G_1 / \mathcal{A}_\mathcal{H} \Longrightarrow \xrightarrow{l}_{\rm a} \Longrightarrow G_1' / \mathcal{A}_\mathcal{H}$ such that $F_1' \setminus \mathcal{A}_\mathcal{H} \approx_{\rm pw} G_1' / \mathcal{A}_\mathcal{H}$. Since synchronization does not apply to τ and $l \notin L$, we have that $(G_1 \parallel_L G_2) / \mathcal{A}_\mathcal{H} \Longrightarrow \xrightarrow{l}_{\rm a} \Longrightarrow (G_1' \parallel_L [1]G_2) / \mathcal{A}_\mathcal{H}$ with $((F_1' \parallel_L [1]F_2) \setminus \mathcal{A}_\mathcal{H}, (G_1' \parallel_L [1]G_2) / \mathcal{A}_\mathcal{H}) \in \mathcal{B}$, where the right subprocess alternates between G_2 and $[1]G_2$ thus allowing the probabilistic transitions along $G_1 / \mathcal{A}_\mathcal{H} \Longrightarrow \xrightarrow{l}_{\rm a} \Longrightarrow G_1' / \mathcal{A}_\mathcal{H}$ to synchronize with the only one of $[1]G_2$.
   - If $(F_1 \parallel_L F_2) \setminus \mathcal{A}_\mathcal{H} \xrightarrow{l}_{\rm a} ([1]F_1 \parallel_L F_2') \setminus \mathcal{A}_\mathcal{H}$ with $F_2 \xrightarrow{l}_{\rm a} F_2'$ and $l \notin L$, then the proof is similar to the one of the previous case.
   - If $(F_1 \parallel_L F_2)\setminus\mathcal{A}_\mathcal{H} \xrightarrow{l}_{\rm a} (F_1' \parallel_L F_2')\setminus\mathcal{A}_\mathcal{H}$ with $F_i \xrightarrow{l}_{\rm a} F_i'$ for $i \in \{1,2\}$ and $l \in L$, then $F_i\setminus\mathcal{A}_\mathcal{H} \xrightarrow{l}_{\rm a} F_i'\setminus\mathcal{A}_\mathcal{H}$ as $l \notin \mathcal{A}_\mathcal{H}$. From $F_i \setminus \mathcal{A}_\mathcal{H} \approx_{\rm pw} G_i / \mathcal{A}_\mathcal{H}$ it follows that there exists $G_i / \mathcal{A}_\mathcal{H} \Longrightarrow \xrightarrow{l}_{\rm a} \Longrightarrow G_i' / \mathcal{A}_\mathcal{H}$ such that $F_i' \setminus \mathcal{A}_\mathcal{H} \approx_{\rm pw} G_i' / \mathcal{A}_\mathcal{H}$. Since synchronization does not apply to τ and $l \in L$, we have that $(G_1 \parallel_L G_2) / \mathcal{A}_\mathcal{H} \Longrightarrow \xrightarrow{l}_{\rm a} \Longrightarrow (G_1' \parallel_L G_2') / \mathcal{A}_\mathcal{H}$ with $((F_1' \parallel_L F_2') \setminus \mathcal{A}_\mathcal{H}, (G_1' \parallel_L G_2') / \mathcal{A}_\mathcal{H}) \in \mathcal{B}$, where subprocess i alternates between G_i and $[1]G_i$ before performing l or between G_i' and $[1]G_i'$ after performing l thus allowing the probabilistic transitions along $G_j / \mathcal{A}_\mathcal{H} \Longrightarrow \xrightarrow{l}_{\rm a} \Longrightarrow G_j' / \mathcal{A}_\mathcal{H}$ for $j \neq i$ to synchronize with the only one of $[1]G_i$ before performing a or the only one of $[1]G_i'$ after performing a.
   - If $(F_1 \parallel_L F_2) \setminus \mathcal{A}_\mathcal{H} \xrightarrow{\tau}_{\rm a} (F_1' \parallel_L [1]F_2) \setminus \mathcal{A}_\mathcal{H}$ with $F_1 \xrightarrow{\tau}_{\rm a} F_1'$, then $F_1 \setminus \mathcal{A}_\mathcal{H} \xrightarrow{\tau}_{\rm a} F_1' \setminus \mathcal{A}_\mathcal{H}$ as $\tau \notin \mathcal{A}_\mathcal{H}$. From $F_1 \setminus \mathcal{A}_\mathcal{H} \approx_{\rm pw} G_1 / \mathcal{A}_\mathcal{H}$ it follows that there exists $G_1 / \mathcal{A}_\mathcal{H} \Longrightarrow G_1' / \mathcal{A}_\mathcal{H}$ such that $F_1' \setminus \mathcal{A}_\mathcal{H} \approx_{\rm pw} G_1' / \mathcal{A}_\mathcal{H}$. Since synchronization does not apply to τ, we have that $(G_1 \parallel_L G_2) / \mathcal{A}_\mathcal{H} \Longrightarrow (G_1' \parallel_L [1]G_2) / \mathcal{A}_\mathcal{H}$ with $((F_1' \parallel_L [1]F_2) \setminus \mathcal{A}_\mathcal{H}, (G_1' \parallel_L [1]G_2) / \mathcal{A}_\mathcal{H}) \in \mathcal{B}$, where the right subprocess alternates between G_2 and $[1]G_2$ thus allowing the probabilistic transitions along $G_1 / \mathcal{A}_\mathcal{H} \Longrightarrow G_1' / \mathcal{A}_\mathcal{H}$ to synchronize with the only one of $[1]G_2$.
   - If $(F_1 \parallel_L F_2) \setminus \mathcal{A}_\mathcal{H} \xrightarrow{\tau}_{\rm a} ([1]F_1 \parallel_L F_2') \setminus \mathcal{A}_\mathcal{H}$ with $F_2 \xrightarrow{\tau}_{\rm a} F_2'$, then the proof is similar to the one of the previous case.

   In the other eight cases, instead, it is $(G_1 \parallel_L G_2) / \mathcal{A}_\mathcal{H}$ to move first:

   - If $(G_1 \parallel_L G_2) / \mathcal{A}_\mathcal{H} \xrightarrow{l}_{\rm a} (G_1' \parallel_L [1]G_2) / \mathcal{A}_\mathcal{H}$ with $G_1 \xrightarrow{l}_{\rm a} G_1'$ and $l \notin L$, then $G_1 / \mathcal{A}_\mathcal{H} \xrightarrow{l}_{\rm a} G_1' / \mathcal{A}_\mathcal{H}$ as $l \notin \mathcal{A}_\mathcal{H}$. From $G_1 / \mathcal{A}_\mathcal{H} \approx_{\rm pw} F_1 \setminus \mathcal{A}_\mathcal{H}$ it follows that there exists $F_1 \setminus \mathcal{A}_\mathcal{H} \Longrightarrow \xrightarrow{l}_{\rm a} \Longrightarrow F_1' \setminus \mathcal{A}_\mathcal{H}$ such that $G_1' / \mathcal{A}_\mathcal{H} \approx_{\rm pw} F_1' \setminus \mathcal{A}_\mathcal{H}$. Since synchronization does not apply to τ and $l \notin L$, we have that $(F_1 \parallel_L F_2) \setminus \mathcal{A}_\mathcal{H} \Longrightarrow \xrightarrow{l}_{\rm a} \Longrightarrow (F_1' \parallel_L [1]F_2) \setminus \mathcal{A}_\mathcal{H}$ with $((G_1' \parallel_L [1]G_2)/\mathcal{A}_\mathcal{H}, (F_1' \parallel_L [1]F_2) \setminus \mathcal{A}_\mathcal{H}) \in \mathcal{B}$, where the right subprocess alternates between F_2 and $[1]F_2$ thus allowing the probabilistic transitions along $F_1 \setminus \mathcal{A}_\mathcal{H} \Longrightarrow \xrightarrow{l}_{\rm a} \Longrightarrow F_1' \setminus \mathcal{A}_\mathcal{H}$ to synchronize with the only one of $[1]F_2$.

- If $(G_1 \parallel_L G_2) / \mathcal{A}_\mathcal{H} \xrightarrow{l}_\mathrm{a} ([1]G_1 \parallel_L G_2') / \mathcal{A}_\mathcal{H}$ with $G_2 \xrightarrow{l}_\mathrm{a} G_2'$ and $l \notin L$, then the proof is similar to the one of the previous case.
- If $(G_1 \parallel_L G_2) / \mathcal{A}_\mathcal{H} \xrightarrow{l}_\mathrm{a} (G_1' \parallel_L G_2') / \mathcal{A}_\mathcal{H}$ with $G_i \xrightarrow{l}_\mathrm{a} G_i'$ for $i \in \{1,2\}$ and $l \in L$, then $G_i / \mathcal{A}_\mathcal{H} \xrightarrow{l}_\mathrm{a} G_i' / \mathcal{A}_\mathcal{H}$ as $l \notin \mathcal{A}_\mathcal{H}$. From $G_i / \mathcal{A}_\mathcal{H} \approx_\mathrm{pw} F_i \setminus \mathcal{A}_\mathcal{H}$ it follows that there exists $F_i \setminus \mathcal{A}_\mathcal{H} \Longrightarrow \xrightarrow{l}_\mathrm{a} \Longrightarrow F_i' \setminus \mathcal{A}_\mathcal{H}$ such that $G_i' / \mathcal{A}_\mathcal{H} \approx_\mathrm{pw} F_i' \setminus \mathcal{A}_\mathcal{H}$. Since synchronization does not apply to τ and $l \in L$, we have that $(F_1 \parallel_L F_2) \setminus \mathcal{A}_\mathcal{H} \Longrightarrow \xrightarrow{l}_\mathrm{a} \Longrightarrow (F_1' \parallel_L F_2') \setminus \mathcal{A}_\mathcal{H}$ with $((G_1' \parallel_L G_2')/\mathcal{A}_\mathcal{H}, (F_1' \parallel_L F_2') \setminus \mathcal{A}_\mathcal{H}) \in \mathcal{B}$, where subprocess i alternates between F_i and $[1]F_i$ before performing l or between F_i' and $[1]F_i'$ after performing l thus allowing the probabilistic transitions along $F_j \setminus \mathcal{A}_\mathcal{H} \Longrightarrow \xrightarrow{l}_\mathrm{a} \Longrightarrow F_j' \setminus \mathcal{A}_\mathcal{H}$ for $j \neq i$ to synchronize with the only one of $[1]F_i$ before performing a or the only one of $[1]F_i'$ after performing a.
- If $(G_1 \parallel_L G_2) / \mathcal{A}_\mathcal{H} \xrightarrow{\tau}_\mathrm{a} (G_1' \parallel_L [1]G_2) / \mathcal{A}_\mathcal{H}$ with $G_1 \xrightarrow{\tau}_\mathrm{a} G_1'$, then $G_1 / \mathcal{A}_\mathcal{H} \xrightarrow{\tau}_\mathrm{a} G_1' / \mathcal{A}_\mathcal{H}$ as $\tau \notin \mathcal{A}_\mathcal{H}$. From $G_1 / \mathcal{A}_\mathcal{H} \approx_\mathrm{pw} F_1 \setminus \mathcal{A}_\mathcal{H}$ it follows that there exists $F_1 \setminus \mathcal{A}_\mathcal{H} \Longrightarrow F_1' \setminus \mathcal{A}_\mathcal{H}$ such that $G_1' / \mathcal{A}_\mathcal{H} \approx_\mathrm{pw} F_1' \setminus \mathcal{A}_\mathcal{H}$. Since synchronization does not apply to τ, we have that $(F_1 \parallel_L F_2) \setminus \mathcal{A}_\mathcal{H} \Longrightarrow (F_1' \parallel_L [1]F_2) \setminus \mathcal{A}_\mathcal{H}$ with $((G_1' \parallel_L [1]G_2)/\mathcal{A}_\mathcal{H}, (F_1' \parallel_L [1]F_2) \setminus \mathcal{A}_\mathcal{H}) \in \mathcal{B}$, where the right subprocess alternates between F_2 and $[1]F_2$ thus allowing the probabilistic transitions along $F_1 \setminus \mathcal{A}_\mathcal{H} \Longrightarrow F_1' \setminus \mathcal{A}_\mathcal{H}$ to synchronize with the only one of $[1]F_2$.
- If $(G_1 \parallel_L G_2) / \mathcal{A}_\mathcal{H} \xrightarrow{\tau}_\mathrm{a} (G_1 \parallel_L G_2') / \mathcal{A}_\mathcal{H}$ with $G_2 \xrightarrow{\tau}_\mathrm{a} G_2'$, then the proof is similar to the one of the previous case.
- If $(G_1 \parallel_L G_2) / \mathcal{A}_\mathcal{H} \xrightarrow{\tau}_\mathrm{a} (G_1' \parallel_L [1]G_2) / \mathcal{A}_\mathcal{H}$ with $G_1 \xrightarrow{h}_\mathrm{a} G_1'$ and $h \notin L$, then $G_1 / \mathcal{A}_\mathcal{H} \xrightarrow{\tau}_\mathrm{a} G_1' / \mathcal{A}_\mathcal{H}$ as $h \in \mathcal{A}_\mathcal{H}$. The rest of the proof is like the one of the fourth case.
- If $(G_1 \parallel_L G_2) / \mathcal{A}_\mathcal{H} \xrightarrow{\tau}_\mathrm{a} ([1]G_1 \parallel_L G_2') / \mathcal{A}_\mathcal{H}$ with $G_2 \xrightarrow{h}_\mathrm{a} G_2'$ and $h \notin L$, then the proof is similar to the one of the previous case.
- If $(G_1 \parallel_L G_2) / \mathcal{A}_\mathcal{H} \xrightarrow{\tau}_\mathrm{a} (G_1' \parallel_L G_2') / \mathcal{A}_\mathcal{H}$ with $G_i \xrightarrow{h}_\mathrm{a} G_i'$ for $i \in \{1,2\}$ and $h \in L$, then $G_i / \mathcal{A}_\mathcal{H} \xrightarrow{\tau}_\mathrm{a} G_i' / \mathcal{A}_\mathcal{H}$ as $h \in \mathcal{A}_\mathcal{H}$. From $G_i / \mathcal{A}_\mathcal{H} \approx_\mathrm{pw} F_i \setminus \mathcal{A}_\mathcal{H}$ it follows that there exists $F_i \setminus \mathcal{A}_\mathcal{H} \Longrightarrow F_i' \setminus \mathcal{A}_\mathcal{H}$ such that $G_i' / \mathcal{A}_\mathcal{H} \approx_\mathrm{pw} F_i' \setminus \mathcal{A}_\mathcal{H}$. Since synchronization does not apply to τ and $h \in L$, we have that $(F_1 \parallel_L F_2) \setminus \mathcal{A}_\mathcal{H} \Longrightarrow (F_1' \parallel_L F_2') \setminus \mathcal{A}_\mathcal{H}$ with $((G_1' \parallel_L G_2') / \mathcal{A}_\mathcal{H}, (F_1' \parallel_L F_2') \setminus \mathcal{A}_\mathcal{H}) \in \mathcal{B}$, where subprocess i alternates between F_i and $[1]F_i$ thus allowing the probabilistic transitions along $F_j \setminus \mathcal{A}_\mathcal{H} \Longrightarrow F_j' \setminus \mathcal{A}_\mathcal{H}$ for $j \neq i$ to synchronize with the only one of $[1]F_i$.

As for probabilities, to avoid trivial cases let $F_1, F_2, G_1, G_2 \in \mathbb{P}_\mathrm{p}$ and consider an equivalence class $C \in \mathbb{P}_\mathrm{pr}/\mathcal{B}$ that involves nondeterministic processes reachable from $E_1 \parallel_L E_2$, specifically $C = \{(H_{1,i} \parallel_L H_{2,i}) \setminus \mathcal{A}_\mathcal{H}, (H_{1,j} \parallel_L H_{2,j}) / \mathcal{A}_\mathcal{H} \mid H_{k,h} \in \mathit{reach}(E_k) \wedge H_{1,h} \parallel_L H_{2,h} \in \mathit{reach}(E_1 \parallel_L E_2) \wedge H_{k,i} \setminus \mathcal{A}_\mathcal{H} \approx_\mathrm{pw} H_{k,j} / \mathcal{A}_\mathcal{H}\}$. Since the restriction and hiding operators do not apply to probabilistic transitions, we have that:

$$\begin{aligned} \mathit{prob}((F_1 \parallel_L F_2) \setminus \mathcal{A}_\mathcal{H}, C) &= \mathit{prob}((F_1 \setminus \mathcal{A}_\mathcal{H}) \parallel_L (F_2 \setminus \mathcal{A}_\mathcal{H}), C) \\ \mathit{prob}((G_1 \parallel_L G_2) / \mathcal{A}_\mathcal{H}, C) &= \mathit{prob}((G_1 / \mathcal{A}_\mathcal{H}) \parallel_L (G_2 / \mathcal{A}_\mathcal{H}), C) \end{aligned}$$

and hence by virtue of Lemma 9.1:

$$\begin{aligned} \mathit{prob}((F_1 \setminus \mathcal{A}_\mathcal{H}) \parallel_L (F_2 \setminus \mathcal{A}_\mathcal{H}), C) &= \mathit{prob}(F_1 \setminus \mathcal{A}_\mathcal{H}, C_1) \cdot \mathit{prob}(F_2 \setminus \mathcal{A}_\mathcal{H}, C_2) \\ \mathit{prob}((G_1 / \mathcal{A}_\mathcal{H}) \parallel_L (G_2 / \mathcal{A}_\mathcal{H}), C) &= \mathit{prob}(G_1 / \mathcal{A}_\mathcal{H}, C_1) \cdot \mathit{prob}(G_2 / \mathcal{A}_\mathcal{H}, C_2) \end{aligned}$$

where:

$$\begin{aligned} C_1 &= \{H_{1,h} \setminus \mathcal{A}_\mathcal{H} \mid (H_{1,h} \parallel_L H_{2,h}) \setminus \mathcal{A}_\mathcal{H} \in C\} \cup \{H_{1,h} / \mathcal{A}_\mathcal{H} \mid (H_{1,h} \parallel_L H_{2,h}) / \mathcal{A}_\mathcal{H} \in C\} \\ C_2 &= \{H_{2,h} \setminus \mathcal{A}_\mathcal{H} \mid (H_{1,h} \parallel_L H_{2,h}) \setminus \mathcal{A}_\mathcal{H} \in C\} \cup \{H_{2,h} / \mathcal{A}_\mathcal{H} \mid (H_{1,h} \parallel_L H_{2,h}) / \mathcal{A}_\mathcal{H} \in C\} \end{aligned}$$

Since $F_k \setminus \mathcal{A}_\mathcal{H} \approx_\mathrm{pw} G_k / \mathcal{A}_\mathcal{H}$ and C_k is the union of some $\approx_\mathrm{pw}$-equivalence classes for $k \in \{1,2\}$, we have

that:

$$\begin{array}{rcl} prob(F_1 \setminus \mathcal{A}_\mathcal{H}, C_1) & = & prob(G_1 \,/\, \mathcal{A}_\mathcal{H}, C_1) \\ prob(F_2 \setminus \mathcal{A}_\mathcal{H}, C_2) & = & prob(G_2 \,/\, \mathcal{A}_\mathcal{H}, C_2) \end{array}$$

2. Starting from $(F \,/\, \mathcal{A}_\mathcal{H}) \setminus L$ and $(G \setminus L) \,/\, \mathcal{A}_\mathcal{H}$ related by $\mathcal{B}$, so that $F \,/\, \mathcal{A}_\mathcal{H} \approx_{\rm pw} G \setminus \mathcal{A}_\mathcal{H}$, there are six cases for action transitions based on the operational semantic rules in Table 9.1. In the first three cases, it is $(F \,/\, \mathcal{A}_\mathcal{H}) \setminus L$ to move first:

   - If $(F \,/\, \mathcal{A}_\mathcal{H}) \setminus L \stackrel{l}{\longrightarrow}_{\rm a} (F' \,/\, \mathcal{A}_\mathcal{H}) \setminus L$ with $F \stackrel{l}{\longrightarrow}_{\rm a} F'$ and $l \notin L$, then $F \,/\, \mathcal{A}_\mathcal{H} \stackrel{l}{\longrightarrow}_{\rm a} F' \,/\, \mathcal{A}_\mathcal{H}$ as $l \notin \mathcal{A}_\mathcal{H}$. From $F \,/\, \mathcal{A}_\mathcal{H} \approx_{\rm pw} G \setminus \mathcal{A}_\mathcal{H}$ it follows that there exists $G \setminus \mathcal{A}_\mathcal{H} \Longrightarrow \stackrel{l}{\longrightarrow}_{\rm a} \Longrightarrow G' \setminus \mathcal{A}_\mathcal{H}$ such that $F' \,/\, \mathcal{A}_\mathcal{H} \approx_{\rm pw} G' \setminus \mathcal{A}_\mathcal{H}$. Since the restriction and hiding operators do not apply to τ, l, and probabilistic transitions, we have that $(G \setminus L) \,/\, \mathcal{A}_\mathcal{H} \Longrightarrow \stackrel{l}{\longrightarrow}_{\rm a} \Longrightarrow (G' \setminus L) \,/\, \mathcal{A}_\mathcal{H}$ with $((F' \,/\, \mathcal{A}_\mathcal{H}) \setminus L, (G' \setminus L) \,/\, \mathcal{A}_\mathcal{H}) \in \mathcal{B}$.
   - If $(F \,/\, \mathcal{A}_\mathcal{H}) \setminus L \stackrel{\tau}{\longrightarrow}_{\rm a} (F' \,/\, \mathcal{A}_\mathcal{H}) \setminus L$ with $F \stackrel{\tau}{\longrightarrow}_{\rm a} F'$, then $F \,/\, \mathcal{A}_\mathcal{H} \stackrel{\tau}{\longrightarrow}_{\rm a} F' \,/\, \mathcal{A}_\mathcal{H}$ as $\tau \notin \mathcal{A}_\mathcal{H}$. From $F \,/\, \mathcal{A}_\mathcal{H} \approx_{\rm pw} G \setminus \mathcal{A}_\mathcal{H}$ it follows that there exists $G \setminus \mathcal{A}_\mathcal{H} \Longrightarrow G' \setminus \mathcal{A}_\mathcal{H}$ such that $F' \,/\, \mathcal{A}_\mathcal{H} \approx_{\rm pw} G' \setminus \mathcal{A}_\mathcal{H}$. Since the restriction and hiding operators do not apply to τ and probabilistic transitions, we have that $(G \setminus L) \,/\, \mathcal{A}_\mathcal{H} \Longrightarrow (G' \setminus L) \,/\, \mathcal{A}_\mathcal{H}$ with $((F' \,/\, \mathcal{A}_\mathcal{H}) \setminus L, (G' \setminus L) \,/\, \mathcal{A}_\mathcal{H}) \in \mathcal{B}$.
   - If $(F \,/\, \mathcal{A}_\mathcal{H}) \setminus L \stackrel{\tau}{\longrightarrow}_{\rm a} (F' \,/\, \mathcal{A}_\mathcal{H}) \setminus L$ with $F \stackrel{h}{\longrightarrow}_{\rm a} F'$, then $F \,/\, \mathcal{A}_\mathcal{H} \stackrel{\tau}{\longrightarrow}_{\rm a} F' \,/\, \mathcal{A}_\mathcal{H}$ as $h \in \mathcal{A}_\mathcal{H}$. The rest of the proof is like the one of the previous case.

   In the other three cases, instead, it is $(G \setminus L) \,/\, \mathcal{A}_\mathcal{H}$ to move first:

   - If $(G \setminus L) \,/\, \mathcal{A}_\mathcal{H} \stackrel{l}{\longrightarrow}_{\rm a} (G' \setminus L) \,/\, \mathcal{A}_\mathcal{H}$ with $G \stackrel{l}{\longrightarrow}_{\rm a} G'$ and $l \notin L$, then $G \setminus \mathcal{A}_\mathcal{H} \stackrel{l}{\longrightarrow}_{\rm a} G' \setminus \mathcal{A}_\mathcal{H}$ as $l \notin \mathcal{A}_\mathcal{H}$. From $G \setminus \mathcal{A}_\mathcal{H} \approx_{\rm pw} F \,/\, \mathcal{A}_\mathcal{H}$ it follows that there exists $F \,/\, \mathcal{A}_\mathcal{H} \Longrightarrow \stackrel{l}{\longrightarrow}_{\rm a} \Longrightarrow F' \,/\, \mathcal{A}_\mathcal{H}$ such that $G' \setminus \mathcal{A}_\mathcal{H} \approx_{\rm pw} F' \,/\, \mathcal{A}_\mathcal{H}$. Since the restriction operator does not apply to τ, l, and probabilistic transitions, we have that $(F \,/\, \mathcal{A}_\mathcal{H}) \setminus L \Longrightarrow \stackrel{l}{\longrightarrow}_{\rm a} \Longrightarrow (F' \,/\, \mathcal{A}_\mathcal{H}) \setminus L$ with $((G' \setminus L) \,/\, \mathcal{A}_\mathcal{H}, (F' \,/\, \mathcal{A}_\mathcal{H}) \setminus L) \in \mathcal{B}$.
   - If $(G \setminus L) \,/\, \mathcal{A}_\mathcal{H} \stackrel{\tau}{\longrightarrow}_{\rm a} (G' \setminus L) \,/\, \mathcal{A}_\mathcal{H}$ with $G \stackrel{\tau}{\longrightarrow}_{\rm a} G'$, then $G \setminus \mathcal{A}_\mathcal{H} \stackrel{\tau}{\longrightarrow}_{\rm a} G' \setminus \mathcal{A}_\mathcal{H}$ as $\tau \notin \mathcal{A}_\mathcal{H}$. From $G \setminus \mathcal{A}_\mathcal{H} \approx_{\rm pw} F \,/\, \mathcal{A}_\mathcal{H}$ it follows that there exists $F \,/\, \mathcal{A}_\mathcal{H} \Longrightarrow F' \,/\, \mathcal{A}_\mathcal{H}$ such that $G' \setminus \mathcal{A}_\mathcal{H} \approx_{\rm pw} F' \,/\, \mathcal{A}_\mathcal{H}$. Since the restriction operator does not apply to τ and probabilistic transitions, we have that $(F \,/\, \mathcal{A}_\mathcal{H}) \setminus L \Longrightarrow (F' \,/\, \mathcal{A}_\mathcal{H}) \setminus L$ with $((G' \setminus L) \,/\, \mathcal{A}_\mathcal{H}, (F' \,/\, \mathcal{A}_\mathcal{H}) \setminus L) \in \mathcal{B}$.
   - If $(G \setminus L) \,/\, \mathcal{A}_\mathcal{H} \stackrel{\tau}{\longrightarrow}_{\rm a} (G' \setminus L) \,/\, \mathcal{A}_\mathcal{H}$ with $G \stackrel{h}{\longrightarrow}_{\rm a} G'$ and $h \notin L$, then $G \,/\, \mathcal{A}_\mathcal{H} \stackrel{\tau}{\longrightarrow}_{\rm a} G' \,/\, \mathcal{A}_\mathcal{H}$ as $h \in \mathcal{A}_\mathcal{H}$ (note that $G \setminus \mathcal{A}_\mathcal{H}$ cannot perform h). From $G \,/\, \mathcal{A}_\mathcal{H} \approx_{\rm pw} G \setminus \mathcal{A}_\mathcal{H}$ – as $E \in {\rm SBSNNI}_{\approx_{\rm pw}}$ and $G \in \mathit{reach}(E)$ – and $G \setminus \mathcal{A}_\mathcal{H} \approx_{\rm pw} F \,/\, \mathcal{A}_\mathcal{H}$ it follows that there exists $F \,/\, \mathcal{A}_\mathcal{H} \Longrightarrow F' \,/\, \mathcal{A}_\mathcal{H}$ such that $G' \,/\, \mathcal{A}_\mathcal{H} \approx_{\rm pw} F' \,/\, \mathcal{A}_\mathcal{H}$ and hence $G' \setminus \mathcal{A}_\mathcal{H} \approx_{\rm pw} F' \,/\, \mathcal{A}_\mathcal{H}$ – as $G' \,/\, \mathcal{A}_\mathcal{H} \approx_{\rm pw} G' \setminus \mathcal{A}_\mathcal{H}$ due to $E \in {\rm SBSNNI}_{\approx_{\rm pw}}$ and $G' \in \mathit{reach}(E)$. Since the restriction operator does not apply to τ and probabilistic transitions, we have that $(F \,/\, \mathcal{A}_\mathcal{H}) \setminus L \Longrightarrow (F' \,/\, \mathcal{A}_\mathcal{H}) \setminus L$ with $((G' \setminus L) \,/\, \mathcal{A}_\mathcal{H}, (F' \,/\, \mathcal{A}_\mathcal{H}) \setminus L) \in \mathcal{B}$.

   As for probabilities, to avoid trivial cases let $F, G \in \mathbb{P}_{\rm p}$ and consider an equivalence class $C \in \mathbb{P}_{\rm pr}/\mathcal{B}$ that involves nondeterministic processes reachable from E, specifically $C = \{(H_i \,/\, \mathcal{A}_\mathcal{H}) \setminus L, (H_j \setminus L) \,/\, \mathcal{A}_\mathcal{H} \mid H_h \in \mathit{reach}(E) \wedge H_i \setminus \mathcal{A}_\mathcal{H} \approx_{\rm pw} H_j \,/\, \mathcal{A}_\mathcal{H}\}$. Since the restriction and hiding operators do not apply to probabilistic transitions, we have that:

$$\begin{array}{rcl} prob((F \,/\, \mathcal{A}_\mathcal{H}) \setminus L, C) & = & prob(F \setminus \mathcal{A}_\mathcal{H}, \bar{C}) \\ prob((G \setminus L) \,/\, \mathcal{A}_\mathcal{H}, C) & = & prob(G \,/\, \mathcal{A}_\mathcal{H}, \bar{C}) \end{array}$$

where:

$$\bar{C} \;=\; \{H_i \setminus \mathcal{A}_\mathcal{H} \mid (H_i \,/\, \mathcal{A}_\mathcal{H}) \setminus L \in C\} \cup \{H_j \,/\, \mathcal{A}_\mathcal{H} \mid (H_j \setminus L) \,/\, \mathcal{A}_\mathcal{H} \in C\}$$

Since $F \setminus \mathcal{A}_\mathcal{H} \approx_{\rm pw} G \,/\, \mathcal{A}_\mathcal{H}$ and $\bar{C}$ is the union of some $\approx_{\rm pw}$-equivalence classes, we have that:

$$prob(F \setminus \mathcal{A}_\mathcal{H}, \bar{C}) \;=\; prob(G \,/\, \mathcal{A}_\mathcal{H}, \bar{C})$$

3. Starting from $(F_1 \parallel_L F_2) \setminus \mathcal{A}_\mathcal{H}$ and $(G_1 \parallel_L G_2) \setminus \mathcal{A}_\mathcal{H}$ related by $\mathcal{B}$, so that $F_1 \setminus \mathcal{A}_\mathcal{H} \approx_{\rm pw} G_1 \setminus \mathcal{A}_\mathcal{H}$ and $F_2 \setminus \mathcal{A}_\mathcal{H} \approx_{\rm pw} G_2 \setminus \mathcal{A}_\mathcal{H}$, there are five cases for action transitions based on the operational semantic rules in Table 9.1:

   - If $(F_1 \parallel_L F_2) \setminus \mathcal{A}_\mathcal{H} \xrightarrow{l}_{\rm a} (F_1' \parallel_L [1]F_2) \setminus \mathcal{A}_\mathcal{H}$ with $F_1 \xrightarrow{l}_{\rm a} F_1'$ and $l \notin L$, then $F_1 \setminus \mathcal{A}_\mathcal{H} \xrightarrow{l}_{\rm a} F_1' \setminus \mathcal{A}_\mathcal{H}$ as $l \notin \mathcal{A}_\mathcal{H}$. From $F_1 \setminus \mathcal{A}_\mathcal{H} \approx_{\rm pw} G_1 \setminus \mathcal{A}_\mathcal{H}$ it follows that there exists $G_1 \setminus \mathcal{A}_\mathcal{H} \Longrightarrow \xrightarrow{l}_{\rm a} \Longrightarrow G_1' \setminus \mathcal{A}_\mathcal{H}$ such that $F_1' \setminus \mathcal{A}_\mathcal{H} \approx_{\rm pw} G_1' \setminus \mathcal{A}_\mathcal{H}$. Since synchronization does not apply to τ and $l \notin L$, we have that $(G_1 \parallel_L G_2) \setminus \mathcal{A}_\mathcal{H} \Longrightarrow \xrightarrow{l}_{\rm a} \Longrightarrow (G_1' \parallel_L [1]G_2) \setminus \mathcal{A}_\mathcal{H}$ with $((F_1' \parallel_L [1]F_2) \setminus \mathcal{A}_\mathcal{H}, (G_1' \parallel_L [1]G_2) \setminus \mathcal{A}_\mathcal{H}) \in \mathcal{B}$, where the right subprocess alternates between G_2 and $[1]G_2$ thus allowing the probabilistic transitions along $G_1 \setminus \mathcal{A}_\mathcal{H} \Longrightarrow \xrightarrow{l}_{\rm a} \Longrightarrow G_1' \setminus \mathcal{A}_\mathcal{H}$ to synchronize with the only one of $[1]G_2$.
   - If $(F_1 \parallel_L F_2) \setminus \mathcal{A}_\mathcal{H} \xrightarrow{l}_{\rm a} ([1]F_1 \parallel_L F_2') \setminus \mathcal{A}_\mathcal{H}$ with $F_2 \xrightarrow{l}_{\rm a} F_2'$ and $l \notin L$, then the proof is similar to the one of the previous case.
   - If $(F_1 \parallel_L F_2) \setminus \mathcal{A}_\mathcal{H} \xrightarrow{l}_{\rm a} (F_1' \parallel_L F_2') \setminus \mathcal{A}_\mathcal{H}$ with $F_i \xrightarrow{l}_{\rm a} F_i'$ for $i \in \{1, 2\}$ and $l \in L$, then $F_i \setminus \mathcal{A}_\mathcal{H} \xrightarrow{l}_{\rm a} F_i' \setminus \mathcal{A}_\mathcal{H}$ as $l \notin \mathcal{A}_\mathcal{H}$. From $F_i \setminus \mathcal{A}_\mathcal{H} \approx_{\rm pw} G_i \setminus \mathcal{A}_\mathcal{H}$ it follows that there exists $G_i \setminus \mathcal{A}_\mathcal{H} \Longrightarrow \xrightarrow{l}_{\rm a} \Longrightarrow G_i' \setminus \mathcal{A}_\mathcal{H}$ such that $F_i' \setminus \mathcal{A}_\mathcal{H} \approx_{\rm pw} G_i' \setminus \mathcal{A}_\mathcal{H}$. Since synchronization does not apply to τ and $l \in L$, we have that $(G_1 \parallel_L G_2) \setminus \mathcal{A}_\mathcal{H} \Longrightarrow \xrightarrow{l}_{\rm a} \Longrightarrow (G_1' \parallel_L G_2') \setminus \mathcal{A}_\mathcal{H}$ with $((F_1' \parallel_L F_2') \setminus \mathcal{A}_\mathcal{H}, (G_1' \parallel_L G_2') \setminus \mathcal{A}_\mathcal{H}) \in \mathcal{B}$, where subprocess i alternates between G_i and $[1]G_i$ before performing l or between G_i' and $[1]G_i'$ after performing l thus allowing the probabilistic transitions along $G_j \setminus \mathcal{A}_\mathcal{H} \Longrightarrow \xrightarrow{l}_{\rm a} \Longrightarrow G_j' \setminus \mathcal{A}_\mathcal{H}$ for $j \neq i$ to synchronize with the only one of $[1]G_i$ before performing a or the only one of $[1]G_i'$ after performing a.
   - If $(F_1 \parallel_L F_2) \setminus \mathcal{A}_\mathcal{H} \xrightarrow{\tau}_{\rm a} (F_1' \parallel_L [1]F_2) \setminus \mathcal{A}_\mathcal{H}$ with $F_1 \xrightarrow{\tau}_{\rm a} F_1'$, then $F_1 \setminus \mathcal{A}_\mathcal{H} \xrightarrow{\tau}_{\rm a} F_1' \setminus \mathcal{A}_\mathcal{H}$ as $\tau \notin \mathcal{A}_\mathcal{H}$. From $F_1 \setminus \mathcal{A}_\mathcal{H} \approx_{\rm pw} G_1 \setminus \mathcal{A}_\mathcal{H}$ it follows that there exists $G_1 \setminus \mathcal{A}_\mathcal{H} \Longrightarrow G_1' \setminus \mathcal{A}_\mathcal{H}$ such that $F_1' \setminus \mathcal{A}_\mathcal{H} \approx_{\rm pw} G_1' \setminus \mathcal{A}_\mathcal{H}$. Since synchronization does not apply to τ, we have that $(G_1 \parallel_L G_2) \setminus \mathcal{A}_\mathcal{H} \Longrightarrow (G_1' \parallel_L G_2) \setminus \mathcal{A}_\mathcal{H}$ with $((F_1' \parallel_L [1]F_2) \setminus \mathcal{A}_\mathcal{H}, (G_1' \parallel_L [1]G_2) \setminus \mathcal{A}_\mathcal{H}) \in \mathcal{B}$, where the right subprocess alternates between G_2 and $[1]G_2$ thus allowing the probabilistic transitions along $G_1 \setminus \mathcal{A}_\mathcal{H} \Longrightarrow G_1' \setminus \mathcal{A}_\mathcal{H}$ to synchronize with the only one of $[1]G_2$.
   - If $(F_1 \parallel_L F_2) \setminus \mathcal{A}_\mathcal{H} \xrightarrow{\tau}_{\rm a} ([1]F_1 \parallel_L F_2') \setminus \mathcal{A}_\mathcal{H}$ with $F_2 \xrightarrow{\tau}_{\rm a} F_2'$, then the proof is similar to the one of the previous case.

As for probabilities, to avoid trivial cases let $F_1, F_2, G_1, G_2 \in \mathbb{P}_{\rm p}$ and consider an equivalence class $C \in \mathbb{P}_{\rm pr}/\mathcal{B}$ that involves nondeterministic processes reachable from $E_1 \parallel_L E_2$, specifically $C = \{(H_{1,i} \parallel_L H_{2,i}) \setminus \mathcal{A}_\mathcal{H} \mid H_{k,h} \in reach(E_k) \wedge H_{1,h} \parallel_L H_{2,h} \in reach(E_1 \parallel_L E_2) \wedge H_{k,i} \setminus \mathcal{A}_\mathcal{H} \approx_{\rm pw} H_{k,j} \setminus \mathcal{A}_\mathcal{H}\}$. Since the restriction operator does not apply to probabilistic transitions, we have that:

$$\begin{aligned} prob((F_1 \parallel_L F_2) \setminus \mathcal{A}_\mathcal{H}, C) \;&=\; prob((F_1 \setminus \mathcal{A}_\mathcal{H}) \parallel_L (F_2 \setminus \mathcal{A}_\mathcal{H}), C) \\ prob((G_1 \parallel_L G_2) \setminus \mathcal{A}_\mathcal{H}, C) \;&=\; prob((G_1 \setminus \mathcal{A}_\mathcal{H}) \parallel_L (G_2 \setminus \mathcal{A}_\mathcal{H}), C) \end{aligned}$$

and hence by virtue of Lemma 9.1 we have that:

$$\begin{aligned} prob((F_1 \setminus \mathcal{A}_\mathcal{H}) \parallel_L (F_2 \setminus \mathcal{A}_\mathcal{H}), C) \;&=\; prob(F_1 \setminus \mathcal{A}_\mathcal{H}, C_1) \cdot prob(F_2 \setminus \mathcal{A}_\mathcal{H}, C_2) \\ prob((G_1 \setminus \mathcal{A}_\mathcal{H}) \parallel_L (G_2 \setminus \mathcal{A}_\mathcal{H}), C) \;&=\; prob(G_1 \setminus \mathcal{A}_\mathcal{H}, C_1) \cdot prob(G_2 \setminus \mathcal{A}_\mathcal{H}, C_2) \end{aligned}$$

where:

$$\begin{array}{rcl} C_1 & = & \{H_{1,h} \setminus \mathcal{A}_\mathcal{H} \mid (H_{1,h} \parallel_L H_{2,h}) \setminus \mathcal{A}_\mathcal{H} \in C\} \\ C_2 & = & \{H_{2,h} \setminus \mathcal{A}_\mathcal{H} \mid (H_{1,h} \parallel_L H_{2,h}) \setminus \mathcal{A}_\mathcal{H} \in C\} \end{array}$$

Since $F_k \setminus \mathcal{A}_\mathcal{H} \approx_{\rm pw} G_k \setminus \mathcal{A}_\mathcal{H}$ and C_k is the union of some $\approx_{\rm pw}$-equivalence classes for $k \in \{1,2\}$, we have that:

$$\begin{array}{rcl} prob(F_1 \setminus \mathcal{A}_\mathcal{H}, C_1) & = & prob(G_1 \setminus \mathcal{A}_\mathcal{H}, C_1) \\ prob(F_2 \setminus \mathcal{A}_\mathcal{H}, C_2) & = & prob(G_2 \setminus \mathcal{A}_\mathcal{H}, C_2) \end{array}$$

We then prove the three results for the $\approx_{\rm pb}$-based properties. Let $\mathcal{B}$ be an equivalence relation containing all the pairs of processes that have to be shown to be $\approx_{\rm pb}$-equivalent according to the considered result:

1. Starting from $(F_1 \parallel_L F_2) \setminus \mathcal{A}_\mathcal{H}$ and $(G_1 \parallel_L G_2) \,/\, \mathcal{A}_\mathcal{H}$ related by $\mathcal{B}$, so that $F_1 \setminus \mathcal{A}_\mathcal{H} \approx_{\rm pb} G_1 \,/\, \mathcal{A}_\mathcal{H}$ and $F_2 \setminus \mathcal{A}_\mathcal{H} \approx_{\rm pb} G_2 \,/\, \mathcal{A}_\mathcal{H}$, there are twelve cases for action transitions based on the operational semantic rules in Table 9.1. In the first five cases, it is $(F_1 \parallel_L F_2) \setminus \mathcal{A}_\mathcal{H}$ to move first:

   - If $(F_1 \parallel_L F_2) \setminus \mathcal{A}_\mathcal{H} \stackrel{l}{\longrightarrow}_{\rm a} (F_1' \parallel_L [1]F_2) \setminus \mathcal{A}_\mathcal{H}$ with $F_1 \stackrel{l}{\longrightarrow}_{\rm a} F_1'$ and $l \notin L$, then $F_1 \setminus \mathcal{A}_\mathcal{H} \stackrel{l}{\longrightarrow}_{\rm a} F_1' \setminus \mathcal{A}_\mathcal{H}$ as $l \notin \mathcal{A}_\mathcal{H}$. From $F_1 \setminus \mathcal{A}_\mathcal{H} \approx_{\rm pb} G_1 \,/\, \mathcal{A}_\mathcal{H}$ it follows that there exists $G_1 \,/\, \mathcal{A}_\mathcal{H} \Longrightarrow \bar{G}_1 \,/\, \mathcal{A}_\mathcal{H} \stackrel{l}{\longrightarrow}_{\rm a} G_1' \,/\, \mathcal{A}_\mathcal{H}$ such that $F_1 \setminus \mathcal{A}_\mathcal{H} \approx_{\rm pb} \bar{G}_1 \,/\, \mathcal{A}_\mathcal{H}$ and $F_1' \setminus \mathcal{A}_\mathcal{H} \approx_{\rm pb} G_1' \,/\, \mathcal{A}_\mathcal{H}$. Since synchronization does not apply to τ and $l \notin L$, we have that $(G_1 \parallel_L G_2) \,/\, \mathcal{A}_\mathcal{H} \Longrightarrow (\bar{G}_1 \parallel_L G_2) \,/\, \mathcal{A}_\mathcal{H} \stackrel{l}{\longrightarrow}_{\rm a} (G_1' \parallel_L [1]G_2) \,/\, \mathcal{A}_\mathcal{H}$ with $((F_1 \parallel_L F_2) \setminus \mathcal{A}_\mathcal{H}, (\bar{G}_1 \parallel_L G_2) \,/\, \mathcal{A}_\mathcal{H}) \in \mathcal{B}$ and $((F_1' \parallel_L [1]F_2) \setminus \mathcal{A}_\mathcal{H}, (G_1' \parallel_L [1]G_2) \,/\, \mathcal{A}_\mathcal{H}) \in \mathcal{B}$, where the right subprocess alternates between G_2 and $[1]G_2$ thus allowing the probabilistic transitions along $G_1 \,/\, \mathcal{A}_\mathcal{H} \Longrightarrow \bar{G}_1 \,/\, \mathcal{A}_\mathcal{H}$ to synchronize with the only one of $[1]G_2$.
   - If $(F_1 \parallel_L F_2) \setminus \mathcal{A}_\mathcal{H} \stackrel{l}{\longrightarrow}_{\rm a} ([1]F_1 \parallel_L F_2') \setminus \mathcal{A}_\mathcal{H}$ with $F_2 \stackrel{l}{\longrightarrow}_{\rm a} F_2'$ and $l \notin L$, then the proof is similar to the one of the previous case.
   - If $(F_1 \parallel_L F_2) \setminus \mathcal{A}_\mathcal{H} \stackrel{l}{\longrightarrow}_{\rm a} (F_1' \parallel_L F_2') \setminus \mathcal{A}_\mathcal{H}$ with $F_i \stackrel{l}{\longrightarrow}_{\rm a} F_i'$ for $i \in \{1,2\}$ and $l \in L$, then $F_i \setminus \mathcal{A}_\mathcal{H} \stackrel{l}{\longrightarrow}_{\rm a} F_i' \setminus \mathcal{A}_\mathcal{H}$ as $l \notin \mathcal{A}_\mathcal{H}$. From $F_i \setminus \mathcal{A}_\mathcal{H} \approx_{\rm pb} G_i \,/\, \mathcal{A}_\mathcal{H}$ it follows that there exists $G_i \,/\, \mathcal{A}_\mathcal{H} \Longrightarrow \bar{G}_i \,/\, \mathcal{A}_\mathcal{H} \stackrel{l}{\longrightarrow}_{\rm a} G_i' \,/\, \mathcal{A}_\mathcal{H}$ such that $F_i \setminus \mathcal{A}_\mathcal{H} \approx_{\rm pb} \bar{G}_i \,/\, \mathcal{A}_\mathcal{H}$ and $F_i' \setminus \mathcal{A}_\mathcal{H} \approx_{\rm pb} G_i' \,/\, \mathcal{A}_\mathcal{H}$. Since synchronization does not apply to τ and $l \in L$, we have that $(G_1 \parallel_L G_2) \,/\, \mathcal{A}_\mathcal{H} \Longrightarrow (\bar{G}_1 \parallel_L \bar{G}_2) \,/\, \mathcal{A}_\mathcal{H} \stackrel{l}{\longrightarrow}_{\rm a} (G_1' \parallel_L G_2') \,/\, \mathcal{A}_\mathcal{H}$ with $((F_1 \parallel_L F_2) \setminus \mathcal{A}_\mathcal{H}, (\bar{G}_1 \parallel_L \bar{G}_2) \,/\, \mathcal{A}_\mathcal{H}) \in \mathcal{B}$ and $((F_1' \parallel_L F_2') \setminus \mathcal{A}_\mathcal{H}, (G_1' \parallel_L G_2') \,/\, \mathcal{A}_\mathcal{H}) \in \mathcal{B}$, where subprocess i alternates between G_i and $[1]G_i$ thus allowing the probabilistic transitions along $G_j \,/\, \mathcal{A}_\mathcal{H} \Longrightarrow \bar{G}_j \,/\, \mathcal{A}_\mathcal{H}$ for $j \neq i$ to synchronize with the only one of $[1]G_i$.
   - If $(F_1 \parallel_L F_2) \setminus \mathcal{A}_\mathcal{H} \stackrel{\tau}{\longrightarrow}_{\rm a} (F_1' \parallel_L [1]F_2) \setminus \mathcal{A}_\mathcal{H}$ with $F_1 \stackrel{\tau}{\longrightarrow}_{\rm a} F_1'$, then $F_1 \setminus \mathcal{A}_\mathcal{H} \stackrel{\tau}{\longrightarrow}_{\rm a} F_1' \setminus \mathcal{A}_\mathcal{H}$ as $\tau \notin \mathcal{A}_\mathcal{H}$. From $F_1 \setminus \mathcal{A}_\mathcal{H} \approx_{\rm pb} G_1 \,/\, \mathcal{A}_\mathcal{H}$ it follows that either $F_1' \setminus \mathcal{A}_\mathcal{H} \approx_{\rm pb} G_1 \,/\, \mathcal{A}_\mathcal{H}$, or there exists $G_1 \,/\, \mathcal{A}_\mathcal{H} \Longrightarrow \bar{G}_1 \,/\, \mathcal{A}_\mathcal{H} \stackrel{\tau}{\longrightarrow}_{\rm a} G_1' \,/\, \mathcal{A}_\mathcal{H}$ such that $F_1 \setminus \mathcal{A}_\mathcal{H} \approx_{\rm pb} \bar{G}_1 \,/\, \mathcal{A}_\mathcal{H}$ and $F_1' \setminus \mathcal{A}_\mathcal{H} \approx_{\rm pb} G_1' \,/\, \mathcal{A}_\mathcal{H}$. Since synchronization does not apply to τ, in the former subcase $(G_1 \parallel_L G_2) \,/\, \mathcal{A}_\mathcal{H}$ is allowed to stay idle with $((F_1' \parallel_L [1]F_2) \setminus \mathcal{A}_\mathcal{H}, (G_1 \parallel_L G_2) \,/\, \mathcal{A}_\mathcal{H}) \in \mathcal{B}$, while in the latter subcase $(G_1 \parallel_L G_2) \,/\, \mathcal{A}_\mathcal{H} \Longrightarrow (\bar{G}_1 \parallel_L G_2) \,/\, \mathcal{A}_\mathcal{H} \stackrel{\tau}{\longrightarrow}_{\rm a} (G_1' \parallel_L [1]G_2) \,/\, \mathcal{A}_\mathcal{H}$ with $((F_1 \parallel_L F_2) \setminus \mathcal{A}_\mathcal{H}, (\bar{G}_1 \parallel_L G_2) / \mathcal{A}_\mathcal{H}) \in \mathcal{B}$ and $((F_1' \parallel_L [1]F_2) \setminus \mathcal{A}_\mathcal{H}, (G_1' \parallel_L [1]G_2) \,/\, \mathcal{A}_\mathcal{H}) \in \mathcal{B}$, where the right subprocess alternates between G_2 and $[1]G_2$ thus allowing the probabilistic transitions along $G_1 \,/\, \mathcal{A}_\mathcal{H} \Longrightarrow \bar{G}_1 \,/\, \mathcal{A}_\mathcal{H}$ to synchronize with the only one of $[1]G_2$.
   - If $(F_1 \parallel_L F_2) \setminus \mathcal{A}_\mathcal{H} \stackrel{\tau}{\longrightarrow}_{\rm a} ([1]F_1 \parallel_L F_2') \setminus \mathcal{A}_\mathcal{H}$ with $F_2 \stackrel{\tau}{\longrightarrow}_{\rm a} F_2'$, then the proof is similar to the one of the previous case.

In the other seven cases, instead, it is $(G_1 \parallel_L G_2) / \mathcal{A}_\mathcal{H}$ to move first:

- If $(G_1 \parallel_L G_2) / \mathcal{A}_\mathcal{H} \xrightarrow{l}_\mathrm{a} (G_1' \parallel_L [1]G_2) / \mathcal{A}_\mathcal{H}$ with $G_1 \xrightarrow{l}_\mathrm{a} G_1'$ and $l \notin L$, then $G_1 / \mathcal{A}_\mathcal{H} \xrightarrow{l}_\mathrm{a} G_1' / \mathcal{A}_\mathcal{H}$ as $l \notin \mathcal{A}_\mathcal{H}$. From $G_1 / \mathcal{A}_\mathcal{H} \approx_\mathrm{pb} F_1 \setminus \mathcal{A}_\mathcal{H}$ it follows that there exists $F_1 \setminus \mathcal{A}_\mathcal{H} \Longrightarrow \bar{F}_1 \setminus \mathcal{A}_\mathcal{H} \xrightarrow{l}_\mathrm{a} F_1' \setminus \mathcal{A}_\mathcal{H}$ such that $G_1 / \mathcal{A}_\mathcal{H} \approx_\mathrm{pb} \bar{F}_1 \setminus \mathcal{A}_\mathcal{H}$ and $G_1' / \mathcal{A}_\mathcal{H} \approx_\mathrm{pb} F_1' \setminus \mathcal{A}_\mathcal{H}$. Since synchronization does not apply to τ and $l \notin L$, we have that $(F_1 \parallel_L F_2) \setminus \mathcal{A}_\mathcal{H} \Longrightarrow (\bar{F}_1 \parallel_L F_2) \setminus \mathcal{A}_\mathcal{H} \xrightarrow{l}_\mathrm{a} (F_1' \parallel_L [1]F_2) \setminus \mathcal{A}_\mathcal{H}$ with $((G_1 \parallel_L G_2)/\mathcal{A}_\mathcal{H}, (\bar{F}_1 \parallel_L F_2) \setminus \mathcal{A}_\mathcal{H}) \in \mathcal{B}$ and $((G_1' \parallel_L [1]G_2)/\mathcal{A}_\mathcal{H}, (F_1' \parallel_L [1]F_2) \setminus \mathcal{A}_\mathcal{H}) \in \mathcal{B}$, where the right subprocess alternates between F_2 and $[1]F_2$ thus allowing the probabilistic transitions along $F_1 \setminus \mathcal{A}_\mathcal{H} \Longrightarrow \bar{F}_1 \setminus \mathcal{A}_\mathcal{H}$ to synchronize with the only one of $[1]F_2$.
- If $(G_1 \parallel_L G_2) / \mathcal{A}_\mathcal{H} \xrightarrow{l}_\mathrm{a} ([1]G_1 \parallel_L G_2') / \mathcal{A}_\mathcal{H}$ with $G_2 \xrightarrow{l}_\mathrm{a} G_2'$ and $l \notin L$, then the proof is similar to the one of the previous case.
- If $(G_1 \parallel_L G_2) / \mathcal{A}_\mathcal{H} \xrightarrow{l}_\mathrm{a} (G_1' \parallel_L G_2') / \mathcal{A}_\mathcal{H}$ with $G_i \xrightarrow{l}_\mathrm{a} G_i'$ for $i \in \{1, 2\}$ and $l \in L$, then $G_i / \mathcal{A}_\mathcal{H} \xrightarrow{l}_\mathrm{a} G_i' / \mathcal{A}_\mathcal{H}$ as $l \notin \mathcal{A}_\mathcal{H}$. From $G_i / \mathcal{A}_\mathcal{H} \approx_\mathrm{pb} F_i \setminus \mathcal{A}_\mathcal{H}$ it follows that there exists $F_i \setminus \mathcal{A}_\mathcal{H} \Longrightarrow \bar{F}_i \setminus \mathcal{A}_\mathcal{H} \xrightarrow{l}_\mathrm{a} F_i' \setminus \mathcal{A}_\mathcal{H}$ such that $G_i / \mathcal{A}_\mathcal{H} \approx_\mathrm{pb} \bar{F}_i \setminus \mathcal{A}_\mathcal{H}$ and $G_i' / \mathcal{A}_\mathcal{H} \approx_\mathrm{pb} F_i' \setminus \mathcal{A}_\mathcal{H}$. Since synchronization does not apply to τ and $l \in L$, we have that $(F_1 \parallel_L F_2) \setminus \mathcal{A}_\mathcal{H} \Longrightarrow (\bar{F}_1 \parallel_L \bar{F}_2) \setminus \mathcal{A}_\mathcal{H} \xrightarrow{l}_\mathrm{a} (F_1' \parallel_L F_2') \setminus \mathcal{A}_\mathcal{H}$ with $((G_1 \parallel_L G_2)/\mathcal{A}_\mathcal{H}, (\bar{F}_1 \parallel_L \bar{F}_2) \setminus \mathcal{A}_\mathcal{H}) \in \mathcal{B}$ and $((G_1' \parallel_L G_2') / \mathcal{A}_\mathcal{H}, (F_1' \parallel_L F_2') \setminus \mathcal{A}_\mathcal{H}) \in \mathcal{B}$, where subprocess i alternates between F_i and $[1]F_i$ thus allowing the probabilistic transitions along $F_j \setminus \mathcal{A}_\mathcal{H} \Longrightarrow \bar{F}_j \setminus \mathcal{A}_\mathcal{H}$ for $j \neq i$ to synchronize with the only one of $[1]F_i$.
- If $(G_1 \parallel_L G_2) / \mathcal{A}_\mathcal{H} \xrightarrow{\tau}_\mathrm{a} (G_1' \parallel_L [1]G_2) / \mathcal{A}_\mathcal{H}$ with $G_1 \xrightarrow{\tau}_\mathrm{a} G_1'$, then $G_1 / \mathcal{A}_\mathcal{H} \xrightarrow{\tau}_\mathrm{a} G_1' / \mathcal{A}_\mathcal{H}$ as $\tau \notin \mathcal{A}_\mathcal{H}$. From $G_1 / \mathcal{A}_\mathcal{H} \approx_\mathrm{pb} F_1 \setminus \mathcal{A}_\mathcal{H}$ it follows that either $G_1' / \mathcal{A}_\mathcal{H} \approx_\mathrm{pb} F_1 \setminus \mathcal{A}_\mathcal{H}$, or there exists $F_1 \setminus \mathcal{A}_\mathcal{H} \Longrightarrow \bar{F}_1 \setminus \mathcal{A}_\mathcal{H} \xrightarrow{\tau}_\mathrm{a} F_1' \setminus \mathcal{A}_\mathcal{H}$ such that $G_1 / \mathcal{A}_\mathcal{H} \approx_\mathrm{pb} \bar{F}_1 \setminus \mathcal{A}_\mathcal{H}$ and $G_1' / \mathcal{A}_\mathcal{H} \approx_\mathrm{pb} F_1' \setminus \mathcal{A}_\mathcal{H}$. Since synchronization does not apply to τ, in the former subcase $(F_1 \parallel_L F_2) \setminus \mathcal{A}_\mathcal{H}$ is allowed to stay idle with $((G_1' \parallel_L [1]G_2)/\mathcal{A}_\mathcal{H}, (F_1 \parallel_L F_2) \setminus \mathcal{A}_\mathcal{H}) \in \mathcal{B}$, while in the latter subcase $(F_1 \parallel_L F_2) \setminus \mathcal{A}_\mathcal{H} \Longrightarrow (\bar{F}_1 \parallel_L F_2) \setminus \mathcal{A}_\mathcal{H} \xrightarrow{\tau}_\mathrm{a} (F_1' \parallel_L [1]F_2) \setminus \mathcal{A}_\mathcal{H}$ with $((G_1 \parallel_L G_2)/\mathcal{A}_\mathcal{H}, (\bar{F}_1 \parallel_L F_2) \setminus \mathcal{A}_\mathcal{H}) \in \mathcal{B}$ and $((G_1' \parallel_L [1]G_2)/\mathcal{A}_\mathcal{H}, (F_1' \parallel_L [1]F_2) \setminus \mathcal{A}_\mathcal{H}) \in \mathcal{B}$, where the right subprocess alternates between F_2 and $[1]F_2$ thus allowing the probabilistic transitions along $F_1 \setminus \mathcal{A}_\mathcal{H} \Longrightarrow \bar{F}_1 \setminus \mathcal{A}_\mathcal{H}$ to synchronize with the only one of $[1]F_2$.
- If $(G_1 \parallel_L G_2) / \mathcal{A}_\mathcal{H} \xrightarrow{\tau}_\mathrm{a} ([1]G_1 \parallel_L G_2') / \mathcal{A}_\mathcal{H}$ with $G_2 \xrightarrow{\tau}_\mathrm{a} G_2'$, then the proof is similar to the one of the previous case.
- If $(G_1 \parallel_L G_2) / \mathcal{A}_\mathcal{H} \xrightarrow{\tau}_\mathrm{a} (G_1' \parallel_L [1]G_2) / \mathcal{A}_\mathcal{H}$ with $G_1 \xrightarrow{h}_\mathrm{a} G_1'$ and $h \notin L$, then $G_1 / \mathcal{A}_\mathcal{H} \xrightarrow{\tau}_\mathrm{a} G_1' / \mathcal{A}_\mathcal{H}$ as $h \in \mathcal{A}_\mathcal{H}$. The rest of the proof is like the one of the fourth case.
- If $(G_1 \parallel_L G_2) / \mathcal{A}_\mathcal{H} \xrightarrow{\tau}_\mathrm{a} ([1]G_1 \parallel_L G_2') / \mathcal{A}_\mathcal{H}$ with $G_2 \xrightarrow{h}_\mathrm{a} G_2'$ and $h \notin L$, then the proof is similar to the one of the previous case.

As for probabilities, we reason like in the proof of the corresponding result for $\approx_\mathrm{pw}$.

2. Starting from $(F / \mathcal{A}_\mathcal{H}) \setminus L$ and $(G \setminus L) / \mathcal{A}_\mathcal{H}$ related by $\mathcal{B}$, so that $F / \mathcal{A}_\mathcal{H} \approx_\mathrm{pb} G \setminus \mathcal{A}_\mathcal{H}$, there are six cases for action transitions based on the operational semantic rules in Table 9.1. In the first three cases, it is $(F / \mathcal{A}_\mathcal{H}) \setminus L$ to move first:

- If $(F / \mathcal{A}_\mathcal{H}) \setminus L \xrightarrow{l}_\mathrm{a} (F' / \mathcal{A}_\mathcal{H}) \setminus L$ with $F \xrightarrow{l}_\mathrm{a} F'$ and $l \notin L$, then $F / \mathcal{A}_\mathcal{H} \xrightarrow{l}_\mathrm{a} F' / \mathcal{A}_\mathcal{H}$ as $l \notin \mathcal{A}_\mathcal{H}$. From $F / \mathcal{A}_\mathcal{H} \approx_\mathrm{pb} G \setminus \mathcal{A}_\mathcal{H}$ it follows that there exists $G \setminus \mathcal{A}_\mathcal{H} \Longrightarrow \bar{G} \setminus \mathcal{A}_\mathcal{H} \xrightarrow{l}_\mathrm{a} G' \setminus \mathcal{A}_\mathcal{H}$ such that

$F \,/\, \mathcal{A}_\mathcal{H} \approx_{\rm pb} \bar{G} \setminus \mathcal{A}_\mathcal{H}$ and $F' \,/\, \mathcal{A}_\mathcal{H} \approx_{\rm pb} G' \setminus \mathcal{A}_\mathcal{H}$. Since the restriction and hiding operators do not apply to τ, l, and probabilistic transitions, we have that $(G \setminus L) \,/\, \mathcal{A}_\mathcal{H} \Longrightarrow (\bar{G} \setminus L) \,/\, \mathcal{A}_\mathcal{H} \xrightarrow{l}_{\rm a} (G' \setminus L) \,/\, \mathcal{A}_\mathcal{H}$ with $((F \,/\, \mathcal{A}_\mathcal{H}) \setminus L, (\bar{G} \setminus L) \,/\, \mathcal{A}_\mathcal{H}) \in \mathcal{B}$ and $((F' \,/\, \mathcal{A}_\mathcal{H}) \setminus L, (G' \setminus L) \,/\, \mathcal{A}_\mathcal{H}) \in \mathcal{B}$.

- If $(F \,/\, \mathcal{A}_\mathcal{H}) \setminus L \xrightarrow{\tau}_{\rm a} (F' \,/\, \mathcal{A}_\mathcal{H}) \setminus L$ with $F \xrightarrow{\tau}_{\rm a} F'$, then $F \,/\, \mathcal{A}_\mathcal{H} \xrightarrow{\tau}_{\rm a} F' \,/\, \mathcal{A}_\mathcal{H}$ as $\tau \notin \mathcal{A}_\mathcal{H}$. From $F \,/\, \mathcal{A}_\mathcal{H} \approx_{\rm pb} G \setminus \mathcal{A}_\mathcal{H}$ it follows that either $F' \,/\, \mathcal{A}_\mathcal{H} \approx_{\rm pb} G \setminus \mathcal{A}_\mathcal{H}$, or there exists $G \setminus \mathcal{A}_\mathcal{H} \Longrightarrow \bar{G} \setminus \mathcal{A}_\mathcal{H} \xrightarrow{\tau}_{\rm a} G' \setminus \mathcal{A}_\mathcal{H}$ such that $F \,/\, \mathcal{A}_\mathcal{H} \approx_{\rm pb} \bar{G} \setminus \mathcal{A}_\mathcal{H}$ and $F' \,/\, \mathcal{A}_\mathcal{H} \approx_{\rm pb} G' \setminus \mathcal{A}_\mathcal{H}$. Since the restriction and hiding operators do not apply to τ and probabilistic transitions, in the former subcase $(G \setminus L) \,/\, \mathcal{A}_\mathcal{H}$ is allowed to stay idle with $((F' \,/\, \mathcal{A}_\mathcal{H}) \setminus L, (G \setminus L) \,/\, \mathcal{A}_\mathcal{H}) \in \mathcal{B}$, while in the latter subcase $(G \setminus L) \,/\, \mathcal{A}_\mathcal{H} \Longrightarrow (\bar{G} \setminus L) \,/\, \mathcal{A}_\mathcal{H} \xrightarrow{\tau}_{\rm a} (G' \setminus L) \,/\, \mathcal{A}_\mathcal{H}$ with $((F \,/\, \mathcal{A}_\mathcal{H}) \setminus L, (\bar{G} \setminus L) \,/\, \mathcal{A}_\mathcal{H}) \in \mathcal{B}$ and $((F' \,/\, \mathcal{A}_\mathcal{H}) \setminus L, (G' \setminus L) \,/\, \mathcal{A}_\mathcal{H}) \in \mathcal{B}$.
- If $(F \,/\, \mathcal{A}_\mathcal{H}) \setminus L \xrightarrow{\tau}_{\rm a} (F' \,/\, \mathcal{A}_\mathcal{H}) \setminus L$ with $F \xrightarrow{h}_{\rm a} F'$, then $F \,/\, \mathcal{A}_\mathcal{H} \xrightarrow{\tau}_{\rm a} F' \,/\, \mathcal{A}_\mathcal{H}$ as $h \in \mathcal{A}_\mathcal{H}$. The rest of the proof is like the one of the previous case.

In the other three cases, instead, it is $(G \setminus L) \,/\, \mathcal{A}_\mathcal{H}$ to move first:

- If $(G \setminus L) \,/\, \mathcal{A}_\mathcal{H} \xrightarrow{l}_{\rm a} (G' \setminus L) \,/\, \mathcal{A}_\mathcal{H}$ with $G \xrightarrow{l}_{\rm a} G'$ and $l \notin L$, then $G \setminus \mathcal{A}_\mathcal{H} \xrightarrow{l}_{\rm a} G' \setminus \mathcal{A}_\mathcal{H}$ as $l \notin \mathcal{A}_\mathcal{H}$. From $G \setminus \mathcal{A}_\mathcal{H} \approx_{\rm pb} F \,/\, \mathcal{A}_\mathcal{H}$ it follows that there exists $F \,/\, \mathcal{A}_\mathcal{H} \Longrightarrow \bar{F} \,/\, \mathcal{A}_\mathcal{H} \xrightarrow{l}_{\rm a} F' \,/\, \mathcal{A}_\mathcal{H}$ such that $G \setminus \mathcal{A}_\mathcal{H} \approx_{\rm pb} \bar{F} \,/\, \mathcal{A}_\mathcal{H}$ and $G' \setminus \mathcal{A}_\mathcal{H} \approx_{\rm pb} F' \,/\, \mathcal{A}_\mathcal{H}$. Since the restriction operator does not apply to τ, l, and probabilistic transitions, we have that $(F \,/\, \mathcal{A}_\mathcal{H}) \setminus L \Longrightarrow (\bar{F} \,/\, \mathcal{A}_\mathcal{H}) \setminus L \xrightarrow{l}_{\rm a} (F' \,/\, \mathcal{A}_\mathcal{H}) \setminus L$ with $((G \setminus L) \,/\, \mathcal{A}_\mathcal{H}, (\bar{F} \,/\, \mathcal{A}_\mathcal{H}) \setminus L) \in \mathcal{B}$ and $((G' \setminus L) \,/\, \mathcal{A}_\mathcal{H}, (F' \,/\, \mathcal{A}_\mathcal{H}) \setminus L) \in \mathcal{B}$.
- If $(G \setminus L) \,/\, \mathcal{A}_\mathcal{H} \xrightarrow{\tau}_{\rm a} (G' \setminus L) \,/\, \mathcal{A}_\mathcal{H}$ with $G \xrightarrow{\tau}_{\rm a} G'$, then $G \setminus \mathcal{A}_\mathcal{H} \xrightarrow{\tau}_{\rm a} G' \setminus \mathcal{A}_\mathcal{H}$ as $\tau \notin \mathcal{A}_\mathcal{H}$. From $G \setminus \mathcal{A}_\mathcal{H} \approx_{\rm pb} F \,/\, \mathcal{A}_\mathcal{H}$ it follows that either $G' \setminus \mathcal{A}_\mathcal{H} \approx_{\rm pb} F \,/\, \mathcal{A}_\mathcal{H}$, or there exists $F \,/\, \mathcal{A}_\mathcal{H} \Longrightarrow \bar{F} \,/\, \mathcal{A}_\mathcal{H} \xrightarrow{\tau}_{\rm a} F' \,/\, \mathcal{A}_\mathcal{H}$ such that $G \setminus \mathcal{A}_\mathcal{H} \approx_{\rm pb} \bar{F} \,/\, \mathcal{A}_\mathcal{H}$ and $G' \setminus \mathcal{A}_\mathcal{H} \approx_{\rm pb} F' \,/\, \mathcal{A}_\mathcal{H}$. Since the restriction operator does not apply to τ and probabilistic transitions, in the former subcase $(F \,/\, \mathcal{A}_\mathcal{H}) \setminus L$ is allowed to stay idle with $((G' \setminus L) / \mathcal{A}_\mathcal{H}, (F / \mathcal{A}_\mathcal{H}) \setminus L) \in \mathcal{B}$, while in the latter subcase $(F \,/\, \mathcal{A}_\mathcal{H}) \setminus L \Longrightarrow (\bar{F} \,/\, \mathcal{A}_\mathcal{H}) \setminus L \xrightarrow{\tau}_{\rm a} (F' \,/\, \mathcal{A}_\mathcal{H}) \setminus L$ with $((G \setminus L) \,/\, \mathcal{A}_\mathcal{H}, (\bar{F} \,/\, \mathcal{A}_\mathcal{H}) \setminus L) \in \mathcal{B}$ and $((G' \setminus L) \,/\, \mathcal{A}_\mathcal{H}, (F' \,/\, \mathcal{A}_\mathcal{H}) \setminus L) \in \mathcal{B}$.
- If $(G \setminus L) \,/\, \mathcal{A}_\mathcal{H} \xrightarrow{\tau}_{\rm a} (G' \setminus L) \,/\, \mathcal{A}_\mathcal{H}$ with $G \xrightarrow{h}_{\rm a} G'$ and $h \notin L$, then $G \,/\, \mathcal{A}_\mathcal{H} \xrightarrow{\tau}_{\rm a} G' \,/\, \mathcal{A}_\mathcal{H}$ as $h \in \mathcal{A}_\mathcal{H}$ (note that $G \setminus \mathcal{A}_\mathcal{H}$ cannot perform h). From $G \,/\, \mathcal{A}_\mathcal{H} \approx_{\rm pb} G \setminus \mathcal{A}_\mathcal{H}$ – as $E \in {\rm SBSNNI}_{\approx_{\rm pb}}$ and $G \in \mathit{reach}(E)$ – and $G \setminus \mathcal{A}_\mathcal{H} \approx_{\rm pb} F \,/\, \mathcal{A}_\mathcal{H}$ it follows that either $G' \,/\, \mathcal{A}_\mathcal{H} \approx_{\rm pb} F \,/\, \mathcal{A}_\mathcal{H}$ and hence $G' \setminus \mathcal{A}_\mathcal{H} \approx_{\rm pb} F \,/\, \mathcal{A}_\mathcal{H}$ – as $G' \,/\, \mathcal{A}_\mathcal{H} \approx_{\rm pb} G' \setminus \mathcal{A}_\mathcal{H}$ due to $E \in {\rm SBSNNI}_{\approx_{\rm pb}}$ and $G' \in \mathit{reach}(E)$ – or there exists $F \,/\, \mathcal{A}_\mathcal{H} \Longrightarrow \bar{F} \,/\, \mathcal{A}_\mathcal{H} \xrightarrow{\tau}_{\rm a} F' \,/\, \mathcal{A}_\mathcal{H}$ such that $G \,/\, \mathcal{A}_\mathcal{H} \approx_{\rm pb} \bar{F} \,/\, \mathcal{A}_\mathcal{H}$ and $G' \,/\, \mathcal{A}_\mathcal{H} \approx_{\rm pb} F' \,/\, \mathcal{A}_\mathcal{H}$ and hence $G \setminus \mathcal{A}_\mathcal{H} \approx_{\rm pb} \bar{F} \,/\, \mathcal{A}_\mathcal{H}$ and $G' \setminus \mathcal{A}_\mathcal{H} \approx_{\rm pb} F' \,/\, \mathcal{A}_\mathcal{H}$. Since the restriction operator does not apply to τ and probabilistic transitions, in the former subcase $(F \,/\, \mathcal{A}_\mathcal{H}) \setminus L$ is allowed to stay idle with $((G' \setminus L) \,/\, \mathcal{A}_\mathcal{H}, (F \,/\, \mathcal{A}_\mathcal{H}) \setminus L) \in \mathcal{B}$, while in the latter subcase $(F \,/\, \mathcal{A}_\mathcal{H}) \setminus L \Longrightarrow (\bar{F} \,/\, \mathcal{A}_\mathcal{H}) \setminus L \xrightarrow{\tau}_{\rm a} (F' \,/\, \mathcal{A}_\mathcal{H}) \setminus L$ with $((G \setminus L) \,/\, \mathcal{A}_\mathcal{H}, (\bar{F} \,/\, \mathcal{A}_\mathcal{H}) \setminus L) \in \mathcal{B}$ and $((G' \setminus L) \,/\, \mathcal{A}_\mathcal{H}, (F' \,/\, \mathcal{A}_\mathcal{H}) \setminus L) \in \mathcal{B}$.

As for probabilities, we reason like in the proof of the corresponding result for $\approx_{\rm pw}$.

3. Starting from $(F_1 \parallel_L F_2) \setminus \mathcal{A}_\mathcal{H}$ and $(G_1 \parallel_L G_2) \setminus \mathcal{A}_\mathcal{H}$ related by $\mathcal{B}$, so that $F_1 \setminus \mathcal{A}_\mathcal{H} \approx_{\rm pb} G_1 \setminus \mathcal{A}_\mathcal{H}$ and $F_2 \setminus \mathcal{A}_\mathcal{H} \approx_{\rm pb} G_2 \setminus \mathcal{A}_\mathcal{H}$, there are five cases for action transitions based on the operational semantic rules in Table 9.1:

- If $(F_1 \parallel_L F_2) \setminus \mathcal{A}_\mathcal{H} \xrightarrow{l}_\mathrm{a} (F_1' \parallel_L [1]F_2) \setminus \mathcal{A}_\mathcal{H}$ with $F_1 \xrightarrow{l}_\mathrm{a} F_1'$ and $l \notin L$, then $F_1 \setminus \mathcal{A}_\mathcal{H} \xrightarrow{l}_\mathrm{a} F_1' \setminus \mathcal{A}_\mathcal{H}$ as $l \notin \mathcal{A}_\mathcal{H}$. From $F_1 \setminus \mathcal{A}_\mathcal{H} \approx_\mathrm{pb} G_1 \setminus \mathcal{A}_\mathcal{H}$ it follows that there exists $G_1 \setminus \mathcal{A}_\mathcal{H} \Longrightarrow \bar{G}_1 \setminus \mathcal{A}_\mathcal{H} \xrightarrow{l}_\mathrm{a} G_1' \setminus \mathcal{A}_\mathcal{H}$ such that $F_1 \setminus \mathcal{A}_\mathcal{H} \approx_\mathrm{pb} \bar{G}_1 \setminus \mathcal{A}_\mathcal{H}$ and $F_1' \setminus \mathcal{A}_\mathcal{H} \approx_\mathrm{pb} G_1' \setminus \mathcal{A}_\mathcal{H}$. Since synchronization does not apply to τ and $l \notin L$, we have that $(G_1 \parallel_L G_2) \setminus \mathcal{A}_\mathcal{H} \Longrightarrow (\bar{G}_1 \parallel_L G_2) \setminus \mathcal{A}_\mathcal{H} \xrightarrow{l}_\mathrm{a} (G_1' \parallel_L [1]G_2) \setminus \mathcal{A}_\mathcal{H}$ with $((F_1 \parallel_L F_2) \setminus \mathcal{A}_\mathcal{H}, (\bar{G}_1 \parallel_L G_2) \setminus \mathcal{A}_\mathcal{H}) \in \mathcal{B}$ and $((F_1' \parallel_L [1]F_2) \setminus \mathcal{A}_\mathcal{H}, (G_1' \parallel_L [1]G_2) \setminus \mathcal{A}_\mathcal{H}) \in \mathcal{B}$, where the right subprocess alternates between G_2 and $[1]G_2$ thus allowing the probabilistic transitions along $G_1 \setminus \mathcal{A}_\mathcal{H} \Longrightarrow \bar{G}_1 \setminus \mathcal{A}_\mathcal{H}$ to synchronize with the only one of $[1]G_2$.
- If $(F_1 \parallel_L F_2) \setminus \mathcal{A}_\mathcal{H} \xrightarrow{l}_\mathrm{a} ([1]F_1 \parallel_L F_2') \setminus \mathcal{A}_\mathcal{H}$ with $F_2 \xrightarrow{l}_\mathrm{a} F_2'$ and $l \notin L$, then the proof is similar to the one of the previous case.
- If $(F_1 \parallel_L F_2) \setminus \mathcal{A}_\mathcal{H} \xrightarrow{l}_\mathrm{a} (F_1' \parallel_L F_2') \setminus \mathcal{A}_\mathcal{H}$ with $F_i \xrightarrow{l}_\mathrm{a} F_i'$ for $i \in \{1, 2\}$ and $l \in L$, then $F_i \setminus \mathcal{A}_\mathcal{H} \xrightarrow{l}_\mathrm{a} F_i' \setminus \mathcal{A}_\mathcal{H}$ as $l \notin \mathcal{A}_\mathcal{H}$. From $F_i \setminus \mathcal{A}_\mathcal{H} \approx_\mathrm{pb} G_i \setminus \mathcal{A}_\mathcal{H}$ it follows that there exists $G_i \setminus \mathcal{A}_\mathcal{H} \Longrightarrow \bar{G}_i \setminus \mathcal{A}_\mathcal{H} \xrightarrow{l}_\mathrm{a} G_i' \setminus \mathcal{A}_\mathcal{H}$ such that $F_i \setminus \mathcal{A}_\mathcal{H} \approx_\mathrm{pb} \bar{G}_i \setminus \mathcal{A}_\mathcal{H}$ and $F_i' \setminus \mathcal{A}_\mathcal{H} \approx_\mathrm{pb} G_i' \setminus \mathcal{A}_\mathcal{H}$. Since synchronization does not apply to τ and $l \in L$, we have that $(G_1 \parallel_L G_2) \setminus \mathcal{A}_\mathcal{H} \Longrightarrow (\bar{G}_1 \parallel_L \bar{G}_2) \setminus \mathcal{A}_\mathcal{H} \xrightarrow{l}_\mathrm{a} (G_1' \parallel_L G_2') \setminus \mathcal{A}_\mathcal{H}$ with $((F_1 \parallel_L F_2) \setminus \mathcal{A}_\mathcal{H}, (\bar{G}_1 \parallel_L \bar{G}_2) \setminus \mathcal{A}_\mathcal{H}) \in \mathcal{B}$ and $((F_1' \parallel_L F_2') \setminus \mathcal{A}_\mathcal{H}, (G_1' \parallel_L G_2') \setminus \mathcal{A}_\mathcal{H}) \in \mathcal{B}$, where subprocess i alternates between G_i and $[1]G_i$ thus allowing the probabilistic transitions along $G_j \setminus \mathcal{A}_\mathcal{H} \Longrightarrow \bar{G}_i \setminus \mathcal{A}_\mathcal{H}$ for $j \neq i$ to synchronize with the only one of $[1]G_i$.
- If $(F_1 \parallel_L F_2) \setminus \mathcal{A}_\mathcal{H} \xrightarrow{\tau}_\mathrm{a} (F_1' \parallel_L [1]F_2) \setminus \mathcal{A}_\mathcal{H}$ with $F_1 \xrightarrow{\tau}_\mathrm{a} F_1'$, then $F_1 \setminus \mathcal{A}_\mathcal{H} \xrightarrow{\tau}_\mathrm{a} F_1' \setminus \mathcal{A}_\mathcal{H}$ as $\tau \notin \mathcal{A}_\mathcal{H}$. From $F_1 \setminus \mathcal{A}_\mathcal{H} \approx_\mathrm{pb} G_1 \setminus \mathcal{A}_\mathcal{H}$ it follows that either $F_1' \setminus \mathcal{A}_\mathcal{H} \approx_\mathrm{pb} G_1 \setminus \mathcal{A}_\mathcal{H}$, or there exists $G_1 \setminus \mathcal{A}_\mathcal{H} \Longrightarrow \bar{G}_1 \setminus \mathcal{A}_\mathcal{H} \xrightarrow{\tau}_\mathrm{a} G_1' \setminus \mathcal{A}_\mathcal{H}$ such that $F_1 \setminus \mathcal{A}_\mathcal{H} \approx_\mathrm{pb} \bar{G}_1 \setminus \mathcal{A}_\mathcal{H}$ and $F_1' \setminus \mathcal{A}_\mathcal{H} \approx_\mathrm{pb} G_1' \setminus \mathcal{A}_\mathcal{H}$. Since synchronization does not apply to τ, in the former subcase $(G_1 \parallel_L G_2) \setminus \mathcal{A}_\mathcal{H}$ is allowed to stay idle with $((F_1' \parallel_L [1]F_2) \setminus \mathcal{A}_\mathcal{H}, (G_1 \parallel_L G_2) \setminus \mathcal{A}_\mathcal{H}) \in \mathcal{B}$, while in the latter subcase $(G_1 \parallel_L G_2) \setminus \mathcal{A}_\mathcal{H} \Longrightarrow (\bar{G}_1 \parallel_L G_2) \setminus \mathcal{A}_\mathcal{H} \xrightarrow{\tau}_\mathrm{a} (G_1' \parallel_L [1]G_2) \setminus \mathcal{A}_\mathcal{H}$ with $((F_1 \parallel_L F_2) \setminus \mathcal{A}_\mathcal{H}, (\bar{G}_1 \parallel_L G_2) \setminus \mathcal{A}_\mathcal{H}) \in \mathcal{B}$ and $((F_1' \parallel_L [1]F_2) \setminus \mathcal{A}_\mathcal{H}, (G_1' \parallel_L [1]G_2) \setminus \mathcal{A}_\mathcal{H}) \in \mathcal{B}$, where the right subprocess alternates between G_2 and $[1]G_2$ thus allowing the probabilistic transitions along $G_1 \setminus \mathcal{A}_\mathcal{H} \Longrightarrow \bar{G}_1 \setminus \mathcal{A}_\mathcal{H}$ to synchronize with the only one of $[1]G_2$.
- If $(F_1 \parallel_L F_2) \setminus \mathcal{A}_\mathcal{H} \xrightarrow{\tau}_\mathrm{a} ([1]F_1 \parallel_L F_2') \setminus \mathcal{A}_\mathcal{H}$ with $F_2 \xrightarrow{\tau}_\mathrm{a} F_2'$, then the proof is similar to the one of the previous case.

As for probabilities, we reason like in the proof of the corresponding result for $\approx_\mathrm{pw}$. ∎

Theorem 9.2. *Let* $E_1, E_2 \in \mathbb{P}_\mathrm{n}$ *or* $E_1, E_2 \in \mathbb{P}_\mathrm{p}$, $E \in \mathbb{P}_\mathrm{pr}$, $\approx \in \{\approx_\mathrm{pw}, \approx_\mathrm{pb}\}$, *and* $\mathcal{P} \in \{\mathrm{SBSNNI}_\approx, \mathrm{P\_BNDC}_\approx, \mathrm{SBNDC}_\approx\}$. *Then:*

1. $E \in \mathcal{P} \Longrightarrow a\,.\,E \in \mathcal{P}$ *for all* $a \in \mathcal{A}_\mathcal{L} \cup \{\tau\}$, *when* $E \in \mathbb{P}_\mathrm{p}$.
2. $E_1, E_2 \in \mathcal{P} \Longrightarrow E_1 \parallel_L E_2 \in \mathcal{P}$ *for all* $L \subseteq \mathcal{A}_\mathcal{L}$ *if* $\mathcal{P} \in \{\mathrm{SBSNNI}_{\approx_\mathrm{pb}}, \mathrm{P\_BNDC}_{\approx_\mathrm{pb}}\}$ *or for all* $L \subseteq \mathcal{A} \setminus \{\tau\}$ *if* $\mathcal{P} \in \{\mathrm{SBSNNI}_{\approx_\mathrm{pw}}, \mathrm{P\_BNDC}_{\approx_\mathrm{pw}}, \mathrm{SBNDC}_{\approx_\mathrm{pw}}, \mathrm{SBNDC}_{\approx_\mathrm{pb}}\}$.
3. $E \in \mathcal{P} \Longrightarrow E \setminus L \in \mathcal{P}$ *for all* $L \subseteq \mathcal{A} \setminus \{\tau\}$.
4. $E \in \mathcal{P} \Longrightarrow E \,/\, L \in \mathcal{P}$ *for all* $L \subseteq \mathcal{A}_\mathcal{L}$.

Proof. We first prove the four results for SBSNNI$_\approx$, from which it will follow that they hold for P_BNDC$_\approx$ too by virtue of the forthcoming Theorem 9.3:

1. Given an arbitrary $E \in \mathbb{P}_{\rm p} \cap {\rm SBSNNI}_\approx$ and an arbitrary $a \in \mathcal{A}_\mathcal{L} \cup \{\tau\}$, from $E \setminus \mathcal{A}_\mathcal{H} \approx E / \mathcal{A}_\mathcal{H}$ we derive that $a \,.\, (E \setminus \mathcal{A}_\mathcal{H}) \approx a \,.\, (E / \mathcal{A}_\mathcal{H})$ because $\approx$ is a congruence with respect to action prefix by virtue of Lemma 9.2(1), from which it follows that $(a \,.\, E) \setminus \mathcal{A}_\mathcal{H} \approx (a \,.\, E) / \mathcal{A}_\mathcal{H}$, i.e., $a \,.\, E \in {\rm BSNNI}_\approx$, because $a \notin \mathcal{A}_\mathcal{H}$. To conclude the proof, it suffices to observe that all the processes reachable from $a \,.\, E$ after performing a are processes reachable from E, which are known to be BSNNI$_\approx$.

2. Given two arbitrary $E_1, E_2 \in \mathbb{P}_{\rm n}$ or $E_1, E_2 \in \mathbb{P}_{\rm p}$ such that $E_1, E_2 \in {\rm SBSNNI}_\approx$ and an arbitrary $L \subseteq \mathcal{A}_\mathcal{L}$, the result follows from Lemma 9.3(1) by taking F_1 identical to G_1 and F_2 identical to G_2.

3. Given an arbitrary $E \in {\rm SBSNNI}_\approx$ and an arbitrary $L \subseteq \mathcal{A} \setminus \{\tau\}$, the result follows from Lemma 9.3(2) by taking F identical to G – which will be denoted by E' – because:

   - $(E' \setminus L) \setminus \mathcal{A}_\mathcal{H} \approx (E' \setminus \mathcal{A}_\mathcal{H}) \setminus L$ as the order in which restriction sets are considered is unimportant.
   - $(E' \setminus \mathcal{A}_\mathcal{H}) \setminus L \approx (E' / \mathcal{A}_\mathcal{H}) \setminus L$ because $E' \setminus \mathcal{A}_\mathcal{H} \approx E' / \mathcal{A}_\mathcal{H}$ – as $E \in {\rm SBSNNI}_\approx$ and $E' \in \mathit{reach}(E)$ – and $\approx$ is a congruence with respect to the restriction operator due to Lemma 9.2(3).
   - $(E' / \mathcal{A}_\mathcal{H}) \setminus L \approx (E' \setminus L) / \mathcal{A}_\mathcal{H}$ as shown in Lemma 9.3(2).
   - From the transitivity of $\approx$ we obtain that $(E' \setminus L) \setminus \mathcal{A}_\mathcal{H} \approx (E' \setminus L) / \mathcal{A}_\mathcal{H}$.

4. Given an arbitrary $E \in {\rm SBSNNI}_\approx$ and an arbitrary $L \subseteq \mathcal{A}_\mathcal{L}$, for every $E' \in \mathit{reach}(E)$ it holds that $E' \setminus \mathcal{A}_\mathcal{H} \approx E' / \mathcal{A}_\mathcal{H}$, from which we derive that $(E' \setminus \mathcal{A}_\mathcal{H}) / L \approx (E'/\mathcal{A}_\mathcal{H}) / L$ because $\approx$ is a congruence with respect to the hiding operator due to Lemma 9.2(4). Since $L \cap \mathcal{A}_\mathcal{H} = \emptyset$, we have that $(E' \setminus \mathcal{A}_\mathcal{H}) / L$ is isomorphic to $(E' / L) \setminus \mathcal{A}_\mathcal{H}$ and $(E' / \mathcal{A}_\mathcal{H}) / L$ is isomorphic to $(E' / L) / \mathcal{A}_\mathcal{H}$, hence $(E' / L) \setminus \mathcal{A}_\mathcal{H} \approx (E' / L) / \mathcal{A}_\mathcal{H}$, i.e., E' / L is BSNNI$_\approx$.

We then prove the four results for SBNDC$_\approx$:

1. Given an arbitrary $E \in \mathbb{P}_{\rm p} \cap {\rm SBNDC}_\approx$ and an arbitrary $a \in \mathcal{A}_\mathcal{L} \cup \{\tau\}$, it trivially holds that $a \,.\, E \in {\rm SBNDC}_\approx$ because a is not high and all the processes reachable from $a \,.\, E$ after performing a are processes reachable from E, which is known to be SBNDC$_\approx$.

2. Given two arbitrary $E_1, E_2 \in \mathbb{P}_{\rm n}$ or $E_1, E_2 \in \mathbb{P}_{\rm p}$ such that $E_1, E_2 \in {\rm SBNDC}_\approx$ and an arbitrary $L \subseteq \mathcal{A} \setminus \{\tau\}$, the result follows from Lemma 9.3(3) as can be seen by observing that whenever $E'_1 \parallel_L E'_2 \xrightarrow{h}_{\rm a} E''_1 \parallel_L E''_2$ for $E'_1 \parallel_L E'_2 \in \mathit{reach}(E_1 \parallel_L E_2)$:

   - If $E'_1 \xrightarrow{h}_{\rm a} E''_1$, $E''_2 = E'_2$ (hence $E'_2 \setminus \mathcal{A}_\mathcal{H} \approx E''_2 \setminus \mathcal{A}_\mathcal{H}$), and $h \notin L$, then from $E_1 \in {\rm SBNDC}_\approx$ it follows that $E'_1 \setminus \mathcal{A}_\mathcal{H} \approx E''_1 \setminus \mathcal{A}_\mathcal{H}$, which in turn entails that $(E'_1 \parallel_L E'_2) \setminus \mathcal{A}_\mathcal{H} \approx (E''_1 \parallel_L E''_2) \setminus \mathcal{A}_\mathcal{H}$ because $\approx$ is a congruence with respect to the parallel composition operator due to Lemma 9.2(2) and restriction distributes over parallel composition.
   - If $E'_2 \xrightarrow{h}_{\rm a} E''_2$, $E''_1 = E'_1$, and $h \notin L$, then we reason like in the previous case.

- If $E_1' \xrightarrow{h}_{\rm a} E_1''$, $E_2' \xrightarrow{h}_{\rm a} E_2''$, and $h \in L$, then from $E_1, E_2 \in {\rm SBNDC}_{\approx}$ it follows that $E_1' \setminus \mathcal{A}_{\mathcal{H}} \approx E_1'' \setminus \mathcal{A}_{\mathcal{H}}$ and $E_2' \setminus \mathcal{A}_{\mathcal{H}} \approx E_2'' \setminus \mathcal{A}_{\mathcal{H}}$, which in turn entail that $(E_1' \parallel_L E_2') \setminus \mathcal{A}_{\mathcal{H}} \approx (E_1'' \parallel_L E_2'') \setminus \mathcal{A}_{\mathcal{H}}$ because $\approx$ is a congruence with respect to the parallel composition operator due to Lemma 9.2(2) and restriction distributes over parallel composition.

3. Given an arbitrary $E \in {\rm SBNDC}_{\approx}$ and an arbitrary $L \subseteq \mathcal{A} \setminus \{\tau\}$, for every $E' \in \mathit{reach}(E)$ and for every E'' such that $E' \xrightarrow{h}_{\rm a} E''$ it holds that $E' \setminus \mathcal{A}_{\mathcal{H}} \approx E'' \setminus \mathcal{A}_{\mathcal{H}}$, from which we derive that $(E' \setminus \mathcal{A}_{\mathcal{H}}) \setminus L \approx (E'' \setminus \mathcal{A}_{\mathcal{H}}) \setminus L$ because $\approx$ is a congruence with respect to the restriction operator due to Lemma 9.2(3). Since $(E' \setminus \mathcal{A}_{\mathcal{H}}) \setminus L$ is isomorphic to $(E' \setminus L) \setminus \mathcal{A}_{\mathcal{H}}$ and $(E'' \setminus \mathcal{A}_{\mathcal{H}}) \setminus L$ is isomorphic to $(E'' \setminus L) \setminus \mathcal{A}_{\mathcal{H}}$, we have that $(E' \setminus L) \setminus \mathcal{A}_{\mathcal{H}} \approx (E'' \setminus L) \setminus \mathcal{A}_{\mathcal{H}}$.

4. Given an arbitrary $E \in {\rm SBNDC}_{\approx}$ and an arbitrary $L \subseteq \mathcal{A}_{\mathcal{L}}$, for every $E' \in \mathit{reach}(E)$ and for every E'' such that $E' \xrightarrow{h}_{\rm a} E''$ it holds that $E' \setminus \mathcal{A}_{\mathcal{H}} \approx E'' \setminus \mathcal{A}_{\mathcal{H}}$, from which we derive that $(E' \setminus \mathcal{A}_{\mathcal{H}}) / L \approx (E'' \setminus \mathcal{A}_{\mathcal{H}}) / L$ because $\approx$ is a congruence with respect to the hiding operator due to Lemma 9.2(4). Since $L \cap \mathcal{A}_{\mathcal{H}} = \emptyset$, we have that $(E' \setminus \mathcal{A}_{\mathcal{H}}) / L$ is isomorphic to $(E' / L) \setminus \mathcal{A}_{\mathcal{H}}$ and $(E'' \setminus \mathcal{A}_{\mathcal{H}}) / L$ is isomorphic to $(E'' / L) \setminus \mathcal{A}_{\mathcal{H}}$, hence $(E' / L) \setminus \mathcal{A}_{\mathcal{H}} \approx (E'' / L) \setminus \mathcal{A}_{\mathcal{H}}$. ■

As far as parallel composition is concerned, the compositionality of ${\rm SBSNNI}_{\approx_{\rm pb}}$ holds only for all $L \subseteq \mathcal{A}_{\mathcal{L}}$. For instance, both $E_1 = h.\underline{0} + l_1.\underline{0} + \tau.\underline{0}$ and $E_2 = h.\underline{0} + l_2.\underline{0} + \tau.\underline{0}$ are ${\rm SBSNNI}_{\approx_{\rm pb}}$, but $E_1 \parallel_{\{h\}} E_2$ is not because the transition $(E_1 \parallel_{\{h\}} E_2) / \mathcal{A}_{\mathcal{H}} \xrightarrow{\tau}_{\rm a} ([1]\underline{0} \parallel_{\{h\}} [1]\underline{0}) / \mathcal{A}_{\mathcal{H}}$ arising from the synchronization between the two h-actions cannot be matched by $(E_1 \parallel_{\{h\}} E_2) \setminus \mathcal{A}_{\mathcal{H}}$ in the probabilistic branching bisimulation game. As a matter of fact, the only two possibilities are $(E_1 \parallel_{\{h\}} E_2) \setminus \mathcal{A}_{\mathcal{H}} \Longrightarrow (E_1 \parallel_{\{h\}} E_2) \setminus \mathcal{A}_{\mathcal{H}} \xrightarrow{\tau}_{\rm a} ([1]\underline{0} \parallel_{\{h\}} [1]E_2) \setminus \mathcal{A}_{\mathcal{H}} \xrightarrow{1}_{\rm p} (\underline{0} \parallel_{\{h\}} E_2) \setminus \mathcal{A}_{\mathcal{H}} \xrightarrow{\tau}_{\rm a} ([1]\underline{0} \parallel_{\{h\}} [1]\underline{0}) \setminus \mathcal{A}_{\mathcal{H}}$ and $(E_1 \parallel_{\{h\}} E_2) \setminus \mathcal{A}_{\mathcal{H}} \Longrightarrow (E_1 \parallel_{\{h\}} E_2) \setminus \mathcal{A}_{\mathcal{H}} \xrightarrow{\tau}_{\rm a} ([1]E_1 \parallel_{\{h\}} [1]\underline{0}) \setminus \mathcal{A}_{\mathcal{H}} \xrightarrow{1}_{\rm p} (E_1 \parallel_{\{h\}} \underline{0}) \setminus \mathcal{A}_{\mathcal{H}} \xrightarrow{\tau}_{\rm a} ([1]\underline{0} \parallel_{\{h\}} [1]\underline{0}) \setminus \mathcal{A}_{\mathcal{H}}$ but neither $([1]\underline{0} \parallel_{\{h\}} [1]E_2) \setminus \mathcal{A}_{\mathcal{H}}$ nor $([1]E_1 \parallel_{\{h\}} [1]\underline{0}) \setminus \mathcal{A}_{\mathcal{H}}$ is $\approx_{\rm pb}$-equivalent to $(E_1 \parallel_{\{h\}} E_2) \setminus \mathcal{A}_{\mathcal{H}}$ when $l_1 \neq l_2$. Note that $(E_1 \parallel_{\{h\}} E_2)/\mathcal{A}_{\mathcal{H}} \approx_{\rm pw} (E_1 \parallel_{\{h\}} E_2) \setminus \mathcal{A}_{\mathcal{H}}$ because $(E_1 \parallel_{\{h\}} E_2)/\mathcal{A}_{\mathcal{H}} \xrightarrow{\tau}_{\rm a} ([1]\underline{0} \parallel_{\{h\}} [1]\underline{0}) / \mathcal{A}_{\mathcal{H}}$ is matched by $(E_1 \parallel_{\{h\}} E_2) \setminus \mathcal{A}_{\mathcal{H}} \Longrightarrow ([1]\underline{0} \parallel_{\{h\}} [1]\underline{0}) \setminus \mathcal{A}_{\mathcal{H}}$. Similar to the previous chapter, it is not only a matter of the higher discriminating power of $\approx_{\rm pb}$ with respect to $\approx_{\rm pw}$. If we used the CCS parallel composition operator [112], which turns the synchronization of two actions into τ thus combining communication with hiding, then the parallel composition of E_1 and E_2 with restriction on $\mathcal{A}_{\mathcal{H}}$ would be able to respond, in the probabilistic branching bisimulation game, with a single τ-transition reaching the parallel composition of $[1]\underline{0}$ and $[1]\underline{0}$ with restriction on $\mathcal{A}_{\mathcal{H}}$.

9.2.2 Taxonomy of Security Properties

Similar to the nondeterministic setting of the previous chapter, the noninterference properties in Definition 9.6 turn out to be increasingly finer. This holds both for those based on $\approx_{\rm pw}$ and for those based on $\approx_{\rm pb}$.

Part of the proof of the forthcoming Theorem 9.3 relies on the bisimulation-up-to technique [131] and requires introducing probabilistic variants of up-to weak [112] and branching [75] bisimulations. In doing so in our quantitative setting, we have to take into account some technicalities mentioned in [44, 91, 79]. In particular, given $\approx \in \{\approx_{\rm pw}, \approx_{\rm pb}\}$ and a related bisimulation $\mathcal{B}$, we cannot consider the relation composition $\approx \mathcal{B} \approx$ like in the fully nondeterministic case as it may not be transitive and this would not make it possible to work with equivalence

classes for the probabilistic part. Rather we have to consider $(\mathcal{B} \cup \mathcal{B}^{-1} \cup \approx)^+ = \bigcup_{n=1}^{\infty} (\mathcal{B} \cup \mathcal{B}^{-1} \cup \approx)^n$ to ensure transitivity in addition to reflexivity and symmetry, where $\mathcal{B}^{-1}$ is the inverse of $\mathcal{B}$ and $\mathcal{B}$ is no longer required to be an equivalence relation thus avoiding redundant information in it. We remind that $(\mathcal{B} \cup \mathcal{B}^{-1} \cup \approx)^n$ for $n > 1$ is the composition of relations $(\mathcal{B} \cup \mathcal{B}^{-1} \cup \approx)^{n-1}$ and $\mathcal{B} \cup \mathcal{B}^{-1} \cup \approx$.

Definition 9.7. *A relation $\mathcal{B}$ over $\mathbb{P}_{\rm pr}$ is a* weak probabilistic bisimulation up to $\approx_{\rm pw}$ *iff, whenever $(E_1, E_2) \in \mathcal{B}$, then:*

- *For each $E_1 \stackrel{a}{\Longrightarrow} E_1'$ there exists $E_2 \stackrel{\hat{a}}{\Longrightarrow} E_2'$ such that $(E_1', E_2') \in (\mathcal{B} \cup \mathcal{B}^{-1} \cup \approx_{\rm pw})^+$, and vice versa.*
- *$prob(E_1, C) = prob(E_2, C)$ for all equivalence classes $C \in \mathbb{P}_{\rm pr}/(\mathcal{B} \cup \mathcal{B}^{-1} \cup \approx_{\rm pw})^+$.* ■

Definition 9.8. *A relation $\mathcal{B}$ over $\mathbb{P}_{\rm pr}$ is a* probabilistic branching bisimulation up to $\approx_{\rm pb}$ *iff, whenever $(E_1,E_2) \in \mathcal{B}$, then:*

- *For each $E_1 \Longrightarrow \bar{E}_1 \stackrel{a}{\longrightarrow}_{\rm a} E_1'$ with $E_1 \approx_{\rm pb} \bar{E}_1$:*
  - *either $a = \tau$ and $\bar{E}_1 \approx_{\rm pb} E_1'$;*
  - *or there exists $E_2 \Longrightarrow \bar{E}_2 \stackrel{a}{\longrightarrow}_{\rm a} E_2'$ such that $(\bar{E}_1, \bar{E}_2) \in (\mathcal{B} \cup \mathcal{B}^{-1} \cup \approx_{\rm pb})^+$ and $(E_1', E_2') \in (\mathcal{B} \cup \mathcal{B}^{-1} \cup \approx_{\rm pb})^+$;*

  and vice versa.
- *$prob(E_1, C) = prob(E_2, C)$ for all equivalence classes $C \in \mathbb{P}_{\rm pr}/(\mathcal{B} \cup \mathcal{B}^{-1} \cup \approx_{\rm pb})^+$.* ■

In the second definition, in the case that $a = \tau$ and $\bar{E}_1 \approx_{\rm pb} E_1'$ it holds that $E_1' \approx_{\rm pb} \bar{E}_1 \approx_{\rm pb} E_1 \; \mathcal{B} \; E_2$, i.e., $(E_1', E_2) \in (\mathcal{B} \cup \mathcal{B}^{-1} \cup \approx_{\rm pb})^+$, because $\approx_{\rm pb}$ is symmetric. We now prove that the two previous notions are correct, i.e., they imply the respective bisimilarities.

Proposition 9.1. *Let $E_1, E_2 \in \mathbb{P}_{\rm pr}$ and $\mathcal{B}$ be a weak probabilistic bisimulation up to $\approx_{\rm pw}$. If $(E_1, E_2) \in \mathcal{B}$ then $E_1 \approx_{\rm pw} E_2$.*

Proof. It suffices to prove that the equivalence relation $(\mathcal{B}' \cup \approx_{\rm pw})^+$ is a weak probabilistic bisimulation, where $\mathcal{B}' = \mathcal{B} \cup \mathcal{B}^{-1}$. Given $(E_1, E_2) \in (\mathcal{B}' \cup \approx_{\rm pw})^+$ and considering the smallest $n \in \mathbb{N}_{>0}$ for which $(E_1, E_2) \in (\mathcal{B}' \cup \approx_{\rm pw})^n$, we proceed by induction on n:

- If $n = 1$ then there are two cases:
  - Let $(E_1, E_2) \in \mathcal{B}'$. If $E_1 \stackrel{a}{\longrightarrow}_{\rm a} E_1'$, hence $E_1 \stackrel{a}{\Longrightarrow} E_1'$, then from the fact that $\mathcal{B}'$ is a weak probabilistic bisimulation up to $\approx_{\rm pw}$ it follows that there exists $E_2 \stackrel{\hat{a}}{\Longrightarrow} E_2'$ such that $(E_1', E_2') \in (\mathcal{B}' \cup \approx_{\rm pw})^+$. Moreover, since $\mathcal{B}'$ is a weak probabilistic bisimulation up to $\approx_{\rm pw}$, we have that $prob(E_1, C) = prob(E_2, C)$ for all $C \in \mathbb{P}_{\rm pr}/(\mathcal{B}' \cup \approx_{\rm pw})^+$.
  - Let $E_1 \approx_{\rm pw} E_2$. If $E_1 \stackrel{a}{\longrightarrow}_{\rm a} E_1'$ then there exists $E_2 \stackrel{\hat{a}}{\Longrightarrow} E_2'$ such that $E_1' \approx_{\rm pw} E_2'$, hence $(E_1', E_2') \in (\mathcal{B}' \cup \approx_{\rm pw})^+$ because $\approx_{\rm pw} \subseteq (\mathcal{B}' \cup \approx_{\rm pw})^+$. Moreover, since $\approx_{\rm pw} \subseteq (\mathcal{B}' \cup \approx_{\rm pw})^+$ implies that every equivalence class of $(\mathcal{B}' \cup \approx_{\rm pw})^+$ is the union of some equivalence classes of $\approx_{\rm pw}$, we have that $prob(E_1, C) = prob(E_2, C)$ for all $C \in \mathbb{P}_{\rm pr}/(\mathcal{B}' \cup \approx_{\rm pw})^+$.

- If $n > 1$ then from $(E_1, E_2) \in (\mathcal{B}' \cup \approx_{\rm pw})^n$ and the minimality of n it follows that there exists $E \in \mathbb{P}_{\rm pr}$ such that $(E_1, E) \in (\mathcal{B}' \cup \approx_{\rm pw})^{n-1}$ and $(E, E_2) \in (\mathcal{B}' \cup \approx_{\rm pw})$. If $E_1 \stackrel{a}{\longrightarrow}_{\rm a} E_1'$ then by the induction hypothesis applied to $(E_1, E) \in (\mathcal{B}' \cup \approx_{\rm pw})^{n-1}$ there exists $E \stackrel{\hat{a}}{\Longrightarrow} E'$ such that $(E_1', E') \in (\mathcal{B}' \cup \approx_{\rm pw})^+$. Therefore by the induction hypothesis applied to $(E, E_2) \in (\mathcal{B}' \cup \approx_{\rm pw})$ there exists $E_2 \stackrel{\hat{a}}{\Longrightarrow} E_2'$ such that $(E', E_2') \in (\mathcal{B}' \cup \approx_{\rm pw})^+$, where $(E_1', E_2') \in (\mathcal{B}' \cup \approx_{\rm pw})^+$ by transitivity. Moreover, from the induction hypothesis applied to $(E_1, E) \in (\mathcal{B}' \cup \approx_{\rm pw})^{n-1}$ and $(E, E_2) \in (\mathcal{B}' \cup \approx_{\rm pw})$ it follows that $prob(E_1, C) = prob(E, C) = prob(E_2, C)$ for all $C \in \mathbb{P}_{\rm pr}/(\mathcal{B}' \cup \approx_{\rm pw})^+$. ■

Proposition 9.2. *Let $E_1, E_2 \in \mathbb{P}_{\rm pr}$ and $\mathcal{B}$ be a probabilistic branching bisimulation up to $\approx_{\rm pb}$. If $(E_1, E_2) \in \mathcal{B}$ then $E_1 \approx_{\rm pb} E_2$.*

Proof. It suffices to prove that the equivalence relation $(\mathcal{B}' \cup \approx_{\rm pb})^+$ is a probabilistic branching bisimulation, where $\mathcal{B}' = \mathcal{B} \cup \mathcal{B}^{-1}$. Given $(E_1, E_2) \in (\mathcal{B}' \cup \approx_{\rm pb})^+$ and considering the smallest $n \in \mathbb{N}_{>0}$ for which $(E_1, E_2) \in (\mathcal{B}' \cup \approx_{\rm pb})^n$, we proceed by induction on n:

- If $n = 1$ then there are two cases:
  - Let $(E_1, E_2) \in \mathcal{B}'$. If $E_1 \stackrel{a}{\longrightarrow}_{\rm a} E_1'$, hence $E_1 \Longrightarrow E_1 \stackrel{a}{\longrightarrow}_{\rm a} E_1'$, then from the fact that $\mathcal{B}'$ is a probabilistic branching bisimulation up to $\approx_{\rm pb}$ it follows that there are two subcases:
    - If $a = \tau$ and $E_1 \approx_{\rm pb} E_1'$, hence $(E_1', E_1) \in (\mathcal{B}' \cup \approx_{\rm pb})^+$ by symmetry, from $(E_1, E_2) \in (\mathcal{B}' \cup \approx_{\rm pb})^+$ it follows that $(E_1', E_2) \in (\mathcal{B}' \cup \approx_{\rm pb})^+$ by transitivity.
    - If there exists $E_2 \Longrightarrow \bar{E}_2 \stackrel{a}{\longrightarrow}_{\rm a} E_2'$ such that $(E_1, \bar{E}_2) \in (\mathcal{B}' \cup \approx_{\rm pb})^+$ and $(E_1', E_2') \in (\mathcal{B}' \cup \approx_{\rm pb})^+$, then we are done.

    Moreover, since $\mathcal{B}'$ is a probabilistic branching bisimulation up to $\approx_{\rm pb}$, we have that $prob(E_1, C) = prob(E_2, C)$ for all $C \in \mathbb{P}_{\rm pr}/(\mathcal{B}' \cup \approx_{\rm pb})^+$.
  - Let $E_1 \approx_{\rm pb} E_2$. If $E_1 \stackrel{a}{\longrightarrow}_{\rm a} E_1'$ then there are two subcases:
    - If $a = \tau$ and $E_1' \approx_{\rm pb} E_2$, then $(E_1', E_2) \in (\mathcal{B}' \cup \approx_{\rm pb})^+$ because $\approx_{\rm pb} \subseteq (\mathcal{B}' \cup \approx_{\rm pb})^+$.
    - If there exists $E_2 \Longrightarrow \bar{E}_2 \stackrel{a}{\longrightarrow}_{\rm a} E_2'$ such that $E_1 \approx_{\rm pb} \bar{E}_2$ and $E_1' \approx_{\rm pb} E_2'$, then $(E_1, \bar{E}_2) \in (\mathcal{B}' \cup \approx_{\rm pb})^+$ and $(E_1', E_2') \in (\mathcal{B}' \cup \approx_{\rm pb})^+$ because $\approx_{\rm pb} \subseteq (\mathcal{B}' \cup \approx_{\rm pb})^+$.

    Moreover, since $\approx_{\rm pb} \subseteq (\mathcal{B}' \cup \approx_{\rm pb})^+$ implies that every equivalence class of $(\mathcal{B}' \cup \approx_{\rm pb})^+$ is the union of some equivalence classes of $\approx_{\rm pb}$, we have that $prob(E_1, C) = prob(E_2, C)$ for all $C \in \mathbb{P}_{\rm pr}/(\mathcal{B}' \cup \approx_{\rm pb})^+$.
- If $n > 1$ then from $(E_1, E_2) \in (\mathcal{B}' \cup \approx_{\rm pb})^n$ and the minimality of n it follows that there exists $E \in \mathbb{P}_{\rm pr}$ such that $(E_1, E) \in (\mathcal{B}' \cup \approx_{\rm pb})^{n-1}$ and $(E, E_2) \in (\mathcal{B}' \cup \approx_{\rm pb})$. If $E_1 \stackrel{a}{\longrightarrow}_{\rm a} E_1'$ then by the induction hypothesis applied to $(E_1, E) \in (\mathcal{B}' \cup \approx_{\rm pb})^{n-1}$ there are two cases:
  - If $a = \tau$ and $(E_1', E) \in (\mathcal{B}' \cup \approx_{\rm pb})^+$, then from $(E, E_2) \in (\mathcal{B}' \cup \approx_{\rm pb})$ it follows that $(E_1', E_2) \in (\mathcal{B}' \cup \approx_{\rm pb})^+$ by transitivity.
  - If there exists $E \Longrightarrow \bar{E} \stackrel{a}{\longrightarrow}_{\rm a} E'$ such that $(E_1, \bar{E}) \in (\mathcal{B}' \cup \approx_{\rm pb})^+$ and $(E_1', E') \in (\mathcal{B}' \cup \approx_{\rm pb})^+$, then by the induction hypothesis applied to $(E, E_2) \in (\mathcal{B}' \cup \approx_{\rm pb})$ there are two subcases:

- If $a = \tau$ and $(E', E_2) \in (\mathcal{B}' \cup \approx_{\rm pb})^+$, then from $(E'_1, E') \in (\mathcal{B}' \cup \approx_{\rm pb})^+$ it follows that $(E'_1, E_2) \in (\mathcal{B}' \cup \approx_{\rm pb})^+$ by transitivity.
- If there exists $E_2 \Longrightarrow \bar{E}_2 \xrightarrow{a}_{\rm a} E'_2$ such that $(\bar{E}, \bar{E}_2) \in (\mathcal{B}' \cup \approx_{\rm pb})^+$ and $(E', E'_2) \in (\mathcal{B}' \cup \approx_{\rm pb})^+$, then from $(E_1, \bar{E}) \in (\mathcal{B}' \cup \approx_{\rm pb})^+$ and $(E'_1, E') \in (\mathcal{B}' \cup \approx_{\rm pb})^+$ it follows that $(E_1, \bar{E}_2) \in (\mathcal{B}' \cup \approx_{\rm pb})^+$ and $(E'_1, E'_2) \in (\mathcal{B}' \cup \approx_{\rm pb})^+$ by transitivity.

Moreover, from the induction hypothesis applied to $(E_1, E) \in (\mathcal{B}' \cup \approx_{\rm pb})^{n-1}$ and $(E, E_2) \in (\mathcal{B}' \cup \approx_{\rm pb})$ it follows that $prob(E_1, C) = prob(E, C) = prob(E_2, C)$ for all $C \in \mathbb{P}_{\rm pr} / (\mathcal{B}' \cup \approx_{\rm pb})^+$. ∎

Before presenting the taxonomy, we prove some further ancillary results about parallel composition, restriction, and hiding under $\text{SBSNNI}_\approx$ and $\text{SBNDC}_\approx$.

Lemma 9.4. *Let $E, E_1, E_2 \in \mathbb{P}_{\rm pr}$ and $\approx \in \{\approx_{\rm pw}, \approx_{\rm pb}\}$. Then:*

1. *If $E \in \text{SBNDC}_\approx$, $E' \in reach(E)$, and $E' / \mathcal{A}_\mathcal{H} \Longrightarrow E'' / \mathcal{A}_\mathcal{H}$, then $E' \setminus \mathcal{A}_\mathcal{H} \Longrightarrow \hat{E}'' \setminus \mathcal{A}_\mathcal{H}$ with $E'' \setminus \mathcal{A}_\mathcal{H} \approx \hat{E}'' \setminus \mathcal{A}_\mathcal{H}$.*
2. *If $E_1, E_2 \in \text{SBNDC}_\approx$ and $E_1 \setminus \mathcal{A}_\mathcal{H} \approx E_2 \setminus \mathcal{A}_\mathcal{H}$, then $E_1 / \mathcal{A}_\mathcal{H} \approx E_2 / \mathcal{A}_\mathcal{H}$.*
3. *If $E_2 \in \text{SBSNNI}_\approx$ and $L \subseteq \mathcal{A}_\mathcal{H}$, then $E'_1 \setminus \mathcal{A}_\mathcal{H} \approx ((E'_2 \parallel_L F) / L) \setminus \mathcal{A}_\mathcal{H}$ for all $F \in \mathbb{P}_{\rm pr}$ having only actions in $\mathcal{A}_\mathcal{H}$ and for all $E'_1 \in reach(E_1)$ and $E'_2 \in reach(E_2)$ such that $E'_1 \setminus \mathcal{A}_\mathcal{H} \approx E'_2 / \mathcal{A}_\mathcal{H}$, when $E'_2, F \in \mathbb{P}_{\rm n}$ or $E'_2, F \in \mathbb{P}_{\rm p}$.*

Proof. We first prove the three results for the $\approx_{\rm pw}$-based properties:

1. We proceed by induction on the number $n \in \mathbb{N}$ of τ- and probabilistic transitions along $E' / \mathcal{A}_\mathcal{H} \Longrightarrow E'' / \mathcal{A}_\mathcal{H}$:
   - If $n = 0$ then $E' / \mathcal{A}_\mathcal{H}$ stays idle and $E'' / \mathcal{A}_\mathcal{H}$ is $E' / \mathcal{A}_\mathcal{H}$. Likewise, $E' \setminus \mathcal{A}_\mathcal{H}$ can stay idle, i.e., $E' \setminus \mathcal{A}_\mathcal{H} \Longrightarrow E' \setminus \mathcal{A}_\mathcal{H}$, with $E' \setminus \mathcal{A}_\mathcal{H} \approx_{\rm pw} E' \setminus \mathcal{A}_\mathcal{H}$ as $\approx_{\rm pw}$ is reflexive.
   - Let $n > 0$ and $E'_0 / \mathcal{A}_\mathcal{H} \Longrightarrow E'_{n-1} / \mathcal{A}_\mathcal{H} \xrightarrow{\tau}_{\rm a} E'_n / \mathcal{A}_\mathcal{H}$ or $E'_0 / \mathcal{A}_\mathcal{H} \Longrightarrow E'_{n-1} / \mathcal{A}_\mathcal{H} \xrightarrow{p}_{\rm p} E'_n / \mathcal{A}_\mathcal{H}$ where E'_0 is E' and E'_n is E''. From the induction hypothesis it follows that $E' \setminus \mathcal{A}_\mathcal{H} \Longrightarrow \hat{E}'_{n-1} \setminus \mathcal{A}_\mathcal{H}$ with $E'_{n-1} \setminus \mathcal{A}_\mathcal{H} \approx_{\rm pw} \hat{E}'_{n-1} \setminus \mathcal{A}_\mathcal{H}$. As far as the n-th transition is concerned, which is $E'_{n-1} / \mathcal{A}_\mathcal{H} \xrightarrow{\tau}_{\rm a} E'_n / \mathcal{A}_\mathcal{H}$ or $E'_{n-1} / \mathcal{A}_\mathcal{H} \xrightarrow{p}_{\rm p} E'_n / \mathcal{A}_\mathcal{H}$, there are three cases depending on whether it is originated from $E'_{n-1} \xrightarrow{\tau}_{\rm a} E'_n$, $E'_{n-1} \xrightarrow{h}_{\rm a} E'_n$, or $E'_{n-1} \xrightarrow{p}_{\rm p} E'_n$:
     - If $E'_{n-1} \xrightarrow{\tau}_{\rm a} E'_n$ then $E'_{n-1} \setminus \mathcal{A}_\mathcal{H} \xrightarrow{\tau}_{\rm a} E'_n \setminus \mathcal{A}_\mathcal{H}$. Since $E'_{n-1} \setminus \mathcal{A}_\mathcal{H} \approx_{\rm pw} \hat{E}'_{n-1} \setminus \mathcal{A}_\mathcal{H}$, there exists $\hat{E}'_{n-1} \setminus \mathcal{A}_\mathcal{H} \Longrightarrow \hat{E}'_n \setminus \mathcal{A}_\mathcal{H}$ such that $E'_n \setminus \mathcal{A}_\mathcal{H} \approx_{\rm pw} \hat{E}'_n \setminus \mathcal{A}_\mathcal{H}$. Therefore $E' \setminus \mathcal{A}_\mathcal{H} \Longrightarrow \hat{E}'_n \setminus \mathcal{A}_\mathcal{H}$ with $E'' \setminus \mathcal{A}_\mathcal{H} \approx_{\rm pw} \hat{E}'_n \setminus \mathcal{A}_\mathcal{H}$.
     - If $E'_{n-1} \xrightarrow{h}_{\rm a} E'_n$ then from $E \in \text{SBNDC}_{\approx_{\rm pw}}$ it follows that $E'_{n-1} \setminus \mathcal{A}_\mathcal{H} \approx_{\rm pw} E'_n \setminus \mathcal{A}_\mathcal{H}$. Since $E'_{n-1} \setminus \mathcal{A}_\mathcal{H} \approx_{\rm pw} \hat{E}'_{n-1} \setminus \mathcal{A}_\mathcal{H}$ and $\approx_{\rm pw}$ is symmetric and transitive, we obtain $E'_n \setminus \mathcal{A}_\mathcal{H} \approx_{\rm pw} \hat{E}'_{n-1} \setminus \mathcal{A}_\mathcal{H}$. Therefore $E' \setminus \mathcal{A}_\mathcal{H} \Longrightarrow \hat{E}'_{n-1} \setminus \mathcal{A}_\mathcal{H}$ with $E'' \setminus \mathcal{A}_\mathcal{H} \approx_{\rm pw} \hat{E}'_{n-1} \setminus \mathcal{A}_\mathcal{H}$.

– If $E'_{n-1} \xrightarrow{p}_{\rm p} E'_n$ then from the fact that $E'_{n-1} \setminus \mathcal{A}_\mathcal{H} \approx_{\rm pw} \hat{E}'_{n-1} \setminus \mathcal{A}_\mathcal{H}$ it follows that $prob(E'_{n-1} \setminus \mathcal{A}_\mathcal{H}, C) = prob(\hat{E}'_{n-1} \setminus \mathcal{A}_\mathcal{H}, C)$ for all $C \in \mathbb{P}_{\rm pr}/\approx_{\rm pw}$ and hence there exists $\hat{E}'_{n-1} \setminus \mathcal{A}_\mathcal{H} \xrightarrow{q}_{\rm p} \hat{E}'_n \setminus \mathcal{A}_\mathcal{H}$ for some $q \in \mathbb{R}_{]0,1]}$ such that $\hat{E}'_n \setminus \mathcal{A}_\mathcal{H} \in [E'_n \setminus \mathcal{A}_\mathcal{H}]_{\approx_{\rm pw}}$. Therefore $E' \setminus \mathcal{A}_\mathcal{H} \Longrightarrow \hat{E}'_n \setminus \mathcal{A}_\mathcal{H}$ with $E'' \setminus \mathcal{A}_\mathcal{H} \approx_{\rm pw} \hat{E}'_n \setminus \mathcal{A}_\mathcal{H}$.

2. Let $\mathcal{B}$ be an equivalence relation containing all the pairs of processes that have to be shown to be $\approx_{\rm pw}$-equivalent according to the considered result. Starting from $(E_1 / \mathcal{A}_\mathcal{H}, E_2 / \mathcal{A}_\mathcal{H}) \in \mathcal{B}$, so that $E_1 \setminus \mathcal{A}_\mathcal{H} \approx_{\rm pw} E_2 \setminus \mathcal{A}_\mathcal{H}$, there are three cases for action transitions based on the operational semantic rules in Table 9.1:

   - If $E_1 / \mathcal{A}_\mathcal{H} \xrightarrow{\tau}_{\rm a} E'_1 / \mathcal{A}_\mathcal{H}$ with $E_1 \xrightarrow{h}_{\rm a} E'_1$, then $E_1 \setminus \mathcal{A}_\mathcal{H} \approx_{\rm pw} E'_1 \setminus \mathcal{A}_\mathcal{H}$ as $h \in \mathcal{A}_\mathcal{H}$ and $E_1 \in {\rm SBNDC}_{\approx_{\rm pw}}$. Since $E'_1 \setminus \mathcal{A}_\mathcal{H} \approx_{\rm pw} E_2 \setminus \mathcal{A}_\mathcal{H}$, as $E_1 \setminus \mathcal{A}_\mathcal{H} \approx_{\rm pw} E_2 \setminus \mathcal{A}_\mathcal{H}$ and $\approx_{\rm pw}$ is symmetric and transitive, with $E'_1, E_2 \in {\rm SBNDC}_{\approx_{\rm pw}}$, we have that $E_2 / \mathcal{A}_\mathcal{H}$ is allowed to stay idle with $(E'_1 / \mathcal{A}_\mathcal{H}, E_2 / \mathcal{A}_\mathcal{H}) \in \mathcal{B}$.
   - If $E_1 / \mathcal{A}_\mathcal{H} \xrightarrow{l}_{\rm a} E'_1 / \mathcal{A}_\mathcal{H}$ with $E_1 \xrightarrow{l}_{\rm a} E'_1$, then $E_1 \setminus \mathcal{A}_\mathcal{H} \xrightarrow{l}_{\rm a} E'_1 \setminus \mathcal{A}_\mathcal{H}$ as $l \notin \mathcal{A}_\mathcal{H}$. From $E_1 \setminus \mathcal{A}_\mathcal{H} \approx_{\rm pw} E_2 \setminus \mathcal{A}_\mathcal{H}$ it follows that there exists $E_2 \setminus \mathcal{A}_\mathcal{H} \stackrel{\hat{l}}{\Longrightarrow} E'_2 \setminus \mathcal{A}_\mathcal{H}$ such that $E'_1 \setminus \mathcal{A}_\mathcal{H} \approx_{\rm pw} E'_2 \setminus \mathcal{A}_\mathcal{H}$. Thus $E_2 / \mathcal{A}_\mathcal{H} \stackrel{\hat{l}}{\Longrightarrow} E'_2 / \mathcal{A}_\mathcal{H}$ as $l, \tau \notin \mathcal{A}_\mathcal{H}$. Since $E'_1 \setminus \mathcal{A}_\mathcal{H} \approx_{\rm pw} E'_2 \setminus \mathcal{A}_\mathcal{H}$ with $E'_1, E'_2 \in {\rm SBNDC}_{\approx_{\rm pw}}$, we have that $(E'_1 / \mathcal{A}_\mathcal{H}, E'_2 / \mathcal{A}_\mathcal{H}) \in \mathcal{B}$.
   - If $E_1 / \mathcal{A}_\mathcal{H} \xrightarrow{\tau}_{\rm a} E'_1 / \mathcal{A}_\mathcal{H}$ with $E_1 \xrightarrow{\tau}_{\rm a} E'_1$, then the proof is like the one of the previous case.

   As for probabilities, since the hiding and restriction operators do not apply to probabilistic transitions, from $E_1 \setminus \mathcal{A}_\mathcal{H} \approx_{\rm pw} E_2 \setminus \mathcal{A}_\mathcal{H}$ it follows that $prob(E_1 / \mathcal{A}_\mathcal{H}, C) = prob(E_1 \setminus \mathcal{A}_\mathcal{H}, C) = prob(E_2 \setminus \mathcal{A}_\mathcal{H}, C) = prob(E_2 / \mathcal{A}_\mathcal{H}, C)$ for all $C \in \mathbb{P}_{\rm pr}/\mathcal{B}$.

3. Let $\mathcal{B}$ be an equivalence relation containing all the pairs of processes that have to be shown to be $\approx_{\rm pw}$-equivalent according to the considered result. Starting from $E'_1 \setminus \mathcal{A}_\mathcal{H}$ and $((E'_2 \parallel_L F) / L) \setminus \mathcal{A}_\mathcal{H}$ related by $\mathcal{B}$, so that $E'_1 \setminus \mathcal{A}_\mathcal{H} \approx_{\rm pw} E'_2 / \mathcal{A}_\mathcal{H}$, there are six cases for action transitions based on the operational semantic rules in Table 9.1. In the first two cases, it is $E'_1 \setminus \mathcal{A}_\mathcal{H}$ to move first:

   - Let $E'_1 \setminus \mathcal{A}_\mathcal{H} \xrightarrow{l}_{\rm a} E''_1 \setminus \mathcal{A}_\mathcal{H}$. We observe that from $E'_2 \in reach(E_2)$ and $E_2 \in {\rm SBSNNI}_{\approx_{\rm pw}}$ it follows that $E'_2 \setminus \mathcal{A}_\mathcal{H} \approx_{\rm pw} E'_2 / \mathcal{A}_\mathcal{H}$, so that $E'_1 \setminus \mathcal{A}_\mathcal{H} \approx_{\rm pw} E'_2 / \mathcal{A}_\mathcal{H} \approx_{\rm pw} E'_2 \setminus \mathcal{A}_\mathcal{H}$, i.e., $E'_1 \setminus \mathcal{A}_\mathcal{H} \approx_{\rm pw} E'_2 \setminus \mathcal{A}_\mathcal{H}$, as $\approx_{\rm pw}$ is symmetric and transitive. As a consequence, since $l \neq \tau$ there exists $E'_2 \setminus \mathcal{A}_\mathcal{H} \stackrel{l}{\Longrightarrow} E''_2 \setminus \mathcal{A}_\mathcal{H}$ such that $E''_1 \setminus \mathcal{A}_\mathcal{H} \approx_{\rm pw} E''_2 \setminus \mathcal{A}_\mathcal{H}$. Thus $((E'_2 \parallel_L F) / L) \setminus \mathcal{A}_\mathcal{H} \stackrel{l}{\Longrightarrow} ((E''_2 \parallel_L F) / L) \setminus \mathcal{A}_\mathcal{H}$ with $(E''_1 \setminus \mathcal{A}_\mathcal{H}, ((E''_2 \parallel_L F) / L) \setminus \mathcal{A}_\mathcal{H}) \in \mathcal{B}$ because $E''_1 \in reach(E_1)$, $E''_2 \in reach(E_2)$, and $E''_1 \setminus \mathcal{A}_\mathcal{H} \approx_{\rm pw} E''_2 / \mathcal{A}_\mathcal{H}$ as $E_2 \in {\rm SBSNNI}_{\approx_{\rm pw}}$, where the right subprocess alternates between F and $[1]F$ thus allowing the probabilistic transitions along $E'_2 \setminus \mathcal{A}_\mathcal{H} \stackrel{l}{\Longrightarrow} E''_2 \setminus \mathcal{A}_\mathcal{H}$ to synchronize with the only one of $[1]F$.
   - Let $E'_1 \setminus \mathcal{A}_\mathcal{H} \xrightarrow{\tau}_{\rm a} E''_1 \setminus \mathcal{A}_\mathcal{H}$. The proof is like the one of the previous case with $\Longrightarrow$ used in place of $\stackrel{l}{\Longrightarrow}$.

   In the other four cases, instead, it is $((E'_2 \parallel_L F) / L) \setminus \mathcal{A}_\mathcal{H}$ to move first:

   - Let $((E'_2 \parallel_L F) / L) \setminus \mathcal{A}_\mathcal{H} \xrightarrow{l}_{\rm a} ((E''_2 \parallel_L [1]F) / L) \setminus \mathcal{A}_\mathcal{H}$ with $E'_2 \xrightarrow{l}_{\rm a} E''_2$ so that $E'_2 \setminus \mathcal{A}_\mathcal{H} \xrightarrow{l}_{\rm a} E''_2 \setminus \mathcal{A}_\mathcal{H}$ as $l \notin \mathcal{A}_\mathcal{H}$. We observe that from $E'_2 \in reach(E_2)$ and $E_2 \in {\rm SBSNNI}_{\approx_{\rm pw}}$ it follows that $E'_2 \setminus \mathcal{A}_\mathcal{H} \approx_{\rm pw} E'_2 / \mathcal{A}_\mathcal{H}$, so that $E'_2 \setminus \mathcal{A}_\mathcal{H} \approx_{\rm pw} E'_2 / \mathcal{A}_\mathcal{H} \approx_{\rm pw} E'_1 \setminus \mathcal{A}_\mathcal{H}$, i.e., $E'_2 \setminus \mathcal{A}_\mathcal{H} \approx_{\rm pw} E'_1 \setminus \mathcal{A}_\mathcal{H}$, as $\approx_{\rm pw}$ is symmetric

and transitive. As a consequence, since $l \neq \tau$ there exists $E'_1 \setminus \mathcal{A}_\mathcal{H} \stackrel{l}{\Longrightarrow} E''_1 \setminus \mathcal{A}_\mathcal{H}$ such that $E''_2 \setminus \mathcal{A}_\mathcal{H} \approx_{\rm pw} E''_1 \setminus \mathcal{A}_\mathcal{H}$. Thus $(((E''_2 \parallel_L [1]F) / L) \setminus \mathcal{A}_\mathcal{H}, E''_1 \setminus \mathcal{A}_\mathcal{H}) \in \mathcal{B}$ because $E''_1 \in \mathit{reach}(E_1)$, $E''_2 \in \mathit{reach}(E_2)$, and $E''_1 \setminus \mathcal{A}_\mathcal{H} \approx_{\rm pw} E''_2 / \mathcal{A}_\mathcal{H}$ as $E_2 \in {\rm SBSNNI}_{\approx_{\rm pw}}$.

- Let $((E'_2 \parallel_L F) / L) \setminus \mathcal{A}_\mathcal{H} \stackrel{\tau}{\longrightarrow}_{\rm a} ((E''_2 \parallel_L [1]F) / L) \setminus \mathcal{A}_\mathcal{H}$ with $E'_2 \stackrel{\tau}{\longrightarrow}_{\rm a} E''_2$ so that $E'_2 \setminus \mathcal{A}_\mathcal{H} \stackrel{\tau}{\longrightarrow}_{\rm a} E''_2 \setminus \mathcal{A}_\mathcal{H}$ as $\tau \notin \mathcal{A}_\mathcal{H}$. The proof is like the one of the previous case with $\Longrightarrow$ used in place of $\stackrel{l}{\Longrightarrow}$.
- If $((E'_2 \parallel_L F) / L) \setminus \mathcal{A}_\mathcal{H} \stackrel{\tau}{\longrightarrow}_{\rm a} (([1]E'_2 \parallel_L F') / L) \setminus \mathcal{A}_\mathcal{H}$ with $F \stackrel{\tau}{\longrightarrow}_{\rm a} F'$, then trivially $((([1]E'_2 \parallel_L F') / L) \setminus \mathcal{A}_\mathcal{H}, E'_1 \setminus \mathcal{A}_\mathcal{H}) \in \mathcal{B}$ as $[1]E'_2 \approx_{\rm pw} E'_2$ and hence $[1]E'_2 / \mathcal{A}_\mathcal{H} \approx_{\rm pw} E'_2 / \mathcal{A}_\mathcal{H}$ by Lemma 9.2(4).
- Let $((E'_2 \parallel_L F) / L) \setminus \mathcal{A}_\mathcal{H} \stackrel{\tau}{\longrightarrow}_{\rm a} ((E''_2 \parallel_L F') / L) \setminus \mathcal{A}_\mathcal{H}$ with $E'_2 \stackrel{h}{\longrightarrow}_{\rm a} E''_2$ – so that $E'_2 / \mathcal{A}_\mathcal{H} \stackrel{\tau}{\longrightarrow}_{\rm a} E''_2 / \mathcal{A}_\mathcal{H}$ as $h \in \mathcal{A}_\mathcal{H}$ – and $F \stackrel{h}{\longrightarrow}_{\rm a} F'$ for $h \in L$. We observe that from $E'_2, E''_2 \in \mathit{reach}(E_2)$ and $E_2 \in {\rm SBSNNI}_{\approx_{\rm pw}}$ it follows that $E'_2 \setminus \mathcal{A}_\mathcal{H} \approx_{\rm pw} E'_2 / \mathcal{A}_\mathcal{H}$ and $E''_2 \setminus \mathcal{A}_\mathcal{H} \approx_{\rm pw} E''_2 / \mathcal{A}_\mathcal{H}$, so that $E'_2 \setminus \mathcal{A}_\mathcal{H} \Longrightarrow E''_2 \setminus \mathcal{A}_\mathcal{H}$ as $E'_2 / \mathcal{A}_\mathcal{H} \stackrel{\tau}{\longrightarrow}_{\rm a} E''_2 / \mathcal{A}_\mathcal{H}$ and $E'_2 \setminus \mathcal{A}_\mathcal{H} \approx_{\rm pw} E'_2 / \mathcal{A}_\mathcal{H} \approx_{\rm pw} E'_1 \setminus \mathcal{A}_\mathcal{H}$, i.e., $E'_2 \setminus \mathcal{A}_\mathcal{H} \approx_{\rm pw} E'_1 \setminus \mathcal{A}_\mathcal{H}$, as $\approx_{\rm pw}$ is symmetric and transitive. As a consequence there exists $E'_1 \setminus \mathcal{A}_\mathcal{H} \Longrightarrow E''_1 \setminus \mathcal{A}_\mathcal{H}$ such that $E''_2 \setminus \mathcal{A}_\mathcal{H} \approx_{\rm pw} E''_1 \setminus \mathcal{A}_\mathcal{H}$. Thus $(((E''_2 \parallel_L F') / L) \setminus \mathcal{A}_\mathcal{H}, E''_1 \setminus \mathcal{A}_\mathcal{H}) \in \mathcal{B}$ because $E''_1 \in \mathit{reach}(E_1)$, $E''_2 \in \mathit{reach}(E_2)$, and $E''_1 \setminus \mathcal{A}_\mathcal{H} \approx_{\rm pw} E''_2 / \mathcal{A}_\mathcal{H}$ as $E_2 \in {\rm SBSNNI}_{\approx_{\rm pw}}$.

As for probabilities, to avoid trivial cases let $E'_1, E'_2, F \in \mathbb{P}_{\rm p}$ and consider an equivalence class $C \in \mathbb{P}_{\rm pr}/\mathcal{B}$ that involves nondeterministic processes reachable from $E'_1 \setminus \mathcal{A}_\mathcal{H}$ and $((E'_2 \parallel_L F) / L) \setminus \mathcal{A}_\mathcal{H}$, specifically $C = \{G_{1,i} \setminus \mathcal{A}_\mathcal{H}, ((G_{2,j} \parallel_L H_j) / L) \setminus \mathcal{A}_\mathcal{H} \mid H_j \in \mathbb{P}_{\rm pr}$ having only actions in $\mathcal{A}_\mathcal{H} \wedge G_{k,h} \in \mathit{reach}(E_k) \wedge G_{1,i} \setminus \mathcal{A}_\mathcal{H} \approx_{\rm pw} G_{2,j} / \mathcal{A}_\mathcal{H}\}$. If we focus on a single probabilistic transition of E'_2, say $E'_2 \stackrel{p}{\longrightarrow}_{\rm p} E''_2$, then $((E'_2 \parallel_L F) / L) \setminus \mathcal{A}_\mathcal{H} \stackrel{p \cdot q_j}{\longrightarrow}_{\rm p} ((E''_2 \parallel_L F_j) / L) \setminus \mathcal{A}_\mathcal{H}$ for all $F \stackrel{q_j}{\longrightarrow}_{\rm p} F_j$. From $\sum_{j \in J} q_j = 1$ it follows that $\mathit{prob}(((E'_2 \parallel_L F) / L) \setminus \mathcal{A}_\mathcal{H}, \{((E''_2 \parallel_L F_j) / L) \setminus \mathcal{A}_\mathcal{H} \mid j \in J\}) = p$, where all processes $((E''_2 \parallel_L F_j) / L) \setminus \mathcal{A}_\mathcal{H}$ belong to the same equivalence class of $\mathcal{B}$ because each F_j has only actions in $\mathcal{A}_\mathcal{H}$. Since the restriction and hiding operators do not apply to probabilistic transitions, we have that:

$$\begin{array}{rcl} \mathit{prob}(E'_1 \setminus \mathcal{A}_\mathcal{H}, C) & = & \mathit{prob}(E'_1 \setminus \mathcal{A}_\mathcal{H}, \bar{C}) \\ \mathit{prob}(((E'_2 \parallel_L F) / L) \setminus \mathcal{A}_\mathcal{H}, C) & = & \mathit{prob}(E'_2 / \mathcal{A}_\mathcal{H}, \bar{C}) \end{array}$$

where:

$$\bar{C} = \{G_{1,i} \setminus \mathcal{A}_\mathcal{H} \in C\} \cup \{G_{2,j} / \mathcal{A}_\mathcal{H} \mid ((G_{2,j} \parallel_L H_j) / L) \setminus \mathcal{A}_\mathcal{H} \in C\}$$

Since $E'_1 \setminus \mathcal{A}_\mathcal{H} \approx_{\rm pw} E'_2 / \mathcal{A}_\mathcal{H}$ and $\bar{C}$ is the union of some $\approx_{\rm pw}$-equivalence classes, we have that:

$$\mathit{prob}(E'_1 \setminus \mathcal{A}_\mathcal{H}, \bar{C}) = \mathit{prob}(E'_2 / \mathcal{A}_\mathcal{H}, \bar{C})$$

We then prove the three results for the $\approx_{\rm pb}$-based properties:

1. We proceed by induction on the number $n \in \mathbb{N}$ of τ- and probabilistic transitions along $E' / \mathcal{A}_\mathcal{H} \Longrightarrow E'' / \mathcal{A}_\mathcal{H}$:

   - If $n = 0$ then the proof is like the one of the corresponding result for $\approx_{\rm pw}$.
   - Let $n > 0$ and $E'_0 / \mathcal{A}_\mathcal{H} \Longrightarrow E'_{n-1} / \mathcal{A}_\mathcal{H} \stackrel{\tau}{\longrightarrow}_{\rm a} E'_n / \mathcal{A}_\mathcal{H}$ or $E'_0 / \mathcal{A}_\mathcal{H} \Longrightarrow E'_{n-1} / \mathcal{A}_\mathcal{H} \stackrel{p}{\longrightarrow}_{\rm p} E'_n / \mathcal{A}_\mathcal{H}$ where E'_0 is E' and E'_n is E''. From the induction hypothesis it follows that $E' \setminus \mathcal{A}_\mathcal{H} \Longrightarrow \hat{E}'_{n-1} \setminus \mathcal{A}_\mathcal{H}$ with $E'_{n-1} \setminus \mathcal{A}_\mathcal{H} \approx_{\rm pb} \hat{E}'_{n-1} \setminus \mathcal{A}_\mathcal{H}$. The rest of the proof is like the one of the corresponding result for $\approx_{\rm pw}$ with the following difference:
     - If $E'_{n-1} \stackrel{\tau}{\longrightarrow}_{\rm a} E'_n$ then $E'_{n-1} \setminus \mathcal{A}_\mathcal{H} \stackrel{\tau}{\longrightarrow}_{\rm a} E'_n \setminus \mathcal{A}_\mathcal{H}$. Since $E'_{n-1} \setminus \mathcal{A}_\mathcal{H} \approx_{\rm pb} \hat{E}'_{n-1} \setminus \mathcal{A}_\mathcal{H}$:

  - either $E'_n \setminus \mathcal{A}_\mathcal{H} \approx_{\rm pb} \hat{E}'_{n-1} \setminus \mathcal{A}_\mathcal{H}$, in which case $\hat{E}'_{n-1} \setminus \mathcal{A}_\mathcal{H}$ stays idle and hence $E' \setminus \mathcal{A}_\mathcal{H} \Longrightarrow \hat{E}'_{n-1} \setminus \mathcal{A}_\mathcal{H}$ with $E'' \setminus \mathcal{A}_\mathcal{H} \approx_{\rm pb} \hat{E}'_{n-1} \setminus \mathcal{A}_\mathcal{H}$;
  - or there exists $\hat{E}'_{n-1} \setminus \mathcal{A}_\mathcal{H} \Longrightarrow \bar{E}_{n-1} \setminus \mathcal{A}_\mathcal{H} \stackrel{\tau}{\longrightarrow}_{\rm a} \hat{E}'_n \setminus \mathcal{A}_\mathcal{H}$ such that $E'_{n-1} \setminus \mathcal{A}_\mathcal{H} \approx_{\rm pb} \bar{E}_{n-1} \setminus \mathcal{A}_\mathcal{H}$ and $E'_n \setminus \mathcal{A}_\mathcal{H} \approx_{\rm pb} \hat{E}'_n \setminus \mathcal{A}_\mathcal{H}$, hence $E' \setminus \mathcal{A}_\mathcal{H} \Longrightarrow \hat{E}'_n \setminus \mathcal{A}_\mathcal{H}$ with $E'' \setminus \mathcal{A}_\mathcal{H} \approx_{\rm pb} \hat{E}'_n \setminus \mathcal{A}_\mathcal{H}$.

2. Let $\mathcal{B}$ be an equivalence relation containing all the pairs of processes that have to be shown to be $\approx_{\rm pb}$-equivalent according to the considered result. Starting from $(E_1 / \mathcal{A}_\mathcal{H}, E_2 / \mathcal{A}_\mathcal{H}) \in \mathcal{B}$, so that $E_1 \setminus \mathcal{A}_\mathcal{H} \approx_{\rm pb} E_2 \setminus \mathcal{A}_\mathcal{H}$, there are three cases for action transitions based on the operational semantic rules in Table 9.1:

   - If $E_1 / \mathcal{A}_\mathcal{H} \stackrel{\tau}{\longrightarrow}_{\rm a} E'_1 / \mathcal{A}_\mathcal{H}$ with $E_1 \stackrel{h}{\longrightarrow}_{\rm a} E'_1$, then the proof is like the one of the corresponding result for $\approx_{\rm pw}$.
   - If $E_1 / \mathcal{A}_\mathcal{H} \stackrel{l}{\longrightarrow}_{\rm a} E'_1 / \mathcal{A}_\mathcal{H}$ with $E_1 \stackrel{l}{\longrightarrow}_{\rm a} E'_1$, then $E_1 \setminus \mathcal{A}_\mathcal{H} \stackrel{l}{\longrightarrow}_{\rm a} E'_1 \setminus \mathcal{A}_\mathcal{H}$ as $l \notin \mathcal{A}_\mathcal{H}$. From $E_1 \setminus \mathcal{A}_\mathcal{H} \approx_{\rm pb} E_2 \setminus \mathcal{A}_\mathcal{H}$ it follows that there exists $E_2 \setminus \mathcal{A}_\mathcal{H} \Longrightarrow \bar{E}_2 \setminus \mathcal{A}_\mathcal{H} \stackrel{l}{\longrightarrow}_{\rm a} E'_2 \setminus \mathcal{A}_\mathcal{H}$ such that $E_1 \setminus \mathcal{A}_\mathcal{H} \approx_{\rm pb} \bar{E}_2 \setminus \mathcal{A}_\mathcal{H}$ and $E'_1 \setminus \mathcal{A}_\mathcal{H} \approx_{\rm pb} E'_2 \setminus \mathcal{A}_\mathcal{H}$. Thus $E_2 / \mathcal{A}_\mathcal{H} \Longrightarrow \bar{E}_2 / \mathcal{A}_\mathcal{H} \stackrel{l}{\longrightarrow}_{\rm a} E'_2 / \mathcal{A}_\mathcal{H}$ as $l, \tau \notin \mathcal{A}_\mathcal{H}$. Since $E_1 \setminus \mathcal{A}_\mathcal{H} \approx_{\rm pb} \bar{E}_2 \setminus \mathcal{A}_\mathcal{H}$ with $E_1, \bar{E}_2 \in {\rm SBNDC}_{\approx_{\rm pb}}$ and $E'_1 \setminus \mathcal{A}_\mathcal{H} \approx_{\rm pb} E'_2 \setminus \mathcal{A}_\mathcal{H}$ with $E'_1, E'_2 \in {\rm SBNDC}_{\approx_{\rm pb}}$, we have that $(E_1 / \mathcal{A}_\mathcal{H}, \bar{E}_2 / \mathcal{A}_\mathcal{H}) \in \mathcal{B}$ and $(E'_1 / \mathcal{A}_\mathcal{H}, E'_2 / \mathcal{A}_\mathcal{H}) \in \mathcal{B}$.
   - If $E_1 / \mathcal{A}_\mathcal{H} \stackrel{\tau}{\longrightarrow}_{\rm a} E'_1 / \mathcal{A}_\mathcal{H}$ with $E_1 \stackrel{\tau}{\longrightarrow}_{\rm a} E'_1$, then $E_1 \setminus \mathcal{A}_\mathcal{H} \stackrel{\tau}{\longrightarrow}_{\rm a} E'_1 \setminus \mathcal{A}_\mathcal{H}$ as $\tau \notin \mathcal{A}_\mathcal{H}$. There are two subcases:
     - If $E'_1 \setminus \mathcal{A}_\mathcal{H} \approx_{\rm pb} E_2 \setminus \mathcal{A}_\mathcal{H}$ then $E_2 \setminus \mathcal{A}_\mathcal{H}$ is allowed to stay idle with $(E'_1 / \mathcal{A}_\mathcal{H}, E_2 / \mathcal{A}_\mathcal{H}) \in \mathcal{B}$ because $E'_1 \setminus \mathcal{A}_\mathcal{H} \approx_{\rm pb} E_2 \setminus \mathcal{A}_\mathcal{H}$ and $E'_1, E_2 \in {\rm SBNDC}_{\approx_{\rm pb}}$.
     - If $E'_1 \setminus \mathcal{A}_\mathcal{H} \not\approx_{\rm pb} E_2 \setminus \mathcal{A}_\mathcal{H}$ then the proof is like the one of the previous case with $\stackrel{\tau}{\longrightarrow}_{\rm a}$ used in place of $\stackrel{l}{\longrightarrow}_{\rm a}$.

   As for probabilities, we reason like in the proof of the corresponding result for $\approx_{\rm pw}$.

3. Let $\mathcal{B}$ be an equivalence relation containing all the pairs of processes that have to be shown to be $\approx_{\rm pb}$-equivalent according to the considered result. Starting from $E'_1 \setminus \mathcal{A}_\mathcal{H}$ and $((E'_2 \parallel_L F) / L) \setminus \mathcal{A}_\mathcal{H}$ related by $\mathcal{B}$, so that $E'_1 \setminus \mathcal{A}_\mathcal{H} \approx_{\rm pb} E'_2 / \mathcal{A}_\mathcal{H}$, there are six cases for action transitions based on the operational semantic rules in Table 9.1. In the first two cases, it is $E'_1 \setminus \mathcal{A}_\mathcal{H}$ to move first:

   - Let $E'_1 \setminus \mathcal{A}_\mathcal{H} \stackrel{l}{\longrightarrow}_{\rm a} E''_1 \setminus \mathcal{A}_\mathcal{H}$. We observe that from $E'_2 \in \mathit{reach}(E_2)$ and $E_2 \in {\rm SBSNNI}_{\approx_{\rm pb}}$ it follows that $E'_2 \setminus \mathcal{A}_\mathcal{H} \approx_{\rm pb} E'_2 / \mathcal{A}_\mathcal{H}$, so that $E'_1 \setminus \mathcal{A}_\mathcal{H} \approx_{\rm pb} E'_2 / \mathcal{A}_\mathcal{H} \approx_{\rm pb} E'_2 \setminus \mathcal{A}_\mathcal{H}$, i.e., $E'_1 \setminus \mathcal{A}_\mathcal{H} \approx_{\rm pb} E'_2 \setminus \mathcal{A}_\mathcal{H}$, as $\approx_{\rm pb}$ is symmetric and transitive. As a consequence, since $l \neq \tau$ there exists $E'_2 \setminus \mathcal{A}_\mathcal{H} \Longrightarrow \bar{E}'_2 \setminus \mathcal{A}_\mathcal{H} \stackrel{l}{\longrightarrow}_{\rm a} E''_2 \setminus \mathcal{A}_\mathcal{H}$ such that $E'_1 \setminus \mathcal{A}_\mathcal{H} \approx_{\rm pb} \bar{E}'_2 \setminus \mathcal{A}_\mathcal{H}$ and $E''_1 \setminus \mathcal{A}_\mathcal{H} \approx_{\rm pb} E''_2 \setminus \mathcal{A}_\mathcal{H}$. Thus $((E'_2 \parallel_L F) / L) \setminus \mathcal{A}_\mathcal{H} \Longrightarrow ((\bar{E}'_2 \parallel_L F) / L) \setminus \mathcal{A}_\mathcal{H} \stackrel{l}{\longrightarrow}_{\rm a} ((E''_2 \parallel_L F) / L) \setminus \mathcal{A}_\mathcal{H}$ with $(E'_1 \setminus \mathcal{A}_\mathcal{H}, ((\bar{E}'_2 \parallel_L F) / L) \setminus \mathcal{A}_\mathcal{H}) \in \mathcal{B}$ – because $E'_1 \in \mathit{reach}(E_1)$, $\bar{E}'_2 \in \mathit{reach}(E_2)$, and $E'_1 \setminus \mathcal{A}_\mathcal{H} \approx_{\rm pb} \bar{E}'_2 / \mathcal{A}_\mathcal{H}$ as $E_2 \in {\rm SBSNNI}_{\approx_{\rm pb}}$ – and $(E''_1 \setminus \mathcal{A}_\mathcal{H}, ((E''_2 \parallel_L F) / L) \setminus \mathcal{A}_\mathcal{H}) \in \mathcal{B}$ – because $E''_1 \in \mathit{reach}(E_1)$, $E''_2 \in \mathit{reach}(E_2)$, and $E''_1 \setminus \mathcal{A}_\mathcal{H} \approx_{\rm pb} E''_2 / \mathcal{A}_\mathcal{H}$ as $E_2 \in {\rm SBSNNI}_{\approx_{\rm pb}}$ – where the right subprocess alternates between F and $[1]F$ thus allowing the probabilistic transitions along $E'_2 \setminus \mathcal{A}_\mathcal{H} \Longrightarrow \bar{E}'_2 \setminus \mathcal{A}_\mathcal{H}$ to synchronize with the only one of $[1]F$.

- If $E_1' \setminus \mathcal{A}_\mathcal{H} \xrightarrow{\tau}_{\mathrm{a}} E_1'' \setminus \mathcal{A}_\mathcal{H}$ there are two subcases:
  - If $E_1'' \setminus \mathcal{A}_\mathcal{H} \approx_{\mathrm{pb}} E_2' / \mathcal{A}_\mathcal{H}$ then $(E_2' \parallel_L F) / L) \setminus \mathcal{A}_\mathcal{H}$ is allowed to stay idle with $(E_1'' \setminus \mathcal{A}_\mathcal{H}, ((E_2' \parallel_L F) / L) \setminus \mathcal{A}_\mathcal{H}) \in \mathcal{B}$ because $E_1'' \in \mathit{reach}(E_1)$ and $E_2' \in \mathit{reach}(E_2)$.
  - If $E_1'' \setminus \mathcal{A}_\mathcal{H} \not\approx_{\mathrm{pb}} E_2' / \mathcal{A}_\mathcal{H}$ then the proof is like the one of the previous case with $\xrightarrow{\tau}_{\mathrm{a}}$ used in place of $\xrightarrow{l}_{\mathrm{a}}$.

In the other four cases, instead, it is $((E_2' \parallel_L F) / L) \setminus \mathcal{A}_\mathcal{H}$ to move first:

- Let $((E_2' \parallel_L F) / L) \setminus \mathcal{A}_\mathcal{H} \xrightarrow{l}_{\mathrm{a}} ((E_2'' \parallel_L [1]F) / L) \setminus \mathcal{A}_\mathcal{H}$ with $E_2' \xrightarrow{l}_{\mathrm{a}} E_2''$ so that $E_2' \setminus \mathcal{A}_\mathcal{H} \xrightarrow{l}_{\mathrm{a}} E_2'' \setminus \mathcal{A}_\mathcal{H}$ as $l \notin \mathcal{A}_\mathcal{H}$. We observe that from $E_2' \in \mathit{reach}(E_2)$ and $E_2 \in \mathrm{SBSNNI}_{\approx_{\mathrm{pb}}}$ it follows that $E_2' \setminus \mathcal{A}_\mathcal{H} \approx_{\mathrm{pb}} E_2' / \mathcal{A}_\mathcal{H}$, so that $E_2' \setminus \mathcal{A}_\mathcal{H} \approx_{\mathrm{pb}} E_2' / \mathcal{A}_\mathcal{H} \approx_{\mathrm{pb}} E_1' \setminus \mathcal{A}_\mathcal{H}$, i.e., $E_2' \setminus \mathcal{A}_\mathcal{H} \approx_{\mathrm{pb}} E_1' \setminus \mathcal{A}_\mathcal{H}$, as $\approx_{\mathrm{pb}}$ is symmetric and transitive. As a consequence, since $l \neq \tau$ there exists $E_1' \setminus \mathcal{A}_\mathcal{H} \Longrightarrow \bar{E}_1' \setminus \mathcal{A}_\mathcal{H} \xrightarrow{l}_{\mathrm{a}} E_1'' \setminus \mathcal{A}_\mathcal{H}$ such that $E_2' \setminus \mathcal{A}_\mathcal{H} \approx_{\mathrm{pb}} \bar{E}_1' \setminus \mathcal{A}_\mathcal{H}$ and $E_2'' \setminus \mathcal{A}_\mathcal{H} \approx_{\mathrm{pb}} E_1'' \setminus \mathcal{A}_\mathcal{H}$. Thus $(((E_2' \parallel_L F) / L) \setminus \mathcal{A}_\mathcal{H}, \bar{E}_1' \setminus \mathcal{A}_\mathcal{H}) \in \mathcal{B}$ – because $\bar{E}_1' \in \mathit{reach}(E_1)$, $E_2' \in \mathit{reach}(E_2)$, and $\bar{E}_1' \setminus \mathcal{A}_\mathcal{H} \approx_{\mathrm{pb}} E_2' / \mathcal{A}_\mathcal{H}$ as $E_2 \in \mathrm{SBSNNI}_{\approx_{\mathrm{pb}}}$ – and $(((E_2'' \parallel_L [1]F) / L) \setminus \mathcal{A}_\mathcal{H}, E_1'' \setminus \mathcal{A}_\mathcal{H}) \in \mathcal{B}$ – because $E_1'' \in \mathit{reach}(E_1)$, $E_2'' \in \mathit{reach}(E_2)$, and $E_1'' \setminus \mathcal{A}_\mathcal{H} \approx_{\mathrm{pb}} E_2'' / \mathcal{A}_\mathcal{H}$ as $E_2 \in \mathrm{SBSNNI}_{\approx_{\mathrm{pb}}}$.
- If $((E_2' \parallel_L F) / L) \setminus \mathcal{A}_\mathcal{H} \xrightarrow{\tau}_{\mathrm{a}} ((E_2'' \parallel_L [1]F) / L) \setminus \mathcal{A}_\mathcal{H}$ with $E_2' \xrightarrow{\tau}_{\mathrm{a}} E_2''$ so that $E_2' \setminus \mathcal{A}_\mathcal{H} \xrightarrow{\tau}_{\mathrm{a}} E_2'' \setminus \mathcal{A}_\mathcal{H}$ as $\tau \notin \mathcal{A}_\mathcal{H}$, there are two subcases:
  - If $E_2'' \setminus \mathcal{A}_\mathcal{H} \approx_{\mathrm{pb}} E_1' \setminus \mathcal{A}_\mathcal{H}$ then $E_1' \setminus \mathcal{A}_\mathcal{H}$ is allowed to stay idle with $(((E_2'' \parallel_L [1]F) / L) \setminus \mathcal{A}_\mathcal{H}, E_1' \setminus \mathcal{A}_\mathcal{H}) \in \mathcal{B}$ because $E_1' \in \mathit{reach}(E_1)$, $E_2'' \in \mathit{reach}(E_2)$, and $E_1' \setminus \mathcal{A}_\mathcal{H} \approx_{\mathrm{pb}} E_2'' / \mathcal{A}_\mathcal{H}$ as $E_2 \in \mathrm{SBSNNI}_{\approx_{\mathrm{pb}}}$.
  - If $E_2'' \setminus \mathcal{A}_\mathcal{H} \not\approx_{\mathrm{pb}} E_1' \setminus \mathcal{A}_\mathcal{H}$ then the proof is like the one of the previous case with $\xrightarrow{\tau}_{\mathrm{a}}$ used in place of $\xrightarrow{l}_{\mathrm{a}}$.
- If $((E_2' \parallel_L F) / L) \setminus \mathcal{A}_\mathcal{H} \xrightarrow{\tau}_{\mathrm{a}} (([1]E_2' \parallel_L F') / L) \setminus \mathcal{A}_\mathcal{H}$ with $F \xrightarrow{\tau}_{\mathrm{a}} F'$, then trivially $((([1]E_2' \parallel_L F') / L) \setminus \mathcal{A}_\mathcal{H}, E_1' \setminus \mathcal{A}_\mathcal{H}) \in \mathcal{B}$ as $[1]E_2' \approx_{\mathrm{pb}} E_2'$ and hence $[1]E_2' / \mathcal{A}_\mathcal{H} \approx_{\mathrm{pb}} E_2' / \mathcal{A}_\mathcal{H}$ by Lemma 9.2(4).
- Let $((E_2' \parallel_L F) / L) \setminus \mathcal{A}_\mathcal{H} \xrightarrow{\tau}_{\mathrm{a}} ((E_2'' \parallel_L F') / L) \setminus \mathcal{A}_\mathcal{H}$ with $E_2' \xrightarrow{h}_{\mathrm{a}} E_2''$ – so that $E_2' / \mathcal{A}_\mathcal{H} \xrightarrow{\tau}_{\mathrm{a}} E_2'' / \mathcal{A}_\mathcal{H}$ as $h \in \mathcal{A}_\mathcal{H}$ – and $F \xrightarrow{h} F'$ for $h \in L$. We observe that from $E_2', E_2'' \in \mathit{reach}(E_2)$ and $E_2 \in \mathrm{SBSNNI}_{\approx_{\mathrm{pb}}}$ it follows that $E_2' \setminus \mathcal{A}_\mathcal{H} \approx_{\mathrm{pb}} E_2' / \mathcal{A}_\mathcal{H}$ and $E_2'' \setminus \mathcal{A}_\mathcal{H} \approx_{\mathrm{pb}} E_2'' / \mathcal{A}_\mathcal{H}$, so that $E_2' \setminus \mathcal{A}_\mathcal{H} \xrightarrow{\tau}_{\mathrm{a}} E_2'' \setminus \mathcal{A}_\mathcal{H}$ and $E_2' \setminus \mathcal{A}_\mathcal{H} \approx_{\mathrm{pb}} E_2' / \mathcal{A}_\mathcal{H} \approx_{\mathrm{pb}} E_1' \setminus \mathcal{A}_\mathcal{H}$, i.e., $E_2' \setminus \mathcal{A}_\mathcal{H} \approx_{\mathrm{pb}} E_1' \setminus \mathcal{A}_\mathcal{H}$, as $\approx_{\mathrm{pb}}$ is symmetric and transitive. There are two subcases:
  - If $E_2'' \setminus \mathcal{A}_\mathcal{H} \approx_{\mathrm{pb}} E_1' \setminus \mathcal{A}_\mathcal{H}$ then $E_1' \setminus \mathcal{A}_\mathcal{H}$ is allowed to stay idle with $(((E_2'' \parallel_L F') / L) \setminus \mathcal{A}_\mathcal{H}, E_1' \setminus \mathcal{A}_\mathcal{H}) \in \mathcal{B}$ because $E_1' \in \mathit{reach}(E_1)$, $E_2'' \in \mathit{reach}(E_2)$, and $E_1' \setminus \mathcal{A}_\mathcal{H} \approx_{\mathrm{pb}} E_2'' / \mathcal{A}_\mathcal{H}$ as $E_2 \in \mathrm{SBSNNI}_{\approx_{\mathrm{pb}}}$.
  - If $E_2'' \setminus \mathcal{A}_\mathcal{H} \not\approx_{\mathrm{pb}} E_1' \setminus \mathcal{A}_\mathcal{H}$ then there exists $E_1' \setminus \mathcal{A}_\mathcal{H} \Longrightarrow \bar{E}_1' \setminus \mathcal{A}_\mathcal{H} \xrightarrow{\tau}_{\mathrm{a}} E_1'' \setminus \mathcal{A}_\mathcal{H}$ such that $E_2' \setminus \mathcal{A}_\mathcal{H} \approx_{\mathrm{pb}} \bar{E}_1' \setminus \mathcal{A}_\mathcal{H}$ and $E_2'' \setminus \mathcal{A}_\mathcal{H} \approx_{\mathrm{pb}} E_1'' \setminus \mathcal{A}_\mathcal{H}$. Thus $(((E_2' \parallel_L F) / L) \setminus \mathcal{A}_\mathcal{H}, \bar{E}_1' \setminus \mathcal{A}_\mathcal{H}) \in \mathcal{B}$ – because $\bar{E}_1' \in \mathit{reach}(E_1)$, $E_2' \in \mathit{reach}(E_2)$, and $\bar{E}_1' \setminus \mathcal{A}_\mathcal{H} \approx_{\mathrm{pb}} E_2' / \mathcal{A}_\mathcal{H}$ as $E_2 \in \mathrm{SBSNNI}_{\approx_{\mathrm{pb}}}$ – and $(((E_2'' \parallel_L F') / L) \setminus \mathcal{A}_\mathcal{H}, E_1'' \setminus \mathcal{A}_\mathcal{H}) \in \mathcal{B}$ – because $E_1'' \in \mathit{reach}(E_1)$, $E_2'' \in \mathit{reach}(E_2)$, and $E_1'' \setminus \mathcal{A}_\mathcal{H} \approx_{\mathrm{pb}} E_2'' / \mathcal{A}_\mathcal{H}$ as $E_2 \in \mathrm{SBSNNI}_{\approx_{\mathrm{pb}}}$.

As for probabilities, we reason like in the proof of the corresponding result for $\approx_{\mathrm{pw}}$. ∎

Theorem 9.3. *Let* $\approx \in \{\approx_{\rm pw}, \approx_{\rm pb}\}$. *Then:*

$$\mathrm{SBNDC}_{\approx} \subsetneq \mathrm{SBSNNI}_{\approx} = \mathrm{P\_BNDC}_{\approx} \subsetneq \mathrm{BNDC}_{\approx} \subsetneq \mathrm{BSNNI}_{\approx}$$

Proof. We first prove the results for the $\approx_{\rm pw}$-based properties. Let us examine each relationship separately:

- $\mathrm{SBNDC}_{\approx_{\rm pw}} \subsetneq \mathrm{SBSNNI}_{\approx_{\rm pw}}$. Given $E \in \mathrm{SBNDC}_{\approx_{\rm pw}}$, the result follows by proving that the relation $\mathcal{B} = \{(E' \setminus \mathcal{A}_{\mathcal{H}}, E' / \mathcal{A}_{\mathcal{H}}) \mid E' \in \mathit{reach}(E)\}$ is a weak probabilistic bisimulation up to $\approx_{\rm pw}$. Starting from $(E' \setminus \mathcal{A}_{\mathcal{H}}, E' / \mathcal{A}_{\mathcal{H}}) \in \mathcal{B}$, there are three cases for action transitions based on the operational semantic rules in Table 9.1. In the first case, it is $E' \setminus \mathcal{A}_{\mathcal{H}}$ to move first:

  - If $E' \setminus \mathcal{A}_{\mathcal{H}} \stackrel{a}{\Longrightarrow} E'' \setminus \mathcal{A}_{\mathcal{H}}$ with $a \in \mathcal{A}_{\mathcal{L}} \cup \{\tau\}$, then $E' / \mathcal{A}_{\mathcal{H}} \stackrel{\hat{a}}{\Longrightarrow} E'' / \mathcal{A}_{\mathcal{H}}$ as $a, \tau \notin \mathcal{A}_{\mathcal{H}}$, with $(E'' \setminus \mathcal{A}_{\mathcal{H}}, E'' / \mathcal{A}_{\mathcal{H}}) \in \mathcal{B}$ as $E'' \in \mathit{reach}(E)$. Thus $(E'' \setminus \mathcal{A}_{\mathcal{H}}, E'' / \mathcal{A}_{\mathcal{H}}) \in (\mathcal{B} \cup \mathcal{B}^{-1} \cup \approx_{\rm pw})^+$.

  In the other two cases, instead, it is $E' / \mathcal{A}_{\mathcal{H}}$ to move first (note that possible τ-transitions along $\Longrightarrow$ arising from high actions in E' can no longer be executed when responding from $E' \setminus \mathcal{A}_{\mathcal{H}}$, but for them we exploit $E \in \mathrm{SBNDC}_{\approx_{\rm pw}}$ and Lemma 9.4(1)):

  - If $E' / \mathcal{A}_{\mathcal{H}} \stackrel{a}{\Longrightarrow} E'' / \mathcal{A}_{\mathcal{H}}$ with $a \in \mathcal{A}_{\mathcal{L}} \cup \{\tau\}$, then there exist two processes $\bar{E}', \bar{E}'' \in \mathit{reach}(E')$ such that $E' / \mathcal{A}_{\mathcal{H}} \Longrightarrow \bar{E}' / \mathcal{A}_{\mathcal{H}} \stackrel{a}{\longrightarrow}_{\rm a} \bar{E}'' / \mathcal{A}_{\mathcal{H}} \Longrightarrow E'' / \mathcal{A}_{\mathcal{H}}$. From $E' / \mathcal{A}_{\mathcal{H}} \Longrightarrow \bar{E}' / \mathcal{A}_{\mathcal{H}}$ and Lemma 9.4(1) it follows that $E' \setminus \mathcal{A}_{\mathcal{H}} \Longrightarrow \hat{E}' \setminus \mathcal{A}_{\mathcal{H}}$ with $\bar{E}' \setminus \mathcal{A}_{\mathcal{H}} \approx_{\rm pw} \hat{E}' \setminus \mathcal{A}_{\mathcal{H}}$. From $\bar{E}' / \mathcal{A}_{\mathcal{H}} \stackrel{a}{\longrightarrow}_{\rm a} \bar{E}'' / \mathcal{A}_{\mathcal{H}}$ it follows that $\bar{E}' \setminus \mathcal{A}_{\mathcal{H}} \stackrel{a}{\longrightarrow}_{\rm a} \bar{E}'' \setminus \mathcal{A}_{\mathcal{H}}$ as $a \notin \mathcal{A}_{\mathcal{H}}$, hence $\hat{E}' \setminus \mathcal{A}_{\mathcal{H}} \stackrel{\hat{a}}{\Longrightarrow} \hat{E}'' \setminus \mathcal{A}_{\mathcal{H}}$ with $\bar{E}'' \setminus \mathcal{A}_{\mathcal{H}} \approx_{\rm pw} \hat{E}'' \setminus \mathcal{A}_{\mathcal{H}}$ as $\bar{E}' \setminus \mathcal{A}_{\mathcal{H}} \approx_{\rm pw} \hat{E}' \setminus \mathcal{A}_{\mathcal{H}}$. From $\bar{E}'' / \mathcal{A}_{\mathcal{H}} \Longrightarrow E'' / \mathcal{A}_{\mathcal{H}}$ and Lemma 9.4(1) it follows that $\bar{E}'' \setminus \mathcal{A}_{\mathcal{H}} \Longrightarrow \hat{E}''' \setminus \mathcal{A}_{\mathcal{H}}$ with $E'' \setminus \mathcal{A}_{\mathcal{H}} \approx_{\rm pw} \hat{E}''' \setminus \mathcal{A}_{\mathcal{H}}$, hence $\hat{E}'' \setminus \mathcal{A}_{\mathcal{H}} \Longrightarrow \hat{E}'''' \setminus \mathcal{A}_{\mathcal{H}}$ with $\hat{E}''' \setminus \mathcal{A}_{\mathcal{H}} \approx_{\rm pw} \hat{E}'''' \setminus \mathcal{A}_{\mathcal{H}}$ as $\bar{E}'' \setminus \mathcal{A}_{\mathcal{H}} \approx_{\rm pw} \hat{E}'' \setminus \mathcal{A}_{\mathcal{H}}$. Note that $E'' \setminus \mathcal{A}_{\mathcal{H}} \approx_{\rm pw} \hat{E}'''' \setminus \mathcal{A}_{\mathcal{H}}$ as $\approx_{\rm pw}$ is transitive. Summing up, we have that $E' \setminus \mathcal{A}_{\mathcal{H}} \stackrel{\hat{a}}{\Longrightarrow} \hat{E}'''' \setminus \mathcal{A}_{\mathcal{H}}$ with $E'' / \mathcal{A}_{\mathcal{H}}\ \mathcal{B}^{-1}\ E'' \setminus \mathcal{A}_{\mathcal{H}} \approx_{\rm pw} \hat{E}'''' \setminus \mathcal{A}_{\mathcal{H}}$, as $E'' \in \mathit{reach}(E)$, and hence $(E'' / \mathcal{A}_{\mathcal{H}}, \hat{E}'''' \setminus \mathcal{A}_{\mathcal{H}}) \in (\mathcal{B} \cup \mathcal{B}^{-1} \cup \approx_{\rm pw})^+$.
  - If $E' / \mathcal{A}_{\mathcal{H}} \stackrel{\tau}{\Longrightarrow} E'' / \mathcal{A}_{\mathcal{H}}$ stems from $\bar{E}' \stackrel{h}{\longrightarrow}_{\rm a} \bar{E}''$ for some $\bar{E}', \bar{E}'' \in \mathit{reach}(E')$, then from Lemma 9.4(1) it follows that $E' \setminus \mathcal{A}_{\mathcal{H}} \Longrightarrow \hat{E}'' \setminus \mathcal{A}_{\mathcal{H}}$ with $E'' \setminus \mathcal{A}_{\mathcal{H}} \approx_{\rm pw} \hat{E}'' \setminus \mathcal{A}_{\mathcal{H}}$. Since $E'' / \mathcal{A}_{\mathcal{H}}\ \mathcal{B}^{-1}\ E'' \setminus \mathcal{A}_{\mathcal{H}} \approx_{\rm pw} \hat{E}'' \setminus \mathcal{A}_{\mathcal{H}}$ as $E'' \in \mathit{reach}(E)$, we have that $(E'' / \mathcal{A}_{\mathcal{H}}, \hat{E}'' \setminus \mathcal{A}_{\mathcal{H}}) \in (\mathcal{B} \cup \mathcal{B}^{-1} \cup \approx_{\rm pw})^+$.

  As for probabilities, since the restriction and hiding operators do not apply to probabilistic transitions, we have that $\mathit{prob}(E' \setminus \mathcal{A}_{\mathcal{H}}, C) = \mathit{prob}(E' / \mathcal{A}_{\mathcal{H}}, C)$ for all $C \in \mathbb{P}_{\rm pr} / (\mathcal{B} \cup \mathcal{B}^{-1} \cup \approx_{\rm pw})^+$.

- $\mathrm{SBSNNI}_{\approx_{\rm pw}} = \mathrm{P\_BNDC}_{\approx_{\rm pw}}$. $\mathrm{SBSNNI}_{\approx_{\rm pw}} \subseteq \mathrm{P\_BNDC}_{\approx_{\rm pw}}$ follows from Lemma 9.4(3) by taking E'_1 identical to E'_2 and both reachable from $E \in \mathrm{SBSNNI}_{\approx_{\rm pw}}$.
  On the other hand, if $E \in \mathrm{P\_BNDC}_{\approx_{\rm pw}}$ then $E' \in \mathrm{BNDC}_{\approx_{\rm pw}}$ for every $E' \in \mathit{reach}(E)$. Since $\mathrm{BNDC}_{\approx_{\rm pw}} \subsetneq \mathrm{BSNNI}_{\approx_{\rm pw}}$ as will be shown in the last case of the proof of this part of the theorem, $E' \in \mathrm{BSNNI}_{\approx_{\rm pw}}$ for every $E' \in \mathit{reach}(E)$, i.e., $E \in \mathrm{SBSNNI}_{\approx_{\rm pw}}$.

- $\mathrm{SBSNNI}_{\approx_{\rm pw}} \subsetneq \mathrm{BNDC}_{\approx_{\rm pw}}$. If $E \in \mathrm{SBSNNI}_{\approx_{\rm pw}} = \mathrm{P\_BNDC}_{\approx_{\rm pw}}$ then it immediately follows that $E \in \mathrm{BNDC}_{\approx_{\rm pw}}$.

- $\mathrm{BNDC}_{\approx_{\rm pw}} \subsetneq \mathrm{BSNNI}_{\approx_{\rm pw}}$. If $E \in \mathrm{BNDC}_{\approx_{\rm pw}}$, i.e., $E \setminus \mathcal{A}_{\mathcal{H}} \approx_{\rm pw} (E \parallel_L F) / L) \setminus \mathcal{A}_{\mathcal{H}}$ for all $F \in \mathbb{P}_{\rm pr}$ such that each of its actions belongs to $\mathcal{A}_{\mathcal{H}}$ – and $E, F \in \mathbb{P}_{\rm n}$ or $E, F \in \mathbb{P}_{\rm p}$ – and for all $L \subseteq \mathcal{A}_{\mathcal{H}}$, then we can consider

in particular $\hat{F}$ capable of stepwise mimicking the high-level behavior of E, in the sense that $\hat{F}$ is able to synchronize with all the high-level actions executed by E and its reachable processes, along with $\hat{L} = \mathcal{A}_\mathcal{H}$. As a consequence $(E \parallel_{\hat{L}} \hat{F}) / \hat{L} \setminus \mathcal{A}_\mathcal{H}$ is isomorphic to $E / \mathcal{A}_\mathcal{H}$, hence $E \setminus \mathcal{A}_\mathcal{H} \approx_{\rm pw} (E \parallel_{\hat{L}} \hat{F}) / \hat{L} \setminus \mathcal{A}_\mathcal{H} \approx_{\rm pw} E / \mathcal{A}_\mathcal{H}$, i.e., $E \in {\rm BSNNI}_{\approx_{\rm pw}}$, as $\approx_{\rm pw}$ is transitive.

We then prove the results for the $\approx_{\rm pb}$-based properties. Let us examine each relationship separately:

- ${\rm SBNDC}_{\approx_{\rm pb}} \subsetneq {\rm SBSNNI}_{\approx_{\rm pb}}$. Given $E \in {\rm SBNDC}_{\approx_{\rm pb}}$, the result follows by proving that the relation $\mathcal{B} = \{(E' \setminus \mathcal{A}_\mathcal{H}, E' / \mathcal{A}_\mathcal{H}) \mid E' \in \mathit{reach}(E)\}$ is a probabilistic branching bisimulation up to $\approx_{\rm pb}$. Starting from $(E' \setminus \mathcal{A}_\mathcal{H}, E' / \mathcal{A}_\mathcal{H}) \in \mathcal{B}$, there are three cases for action transitions based on the operational semantic rules in Table 9.1. In the first case, it is $E' \setminus \mathcal{A}_\mathcal{H}$ to move first:

  - If $E' \setminus \mathcal{A}_\mathcal{H} \Longrightarrow \bar{E}' \setminus \mathcal{A}_\mathcal{H} \xrightarrow{a}_{\rm a} E'' \setminus \mathcal{A}_\mathcal{H}$ with $a \in \mathcal{A}_\mathcal{L} \cup \{\tau\}$, then $E' / \mathcal{A}_\mathcal{H} \Longrightarrow \bar{E}' / \mathcal{A}_\mathcal{H} \xrightarrow{a}_{\rm a} E'' / \mathcal{A}_\mathcal{H}$ as $a, \tau \notin \mathcal{A}_\mathcal{H}$, with $(\bar{E}' \setminus \mathcal{A}_\mathcal{H}, \bar{E}' / \mathcal{A}_\mathcal{H}) \in \mathcal{B}$ and $(E'' \setminus \mathcal{A}_\mathcal{H}, E'' / \mathcal{A}_\mathcal{H}) \in \mathcal{B}$ as $\bar{E}', E'' \in \mathit{reach}(E)$. Thus $(\bar{E}' \setminus \mathcal{A}_\mathcal{H}, \bar{E}' / \mathcal{A}_\mathcal{H}) \in (\mathcal{B} \cup \mathcal{B}^{-1} \cup \approx_{\rm pb})^+$ and $(E'' \setminus \mathcal{A}_\mathcal{H}, E'' / \mathcal{A}_\mathcal{H}) \in (\mathcal{B} \cup \mathcal{B}^{-1} \cup \approx_{\rm pb})^+$.

  In the other two cases, instead, it is $E' / \mathcal{A}_\mathcal{H}$ to move first (note that possible τ-transitions along $\Longrightarrow$ arising from high actions in E' can no longer be executed when responding from $E' \setminus \mathcal{A}_\mathcal{H}$, but for them we exploit $E \in {\rm SBNDC}_{\approx_{\rm pb}}$ and Lemma 9.4(1)):

  - Let $E' / \mathcal{A}_\mathcal{H} \Longrightarrow \bar{E}' / \mathcal{A}_\mathcal{H} \xrightarrow{a}_{\rm a} E'' / \mathcal{A}_\mathcal{H}$ with $a \in \mathcal{A}_\mathcal{L} \cup \{\tau\}$. From $E' / \mathcal{A}_\mathcal{H} \Longrightarrow \bar{E}' / \mathcal{A}_\mathcal{H}$ and Lemma 9.4(1) it follows that $E' \setminus \mathcal{A}_\mathcal{H} \Longrightarrow \hat{E}' \setminus \mathcal{A}_\mathcal{H}$ with $\bar{E}' \setminus \mathcal{A}_\mathcal{H} \approx_{\rm pb} \hat{E}' \setminus \mathcal{A}_\mathcal{H}$. From $\bar{E}' / \mathcal{A}_\mathcal{H} \xrightarrow{a}_{\rm a} E'' / \mathcal{A}_\mathcal{H}$ it follows that $\bar{E}' \setminus \mathcal{A}_\mathcal{H} \xrightarrow{a}_{\rm a} E'' \setminus \mathcal{A}_\mathcal{H}$ as $a \notin \mathcal{A}_\mathcal{H}$. Since $\bar{E}' \setminus \mathcal{A}_\mathcal{H} \approx_{\rm pb} \hat{E}' \setminus \mathcal{A}_\mathcal{H}$ there are two subcases:
    - If $a = \tau$ and $E'' \setminus \mathcal{A}_\mathcal{H} \approx_{\rm pb} \hat{E}' \setminus \mathcal{A}_\mathcal{H}$, then $\bar{E}' \setminus \mathcal{A}_\mathcal{H} \approx_{\rm pb} E'' \setminus \mathcal{A}_\mathcal{H}$ as $\approx_{\rm pb}$ is symmetric and transitive. From $\bar{E}', E'' \in {\rm SBNDC}_{\approx_{\rm pb}}$ and Lemma 9.4(2) it follows that $\bar{E}' / \mathcal{A}_\mathcal{H} \approx_{\rm pb} E'' / \mathcal{A}_\mathcal{H}$. Thus $E' \setminus \mathcal{A}_\mathcal{H}$ is allowed to stay idle.
    - Otherwise there exists $\hat{E}' \setminus \mathcal{A}_\mathcal{H} \Longrightarrow \hat{E}'' \setminus \mathcal{A}_\mathcal{H} \xrightarrow{a}_{\rm a} \hat{E}''' \setminus \mathcal{A}_\mathcal{H}$ such that $\bar{E}' \setminus \mathcal{A}_\mathcal{H} \approx_{\rm pb} \hat{E}'' \setminus \mathcal{A}_\mathcal{H}$ and $E'' \setminus \mathcal{A}_\mathcal{H} \approx_{\rm pb} \hat{E}''' \setminus \mathcal{A}_\mathcal{H}$. Summing up, we have that $E' \setminus \mathcal{A}_\mathcal{H} \Longrightarrow \hat{E}'' \setminus \mathcal{A}_\mathcal{H} \xrightarrow{a}_{\rm a} \hat{E}''' \setminus \mathcal{A}_\mathcal{H}$ with $\bar{E}' / \mathcal{A}_\mathcal{H} \; \mathcal{B}^{-1} \; \bar{E}' \setminus \mathcal{A}_\mathcal{H} \approx_{\rm pb} \hat{E}'' \setminus \mathcal{A}_\mathcal{H}$ and $E'' / \mathcal{A}_\mathcal{H} \; \mathcal{B}^{-1} \; E'' \setminus \mathcal{A}_\mathcal{H} \approx_{\rm pb} \hat{E}''' \setminus \mathcal{A}_\mathcal{H}$, as $\bar{E}', E'' \in \mathit{reach}(E)$, and hence $(\bar{E}' / \mathcal{A}_\mathcal{H}, \hat{E}'' \setminus \mathcal{A}_\mathcal{H}) \in (\mathcal{B} \cup \mathcal{B}^{-1} \cup \approx_{\rm pb})^+$ and $(E'' / \mathcal{A}_\mathcal{H}, \hat{E}''' \setminus \mathcal{A}_\mathcal{H}) \in (\mathcal{B} \cup \mathcal{B}^{-1} \cup \approx_{\rm pb})^+$.
  - Let $E' / \mathcal{A}_\mathcal{H} \Longrightarrow \bar{E}' / \mathcal{A}_\mathcal{H} \xrightarrow{\tau}_{\rm a} E'' / \mathcal{A}_\mathcal{H}$ with $\bar{E}' \xrightarrow{h}_{\rm a} E''$. From $\bar{E}' \in \mathit{reach}(E)$ and $E \in {\rm SBNDC}_{\approx_{\rm pb}}$ it follows that $\bar{E}' \setminus \mathcal{A}_\mathcal{H} \approx_{\rm pb} E'' \setminus \mathcal{A}_\mathcal{H}$, hence $\bar{E}' / \mathcal{A}_\mathcal{H} \approx_{\rm pb} E'' / \mathcal{A}_\mathcal{H}$ by virtue of Lemma 9.4(2) as $\bar{E}', E'' \in {\rm SBNDC}_{\approx_{\rm pb}}$. Thus $E' \setminus \mathcal{A}_\mathcal{H}$ is allowed to stay idle.

  As for probabilities, the proof is like the one of the corresponding result for $\approx_{\rm pw}$.

- ${\rm SBSNNI}_{\approx_{\rm pb}} = {\rm P\_BNDC}_{\approx_{\rm pb}}$. The proof is like the one of the corresponding result for $\approx_{\rm pw}$.

- ${\rm SBSNNI}_{\approx_{\rm pb}} \subsetneq {\rm BNDC}_{\approx_{\rm pb}}$. The proof is like the one of the corresponding result for $\approx_{\rm pw}$.

- ${\rm BNDC}_{\approx_{\rm pb}} \subsetneq {\rm BSNNI}_{\approx_{\rm pb}}$. The proof is like the one of the corresponding result for $\approx_{\rm pw}$. ■

All the inclusions in the previous theorem are strict as shown by the same counterexamples as those after Theorem 8.4 suitably extended with occurrences of [1].

We further observe that each of the $\approx_{\mathrm{pb}}$-based noninterference properties implies the corresponding $\approx_{\mathrm{pw}}$-based one, due to the fact that $\approx_{\mathrm{pb}}$ is finer than $\approx_{\mathrm{pw}}$.

Theorem 9.4. *The following inclusions hold:*

1. $\mathrm{BSNNI}_{\approx_{\mathrm{pb}}} \subsetneq \mathrm{BSNNI}_{\approx_{\mathrm{pw}}}$.
2. $\mathrm{BNDC}_{\approx_{\mathrm{pb}}} \subsetneq \mathrm{BNDC}_{\approx_{\mathrm{pw}}}$.
3. $\mathrm{SBSNNI}_{\approx_{\mathrm{pb}}} \subsetneq \mathrm{SBSNNI}_{\approx_{\mathrm{pw}}}$.
4. $\mathrm{P\_BNDC}_{\approx_{\mathrm{pb}}} \subsetneq \mathrm{P\_BNDC}_{\approx_{\mathrm{pw}}}$.
5. $\mathrm{SBNDC}_{\approx_{\mathrm{pb}}} \subsetneq \mathrm{SBNDC}_{\approx_{\mathrm{pw}}}$. ∎

All the inclusions above are strict by virtue of the following result; for an example of E_1 and E_2 below, see Figure 9.1 with both systems extended with an identical action transition at the beginning.

Theorem 9.5. *Let $E_1, E_2 \in \mathbb{P}_{\mathrm{n}}$ be such that $E_1 \approx_{\mathrm{pw}} E_2$ but $E_1 \not\approx_{\mathrm{pb}} E_2$. If no high-level actions occur in E_1 and E_2, then $F \in \{E_1 + h\,.\,[1]E_2, E_2 + h\,.\,[1]E_1\}$ is such that:*

1. *$F \in \mathrm{BSNNI}_{\approx_{\mathrm{pw}}}$ but $F \notin \mathrm{BSNNI}_{\approx_{\mathrm{pb}}}$.*
2. *$F \in \mathrm{BNDC}_{\approx_{\mathrm{pw}}}$ but $F \notin \mathrm{BNDC}_{\approx_{\mathrm{pb}}}$.*
3. *$F \in \mathrm{SBSNNI}_{\approx_{\mathrm{pw}}}$ but $F \notin \mathrm{SBSNNI}_{\approx_{\mathrm{pb}}}$.*
4. *$F \in \mathrm{P\_BNDC}_{\approx_{\mathrm{pw}}}$ but $F \notin \mathrm{P\_BNDC}_{\approx_{\mathrm{pb}}}$.*
5. *$F \in \mathrm{SBNDC}_{\approx_{\mathrm{pw}}}$ but $F \notin \mathrm{SBNDC}_{\approx_{\mathrm{pb}}}$.*

Proof. Let F be $E_1 + h\,.\,[1]E_2$ (the proof is similar for F equal to $E_2 + h\,.\,[1]E_1$) and observe that no high-level actions occur in every process reachable from F except F itself:

1. Since the only high-level action occurring in F is h, in the proof of $F \in \mathrm{BSNNI}_{\approx_{\mathrm{pw}}}$ the only interesting case is the transition $F \,/\, \mathcal{A}_{\mathcal{H}} \xrightarrow{\tau}_{\mathrm{a}} ([1]E_2) \,/\, \mathcal{A}_{\mathcal{H}}$, to which $F \setminus \mathcal{A}_{\mathcal{H}}$ responds by staying idle because $([1]E_2) \,/\, \mathcal{A}_{\mathcal{H}} \approx_{\mathrm{pw}} [1]E_2 \approx_{\mathrm{pw}} E_2 \approx_{\mathrm{pw}} E_1 \approx_{\mathrm{pw}} F \setminus \mathcal{A}_{\mathcal{H}}$, i.e., $([1]E_2) \,/\, \mathcal{A}_{\mathcal{H}} \approx_{\mathrm{pw}} F \setminus \mathcal{A}_{\mathcal{H}}$ as $\approx_{\mathrm{pw}}$ is symmetric and transitive.
   On the other hand, $F \notin \mathrm{BSNNI}_{\approx_{\mathrm{pb}}}$ because $E_2 \not\approx_{\mathrm{pb}} E_1$ in the same situation as before.
2. Since $F \in \mathrm{BSNNI}_{\approx_{\mathrm{pw}}}$ by the previous result and no high-level actions occur in every process reachable from F other than F, it holds that $F \in \mathrm{SBSNNI}_{\approx_{\mathrm{pw}}}$ and hence $F \in \mathrm{BNDC}_{\approx_{\mathrm{pw}}}$ by virtue of Theorem 9.3.
   On the other hand, from $F \notin \mathrm{BSNNI}_{\approx_{\mathrm{pb}}}$ by the previous result it follows that $F \notin \mathrm{BNDC}_{\approx_{\mathrm{pb}}}$ by virtue of Theorem 9.3.
3. We already know from the proof of the previous result that $F \in \mathrm{SBSNNI}_{\approx_{\mathrm{pw}}}$.
   On the other hand, from $F \notin \mathrm{BSNNI}_{\approx_{\mathrm{pb}}}$ by the first result it follows that $F \notin \mathrm{SBSNNI}_{\approx_{\mathrm{pb}}}$ by virtue of Theorem 9.3.

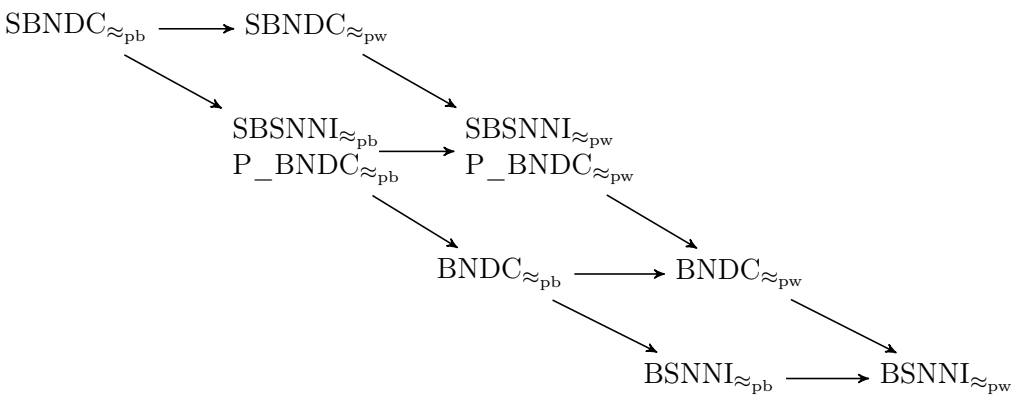


Figure 9.2: Taxonomy of security properties based on probabilistic weak and branching bisimilarities

4. An immediate consequence of P_BNDC$_{\approx_{pw}}$ = SBSNNI$_{\approx_{pw}}$ and P_BNDC$_{\approx_{pb}}$ = SBSNNI$_{\approx_{pb}}$ as established by Theorem 9.3.

5. Since the only high-level action occurring in F is h, in the proof of $F \in \text{SBNDC}_{\approx_{pw}}$ the only interesting case is the transition $F \xrightarrow{h}_{a} [1]E_2$, for which it holds that $F \setminus \mathcal{A}_{\mathcal{H}} \approx_{pw} E_1 \approx_{pw} E_2 \approx_{pw} [1]E_2 \approx_{pw} ([1]E_2) \setminus \mathcal{A}_{\mathcal{H}}$, i.e., $F \setminus \mathcal{A}_{\mathcal{H}} \approx_{pw} ([1]E_2) \setminus \mathcal{A}_{\mathcal{H}}$ as $\approx_{pw}$ is transitive.
On the other hand, $F \notin \text{SBNDC}_{\approx_{pb}}$ because $E_1 \not\approx_{pb} E_2$ in the same situation as before. ■

The diagram in Figure 9.2 summarizes the inclusions among the various noninterference properties based on the results in Theorems 9.3 and 9.4, where $\mathcal{P} \to \mathcal{Q}$ means that $\mathcal{P}$ is strictly included in $\mathcal{Q}$. These inclusions follow the same pattern as the nondeterministic setting in Figure 8.4. The arrows missing in the diagram, witnessing incomparability, are justified by the same counterexamples as those after Proposition 8.3 suitably extended with occurrences of [1]. As an additional counterexample, for BNDC$_{\approx_{pw}}$ vs. BSNNI$_{\approx_{pb}}$ we have that the process $l\,.\,\underline{0} + l\,.\,([0.5]h_1\,.\,l_1\,.\,\underline{0} \oplus [0.5]h_2\,.\,l_2\,.\,\underline{0}) + l\,.\,([0.5]l_1\,.\,\underline{0} \oplus [0.5]l_2\,.\,\underline{0})$ is BSNNI$_{\approx_{pb}}$ but not BNDC$_{\approx_{pw}}$ as discussed in Section 9.2, while the process F mentioned in Theorem 9.5 is both BSNNI$_{\approx_{pw}}$ and BNDC$_{\approx_{pw}}$ but not BSNNI$_{\approx_{pb}}$.

Like in the nondeterministic setting of the previous chapter, the strongest property based on weak probabilistic bisimilarity (SBNDC$_{\approx_{pw}}$) and the weakest property based on probabilistic branching bisimilarity (BSNNI$_{\approx_{pb}}$) are incomparable too. The former is a very restrictive property because it requires a local check every time a high-level action is performed, while the latter requires a check only on the initial state. On the other hand, as shown in Theorem 9.5, it is very easy to construct processes that are secure under properties based on $\approx_{pw}$ but not on $\approx_{pb}$, due to the minimal number of high-level actions in F.

9.2.3 Relating Nondeterministic and Probabilistic Taxonomies

Let us compare our probabilistic taxonomy with the nondeterministic one of the previous chapter. In the following, we assume that $\approx_{w}$ denotes the weak nondeterministic bisimilarity of [112] and $\approx_{b}$ denotes the nondeterministic branching bisimilarity of [80], which we have used in the previous chapter. These can also be obtained from the

corresponding definitions in Section 9.1.2 by restricting to nondeterministic states and ignoring the clause involving the *prob* function. Since we are considering probabilistic choices as internal, given a process $E \in \mathbb{P}_{\rm pr}$ we can obtain its nondeterministic variant, denoted by $nd(E)$, by replacing every occurrence of $\bigoplus_{i\in I}[p_i]N_i$ with $\sum_{i\in I}\tau\,.\,N_i$.

The next proposition states that if two processes are equivalent according to any of the weak bisimilarities in Section 9.1.2, then their nondeterministic variants are equivalent according to the corresponding nondeterministic weak bisimilarity. The inverse does not hold: e.g., processes $E_1 = [0.5]a_1\,.\,\underline{0} \oplus [0.5]a_2\,.\,\underline{0}$ and $E_2 = [0.8]a_1\,.\,\underline{0} \oplus [0.2]a_2\,.\,\underline{0}$ are such that $E_1 \not\approx_{\rm pw} E_2$ and $E_1 \not\approx_{\rm pb} E_2$, but their nondeterministic counterparts coincide as both of them are equal to $\tau\,.\,a_1\,.\,\underline{0} + \tau\,.\,a_2\,.\,\underline{0}$.

Proposition 9.3. *Let $E_1, E_2 \in \mathbb{P}_{\rm pr}$. Then:*

1. $E_1 \approx_{\rm pw} E_2 \Longrightarrow nd(E_1) \approx_{\rm w} nd(E_2)$.
2. $E_1 \approx_{\rm pb} E_2 \Longrightarrow nd(E_1) \approx_{\rm b} nd(E_2)$.

Proof. Let us denote by $\stackrel{\hat{a}}{\Longrightarrow}_{\rm a}$ the variant of $\stackrel{\hat{a}}{\Longrightarrow}$ in which there are no probabilistic transitions and by $\stackrel{\tau^*}{\Longrightarrow}_{\rm a}$ a possibly empty sequence of τ-transitions:

1. We need to prove that the symmetric relation $\mathcal{B} = \{(nd(E_1), nd(E_2)) \mid E_1 \approx_{\rm pw} E_2\}$ is a weak bisimulation. We start by observing that from $E_1 \approx_{\rm pw} E_2$ it follows that for each $E_1 \stackrel{a}{\longrightarrow}_{\rm a} E_1'$ there exists $E_2 \stackrel{\hat{a}}{\Longrightarrow} E_2'$ such that $E_1' \approx_{\rm pw} E_2'$. Since $nd(E_1)$ and $nd(E_2)$ are obtained by replacing each probabilistic transition with a τ-transition, for each $nd(E_1) \stackrel{a}{\longrightarrow}_{\rm a} nd(E_1')$ there exists $nd(E_2) \stackrel{\hat{a}}{\Longrightarrow}_{\rm a} nd(E_2')$ such that $(nd(E_1'), nd(E_2')) \in \mathcal{B}$.
2. We need to prove that the symmetric relation $\mathcal{B} = \{nd(E_1), nd(E_2)) \mid E_1 \approx_{\rm pb} E_2\}$ is a branching bisimulation. We start by observing that from $E_1 \approx_{\rm pb} E_2$ it follows that for each $E_1 \stackrel{a}{\longrightarrow}_{\rm a} E_1'$ either $a = \tau$ and $E_1' \approx_{\rm pb} E_2$, or there exists $E_2 \Longrightarrow \bar{E}_2 \stackrel{a}{\longrightarrow}_{\rm a} E_2'$ such that $E_1 \approx_{\rm pb} \bar{E}_2$ and $E_1' \approx_{\rm pb} E_2'$. Since $nd(E_1)$ and $nd(E_2)$ are obtained by replacing each probabilistic transition with a τ-transition, for each $nd(E_1) \stackrel{a}{\longrightarrow}_{\rm a} nd(E_1')$ either $a = \tau$ and $(nd(E_1'), nd(E_2)) \in \mathcal{B}$, or there exists $nd(E_2) \stackrel{\tau^*}{\Longrightarrow}_{\rm a} nd(\bar{E}_2) \stackrel{a}{\longrightarrow}_{\rm a} nd(E_2')$ such that $(nd(E_1), nd(\bar{E}_2)) \in \mathcal{B}$ and $(nd(E_1'), nd(E_2')) \in \mathcal{B}$. ∎

An immediate consequence is that if a process is secure under any of the probabilistic noninterference properties of Section 9.2, then its nondeterministic variant is secure under the corresponding nondeterministic property. The taxonomy of Figure 9.2 thus extends to the left the one in Figure 8.4, as each of the properties of Section 9.2 is finer than its nondeterministic counterpart.

Corollary 9.1. *Let $\mathcal{P}_{\rm pr} \in \{\mathrm{BSNNI}_{\approx_{\rm pr}}, \mathrm{BNDC}_{\approx_{\rm pr}}, \mathrm{SBSNNI}_{\approx_{\rm pr}}, \mathrm{P\_BNDC}_{\approx_{\rm pr}}, \mathrm{SBNDC}_{\approx_{\rm pr}}\}$ and $\mathcal{P}_{\rm nd} \in \{\mathrm{BSNNI}_{\approx_{\rm nd}}, \mathrm{BNDC}_{\approx_{\rm nd}}, \mathrm{SBSNNI}_{\approx_{\rm nd}}, \mathrm{P\_BNDC}_{\approx_{\rm nd}}, \mathrm{SBNDC}_{\approx_{\rm nd}}\}$ for $\approx_{\rm pr} \in \{\approx_{\rm pw}, \approx_{\rm pb}\}$ and $\approx_{\rm nd} \in \{\approx_{\rm w}, \approx_{\rm b}\}$, where $\mathcal{P}_{\rm nd}$ is meant to be the nondeterministic variant of $\mathcal{P}_{\rm pr}$. Then $E \in \mathcal{P}_{\rm pr} \Longrightarrow nd(E) \in \mathcal{P}_{\rm nd}$ for all $E \in \mathbb{P}_{\rm pr}$.*

Proof. The result directly follows from Proposition 9.3. ∎

9.3 Reversibility via Weak Probabilistic Back-and-Forth Bisimilarity

As recalled in the previous chapter, weak back-and-forth bisimilarity coincides with branching bisimilarity over nodeterministic processes [57]. In this section we extend that result so that probabilistic branching bisimilarity can be employed in the noninterference analysis of reversible processes featuring nondeterminism and probabilities.

A PLTS $(\mathcal{S}, \mathcal{A}, \longrightarrow)$ represents a reversible process if each of its transitions is seen as bidirectional. When going backward, it is of paramount importance to respect causality, i.e., the last performed transition must be the first one to be undone. Following [57] we set up an equivalence that enforces not only causality but also history preservation. This means that, when going backward, a process can only move along the path representing the history that brought the process to the current state even in the presence of concurrency. To accomplish this, the equivalence has to be defined over computations, not over states, and the notion of transition has to be suitably revised. We start by adapting the notation of the nondeterministic setting of [57] to our strictly alternating probabilistic setting. We use ℓ for a label in $\mathcal{A} \cup \mathbb{R}_{]0,1[}$.

Definition 9.9. *A sequence $\xi = (s_0, \ell_1, s_1)(s_1, \ell_2, s_2) \ldots (s_{n-1}, \ell_n, s_n) \in \longrightarrow^*$ is a* path *of length n from state s_0. We let $first(\xi) = s_0$ and $last(\xi) = s_n$; the empty path is indicated with ε. We denote by $path(s)$ the set of paths from s.* ■

Definition 9.10. *A pair $\rho = (s, \xi)$ is called a* run *from state s iff $\xi \in path(s)$, in which case we let $path(\rho) = \xi$, $first(\rho) = first(\xi) = s$, and $last(\rho) = last(\xi)$, with $first(\rho) = last(\rho) = s$ when $\xi = \varepsilon$. We denote by $run(s)$ the set of runs from state s. Given $\rho = (s, \xi) \in run(s)$ and $\rho' = (s', \xi') \in run(s')$, their composition $\rho\rho' = (s, \xi\xi') \in run(s)$ is defined iff $last(\rho) = first(\rho') = s'$. We write $\rho \stackrel{\ell}{\longrightarrow} \rho'$ iff there exists $\bar{\rho} = (\bar{s}, (\bar{s}, \ell, s'))$ with $\bar{s} = last(\rho)$ such that $\rho' = \rho\bar{\rho}$; note that $first(\rho) = first(\rho')$. Moreover prob is lifted in the expected way.* ■

In the considered PLTS we work with the set $\mathcal{U}$ of runs in lieu of $\mathcal{S}$. Following [57], given a run ρ, we distinguish between outgoing and incoming action transitions of ρ during the weak bisimulation game. Like in [32], this does not apply to probabilistic transitions, which are thus considered only in the forward direction. If the labels of incoming probabilistic transitions were taken into account, then the nondeterministic state $a \,.\, \underline{0}$ and the probabilistic state $[p]a \,.\, \underline{0} \oplus [1-p]a \,.\, \underline{0}$ would be told apart, because $a \,.\, \underline{0}$ in the former state has no incoming probabilistic transitions while $a \,.\, \underline{0}$ in the latter state is reached with cumulative probability 1. Unlike [32], where action execution and quantitative aspects are integrated in a single transition relation, even a simpler clause requiring for any two related runs that they both have incoming probabilistic transitions or neither has – regardless of cumulative probabilities – would distinguish the two states exemplified before.

Definition 9.11. *Let $(\mathcal{S}, \mathcal{A}, \longrightarrow)$ be a PLTS. We say that $s_1, s_2 \in \mathcal{S}$ are* weakly probabilistic back-and-forth bisimilar*, written $s_1 \approx_{\rm pbf} s_2$, iff $((s_1, \varepsilon), (s_2, \varepsilon)) \in \mathcal{B}$ for some weak probabilistic back-and-forth bisimulation $\mathcal{B}$. An equivalence relation $\mathcal{B}$ over $\mathcal{U}$ is a* weak probabilistic back-and-forth bisimulation *iff, whenever $(\rho_1, \rho_2) \in \mathcal{B}$, then:*

- *For each $\rho_1 \stackrel{a}{\longrightarrow}_{\rm a} \rho_1'$ there exists $\rho_2 \stackrel{\hat{a}}{\Longrightarrow} \rho_2'$ such that $(\rho_1', \rho_2') \in \mathcal{B}$.*
- *For each $\rho_1' \stackrel{a}{\longrightarrow}_{\rm a} \rho_1$ there exists $\rho_2' \stackrel{\hat{a}}{\Longrightarrow} \rho_2$ such that $(\rho_1', \rho_2') \in \mathcal{B}$.*
- *$prob(\rho_1, C) = prob(\rho_2, C)$ for all equivalence classes $C \in \mathcal{U}/\mathcal{B}$.* ■

We show that weak probabilistic back-and-forth bisimilarity over runs coincides with $\approx_{\rm pb}$, the forward-only probabilistic branching bisimilarity over states. We proceed by adopting the proof strategy followed in [57] to show

that their weak back-and-forth bisimilarity over runs coincides with the forward-only branching bisimilarity over states of [80]. Therefore we start by proving that $\approx_{\rm pbf}$ satisfies the *cross property*. This means that, whenever two runs of two $\approx_{\rm pbf}$-equivalent states can perform a sequence of finitely many τ-transitions, alternating with probabilistic transitions, such that each of the two target runs ends in a nondeterministic state and is $\approx_{\rm pbf}$-equivalent to the source run of the other sequence, then the two target runs are $\approx_{\rm pbf}$-equivalent to each other as well.

Lemma 9.5. *Let $s_1, s_2 \in \mathcal{S}$ with $s_1 \approx_{\rm pbf} s_2$. For all $\rho_1', \rho_1'' \in run(s_1)$ such that $\rho_1' \Longrightarrow \rho_1''$ with $last(\rho_1'') \in \mathcal{S}_{\rm n}$ and for all $\rho_2', \rho_2'' \in run(s_2)$ such that $\rho_2' \Longrightarrow \rho_2''$ with $last(\rho_2'') \in \mathcal{S}_{\rm n}$, if $\rho_1' \approx_{\rm pbf} \rho_2''$ and $\rho_1'' \approx_{\rm pbf} \rho_2'$ then $\rho_1'' \approx_{\rm pbf} \rho_2''$.*

Proof. Given $s_1, s_2 \in \mathcal{S}$ with $s_1 \approx_{\rm pbf} s_2$, consider the transitive closure $\mathcal{B}^+$ of the reflexive and symmetric relation $\mathcal{B} = \approx_{\rm pbf} \cup \{(\rho_1'', \rho_2''), (\rho_2'', \rho_1'') \in (run(s_1) \times run(s_2)) \cup (run(s_2) \times run(s_1)) \mid last(\rho_1''), last(\rho_2'') \in \mathcal{S}_{\tt n} \wedge \exists \rho_1' \in run(s_1), \rho_2' \in run(s_2).\, \rho_1' \Longrightarrow \rho_1'' \wedge \rho_2' \Longrightarrow \rho_2'' \wedge \rho_1' \approx_{\rm pbf} \rho_2'' \wedge \rho_1'' \approx_{\rm pbf} \rho_2'\}$. The result will follow by proving that $\mathcal{B}^+$ is a weak probabilistic back-and-forth bisimulation, because this implies that $\rho_1'' \approx_{\rm pbf} \rho_2''$ for every additional pair – i.e., $\mathcal{B}^+$ satisfies the cross property – as well as $\mathcal{B}^+ = \approx_{\rm pbf}$ – hence $\approx_{\rm pbf}$ satisfies the cross property too.
Let $(\rho_1'', \rho_2'') \in \mathcal{B} \setminus \approx_{\rm pbf}$ to avoid trivial cases. Then $last(\rho_1''), last(\rho_2'') \in \mathcal{S}_{\tt n}$ and there exist $\rho_1' \in run(s_1)$ and $\rho_2' \in run(s_2)$ such that $\rho_1' \Longrightarrow \rho_1''$, $\rho_2' \Longrightarrow \rho_2''$, $\rho_1' \approx_{\rm pbf} \rho_2''$, and $\rho_1'' \approx_{\rm pbf} \rho_2'$. There are two cases for action transitions:

- In the forward case, assume that $\rho_1'' \xrightarrow{a}_{\rm a} \rho_1'''$, from which we derive $\rho_1' \Longrightarrow \rho_1'' \xrightarrow{a}_{\rm a} \rho_1'''$. From $\rho_1' \approx_{\rm pbf} \rho_2''$ it follows that there exists $\rho_2'' \Longrightarrow \rho_2'''$ if $a = \tau$ or $\rho_2'' \Longrightarrow \xrightarrow{a}_{\rm a} \Longrightarrow \rho_2'''$ if $a \neq \tau$, such that $\rho_1''' \approx_{\rm pbf} \rho_2'''$ and hence $(\rho_1''', \rho_2''') \in \mathcal{B}$.
  When starting from $\rho_2'' \xrightarrow{a}_{\rm a} \rho_2'''$, we exploit $\rho_2' \Longrightarrow \rho_2''$ and $\rho_1'' \approx_{\rm pbf} \rho_2'$ instead.

- In the backward case, assume that $\rho_1''' \xrightarrow{a}_{\rm a} \rho_1''$. From $\rho_1'' \approx_{\rm pbf} \rho_2'$ it follows that there exists $\rho_2''' \Longrightarrow \rho_2'$ if $a = \tau$, so that $\rho_2''' \Longrightarrow \rho_2''$, or $\rho_2''' \Longrightarrow \xrightarrow{a}_{\rm a} \Longrightarrow \rho_2'$ if $a \neq \tau$, so that $\rho_2''' \Longrightarrow \xrightarrow{a}_{\rm a} \Longrightarrow \rho_2''$, such that $\rho_1''' \approx_{\rm pbf} \rho_2'''$ and hence $(\rho_1''', \rho_2''') \in \mathcal{B}$.
  When starting from $\rho_2''' \xrightarrow{a}_{\rm a} \rho_2''$, we exploit $\rho_1' \approx_{\rm pbf} \rho_2''$ and $\rho_1' \Longrightarrow \rho_1''$ instead.

As for probabilities, from $last(\rho_1''), last(\rho_2'') \in \mathcal{S}_{\tt n}$ it follows that $prob(\rho_1'', \bar{C}) = 1 = prob(\rho_2'', \bar{C})$ when $\bar{C}$ is the equivalence class with respect to $\mathcal{B}^+$ that contains ρ_1'' and ρ_2'', while $prob(\rho_1'', C) = 0 = prob(\rho_2'', C)$ for any other equivalence class C. ∎

Theorem 9.6. *Let $s_1, s_2 \in \mathcal{S}$. Then $s_1 \approx_{\rm pbf} s_2 \iff s_1 \approx_{\rm pb} s_2$.*

Proof. The proof is divided into two parts:

- Suppose that $s_1 \approx_{\rm pbf} s_2$ and let $\mathcal{B}$ be a weak probabilistic back-and-forth bisimulation over $\mathcal{U}$ such that $((s_1, \varepsilon), (s_2, \varepsilon)) \in \mathcal{B}$. Assume that $\mathcal{B}$ only contains all the pairs of $\approx_{\rm pbf}$-equivalent runs from s_1 and s_2, so that Lemma 9.5 is applicable to $\mathcal{B}$. We show that $\mathcal{B}' = \{(last(\rho_1), last(\rho_2)) \mid (\rho_1, \rho_2) \in \mathcal{B}\}$ is a probabilistic branching bisimulation over the states in $\mathcal{S}$ reachable from s_1 and s_2, from which $s_1 \approx_{\rm pb} s_2$ will follow. Note that $\mathcal{B}'$ is an equivalence relation because so is $\mathcal{B}$.
  Given $(last(\rho_1), last(\rho_2)) \in \mathcal{B}'$, by definition of $\mathcal{B}'$ we have that $(\rho_1, \rho_2) \in \mathcal{B}$. Let $r_k = last(\rho_k)$ for $k \in \{1, 2\}$, so that $(r_1, r_2) \in \mathcal{B}'$. Suppose that $r_1 \xrightarrow{a}_{\rm a} r_1'$, i.e., $\rho_1 \xrightarrow{a}_{\rm a} \rho_1'$ where $last(\rho_1') = r_1'$. There are two cases:

– If $a = \tau$ then from $(\rho_1, \rho_2) \in \mathcal{B}$ it follows that there exists $\rho_2 \Longrightarrow \rho_2'$ such that $(\rho_1', \rho_2') \in \mathcal{B}$. This means that we have a sequence of $n \geq 0$ transitions of the form $\rho_{2,i} \xrightarrow{\tau}_{\rm a} \rho_{2,i+1}$ or $\rho_{2,i} \xrightarrow{p_i}_{\rm p} \rho_{2,i+1}$ for all $0 \leq i \leq n-1$ – with τ-transitions and probabilistic transitions alternating – where $\rho_{2,0}$ is ρ_2 while $\rho_{2,n}$ is ρ_2' so that $(\rho_1', \rho_{2,n}) \in \mathcal{B}$ as $(\rho_1', \rho_2') \in \mathcal{B}$.
If $n = 0$ then we are done because ρ_2' is ρ_2 and hence $(\rho_1', \rho_2) \in \mathcal{B}$ as $(\rho_1', \rho_2') \in \mathcal{B}$ – thus $(r_1', r_2) \in \mathcal{B}'$ – otherwise from $\rho_{2,n}$ we go back to $\rho_{2,n-1}$ via $\rho_{2,n-1} \xrightarrow{\tau}_{\rm a} \rho_{2,n}$ or $\rho_{2,n-1} \xrightarrow{p_{n-1}}_{\rm p} \rho_{2,n}$. Recalling that $(\rho_1', \rho_{2,n}) \in \mathcal{B}$, if it is a τ-transition and ρ_1' can respond by staying idle, so that $(\rho_1', \rho_{2,n-1}) \in \mathcal{B}$, or it is a probabilistic transition with $(\rho_1', \rho_{2,n-1}) \in \mathcal{B}$, and $n = 1$, then we are done because $\rho_{2,n-1}$ is ρ_2 and hence $(\rho_1', \rho_2) \in \mathcal{B}$ as $(\rho_1', \rho_{2,n-1}) \in \mathcal{B}$ – thus $(r_1', r_2) \in \mathcal{B}'$ – otherwise we go further back to $\rho_{2,n-2}$ via $\rho_{2,n-2} \xrightarrow{\tau}_{\rm a} \rho_{2,n-1}$ or $\rho_{2,n-2} \xrightarrow{p_{n-2}}_{\rm p} \rho_{2,n-1}$. If it is a τ-transition and ρ_1' can respond by staying idle, so that $(\rho_1', \rho_{2,n-2}) \in \mathcal{B}$, or it is a probabilistic transition with $(\rho_1', \rho_{2,n-2}) \in \mathcal{B}$, and $n = 2$, then we are done because $\rho_{2,n-2}$ is ρ_2 and hence $(\rho_1', \rho_2) \in \mathcal{B}$ as $(\rho_1', \rho_{2,n-2}) \in \mathcal{B}$ – thus $(r_1', r_2) \in \mathcal{B}'$ – otherwise we keep going backward.
By repeating this procedure, since $(\rho_1', \rho_{2,n}) \in \mathcal{B}$ either we get to $(\rho_1', \rho_{2,n-n}) \in \mathcal{B}$ and we are done because this implies that $(\rho_1', \rho_2) \in \mathcal{B}$ – thus $(r_1', r_2) \in \mathcal{B}'$ – or for some $0 < m \leq n$ such that $(\rho_1', \rho_{2,m}) \in \mathcal{B}$ the incoming transition $\rho_{2,m-1} \xrightarrow{\tau}_{\rm a} \rho_{2,m}$ is matched by $\bar\rho_1 \Longrightarrow \rho_1 \xrightarrow{\tau}_{\rm a} \rho_1'$ with $(\bar\rho_1, \rho_{2,m-1}) \in \mathcal{B}$. In the latter case, since $last(\rho_1), last(\rho_{2,m-1}) \in \mathcal{S}_{\tt n}$, $\bar\rho_1 \Longrightarrow \rho_1$, $\rho_2 \Longrightarrow \rho_{2,m-1}$, $(\bar\rho_1, \rho_{2,m-1}) \in \mathcal{B}$, and $(\rho_1, \rho_2) \in \mathcal{B}$, from Lemma 9.5 we derive that $(\rho_1, \rho_{2,m-1}) \in \mathcal{B}$. Consequently $\rho_2 \Longrightarrow \rho_{2,m-1} \xrightarrow{\tau}_{\rm a} \rho_{2,m}$ with $(\rho_1, \rho_{2,m-1}) \in \mathcal{B}$ and $(\rho_1', \rho_{2,m}) \in \mathcal{B}$, thus $r_2 \Longrightarrow last(\rho_{2,m-1}) \xrightarrow{\tau}_{\rm a} last(\rho_{2,m})$ with $(r_1, last(\rho_{2,m-1})) \in \mathcal{B}'$ and $(r_1', last(\rho_{2,m})) \in \mathcal{B}'$.

– If $a \neq \tau$ then from $(\rho_1, \rho_2) \in \mathcal{B}$ it follows that there exists $\rho_2 \Longrightarrow \bar\rho_2 \xrightarrow{a}_{\rm a} \bar\rho_2' \Longrightarrow \rho_2'$ such that $(\rho_1', \rho_2') \in \mathcal{B}$. From $(\rho_1', \rho_2') \in \mathcal{B}$ and $\bar\rho_2' \Longrightarrow \rho_2'$ it follows that there exists $\bar\rho_1' \Longrightarrow \rho_1'$ such that $(\bar\rho_1', \bar\rho_2') \in \mathcal{B}$. Since $\rho_1 \xrightarrow{a}_{\rm a} \rho_1'$ and hence the last transition in ρ_1' is labeled with a, we derive that $\bar\rho_1'$ is ρ_1' and hence $(\rho_1', \bar\rho_2') \in \mathcal{B}$.
From $(\rho_1', \bar\rho_2') \in \mathcal{B}$ and $\bar\rho_2 \xrightarrow{a}_{\rm a} \bar\rho_2'$ it follows that there exists $\bar\rho_1 \Longrightarrow \rho_1 \xrightarrow{a}_{\rm a} \rho_1'$ such that $(\bar\rho_1, \bar\rho_2) \in \mathcal{B}$. Since $last(\rho_1), last(\bar\rho_2) \in \mathcal{S}_{\tt n}$, $\bar\rho_1 \Longrightarrow \rho_1$, $\rho_2 \Longrightarrow \bar\rho_2$, $(\bar\rho_1, \bar\rho_2) \in \mathcal{B}$, and $(\rho_1, \rho_2) \in \mathcal{B}$, from Lemma 9.5 we derive that $(\rho_1, \bar\rho_2) \in \mathcal{B}$.
Consequently $\rho_2 \Longrightarrow \bar\rho_2 \xrightarrow{a}_{\rm a} \bar\rho_2'$ with $(\rho_1, \bar\rho_2) \in \mathcal{B}$ and $(\rho_1', \bar\rho_2') \in \mathcal{B}$, thus $r_2 \Longrightarrow last(\bar\rho_2) \xrightarrow{a}_{\rm a} last(\bar\rho_2')$ with $(r_1, last(\bar\rho_2)) \in \mathcal{B}'$ and $(r_1', last(\bar\rho_2')) \in \mathcal{B}'$.

As for probabilities, given $\rho \in run(s_1) \cup run(s_2)$, the equivalence class C_ρ' with respect to $\mathcal{B}'$ is of the form $[last(\rho)]_{\mathcal{B}'} = \{last(\rho') \mid (last(\rho), last(\rho')) \in \mathcal{B}'\} = last(\{\rho' \mid (\rho, \rho') \in \mathcal{B}\}) = last([\rho]_{\mathcal{B}})$, i.e., $C_\rho' = last(C_\rho)$ for some equivalence class C_ρ with respect to $\mathcal{B}$, provided that function $last$ is lifted from runs to sets of runs. Therefore $prob(r_1, C_\rho') = prob(\rho_1, C_\rho) = prob(\rho_2, C_\rho) = prob(r_2, C_\rho')$ for all equivalence classes C_ρ' with respect to $\mathcal{B}'$ such that $C_\rho' = last(C_\rho)$ for some equivalence class C_ρ with respect to $\mathcal{B}$.

- Suppose that $s_1 \approx_{\rm pb} s_2$ and let $\mathcal{B}$ be a probabilistic branching bisimulation over $\mathcal{S}$ such that $(s_1, s_2) \in \mathcal{B}$. Assume that $\mathcal{B}$ only contains all the pairs of $\approx_{\rm pb}$-equivalent states reachable from s_1 and s_2. We show that the reflexive and transitive closure $\mathcal{B}'^*$ of $\mathcal{B}' = \{(\rho_1, \rho_2), (\rho_2, \rho_1) \in (run(s_1) \times run(s_2)) \cup (run(s_2) \times run(s_1)) \mid (last(\rho_1), last(\rho_2)) \in \mathcal{B}\}$ is a weak probabilistic back-and-forth bisimulation over the runs in $\mathcal{U}$ from s_1 and s_2, from which $(s_1, \varepsilon) \approx_{\rm pbf} (s_2, \varepsilon)$, i.e., $s_1 \approx_{\rm pbf} s_2$, will follow.
Given $(\rho_1, \rho_2) \in \mathcal{B}'$, by definition of $\mathcal{B}'$ we have that $(last(\rho_1), last(\rho_2)) \in \mathcal{B}$. Let $r_k = last(\rho_k)$ for $k \in \{1, 2\}$, so that $(r_1, r_2) \in \mathcal{B}$. There are two cases for action transitions:

– If $\rho_1 \xrightarrow{a}_{\rm a} \rho_1'$, i.e., $r_1 \xrightarrow{a}_{\rm a} r_1'$ where $r_1' = last(\rho_1')$, then either $a = \tau$ and $(r_1', r_2') \in \mathcal{B}$ where $r_2' = r_2$, or there exists $r_2 \Longrightarrow \bar{r}_2 \xrightarrow{a}_{\rm a} r_2'$ such that $(r_1, \bar{r}_2) \in \mathcal{B}$ and $(r_1', r_2') \in \mathcal{B}$. In both cases $\rho_2 \stackrel{\hat{a}}{\Longrightarrow} \rho_2'$ where $last(\rho_2') = r_2'$, so that $(\rho_1', \rho_2') \in \mathcal{B}'$.

– If $\rho_1' \xrightarrow{a}_{\rm a} \rho_1$, i.e., $r_1' \xrightarrow{a}_{\rm a} r_1$ where $r_1' = last(\rho_1')$, there are two subcases:

  * If ρ_1' is (s_1, ε), i.e., $r_1' \xrightarrow{a}_{\rm a} r_1$ is $s_1 \xrightarrow{a}_{\rm a} r_1$ and $last(\rho_1') = s_1$, then from $(s_1, s_2) \in \mathcal{B}$ it follows that either $a = \tau$ and $(r_1, r_2) \in \mathcal{B}$ where $r_2 = s_2$, or there exists $s_2 \Longrightarrow \bar{r}_2 \xrightarrow{a}_{\rm a} r_2$ such that $(s_1, \bar{r}_2) \in \mathcal{B}$ and $(r_1, r_2) \in \mathcal{B}$. In both cases $\rho_2' \stackrel{\hat{a}}{\Longrightarrow} \rho_2$ where $last(\rho_2') = s_2$, so that $(\rho_1', \rho_2') \in \mathcal{B}'$.
  * If ρ_1' is not (s_1, ε) then from $(s_1, s_2) \in \mathcal{B}$ it follows that s_1 reaches r_1' with a sequence of moves that are $\mathcal{B}$-compatible with those with which s_2 reaches some r_2' such that $(r_1', r_2') \in \mathcal{B}$ as $\mathcal{B}$ only contains all the states reachable from s_1 and s_2. Therefore either $a = \tau$ and $(r_1, r_2') \in \mathcal{B}$ where $r_2' = r_2$, or there exists $r_2' \Longrightarrow \bar{r}_2 \xrightarrow{a}_{\rm a} r_2$ such that $(r_1', \bar{r}_2) \in \mathcal{B}$ and $(r_1, r_2) \in \mathcal{B}$. In both cases $\rho_2' \stackrel{\hat{a}}{\Longrightarrow} \rho_2$ where $last(\rho_2') = r_2'$, so that $(\rho_1', \rho_2') \in \mathcal{B}'$.

As for probabilities, given $\rho \in run(s_1) \cup run(s_2)$, the equivalence class C_ρ' with respect to $\mathcal{B}'^*$ is of the form $[\rho]_{\mathcal{B}'^*} = \{\rho' \in run(s_1) \cup run(s_2) \mid last(\rho') \in [last(\rho)]_{\mathcal{B}}\}$, i.e., C_ρ' corresponds to some equivalence class C_ρ with respect to $\mathcal{B}$. Therefore $prob(\rho_1, C_\rho') = prob(last(\rho_1), C_\rho) = prob(last(\rho_2), C_\rho) = prob(\rho_2, C_\rho')$ for all equivalence classes C_ρ' with respect to $\mathcal{B}'^*$. ■

Therefore the properties BSNNI$_{\approx_{\rm pb}}$, BNDC$_{\approx_{\rm pb}}$, SBSNNI$_{\approx_{\rm pb}}$, P_BNDC$_{\approx_{\rm pb}}$, SBNDC$_{\approx_{\rm pb}}$ do not change if $\approx_{\rm pb}$ is replaced by $\approx_{\rm pbf}$. This allows us to study noninterference properties for reversible systems featuring nondeterminism and probabilities by using $\approx_{\rm pb}$ in a standard probabilistic process calculus like the one of Section 9.1.3.

9.4 Use Case: Probabilistic Smart Contract Lottery

Probabilistic modeling [11] and verification [136, 99] of smart contracts for blockchain-based, decentralized systems enable an in-depth analysis of potential vulnerabilities. This is even more important if we consider that probabilistic smart contracts for financial and gaming applications [51, 128, 118] have recently emerged in modern systems. In fact, subtle effects may be hidden in the implementation of randomness or in the inherent behavior of smart contracts.

As an example, in this section we employ our noninterference theory to analyze two vulnerabilities of a lottery implemented with a probabilistic smart contract [51] based on a public blockchain like, e.g., Ethereum. The first vulnerability can only be revealed by considering the probabilistic behavior of the smart contract, while the second one is intended to motivate the need to exploit the greater expressive power of branching bisimulation semantics over weak bisimulation semantics.

In the lottery, initially anyone can buy a ticket by invoking a dedicated smart contract function that allows one to pay a predefined amount for the ticket. When the lottery is closed, anyone can invoke another smart contract function, call it draw(), in which a random number x, between 1 and the number of sold tickets, is drawn and the entire amount of money is paid to the owner of ticket x.

The first critical issue that we consider is the randomization procedure of function draw(), which is not natively available to smart contract programmers. A widely adopted approach consists of using the timestamp of the

block including the transaction of the draw() invocation as the seed for random number generation. However, this approach is vulnerable in the presence of a malicious miner – who is also a lottery participant and hence buys a ticket – succeeding in mining the aforementioned block by choosing a timestamp that allows the miner to win the lottery.

Since both honest users and the malicious miner employ the same functionalities of the smart contract, we consider the invocations of smart contract functions as publicly observable low-level actions. To distinguish the interactions of the malicious miner from those of honest users, such actions are guarded by a high-level action h whenever they refer to the malicious miner. In this way, by looking at the public behavior of the smart contract, a low-level observer can detect whether or not the functioning of the lottery can be compromised by the malicious miner.

For simplicity, we assume that there are only two users buying one ticket each, where the malicious miner is the user buying ticket 1 whilst the honest user buys ticket 2. This scenario can be modeled in our probabilistic framework as follows where we omit [1]-prefixes:

$$\begin{aligned} \mathit{Lottery} \triangleq\ & \tau \,.\, \mathit{draw} \,.\, ([0.5]\mathit{winner}_1 \,.\, \mathit{notif}_1 \,.\, \underline{0} \oplus [0.5]\mathit{winner}_2 \,.\, \mathit{notif}_2 \,.\, \underline{0}) + \\ & h \,.\, \mathit{draw} \,.\, ([1-\varepsilon]\mathit{winner}_1 \,.\, \mathit{notif}_1 \,.\, \underline{0} \oplus [\varepsilon]\mathit{winner}_2 \,.\, \mathit{notif}_2 \,.\, \underline{0}) \end{aligned}$$

The invocation of function draw() shall lead to the probabilistic extraction of the ticket (action *draw*), the determination of the winner (actions winner_i), and the notification of the winner (actions notif_i). The initial nondeterministic choice between action τ and the only high-level action h models in the latter case the situation in which this procedure, instead of being fair, is guided by the malicious miner who is able to pilot the extraction at will ($\varepsilon > 0$ is considered to be negligible).

As far as nondeterministic noninterference analysis is concerned, process *Lottery* does not leak any information. More precisely, its nondeterministic variant satisfies all the security properties, for both nondeterministic weak bisimilarity and branching bisimilarity. The reason is that if we abstract away from probabilities, the behavior of the malicious miner (h-branch) is indistinguishable from the behavior of the honest user (τ-branch). However, *Lottery* is not $\mathrm{BSNNI}_{\approx}$ for $\approx \in \{\approx_{\mathrm{pw}}, \approx_{\mathrm{pb}}\}$, hence both bisimilarities can be used to capture the aforementioned interference in the probabilistic setting. Indeed, the version of *Lottery* with high-level actions hidden – which includes both the branch with fair extraction and the branch with unfair extraction – and the version of *Lottery* with high-level actions restricted – which includes only the fair branch – cannot be $\approx$-equivalent, because $[0.5]N_1 \oplus [0.5]N_2 \not\approx [1-\varepsilon]N_1 \oplus [\varepsilon]N_2$ for any pair of $\approx_{\mathrm{pr}}$-inequivalent nondeterministic processes N_1 and N_2 when $\varepsilon \neq 0.5$.

Assuming that the seed for random number generation cannot be manipulated, the second critical issue that we consider has to do with another vulnerability that emerges because of the peculiarities of the mining procedure. In fact, if the malicious miner realizes that he is going to lose the lottery and succeeds in mining the block, he can simply ignore the transaction related to the lottery extraction and force its rollback. We model such a behavior in the following way:

$$\begin{aligned} \mathit{Lottery}' \triangleq\ & \mathit{draw} \,.\, ([0.5]\mathit{winner}_1 \,.\, \mathit{notif}_1 \,.\, (\tau \,.\, (\mathit{success} \,.\, \underline{0} + \tau \,.\, \mathit{failure} \,.\, \underline{0})) \oplus \\ & [0.5]\mathit{winner}_2 \,.\, \mathit{notif}_2 \,.\, (\tau \,.\, (\mathit{success} \,.\, \underline{0} + \tau \,.\, \mathit{failure} \,.\, \underline{0}) + \\ & h \,.\, (\tau \,.\, (\mathit{success} \,.\, \underline{0} + \tau \,.\, \mathit{failure} \,.\, \underline{0}) + \\ & \mathit{failure} \,.\, \underline{0}))) \end{aligned}$$

With respect to the previous scenario, the malicious miner cannot affect the probabilistic behavior of the smart contract, i.e., the extraction procedure. However, he can try to interfere if the outcome of the extraction makes him lose, i.e., it is different from ticket 1.

On the one hand, consider the branch after action notif_1, which models the block mining procedure. The first τ-action expresses that the honest user is picked as a miner. The subsequent choice is between the successful mining (action *success*) and an event not depending on the miner (action τ) that causes the failure of the mining

(action *failure*). Notice that there might be several causes for this failure, such as a wrong transaction in the block, a fork in the blockchain, and so on. On the other hand, in the branch after action $notif_2$, the malicious miner may decide to participate actively in the mining procedure, as can be seen from the choice between the action τ, leading to the same behavior surveyed above, and the high-level action h. In the latter case, the race between the malicious miner and the honest user is solved nondeterministically through a choice between action τ and action *failure*. The former leads to the behavior of the honest user, while the latter represents the behavior of the malicious miner, who decides to cause the immediate failure of the mining operation.

Formally, process $Lottery'$ is $\mathrm{SBNDC}_{\approx_{\mathrm{pw}}}$. Indeed, observing that we have only one occurrence of the high-level action h, it holds that the subprocess $N_1 = \tau \,.\, (success \,.\, \underline{0} + \tau \,.\, failure \,.\, \underline{0})$ – denoting the low-level view before executing h – is weakly probabilistic bisimilar to the subprocess $N_2 = \tau \,.\, (success \,.\, \underline{0} + \tau \,.\, failure \,.\, \underline{0}) + failure \,.\, \underline{0}$ – denoting the low-level view after executing h. However, $Lottery'$ is not $\mathrm{BSNNI}_{\approx_{\mathrm{pb}}}$ as can be seen by comparing the only part – which is after action $notif_2$ – in which $Lottery' \setminus \{h\}$ and $Lottery' \,/\, \{h\}$ differ, i.e., N_1 and $N_1 + \tau \,.\, N_2$ respectively. In fact, N_1 is not probabilistic branching bisimilar to $N_1 + \tau \,.\, N_2$. This is because $N_1 \not\approx_{\mathrm{pb}} N_2$, while they are equated by $\approx_{\mathrm{pw}}$. In essence, N_1 cannot respond in accordance with $\approx_{\mathrm{pb}}$ when N_2 immediately executes action *failure*.

Intuitively, by applying back-and-forth reasoning to N_2 – which comes after action h – undoing the rightmost action *failure* reveals that the failure has been forced by the malicious miner, while undoing the leftmost action *failure* reveals that the failure has been the consequence of a choice involving also the action *success*. This is sufficient to expose the behavior of the malicious miner, which would not be detected by analyzing only the forward computations though. To conclude, the noninterference analysis based on the strongest $\approx_{\mathrm{pw}}$-based property of Figure 9.2 fails to reveal the covert channel caused by the malicious miner, while the weakest $\approx_{\mathrm{pb}}$-based property of Figure 9.2 can detect it.

Chapter 10

Noninterference Analysis of Stochastically Timed Reversible Systems

In this chapter, whose contents have appeared in [63], we extend the approach of the two previous chapters to a stochastically timed setting, so as to address noninterference properties in a framework featuring nondeterminism, time, and reversibility. More precisely, we move to a setting combining nondeterminism and stochastic time through the interactive Markov chain model of [90], in which transitions are divided into action transitions, each labeled with an action, and rate transitions, each labeled with a positive real number called rate that expresses an exponentially distributed time lapse. The reason for choosing this model in which time passing is orthogonal to action execution, with respect to a model in which action execution and time passing are integrated [83, 92, 93, 47, 127, 30, 23, 21] (see [24] for encodings between integrated-time and orthogonal-time calculi), is that the former naturally supports the definition of behavioral equivalences abstracting from unobservable actions [90], which are necessary for noninterference analysis, whereas this is not the case in the latter [22], which was employed in [5] for stochastic variants of BSNNI and SBNDC and in [94] for a stochastic variant of P_BNDC.

Following [90] we build a process calculus featuring action prefix separated from rate prefix. As for behavioral equivalences, we adopt the weak Markovian bisimilarity of [90] and introduce a Markovian branching bisimilarity. By using these two equivalences we recast the noninterference properties of [67, 69] for irreversible systems and the noninterference properties of the two previous chapters for reversible systems, respectively, to study their preservation and compositionality aspects as well as to provide a taxonomy similar to those in the two previous chapters. Reversibility comes into play by extending one of the results of [57] to the interactive Markov chain model; we show that a Markovian variant of weak back-and-forth bisimilarity coincides with our Markovian branching bisimilarity. Like in the previous chapter, for proving some results we have to resort to the bisimulation-up-to technique [131] and therefore introduce Markovian variants of up-to weak [112] and branching [75] bisimulations.

This chapter is organized as follows. In Section 10.1 we recall the interactive Markov chain model along with the definitions of strong and weak bisimilarities for it given in [90], a new notion of branching bisimilarity, and a process calculus interpreted on this model. In Section 10.2 we recast in this Markovian framework the aforementioned selection of noninterfence properties, study their preservation and compositionality characteristics, develop their taxonomy, and relate it to the nondeterministic and probabilistic taxonomies. In Section 10.3 we establish a connection with reversibility by introducing a weak Markovian back-and-forth bisimilarity and proving that it coincides with Markovian branching bisimilarity. Finally, in Section 10.4 we extend the DBMS example of Sections 8.2 and 8.5 with time-related information and obfuscation and permission mechanisms to show the adequacy of our approach to handle information flows in systems featuring nondeterminism and stochastic time.

10.1 Background Definitions and Results

In this section we recall the interactive Markov chain model of [90] (Section 10.1.1) along with its strong and weak Markovian bisimilarities and define a novel Markovian branching bisimilarity (Section 10.1.2). Then we introduce a Markovian process language inspired by [90] (Section 10.1.3) through which we will express bisimulation-based information-flow security properties accounting for nondeterminism and stochastic time.

10.1.1 Markovian Labeled Transition Systems

To represent the behavior of a process featuring nondeterminism and stochastic time, we use a Markovian labeled transition system. This is a variant of a labeled transition system [97] where, according to the interactive Markov chain model of [90], transitions are labeled with actions or positive real numbers called rates expressing exponentially distributed delays. We recall that the action set $\mathcal{A}$ contains the unobservable action τ.

Definition 10.1. *A* Markovian labeled transition system (MLTS) *is a triple* $(\mathcal{S}, \mathcal{A}, \longrightarrow)$ *where* $\mathcal{S}$ *is an at most countable set of states,* $\mathcal{A}$ *is a countable set of actions, and* $\longrightarrow = \longrightarrow_{\rm a} \cup \longrightarrow_{\rm r}$ *is the transition relation, with* $\longrightarrow_{\rm a} \subseteq \mathcal{S} \times \mathcal{A} \times \mathcal{S}$ *being the action transition relation whilst* $\longrightarrow_{\rm r} \subseteq \mathcal{S} \times \mathbb{R}_{>0} \times \mathcal{S}$ *being the rate transition relation.* ■

An action transition (s, a, s') is written $s \stackrel{a}{\longrightarrow}_{\rm a} s'$ while a rate transition (s, λ, s') is written $s \stackrel{\lambda}{\longrightarrow}_{\rm r} s'$, where s is the source state and s' is the target state. We say that s' is reachable from s, written $s' \in \mathit{reach}(s)$, iff $s' = s$ or there exists a sequence of finitely many transitions such that the target state of each of them coincides with the source state of the subsequent one, with the source of the first one being s and the target of the last one being s'.

The label of a rate transition is the inverse of the average duration of the corresponding exponentially distributed delay, which enjoys the *memoryless property*: the residual duration after the execution starts is still exponentially distributed with the same rate. If the outgoing rate transitions of state s are $s \stackrel{\lambda_i}{\longrightarrow}_{\rm r} s_i$ for $1 \leq i \leq n$, then the *race policy* applies. This means that the average sojourn time in s is given by the minimum of the n exponentially distributed delays – which is exponentially distributed with rate $\sum_{1 \leq i \leq n} \lambda_i$ – and the execution probability of transition j is given by $\lambda_j / \sum_{1 \leq i \leq n} \lambda_i$. As for the interplay between action transitions and rate transitions, like in [90] we assume *maximal progress*, i.e., τ-transitions take precedence over rate transitions.

10.1.2 Markovian Bisimulation Equivalences

Bisimilarity [117, 112] identifies processes that are able to mimic each other's behavior stepwise, i.e., having the same branching structure. In the interactive Markov chain model, this extends to stochastic behavior [90]. Let $\mathit{rate}(s, C) = \sum_{s \stackrel{\lambda}{\longrightarrow}_{\rm r} s', s' \in C} \lambda$ be the cumulative rate with which state s reaches a state in C. Due to maximal progress, cumulative rates are compared only in states with no outgoing τ-transitions, denoted $\stackrel{\tau}{\not\longrightarrow}_{\rm a}$.

Definition 10.2. *Let* $(\mathcal{S}, \mathcal{A}, \longrightarrow)$ *be an MLTS. We say that* $s_1, s_2 \in \mathcal{S}$ *are* strongly Markovian bisimilar*, written* $s_1 \sim_{\rm m} s_2$*, iff* $(s_1, s_2) \in \mathcal{B}$ *for some strong Markovian bisimulation* $\mathcal{B}$*. An equivalence relation* $\mathcal{B}$ *over* $\mathcal{S}$ *is a* strong Markovian bisimulation *iff, whenever* $(s_1, s_2) \in \mathcal{B}$*, then:*

- *For each* $s_1 \stackrel{a}{\longrightarrow}_{\rm a} s_1'$ *there exists* $s_2 \stackrel{a}{\longrightarrow}_{\rm a} s_2'$ *such that* $(s_1', s_2') \in \mathcal{B}$*.*
- *If* $s_1 \stackrel{\tau}{\not\longrightarrow}_{\rm a}$ *then* $\mathit{rate}(s_1, C) = \mathit{rate}(s_2, C)$ *for all equivalence classes* $C \in \mathcal{S}/\mathcal{B}$*.* ■

Weak bisimilarity [112] is additionally capable of abstracting from unobservable actions. Let $s \stackrel{\tau^*}{\Longrightarrow}_{\rm a} s'$ mean that $s' \in reach(s)$ and, when $s' \neq s$, there exists a finite sequence of transitions from s to s' each of which is labeled with τ. Moreover let $\stackrel{\hat{a}}{\Longrightarrow}_{\rm a}$ stand for $\stackrel{\tau^*}{\Longrightarrow}_{\rm a}$ if $a = \tau$ or $\stackrel{\tau^*}{\Longrightarrow}_{\rm a} \stackrel{a}{\longrightarrow}_{\rm a} \stackrel{\tau^*}{\Longrightarrow}_{\rm a}$ if $a \neq \tau$. The Markovian adaptation below is taken from [90]. Unlike [112], due to its second clause it is sensitive to divergence, i.e., cycles of τ-transitions.

Definition 10.3. *Let $(\mathcal{S}, \mathcal{A}, \longrightarrow)$ be an MLTS. We say that $s_1, s_2 \in \mathcal{S}$ are* weakly Markovian bisimilar*, written $s_1 \approx_{\rm mw} s_2$, iff $(s_1, s_2) \in \mathcal{B}$ for some weak Markovian bisimulation $\mathcal{B}$. An equivalence relation $\mathcal{B}$ over $\mathcal{S}$ is a* weak Markovian bisimulation *iff, whenever $(s_1, s_2) \in \mathcal{B}$, then:*

- *For each $s_1 \stackrel{a}{\longrightarrow}_{\rm a} s_1'$ there exists $s_2 \stackrel{\hat{a}}{\Longrightarrow}_{\rm a} s_2'$ such that $(s_1', s_2') \in \mathcal{B}$.*
- *If $s_1 \stackrel{\tau}{\not\longrightarrow}_{\rm a}$ then there exists $s_2 \stackrel{\tau^*}{\Longrightarrow}_{\rm a} \bar{s}_2$ such that $\bar{s}_2 \stackrel{\tau}{\not\longrightarrow}_{\rm a}$, $(s_1, \bar{s}_2) \in \mathcal{B}$, and $rate(s_1, C) = rate(\bar{s}_2, C)$ for all equivalence classes $C \in \mathcal{S}/\mathcal{B}$.* ■

Branching bisimilarity [80] is finer than weak bisimilarity as it preserves the branching structure of processes even when abstracting from τ-actions – see condition $(s_1, \bar{s}_2) \in \mathcal{B}$ in the definition below. We adapt it to the Markovian setting as follows.

Definition 10.4. *Let $(\mathcal{S}, \mathcal{A}, \longrightarrow)$ be an MLTS. We say that $s_1, s_2 \in \mathcal{S}$ are* Markovian branching bisimilar*, written $s_1 \approx_{\rm mb} s_2$, iff $(s_1, s_2) \in \mathcal{B}$ for some Markovian branching bisimulation $\mathcal{B}$. An equivalence relation $\mathcal{B}$ over $\mathcal{S}$ is a* Markovian branching bisimulation *iff, whenever $(s_1, s_2) \in \mathcal{B}$, then:*

- *For each $s_1 \stackrel{a}{\longrightarrow}_{\rm a} s_1'$:*
  - *either $a = \tau$ and $(s_1', s_2) \in \mathcal{B}$;*
  - *or there exists $s_2 \stackrel{\tau^*}{\Longrightarrow}_{\rm a} \bar{s}_2 \stackrel{a}{\longrightarrow}_{\rm a} s_2'$ such that $(s_1, \bar{s}_2) \in \mathcal{B}$ and $(s_1', s_2') \in \mathcal{B}$.*
- *If $s_1 \stackrel{\tau}{\not\longrightarrow}_{\rm a}$ then there exists $s_2 \stackrel{\tau^*}{\Longrightarrow}_{\rm a} \bar{s}_2$ such that $\bar{s}_2 \stackrel{\tau}{\not\longrightarrow}_{\rm a}$, $(s_1, \bar{s}_2) \in \mathcal{B}$, and $rate(s_1, C) = rate(\bar{s}_2, C)$ for all equivalence classes $C \in \mathcal{S}/\mathcal{B}$.* ■

In [90] it is argued that the weak bisimilarity of Definition 10.3 is already very close to branching bisimilarity, because maximal progress forces a check given by condition $(s_1, \bar{s}_2) \in \mathcal{B}$ on the branching structure of the considered processes. We show that our novel Definition 10.4, which sticks to the original one of [80], is more discriminating. Consider Figure 10.1, where every MLTS is depicted as a directed graph in which vertices represent states and action- or rate-labeled edges represent transitions. The initial states s_1 and s_2 of the two MLTSs are weakly Markovian bisimilar but not Markovian branching bisimilar. On the one hand, each of the two states reachable from s_1 with rate 3.4 and the state reachable from s_2 with rate 6.8 after a τ-transition are all weakly Markovian bisimilar and hence the cumulative rate to reach them is the same from both initial states. On the other hand, the two states reachable from s_1 are not Markovian branching bisimilar, because if the one on the right performs a then the one on the left cannot respond by performing τ followed by a because the state reached after τ no longer enables b. Thus, with respect to Markovian branching bisimilarity, s_1 reaches with rate 3.4 two different equivalence classes, while s_2 reaches with rate 6.8 only one of them.

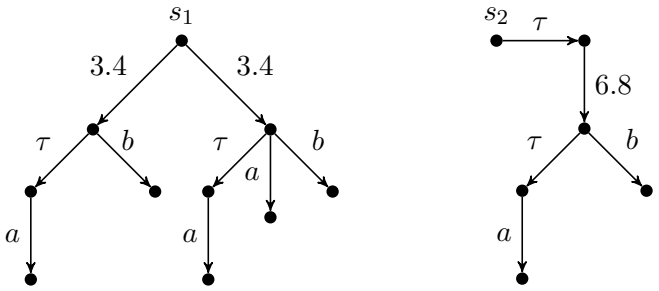


Figure 10.1: States related by $\approx_{\mathrm{mw}}$ but distinguished by $\approx_{\mathrm{mb}}$

10.1.3 A Markovian Process Calculus with High and Low Actions

We now introduce a Markovian process calculus to formalize the security properties of interest. To address two security levels, like in the two previous chapters we partition the set $\mathcal{A} \setminus \{\tau\}$ of observable actions into $\mathcal{A}_{\mathcal{H}} \cup \mathcal{A}_{\mathcal{L}}$, with $\mathcal{A}_{\mathcal{H}} \cap \mathcal{A}_{\mathcal{L}} = \emptyset$, where $\mathcal{A}_{\mathcal{H}}$ is the set of high-level actions, ranged over by h, and $\mathcal{A}_{\mathcal{L}}$ is the set of low-level actions, ranged over by l. Note that $\tau \notin \mathcal{A}_{\mathcal{H}} \cup \mathcal{A}_{\mathcal{L}}$.

The set $\mathbb{P}_{\mathrm{mk}}$ of process terms is obtained by considering typical operators from CCS [112] and CSP [45] together with rate prefix from [90]. In addition to prefix, choice, and parallel composition – taken from CSP so as not to turn synchronizations among high-level actions into τ as would happen with the CCS parallel composition – we include restriction and hiding, as they are necessary to formalize noninterference properties, and recursion. The syntax for $\mathbb{P}_{\mathrm{mk}}$ is:

$$P ::= \underline{0} \mid a \,.\, P \mid (\lambda) \,.\, P \mid P + P \mid P \parallel_L P \mid P \setminus L \mid P / L \mid K$$

where:

- $\underline{0}$ is the terminated process.
- $a \,.\, \_$, for $a \in \mathcal{A}$, is the action prefix operator describing a process that can initially perform action a.
- $(\lambda) \,.\, \_$, for $\lambda \in \mathbb{R}_{>0}$, is the rate prefix operator describing a process that can initially let an exponentially distributed delay pass with average duration $1/\lambda$.
- $\_ + \_$ is the alternative composition operator expressing a choice between two processes, which is nondeterministic in case of actions, probabilistic in case of rates according to the race policy, or subject to maximal progress otherwise.
- $\_ \parallel_L \_$, for $L \subseteq \mathcal{A} \setminus \{\tau\}$, is the parallel composition operator allowing two processes to proceed independently on any action not in L as well as on rates thanks to the memoryless property of exponential distributions [90] and forcing them to synchronize on every action in L.
- $\_ \setminus L$, for $L \subseteq \mathcal{A} \setminus \{\tau\}$, is the restriction operator, which prevents the execution of all actions belonging to L.
- $\_ / L$, for $L \subseteq \mathcal{A} \setminus \{\tau\}$, is the hiding operator, which turns all the executed actions belonging to L into the unobservable action τ.

Prefix	$a \,.\, P \xrightarrow{a}_{\mathrm{a}} P$
Choice	$\dfrac{P_1 \xrightarrow{a}_{\mathrm{a}} P_1'}{P_1 + P_2 \xrightarrow{a}_{\mathrm{a}} P_1'} \qquad \dfrac{P_2 \xrightarrow{a}_{\mathrm{a}} P_2'}{P_1 + P_2 \xrightarrow{a}_{\mathrm{a}} P_2'}$
Parallel	$\dfrac{P_1 \xrightarrow{a}_{\mathrm{a}} P_1' \quad a \notin L}{P_1 \parallel_L P_2 \xrightarrow{a}_{\mathrm{a}} P_1' \parallel_L P_2} \qquad \dfrac{P_2 \xrightarrow{a}_{\mathrm{a}} P_2' \quad a \notin L}{P_1 \parallel_L P_2 \xrightarrow{a}_{\mathrm{a}} P_1 \parallel_L P_2'}$
Synch	$\dfrac{P_1 \xrightarrow{a}_{\mathrm{a}} P_1' \quad P_2 \xrightarrow{a}_{\mathrm{a}} P_2' \quad a \in L}{P_1 \parallel_L P_2 \xrightarrow{a}_{\mathrm{a}} P_1' \parallel_L P_2'}$
Restriction	$\dfrac{P \xrightarrow{a}_{\mathrm{a}} P' \quad a \notin L}{P \setminus L \xrightarrow{a}_{\mathrm{a}} P' \setminus L}$
Hiding	$\dfrac{P \xrightarrow{a}_{\mathrm{a}} P' \quad a \in L}{P \,/\, L \xrightarrow{\tau}_{\mathrm{a}} P' \,/\, L} \qquad \dfrac{P \xrightarrow{a}_{\mathrm{a}} P' \quad a \notin L}{P \,/\, L \xrightarrow{a}_{\mathrm{a}} P' \,/\, L}$
Constant	$\dfrac{K \triangleq P \quad P \xrightarrow{a}_{\mathrm{a}} P'}{K \xrightarrow{a}_{\mathrm{a}} P'}$

Table 10.1: Operational semantic rules for action transitions

- K is a process constant equipped with a defining equation of the form $K \triangleq P$, where every constant possibly occurring in P – including K itself thus allowing for recursion – must be in the scope of an action prefix.

The operational semantic rules for the process language are shown in Tables 10.1 and 10.2 for action and rate transitions respectively. Together they produce the MLTS $(\mathbb{P}_{\mathrm{mk}}, \mathcal{A}, \longrightarrow)$ where $\longrightarrow = \longrightarrow_{\mathrm{a}} \cup \longrightarrow_{\mathrm{r}}$, to which the bisimulation equivalences defined in Section 10.1.2 are applicable. While $\longrightarrow_{\mathrm{a}} \subseteq \mathbb{P}_{\mathrm{mk}} \times \mathcal{A} \times \mathbb{P}_{\mathrm{mk}}$ is a relation, $\longrightarrow_{\mathrm{r}} \subseteq \mathbb{P}_{\mathrm{mk}} \times \mathbb{R}_{>0} \times \mathbb{P}_{\mathrm{mk}}$ is deemed to be a multirelation [90]; e.g., from $(\lambda_1) \,.\, P + (\lambda_2) \,.\, P$ there must be two rate transitions to P even when $\lambda_1 = \lambda_2$ otherwise the average sojourn time in the source process would be altered.

10.2 Markovian Information-Flow Security Properties

In this section, after recasting the definitions of noninterference properties of the two previous chapters by taking as behavioral equivalence the weak or branching bisimilarity of Section 10.1.2, we investigate their preservation and compositionality characteristics (Section 10.2.1), we show the inclusion relationships between the ones based on $\approx_{\mathrm{mw}}$ and the ones based on $\approx_{\mathrm{mb}}$ (Section 10.2.2), and we relate the resulting Markovian taxonomy with the nondeterministic and probabilistic ones (Section 10.2.3).

Definition 10.5. *Let $P \in \mathbb{P}_{\mathrm{mk}}$ and $\approx \in \{\approx_{\mathrm{mw}}, \approx_{\mathrm{mb}}\}$:*

- $P \in \mathrm{BSNNI}_{\approx} \iff P \setminus \mathcal{A}_{\mathcal{H}} \approx P \,/\, \mathcal{A}_{\mathcal{H}}$.
- $P \in \mathrm{BNDC}_{\approx} \iff$ *for all $Q \in \mathbb{P}_{\mathrm{mk}}$ such that each of its prefixes belongs to $\mathcal{A}_{\mathcal{H}}$ and for all $L \subseteq \mathcal{A}_{\mathcal{H}}$, $P \setminus \mathcal{A}_{\mathcal{H}} \approx ((P \parallel_L Q) \,/\, L) \setminus \mathcal{A}_{\mathcal{H}}$.*

$$\textit{RatePrefix}\quad (\lambda)\,.\,P \xrightarrow{\lambda}_{\mathrm{r}} P$$

$$\textit{RateChoice}\quad \frac{P_1 \xrightarrow{\lambda}_{\mathrm{r}} P_1'}{P_1 + P_2 \xrightarrow{\lambda}_{\mathrm{r}} P_1'} \qquad \frac{P_2 \xrightarrow{\lambda}_{\mathrm{r}} P_2'}{P_1 + P_2 \xrightarrow{\lambda}_{\mathrm{r}} P_2'}$$

$$\textit{RateParallel}\quad \frac{P_1 \xrightarrow{\lambda}_{\mathrm{r}} P_1'}{P_1 \parallel_L P_2 \xrightarrow{\lambda}_{\mathrm{r}} P_1' \parallel_L P_2} \qquad \frac{P_2 \xrightarrow{\lambda}_{\mathrm{r}} P_2'}{P_1 \parallel_L P_2 \xrightarrow{\lambda}_{\mathrm{r}} P_1 \parallel_L P_2'}$$

$$\textit{RateRestriction}\quad \frac{P \xrightarrow{\lambda}_{\mathrm{r}} P'}{P \setminus L \xrightarrow{\lambda}_{\mathrm{r}} P' \setminus L}$$

$$\textit{RateHiding}\quad \frac{P \xrightarrow{\lambda}_{\mathrm{r}} P'}{P \,/\, L \xrightarrow{\lambda}_{\mathrm{r}} P' \,/\, L}$$

$$\textit{RateConstant}\quad \frac{K \triangleq P \quad P \xrightarrow{\lambda}_{\mathrm{r}} P'}{K \xrightarrow{\lambda}_{\mathrm{r}} P'}$$

Table 10.2: Operational semantic rules for rate transitions

- $P \in \mathrm{SBSNNI}_{\approx} \iff$ *for all* $P' \in \mathit{reach}(P)$, $P' \in \mathrm{BSNNI}_{\approx}$.
- $P \in \mathrm{P\_BNDC}_{\approx} \iff$ *for all* $P' \in \mathit{reach}(P)$, $P' \in \mathrm{BNDC}_{\approx}$.
- $P \in \mathrm{SBNDC}_{\approx} \iff$ *for all* $P', P'' \in \mathit{reach}(P)$ *such that* $P' \xrightarrow{h}_{\mathrm{a}} P''$, $P' \setminus \mathcal{A}_{\mathcal{H}} \approx P'' \setminus \mathcal{A}_{\mathcal{H}}$. ■

To see the different distinguishing power of these Markovian noninterference properties, we can adapt the examples of Section 8.1.4. For instance, in this Markovian setting, a low-level agent that observes the execution of l in $P = l\,.\,(2 \cdot \lambda)\,.\,\underline{0} + l\,.\,((\lambda)\,.\,h\,.\,l_1\,.\,\underline{0} + (\lambda)\,.\,h\,.\,l_2\,.\,\underline{0}) + l\,.\,((\lambda)\,.\,l_1\,.\,\underline{0} + (\lambda)\,.\,l_2\,.\,\underline{0})$ cannot infer anything about the execution of h. Indeed, after the execution of l, what the low-level agent observes is either a terminal state, reached with rate $2 \cdot \lambda$, or the execution of either l_1 or l_2, both with rate λ. Formally, $P \setminus \{h\} \approx P \,/\, \{h\}$ because $l\,.\,(2 \cdot \lambda)\,.\,\underline{0} + l\,.\,((\lambda)\,.\,\underline{0} + (\lambda)\,.\,\underline{0}) + l\,.\,((\lambda)\,.\,l_1\,.\,\underline{0} + (\lambda)\,.\,l_2\,.\,\underline{0}) \approx l\,.\,(2 \cdot \lambda)\,.\,\underline{0} + l\,.\,((\lambda)\,.\,\tau\,.\,l_1\,.\,\underline{0} + (\lambda)\,.\,\tau\,.\,l_2\,.\,\underline{0}) + l\,.\,((\lambda)\,.\,l_1\,.\,\underline{0} + (\lambda)\,.\,l_2\,.\,\underline{0})$, hence P is $\mathrm{BSNNI}_{\approx}$.

On the other hand, in $Q = l\,.\,(2 \cdot \lambda)\,.\,\underline{0} + l\,.\,((\lambda)\,.\,h_1\,.\,l_1\,.\,\underline{0} + (\lambda)\,.\,h_2\,.\,l_2\,.\,\underline{0}) + l\,.\,((\lambda)\,.\,l_1\,.\,\underline{0} + (\lambda)\,.\,l_2\,.\,\underline{0})$, which is $\mathrm{BSNNI}_{\approx}$ for the same reason discussed above, a high-level agent could decide to enable only h_1, thus turning the low-level view of the system into $l\,.\,(2 \cdot \lambda)\,.\,\underline{0} + l\,.\,((\lambda)\,.\,\tau\,.\,l_1\,.\,\underline{0} + (\lambda)\,.\,\underline{0}) + l\,.\,((\lambda)\,.\,l_1\,.\,\underline{0} + (\lambda)\,.\,l_2\,.\,\underline{0})$, which is clearly distinguishable from $l\,.\,(2 \cdot \lambda)\,.\,\underline{0} + l\,.\,((\lambda)\,.\,\underline{0} + (\lambda)\,.\,\underline{0}) + l\,.\,((\lambda)\,.\,l_1\,.\,\underline{0} + (\lambda)\,.\,l_2\,.\,\underline{0})$, as in the former there is a case in which the low-level agent can observe l_1 but not l_2 after the execution of l. In other words, Q is not $\mathrm{BNDC}_{\approx}$.

Note that in this Markovian setting the high-level agent Q cannot exhibit any rate prefix by definition, otherwise no process would satisfy the BNDC property. To see why, consider the trivially safe process $l\,.\,\underline{0}$ and the high-level agent $(\lambda)\,.\,h\,.\,\underline{0}$. The processes $(l\,.\,\underline{0}) \setminus \mathcal{A}_{\mathcal{H}}$ and $((l\,.\,\underline{0} \parallel_L (\lambda)\,.\,h\,.\,\underline{0}) \,/\, L) \setminus \mathcal{A}_{\mathcal{H}}$ are not equivalent, regardless of the specific $L \subseteq \mathcal{A}_{\mathcal{H}}$, because the former can only perform the low-level action l while the latter can also let time pass before or after the execution of l.

10.2.1 Preservation and Compositionality

All the Markovian noninterference properties of Definition 10.5 turn out to be preserved by the bisimilarity employed in their definition. This means that if a process P_1 is secure under any of such properties, then every other equivalent process P_2 is secure too according to the same property. This is very useful for automated property verification, as it allows us to work with the process with the smallest state space among the equivalent ones.

The preservation result of Theorem 10.1 immediately follows from Lemma 10.1 below, which ensures that $\approx_{\rm mw}$ and $\approx_{\rm mb}$ are congruences with respect to all the operators occurring in the aforementioned noninterference properties. Congruence with respect to action and rate prefixes is also addressed as it will be exploited in the proof of the compositionality result of Theorem 10.2. Some of the following congruence properties for $\approx_{\rm mw}$ are already known from [90].

Lemma 10.1. *Let $P_1, P_2 \in \mathbb{P}_{\rm mk}$ and $\approx \in \{\approx_{\rm mw}, \approx_{\rm mb}\}$. If $P_1 \approx P_2$ then:*

1. *$a\,.\,P_1 \approx a\,.\,P_2$ for all $a \in \mathcal{A}$.*
2. *$(\lambda)\,.\,P_1 \approx (\lambda)\,.\,P_2$ for all $\lambda \in \mathbb{R}_{>0}$.*
3. *$P_1 \parallel_L P \approx P_2 \parallel_L P$ and $P \parallel_L P_1 \approx P \parallel_L P_2$ for all $L \subseteq \mathcal{A} \setminus \{\tau\}$ and $P \in \mathbb{P}_{\rm mk}$.*
4. *$P_1 \setminus L \approx P_2 \setminus L$ for all $L \subseteq \mathcal{A} \setminus \{\tau\}$.*
5. *$P_1 / L \approx P_2 / L$ for all $L \subseteq \mathcal{A} \setminus \{\tau\}$.* ∎

Proof. We first prove the five results for the $\approx_{\rm pw}$-based properties. The congruence of $\approx_{\rm mw}$ with respect to action prefix, rate prefix, parallel composition, and hiding has already been proven in [90], so we focus only on restriction. Let $\mathcal{B}$ be a weak Markovian bisimulation witnessing $P_1 \approx_{\rm mw} P_2$:

1. The equivalence relation $\mathcal{B}' = \mathcal{I}_{\mathbb{P}_{\rm mk}} \cup \{(Q_1 \setminus L, Q_2 \setminus L) \mid (Q_1, Q_2) \in \mathcal{B}\}$ is a weak Markovian bisimulation too. Given $(Q_1 \setminus L, Q_2 \setminus L) \in \mathcal{B}'$ with $(Q_1, Q_2) \in \mathcal{B}$, there are two cases for action transitions based on the operational semantic rules in Table 10.1:

   - If $Q_1 \setminus L \xrightarrow{\tau}_{\rm a} Q_1' \setminus L$ with $Q_1 \xrightarrow{\tau}_{\rm a} Q_1'$, then there exists $Q_2 \xRightarrow{\tau^*}_{\rm a} Q_2'$ such that $(Q_1', Q_2') \in \mathcal{B}$. Since the restriction operator does not apply to τ, we have that $Q_2 \setminus L \xRightarrow{\tau^*}_{\rm a} Q_2' \setminus L$ with $(Q_1' \setminus L, Q_2' \setminus L) \in \mathcal{B}'$.
   - If $Q_1 \setminus L \xrightarrow{a}_{\rm a} Q_1' \setminus L$ with $Q_1 \xrightarrow{a}_{\rm a} Q_1'$ and $a \notin L \cup \{\tau\}$, then there exists $Q_2 \xRightarrow{\tau^*}_{\rm a} \xrightarrow{a}_{\rm a} \xRightarrow{\tau^*}_{\rm a} Q_2'$ such that $(Q_1', Q_2') \in \mathcal{B}$. Since the restriction operator does not apply to τ and $a \notin L$, we have that $Q_2 \setminus L \xRightarrow{\tau^*}_{\rm a} \xrightarrow{a}_{\rm a} \xRightarrow{\tau^*}_{\rm a} Q_2' \setminus L$ with $(Q_1' \setminus L, Q_2' \setminus L) \in \mathcal{B}'$.

   As for rates, to avoid trivial cases consider an equivalence class $C' = C \setminus L = \{Q \setminus L \mid Q \in C\}$ for some $C \in \mathbb{P}_{\rm mk}/\mathcal{B}$. Suppose that $Q_1 \setminus L \not\xrightarrow{\tau}_{\rm a}$ so that $Q_1 \not\xrightarrow{\tau}_{\rm a}$ too and hence from $(Q_1, Q_2) \in \mathcal{B}$ it follows that there exists $Q_2 \xRightarrow{\tau^*}_{\rm a} \bar{Q}_2$ such that $\bar{Q}_2 \not\xrightarrow{\tau}_{\rm a}$, $(Q_1, \bar{Q}_2) \in \mathcal{B}$, and $rate(Q_1, C) = rate(\bar{Q}_2, C)$. Since the restriction operator does not apply to τ and rate transitions, we have that $Q_2 \setminus L \xRightarrow{\tau^*}_{\rm a} \bar{Q}_2 \setminus L$ with $\bar{Q}_2 \setminus L \not\xrightarrow{\tau}_{\rm a}$, $(Q_1 \setminus L, \bar{Q}_2 \setminus L) \in \mathcal{B}'$, and $rate(Q_1 \setminus L, C') = rate(Q_1, C) = rate(\bar{Q}_2, C) = rate(\bar{Q}_2 \setminus L, C')$.

We then prove the five results for the $\approx_{\rm mb}$-based properties. Let $\mathcal{B}$ be a Markovian branching bisimulation witnessing $P_1 \approx_{\rm mb} P_2$:

1. The equivalence relation $\mathcal{B}' = (\mathcal{B} \cup \{(a\,.\,Q_1, a\,.\,Q_2) \mid (Q_1, Q_2) \in \mathcal{B}\})^+$ is a Markovian branching bisimulation too. The result immediately follows from the fact that, given $(a\,.\,Q_1, a\,.\,Q_2) \in \mathcal{B}'$ with $(Q_1, Q_2) \in \mathcal{B}$, $a\,.\,Q_1 \xrightarrow{a}_{\rm a} Q_1$ is matched by $a\,.\,Q_2 \stackrel{\tau^*}{\Longrightarrow}_{\rm a} a\,.\,Q_2 \xrightarrow{a}_{\rm a} Q_2$ with $(a\,.\,Q_1, a\,.\,Q_2) \in \mathcal{B}'$ and $(Q_1, Q_2) \in \mathcal{B}'$ as well as, in the case $a \neq \tau$, $a\,.\,Q_1 \stackrel{\tau}{\not\longrightarrow}_{\rm a}$ with $a\,.\,Q_2 \stackrel{\tau^*}{\Longrightarrow}_{\rm a} a\,.\,Q_2 \stackrel{\tau}{\not\longrightarrow}_{\rm a}$ and $\mathit{rate}(a\,.\,Q_1, C') = \mathit{rate}(a\,.\,Q_2, C') = 0$ for all $C' \in \mathbb{P}_{\rm mk}/\mathcal{B}'$.

2. The equivalence relation $\mathcal{B}' = (\mathcal{B} \cup \{((\lambda)\,.\,Q_1, (\lambda)\,.\,Q_2) \mid (Q_1, Q_2) \in \mathcal{B}\})^+$ is a Markovian branching bisimulation too. The result immediately follows from the fact that, given $((\lambda)\,.\,Q_1, (\lambda)\,.\,Q_2) \in \mathcal{B}'$ with $(Q_1, Q_2) \in \mathcal{B}$, both processes can only perform a λ-transition. Precisely, $(\lambda)\,.\,Q_1 \stackrel{\tau}{\not\longrightarrow}_{\rm a}$ with $(\lambda)\,.\,Q_2 \stackrel{\tau^*}{\Longrightarrow}_{\rm a} (\lambda)\,.\,Q_2 \stackrel{\tau}{\not\longrightarrow}_{\rm a}$ and $\mathit{rate}((\lambda)\,.\,Q_1, \bar{C}) = \mathit{rate}((\lambda)\,.\,Q_2, \bar{C}) = \lambda$ for $\bar{C} = [Q_1]_{\mathcal{B}'}$ while $\mathit{rate}((\lambda)\,.\,Q_1, C') = \mathit{rate}((\lambda)\,.\,Q_2, C') = 0$ for any other $C' \in \mathbb{P}_{\rm mk}/\mathcal{B}'$.

3. The equivalence relation $\mathcal{B}' = \mathcal{I}_{\mathbb{P}_{\rm mk}} \cup \{(Q_1 \parallel_L Q, Q_2 \parallel_L Q) \mid (Q_1, Q_2) \in \mathcal{B} \wedge Q \in \mathbb{P}_{\rm mk}\}$ and its variant $\mathcal{B}''$ in which Q occurs to the left of parallel composition in each pair are Markovian branching bisimulations too. Let us focus on $\mathcal{B}'$. Given $(Q_1 \parallel_L Q, Q_2 \parallel_L Q) \in \mathcal{B}'$ with $(Q_1, Q_2) \in \mathcal{B}$, there are three cases for action transitions based on the operational semantic rules in Table 10.1:

   - If $Q_1 \parallel_L Q \xrightarrow{a}_{\rm a} Q_1' \parallel_L Q$ with $Q_1 \xrightarrow{a}_{\rm a} Q_1'$ and $a \notin L$, then either $a = \tau$ and $(Q_1', Q_2) \in \mathcal{B}$, or there exists $Q_2 \stackrel{\tau^*}{\Longrightarrow}_{\rm a} \bar{Q}_2 \xrightarrow{a}_{\rm a} Q_2'$ such that $(Q_1, \bar{Q}_2) \in \mathcal{B}$ and $(Q_1', Q_2') \in \mathcal{B}$. Since synchronization does not apply to τ and $a \notin L$, in the former subcase $Q_2 \parallel_L Q$ is allowed to stay idle with $(Q_1' \parallel_L Q, Q_2 \parallel_L Q) \in \mathcal{B}'$, while in the latter subcase $Q_2 \parallel_L Q \stackrel{\tau^*}{\Longrightarrow}_{\rm a} \bar{Q}_2 \parallel_L Q \xrightarrow{a}_{\rm a} Q_2' \parallel_L Q$ with $(Q_1 \parallel_L Q, \bar{Q}_2 \parallel_L Q) \in \mathcal{B}'$ and $(Q_1' \parallel_L Q, Q_2' \parallel_L Q) \in \mathcal{B}'$.
   - The case $Q_1 \parallel_L Q \xrightarrow{a}_{\rm a} Q_1 \parallel_L Q'$ with $Q \xrightarrow{a}_{\rm a} Q'$ and $a \notin L$ is trivial.
   - If $Q_1 \parallel_L Q \xrightarrow{a}_{\rm a} Q_1' \parallel_L Q'$ with $Q_1 \xrightarrow{a}_{\rm a} Q_1'$, $Q \xrightarrow{a}_{\rm a} Q'$, and $a \in L$, then there exists $Q_2 \stackrel{\tau^*}{\Longrightarrow}_{\rm a} \bar{Q}_2 \xrightarrow{a}_{\rm a} Q_2'$ such that $(Q_1, \bar{Q}_2) \in \mathcal{B}$ and $(Q_1', Q_2') \in \mathcal{B}$. Since synchronization does not apply to τ and $a \in L$, we have that $Q_2 \parallel_L Q \stackrel{\tau^*}{\Longrightarrow}_{\rm a} \bar{Q}_2 \parallel_L Q \xrightarrow{a}_{\rm a} Q_2' \parallel_L Q'$ with $(Q_1 \parallel_L Q, \bar{Q}_2 \parallel_L Q) \in \mathcal{B}'$ and $(Q_1' \parallel_L Q', Q_2' \parallel_L Q') \in \mathcal{B}'$.

   As for rates, to avoid trivial cases consider an equivalence class $C' = C \parallel_L Q' = \{R \parallel_L Q' \mid R \in C\}$ for some $C \in \mathbb{P}_{\rm mk}/\mathcal{B}$. Suppose that $Q_1 \parallel_L Q \stackrel{\tau}{\not\longrightarrow}_{\rm a}$ so that $Q_1 \stackrel{\tau}{\not\longrightarrow}_{\rm a}$ and $Q \stackrel{\tau}{\not\longrightarrow}_{\rm a}$ too and hence from $(Q_1, Q_2) \in \mathcal{B}$ it follows that there exists $Q_2 \stackrel{\tau^*}{\Longrightarrow}_{\rm a} \bar{Q}_2$ such that $\bar{Q}_2 \stackrel{\tau}{\not\longrightarrow}_{\rm a}$, $(Q_1, \bar{Q}_2) \in \mathcal{B}$, and $\mathit{rate}(Q_1, C) = \mathit{rate}(\bar{Q}_2, C)$. Since synchronization does not apply to τ and rate transitions, we have that $Q_2 \parallel_L Q \stackrel{\tau^*}{\Longrightarrow}_{\rm a} \bar{Q}_2 \parallel_L Q$ with $\bar{Q}_2 \parallel_L Q \stackrel{\tau}{\not\longrightarrow}_{\rm a}$, $(Q_1 \parallel_L Q, \bar{Q}_2 \parallel_L Q) \in \mathcal{B}'$, and $\mathit{rate}(Q_1 \parallel_L Q, C') = \mathit{rate}(Q_1, C) = \mathit{rate}(\bar{Q}_2, C) = \mathit{rate}(\bar{Q}_2 \parallel_L Q, C')$ if $Q = Q'$, $\mathit{rate}(Q_1 \parallel_L Q, C') = \mathit{rate}(Q, \{Q'\}) = \mathit{rate}(\bar{Q}_2 \parallel_L Q, C')$ if $Q_1, \bar{Q}_2 \in C$, $\mathit{rate}(Q_1 \parallel_L Q, C') = 0 = \mathit{rate}(\bar{Q}_2 \parallel_L Q, C')$ otherwise.

4. The equivalence relation $\mathcal{B}' = \mathcal{I}_{\mathbb{P}_{\rm mk}} \cup \{(Q_1 \setminus L, Q_2 \setminus L) \mid (Q_1, Q_2) \in \mathcal{B}\}$ is a Markovian branching bisimulation too. Given $(Q_1 \setminus L, Q_2 \setminus L) \in \mathcal{B}'$ with $(Q_1, Q_2) \in \mathcal{B}$, there are two cases for action transitions based on the operational semantic rules in Table 10.1:

   - If $Q_1 \setminus L \xrightarrow{\tau}_{\rm a} Q_1' \setminus L$ with $Q_1 \xrightarrow{\tau}_{\rm a} Q_1'$, then either $(Q_1', Q_2) \in \mathcal{B}$, or there exists $Q_2 \stackrel{\tau^*}{\Longrightarrow}_{\rm a} \bar{Q}_2 \xrightarrow{\tau}_{\rm a} Q_2'$ such that $(Q_1, \bar{Q}_2) \in \mathcal{B}$ and $(Q_1', Q_2') \in \mathcal{B}$. Since the restriction operator does not apply to τ, in the former subcase $Q_2 \setminus L$ is allowed to stay idle with $(Q_1' \setminus L, Q_2 \setminus L) \in \mathcal{B}'$, while in the latter subcase $Q_2 \setminus L \stackrel{\tau^*}{\Longrightarrow}_{\rm a} \bar{Q}_2 \setminus L \xrightarrow{\tau}_{\rm a} Q_2' \setminus L$ with $(Q_1 \setminus L, \bar{Q}_2 \setminus L) \in \mathcal{B}'$ and $(Q_1' \setminus L, Q_2' \setminus L) \in \mathcal{B}'$.

- If $Q_1 \setminus L \xrightarrow{a}_{\rm a} Q_1' \setminus L$ with $Q_1 \xrightarrow{a}_{\rm a} Q_1'$ and $a \notin L \cup \{\tau\}$, then there exists $Q_2 \stackrel{\tau^*}{\Longrightarrow}_{\rm a} \bar{Q}_2 \xrightarrow{a}_{\rm a} Q_2'$ such that $(Q_1, \bar{Q}_2) \in \mathcal{B}$ and $(Q_1', Q_2') \in \mathcal{B}$. Since the restriction operator does not apply to τ and $a \notin L$, we have that $Q_2 \setminus L \stackrel{\tau^*}{\Longrightarrow}_{\rm a} \bar{Q}_2 \setminus L \xrightarrow{a}_{\rm a} Q_2' \setminus L$ with $(Q_1 \setminus L, \bar{Q}_2 \setminus L) \in \mathcal{B}'$ and $(Q_1' \setminus L, Q_2' \setminus L) \in \mathcal{B}'$.

As for rates, we reason like in the proof of the corresponding result for $\approx_{\rm mw}$.

5. The equivalence relation $\mathcal{B}' = \mathcal{I}_{\mathbb{P}_{\rm mk}} \cup \{(Q_1 \,/\, L, Q_2 \,/\, L) \mid (Q_1, Q_2) \in \mathcal{B}\}$ is a Markovian branching bisimulation too. Given $(Q_1 \,/\, L, Q_2 \,/\, L) \in \mathcal{B}'$ with $(Q_1, Q_2) \in \mathcal{B}$, there are two cases for action transitions based on the operational semantic rules in Table 10.1:

   - If $Q_1 \,/\, L \xrightarrow{\tau}_{\rm a} Q_1' \,/\, L$ with $Q_1 \xrightarrow{\tau}_{\rm a} Q_1'$, then either $(Q_1', Q_2) \in \mathcal{B}$, or there exists $Q_2 \stackrel{\tau^*}{\Longrightarrow}_{\rm a} \bar{Q}_2 \xrightarrow{\tau}_{\rm a} Q_2'$ such that $(Q_1, \bar{Q}_2) \in \mathcal{B}$ and $(Q_1', Q_2') \in \mathcal{B}$. Since the hiding operator does not apply to τ, in the former subcase $Q_2 \,/\, L$ is allowed to stay idle with $(Q_1' \,/\, L, Q_2 \,/\, L) \in \mathcal{B}'$, while in the latter subcase $Q_2 \,/\, L \stackrel{\tau^*}{\Longrightarrow}_{\rm a} \bar{Q}_2 \,/\, L \xrightarrow{\tau}_{\rm a} Q_2' \,/\, L$ with $(Q_1 \,/\, L, \bar{Q}_2 \,/\, L) \in \mathcal{B}'$ and $(Q_1' \,/\, L, Q_2' \,/\, L) \in \mathcal{B}'$.
   - If $Q_1 \,/\, L \xrightarrow{a}_{\rm a} Q_1' \,/\, L$ with $Q_1 \xrightarrow{b}_{\rm a} Q_1'$ and $b \in L \wedge a = \tau$ or $b \notin L \cup \{\tau\} \wedge a = b$, then there exists $Q_2 \stackrel{\tau^*}{\Longrightarrow}_{\rm a} \bar{Q}_2 \xrightarrow{b}_{\rm a} Q_2'$ such that $(Q_1, \bar{Q}_2) \in \mathcal{B}$ and $(Q_1', Q_2') \in \mathcal{B}$. Since the hiding operator does not apply to τ, we have that $Q_2 \,/\, L \stackrel{\tau^*}{\Longrightarrow}_{\rm a} \bar{Q}_2 \,/\, L \xrightarrow{a}_{\rm a} Q_2' \,/\, L$ with $(Q_1 \,/\, L, \bar{Q}_2 \,/\, L) \in \mathcal{B}'$ and $(Q_1' \,/\, L, Q_2' \,/\, L) \in \mathcal{B}'$.

   As for rates, to avoid trivial cases consider an equivalence class $C' = C \,/\, L = \{Q \,/\, L \mid Q \in C\}$ for some $C \in \mathbb{P}_{\rm mk}/\mathcal{B}$. Suppose that $Q_1 \,/\, L \not\xrightarrow{\tau}_{\rm a}$ so that $Q_1 \not\xrightarrow{\tau}_{\rm a}$ too and hence from $(Q_1, Q_2) \in \mathcal{B}$ it follows that there exists $Q_2 \stackrel{\tau^*}{\Longrightarrow}_{\rm a} \bar{Q}_2$ such that $\bar{Q}_2 \not\xrightarrow{\tau}_{\rm a}$, $(Q_1, \bar{Q}_2) \in \mathcal{B}$, and $\mathit{rate}(Q_1, C) = \mathit{rate}(\bar{Q}_2, C)$. Since the hiding operator does not apply to τ and rate transitions, we have that $Q_2 \,/\, L \stackrel{\tau^*}{\Longrightarrow}_{\rm a} \bar{Q}_2 \,/\, L$ with $\bar{Q}_2 \,/\, L \not\xrightarrow{\tau}_{\rm a}$, $(Q_1 \,/\, L, \bar{Q}_2 \,/\, L) \in \mathcal{B}'$, and $\mathit{rate}(Q_1 \,/\, L, C') = \mathit{rate}(Q_1, C) = \mathit{rate}(\bar{Q}_2, C) = \mathit{rate}(\bar{Q}_2 \,/\, L, C')$. ∎

Theorem 10.1. *Let* $P_1, P_2 \in \mathbb{P}$, $\approx \in \{\approx_{\rm mw}, \approx_{\rm mb}\}$, *and* $\mathcal{P} \in \{\mathrm{BSNNI}_\approx, \mathrm{BNDC}_\approx, \mathrm{SBSNNI}_\approx, \mathrm{P\_BNDC}_\approx, \mathrm{SBNDC}_\approx\}$. *If* $P_1 \approx P_2$ *then* $P_1 \in \mathcal{P} \iff P_2 \in \mathcal{P}$.

Proof. A straightforward consequence of the definition of the various properties, i.e., Definition 10.5, and Lemma 10.1. ∎

As far as modular verification is concerned, like in the nondeterministic and probabilistic settings of the two previous chapters only the local properties $\mathrm{SBSNNI}_\approx$, $\mathrm{P\_BNDC}_\approx$, and $\mathrm{SBNDC}_\approx$ are compositional, i.e., are preserved by some operators of the calculus in certain circumstances. Moreover, similar to the two previous chapters, compositionality with respect to parallel composition is limited, for $\mathrm{SBSNNI}_{\approx_{\rm mb}}$ and $\mathrm{P\_BNDC}_{\approx_{\rm mb}}$, to the case in which synchronizations can take place only among low-level actions, i.e., $L \subseteq \mathcal{A}_{\mathcal{L}}$. A limitation to low-level actions applies to action prefix and hiding as well, whilst this is not the case for restriction. Another analogy with the nondeterministic and probabilistic settings of the two previous chapters is that none of the considered noninterference properties is compositional with respect to alternative composition, as can be noted by examining $P_1 + P_2$ where $P_1 = l \,.\, \underline{0}$ and $P_2 = h \,.\, \underline{0}$ (see after Theorem 8.2).

To establish compositionality, we first prove some ancillary results about parallel composition, restriction, and hiding under SBSNNI and SBNDC similar to those in the two previous chapters.

Lemma 10.2. *Let $P_1, P_2, P \in \mathbb{P}_{\rm mk}$ and $\approx \in \{\approx_{\rm mw}, \approx_{\rm mb}\}$. Then:*

1. *If $P_1, P_2 \in \text{SBSNNI}_{\approx}$ and $L \subseteq \mathcal{A} \setminus \{\tau\}$ for $\approx_{\rm mw}$ or $L \subseteq \mathcal{A}_{\mathcal{L}}$ for $\approx_{\rm mb}$, then $(Q_1 \parallel_L Q_2) \setminus \mathcal{A}_{\mathcal{H}} \approx (R_1 \parallel_L R_2) / \mathcal{A}_{\mathcal{H}}$ for all $Q_1, R_1 \in reach(P_1)$ and $Q_2, R_2 \in reach(P_2)$ such that $Q_1 \parallel_L Q_2, R_1 \parallel_L R_2 \in reach(P_1 \parallel_L P_2)$, $Q_1 \setminus \mathcal{A}_{\mathcal{H}} \approx R_1 / \mathcal{A}_{\mathcal{H}}$, and $Q_2 \setminus \mathcal{A}_{\mathcal{H}} \approx R_2 / \mathcal{A}_{\mathcal{H}}$.*
2. *If $P \in \text{SBSNNI}_{\approx}$ and $L \subseteq \mathcal{A} \setminus \{\tau\}$, then $(Q / \mathcal{A}_{\mathcal{H}}) \setminus L \approx (R \setminus L) / \mathcal{A}_{\mathcal{H}}$ for all $Q, R \in reach(P)$ such that $Q / \mathcal{A}_{\mathcal{H}} \approx R \setminus \mathcal{A}_{\mathcal{H}}$.*
3. *If $P_1, P_2 \in \text{SBNDC}_{\approx}$ and $L \subseteq \mathcal{A} \setminus \{\tau\}$, then $(Q_1 \parallel_L Q_2) \setminus \mathcal{A}_{\mathcal{H}} \approx (R_1 \parallel_L R_2) \setminus \mathcal{A}_{\mathcal{H}}$ for all $Q_1, R_1 \in reach(P_1)$ and $Q_2, R_2 \in reach(P_2)$ such that $Q_1 \parallel_L Q_2, R_1 \parallel_L R_2 \in reach(P_1 \parallel_L P_2)$, $Q_1 \setminus \mathcal{A}_{\mathcal{H}} \approx R_1 \setminus \mathcal{A}_{\mathcal{H}}$ and $Q_2 \setminus \mathcal{A}_{\mathcal{H}} \approx R_2 \setminus \mathcal{A}_{\mathcal{H}}$.*

Proof. We first prove the three results for the $\approx_{\rm mw}$-based properties. Let $\mathcal{B}$ be an equivalence relation containing all the pairs of processes that have to be shown to be $\approx_{\rm mw}$-equivalent according to the considered result:

1. Starting from $(Q_1 \parallel_L Q_2) \setminus \mathcal{A}_{\mathcal{H}}$ and $(R_1 \parallel_L R_2) / \mathcal{A}_{\mathcal{H}}$ related by $\mathcal{B}$, so that $Q_1 \setminus \mathcal{A}_{\mathcal{H}} \approx_{\rm mw} R_1 / \mathcal{A}_{\mathcal{H}}$ and $Q_2 \setminus \mathcal{A}_{\mathcal{H}} \approx_{\rm mw} R_2 / \mathcal{A}_{\mathcal{H}}$, there are thirteen cases for action transitions based on the operational semantic rules in Table 10.1. In the first five cases, it is $(Q_1 \parallel_L Q_2) \setminus \mathcal{A}_{\mathcal{H}}$ to move first:

   - If $(Q_1 \parallel_L Q_2) \setminus \mathcal{A}_{\mathcal{H}} \xrightarrow{l}_{\rm a} (Q_1' \parallel_L Q_2) \setminus \mathcal{A}_{\mathcal{H}}$ with $Q_1 \xrightarrow{l}_{\rm a} Q_1'$ and $l \notin L$, then $Q_1 \setminus \mathcal{A}_{\mathcal{H}} \xrightarrow{l}_{\rm a} Q_1' \setminus \mathcal{A}_{\mathcal{H}}$ as $l \notin \mathcal{A}_{\mathcal{H}}$. From $Q_1 \setminus \mathcal{A}_{\mathcal{H}} \approx_{\rm mw} R_1 / \mathcal{A}_{\mathcal{H}}$ it follows that there exists $R_1 / \mathcal{A}_{\mathcal{H}} \xRightarrow{\tau^*}_{\rm a} \xrightarrow{l}_{\rm a} \xRightarrow{\tau^*}_{\rm a} R_1' / \mathcal{A}_{\mathcal{H}}$ such that $Q_1' \setminus \mathcal{A}_{\mathcal{H}} \approx_{\rm mw} R_1' / \mathcal{A}_{\mathcal{H}}$. Since synchronization does not apply to τ and $l \notin L$, we have that $(Q_1 \parallel_L Q_2) / \mathcal{A}_{\mathcal{H}} \xRightarrow{\tau^*}_{\rm a} \xrightarrow{l}_{\rm a} \xRightarrow{\tau^*}_{\rm a} (R_1' \parallel_L R_2) / \mathcal{A}_{\mathcal{H}}$ with $((Q_1' \parallel_L Q_2) \setminus \mathcal{A}_{\mathcal{H}}, (R_1' \parallel_L R_2) / \mathcal{A}_{\mathcal{H}}) \in \mathcal{B}$.
   - If $(Q_1 \parallel_L Q_2) \setminus \mathcal{A}_{\mathcal{H}} \xrightarrow{l}_{\rm a} (Q_1 \parallel_L Q_2') \setminus \mathcal{A}_{\mathcal{H}}$ with $Q_2 \xrightarrow{l}_{\rm a} Q_2'$ and $l \notin L$, then the proof is similar to the one of the previous case.
   - If $(Q_1 \parallel_L Q_2) \setminus \mathcal{A}_{\mathcal{H}} \xrightarrow{l}_{\rm a} (Q_1' \parallel_L Q_2') \setminus \mathcal{A}_{\mathcal{H}}$ with $Q_i \xrightarrow{l}_{\rm a} Q_i'$ for $i \in \{1, 2\}$ and $l \in L$, then $Q_i \setminus \mathcal{A}_{\mathcal{H}} \xrightarrow{l}_{\rm a} Q_i' \setminus \mathcal{A}_{\mathcal{H}}$ as $l \notin \mathcal{A}_{\mathcal{H}}$. From $Q_i \setminus \mathcal{A}_{\mathcal{H}} \approx_{\rm mw} R_i / \mathcal{A}_{\mathcal{H}}$ it follows that there exists $R_i / \mathcal{A}_{\mathcal{H}} \xRightarrow{\tau^*}_{\rm a} \xrightarrow{l}_{\rm a} \xRightarrow{\tau^*}_{\rm a} R_i' / \mathcal{A}_{\mathcal{H}}$ such that $Q_i' \setminus \mathcal{A}_{\mathcal{H}} \approx_{\rm mw} R_i' / \mathcal{A}_{\mathcal{H}}$. Since synchronization does not apply to τ and $l \in L$, we have that $(R_1 \parallel_L R_2) / \mathcal{A}_{\mathcal{H}} \xRightarrow{\tau^*}_{\rm a} \xrightarrow{l}_{\rm a} \xRightarrow{\tau^*}_{\rm a} (R_1' \parallel_L R_2') / \mathcal{A}_{\mathcal{H}}$ with $((Q_1' \parallel_L Q_2') \setminus \mathcal{A}_{\mathcal{H}}, (R_1' \parallel_L R_2') / \mathcal{A}_{\mathcal{H}}) \in \mathcal{B}$.
   - If $(Q_1 \parallel_L Q_2) \setminus \mathcal{A}_{\mathcal{H}} \xrightarrow{\tau}_{\rm a} (Q_1' \parallel_L Q_2) \setminus \mathcal{A}_{\mathcal{H}}$ with $Q_1 \xrightarrow{\tau}_{\rm a} Q_1'$, then $Q_1 \setminus \mathcal{A}_{\mathcal{H}} \xrightarrow{\tau}_{\rm a} Q_1' \setminus \mathcal{A}_{\mathcal{H}}$ as $\tau \notin \mathcal{A}_{\mathcal{H}}$. From $Q_1 \setminus \mathcal{A}_{\mathcal{H}} \approx_{\rm mw} R_1 / \mathcal{A}_{\mathcal{H}}$ it follows that there exists $R_1 / \mathcal{A}_{\mathcal{H}} \xRightarrow{\tau^*}_{\rm a} R_1' / \mathcal{A}_{\mathcal{H}}$ such that $Q_1' \setminus \mathcal{A}_{\mathcal{H}} \approx_{\rm mw} R_1' / \mathcal{A}_{\mathcal{H}}$. Since synchronization does not apply to τ, we have that $(R_1 \parallel_L R_2) / \mathcal{A}_{\mathcal{H}} \xRightarrow{\tau^*}_{\rm a} (R_1' \parallel_L R_2) / \mathcal{A}_{\mathcal{H}}$ with $((Q_1' \parallel_L Q_2) \setminus \mathcal{A}_{\mathcal{H}}, (R_1' \parallel_L R_2) / \mathcal{A}_{\mathcal{H}}) \in \mathcal{B}$.
   - If $(Q_1 \parallel_L Q_2) \setminus \mathcal{A}_{\mathcal{H}} \xrightarrow{\tau}_{\rm a} (Q_1 \parallel_L Q_2') \setminus \mathcal{A}_{\mathcal{H}}$ with $Q_2 \xrightarrow{\tau}_{\rm a} Q_2'$, then the proof is similar to the one of the previous case.

   In the other eight cases, instead, it is $(R_1 \parallel_L R_2) / \mathcal{A}_{\mathcal{H}}$ to move first:

   - If $(R_1 \parallel_L R_2) / \mathcal{A}_{\mathcal{H}} \xrightarrow{l}_{\rm a} (R_1' \parallel_L R_2) / \mathcal{A}_{\mathcal{H}}$ with $R_1 \xrightarrow{l}_{\rm a} R_1'$ and $l \notin L$, then $R_1 / \mathcal{A}_{\mathcal{H}} \xrightarrow{l}_{\rm a} R_1' / \mathcal{A}_{\mathcal{H}}$ as $l \notin \mathcal{A}_{\mathcal{H}}$. From $R_1 / \mathcal{A}_{\mathcal{H}} \approx_{\rm mw} Q_1 \setminus \mathcal{A}_{\mathcal{H}}$ it follows that there exists $Q_1 \setminus \mathcal{A}_{\mathcal{H}} \xRightarrow{\tau^*}_{\rm a} \xrightarrow{l}_{\rm a} \xRightarrow{\tau^*}_{\rm a} Q_1' \setminus \mathcal{A}_{\mathcal{H}}$ such that $R_1' / \mathcal{A}_{\mathcal{H}} \approx_{\rm mw} Q_1' \setminus \mathcal{A}_{\mathcal{H}}$. Since synchronization does not apply to τ and $l \notin L$, we have that $(Q_1 \parallel_L Q_2) \setminus \mathcal{A}_{\mathcal{H}} \xRightarrow{\tau^*}_{\rm a} \xrightarrow{l}_{\rm a} \xRightarrow{\tau^*}_{\rm a} (Q_1' \parallel_L Q_2) \setminus \mathcal{A}_{\mathcal{H}}$ with $((R_1' \parallel_L R_2) / \mathcal{A}_{\mathcal{H}}, (Q_1' \parallel_L Q_2) \setminus \mathcal{A}_{\mathcal{H}}) \in \mathcal{B}$.

- If $(R_1 \parallel_L R_2) / \mathcal{A}_\mathcal{H} \xrightarrow{l}_\mathrm{a} (R_1 \parallel_L R'_2) / \mathcal{A}_\mathcal{H}$ with $R_2 \xrightarrow{l}_\mathrm{a} R'_2$ and $l \notin L$, then the proof is similar to the one of the previous case.
- If $(R_1 \parallel_L R_2) / \mathcal{A}_\mathcal{H} \xrightarrow{l}_\mathrm{a} (R'_1 \parallel_L R'_2) / \mathcal{A}_\mathcal{H}$ with $R_i \xrightarrow{l}_\mathrm{a} R'_i$ for $i \in \{1,2\}$ and $l \in L$, then $R_i / \mathcal{A}_\mathcal{H} \xrightarrow{l}_\mathrm{a} R'_i / \mathcal{A}_\mathcal{H}$ as $l \notin \mathcal{A}_\mathcal{H}$. From $R_i / \mathcal{A}_\mathcal{H} \approx_\mathrm{mw} Q_i \setminus \mathcal{A}_\mathcal{H}$ it follows that there exists $Q_i \setminus \mathcal{A}_\mathcal{H} \xRightarrow{\tau^*}_\mathrm{a} \xrightarrow{l}_\mathrm{a} \xRightarrow{\tau^*}_\mathrm{a} Q'_i \setminus \mathcal{A}_\mathcal{H}$ such that $R'_i / \mathcal{A}_\mathcal{H} \approx_\mathrm{mw} Q'_i \setminus \mathcal{A}_\mathcal{H}$. Since synchronization does not apply to τ and $l \in L$, we have that $(Q_1 \parallel_L Q_2) \setminus \mathcal{A}_\mathcal{H} \xRightarrow{\tau^*}_\mathrm{a} \xrightarrow{l}_\mathrm{a} \xRightarrow{\tau^*}_\mathrm{a} (Q'_1 \parallel_L Q'_2) \setminus \mathcal{A}_\mathcal{H}$ with $((R'_1 \parallel_L R'_2)/\mathcal{A}_\mathcal{H}, (Q'_1 \parallel_L Q'_2) \setminus \mathcal{A}_\mathcal{H}) \in \mathcal{B}$.
- If $(R_1 \parallel_L R_2) / \mathcal{A}_\mathcal{H} \xrightarrow{\tau}_\mathrm{a} (R'_1 \parallel_L R_2) / \mathcal{A}_\mathcal{H}$ with $R_1 \xrightarrow{\tau}_\mathrm{a} R'_1$, then $R_1 / \mathcal{A}_\mathcal{H} \xrightarrow{\tau}_\mathrm{a} R'_1 / \mathcal{A}_\mathcal{H}$ as $\tau \notin \mathcal{A}_\mathcal{H}$. From $R_1 / \mathcal{A}_\mathcal{H} \approx_\mathrm{mw} Q_1 \setminus \mathcal{A}_\mathcal{H}$ it follows that there exists $Q_1 \setminus \mathcal{A}_\mathcal{H} \xRightarrow{\tau^*}_\mathrm{a} Q'_1 \setminus \mathcal{A}_\mathcal{H}$ such that $R'_1 / \mathcal{A}_\mathcal{H} \approx_\mathrm{mw} Q'_1 \setminus \mathcal{A}_\mathcal{H}$. Since synchronization does not apply to τ, we have that $(Q_1 \parallel_L Q_2) \setminus \mathcal{A}_\mathcal{H} \xRightarrow{\tau^*}_\mathrm{a} (Q'_1 \parallel_L Q_2) \setminus \mathcal{A}_\mathcal{H}$ with $((R'_1 \parallel_L R_2)/\mathcal{A}_\mathcal{H}, (Q'_1 \parallel_L Q_2) \setminus \mathcal{A}_\mathcal{H}) \in \mathcal{B}$.
- If $(R_1 \parallel_L R_2) / \mathcal{A}_\mathcal{H} \xrightarrow{\tau}_\mathrm{a} (R_1 \parallel_L R'_2) / \mathcal{A}_\mathcal{H}$ with $R_2 \xrightarrow{\tau}_\mathrm{a} R'_2$, then the proof is similar to the one of the previous case.
- If $(R_1 \parallel_L R_2) / \mathcal{A}_\mathcal{H} \xrightarrow{\tau}_\mathrm{a} (R'_1 \parallel_L R_2) / \mathcal{A}_\mathcal{H}$ with $R_1 \xrightarrow{h}_\mathrm{a} R'_1$ and $h \notin L$, then $R_1 / \mathcal{A}_\mathcal{H} \xrightarrow{\tau}_\mathrm{a} R'_1 / \mathcal{A}_\mathcal{H}$ as $h \in \mathcal{A}_\mathcal{H}$. The rest of the proof is like the one of the fourth case.
- If $(R_1 \parallel_L R_2) / \mathcal{A}_\mathcal{H} \xrightarrow{\tau}_\mathrm{a} (R_1 \parallel_L R'_2) / \mathcal{A}_\mathcal{H}$ with $R_2 \xrightarrow{h}_\mathrm{a} R'_2$ and $h \notin L$, then the proof is similar to the one of the previous case.
- If $(R_1 \parallel_L R_2) / \mathcal{A}_\mathcal{H} \xrightarrow{\tau}_\mathrm{a} (R'_1 \parallel_L R'_2) / \mathcal{A}_\mathcal{H}$ with $R_i \xrightarrow{h}_\mathrm{a} R'_i$ for $i \in \{1,2\}$ and $h \in L$, then $R_i / \mathcal{A}_\mathcal{H} \xrightarrow{\tau}_\mathrm{a} R'_i / \mathcal{A}_\mathcal{H}$ as $h \in \mathcal{A}_\mathcal{H}$. From $R_i / \mathcal{A}_\mathcal{H} \approx_\mathrm{mw} Q_i \setminus \mathcal{A}_\mathcal{H}$ it follows that there exists $Q_i \setminus \mathcal{A}_\mathcal{H} \xRightarrow{\tau^*}_\mathrm{a} Q'_i \setminus \mathcal{A}_\mathcal{H}$ such that $R'_i / \mathcal{A}_\mathcal{H} \approx_\mathrm{mw} Q'_i \setminus \mathcal{A}_\mathcal{H}$. Since synchronization does not apply to τ and $h \in L$, we have that $(Q_1 \parallel_L Q_2) \setminus \mathcal{A}_\mathcal{H} \xRightarrow{\tau^*}_\mathrm{a} (Q'_1 \parallel_L Q'_2) \setminus \mathcal{A}_\mathcal{H}$ with $((R'_1 \parallel_L R'_2) / \mathcal{A}_\mathcal{H}, (Q'_1 \parallel_L Q'_2) \setminus \mathcal{A}_\mathcal{H}) \in \mathcal{B}$.

As for rates, to avoid trivial cases consider an equivalence class $C \in \mathbb{P}_\mathrm{mk}/\mathcal{B}$ that involves processes reachable from $P_1 \parallel_L P_2$, specifically $C = \{(S_{1,i} \parallel_L S_{2,i}) \setminus \mathcal{A}_\mathcal{H}, (S_{1,j} \parallel_L S_{2,j}) / \mathcal{A}_\mathcal{H} \mid S_{k,h} \in \mathit{reach}(P_k) \wedge S_{1,h} \parallel_L S_{2,h} \in \mathit{reach}(P_1 \parallel_L P_2) \wedge S_{k,i} \setminus \mathcal{A}_\mathcal{H} \approx_\mathrm{mw} S_{k,j} / \mathcal{A}_\mathcal{H}\}$. Suppose that $(Q_1 \parallel_L Q_2) \setminus \mathcal{A}_\mathcal{H} \not\xrightarrow{\tau}_\mathrm{a}$ so that $Q_k \setminus \mathcal{A}_\mathcal{H} \not\xrightarrow{\tau}_\mathrm{a}$ too and hence from $Q_k \setminus \mathcal{A}_\mathcal{H} \approx_\mathrm{mw} R_k / \mathcal{A}_\mathcal{H}$ it follows that there exists $R_k / \mathcal{A}_\mathcal{H} \xRightarrow{\tau^*}_\mathrm{a} \bar{R}_k / \mathcal{A}_\mathcal{H}$ such that $\bar{R}_k / \mathcal{A}_\mathcal{H} \not\xrightarrow{\tau}_\mathrm{a}$, $Q_k \setminus \mathcal{A}_\mathcal{H} \approx_\mathrm{mw} \bar{R}_k / \mathcal{A}_\mathcal{H}$, and $\mathit{rate}(Q_k \setminus \mathcal{A}_\mathcal{H}, C') = \mathit{rate}(\bar{R}_k / \mathcal{A}_\mathcal{H}, C')$ for all $C' \in \mathbb{P}_\mathrm{mk}/\approx_\mathrm{mw}$. Since synchronization does not apply to τ, we have that $(R_1 \parallel_L R_2) / \mathcal{A}_\mathcal{H} \xRightarrow{\tau^*}_\mathrm{a} (\bar{R}_1 \parallel_L \bar{R}_2) / \mathcal{A}_\mathcal{H}$ with $(\bar{R}_1 \parallel_L \bar{R}_2) / \mathcal{A}_\mathcal{H} \not\xrightarrow{\tau}_\mathrm{a}$ and $((Q_1 \parallel_L Q_2) \setminus \mathcal{A}_\mathcal{H}, (\bar{R}_1 \parallel_L \bar{R}_2) / \mathcal{A}_\mathcal{H}) \in \mathcal{B}$. Since the restriction and hiding operators do not apply to rate transitions, we have that:

$$\begin{array}{rcl} \mathit{rate}((Q_1 \parallel_L Q_2) \setminus \mathcal{A}_\mathcal{H}, C) & = & \mathit{rate}((Q_1 \setminus \mathcal{A}_\mathcal{H}) \parallel_L (Q_2 \setminus \mathcal{A}_\mathcal{H}), C) \\ \mathit{rate}((\bar{R}_1 \parallel_L \bar{R}_2) / \mathcal{A}_\mathcal{H}, C) & = & \mathit{rate}((\bar{R}_1 / \mathcal{A}_\mathcal{H}) \parallel_L (\bar{R}_2 / \mathcal{A}_\mathcal{H}), C) \end{array}$$

Based on which subprocess moves so that the overall process reaches C (which we assume to be reachable in one move to avoid trivial cases in which cumulative rates are zero), we have that:

$$\begin{array}{rcl} \mathit{rate}((Q_1 \setminus \mathcal{A}_\mathcal{H}) \parallel_L (Q_2 \setminus \mathcal{A}_\mathcal{H}), C) & = & \mathit{rate}(Q_1 \setminus \mathcal{A}_\mathcal{H}, C_1) \\ \mathit{rate}((\bar{R}_1 / \mathcal{A}_\mathcal{H}) \parallel_L (\bar{R}_2 / \mathcal{A}_\mathcal{H}), C) & = & \mathit{rate}(\bar{R}_1 / \mathcal{A}_\mathcal{H}, C_1) \end{array}$$

or:

$$\begin{array}{rcl} \mathit{rate}((Q_1 \setminus \mathcal{A}_\mathcal{H}) \parallel_L (Q_2 \setminus \mathcal{A}_\mathcal{H}), C) & = & \mathit{rate}(Q_2 \setminus \mathcal{A}_\mathcal{H}, C_2) \\ \mathit{rate}((\bar{R}_1 / \mathcal{A}_\mathcal{H}) \parallel_L (\bar{R}_2 / \mathcal{A}_\mathcal{H}), C) & = & \mathit{rate}(\bar{R}_2 / \mathcal{A}_\mathcal{H}, C_2) \end{array}$$

where:

$$C_1 = \{S_{1,h} \setminus \mathcal{A}_\mathcal{H} \mid (S_{1,h} \parallel_L S_{2,h}) \setminus \mathcal{A}_\mathcal{H} \in C\} \cup \{S_{1,h} / \mathcal{A}_\mathcal{H} \mid (S_{1,h} \parallel_L S_{2,h}) / \mathcal{A}_\mathcal{H} \in C\}$$
$$C_2 = \{S_{2,h} \setminus \mathcal{A}_\mathcal{H} \mid (S_{1,h} \parallel_L S_{2,h}) \setminus \mathcal{A}_\mathcal{H} \in C\} \cup \{S_{2,h} / \mathcal{A}_\mathcal{H} \mid (S_{1,h} \parallel_L S_{2,h}) / \mathcal{A}_\mathcal{H} \in C\}$$

Since $Q_k \setminus \mathcal{A}_\mathcal{H} \approx_{\rm mw} \bar{R}_k / \mathcal{A}_\mathcal{H}$ and C_k is the union of some $\approx_{\rm mw}$-equivalence classes for $k \in \{1,2\}$, we have that:

$$rate(Q_1 \setminus \mathcal{A}_\mathcal{H}, C_1) = rate(\bar{R}_1 / \mathcal{A}_\mathcal{H}, C_1)$$
$$rate(Q_2 \setminus \mathcal{A}_\mathcal{H}, C_2) = rate(\bar{R}_2 / \mathcal{A}_\mathcal{H}, C_2)$$

If we start from $(R_1 \parallel_L R_2) / \mathcal{A}_\mathcal{H} \stackrel{\tau}{\not\longrightarrow}_{\rm a}$, then the proof is similar.

2. Starting from $(Q / \mathcal{A}_\mathcal{H}) \setminus L$ and $(R \setminus L) / \mathcal{A}_\mathcal{H}$ related by $\mathcal{B}$, so that $Q / \mathcal{A}_\mathcal{H} \approx_{\rm mw} R \setminus \mathcal{A}_\mathcal{H}$, there are six cases for action transitions based on the operational semantic rules in Table 10.1. In the first three cases, it is $(Q / \mathcal{A}_\mathcal{H}) \setminus L$ to move first:

   - If $(Q / \mathcal{A}_\mathcal{H}) \setminus L \stackrel{l}{\longrightarrow}_{\rm a} (Q' / \mathcal{A}_\mathcal{H}) \setminus L$ with $Q \stackrel{l}{\longrightarrow}_{\rm a} Q'$ and $l \notin L$, then $Q / \mathcal{A}_\mathcal{H} \stackrel{l}{\longrightarrow}_{\rm a} Q' / \mathcal{A}_\mathcal{H}$ as $l \notin \mathcal{A}_\mathcal{H}$. From $Q / \mathcal{A}_\mathcal{H} \approx_{\rm mw} R \setminus \mathcal{A}_\mathcal{H}$ it follows that there exists $Q \setminus \mathcal{A}_\mathcal{H} \stackrel{\tau^*}{\Longrightarrow}_{\rm a} \stackrel{l}{\longrightarrow}_{\rm a} \stackrel{\tau^*}{\Longrightarrow}_{\rm a} R' \setminus \mathcal{A}_\mathcal{H}$ such that $Q' / \mathcal{A}_\mathcal{H} \approx_{\rm mw} R' \setminus \mathcal{A}_\mathcal{H}$. Since the restriction and hiding operators do not apply to τ and l, we have that $(R \setminus L) / \mathcal{A}_\mathcal{H} \stackrel{\tau^*}{\Longrightarrow}_{\rm a} \stackrel{l}{\longrightarrow}_{\rm a} \stackrel{\tau^*}{\Longrightarrow}_{\rm a} (R' \setminus L) / \mathcal{A}_\mathcal{H}$ with $((Q' / \mathcal{A}_\mathcal{H}) \setminus L, (R' \setminus L) / \mathcal{A}_\mathcal{H}) \in \mathcal{B}$.
   - If $(Q / \mathcal{A}_\mathcal{H}) \setminus L \stackrel{\tau}{\longrightarrow}_{\rm a} (Q' / \mathcal{A}_\mathcal{H}) \setminus L$ with $Q \stackrel{\tau}{\longrightarrow}_{\rm a} Q'$, then $Q / \mathcal{A}_\mathcal{H} \stackrel{\tau}{\longrightarrow}_{\rm a} Q' / \mathcal{A}_\mathcal{H}$ as $\tau \notin \mathcal{A}_\mathcal{H}$. From $Q / \mathcal{A}_\mathcal{H} \approx_{\rm mw} R \setminus \mathcal{A}_\mathcal{H}$ it follows that there exists $R \setminus \mathcal{A}_\mathcal{H} \stackrel{\tau^*}{\Longrightarrow}_{\rm a} R' \setminus \mathcal{A}_\mathcal{H}$ such that $Q' / \mathcal{A}_\mathcal{H} \approx_{\rm mw} R' \setminus \mathcal{A}_\mathcal{H}$. Since the restriction and hiding operators do not apply to τ, we have that $(R \setminus L) / \mathcal{A}_\mathcal{H} \stackrel{\tau^*}{\Longrightarrow}_{\rm a} (R' \setminus L) / \mathcal{A}_\mathcal{H}$ with $((Q' / \mathcal{A}_\mathcal{H}) \setminus L, (R' \setminus L) / \mathcal{A}_\mathcal{H}) \in \mathcal{B}$.
   - If $(Q / \mathcal{A}_\mathcal{H}) \setminus L \stackrel{\tau}{\longrightarrow}_{\rm a} (Q' / \mathcal{A}_\mathcal{H}) \setminus L$ with $Q \stackrel{h}{\longrightarrow}_{\rm a} Q'$, then $Q / \mathcal{A}_\mathcal{H} \stackrel{\tau}{\longrightarrow}_{\rm a} Q' / \mathcal{A}_\mathcal{H}$ as $h \in \mathcal{A}_\mathcal{H}$. The rest of the proof is like the one of the previous case.

   In the other three cases, instead, it is $(R \setminus L) / \mathcal{A}_\mathcal{H}$ to move first:

   - If $(R \setminus L) / \mathcal{A}_\mathcal{H} \stackrel{l}{\longrightarrow}_{\rm a} (R' \setminus L) / \mathcal{A}_\mathcal{H}$ with $R \stackrel{l}{\longrightarrow}_{\rm a} R'$ and $l \notin L$, then $R \setminus \mathcal{A}_\mathcal{H} \stackrel{l}{\longrightarrow}_{\rm a} R' \setminus \mathcal{A}_\mathcal{H}$ as $l \notin \mathcal{A}_\mathcal{H}$. From $R \setminus \mathcal{A}_\mathcal{H} \approx_{\rm mw} Q / \mathcal{A}_\mathcal{H}$ it follows that there exists $Q / \mathcal{A}_\mathcal{H} \stackrel{\tau^*}{\Longrightarrow}_{\rm a} \stackrel{l}{\longrightarrow}_{\rm a} \stackrel{\tau^*}{\Longrightarrow}_{\rm a} Q' / \mathcal{A}_\mathcal{H}$ such that $R' \setminus \mathcal{A}_\mathcal{H} \approx_{\rm mw} Q' / \mathcal{A}_\mathcal{H}$. Since the restriction operator does not apply to τ and l, we have that $(Q / \mathcal{A}_\mathcal{H}) \setminus L \stackrel{\tau^*}{\Longrightarrow}_{\rm a} \stackrel{l}{\longrightarrow}_{\rm a} \stackrel{\tau^*}{\Longrightarrow}_{\rm a} (Q' / \mathcal{A}_\mathcal{H}) \setminus L$ with $((R' \setminus L) / \mathcal{A}_\mathcal{H}, (Q' / \mathcal{A}_\mathcal{H}) \setminus L) \in \mathcal{B}$.
   - If $(R \setminus L) / \mathcal{A}_\mathcal{H} \stackrel{\tau}{\longrightarrow}_{\rm a} (R' \setminus L) / \mathcal{A}_\mathcal{H}$ with $R \stackrel{\tau}{\longrightarrow}_{\rm a} R'$, then $R \setminus \mathcal{A}_\mathcal{H} \stackrel{\tau}{\longrightarrow}_{\rm a} R' \setminus \mathcal{A}_\mathcal{H}$ as $\tau \notin \mathcal{A}_\mathcal{H}$. From $R \setminus \mathcal{A}_\mathcal{H} \approx_{\rm mw} Q / \mathcal{A}_\mathcal{H}$ it follows that there exists $Q / \mathcal{A}_\mathcal{H} \stackrel{\tau^*}{\Longrightarrow}_{\rm a} Q' / \mathcal{A}_\mathcal{H}$ such that $R' \setminus \mathcal{A}_\mathcal{H} \approx_{\rm mw} Q' / \mathcal{A}_\mathcal{H}$. Since the restriction operator does not apply to τ, we have that $(Q / \mathcal{A}_\mathcal{H}) \setminus L \stackrel{\tau^*}{\Longrightarrow}_{\rm a} (Q' / \mathcal{A}_\mathcal{H}) \setminus L$ with $((R' \setminus L) / \mathcal{A}_\mathcal{H}, (Q' / \mathcal{A}_\mathcal{H}) \setminus L) \in \mathcal{B}$.
   - If $(R \setminus L) / \mathcal{A}_\mathcal{H} \stackrel{\tau}{\longrightarrow}_{\rm a} (R' \setminus L) / \mathcal{A}_\mathcal{H}$ with $R \stackrel{h}{\longrightarrow}_{\rm a} R'$ and $h \notin L$, then $R / \mathcal{A}_\mathcal{H} \stackrel{\tau}{\longrightarrow}_{\rm a} R' / \mathcal{A}_\mathcal{H}$ as $h \in \mathcal{A}_\mathcal{H}$ (note that $R \setminus \mathcal{A}_\mathcal{H}$ cannot perform h). From $R / \mathcal{A}_\mathcal{H} \approx_{\rm mw} R \setminus \mathcal{A}_\mathcal{H}$ – as $P \in {\rm SBSNNI}_{\approx_{\rm mw}}$ and $R \in reach(P)$ – and $R \setminus \mathcal{A}_\mathcal{H} \approx_{\rm mw} Q / \mathcal{A}_\mathcal{H}$ it follows that there exists $Q / \mathcal{A}_\mathcal{H} \stackrel{\tau^*}{\Longrightarrow}_{\rm a} Q' / \mathcal{A}_\mathcal{H}$ such that $R' / \mathcal{A}_\mathcal{H} \approx_{\rm mw} Q' / \mathcal{A}_\mathcal{H}$ and hence $R' \setminus \mathcal{A}_\mathcal{H} \approx_{\rm mw} Q' / \mathcal{A}_\mathcal{H}$ – as $R' / \mathcal{A}_\mathcal{H} \approx_{\rm mw} R' \setminus \mathcal{A}_\mathcal{H}$ due to $P \in {\rm SBSNNI}_{\approx_{\rm mw}}$ and $R' \in reach(P)$. Since the restriction operator does not apply to τ, we have that $(Q / \mathcal{A}_\mathcal{H}) \setminus L \stackrel{\tau^*}{\Longrightarrow}_{\rm a} (Q' / \mathcal{A}_\mathcal{H}) \setminus L$ with $((R' \setminus L) / \mathcal{A}_\mathcal{H}, (Q' / \mathcal{A}_\mathcal{H}) \setminus L) \in \mathcal{B}$.

   As for rates, to avoid trivial cases consider an equivalence class $C \in \mathbb{P}_{\rm mk}/\mathcal{B}$ that involves processes reachable from P, specifically $C = \{(S_i / \mathcal{A}_\mathcal{H}) \setminus L, (S_j \setminus L) / \mathcal{A}_\mathcal{H} \mid S_h \in reach(P) \wedge S_i \setminus \mathcal{A}_\mathcal{H} \approx_{\rm mw} S_j / \mathcal{A}_\mathcal{H}\}$. Suppose

that $(Q \,/\, \mathcal{A}_\mathcal{H}) \setminus L \stackrel{\tau}{\not\longrightarrow}_\mathrm{a}$ so that $Q \,/\, \mathcal{A}_\mathcal{H} \stackrel{\tau}{\not\longrightarrow}_\mathrm{a}$ too and hence from $Q \,/\, \mathcal{A}_\mathcal{H} \approx_\mathrm{mw} R \setminus \mathcal{A}_\mathcal{H} \approx_\mathrm{mw} R \,/\, \mathcal{A}_\mathcal{H}$ – as $P \in \mathrm{SBSNNI}_{\approx_\mathrm{mw}}$ and $R \in \mathit{reach}(P)$ – it follows that there exists $R \,/\, \mathcal{A}_\mathcal{H} \stackrel{\tau^*}{\Longrightarrow}_\mathrm{a} \bar{R} \,/\, \mathcal{A}_\mathcal{H}$ such that $\bar{R} \,/\, \mathcal{A}_\mathcal{H} \stackrel{\tau}{\not\longrightarrow}_\mathrm{a}$, $Q \,/\, \mathcal{A}_\mathcal{H} \approx_\mathrm{mw} \bar{R} \,/\, \mathcal{A}_\mathcal{H} \approx_\mathrm{mw} \bar{R} \setminus \mathcal{A}_\mathcal{H}$, and $\mathit{rate}(Q \,/\, \mathcal{A}_\mathcal{H}, C) = \mathit{rate}(\bar{R} \setminus \mathcal{A}_\mathcal{H}, C)$ for all $C \in \mathbb{P}_\mathrm{mk}/\approx_\mathrm{mw}$. Since the restriction and hiding operators do not apply to τ, we have that $(R \setminus L) \,/\, \mathcal{A}_\mathcal{H} \stackrel{\tau^*}{\Longrightarrow}_\mathrm{a} (\bar{R} \setminus L) \,/\, \mathcal{A}_\mathcal{H}$ with $(\bar{R} \setminus L) \,/\, \mathcal{A}_\mathcal{H} \stackrel{\tau}{\not\longrightarrow}_\mathrm{a}$ – as $\bar{R} \,/\, \mathcal{A}_\mathcal{H} \stackrel{\tau}{\not\longrightarrow}_\mathrm{a}$ – and $((Q \,/\, \mathcal{A}_\mathcal{H}) \setminus L, (\bar{R} \setminus L) \,/\, \mathcal{A}_\mathcal{H}) \in \mathcal{B}$. Since the restriction and hiding operators do not apply to rate transitions, we have that:

$$\begin{aligned} \mathit{rate}((Q \,/\, \mathcal{A}_\mathcal{H}) \setminus L, C) &= \mathit{rate}(Q \setminus \mathcal{A}_\mathcal{H}, \bar{C}) \\ \mathit{rate}((\bar{R} \setminus L) \,/\, \mathcal{A}_\mathcal{H}, C) &= \mathit{rate}(\bar{R} \,/\, \mathcal{A}_\mathcal{H}, \bar{C}) \end{aligned}$$

where:

$$\bar{C} = \{S_i \setminus \mathcal{A}_\mathcal{H} \mid (S_i \,/\, \mathcal{A}_\mathcal{H}) \setminus L \in C\} \cup \{S_j \,/\, \mathcal{A}_\mathcal{H} \mid (S_j \setminus L) \,/\, \mathcal{A}_\mathcal{H} \in C\}$$

Since $Q \setminus \mathcal{A}_\mathcal{H} \approx_\mathrm{mw} \bar{R} \,/\, \mathcal{A}_\mathcal{H}$ and $\bar{C}$ is the union of some $\approx_\mathrm{mw}$-equivalence classes, we have that:

$$\mathit{rate}(Q \setminus \mathcal{A}_\mathcal{H}, \bar{C}) = \mathit{rate}(\bar{R} \,/\, \mathcal{A}_\mathcal{H}, \bar{C})$$

If we start from $(R \setminus L) \,/\, \mathcal{A}_\mathcal{H} \stackrel{\tau}{\not\longrightarrow}_\mathrm{a}$, then the proof is similar.

3. Starting from $(Q_1 \parallel_L Q_2) \setminus \mathcal{A}_\mathcal{H}$ and $(R_1 \parallel_L R_2) \setminus \mathcal{A}_\mathcal{H}$ related by $\mathcal{B}$, so that $Q_1 \setminus \mathcal{A}_\mathcal{H} \approx_\mathrm{mw} R_1 \setminus \mathcal{A}_\mathcal{H}$ and $Q_2 \setminus \mathcal{A}_\mathcal{H} \approx_\mathrm{mw} R_2 \setminus \mathcal{A}_\mathcal{H}$, there are five cases for action transitions based on the operational semantic rules in Table 10.1:

   - If $(Q_1 \parallel_L Q_2) \setminus \mathcal{A}_\mathcal{H} \stackrel{l}{\longrightarrow}_\mathrm{a} (Q_1' \parallel_L Q_2) \setminus \mathcal{A}_\mathcal{H}$ with $Q_1 \stackrel{l}{\longrightarrow}_\mathrm{a} Q_1'$ and $l \notin L$, then $Q_1 \setminus \mathcal{A}_\mathcal{H} \stackrel{l}{\longrightarrow}_\mathrm{a} Q_1' \setminus \mathcal{A}_\mathcal{H}$ as $l \notin \mathcal{A}_\mathcal{H}$. From $Q_1 \setminus \mathcal{A}_\mathcal{H} \approx_\mathrm{mw} R_1 \setminus \mathcal{A}_\mathcal{H}$ it follows that there exists $R_1 \setminus \mathcal{A}_\mathcal{H} \stackrel{\tau^*}{\Longrightarrow}_\mathrm{a} \stackrel{l}{\longrightarrow}_\mathrm{a} \stackrel{\tau^*}{\Longrightarrow}_\mathrm{a} R_1' \setminus \mathcal{A}_\mathcal{H}$ such that $Q_1' \setminus \mathcal{A}_\mathcal{H} \approx_\mathrm{mw} R_1' \setminus \mathcal{A}_\mathcal{H}$. Since synchronization does not apply to τ and $l \notin L$, we have that $(R_1 \parallel_L R_2) \setminus \mathcal{A}_\mathcal{H} \stackrel{\tau^*}{\Longrightarrow}_\mathrm{a} \stackrel{l}{\longrightarrow}_\mathrm{a} \stackrel{\tau^*}{\Longrightarrow}_\mathrm{a} (R_1' \parallel_L R_2) \setminus \mathcal{A}_\mathcal{H}$ with $((Q_1' \parallel_L Q_2) \setminus \mathcal{A}_\mathcal{H}, (R_1' \parallel_L R_2) \setminus \mathcal{A}_\mathcal{H}) \in \mathcal{B}$.
   - If $(Q_1 \parallel_L Q_2) \setminus \mathcal{A}_\mathcal{H} \stackrel{l}{\longrightarrow}_\mathrm{a} (Q_1 \parallel_L Q_2') \setminus \mathcal{A}_\mathcal{H}$ with $Q_2 \stackrel{l}{\longrightarrow}_\mathrm{a} Q_2'$ and $l \notin L$, then the proof is similar to the one of the previous case.
   - If $(Q_1 \parallel_L Q_2) \setminus \mathcal{A}_\mathcal{H} \stackrel{l}{\longrightarrow}_\mathrm{a} (Q_1' \parallel_L Q_2') \setminus \mathcal{A}_\mathcal{H}$ with $Q_i \stackrel{l}{\longrightarrow}_\mathrm{a} Q_i'$ for $i \in \{1, 2\}$ and $l \in L$, then $Q_i \setminus \mathcal{A}_\mathcal{H} \stackrel{l}{\longrightarrow}_\mathrm{a} Q_i' \setminus \mathcal{A}_\mathcal{H}$ as $l \notin \mathcal{A}_\mathcal{H}$. From $Q_i \setminus \mathcal{A}_\mathcal{H} \approx_\mathrm{mw} R_i \setminus \mathcal{A}_\mathcal{H}$ it follows that there exists $R_i \setminus \mathcal{A}_\mathcal{H} \stackrel{\tau^*}{\Longrightarrow}_\mathrm{a} \stackrel{l}{\longrightarrow}_\mathrm{a} \stackrel{\tau^*}{\Longrightarrow}_\mathrm{a} R_i' \setminus \mathcal{A}_\mathcal{H}$ such that $Q_i' \setminus \mathcal{A}_\mathcal{H} \approx_\mathrm{mw} R_i' \setminus \mathcal{A}_\mathcal{H}$. Since synchronization does not apply to τ and $l \in L$, we have that $(R_1 \parallel_L R_2) \setminus \mathcal{A}_\mathcal{H} \stackrel{\tau^*}{\Longrightarrow}_\mathrm{a} \stackrel{l}{\longrightarrow}_\mathrm{a} \stackrel{\tau^*}{\Longrightarrow}_\mathrm{a} (R_1' \parallel_L R_2') \setminus \mathcal{A}_\mathcal{H}$ with $((Q_1' \parallel_L Q_2') \setminus \mathcal{A}_\mathcal{H}, (R_1' \parallel_L R_2') \setminus \mathcal{A}_\mathcal{H}) \in \mathcal{B}$.
   - If $(Q_1 \parallel_L Q_2) \setminus \mathcal{A}_\mathcal{H} \stackrel{\tau}{\longrightarrow}_\mathrm{a} (Q_1' \parallel_L Q_2) \setminus \mathcal{A}_\mathcal{H}$ with $Q_1 \stackrel{\tau}{\longrightarrow}_\mathrm{a} Q_1'$, then $Q_1 \setminus \mathcal{A}_\mathcal{H} \stackrel{\tau}{\longrightarrow}_\mathrm{a} Q_1' \setminus \mathcal{A}_\mathcal{H}$ as $\tau \notin \mathcal{A}_\mathcal{H}$. From $Q_1 \setminus \mathcal{A}_\mathcal{H} \approx_\mathrm{mw} R_1 \setminus \mathcal{A}_\mathcal{H}$ it follows that there exists $R_1 \setminus \mathcal{A}_\mathcal{H} \stackrel{\tau^*}{\Longrightarrow}_\mathrm{a} R_1' \setminus \mathcal{A}_\mathcal{H}$ such that $Q_1' \setminus \mathcal{A}_\mathcal{H} \approx_\mathrm{mw} R_1' \setminus \mathcal{A}_\mathcal{H}$. Since synchronization does not apply to τ, we have that $(R_1 \parallel_L R_2) \setminus \mathcal{A}_\mathcal{H} \stackrel{\tau^*}{\Longrightarrow}_\mathrm{a} (R_1' \parallel_L R_2) \setminus \mathcal{A}_\mathcal{H}$ with $((Q_1' \parallel_L Q_2) \setminus \mathcal{A}_\mathcal{H}, (R_1' \parallel_L R_2) \setminus \mathcal{A}_\mathcal{H}) \in \mathcal{B}$.
   - If $(Q_1 \parallel_L Q_2) \setminus \mathcal{A}_\mathcal{H} \stackrel{\tau}{\longrightarrow}_\mathrm{a} (Q_1 \parallel_L Q_2') \setminus \mathcal{A}_\mathcal{H}$ with $Q_2 \stackrel{\tau}{\longrightarrow}_\mathrm{a} Q_2'$, then the proof is similar to the one of the previous case.

   As for rates, to avoid trivial cases consider an equivalence class $C \in \mathbb{P}_\mathrm{mk}/\mathcal{B}$ that involves processes reachable from $P_1 \parallel_L P_2$, specifically $C = \{(S_{1,i} \parallel_L S_{2,i}) \setminus \mathcal{A}_\mathcal{H} \mid S_{k,h} \in \mathit{reach}(P_k) \wedge S_{1,h} \parallel_L S_{2,h} \in \mathit{reach}(P_1 \parallel_L P_2) \wedge S_{k,i} \setminus \mathcal{A}_\mathcal{H} \approx_\mathrm{mw} S_{k,j} \setminus \mathcal{A}_\mathcal{H}\}$. Suppose that $(Q_1 \parallel_L Q_2) \setminus \mathcal{A}_\mathcal{H} \stackrel{\tau}{\not\longrightarrow}_\mathrm{a}$ so that $Q_k \setminus \mathcal{A}_\mathcal{H} \stackrel{\tau}{\not\longrightarrow}_\mathrm{a}$ too and hence from $Q_k \setminus \mathcal{A}_\mathcal{H} \approx_\mathrm{mw} R_k \setminus \mathcal{A}_\mathcal{H}$ it follows that there exists $R_k \setminus \mathcal{A}_\mathcal{H} \stackrel{\tau^*}{\Longrightarrow}_\mathrm{a} \bar{R}_k \setminus \mathcal{A}_\mathcal{H}$ such that

$\bar{R}_k \setminus \mathcal{A}_\mathcal{H} \stackrel{\tau}{\not\longrightarrow}_\mathrm{a}$, $Q_k \setminus \mathcal{A}_\mathcal{H} \approx_\mathrm{mw} \bar{R}_k \setminus \mathcal{A}_\mathcal{H}$, and $rate(Q_k \setminus \mathcal{A}_\mathcal{H}, C') = rate(\bar{R}_k \setminus \mathcal{A}_\mathcal{H}, C')$ for all $C' \in \mathbb{P}_\mathrm{mk}/\approx_\mathrm{mw}$. Since synchronization does not apply to τ, we have that $(R_1 \parallel_L R_2) \setminus \mathcal{A}_\mathcal{H} \stackrel{\tau^*}{\Longrightarrow}_\mathrm{a} (\bar{R}_1 \parallel_L \bar{R}_2) \setminus \mathcal{A}_\mathcal{H}$ with $(\bar{R}_1 \parallel_L \bar{R}_2) \setminus \mathcal{A}_\mathcal{H} \stackrel{\tau}{\not\longrightarrow}_\mathrm{a}$ and $((Q_1 \parallel_L Q_2) \setminus \mathcal{A}_\mathcal{H}, (\bar{R}_1 \parallel_L \bar{R}_2) \setminus \mathcal{A}_\mathcal{H}) \in \mathcal{B}$. Since the restriction operator does not apply to rate transitions, we have that:

$$\begin{array}{rcl} rate((Q_1 \parallel_L Q_2) \setminus \mathcal{A}_\mathcal{H}, C) & = & rate((Q_1 \setminus \mathcal{A}_\mathcal{H}) \parallel_L (Q_2 \setminus \mathcal{A}_\mathcal{H}), C) \\ rate((\bar{R}_1 \parallel_L \bar{R}_2) \setminus \mathcal{A}_\mathcal{H}, C) & = & rate((\bar{R}_1 \setminus \mathcal{A}_\mathcal{H}) \parallel_L (\bar{R}_2 \setminus \mathcal{A}_\mathcal{H}), C) \end{array}$$

Based on which subprocess moves so that the overall process reaches C (which we assume to be reachable in one move to avoid trivial cases in which cumulative rates are zero), we have that:

$$\begin{array}{rcl} rate((Q_1 \setminus \mathcal{A}_\mathcal{H}) \parallel_L (Q_2 \setminus \mathcal{A}_\mathcal{H}), C) & = & rate(Q_1 \setminus \mathcal{A}_\mathcal{H}, C_1) \\ rate((\bar{R}_1 \setminus \mathcal{A}_\mathcal{H}) \parallel_L (\bar{R}_2 \setminus \mathcal{A}_\mathcal{H}), C) & = & rate(\bar{R}_1 \setminus \mathcal{A}_\mathcal{H}, C_1) \end{array}$$

or:

$$\begin{array}{rcl} rate((Q_1 \setminus \mathcal{A}_\mathcal{H}) \parallel_L (Q_2 \setminus \mathcal{A}_\mathcal{H}), C) & = & rate(Q_2 \setminus \mathcal{A}_\mathcal{H}, C_2) \\ rate((\bar{R}_1 \setminus \mathcal{A}_\mathcal{H}) \parallel_L (\bar{R}_2 \setminus \mathcal{A}_\mathcal{H}), C) & = & rate(\bar{R}_2 \setminus \mathcal{A}_\mathcal{H}, C_2) \end{array}$$

where:

$$\begin{array}{rcl} C_1 & = & \{S_{1,h} \setminus \mathcal{A}_\mathcal{H} \mid (S_{1,h} \parallel_L S_{2,h}) \setminus \mathcal{A}_\mathcal{H} \in C\} \\ C_2 & = & \{S_{2,h} \setminus \mathcal{A}_\mathcal{H} \mid (S_{1,h} \parallel_L S_{2,h}) \setminus \mathcal{A}_\mathcal{H} \in C\} \end{array}$$

Since $Q_k \setminus \mathcal{A}_\mathcal{H} \approx_\mathrm{mw} \bar{R}_k \setminus \mathcal{A}_\mathcal{H}$ and C_k is the union of some $\approx_\mathrm{mw}$-equivalence classes for $k \in \{1, 2\}$, we have that:

$$\begin{array}{rcl} rate(Q_1 \setminus \mathcal{A}_\mathcal{H}, C_1) & = & rate(\bar{R}_1 \setminus \mathcal{A}_\mathcal{H}, C_1) \\ rate(Q_2 \setminus \mathcal{A}_\mathcal{H}, C_2) & = & rate(\bar{R}_2 \setminus \mathcal{A}_\mathcal{H}, C_2) \end{array}$$

If we start from $(R_1 \parallel_L R_2) \setminus \mathcal{A}_\mathcal{H} \stackrel{\tau}{\not\longrightarrow}_\mathrm{a}$, then the proof is similar.

We then prove the three results for the $\approx_\mathrm{mb}$-based properties. Let $\mathcal{B}$ be an equivalence relation containing all the pairs of processes that have to be shown to be $\approx_\mathrm{mb}$-equivalent according to the considered result:

1. Starting from $(Q_1 \parallel_L Q_2) \setminus \mathcal{A}_\mathcal{H}$ and $(R_1 \parallel_L R_2) / \mathcal{A}_\mathcal{H}$ related by $\mathcal{B}$, so that $Q_1 \setminus \mathcal{A}_\mathcal{H} \approx_\mathrm{mb} R_1 / \mathcal{A}_\mathcal{H}$ and $Q_2 \setminus \mathcal{A}_\mathcal{H} \approx_\mathrm{mb} R_2 / \mathcal{A}_\mathcal{H}$, there are twelve cases for action transitions based on the operational semantic rules in Table 10.1. In the first five cases, it is $(Q_1 \parallel_L Q_2) \setminus \mathcal{A}_\mathcal{H}$ to move first:

   - If $(Q_1 \parallel_L Q_2) \setminus \mathcal{A}_\mathcal{H} \stackrel{l}{\longrightarrow}_\mathrm{a} (Q_1' \parallel_L Q_2) \setminus \mathcal{A}_\mathcal{H}$ with $Q_1 \stackrel{l}{\longrightarrow}_\mathrm{a} Q_1'$ and $l \notin L$, then $Q_1 \setminus \mathcal{A}_\mathcal{H} \stackrel{l}{\longrightarrow}_\mathrm{a} Q_1' \setminus \mathcal{A}_\mathcal{H}$ as $l \notin \mathcal{A}_\mathcal{H}$. From $Q_1 \setminus \mathcal{A}_\mathcal{H} \approx_\mathrm{mb} R_1 / \mathcal{A}_\mathcal{H}$ it follows that there exists $R_1 / \mathcal{A}_\mathcal{H} \stackrel{\tau^*}{\Longrightarrow}_\mathrm{a} \bar{R}_1 / \mathcal{A}_\mathcal{H} \stackrel{l}{\longrightarrow}_\mathrm{a} R_1' / \mathcal{A}_\mathcal{H}$ such that $Q_1 \setminus \mathcal{A}_\mathcal{H} \approx_\mathrm{mb} \bar{R}_1 / \mathcal{A}_\mathcal{H}$ and $Q_1' \setminus \mathcal{A}_\mathcal{H} \approx_\mathrm{mb} R_1' / \mathcal{A}_\mathcal{H}$. Since synchronization does not apply to τ and $l \notin L$, we have that $(R_1 \parallel_L R_2) / \mathcal{A}_\mathcal{H} \stackrel{\tau^*}{\Longrightarrow}_\mathrm{a} (\bar{R}_1 \parallel_L R_2) / \mathcal{A}_\mathcal{H} \stackrel{l}{\longrightarrow}_\mathrm{a} (R_1' \parallel_L R_2) / \mathcal{A}_\mathcal{H}$ with $((Q_1 \parallel_L Q_2) \setminus \mathcal{A}_\mathcal{H}, (\bar{R}_1 \parallel_L R_2) / \mathcal{A}_\mathcal{H}) \in \mathcal{B}$ and $((Q_1' \parallel_L Q_2) \setminus \mathcal{A}_\mathcal{H}, (R_1' \parallel_L R_2) / \mathcal{A}_\mathcal{H}) \in \mathcal{B}$.
   - If $(Q_1 \parallel_L Q_2) \setminus \mathcal{A}_\mathcal{H} \stackrel{l}{\longrightarrow}_\mathrm{a} (Q_1 \parallel_L Q_2') \setminus \mathcal{A}_\mathcal{H}$ with $Q_2 \stackrel{l}{\longrightarrow}_\mathrm{a} Q_2'$ and $l \notin L$, then the proof is similar to the one of the previous case.
   - If $(Q_1 \parallel_L Q_2) \setminus \mathcal{A}_\mathcal{H} \stackrel{l}{\longrightarrow}_\mathrm{a} (Q_1' \parallel_L Q_2') \setminus \mathcal{A}_\mathcal{H}$ with $Q_i \stackrel{l}{\longrightarrow}_\mathrm{a} Q_i'$ for $i \in \{1, 2\}$ and $l \in L$, then $Q_i \setminus \mathcal{A}_\mathcal{H} \stackrel{l}{\longrightarrow}_\mathrm{a} Q_i' \setminus \mathcal{A}_\mathcal{H}$ as $l \notin \mathcal{A}_\mathcal{H}$. From $Q_i \setminus \mathcal{A}_\mathcal{H} \approx_\mathrm{mb} R_i / \mathcal{A}_\mathcal{H}$ it follows that there exists $R_i / \mathcal{A}_\mathcal{H} \stackrel{\tau^*}{\Longrightarrow}_\mathrm{a} \bar{R}_i / \mathcal{A}_\mathcal{H} \stackrel{l}{\longrightarrow}_\mathrm{a} R_i' / \mathcal{A}_\mathcal{H}$ such that $Q_i \setminus \mathcal{A}_\mathcal{H} \approx_\mathrm{mb} \bar{R}_i / \mathcal{A}_\mathcal{H}$ and $Q_i' \setminus \mathcal{A}_\mathcal{H} \approx_\mathrm{mb} R_i' / \mathcal{A}_\mathcal{H}$. Since synchronization does not apply to τ and $l \in L$, we have that $(R_1 \parallel_L R_2) / \mathcal{A}_\mathcal{H} \stackrel{\tau^*}{\Longrightarrow}_\mathrm{a} (\bar{R}_1 \parallel_L \bar{R}_2) / \mathcal{A}_\mathcal{H} \stackrel{l}{\longrightarrow}_\mathrm{a} (R_1' \parallel_L R_2') / \mathcal{A}_\mathcal{H}$ with $((Q_1 \parallel_L Q_2) \setminus \mathcal{A}_\mathcal{H}, (\bar{R}_1 \parallel_L \bar{R}_2) / \mathcal{A}_\mathcal{H}) \in \mathcal{B}$ and $((Q_1' \parallel_L Q_2') \setminus \mathcal{A}_\mathcal{H}, (R_1' \parallel_L R_2') / \mathcal{A}_\mathcal{H}) \in \mathcal{B}$.
   - If $(Q_1 \parallel_L Q_2) \setminus \mathcal{A}_\mathcal{H} \stackrel{\tau}{\longrightarrow}_\mathrm{a} (Q_1' \parallel_L Q_2) \setminus \mathcal{A}_\mathcal{H}$ with $Q_1 \stackrel{\tau}{\longrightarrow}_\mathrm{a} Q_1'$, then $Q_1 \setminus \mathcal{A}_\mathcal{H} \stackrel{\tau}{\longrightarrow}_\mathrm{a} Q_1' \setminus \mathcal{A}_\mathcal{H}$ as $\tau \notin \mathcal{A}_\mathcal{H}$. From $Q_1 \setminus \mathcal{A}_\mathcal{H} \approx_\mathrm{mb} R_1 / \mathcal{A}_\mathcal{H}$ it follows that either $Q_1' \setminus \mathcal{A}_\mathcal{H} \approx_\mathrm{mb} R_1 / \mathcal{A}_\mathcal{H}$, or there exists $R_1 / \mathcal{A}_\mathcal{H} \stackrel{\tau^*}{\Longrightarrow}_\mathrm{a} \bar{R}_1 / \mathcal{A}_\mathcal{H} \stackrel{\tau}{\longrightarrow}_\mathrm{a} R_1' / \mathcal{A}_\mathcal{H}$ such that $Q_1 \setminus \mathcal{A}_\mathcal{H} \approx_\mathrm{mb} \bar{R}_1 / \mathcal{A}_\mathcal{H}$ and $Q_1' \setminus \mathcal{A}_\mathcal{H} \approx_\mathrm{mb}$

$R'_1 / \mathcal{A}_\mathcal{H}$. Since synchronization does not apply to τ, in the former subcase $(R_1 \parallel_L R_2) / \mathcal{A}_\mathcal{H}$ is allowed to stay idle with $((Q'_1 \parallel_L Q_2) \setminus \mathcal{A}_\mathcal{H}, (R_1 \parallel_L R_2) / \mathcal{A}_\mathcal{H}) \in \mathcal{B}$, while in the latter subcase $(R_1 \parallel_L R_2) / \mathcal{A}_\mathcal{H} \stackrel{\tau^*}{\Longrightarrow}_\mathrm{a} (\bar{R}_1 \parallel_L R_2) / \mathcal{A}_\mathcal{H} \stackrel{\tau}{\longrightarrow}_\mathrm{a} (R'_1 \parallel_L R_2) / \mathcal{A}_\mathcal{H}$ with $((Q_1 \parallel_L Q_2) \setminus \mathcal{A}_\mathcal{H}, (\bar{R}_1 \parallel_L R_2) / \mathcal{A}_\mathcal{H}) \in \mathcal{B}$ and $((Q'_1 \parallel_L Q_2) \setminus \mathcal{A}_\mathcal{H}, (R'_1 \parallel_L R_2) / \mathcal{A}_\mathcal{H}) \in \mathcal{B}$.

- If $(Q_1 \parallel_L Q_2) \setminus \mathcal{A}_\mathcal{H} \stackrel{\tau}{\longrightarrow}_\mathrm{a} (Q_1 \parallel_L Q'_2) \setminus \mathcal{A}_\mathcal{H}$ with $Q_2 \stackrel{\tau}{\longrightarrow}_\mathrm{a} Q'_2$, then the proof is similar to the one of the previous case.

In the other seven cases, instead, it is $(R_1 \parallel_L R_2) / \mathcal{A}_\mathcal{H}$ to move first:

- If $(R_1 \parallel_L R_2) / \mathcal{A}_\mathcal{H} \stackrel{l}{\longrightarrow}_\mathrm{a} (R'_1 \parallel_L R_2) / \mathcal{A}_\mathcal{H}$ with $R_1 \stackrel{l}{\longrightarrow}_\mathrm{a} R'_1$ and $l \notin L$, then $R_1 / \mathcal{A}_\mathcal{H} \stackrel{l}{\longrightarrow}_\mathrm{a} R'_1 / \mathcal{A}_\mathcal{H}$ as $l \notin \mathcal{A}_\mathcal{H}$. From $R_1 / \mathcal{A}_\mathcal{H} \approx_\mathrm{mb} Q_1 \setminus \mathcal{A}_\mathcal{H}$ it follows that there exists $Q_1 \setminus \mathcal{A}_\mathcal{H} \stackrel{\tau^*}{\Longrightarrow}_\mathrm{a} \bar{Q}_1 \setminus \mathcal{A}_\mathcal{H} \stackrel{l}{\longrightarrow}_\mathrm{a} Q'_1 \setminus \mathcal{A}_\mathcal{H}$ such that $R_1 / \mathcal{A}_\mathcal{H} \approx_\mathrm{mb} \bar{Q}_1 \setminus \mathcal{A}_\mathcal{H}$ and $R'_1 / \mathcal{A}_\mathcal{H} \approx_\mathrm{mb} Q'_1 \setminus \mathcal{A}_\mathcal{H}$. Since synchronization does not apply to τ and $l \notin L$, we have that $(Q_1 \parallel_L Q_2) \setminus \mathcal{A}_\mathcal{H} \stackrel{\tau^*}{\Longrightarrow}_\mathrm{a} (\bar{Q}_1 \parallel_L Q_2) \setminus \mathcal{A}_\mathcal{H} \stackrel{l}{\longrightarrow}_\mathrm{a} (Q'_1 \parallel_L Q_2) \setminus \mathcal{A}_\mathcal{H}$ with $((R_1 \parallel_L R_2)/\mathcal{A}_\mathcal{H}, (\bar{Q}_1 \parallel_L Q_2) \setminus \mathcal{A}_\mathcal{H}) \in \mathcal{B}$ and $((R'_1 \parallel_L R_2)/\mathcal{A}_\mathcal{H}, (Q'_1 \parallel_L Q_2) \setminus \mathcal{A}_\mathcal{H}) \in \mathcal{B}$.
- If $(R_1 \parallel_L R_2) / \mathcal{A}_\mathcal{H} \stackrel{l}{\longrightarrow}_\mathrm{a} (R_1 \parallel_L R'_2) / \mathcal{A}_\mathcal{H}$ with $R_2 \stackrel{l}{\longrightarrow}_\mathrm{a} R'_2$ and $l \notin L$, then the proof is similar to the one of the previous case.
- If $(R_1 \parallel_L R_2) / \mathcal{A}_\mathcal{H} \stackrel{l}{\longrightarrow}_\mathrm{a} (R'_1 \parallel_L R'_2) / \mathcal{A}_\mathcal{H}$ with $R_i \stackrel{l}{\longrightarrow}_\mathrm{a} R'_i$ for $i \in \{1, 2\}$ and $l \in L$, then $R_i / \mathcal{A}_\mathcal{H} \stackrel{l}{\longrightarrow}_\mathrm{a} R'_i / \mathcal{A}_\mathcal{H}$ as $l \notin \mathcal{A}_\mathcal{H}$. From $R_i / \mathcal{A}_\mathcal{H} \approx_\mathrm{mb} Q_i \setminus \mathcal{A}_\mathcal{H}$ it follows that there exists $Q_i \setminus \mathcal{A}_\mathcal{H} \stackrel{\tau^*}{\Longrightarrow}_\mathrm{a} \bar{Q}_i \setminus \mathcal{A}_\mathcal{H} \stackrel{l}{\longrightarrow}_\mathrm{a} Q'_i \setminus \mathcal{A}_\mathcal{H}$ such that $R_i / \mathcal{A}_\mathcal{H} \approx_\mathrm{mb} \bar{Q}_i \setminus \mathcal{A}_\mathcal{H}$ and $R'_i / \mathcal{A}_\mathcal{H} \approx_\mathrm{mb} Q'_i \setminus \mathcal{A}_\mathcal{H}$. Since synchronization does not apply to τ and $l \in L$, we have that $(Q_1 \parallel_L Q_2) \setminus \mathcal{A}_\mathcal{H} \stackrel{\tau^*}{\Longrightarrow}_\mathrm{a} (\bar{Q}_1 \parallel_L \bar{Q}_2) \setminus \mathcal{A}_\mathcal{H} \stackrel{l}{\longrightarrow}_\mathrm{a} (Q'_1 \parallel_L Q'_2) \setminus \mathcal{A}_\mathcal{H}$ with $((R_1 \parallel_L R_2)/\mathcal{A}_\mathcal{H}, (\bar{Q}_1 \parallel_L \bar{Q}_2) \setminus \mathcal{A}_\mathcal{H}) \in \mathcal{B}$ and $((R'_1 \parallel_L R'_2) / \mathcal{A}_\mathcal{H}, (Q'_1 \parallel_L Q'_2) \setminus \mathcal{A}_\mathcal{H}) \in \mathcal{B}$.
- If $(R_1 \parallel_L R_2) / \mathcal{A}_\mathcal{H} \stackrel{\tau}{\longrightarrow}_\mathrm{a} (R'_1 \parallel_L R_2) / \mathcal{A}_\mathcal{H}$ with $R_1 \stackrel{\tau}{\longrightarrow}_\mathrm{a} R'_1$, then $R_1 / \mathcal{A}_\mathcal{H} \stackrel{\tau}{\longrightarrow}_\mathrm{a} R'_1 / \mathcal{A}_\mathcal{H}$ as $\tau \notin \mathcal{A}_\mathcal{H}$. From $R_1 / \mathcal{A}_\mathcal{H} \approx_\mathrm{mb} Q_1 \setminus \mathcal{A}_\mathcal{H}$ it follows that either $R'_1 / \mathcal{A}_\mathcal{H} \approx_\mathrm{mb} Q_1 \setminus \mathcal{A}_\mathcal{H}$, or there exists $Q_1 \setminus \mathcal{A}_\mathcal{H} \stackrel{\tau^*}{\Longrightarrow}_\mathrm{a} \bar{Q}_1 \setminus \mathcal{A}_\mathcal{H} \stackrel{\tau}{\longrightarrow}_\mathrm{a} Q'_1 \setminus \mathcal{A}_\mathcal{H}$ such that $R_1 / \mathcal{A}_\mathcal{H} \approx_\mathrm{mb} \bar{Q}_1 \setminus \mathcal{A}_\mathcal{H}$ and $R'_1 / \mathcal{A}_\mathcal{H} \approx_\mathrm{mb} Q'_1 \setminus \mathcal{A}_\mathcal{H}$. Since synchronization does not apply to τ, in the former subcase $(Q_1 \parallel_L Q_2) \setminus \mathcal{A}_\mathcal{H}$ is allowed to stay idle with $((R'_1 \parallel_L R_2)/\mathcal{A}_\mathcal{H}, (Q_1 \parallel_L Q_2) \setminus \mathcal{A}_\mathcal{H}) \in \mathcal{B}$, while in the latter subcase $(Q_1 \parallel_L Q_2) \setminus \mathcal{A}_\mathcal{H} \stackrel{\tau^*}{\Longrightarrow}_\mathrm{a} (\bar{Q}_1 \parallel_L Q_2) \setminus \mathcal{A}_\mathcal{H} \stackrel{\tau}{\longrightarrow}_\mathrm{a} (Q'_1 \parallel_L Q_2) \setminus \mathcal{A}_\mathcal{H}$ with $((R_1 \parallel_L R_2)/\mathcal{A}_\mathcal{H}, (\bar{Q}_1 \parallel_L Q_2) \setminus \mathcal{A}_\mathcal{H}) \in \mathcal{B}$ and $((R'_1 \parallel_L R_2)/\mathcal{A}_\mathcal{H}, (Q'_1 \parallel_L Q_2) \setminus \mathcal{A}_\mathcal{H}) \in \mathcal{B}$.
- If $(R_1 \parallel_L R_2) / \mathcal{A}_\mathcal{H} \stackrel{\tau}{\longrightarrow}_\mathrm{a} (R_1 \parallel_L R'_2) / \mathcal{A}_\mathcal{H}$ with $R_2 \stackrel{\tau}{\longrightarrow}_\mathrm{a} R'_2$, then the proof is similar to the one of the previous case.
- If $(R_1 \parallel_L R_2) / \mathcal{A}_\mathcal{H} \stackrel{\tau}{\longrightarrow}_\mathrm{a} (R'_1 \parallel_L R_2) / \mathcal{A}_\mathcal{H}$ with $R_1 \stackrel{h}{\longrightarrow}_\mathrm{a} R'_1$ and $h \notin L$, then $R_1 / \mathcal{A}_\mathcal{H} \stackrel{\tau}{\longrightarrow}_\mathrm{a} R'_1 / \mathcal{A}_\mathcal{H}$ as $h \in \mathcal{A}_\mathcal{H}$. The rest of the proof is like the one of the fourth case.
- If $(R_1 \parallel_L R_2) / \mathcal{A}_\mathcal{H} \stackrel{\tau}{\longrightarrow}_\mathrm{a} (R_1 \parallel_L R'_2) / \mathcal{A}_\mathcal{H}$ with $R_2 \stackrel{h}{\longrightarrow}_\mathrm{a} R'_2$ and $h \notin L$, then the proof is similar to the one of the previous case.

As for rates, we reason like in the proof of the corresponding result for $\approx_\mathrm{mw}$.

2. Starting from $(Q / \mathcal{A}_\mathcal{H}) \setminus L$ and $(R \setminus L) / \mathcal{A}_\mathcal{H}$ related by $\mathcal{B}$, so that $Q / \mathcal{A}_\mathcal{H} \approx_\mathrm{mb} R \setminus \mathcal{A}_\mathcal{H}$, there are six cases for action transitions based on the operational semantic rules in Table 10.1. In the first three cases, it is $(Q / \mathcal{A}_\mathcal{H}) \setminus L$ to move first:

- If $(Q \,/\, \mathcal{A}_\mathcal{H}) \setminus L \xrightarrow{l}_\mathrm{a} (Q' \,/\, \mathcal{A}_\mathcal{H}) \setminus L$ with $Q \xrightarrow{l}_\mathrm{a} Q'$ and $l \notin L$, then $Q \,/\, \mathcal{A}_\mathcal{H} \xrightarrow{l}_\mathrm{a} Q' \,/\, \mathcal{A}_\mathcal{H}$ as $l \notin \mathcal{A}_\mathcal{H}$. From $Q \,/\, \mathcal{A}_\mathcal{H} \approx_\mathrm{mb} R \setminus \mathcal{A}_\mathcal{H}$ it follows that there exists $R \setminus \mathcal{A}_\mathcal{H} \xRightarrow{\tau^*}_\mathrm{a} \bar{R} \setminus \mathcal{A}_\mathcal{H} \xrightarrow{l}_\mathrm{a} R' \setminus \mathcal{A}_\mathcal{H}$ such that $Q \,/\, \mathcal{A}_\mathcal{H} \approx_\mathrm{mb} \bar{R} \setminus \mathcal{A}_\mathcal{H}$ and $Q' \,/\, \mathcal{A}_\mathcal{H} \approx_\mathrm{mb} R' \setminus \mathcal{A}_\mathcal{H}$. Since the restriction and hiding operators do not apply to τ and l, we have that $(R \setminus L) \,/\, \mathcal{A}_\mathcal{H} \xRightarrow{\tau^*}_\mathrm{a} (\bar{R} \setminus L) \,/\, \mathcal{A}_\mathcal{H} \xrightarrow{l}_\mathrm{a} (R' \setminus L) \,/\, \mathcal{A}_\mathcal{H}$ with $((Q \,/\, \mathcal{A}_\mathcal{H}) \setminus L, (\bar{R} \setminus L) \,/\, \mathcal{A}_\mathcal{H}) \in \mathcal{B}$ and $((Q' \,/\, \mathcal{A}_\mathcal{H}) \setminus L, (R' \setminus L) \,/\, \mathcal{A}_\mathcal{H}) \in \mathcal{B}$.
- If $(Q \,/\, \mathcal{A}_\mathcal{H}) \setminus L \xrightarrow{\tau}_\mathrm{a} (Q' \,/\, \mathcal{A}_\mathcal{H}) \setminus L$ with $Q \xrightarrow{\tau}_\mathrm{a} Q'$, then $Q \,/\, \mathcal{A}_\mathcal{H} \xrightarrow{\tau}_\mathrm{a} Q' \,/\, \mathcal{A}_\mathcal{H}$ as $\tau \notin \mathcal{A}_\mathcal{H}$. From $Q \,/\, \mathcal{A}_\mathcal{H} \approx_\mathrm{mb} R \setminus \mathcal{A}_\mathcal{H}$ it follows that either $Q' \,/\, \mathcal{A}_\mathcal{H} \approx_\mathrm{mb} R \setminus \mathcal{A}_\mathcal{H}$, or there exists $R \setminus \mathcal{A}_\mathcal{H} \xRightarrow{\tau^*}_\mathrm{a} \bar{R} \setminus \mathcal{A}_\mathcal{H} \xrightarrow{\tau}_\mathrm{a} R' \setminus \mathcal{A}_\mathcal{H}$ such that $Q \,/\, \mathcal{A}_\mathcal{H} \approx_\mathrm{mb} \bar{R} \setminus \mathcal{A}_\mathcal{H}$ and $Q' \,/\, \mathcal{A}_\mathcal{H} \approx_\mathrm{mb} R' \setminus \mathcal{A}_\mathcal{H}$. Since the restriction and hiding operators do not apply to τ, in the former subcase $(R \setminus L) \,/\, \mathcal{A}_\mathcal{H}$ is allowed to stay idle with $((Q' \,/\, \mathcal{A}_\mathcal{H}) \setminus L, (R \setminus L) \,/\, \mathcal{A}_\mathcal{H}) \in \mathcal{B}$, while in the latter subcase $(R \setminus L) \,/\, \mathcal{A}_\mathcal{H} \xRightarrow{\tau^*}_\mathrm{a} (\bar{R} \setminus L) \,/\, \mathcal{A}_\mathcal{H} \xrightarrow{\tau}_\mathrm{a} (R' \setminus L) \,/\, \mathcal{A}_\mathcal{H}$ with $((Q \,/\, \mathcal{A}_\mathcal{H}) \setminus L, (\bar{R} \setminus L) \,/\, \mathcal{A}_\mathcal{H}) \in \mathcal{B}$ and $((Q' \,/\, \mathcal{A}_\mathcal{H}) \setminus L, (R' \setminus L) \,/\, \mathcal{A}_\mathcal{H}) \in \mathcal{B}$.
- If $(Q \,/\, \mathcal{A}_\mathcal{H}) \setminus L \xrightarrow{\tau}_\mathrm{a} (Q' \,/\, \mathcal{A}_\mathcal{H}) \setminus L$ with $Q \xrightarrow{h}_\mathrm{a} Q'$, then $Q \,/\, \mathcal{A}_\mathcal{H} \xrightarrow{\tau}_\mathrm{a} Q' \,/\, \mathcal{A}_\mathcal{H}$ as $h \in \mathcal{A}_\mathcal{H}$. The rest of the proof is like the one of the previous case.

In the other three cases, instead, it is $(R \setminus L) \,/\, \mathcal{A}_\mathcal{H}$ to move first:

- If $(R \setminus L) \,/\, \mathcal{A}_\mathcal{H} \xrightarrow{l}_\mathrm{a} (R' \setminus L) \,/\, \mathcal{A}_\mathcal{H}$ with $R \xrightarrow{l}_\mathrm{a} R'$ and $l \notin L$, then $R \setminus \mathcal{A}_\mathcal{H} \xrightarrow{l}_\mathrm{a} R' \setminus \mathcal{A}_\mathcal{H}$ as $l \notin \mathcal{A}_\mathcal{H}$. From $R \setminus \mathcal{A}_\mathcal{H} \approx_\mathrm{mb} Q \,/\, \mathcal{A}_\mathcal{H}$ it follows that there exists $Q \,/\, \mathcal{A}_\mathcal{H} \xRightarrow{\tau^*}_\mathrm{a} \bar{Q} \,/\, \mathcal{A}_\mathcal{H} \xrightarrow{l}_\mathrm{a} Q' \,/\, \mathcal{A}_\mathcal{H}$ such that $R \setminus \mathcal{A}_\mathcal{H} \approx_\mathrm{mb} \bar{Q} \,/\, \mathcal{A}_\mathcal{H}$ and $R' \setminus \mathcal{A}_\mathcal{H} \approx_\mathrm{mb} Q' \,/\, \mathcal{A}_\mathcal{H}$. Since the restriction operator does not apply to τ and l, we have that $(Q \,/\, \mathcal{A}_\mathcal{H}) \setminus L \xRightarrow{\tau^*}_\mathrm{a} (\bar{Q} \,/\, \mathcal{A}_\mathcal{H}) \setminus L \xrightarrow{l}_\mathrm{a} (Q' \,/\, \mathcal{A}_\mathcal{H}) \setminus L$ with $((R \setminus L) \,/\, \mathcal{A}_\mathcal{H}, (\bar{Q} \,/\, \mathcal{A}_\mathcal{H}) \setminus L) \in \mathcal{B}$ and $((R' \setminus L) \,/\, \mathcal{A}_\mathcal{H}, (Q' \,/\, \mathcal{A}_\mathcal{H}) \setminus L) \in \mathcal{B}$.
- If $(R \setminus L) \,/\, \mathcal{A}_\mathcal{H} \xrightarrow{\tau}_\mathrm{a} (R' \setminus L) \,/\, \mathcal{A}_\mathcal{H}$ with $R \xrightarrow{\tau}_\mathrm{a} R'$, then $R \setminus \mathcal{A}_\mathcal{H} \xrightarrow{\tau}_\mathrm{a} R' \setminus \mathcal{A}_\mathcal{H}$ as $\tau \notin \mathcal{A}_\mathcal{H}$. From $R \setminus \mathcal{A}_\mathcal{H} \approx_\mathrm{mb} Q \,/\, \mathcal{A}_\mathcal{H}$ it follows that either $R' \setminus \mathcal{A}_\mathcal{H} \approx_\mathrm{mb} Q \,/\, \mathcal{A}_\mathcal{H}$, or there exists $Q \,/\, \mathcal{A}_\mathcal{H} \xRightarrow{\tau^*}_\mathrm{a} \bar{Q} \,/\, \mathcal{A}_\mathcal{H} \xrightarrow{\tau}_\mathrm{a} Q' \,/\, \mathcal{A}_\mathcal{H}$ such that $R \setminus \mathcal{A}_\mathcal{H} \approx_\mathrm{mb} \bar{Q} \,/\, \mathcal{A}_\mathcal{H}$ and $R' \setminus \mathcal{A}_\mathcal{H} \approx_\mathrm{mb} Q' \,/\, \mathcal{A}_\mathcal{H}$. Since the restriction operator does not apply to τ, in the former subcase $(Q \,/\, \mathcal{A}_\mathcal{H}) \setminus L$ is allowed to stay idle with $((R' \setminus L) \,/\, \mathcal{A}_\mathcal{H}, (Q \,/\, \mathcal{A}_\mathcal{H}) \setminus L) \in \mathcal{B}$, while in the latter subcase $(Q \,/\, \mathcal{A}_\mathcal{H}) \setminus L \xRightarrow{\tau^*}_\mathrm{a} (\bar{Q} \,/\, \mathcal{A}_\mathcal{H}) \setminus L \xrightarrow{\tau}_\mathrm{a} (Q' \,/\, \mathcal{A}_\mathcal{H}) \setminus L$ with $((R \setminus L) \,/\, \mathcal{A}_\mathcal{H}, (\bar{Q} \,/\, \mathcal{A}_\mathcal{H}) \setminus L) \in \mathcal{B}$ and $((R' \setminus L) \,/\, \mathcal{A}_\mathcal{H}, (Q' \,/\, \mathcal{A}_\mathcal{H}) \setminus L) \in \mathcal{B}$.
- If $(R \setminus L) \,/\, \mathcal{A}_\mathcal{H} \xrightarrow{\tau}_\mathrm{a} (R' \setminus L) \,/\, \mathcal{A}_\mathcal{H}$ with $R \xrightarrow{h}_\mathrm{a} R'$ and $h \notin L$, then $R \,/\, \mathcal{A}_\mathcal{H} \xrightarrow{\tau}_\mathrm{a} R' \,/\, \mathcal{A}_\mathcal{H}$ as $h \in \mathcal{A}_\mathcal{H}$ (note that $R \setminus \mathcal{A}_\mathcal{H}$ cannot perform h). From $R \,/\, \mathcal{A}_\mathcal{H} \approx_\mathrm{mb} R \setminus \mathcal{A}_\mathcal{H}$ – as $P \in \mathrm{SBSNNI}_{\approx_\mathrm{mb}}$ and $R \in \mathit{reach}(P)$ – and $R \setminus \mathcal{A}_\mathcal{H} \approx_\mathrm{mb} Q \,/\, \mathcal{A}_\mathcal{H}$ it follows that either $R' \,/\, \mathcal{A}_\mathcal{H} \approx_\mathrm{mb} Q \,/\, \mathcal{A}_\mathcal{H}$ and hence $R' \setminus \mathcal{A}_\mathcal{H} \approx_\mathrm{mb} Q \,/\, \mathcal{A}_\mathcal{H}$ – as $R' \,/\, \mathcal{A}_\mathcal{H} \approx_\mathrm{mb} R' \setminus \mathcal{A}_\mathcal{H}$ due to $P \in \mathrm{SBSNNI}_{\approx_\mathrm{mb}}$ and $R' \in \mathit{reach}(P)$ – or there exists $Q \,/\, \mathcal{A}_\mathcal{H} \xRightarrow{\tau^*}_\mathrm{a} \bar{Q} \,/\, \mathcal{A}_\mathcal{H} \xrightarrow{\tau}_\mathrm{a} Q' \,/\, \mathcal{A}_\mathcal{H}$ such that $R \,/\, \mathcal{A}_\mathcal{H} \approx_\mathrm{mb} \bar{Q} \,/\, \mathcal{A}_\mathcal{H}$ and $R' \,/\, \mathcal{A}_\mathcal{H} \approx_\mathrm{mb} Q' \,/\, \mathcal{A}_\mathcal{H}$ and hence $R \setminus \mathcal{A}_\mathcal{H} \approx_\mathrm{mb} \bar{Q} \,/\, \mathcal{A}_\mathcal{H}$ and $R' \setminus \mathcal{A}_\mathcal{H} \approx_\mathrm{mb} Q' \,/\, \mathcal{A}_\mathcal{H}$. Since the restriction operator does not apply to τ, in the former subcase $(Q \,/\, \mathcal{A}_\mathcal{H}) \setminus L$ is allowed to stay idle with $((R' \setminus L) \,/\, \mathcal{A}_\mathcal{H}, (Q \,/\, \mathcal{A}_\mathcal{H}) \setminus L) \in \mathcal{B}$, while in the latter subcase $(Q \,/\, \mathcal{A}_\mathcal{H}) \setminus L \xRightarrow{\tau^*}_\mathrm{a} (\bar{Q} \,/\, \mathcal{A}_\mathcal{H}) \setminus L \xrightarrow{\tau}_\mathrm{a} (Q' \,/\, \mathcal{A}_\mathcal{H}) \setminus L$ with $((R \setminus L) \,/\, \mathcal{A}_\mathcal{H}, (\bar{Q} \,/\, \mathcal{A}_\mathcal{H}) \setminus L) \in \mathcal{B}$ and $((R' \setminus L) \,/\, \mathcal{A}_\mathcal{H}, (Q' \,/\, \mathcal{A}_\mathcal{H}) \setminus L) \in \mathcal{B}$.

As for rates, we reason like in the proof of the corresponding result for $\approx_\mathrm{mw}$.

3. Starting from $(Q_1 \parallel_L Q_2) \setminus \mathcal{A}_\mathcal{H}$ and $(R_1 \parallel_L R_2) \setminus \mathcal{A}_\mathcal{H}$ related by $\mathcal{B}$, so that $Q_1 \setminus \mathcal{A}_\mathcal{H} \approx_{\rm mb} R_1 \setminus \mathcal{A}_\mathcal{H}$ and $Q_2 \setminus \mathcal{A}_\mathcal{H} \approx_{\rm mb} R_2 \setminus \mathcal{A}_\mathcal{H}$, there are five cases for action transitions based on the operational semantic rules in Table 10.1:

   - If $(Q_1 \parallel_L Q_2) \setminus \mathcal{A}_\mathcal{H} \stackrel{l}{\longrightarrow}_{\rm a} (Q_1' \parallel_L Q_2) \setminus \mathcal{A}_\mathcal{H}$ with $Q_1 \stackrel{l}{\longrightarrow}_{\rm a} Q_1'$ and $l \notin L$, then $Q_1 \setminus \mathcal{A}_\mathcal{H} \stackrel{l}{\longrightarrow}_{\rm a} Q_1' \setminus \mathcal{A}_\mathcal{H}$ as $l \notin \mathcal{A}_\mathcal{H}$. From $Q_1 \setminus \mathcal{A}_\mathcal{H} \approx_{\rm mb} R_1 \setminus \mathcal{A}_\mathcal{H}$ it follows that there exists $R_1 \setminus \mathcal{A}_\mathcal{H} \stackrel{\tau^*}{\Longrightarrow}_{\rm a} \bar{R}_1 \setminus \mathcal{A}_\mathcal{H} \stackrel{l}{\longrightarrow}_{\rm a} R_1' \setminus \mathcal{A}_\mathcal{H}$ such that $Q_1 \setminus \mathcal{A}_\mathcal{H} \approx_{\rm mb} \bar{R}_1 \setminus \mathcal{A}_\mathcal{H}$ and $Q_1' \setminus \mathcal{A}_\mathcal{H} \approx_{\rm mb} R_1' \setminus \mathcal{A}_\mathcal{H}$. Since synchronization does not apply to τ and $l \notin L$, we have that $(R_1 \parallel_L R_2) \setminus \mathcal{A}_\mathcal{H} \stackrel{\tau^*}{\Longrightarrow}_{\rm a} (\bar{R}_1 \parallel_L R_2) \setminus \mathcal{A}_\mathcal{H} \stackrel{l}{\longrightarrow}_{\rm a} (R_1' \parallel_L R_2) \setminus \mathcal{A}_\mathcal{H}$ with $((Q_1 \parallel_L Q_2) \setminus \mathcal{A}_\mathcal{H}, (\bar{R}_1 \parallel_L R_2) \setminus \mathcal{A}_\mathcal{H}) \in \mathcal{B}$ and $((Q_1' \parallel_L Q_2) \setminus \mathcal{A}_\mathcal{H}, (R_1' \parallel_L R_2) \setminus \mathcal{A}_\mathcal{H}) \in \mathcal{B}$.
   - If $(Q_1 \parallel_L Q_2) \setminus \mathcal{A}_\mathcal{H} \stackrel{l}{\longrightarrow}_{\rm a} (Q_1 \parallel_L Q_2') \setminus \mathcal{A}_\mathcal{H}$ with $Q_2 \stackrel{l}{\longrightarrow}_{\rm a} Q_2'$ and $l \notin L$, then the proof is similar to the one of the previous case.
   - If $(Q_1 \parallel_L Q_2) \setminus \mathcal{A}_\mathcal{H} \stackrel{l}{\longrightarrow}_{\rm a} (Q_1' \parallel_L Q_2') \setminus \mathcal{A}_\mathcal{H}$ with $Q_i \stackrel{l}{\longrightarrow}_{\rm a} Q_i'$ for $i \in \{1,2\}$ and $l \in L$, then $Q_i \setminus \mathcal{A}_\mathcal{H} \stackrel{l}{\longrightarrow}_{\rm a} Q_i' \setminus \mathcal{A}_\mathcal{H}$ as $l \notin \mathcal{A}_\mathcal{H}$. From $Q_i \setminus \mathcal{A}_\mathcal{H} \approx_{\rm mb} R_i \setminus \mathcal{A}_\mathcal{H}$ it follows that there exists $R_i \setminus \mathcal{A}_\mathcal{H} \stackrel{\tau^*}{\Longrightarrow}_{\rm a} \bar{R}_i \setminus \mathcal{A}_\mathcal{H} \stackrel{l}{\longrightarrow}_{\rm a} R_i' \setminus \mathcal{A}_\mathcal{H}$ such that $Q_i \setminus \mathcal{A}_\mathcal{H} \approx_{\rm mb} \bar{R}_i \setminus \mathcal{A}_\mathcal{H}$ and $Q_i' \setminus \mathcal{A}_\mathcal{H} \approx_{\rm mb} R_i' \setminus \mathcal{A}_\mathcal{H}$. Since synchronization does not apply to τ and $l \in L$, we have that $(R_1 \parallel_L R_2) \setminus \mathcal{A}_\mathcal{H} \stackrel{\tau^*}{\Longrightarrow}_{\rm a} (\bar{R}_1 \parallel_L \bar{R}_2) \setminus \mathcal{A}_\mathcal{H} \stackrel{l}{\longrightarrow}_{\rm a} (R_1' \parallel_L R_2') \setminus \mathcal{A}_\mathcal{H}$ with $((Q_1 \parallel_L Q_2) \setminus \mathcal{A}_\mathcal{H}, (\bar{R}_1 \parallel_L \bar{R}_2) \setminus \mathcal{A}_\mathcal{H}) \in \mathcal{B}$ and $((Q_1' \parallel_L Q_2') \setminus \mathcal{A}_\mathcal{H}, (R_1' \parallel_L R_2') \setminus \mathcal{A}_\mathcal{H}) \in \mathcal{B}$.
   - If $(Q_1 \parallel_L Q_2) \setminus \mathcal{A}_\mathcal{H} \stackrel{\tau}{\longrightarrow}_{\rm a} (Q_1' \parallel_L Q_2) \setminus \mathcal{A}_\mathcal{H}$ with $Q_1 \stackrel{\tau}{\longrightarrow}_{\rm a} Q_1'$, then $Q_1 \setminus \mathcal{A}_\mathcal{H} \stackrel{\tau}{\longrightarrow}_{\rm a} Q_1' \setminus \mathcal{A}_\mathcal{H}$ as $\tau \notin \mathcal{A}_\mathcal{H}$. From $Q_1 \setminus \mathcal{A}_\mathcal{H} \approx_{\rm mb} R_1 \setminus \mathcal{A}_\mathcal{H}$ it follows that either $Q_1' \setminus \mathcal{A}_\mathcal{H} \approx_{\rm mb} R_1 \setminus \mathcal{A}_\mathcal{H}$, or there exists $R_1 \setminus \mathcal{A}_\mathcal{H} \stackrel{\tau^*}{\Longrightarrow}_{\rm a} \bar{R}_1 \setminus \mathcal{A}_\mathcal{H} \stackrel{\tau}{\longrightarrow}_{\rm a} R_1' \setminus \mathcal{A}_\mathcal{H}$ such that $Q_1 \setminus \mathcal{A}_\mathcal{H} \approx_{\rm mb} \bar{R}_1 \setminus \mathcal{A}_\mathcal{H}$ and $Q_1' \setminus \mathcal{A}_\mathcal{H} \approx_{\rm mb} R_1' \setminus \mathcal{A}_\mathcal{H}$. Since synchronization does not apply to τ, in the former subcase $(R_1 \parallel_L R_2) \setminus \mathcal{A}_\mathcal{H}$ is allowed to stay idle with $((Q_1' \parallel_L Q_2) \setminus \mathcal{A}_\mathcal{H}, (R_1 \parallel_L R_2) \setminus \mathcal{A}_\mathcal{H}) \in \mathcal{B}$, while in the latter subcase $(R_1 \parallel_L R_2) \setminus \mathcal{A}_\mathcal{H} \stackrel{\tau^*}{\Longrightarrow}_{\rm a} (\bar{R}_1 \parallel_L R_2) \setminus \mathcal{A}_\mathcal{H} \stackrel{\tau}{\longrightarrow}_{\rm a} (R_1' \parallel_L R_2) \setminus \mathcal{A}_\mathcal{H}$ with $((Q_1 \parallel_L Q_2) \setminus \mathcal{A}_\mathcal{H}, (\bar{R}_1 \parallel_L R_2) \setminus \mathcal{A}_\mathcal{H}) \in \mathcal{B}$ and $((Q_1' \parallel_L Q_2) \setminus \mathcal{A}_\mathcal{H}, (R_1' \parallel_L R_2) \setminus \mathcal{A}_\mathcal{H}) \in \mathcal{B}$.
   - If $(Q_1 \parallel_L Q_2) \setminus \mathcal{A}_\mathcal{H} \stackrel{\tau}{\longrightarrow}_{\rm a} (Q_1 \parallel_L Q_2') \setminus \mathcal{A}_\mathcal{H}$ with $Q_2 \stackrel{\tau}{\longrightarrow}_{\rm a} Q_2'$, then the proof is similar to the one of the previous case.

   As for rates, we reason like in the proof of the corresponding result for $\approx_{\rm mw}$. ∎

Theorem 10.2. *Let* $P, P_1, P_2 \in \mathbb{P}_{\rm mk}$, $\approx \in \{\approx_{\rm mw}, \approx_{\rm mb}\}$, *and* $\mathcal{P} \in \{{\rm SBSNNI}_\approx, {\rm P\_BNDC}_\approx, {\rm SBNDC}_\approx\}$. *Then:*

1. $P \in \mathcal{P} \Longrightarrow a \,.\, P \in \mathcal{P}$ *for all* $a \in \mathcal{A}_\mathcal{L} \cup \{\tau\}$.
2. $P \in \mathcal{P} \Longrightarrow (\lambda) \,.\, P \in \mathcal{P}$ *for all* $\lambda \in \mathbb{R}_{>0}$.
3. $P_1, P_2 \in \mathcal{P} \Longrightarrow P_1 \parallel_L P_2 \in \mathcal{P}$ *for all* $L \subseteq \mathcal{A}_\mathcal{L}$ *if* $\mathcal{P} \in \{{\rm SBSNNI}_{\approx_{\rm mb}}, {\rm P\_BNDC}_{\approx_{\rm mb}}\}$ *or for all* $L \subseteq \mathcal{A} \setminus \{\tau\}$ *if* $\mathcal{P} \in \{{\rm SBSNNI}_{\approx_{\rm mw}}, {\rm P\_BNDC}_{\approx_{\rm mw}}, {\rm SBNDC}_{\approx_{\rm mw}}, {\rm SBNDC}_{\approx_{\rm mb}}\}$.
4. $P \in \mathcal{P} \Longrightarrow P \setminus L \in \mathcal{P}$ *for all* $L \subseteq \mathcal{A} \setminus \{\tau\}$.
5. $P \in \mathcal{P} \Longrightarrow P \,/\, L \in \mathcal{P}$ *for all* $L \subseteq \mathcal{A}_\mathcal{L}$.

Proof. We first prove the five results for $\text{SBSNNI}_\approx$, from which it will follow that they hold for $\text{P\_BNDC}_\approx$ too by virtue of the forthcoming Theorem 10.3:

1. Given an arbitrary $P \in \text{SBSNNI}_\approx$ and an arbitrary $a \in \mathcal{A}_\mathcal{L} \cup \{\tau\}$, from $P \setminus \mathcal{A}_\mathcal{H} \approx P / \mathcal{A}_\mathcal{H}$ we derive that $a \,.\, (P \setminus \mathcal{A}_\mathcal{H}) \approx a \,.\, (P / \mathcal{A}_\mathcal{H})$ because $\approx$ is a congruence with respect to action prefix by virtue of Lemma 10.1(1), from which it follows that $(a \,.\, P) \setminus \mathcal{A}_\mathcal{H} \approx (a \,.\, P) / \mathcal{A}_\mathcal{H}$, i.e., $a \,.\, P \in \text{BSNNI}_\approx$, because $a \notin \mathcal{A}_\mathcal{H}$. To conclude the proof, it suffices to observe that all the processes reachable from $a \,.\, P$ after performing a are processes reachable from P, which are known to be $\text{BSNNI}_\approx$.

2. Given an arbitrary $P \in \text{SBSNNI}_\approx$ and an arbitrary $\lambda \in \mathbb{R}_{>0}$, from $P \setminus \mathcal{A}_\mathcal{H} \approx P / \mathcal{A}_\mathcal{H}$ we derive that $(\lambda) \,.\, (P \setminus \mathcal{A}_\mathcal{H}) \approx (\lambda) \,.\, (P / \mathcal{A}_\mathcal{H})$ because $\approx$ is a congruence with respect to rate prefix by virtue of Lemma 10.1(2), from which it follows that $((\lambda) \,.\, P) \setminus \mathcal{A}_\mathcal{H} \approx ((\lambda) \,.\, P) / \mathcal{A}_\mathcal{H}$, i.e., $(\lambda) \,.\, P \in \text{BSNNI}_\approx$, because the restriction and hiding operators do not apply to rates. To conclude the proof, it suffices to observe that all the processes reachable from $(\lambda) \,.\, P$ after a delay governed by λ has elapsed are processes reachable from P, which are known to be $\text{BSNNI}_\approx$.

3. Given two arbitrary $P_1, P_2 \in \mathbb{P}_\text{mk}$ such that $P_1, P_2 \in \text{SBSNNI}_\approx$ and an arbitrary $L \subseteq \mathcal{A}_\mathcal{L}$, the result follows from Lemma 10.2(1) by taking Q_1 identical to R_1 and Q_2 identical to R_2.

4. Given an arbitrary $P \in \text{SBSNNI}_\approx$ and an arbitrary $L \subseteq \mathcal{A} \setminus \{\tau\}$, the result follows from Lemma 10.2(2) by taking Q identical to R – which will be denoted by P' – because:

   - $(P' \setminus L) \setminus \mathcal{A}_\mathcal{H} \approx (P' \setminus \mathcal{A}_\mathcal{H}) \setminus L$ as the order in which restriction sets are considered is unimportant.
   - $(P' \setminus \mathcal{A}_\mathcal{H}) \setminus L \approx (P' / \mathcal{A}_\mathcal{H}) \setminus L$ because $P' \setminus \mathcal{A}_\mathcal{H} \approx P' / \mathcal{A}_\mathcal{H}$ – as $P \in \text{SBSNNI}_\approx$ and $P' \in \mathit{reach}(P)$ – and $\approx$ is a congruence with respect to the restriction operator due to Lemma 10.1(4).
   - $(P' / \mathcal{A}_\mathcal{H}) \setminus L \approx (P' \setminus L) / \mathcal{A}_\mathcal{H}$ as shown in Lemma 10.2(2).
   - From the transitivity of $\approx$ we obtain that $(P' \setminus L) \setminus \mathcal{A}_\mathcal{H} \approx (P' \setminus L) / \mathcal{A}_\mathcal{H}$.

5. Given an arbitrary $P \in \text{SBSNNI}_\approx$ and an arbitrary $L \subseteq \mathcal{A}_\mathcal{L}$, for every $P' \in \mathit{reach}(P)$ it holds that $P' \setminus \mathcal{A}_\mathcal{H} \approx P' / \mathcal{A}_\mathcal{H}$, from which we derive that $(P' \setminus \mathcal{A}_\mathcal{H}) / L \approx (P' / \mathcal{A}_\mathcal{H}) / L$ because $\approx$ is a congruence with respect to the hiding operator due to Lemma 10.1(5). Since $L \cap \mathcal{A}_\mathcal{H} = \emptyset$, we have that $(P' \setminus \mathcal{A}_\mathcal{H}) / L$ is isomorphic to $(P' / L) \setminus \mathcal{A}_\mathcal{H}$ and $(P' / \mathcal{A}_\mathcal{H}) / L$ is isomorphic to $(P' / L) / \mathcal{A}_\mathcal{H}$, hence $(P' / L) \setminus \mathcal{A}_\mathcal{H} \approx (P' / L) / \mathcal{A}_\mathcal{H}$, i.e., P' / L is $\text{BSNNI}_\approx$.

We then prove the five results for $\text{SBNDC}_\approx$:

1. Given an arbitrary $P \in \text{SBNDC}_\approx$ and an arbitrary $a \in \mathcal{A}_\mathcal{L} \cup \{\tau\}$, it trivially holds that $a \,.\, P \in \text{SBNDC}_\approx$ because a is not high and all the processes reachable from $a \,.\, P$ after performing a are processes reachable from P, which is known to be $\text{SBNDC}_\approx$.

2. Given an arbitrary $P \in \text{SBNDC}_\approx$ and an arbitrary $\lambda \in \mathbb{R}_{>0}$, it trivially holds that $(\lambda) \,.\, P \in \text{SBNDC}_\approx$ because all the processes reachable from $(\lambda) \,.\, P$ after a delay governed by λ has elapsed are processes reachable from P, which is known to be $\text{SBNDC}_\approx$.

3. Given two arbitrary $P_1, P_2 \in \mathbb{P}_{\rm mk}$ such that $P_1, P_2 \in {\rm SBNDC}_\approx$ and an arbitrary $L \subseteq \mathcal{A} \setminus \{\tau\}$, the result follows from Lemma 10.2(3) as can be seen by observing that whenever $P_1' \parallel_L P_2' \xrightarrow{h}_{\rm a} P_1'' \parallel_L P_2''$ for $P_1' \parallel_L P_2' \in \mathit{reach}(P_1 \parallel_L P_2)$:

   - If $P_1' \xrightarrow{h}_{\rm a} P_1''$, $P_2'' = P_2'$ (hence $P_2' \setminus \mathcal{A}_\mathcal{H} \approx P_2'' \setminus \mathcal{A}_\mathcal{H}$), and $h \notin L$, then from $P_1 \in {\rm SBNDC}_\approx$ it follows that $P_1' \setminus \mathcal{A}_\mathcal{H} \approx P_1'' \setminus \mathcal{A}_\mathcal{H}$, which in turn entails that $(P_1' \parallel_L P_2') \setminus \mathcal{A}_\mathcal{H} \approx (P_1'' \parallel_L P_2'') \setminus \mathcal{A}_\mathcal{H}$ because $\approx$ is a congruence with respect to the parallel composition operator due to Lemma 10.1(3) and restriction distributes over parallel composition.
   - If $P_2' \xrightarrow{h}_{\rm a} P_2''$, $P_1'' = P_1'$, and $h \notin L$, then we reason like in the previous case.
   - If $P_1' \xrightarrow{h}_{\rm a} P_1''$, $P_2' \xrightarrow{h}_{\rm a} P_2''$, and $h \in L$, then from $P_1, P_2 \in {\rm SBNDC}_\approx$ it follows that $P_1' \setminus \mathcal{A}_\mathcal{H} \approx P_1'' \setminus \mathcal{A}_\mathcal{H}$ and $P_2' \setminus \mathcal{A}_\mathcal{H} \approx P_2'' \setminus \mathcal{A}_\mathcal{H}$, which in turn entail that $(P_1' \parallel_L P_2') \setminus \mathcal{A}_\mathcal{H} \approx (P_1'' \parallel_L P_2'') \setminus \mathcal{A}_\mathcal{H}$ because $\approx$ is a congruence with respect to the parallel composition operator due to Lemma 10.1(3) and restriction distributes over parallel composition.

4. Given an arbitrary $P \in {\rm SBNDC}_\approx$ and an arbitrary $L \subseteq \mathcal{A} \setminus \{\tau\}$, for every $P' \in \mathit{reach}(P)$ and for every P'' such that $P' \xrightarrow{h}_{\rm a} P''$ it holds that $P' \setminus \mathcal{A}_\mathcal{H} \approx P'' \setminus \mathcal{A}_\mathcal{H}$, from which we derive that $(P' \setminus \mathcal{A}_\mathcal{H}) \setminus L \approx (P'' \setminus \mathcal{A}_\mathcal{H}) \setminus L$ because $\approx$ is a congruence with respect to the restriction operator due to Lemma 10.1(4). Since $(P' \setminus \mathcal{A}_\mathcal{H}) \setminus L$ is isomorphic to $(P' \setminus L) \setminus \mathcal{A}_\mathcal{H}$ and $(P'' \setminus \mathcal{A}_\mathcal{H}) \setminus L$ is isomorphic to $(P'' \setminus L) \setminus \mathcal{A}_\mathcal{H}$, we have that $(P' \setminus L) \setminus \mathcal{A}_\mathcal{H} \approx (P'' \setminus L) \setminus \mathcal{A}_\mathcal{H}$.

5. Given an arbitrary $P \in {\rm SBNDC}_\approx$ and an arbitrary $L \subseteq \mathcal{A}_\mathcal{L}$, for every $P' \in \mathit{reach}(P)$ and for every P'' such that $P' \xrightarrow{h}_{\rm a} P''$ it holds that $P' \setminus \mathcal{A}_\mathcal{H} \approx P'' \setminus \mathcal{A}_\mathcal{H}$, from which we derive that $(P' \setminus \mathcal{A}_\mathcal{H}) / L \approx (P'' \setminus \mathcal{A}_\mathcal{H}) / L$ because $\approx$ is a congruence with respect to the hiding operator due to Lemma 10.1(5). Since $L \cap \mathcal{A}_\mathcal{H} = \emptyset$, we have that $(P' \setminus \mathcal{A}_\mathcal{H}) / L$ is isomorphic to $(P' / L) \setminus \mathcal{A}_\mathcal{H}$ and $(P'' \setminus \mathcal{A}_\mathcal{H}) / L$ is isomorphic to $(P'' / L) \setminus \mathcal{A}_\mathcal{H}$, hence $(P' / L) \setminus \mathcal{A}_\mathcal{H} \approx (P'' / L) \setminus \mathcal{A}_\mathcal{H}$. ■

As far as parallel composition is concerned, the compositionality of ${\rm SBSNNI}_{\approx_{\rm mb}}$ holds only for all $L \subseteq \mathcal{A}_\mathcal{L}$. For example, like in the nondeterministic setting (see after Theorem 8.3), both $P_1 = h \,.\, \underline{0} + l_1 \,.\, \underline{0} + \tau \,.\, \underline{0}$ and $P_2 = h \,.\, \underline{0} + l_2 \,.\, \underline{0} + \tau \,.\, \underline{0}$ are ${\rm SBSNNI}_{\approx_{\rm mb}}$, but $P_1 \parallel_{\{h\}} P_2$ is not. Similar to the two previous chapters, it is not only a matter of the higher discriminating power of $\approx_{\rm mb}$ with respect to $\approx_{\rm mw}$, but also of the specific parallel composition operator that we have adopted, which does not mix synchronization with hiding.

10.2.2 Taxonomy of Security Properties

Similar to the nondeterministic and probabilistic settings of the two previous chapters, the noninterference properties in Definition 10.5 turn out to be increasingly finer. This holds both for those based on $\approx_{\rm mw}$ and for those based on $\approx_{\rm mb}$.

Part of the proof of the forthcoming Theorem 10.3 relies on the bisimulation-up-to technique [131] and requires introducing Markovian variants of up-to weak [112] and branching [75] bisimulations. Similar to the probabilistic setting of the previous chapter, we have to take into account some technicalities mentioned in [44, 91, 79]. In particular, given $\approx \in \{\approx_{\rm mw}, \approx_{\rm mb}\}$ and a related bisimulation $\mathcal{B}$, we cannot consider the relation composition $\approx \mathcal{B} \approx$

like in the fully nondeterministic case as it may not be transitive and this would not make it possible to work with equivalence classes for the Markovian part. Rather we have to consider $(\mathcal{B} \cup \mathcal{B}^{-1} \cup \approx)^+ = \bigcup_{n=1}^{\infty} (\mathcal{B} \cup \mathcal{B}^{-1} \cup \approx)^n$ to ensure transitivity in addition to reflexivity and symmetry, where $\mathcal{B}^{-1}$ is the inverse of $\mathcal{B}$ and $\mathcal{B}$ is no longer required to be an equivalence relation thus avoiding redundant information in it. We remind that $(\mathcal{B} \cup \mathcal{B}^{-1} \cup \approx)^n$ for $n > 1$ is the composition of relations $(\mathcal{B} \cup \mathcal{B}^{-1} \cup \approx)^{n-1}$ and $\mathcal{B} \cup \mathcal{B}^{-1} \cup \approx$.

Definition 10.6. *A relation $\mathcal{B}$ over $\mathbb{P}_{\rm mk}$ is a* weak Markovian bisimulation up to $\approx_{\rm mw}$ *iff, whenever $(P_1, P_2) \in \mathcal{B}$, then:*

- *For each $P_1 \stackrel{a}{\Longrightarrow}_{\rm a} P_1'$ there exists $P_2 \stackrel{\hat{a}}{\Longrightarrow}_{\rm a} P_2'$ such that $(P_1', P_2') \in (\mathcal{B} \cup \mathcal{B}^{-1} \cup \approx_{\rm mw})^+$, and vice versa.*
- *If $P_1 \stackrel{\tau}{\not\longrightarrow}_{\rm a}$ then there exists $P_2 \stackrel{\tau^*}{\Longrightarrow}_{\rm a} \bar{P}_2$ such that $\bar{P}_2 \stackrel{\tau}{\not\longrightarrow}_{\rm a}$, $(P_1, \bar{P}_2) \in (\mathcal{B} \cup \mathcal{B}^{-1} \cup \approx_{\rm mw})^+$, and $rate(P_1, C) = rate(\bar{P}_2, C)$ for all equivalence classes $C \in \mathbb{P}_{\rm mk}/(\mathcal{B} \cup \mathcal{B}^{-1} \cup \approx_{\rm mw})^+$, and vice versa.* ∎

Definition 10.7. *A relation $\mathcal{B}$ over $\mathbb{P}_{\rm mk}$ is a* Markovian branching bisimulation up to $\approx_{\rm mb}$ *iff, whenever $(P_1, P_2) \in \mathcal{B}$, then:*

- *For each $P_1 \stackrel{\tau^*}{\Longrightarrow}_{\rm a} \bar{P}_1 \stackrel{a}{\longrightarrow}_{\rm a} P_1'$ with $P_1 \approx_{\rm mb} \bar{P}_1$:*
  - *either $a = \tau$ and $\bar{P}_1 \approx_{\rm mb} P_1'$;*
  - *or there exists $P_2 \stackrel{\tau^*}{\Longrightarrow}_{\rm a} \bar{P}_2 \stackrel{a}{\longrightarrow}_{\rm a} P_2'$ such that $(\bar{P}_1, \bar{P}_2) \in (\mathcal{B} \cup \mathcal{B}^{-1} \cup \approx_{\rm mb})^+$ and $(P_1', P_2') \in (\mathcal{B} \cup \mathcal{B}^{-1} \cup \approx_{\rm mb})^+$;*

  and vice versa.
- *If $P_1 \stackrel{\tau}{\not\longrightarrow}_{\rm a}$ then there exists $P_2 \stackrel{\tau^*}{\Longrightarrow}_{\rm a} \bar{P}_2$ such that $\bar{P}_2 \stackrel{\tau}{\not\longrightarrow}_{\rm a}$, $(P_1, \bar{P}_2) \in (\mathcal{B} \cup \mathcal{B}^{-1} \cup \approx_{\rm mb})^+$, and $rate(P_1, C) = rate(\bar{P}_2, C)$ for all equivalence classes $C \in \mathbb{P}_{\rm mk}/(\mathcal{B} \cup \mathcal{B}^{-1} \cup \approx_{\rm mb})^+$, and vice versa.* ∎

It is worth noting that a weak Markovian bisimulation up to $\approx_{\rm mw}$ is also present in [90], but its definition is different from the first definition above. In the second definition, in the case that $a = \tau$ and $\bar{P}_1 \approx_{\rm mb} P_1'$ it holds that $P_1' \approx_{\rm mb} \bar{P}_1 \approx_{\rm mb} P_1$ $\mathcal{B}$ P_2, i.e., $(P_1', P_2) \in (\mathcal{B} \cup \mathcal{B}^{-1} \cup \approx_{\rm mb})^+$, because $\approx_{\rm mb}$ is symmetric. We now prove that the two previous notions are correct, i.e., they imply the respective bisimilarities.

Proposition 10.1. *Let $P_1, P_2 \in \mathbb{P}_{\rm mk}$ and $\mathcal{B}$ be a weak Markovian bisimulation up to $\approx_{\rm mw}$. If $(P_1, P_2) \in \mathcal{B}$ then $P_1 \approx_{\rm mw} P_2$.*

Proof. It suffices to prove that the equivalence relation $(\mathcal{B}' \cup \approx_{\rm mw})^+$ is a weak Markovian bisimulation, where $\mathcal{B}' = \mathcal{B} \cup \mathcal{B}^{-1}$. Given $(P_1, P_2) \in (\mathcal{B}' \cup \approx_{\rm mw})^+$ and considering the smallest $n \in \mathbb{N}_{>0}$ for which $(P_1, P_2) \in (\mathcal{B}' \cup \approx_{\rm mw})^n$, we proceed by induction on n:

- If $n = 1$ then there are two cases:
  - Let $(P_1, P_2) \in \mathcal{B}'$. If $P_1 \stackrel{a}{\longrightarrow}_{\rm a} P_1'$, hence $P_1 \stackrel{a}{\Longrightarrow}_{\rm a} P_1'$, then from the fact that $\mathcal{B}'$ is a weak Markovian bisimulation up to $\approx_{\rm mw}$ it follows that there exists $P_2 \stackrel{\hat{a}}{\Longrightarrow}_{\rm a} P_2'$ such that $(P_1', P_2') \in (\mathcal{B}' \cup \approx_{\rm mw})^+$. Moreover, since $\mathcal{B}'$ is a weak Markovian bisimulation up to $\approx_{\rm mw}$, we have that if $P_1 \stackrel{\tau}{\not\longrightarrow}_{\rm a}$ then there exists $P_2 \stackrel{\tau^*}{\Longrightarrow}_{\rm a} \bar{P}_2$ such that $\bar{P}_2 \stackrel{\tau}{\not\longrightarrow}_{\rm a}$, $(P_1, \bar{P}_2) \in (\mathcal{B}' \cup \approx_{\rm mw})^+$, and $rate(P_1, C) = rate(\bar{P}_2, C)$ for all $C \in \mathbb{P}_{\rm mk}/(\mathcal{B}' \cup \approx_{\rm mw})^+$.

  - Let $P_1 \approx_{\rm mw} P_2$. If $P_1 \stackrel{a}{\longrightarrow}_{\rm a} P_1'$ then there exists $P_2 \stackrel{\hat{a}}{\Longrightarrow}_{\rm a} P_2'$ such that $P_1' \approx_{\rm mw} P_2'$, hence $(P_1', P_2') \in (\mathcal{B}' \cup \approx_{\rm mw})^+$ because $\approx_{\rm mw} \subseteq (\mathcal{B}' \cup \approx_{\rm mw})^+$. Moreover, since $\approx_{\rm mw} \subseteq (\mathcal{B}' \cup \approx_{\rm mw})^+$ implies that every equivalence class of $(\mathcal{B}' \cup \approx_{\rm mw})^+$ is the union of some equivalence classes of $\approx_{\rm mw}$, we have that if $P_1 \stackrel{\tau}{\not\longrightarrow}_{\rm a}$ then there exists $P_2 \stackrel{\tau^*}{\Longrightarrow}_{\rm a} \bar{P}_2$ such that $\bar{P}_2 \stackrel{\tau}{\not\longrightarrow}_{\rm a}$, $P_1 \approx_{\rm mw} \bar{P}_2$, hence $(P_1, \bar{P}_2) \in (\mathcal{B}' \cup \approx_{\rm mw})^+$, and $rate(P_1, C) = rate(\bar{P}_2, C)$ for all $C \in \mathbb{P}_{\rm mk}/(\mathcal{B}' \cup \approx_{\rm mw})^+$.

- If $n > 1$ then from $(P_1, P_2) \in (\mathcal{B}' \cup \approx_{\rm mw})^n$ and the minimality of n it follows that there exists $P \in \mathbb{P}_{\rm mk}$ such that $(P_1, P) \in (\mathcal{B}' \cup \approx_{\rm mw})^{n-1}$ and $(P, P_2) \in (\mathcal{B}' \cup \approx_{\rm mw})$. If $P_1 \stackrel{a}{\longrightarrow}_{\rm a} P_1'$ then by the induction hypothesis applied to $(P_1, P) \in (\mathcal{B}' \cup \approx_{\rm mw})^{n-1}$ there exists $P \stackrel{\hat{a}}{\Longrightarrow}_{\rm a} P'$ such that $(P_1', P') \in (\mathcal{B}' \cup \approx_{\rm mw})^+$. Therefore by the induction hypothesis applied to $(P, P_2) \in (\mathcal{B}' \cup \approx_{\rm mw})$ there exists $P_2 \stackrel{\hat{a}}{\Longrightarrow}_{\rm a} P_2'$ such that $(P', P_2') \in (\mathcal{B}' \cup \approx_{\rm mw})^+$, where $(P_1', P_2') \in (\mathcal{B}' \cup \approx_{\rm mw})^+$ by transitivity. Moreover, by the induction hypothesis applied to $(P_1, P) \in (\mathcal{B}' \cup \approx_{\rm mw})^{n-1}$, if $P_1 \stackrel{\tau}{\not\longrightarrow}_{\rm a}$ then there exists $P \stackrel{\tau^*}{\Longrightarrow}_{\rm a} \bar{P}$ such that $\bar{P} \stackrel{\tau}{\not\longrightarrow}_{\rm a}$, $(P_1, \bar{P}) \in (\mathcal{B}' \cup \approx_{\rm mw})^+$, and $rate(P_1, C) = rate(\bar{P}, C)$ for all $C \in \mathbb{P}_{\rm mk}/(\mathcal{B}' \cup \approx_{\rm mw})^+$. Therefore, by the induction hypothesis applied to $(P, P_2) \in (\mathcal{B}' \cup \approx_{\rm mw})$, from $P \stackrel{\tau^*}{\Longrightarrow}_{\rm a} \bar{P}$ with $\bar{P} \stackrel{\tau}{\not\longrightarrow}_{\rm a}$ it follows that there exists $P_2 \stackrel{\tau^*}{\Longrightarrow}_{\rm a} \bar{P}_2$ such that $\bar{P}_2 \stackrel{\tau}{\not\longrightarrow}_{\rm a}$, $(\bar{P}, \bar{P}_2) \in (\mathcal{B}' \cup \approx_{\rm mw})^+$, and $rate(\bar{P}, C) = rate(\bar{P}_2, C)$ for all $C \in \mathbb{P}_{\rm mk}/(\mathcal{B}' \cup \approx_{\rm mw})^+$. Thus $rate(P_1, C) = rate(\bar{P}_2, C)$ for all $C \in \mathbb{P}_{\rm mk}/(\mathcal{B}' \cup \approx_{\rm mw})^+$, where $(P_1, \bar{P}_2) \in (\mathcal{B}' \cup \approx_{\rm mw})^+$ by transitivity. ∎

Proposition 10.2. *Let $P_1, P_2 \in \mathbb{P}_{\rm mk}$ and $\mathcal{B}$ be a Markovian branching bisimulation up to $\approx_{\rm mb}$. If $(P_1, P_2) \in \mathcal{B}$ then $P_1 \approx_{\rm mb} P_2$.*

Proof. It suffices to prove that the equivalence relation $(\mathcal{B}' \cup \approx_{\rm mb})^+$ is a Markovian branching bisimulation, where $\mathcal{B}' = \mathcal{B} \cup \mathcal{B}^{-1}$. Given $(P_1, P_2) \in (\mathcal{B}' \cup \approx_{\rm mb})^+$ and considering the smallest $n \in \mathbb{N}_{>0}$ for which $(P_1, P_2) \in (\mathcal{B}' \cup \approx_{\rm mb})^n$, we proceed by induction on n:

- If $n = 1$ then there are two cases:

  - Let $(P_1, P_2) \in \mathcal{B}'$. If $P_1 \stackrel{a}{\longrightarrow}_{\rm a} P_1'$, hence $P_1 \stackrel{\tau^*}{\Longrightarrow}_{\rm a} P_1 \stackrel{a}{\longrightarrow}_{\rm a} P_1'$, then from the fact that $\mathcal{B}'$ is a Markovian branching bisimulation up to $\approx_{\rm mb}$ it follows that there are two subcases:
    * If $a = \tau$ and $P_1 \approx_{\rm mb} P_1'$, hence $(P_1', P_1) \in (\mathcal{B}' \cup \approx_{\rm mb})^+$ by symmetry, from $(P_1, P_2) \in (\mathcal{B}' \cup \approx_{\rm mb})^+$ it follows that $(P_1', P_2) \in (\mathcal{B}' \cup \approx_{\rm mb})^+$ by transitivity.
    * If there exists $P_2 \stackrel{\tau^*}{\Longrightarrow}_{\rm a} \bar{P}_2 \stackrel{a}{\longrightarrow}_{\rm a} P_2'$ such that $(P_1, \bar{P}_2) \in (\mathcal{B}' \cup \approx_{\rm mb})^+$ and $(P_1', P_2') \in (\mathcal{B}' \cup \approx_{\rm mb})^+$, then we are done.

    Moreover, since $\mathcal{B}'$ is a Markovian branching bisimulation up to $\approx_{\rm mb}$, we have that if $P_1 \stackrel{\tau}{\not\longrightarrow}_{\rm a}$ then there exists $P_2 \stackrel{\tau^*}{\Longrightarrow}_{\rm a} \bar{P}_2$ such that $\bar{P}_2 \stackrel{\tau}{\not\longrightarrow}_{\rm a}$, $(P_1, \bar{P}_2) \in (\mathcal{B}' \cup \approx_{\rm mb})^+$, and $rate(P_1, C) = rate(\bar{P}_2, C)$ for all $C \in \mathbb{P}_{\rm mk}/(\mathcal{B}' \cup \approx_{\rm mb})^+$.
  - Let $P_1 \approx_{\rm mb} P_2$. If $P_1 \stackrel{a}{\longrightarrow}_{\rm a} P_1'$ then there are two subcases:
    * If $a = \tau$ and $P_1' \approx_{\rm mb} P_2$, then $(P_1', P_2) \in (\mathcal{B}' \cup \approx_{\rm mb})^+$ because $\approx_{\rm mb} \subseteq (\mathcal{B}' \cup \approx_{\rm mb})^+$.
    * If there exists $P_2 \stackrel{\tau^*}{\Longrightarrow}_{\rm a} \bar{P}_2 \stackrel{a}{\longrightarrow}_{\rm a} P_2'$ such that $P_1 \approx_{\rm mb} \bar{P}_2$ and $P_1' \approx_{\rm mb} P_2'$, then $(P_1, \bar{P}_2) \in (\mathcal{B}' \cup \approx_{\rm mb})^+$ and $(P_1', P_2') \in (\mathcal{B}' \cup \approx_{\rm mb})^+$ because $\approx_{\rm mb} \subseteq (\mathcal{B}' \cup \approx_{\rm mb})^+$.

Moreover, since $\approx_{\rm mb} \subseteq (\mathcal{B}' \cup \approx_{\rm mb})^+$ implies that every equivalence class of $(\mathcal{B}' \cup \approx_{\rm mb})^+$ is the union of some equivalence classes of $\approx_{\rm mb}$, we have that if $P_1 \stackrel{\tau}{\not\longrightarrow}_{\rm a}$ then there exists $P_2 \stackrel{\tau^*}{\Longrightarrow}_{\rm a} \bar{P}_2$ such that $\bar{P}_2 \stackrel{\tau}{\not\longrightarrow}_{\rm a}$, $P_1 \approx_{\rm mb} \bar{P}_2$, hence $(P_1, \bar{P}_2) \in (\mathcal{B}' \cup \approx_{\rm mb})^+$, and $rate(P_1, C) = rate(\bar{P}_2, C)$ for all $C \in \mathbb{P}_{\rm mk}/(\mathcal{B}' \cup \approx_{\rm mb})^+$.

- If $n > 1$ then from $(P_1, P_2) \in (\mathcal{B}' \cup \approx_{\rm mb})^n$ and the minimality of n it follows that there exists $P \in \mathbb{P}_{\rm mk}$ such that $(P_1, P) \in (\mathcal{B}' \cup \approx_{\rm mb})^{n-1}$ and $(P, P_2) \in (\mathcal{B}' \cup \approx_{\rm mb})$. If $P_1 \stackrel{a}{\longrightarrow}_{\rm a} P_1'$ then by the induction hypothesis applied to $(P_1, P) \in (\mathcal{B}' \cup \approx_{\rm mb})^{n-1}$ there are two cases:
  - If $a = \tau$ and $(P_1', P) \in (\mathcal{B}' \cup \approx_{\rm mb})^+$, then from $(P, P_2) \in (\mathcal{B}' \cup \approx_{\rm mb})$ it follows that $(P_1', P_2) \in (\mathcal{B}' \cup \approx_{\rm mb})^+$ by transitivity.
  - If there exists $P \stackrel{\tau^*}{\Longrightarrow}_{\rm a} \bar{P} \stackrel{a}{\longrightarrow}_{\rm a} P'$ such that $(P_1, \bar{P}) \in (\mathcal{B}' \cup \approx_{\rm mb})^+$ and $(P_1', P') \in (\mathcal{B}' \cup \approx_{\rm mb})^+$, then by the induction hypothesis applied to $(P, P_2) \in (\mathcal{B}' \cup \approx_{\rm mb})$ there are two subcases:
    * If $a = \tau$ and $(P', P_2) \in (\mathcal{B}' \cup \approx_{\rm mb})^+$, then from $(P_1', P') \in (\mathcal{B}' \cup \approx_{\rm mb})^+$ it follows that $(P_1', P_2) \in (\mathcal{B}' \cup \approx_{\rm mb})^+$ by transitivity.
    * If there exists $P_2 \stackrel{\tau^*}{\Longrightarrow}_{\rm a} \bar{P}_2 \stackrel{a}{\longrightarrow}_{\rm a} P_2'$ such that $(\bar{P}, \bar{P}_2) \in (\mathcal{B}' \cup \approx_{\rm mb})^+$ and $(P', P_2') \in (\mathcal{B}' \cup \approx_{\rm mb})^+$, then from $(P_1, \bar{P}) \in (\mathcal{B}' \cup \approx_{\rm mb})^+$ and $(P_1', P') \in (\mathcal{B}' \cup \approx_{\rm mb})^+$ it follows that $(P_1, \bar{P}_2) \in (\mathcal{B}' \cup \approx_{\rm mb})^+$ and $(P_1', P_2') \in (\mathcal{B}' \cup \approx_{\rm mb})^+$ by transitivity.

  Moreover, by the induction hypothesis applied to $(P_1, P) \in (\mathcal{B}' \cup \approx_{\rm mb})^{n-1}$, if $P_1 \stackrel{\tau}{\not\longrightarrow}_{\rm a}$ then there exists $P \stackrel{\tau^*}{\Longrightarrow}_{\rm a} \bar{P}$ such that $\bar{P} \stackrel{\tau}{\not\longrightarrow}_{\rm a}$, $(P_1, \bar{P}) \in (\mathcal{B}' \cup \approx_{\rm mb})^+$, and $rate(P_1, C) = rate(\bar{P}, C)$ for all $C \in \mathbb{P}_{\rm mk}/(\mathcal{B}' \cup \approx_{\rm mb})^+$. Therefore, by the induction hypothesis applied to $(P, P_2) \in (\mathcal{B}' \cup \approx_{\rm mb})$, from $P \stackrel{\tau^*}{\Longrightarrow}_{\rm a} \bar{P}$ with $\bar{P} \stackrel{\tau}{\not\longrightarrow}_{\rm a}$ it follows that there exists $P_2 \stackrel{\tau^*}{\Longrightarrow}_{\rm a} \bar{P}_2$ such that $\bar{P}_2 \stackrel{\tau}{\not\longrightarrow}_{\rm a}$, $(\bar{P}, \bar{P}_2) \in (\mathcal{B}' \cup \approx_{\rm mb})^+$, and $rate(\bar{P}, C) = rate(\bar{P}_2, C)$ for all $C \in \mathbb{P}_{\rm mk}/(\mathcal{B}' \cup \approx_{\rm mb})^+$. Thus $rate(P_1, C) = rate(\bar{P}_2, C)$ for all $C \in \mathbb{P}_{\rm mk}/(\mathcal{B}' \cup \approx_{\rm mb})^+$, where $(P_1, \bar{P}_2) \in (\mathcal{B}' \cup \approx_{\rm mb})^+$ by transitivity. ∎

The combination of divergence, i.e., cycles of τ-transitions, and maximal progress poses a challenge in obtaining a taxonomy similar to the ones of the nondeterministic and probabilistic settings. To see why, consider the recursive process $K \triangleq (\lambda)\,.\,\underline{0} + h\,.\,K$. This process is not BSNNI$_\approx$ because its low-level views $K \setminus \{h\}$, which is isomorphic to $(\lambda)\,.\,\underline{0}$, and $K / \{h\}$, which is isomorphic to $K' \triangleq (\lambda)\,.\,\underline{0} + \tau\,.\,K'$, are not $\approx$-equivalent as the former enables a λ-transition while the latter, due to maximal progress, is forced to endlessly loop on the τ-transition without ever allowing a delay governed by λ to elapse. Likewise, it can be shown that K is not BNDC$_\approx$, SBSNNI$_\approx$, or P_BNDC$_\approx$. However, it is SBNDC$_\approx$ due to the fact that the only high action h loops on K and hence to satisfy SBNDC$_\approx$ we have to check whether $K \setminus \{h\} \approx K \setminus \{h\}$, which is trivially true. Further issues arise from the application of the hiding operator on high actions – which frequently occurs in information flow analysis – to cycles comprising τ-transitions and high action transitions, as this yields divergence. In order to derive a taxonomy aligned with the ones of the two previous chapters, we restrict ourselves to the set $\mathbb{P}_{\rm mk,nhc}$ of processes whose underlying MLTS has no cycles (i) involving high action transitions that are alternative to rate transitions or (ii) composed only of τ-transitions and high action transitions with at least one of the latter.

Before presenting the taxonomy, we prove some further ancillary results about parallel composition, restriction, and hiding under SBSNNI$_\approx$ and SBNDC$_\approx$, where the limitation to $\mathbb{P}_{\rm mk,nhc}$ is already needed.

Lemma 10.3. *Let $P, P_1, P_2 \in \mathbb{P}_{\rm mk}$ and $\approx \in \{\approx_{\rm mw}, \approx_{\rm mb}\}$. Then:*

1. *If $P \in {\rm SBNDC}_{\approx}$, $P' \in reach(P)$, and $P' \,/\, \mathcal{A}_{\mathcal{H}} \stackrel{\tau^*}{\Longrightarrow}_{\rm a} P'' \,/\, \mathcal{A}_{\mathcal{H}}$, then $P' \setminus \mathcal{A}_{\mathcal{H}} \stackrel{\tau^*}{\Longrightarrow}_{\rm a} \hat{P}'' \setminus \mathcal{A}_{\mathcal{H}}$ with $P'' \setminus \mathcal{A}_{\mathcal{H}} \approx \hat{P}'' \setminus \mathcal{A}_{\mathcal{H}}$.*
2. *If $P_1, P_2 \in {\rm SBNDC}_{\approx} \cap \mathbb{P}_{\rm mk,nhc}$ and $P_1 \setminus \mathcal{A}_{\mathcal{H}} \approx P_2 \setminus \mathcal{A}_{\mathcal{H}}$, then $P_1 \,/\, \mathcal{A}_{\mathcal{H}} \approx P_2 \,/\, \mathcal{A}_{\mathcal{H}}$.*
3. *If $P_2 \in {\rm SBSNNI}_{\approx}$ and $L \subseteq \mathcal{A}_{\mathcal{H}}$, then $P_1' \setminus \mathcal{A}_{\mathcal{H}} \approx ((P_2' \parallel_L Q) \,/\, L) \setminus \mathcal{A}_{\mathcal{H}}$ for all $Q \in \mathbb{P}_{\rm mk}$ having only prefixes in $\mathcal{A}_{\mathcal{H}}$ and for all $P_1' \in reach(P_1)$ and $P_2' \in reach(P_2)$ such that $P_1' \setminus \mathcal{A}_{\mathcal{H}} \approx P_2' \,/\, \mathcal{A}_{\mathcal{H}}$.*

Proof. We first prove the three results for the $\approx_{\rm mw}$-based properties:

1. We proceed by induction on the number $n \in \mathbb{N}$ of τ-transitions along $P' \,/\, \mathcal{A}_{\mathcal{H}} \stackrel{\tau^*}{\Longrightarrow}_{\rm a} P'' \,/\, \mathcal{A}_{\mathcal{H}}$:
   - If $n = 0$ then $P' \,/\, \mathcal{A}_{\mathcal{H}}$ stays idle and $P'' \,/\, \mathcal{A}_{\mathcal{H}}$ is $P' \,/\, \mathcal{A}_{\mathcal{H}}$. Likewise, $P' \setminus \mathcal{A}_{\mathcal{H}}$ can stay idle, i.e., $P' \setminus \mathcal{A}_{\mathcal{H}} \stackrel{\tau^*}{\Longrightarrow}_{\rm a} P' \setminus \mathcal{A}_{\mathcal{H}}$, with $P' \setminus \mathcal{A}_{\mathcal{H}} \approx_{\rm mw} P' \setminus \mathcal{A}_{\mathcal{H}}$ as $\approx_{\rm mw}$ is reflexive.
   - Let $n > 0$ and $P_0' \,/\, \mathcal{A}_{\mathcal{H}} \stackrel{\tau}{\longrightarrow}_{\rm a} P_1' \,/\, \mathcal{A}_{\mathcal{H}} \stackrel{\tau}{\longrightarrow}_{\rm a} \ldots \stackrel{\tau}{\longrightarrow}_{\rm a} P_{n-1}' \,/\, \mathcal{A}_{\mathcal{H}} \stackrel{\tau}{\longrightarrow}_{\rm a} P_n' \,/\, \mathcal{A}_{\mathcal{H}}$ where P_0' is P' and P_n' is P''. From the induction hypothesis it follows that $P' \setminus \mathcal{A}_{\mathcal{H}} \stackrel{\tau^*}{\Longrightarrow}_{\rm a} \hat{P}_{n-1}' \setminus \mathcal{A}_{\mathcal{H}}$ with $P_{n-1}' \setminus \mathcal{A}_{\mathcal{H}} \approx_{\rm mw} \hat{P}_{n-1}' \setminus \mathcal{A}_{\mathcal{H}}$. As far as the n-th τ-transition $P_{n-1}' \,/\, \mathcal{A}_{\mathcal{H}} \stackrel{\tau}{\longrightarrow} P_n' \,/\, \mathcal{A}_{\mathcal{H}}$ is concerned, there are two cases depending on whether it is originated from $P_{n-1}' \stackrel{\tau}{\longrightarrow}_{\rm a} P_n'$ or $P_{n-1}' \stackrel{h}{\longrightarrow}_{\rm a} P_n'$:
     - If $P_{n-1}' \stackrel{\tau}{\longrightarrow}_{\rm a} P_n'$ then $P_{n-1}' \setminus \mathcal{A}_{\mathcal{H}} \stackrel{\tau}{\longrightarrow}_{\rm a} P_n' \setminus \mathcal{A}_{\mathcal{H}}$. Since $P_{n-1}' \setminus \mathcal{A}_{\mathcal{H}} \approx_{\rm mw} \hat{P}_{n-1}' \setminus \mathcal{A}_{\mathcal{H}}$, there exists $\hat{P}_{n-1}' \setminus \mathcal{A}_{\mathcal{H}} \stackrel{\tau^*}{\Longrightarrow}_{\rm a} \hat{P}_n' \setminus \mathcal{A}_{\mathcal{H}}$ such that $P_n' \setminus \mathcal{A}_{\mathcal{H}} \approx_{\rm mw} \hat{P}_n' \setminus \mathcal{A}_{\mathcal{H}}$. Therefore $P' \setminus \mathcal{A}_{\mathcal{H}} \stackrel{\tau^*}{\Longrightarrow}_{\rm a} \hat{P}_n' \setminus \mathcal{A}_{\mathcal{H}}$ with $P'' \setminus \mathcal{A}_{\mathcal{H}} \approx_{\rm mw} \hat{P}_n' \setminus \mathcal{A}_{\mathcal{H}}$.
     - If $P_{n-1}' \stackrel{h}{\longrightarrow}_{\rm a} P_n'$ then from $P \in {\rm SBNDC}_{\approx_{\rm mw}}$ it follows that $P_{n-1}' \setminus \mathcal{A}_{\mathcal{H}} \approx_{\rm mw} P_n' \setminus \mathcal{A}_{\mathcal{H}}$. Since $P_{n-1}' \setminus \mathcal{A}_{\mathcal{H}} \approx_{\rm mw} \hat{P}_{n-1}' \setminus \mathcal{A}_{\mathcal{H}}$ and $\approx_{\rm mw}$ is symmetric and transitive, we obtain $P_n' \setminus \mathcal{A}_{\mathcal{H}} \approx_{\rm mw} \hat{P}_{n-1}' \setminus \mathcal{A}_{\mathcal{H}}$. Therefore $P' \setminus \mathcal{A}_{\mathcal{H}} \stackrel{\tau^*}{\Longrightarrow}_{\rm a} \hat{P}_{n-1}' \setminus \mathcal{A}_{\mathcal{H}}$ with $P'' \setminus \mathcal{A}_{\mathcal{H}} \approx_{\rm mw} \hat{P}_{n-1}' \setminus \mathcal{A}_{\mathcal{H}}$.
2. Let $\mathcal{B}$ be an equivalence relation containing all the pairs of processes that have to be shown to be $\approx_{\rm mw}$-equivalent according to the considered result. Starting from $(P_1 \,/\, \mathcal{A}_{\mathcal{H}}, P_2 \,/\, \mathcal{A}_{\mathcal{H}}) \in \mathcal{B}$, so that $P_1 \setminus \mathcal{A}_{\mathcal{H}} \approx_{\rm mw} P_2 \setminus \mathcal{A}_{\mathcal{H}}$, there are three cases for action transitions based on the operational semantic rules in Table 10.1:
   - If $P_1 \,/\, \mathcal{A}_{\mathcal{H}} \stackrel{\tau}{\longrightarrow}_{\rm a} P_1' \,/\, \mathcal{A}_{\mathcal{H}}$ with $P_1 \stackrel{h}{\longrightarrow}_{\rm a} P_1'$, then $P_1 \setminus \mathcal{A}_{\mathcal{H}} \approx_{\rm mw} P_1' \setminus \mathcal{A}_{\mathcal{H}}$ as $h \in \mathcal{A}_{\mathcal{H}}$ and $P_1 \in {\rm SBNDC}_{\approx_{\rm mw}}$. Since $P_1' \setminus \mathcal{A}_{\mathcal{H}} \approx_{\rm mw} P_2 \setminus \mathcal{A}_{\mathcal{H}}$, as $P_1 \setminus \mathcal{A}_{\mathcal{H}} \approx_{\rm mw} P_2 \setminus \mathcal{A}_{\mathcal{H}}$ and $\approx_{\rm mw}$ is symmetric and transitive, with $P_1', P_2 \in {\rm SBNDC}_{\approx_{\rm mw}}$, we have that $P_2 \,/\, \mathcal{A}_{\mathcal{H}}$ is allowed to stay idle with $(P_1' \,/\, \mathcal{A}_{\mathcal{H}}, P_2 \,/\, \mathcal{A}_{\mathcal{H}}) \in \mathcal{B}$.
   - If $P_1 \,/\, \mathcal{A}_{\mathcal{H}} \stackrel{l}{\longrightarrow}_{\rm a} P_1' \,/\, \mathcal{A}_{\mathcal{H}}$ with $P_1 \stackrel{l}{\longrightarrow}_{\rm a} P_1'$, then $P_1 \setminus \mathcal{A}_{\mathcal{H}} \stackrel{l}{\longrightarrow}_{\rm a} P_1' \setminus \mathcal{A}_{\mathcal{H}}$ as $l \notin \mathcal{A}_{\mathcal{H}}$. From $P_1 \setminus \mathcal{A}_{\mathcal{H}} \approx_{\rm mw} P_2 \setminus \mathcal{A}_{\mathcal{H}}$ it follows that there exists $P_2 \setminus \mathcal{A}_{\mathcal{H}} \stackrel{\hat{l}}{\Longrightarrow}_{\rm a} P_2' \setminus \mathcal{A}_{\mathcal{H}}$ such that $P_1' \setminus \mathcal{A}_{\mathcal{H}} \approx_{\rm mw} P_2' \setminus \mathcal{A}_{\mathcal{H}}$. Thus $P_2 \,/\, \mathcal{A}_{\mathcal{H}} \stackrel{\hat{l}}{\Longrightarrow}_{\rm a} P_2' \,/\, \mathcal{A}_{\mathcal{H}}$ as $l, \tau \notin \mathcal{A}_{\mathcal{H}}$. Since $P_1' \setminus \mathcal{A}_{\mathcal{H}} \approx_{\rm mw} P_2' \setminus \mathcal{A}_{\mathcal{H}}$ with $P_1', P_2' \in {\rm SBNDC}_{\approx_{\rm mw}}$, we have that $(P_1' \,/\, \mathcal{A}_{\mathcal{H}}, P_2' \,/\, \mathcal{A}_{\mathcal{H}}) \in \mathcal{B}$.
   - If $P_1 \,/\, \mathcal{A}_{\mathcal{H}} \stackrel{\tau}{\longrightarrow}_{\rm a} P_1' \,/\, \mathcal{A}_{\mathcal{H}}$ with $P_1 \stackrel{\tau}{\longrightarrow}_{\rm a} P_1'$, then the proof is like the one of the previous case.

As for rates, suppose that $P_1 / \mathcal{A}_\mathcal{H} \not\xrightarrow{\tau}_a$ so that $P_1 \setminus \mathcal{A}_\mathcal{H} \not\xrightarrow{\tau}_a$ too and hence from $P_1 \setminus \mathcal{A}_\mathcal{H} \approx_{mw} P_2 \setminus \mathcal{A}_\mathcal{H}$ it follows that there exists $P_2 \setminus \mathcal{A}_\mathcal{H} \stackrel{\tau^*}{\Longrightarrow}_a \bar{P}_2 \setminus \mathcal{A}_\mathcal{H}$ such that $\bar{P}_2 \setminus \mathcal{A}_\mathcal{H} \not\xrightarrow{\tau}_a$, $P_1 \setminus \mathcal{A}_\mathcal{H} \approx_{mw} \bar{P}_2 \setminus \mathcal{A}_\mathcal{H}$, and $rate(P_1 \setminus \mathcal{A}_\mathcal{H}, C) = rate(\bar{P}_2 \setminus \mathcal{A}_\mathcal{H}, C)$ for all $C \in \mathbb{P}_{mk}/\mathcal{B}$. Since the hiding and restriction operators do not apply to τ and rate transitions, it follows that $P_2 / \mathcal{A}_\mathcal{H} \stackrel{\tau^*}{\Longrightarrow}_a \bar{P}_2 / \mathcal{A}_\mathcal{H}$ with $\bar{P}_2 / \mathcal{A}_\mathcal{H} \not\xrightarrow{\tau}_a$ (if $\bar{P}_2 / \mathcal{A}_\mathcal{H}$ could perform τ due to $\bar{P}_2 \xrightarrow{h}_a \bar{P}_2'$, then $\bar{P}_2 \setminus \mathcal{A}_\mathcal{H} \approx_{mw} \bar{P}_2' \setminus \mathcal{A}_\mathcal{H}$ as $\bar{P}_2 \in SBNDC_{\approx_{mw}}$, hence it would just be a matter of going ahead until one not enabling τ is encountered, which certainly happens because the considered processes belong to $\mathbb{P}_{mk,nhc}$), $(P_1 / \mathcal{A}_\mathcal{H}, \bar{P}_2 / \mathcal{A}_\mathcal{H}) \in \mathcal{B}$, and $rate(P_1 / \mathcal{A}_\mathcal{H}, C) = rate(P_1 \setminus \mathcal{A}_\mathcal{H}, C) = rate(\bar{P}_2 \setminus \mathcal{A}_\mathcal{H}, C) = rate(\bar{P}_2 / \mathcal{A}_\mathcal{H}, C)$ for all $C \in \mathbb{P}_{mk}/\mathcal{B}$.

3. Let $\mathcal{B}$ be an equivalence relation containing all the pairs of processes that have to be shown to be $\approx_{mw}$-equivalent according to the considered result. Starting from $P_1' \setminus \mathcal{A}_\mathcal{H}$ and $((P_2' \parallel_L Q) / L) \setminus \mathcal{A}_\mathcal{H}$ related by $\mathcal{B}$, so that $P_1' \setminus \mathcal{A}_\mathcal{H} \approx_{mw} P_2' / \mathcal{A}_\mathcal{H}$, there are six cases for action transitions based on the operational semantic rules in Table 10.1. In the first two cases, it is $P_1' \setminus \mathcal{A}_\mathcal{H}$ to move first:

   - Let $P_1' \setminus \mathcal{A}_\mathcal{H} \xrightarrow{l}_a P_1'' \setminus \mathcal{A}_\mathcal{H}$. We observe that from $P_2' \in reach(P_2)$ and $P_2 \in SBSNNI_{\approx_{mw}}$ it follows that $P_2' \setminus \mathcal{A}_\mathcal{H} \approx_{mw} P_2' / \mathcal{A}_\mathcal{H}$, so that $P_1' \setminus \mathcal{A}_\mathcal{H} \approx_{mw} P_2' / \mathcal{A}_\mathcal{H} \approx_{mw} P_2' \setminus \mathcal{A}_\mathcal{H}$, i.e., $P_1' \setminus \mathcal{A}_\mathcal{H} \approx_{mw} P_2' \setminus \mathcal{A}_\mathcal{H}$, as $\approx_{mw}$ is symmetric and transitive. As a consequence, since $l \neq \tau$ there exists $P_2' \setminus \mathcal{A}_\mathcal{H} \stackrel{l}{\Longrightarrow}_a P_2'' \setminus \mathcal{A}_\mathcal{H}$ such that $P_1'' \setminus \mathcal{A}_\mathcal{H} \approx_{mw} P_2'' \setminus \mathcal{A}_\mathcal{H}$. Thus $((P_2' \parallel_L Q) / L) \setminus \mathcal{A}_\mathcal{H} \stackrel{l}{\Longrightarrow}_a ((P_2'' \parallel_L Q) / L) \setminus \mathcal{A}_\mathcal{H}$ with $(P_1'' \setminus \mathcal{A}_\mathcal{H}, ((P_2'' \parallel_L Q) / L) \setminus \mathcal{A}_\mathcal{H}) \in \mathcal{B}$ because $P_1'' \in reach(P_1)$, $P_2'' \in reach(P_2)$, and $P_1'' \setminus \mathcal{A}_\mathcal{H} \approx_{mw} P_2'' / \mathcal{A}_\mathcal{H}$ as $P_2 \in SBSNNI_{\approx_{mw}}$.
   - Let $P_1' \setminus \mathcal{A}_\mathcal{H} \xrightarrow{\tau}_a P_1'' \setminus \mathcal{A}_\mathcal{H}$. The proof is like the one of the previous case with $\stackrel{\tau^*}{\Longrightarrow}_a$ used in place of $\stackrel{l}{\Longrightarrow}_a$.

   In the other four cases, instead, it is $((P_2' \parallel_L Q) / L) \setminus \mathcal{A}_\mathcal{H}$ to move first:

   - Let $((P_2' \parallel_L Q) / L) \setminus \mathcal{A}_\mathcal{H} \xrightarrow{l}_a ((P_2'' \parallel_L Q) / L) \setminus \mathcal{A}_\mathcal{H}$ with $P_2' \xrightarrow{l}_a P_2''$ so that $P_2' \setminus \mathcal{A}_\mathcal{H} \xrightarrow{l}_a P_2'' \setminus \mathcal{A}_\mathcal{H}$ as $l \notin \mathcal{A}_\mathcal{H}$. We observe that from $P_2' \in reach(P_2)$ and $P_2 \in SBSNNI_{\approx_{mw}}$ it follows that $P_2' \setminus \mathcal{A}_\mathcal{H} \approx_{mw} P_2' / \mathcal{A}_\mathcal{H}$, so that $P_2' \setminus \mathcal{A}_\mathcal{H} \approx_{mw} P_2' / \mathcal{A}_\mathcal{H} \approx_{mw} P_1' \setminus \mathcal{A}_\mathcal{H}$, i.e., $P_2' \setminus \mathcal{A}_\mathcal{H} \approx_{mw} P_1' \setminus \mathcal{A}_\mathcal{H}$, as $\approx_{mw}$ is symmetric and transitive. As a consequence, since $l \neq \tau$ there exists $P_1' \setminus \mathcal{A}_\mathcal{H} \stackrel{l}{\Longrightarrow}_a P_1'' \setminus \mathcal{A}_\mathcal{H}$ such that $P_2'' \setminus \mathcal{A}_\mathcal{H} \approx_{mw} P_1'' \setminus \mathcal{A}_\mathcal{H}$. Thus $(((P_2'' \parallel_L Q) / L) \setminus \mathcal{A}_\mathcal{H}, P_1'' \setminus \mathcal{A}_\mathcal{H}) \in \mathcal{B}$ because $P_1'' \in reach(P_1)$, $P_2'' \in reach(P_2)$, and $P_1'' \setminus \mathcal{A}_\mathcal{H} \approx_{mw} P_2'' / \mathcal{A}_\mathcal{H}$ as $P_2 \in SBSNNI_{\approx_{mw}}$.
   - Let $((P_2' \parallel_L Q) / L) \setminus \mathcal{A}_\mathcal{H} \xrightarrow{\tau}_a ((P_2'' \parallel_L Q) / L) \setminus \mathcal{A}_\mathcal{H}$ with $P_2' \xrightarrow{\tau}_a P_2''$ so that $P_2' \setminus \mathcal{A}_\mathcal{H} \xrightarrow{\tau}_a P_2'' \setminus \mathcal{A}_\mathcal{H}$ as $\tau \notin \mathcal{A}_\mathcal{H}$. The proof is like the one of the previous case with $\stackrel{\tau^*}{\Longrightarrow}_a$ used in place of $\stackrel{l}{\Longrightarrow}_a$.
   - If $((P_2' \parallel_L Q) / L) \setminus \mathcal{A}_\mathcal{H} \xrightarrow{\tau}_a ((P_2' \parallel_L Q') / L) \setminus \mathcal{A}_\mathcal{H}$ with $Q \xrightarrow{\tau}_a Q'$, then trivially $(((P_2' \parallel_L Q') / L) \setminus \mathcal{A}_\mathcal{H}, P_1' \setminus \mathcal{A}_\mathcal{H}) \in \mathcal{B}$ as $P_2' \approx_{mw} P_2'$ and hence $P_2' / \mathcal{A}_\mathcal{H} \approx_{mw} P_2' / \mathcal{A}_\mathcal{H}$ by Lemma 10.1(5).
   - Let $((P_2' \parallel_L Q) / L) \setminus \mathcal{A}_\mathcal{H} \xrightarrow{\tau}_a ((P_2'' \parallel_L Q') / L) \setminus \mathcal{A}_\mathcal{H}$ with $P_2' \xrightarrow{h}_a P_2''$ – so that $P_2' / \mathcal{A}_\mathcal{H} \xrightarrow{\tau}_a P_2'' / \mathcal{A}_\mathcal{H}$ as $h \in \mathcal{A}_\mathcal{H}$ – and $Q \xrightarrow{h}_a Q'$ for $h \in L$. We observe that from $P_2', P_2'' \in reach(P_2)$ and $P_2 \in SBSNNI_{\approx_{mw}}$ it follows that $P_2' \setminus \mathcal{A}_\mathcal{H} \approx_{mw} P_2' / \mathcal{A}_\mathcal{H}$ and $P_2'' \setminus \mathcal{A}_\mathcal{H} \approx_{mw} P_2'' / \mathcal{A}_\mathcal{H}$, so that $P_2' \setminus \mathcal{A}_\mathcal{H} \stackrel{\tau^*}{\Longrightarrow}_a P_2'' \setminus \mathcal{A}_\mathcal{H}$ as $P_2' / \mathcal{A}_\mathcal{H} \xrightarrow{\tau}_a P_2'' / \mathcal{A}_\mathcal{H}$ and $P_2' \setminus \mathcal{A}_\mathcal{H} \approx_{mw} P_2' / \mathcal{A}_\mathcal{H} \approx_{mw} P_1' \setminus \mathcal{A}_\mathcal{H}$, i.e., $P_2' \setminus \mathcal{A}_\mathcal{H} \approx_{mw} P_1' \setminus \mathcal{A}_\mathcal{H}$, as $\approx_{mw}$ is symmetric and transitive. As a consequence there exists $P_1' \setminus \mathcal{A}_\mathcal{H} \stackrel{\tau^*}{\Longrightarrow}_a P_1'' \setminus \mathcal{A}_\mathcal{H}$ such that $P_2'' \setminus \mathcal{A}_\mathcal{H} \approx_{mw}$

$P_1'' \setminus \mathcal{A}_\mathcal{H}$. Thus $(((P_2'' \parallel_L Q') / L) \setminus \mathcal{A}_\mathcal{H}, P_1'' \setminus \mathcal{A}_\mathcal{H}) \in \mathcal{B}$ because $P_1'' \in reach(P_1)$, $P_2'' \in reach(P_2)$, and $P_1'' \setminus \mathcal{A}_\mathcal{H} \approx_{\rm mw} P_2'' / \mathcal{A}_\mathcal{H}$ as $P_2 \in {\rm SBSNNI}_{\approx_{\rm mw}}$.

As for rates, to avoid trivial cases consider an equivalence class $C \in \mathbb{P}_{\rm mk}/\mathcal{B}$ that involves processes reachable from $P_1' \setminus \mathcal{A}_\mathcal{H}$ and $((P_2' \parallel_L Q) / L) \setminus \mathcal{A}_\mathcal{H}$, specifically $C = \{R_{1,i} \setminus \mathcal{A}_\mathcal{H}, ((R_{2,j} \parallel_L S_j) / L) \setminus \mathcal{A}_\mathcal{H} \mid S_j \in \mathbb{P}_{\rm mk}$ having only prefixes in $\mathcal{A}_\mathcal{H} \wedge R_{k,h} \in reach(P_k) \wedge R_{1,i} \setminus \mathcal{A}_\mathcal{H} \approx_{\rm mw} R_{2,j} / \mathcal{A}_\mathcal{H}\}$. If $P_1' \setminus \mathcal{A}_\mathcal{H} \stackrel{\tau}{\not\longrightarrow}_{\rm a}$ then from $P_1' \setminus \mathcal{A}_\mathcal{H} \approx_{\rm mw} P_2' / \mathcal{A}_\mathcal{H}$ it follows that there exists $P_2' / \mathcal{A}_\mathcal{H} \stackrel{\tau^*}{\Longrightarrow}_{\rm a} \bar{P}_2' / \mathcal{A}_\mathcal{H}$ such that $\bar{P}_2' / \mathcal{A}_\mathcal{H} \stackrel{\tau}{\not\longrightarrow}_{\rm a}$, $P_1' \setminus \mathcal{A}_\mathcal{H} \approx_{\rm mw} \bar{P}_2' / \mathcal{A}_\mathcal{H}$, and $rate(P_1' \setminus \mathcal{A}_\mathcal{H}, C') = rate(\bar{P}_2' / \mathcal{A}_\mathcal{H}, C')$ for all $C' \in \mathbb{P}_{\rm mk}/\approx_{\rm mw}$. Since synchronization as well as the restriction and hiding operators do not apply to τ, we have that $((P_2' \parallel_L Q) / L) \setminus \mathcal{A}_\mathcal{H} \stackrel{\tau^*}{\Longrightarrow}_{\rm a} ((\bar{P}_2' \parallel_L Q') / L) \setminus \mathcal{A}_\mathcal{H}$ with $((\bar{P}_2' \parallel_L Q') / L) \setminus \mathcal{A}_\mathcal{H} \stackrel{\tau}{\not\longrightarrow}_{\rm a}$ and $(P_1' \setminus \mathcal{A}_\mathcal{H}, ((\bar{P}_2' \parallel_L Q') / L) \setminus \mathcal{A}_\mathcal{H}) \in \mathcal{B}$. Since the restriction and hiding operators do not apply to rate transitions and Q cannot perform any rate transition, we have that:

$$\begin{array}{rcl} rate(P_1' \setminus \mathcal{A}_\mathcal{H}, C) & = & rate(P_1' \setminus \mathcal{A}_\mathcal{H}, \bar{C}) \\ rate(((\bar{P}_2' \parallel_L Q) / L) \setminus \mathcal{A}_\mathcal{H}, C) & = & rate(\bar{P}_2' / \mathcal{A}_\mathcal{H}, \bar{C}) \end{array}$$

where:

$$\bar{C} = \{R_{1,i} \setminus \mathcal{A}_\mathcal{H} \in C\} \cup \{R_{2,j} / \mathcal{A}_\mathcal{H} \mid ((R_{2,j} \parallel_L S_j) / L) \setminus \mathcal{A}_\mathcal{H} \in C\}$$

Since $P_1' \setminus \mathcal{A}_\mathcal{H} \approx_{\rm mw} \bar{P}_2' / \mathcal{A}_\mathcal{H}$ and $\bar{C}$ is the union of some $\approx_{\rm mw}$-equivalence classes, we have that:

$$rate(P_1' \setminus \mathcal{A}_\mathcal{H}, \bar{C}) = rate(\bar{P}_2' / \mathcal{A}_\mathcal{H}, \bar{C})$$

If we start from $((P_2' \parallel_L Q) / L) \setminus \mathcal{A}_\mathcal{H} \stackrel{\tau}{\not\longrightarrow}_{\rm a}$, then the proof is similar.

We then prove the three results for the $\approx_{\rm mb}$-based properties:

1. We proceed by induction on the number $n \in \mathbb{N}$ of τ-transitions along $P' / \mathcal{A}_\mathcal{H} \stackrel{\tau^*}{\Longrightarrow}_{\rm a} P'' / \mathcal{A}_\mathcal{H}$:

   - If $n = 0$ then the proof is like the one of the corresponding result for $\approx_{\rm mw}$.
   - Let $n > 0$ and $P_0' / \mathcal{A}_\mathcal{H} \stackrel{\tau}{\longrightarrow}_{\rm a} P_1' / \mathcal{A}_\mathcal{H} \stackrel{\tau}{\longrightarrow}_{\rm a} \ldots \stackrel{\tau}{\longrightarrow}_{\rm a} P_{n-1}' / \mathcal{A}_\mathcal{H} \stackrel{\tau}{\longrightarrow}_{\rm a} P_n' / \mathcal{A}_\mathcal{H}$ where P_0' is P' and P_n' is P''. From the induction hypothesis it follows that $P' \setminus \mathcal{A}_\mathcal{H} \stackrel{\tau^*}{\Longrightarrow}_{\rm a} \hat{P}_{n-1}' \setminus \mathcal{A}_\mathcal{H}$ with $P_{n-1}' \setminus \mathcal{A}_\mathcal{H} \approx_{\rm mb} \hat{P}_{n-1}' \setminus \mathcal{A}_\mathcal{H}$. The rest of the proof is like the one of the corresponding result for $\approx_{\rm mw}$ with the following difference:
     - If $P_{n-1}' \stackrel{\tau}{\longrightarrow}_{\rm a} P_n'$ then $P_{n-1}' \setminus \mathcal{A}_\mathcal{H} \stackrel{\tau}{\longrightarrow}_{\rm a} P_n' \setminus \mathcal{A}_\mathcal{H}$. Since $P_{n-1}' \setminus \mathcal{A}_\mathcal{H} \approx_{\rm mb} \hat{P}_{n-1}' \setminus \mathcal{A}_\mathcal{H}$:
       * either $P_n' \setminus \mathcal{A}_\mathcal{H} \approx_{\rm mb} \hat{P}_{n-1}' \setminus \mathcal{A}_\mathcal{H}$, in which case $\hat{P}_{n-1}' \setminus \mathcal{A}_\mathcal{H}$ stays idle and hence $P' \setminus \mathcal{A}_\mathcal{H} \stackrel{\tau^*}{\Longrightarrow}_{\rm a} \hat{P}_{n-1}' \setminus \mathcal{A}_\mathcal{H}$ with $P'' \setminus \mathcal{A}_\mathcal{H} \approx_{\rm mb} \hat{P}_{n-1}' \setminus \mathcal{A}_\mathcal{H}$;
       * or there exists $\hat{P}_{n-1}' \setminus \mathcal{A}_\mathcal{H} \stackrel{\tau^*}{\Longrightarrow}_{\rm a} \bar{P}_{n-1} \setminus \mathcal{A}_\mathcal{H} \stackrel{\tau}{\longrightarrow}_{\rm a} \hat{P}_n' \setminus \mathcal{A}_\mathcal{H}$ such that $P_{n-1}' \setminus \mathcal{A}_\mathcal{H} \approx_{\rm mb} \bar{P}_{n-1} \setminus \mathcal{A}_\mathcal{H}$ and $P_n' \setminus \mathcal{A}_\mathcal{H} \approx_{\rm mb} \hat{P}_n' \setminus \mathcal{A}_\mathcal{H}$, hence $P' \setminus \mathcal{A}_\mathcal{H} \stackrel{\tau^*}{\Longrightarrow}_{\rm a} \hat{P}_n' \setminus \mathcal{A}_\mathcal{H}$ with $P'' \setminus \mathcal{A}_\mathcal{H} \approx_{\rm mb} \hat{P}_n' \setminus \mathcal{A}_\mathcal{H}$.

2. Let $\mathcal{B}$ be an equivalence relation containing all the pairs of processes that have to be shown to be $\approx_{\rm mb}$-equivalent according to the considered result. Starting from $(P_1 / \mathcal{A}_\mathcal{H}, P_2 / \mathcal{A}_\mathcal{H}) \in \mathcal{B}$, so that $P_1 \setminus \mathcal{A}_\mathcal{H} \approx_{\rm mb} P_2 \setminus \mathcal{A}_\mathcal{H}$, there are three cases for action transitions based on the operational semantic rules in Table 10.1:

   - If $P_1 / \mathcal{A}_\mathcal{H} \stackrel{\tau}{\longrightarrow}_{\rm a} P_1' / \mathcal{A}_\mathcal{H}$ with $P_1 \stackrel{h}{\longrightarrow}_{\rm a} P_1'$, then the proof is like the one of the corresponding result for $\approx_{\rm mw}$.

- If $P_1 \,/\, \mathcal{A}_\mathcal{H} \xrightarrow{l}_\mathrm{a} P_1' \,/\, \mathcal{A}_\mathcal{H}$ with $P_1 \xrightarrow{l}_\mathrm{a} P_1'$, then $P_1 \backslash \mathcal{A}_\mathcal{H} \xrightarrow{l}_\mathrm{a} P_1' \backslash \mathcal{A}_\mathcal{H}$ as $l \notin \mathcal{A}_\mathcal{H}$. From $P_1 \backslash \mathcal{A}_\mathcal{H} \approx_\mathrm{mb} P_2 \backslash \mathcal{A}_\mathcal{H}$ it follows that there exists $P_2 \setminus \mathcal{A}_\mathcal{H} \xRightarrow{\tau^*}_\mathrm{a} \bar{P}_2 \setminus \mathcal{A}_\mathcal{H} \xrightarrow{l}_\mathrm{a} P_2' \setminus \mathcal{A}_\mathcal{H}$ such that $P_1 \setminus \mathcal{A}_\mathcal{H} \approx_\mathrm{mb} \bar{P}_2 \setminus \mathcal{A}_\mathcal{H}$ and $P_1' \setminus \mathcal{A}_\mathcal{H} \approx_\mathrm{mb} P_2' \setminus \mathcal{A}_\mathcal{H}$. Thus $P_2 \,/\, \mathcal{A}_\mathcal{H} \xRightarrow{\tau^*}_\mathrm{a} \bar{P}_2 \,/\, \mathcal{A}_\mathcal{H} \xrightarrow{l}_\mathrm{a} P_2' \,/\, \mathcal{A}_\mathcal{H}$ as $l, \tau \notin \mathcal{A}_\mathcal{H}$. Since $P_1 \setminus \mathcal{A}_\mathcal{H} \approx_\mathrm{mb} \bar{P}_2 \setminus \mathcal{A}_\mathcal{H}$ with $P_1, \bar{P}_2 \in \mathrm{SBNDC}_{\approx_\mathrm{mb}}$ and $P_1' \setminus \mathcal{A}_\mathcal{H} \approx_\mathrm{mb} P_2' \setminus \mathcal{A}_\mathcal{H}$ with $P_1', P_2' \in \mathrm{SBNDC}_{\approx_\mathrm{mb}}$, we have that $(P_1 \,/\, \mathcal{A}_\mathcal{H}, \bar{P}_2 \,/\, \mathcal{A}_\mathcal{H}) \in \mathcal{B}$ and $(P_1' \,/\, \mathcal{A}_\mathcal{H}, P_2' \,/\, \mathcal{A}_\mathcal{H}) \in \mathcal{B}$.
- If $P_1 \,/\, \mathcal{A}_\mathcal{H} \xrightarrow{\tau}_\mathrm{a} P_1' \,/\, \mathcal{A}_\mathcal{H}$ with $P_1 \xrightarrow{\tau}_\mathrm{a} P_1'$, then $P_1 \setminus \mathcal{A}_\mathcal{H} \xrightarrow{\tau}_\mathrm{a} P_1' \setminus \mathcal{A}_\mathcal{H}$ as $\tau \notin \mathcal{A}_\mathcal{H}$. There are two subcases:
  - If $P_1' \setminus \mathcal{A}_\mathcal{H} \approx_\mathrm{mb} P_2 \setminus \mathcal{A}_\mathcal{H}$ then $P_2 \setminus \mathcal{A}_\mathcal{H}$ is allowed to stay idle with $(P_1' \,/\, \mathcal{A}_\mathcal{H}, P_2 \,/\, \mathcal{A}_\mathcal{H}) \in \mathcal{B}$ because $P_1' \setminus \mathcal{A}_\mathcal{H} \approx_\mathrm{mb} P_2 \setminus \mathcal{A}_\mathcal{H}$ and $P_1', P_2 \in \mathrm{SBNDC}_{\approx_\mathrm{mb}}$.
  - If $P_1' \setminus \mathcal{A}_\mathcal{H} \not\approx_\mathrm{mb} P_2 \setminus \mathcal{A}_\mathcal{H}$ then the proof is like the one of the previous case with $\xrightarrow{\tau}_\mathrm{a}$ used in place of $\xrightarrow{l}_\mathrm{a}$.

As for rates, we reason like in the proof of the corresponding result for $\approx_\mathrm{mw}$.

3. Let $\mathcal{B}$ be an equivalence relation containing all the pairs of processes that have to be shown to be $\approx_\mathrm{mb}$-equivalent according to the considered result. Starting from $P_1' \setminus \mathcal{A}_\mathcal{H}$ and $((P_2' \parallel_L Q) \,/\, L) \setminus \mathcal{A}_\mathcal{H}$ related by $\mathcal{B}$, so that $P_1' \setminus \mathcal{A}_\mathcal{H} \approx_\mathrm{mb} P_2' \,/\, \mathcal{A}_\mathcal{H}$, there are six cases for action transitions based on the operational semantic rules in Table 10.1. In the first two cases, it is $P_1' \setminus \mathcal{A}_\mathcal{H}$ to move first:

   - Let $P_1' \setminus \mathcal{A}_\mathcal{H} \xrightarrow{l}_\mathrm{a} P_1'' \setminus \mathcal{A}_\mathcal{H}$. We observe that from $P_2' \in \mathit{reach}(P_2)$ and $P_2 \in \mathrm{SBSNNI}_{\approx_\mathrm{mb}}$ it follows that $P_2' \backslash \mathcal{A}_\mathcal{H} \approx_\mathrm{mb} P_2' \,/\, \mathcal{A}_\mathcal{H}$, so that $P_1' \backslash \mathcal{A}_\mathcal{H} \approx_\mathrm{mb} P_2' \,/\, \mathcal{A}_\mathcal{H} \approx_\mathrm{mb} P_2' \backslash \mathcal{A}_\mathcal{H}$, i.e., $P_1' \backslash \mathcal{A}_\mathcal{H} \approx_\mathrm{mb} P_2' \backslash \mathcal{A}_\mathcal{H}$, as $\approx_\mathrm{mb}$ is symmetric and transitive. As a consequence, since $l \neq \tau$ there exists $P_2' \setminus \mathcal{A}_\mathcal{H} \xRightarrow{\tau^*}_\mathrm{a} \bar{P}_2' \setminus \mathcal{A}_\mathcal{H} \xrightarrow{l}_\mathrm{a} P_2'' \setminus \mathcal{A}_\mathcal{H}$ such that $P_1' \backslash \mathcal{A}_\mathcal{H} \approx_\mathrm{mb} \bar{P}_2' \backslash \mathcal{A}_\mathcal{H}$ and $P_1'' \backslash \mathcal{A}_\mathcal{H} \approx_\mathrm{mb} P_2'' \backslash \mathcal{A}_\mathcal{H}$. Thus $((P_2' \parallel_L Q) \,/\, L) \backslash \mathcal{A}_\mathcal{H} \xRightarrow{\tau^*}_\mathrm{a} ((\bar{P}_2' \parallel_L Q) \,/\, L) \backslash \mathcal{A}_\mathcal{H} \xrightarrow{l}_\mathrm{a} ((P_2'' \parallel_L Q) \,/\, L) \setminus \mathcal{A}_\mathcal{H}$ with $(P_1' \setminus \mathcal{A}_\mathcal{H}, ((\bar{P}_2' \parallel_L Q) \,/\, L) \setminus \mathcal{A}_\mathcal{H}) \in \mathcal{B}$ – because $P_1' \in \mathit{reach}(P_1)$, $\bar{P}_2' \in \mathit{reach}(P_2)$, and $P_1' \backslash \mathcal{A}_\mathcal{H} \approx_\mathrm{mb} \bar{P}_2' \,/\, \mathcal{A}_\mathcal{H}$ as $P_2 \in \mathrm{SBSNNI}_{\approx_\mathrm{mb}}$ – and $(P_1'' \backslash \mathcal{A}_\mathcal{H}, ((P_2'' \parallel_L Q) \,/\, L) \backslash \mathcal{A}_\mathcal{H}) \in \mathcal{B}$ – because $P_1'' \in \mathit{reach}(P_1)$, $P_2'' \in \mathit{reach}(P_2)$, and $P_1'' \setminus \mathcal{A}_\mathcal{H} \approx_\mathrm{mb} P_2'' \,/\, \mathcal{A}_\mathcal{H}$ as $P_2 \in \mathrm{SBSNNI}_{\approx_\mathrm{mb}}$.
   - If $P_1' \setminus \mathcal{A}_\mathcal{H} \xrightarrow{\tau}_\mathrm{a} P_1'' \setminus \mathcal{A}_\mathcal{H}$ there are two subcases:
     - If $P_1'' \setminus \mathcal{A}_\mathcal{H} \approx_\mathrm{mb} P_2' \,/\, \mathcal{A}_\mathcal{H}$ then $(P_2' \parallel_L Q) \,/\, L) \setminus \mathcal{A}_\mathcal{H}$ is allowed to stay idle with $(P_1'' \setminus \mathcal{A}_\mathcal{H}, ((P_2' \parallel_L Q) \,/\, L) \setminus \mathcal{A}_\mathcal{H}) \in \mathcal{B}$ because $P_1'' \in \mathit{reach}(P_1)$ and $P_2' \in \mathit{reach}(P_2)$.
     - If $P_1'' \setminus \mathcal{A}_\mathcal{H} \not\approx_\mathrm{mb} P_2' \,/\, \mathcal{A}_\mathcal{H}$ then the proof is like the one of the previous case with $\xrightarrow{\tau}_\mathrm{a}$ used in place of $\xrightarrow{l}_\mathrm{a}$.

   In the other four cases, instead, it is $((P_2' \parallel_L Q) \,/\, L) \setminus \mathcal{A}_\mathcal{H}$ to move first:

   - Let $((P_2' \parallel_L Q) \,/\, L) \setminus \mathcal{A}_\mathcal{H} \xrightarrow{l}_\mathrm{a} ((P_2'' \parallel_L Q) \,/\, L) \setminus \mathcal{A}_\mathcal{H}$ with $P_2' \xrightarrow{l}_\mathrm{a} P_2''$ so that $P_2' \setminus \mathcal{A}_\mathcal{H} \xrightarrow{l}_\mathrm{a} P_2'' \setminus \mathcal{A}_\mathcal{H}$ as $l \notin \mathcal{A}_\mathcal{H}$. We observe that from $P_2' \in \mathit{reach}(P_2)$ and $P_2 \in \mathrm{SBSNNI}_{\approx_\mathrm{mb}}$ it follows that $P_2' \backslash \mathcal{A}_\mathcal{H} \approx_\mathrm{mb} P_2' \,/\, \mathcal{A}_\mathcal{H}$, so that $P_2' \backslash \mathcal{A}_\mathcal{H} \approx_\mathrm{mb} P_2' \,/\, \mathcal{A}_\mathcal{H} \approx_\mathrm{mb} P_1' \backslash \mathcal{A}_\mathcal{H}$, i.e., $P_2' \backslash \mathcal{A}_\mathcal{H} \approx_\mathrm{mb} P_1' \backslash \mathcal{A}_\mathcal{H}$, as $\approx_\mathrm{mb}$ is symmetric and transitive. As a consequence, since $l \neq \tau$ there exists $P_1' \setminus \mathcal{A}_\mathcal{H} \xRightarrow{\tau^*}_\mathrm{a} \bar{P}_1' \setminus \mathcal{A}_\mathcal{H} \xrightarrow{l}_\mathrm{a} P_1'' \setminus \mathcal{A}_\mathcal{H}$ such that $P_2' \setminus \mathcal{A}_\mathcal{H} \approx_\mathrm{mb} \bar{P}_1' \setminus \mathcal{A}_\mathcal{H}$ and $P_2'' \setminus \mathcal{A}_\mathcal{H} \approx_\mathrm{mb} P_1'' \setminus \mathcal{A}_\mathcal{H}$. Thus $(((P_2' \parallel_L Q) \,/\, L) \setminus \mathcal{A}_\mathcal{H}, \bar{P}_1' \setminus \mathcal{A}_\mathcal{H}) \in \mathcal{B}$ – because $\bar{P}_1' \in \mathit{reach}(P_1)$, $P_2' \in \mathit{reach}(P_2)$, and $\bar{P}_1' \backslash \mathcal{A}_\mathcal{H} \approx_\mathrm{mb} P_2' \,/\, \mathcal{A}_\mathcal{H}$ as $P_2 \in \mathrm{SBSNNI}_{\approx_\mathrm{mb}}$ – and $(((P_2'' \parallel_L Q) \,/\, L) \backslash \mathcal{A}_\mathcal{H}, P_1'' \backslash \mathcal{A}_\mathcal{H}) \in \mathcal{B}$ – because $P_1'' \in \mathit{reach}(P_1)$, $P_2'' \in \mathit{reach}(P_2)$, and $P_1'' \setminus \mathcal{A}_\mathcal{H} \approx_\mathrm{mb} P_2'' \,/\, \mathcal{A}_\mathcal{H}$ as $P_2 \in \mathrm{SBSNNI}_{\approx_\mathrm{mb}}$.

- If $((P_2' \parallel_L Q) / L) \backslash \mathcal{A}_\mathcal{H} \xrightarrow{\tau}_{\rm a} ((P_2'' \parallel_L Q) / L) \backslash \mathcal{A}_\mathcal{H}$ with $P_2' \xrightarrow{\tau}_{\rm a} P_2''$ so that $P_2' \backslash \mathcal{A}_\mathcal{H} \xrightarrow{\tau}_{\rm a} P_2'' \backslash \mathcal{A}_\mathcal{H}$ as $\tau \notin \mathcal{A}_\mathcal{H}$, there are two subcases:
  - If $P_2'' \backslash \mathcal{A}_\mathcal{H} \approx_{\rm mb} P_1' \backslash \mathcal{A}_\mathcal{H}$ then $P_1' \backslash \mathcal{A}_\mathcal{H}$ is allowed to stay idle with $(((P_2'' \parallel_L Q) / L) \backslash \mathcal{A}_\mathcal{H}, P_1' \backslash \mathcal{A}_\mathcal{H}) \in \mathcal{B}$ because $P_1' \in \mathit{reach}(P_1)$, $P_2'' \in \mathit{reach}(P_2)$, and $P_1' \setminus \mathcal{A}_\mathcal{H} \approx_{\rm mb} P_2'' / \mathcal{A}_\mathcal{H}$ as $P_2 \in {\rm SBSNNI}_{\approx_{\rm mb}}$.
  - If $P_2'' \setminus \mathcal{A}_\mathcal{H} \not\approx_{\rm mb} P_1' \setminus \mathcal{A}_\mathcal{H}$ then the proof is like the one of the previous case with $\xrightarrow{\tau}_{\rm a}$ used in place of $\xrightarrow{l}_{\rm a}$.
- If $((P_2' \parallel_L Q) / L) \setminus \mathcal{A}_\mathcal{H} \xrightarrow{\tau}_{\rm a} ((P_2' \parallel_L Q') / L) \setminus \mathcal{A}_\mathcal{H}$ with $Q \xrightarrow{\tau}_{\rm a} Q'$, then trivially $(((P_2' \parallel_L Q') / L) \setminus \mathcal{A}_\mathcal{H}, P_1' \setminus \mathcal{A}_\mathcal{H}) \in \mathcal{B}$ as $P_2' \approx_{\rm mb} P_2'$ and hence $P_2' / \mathcal{A}_\mathcal{H} \approx_{\rm mb} P_2' / \mathcal{A}_\mathcal{H}$ by Lemma 10.1(5).
- Let $((P_2' \parallel_L Q) / L) \setminus \mathcal{A}_\mathcal{H} \xrightarrow{\tau}_{\rm a} ((P_2'' \parallel_L Q') / L) \setminus \mathcal{A}_\mathcal{H}$ with $P_2' \xrightarrow{h}_{\rm a} P_2''$ – so that $P_2' / \mathcal{A}_\mathcal{H} \xrightarrow{\tau}_{\rm a} P_2'' / \mathcal{A}_\mathcal{H}$ as $h \in \mathcal{A}_\mathcal{H}$ – and $Q \xrightarrow{h}_{\rm a} Q'$ for $h \in L$. We observe that from $P_2', P_2'' \in \mathit{reach}(P_2)$ and $P_2 \in {\rm SBSNNI}_{\approx_{\rm mb}}$ it follows that $P_2' \setminus \mathcal{A}_\mathcal{H} \approx_{\rm mb} P_2' / \mathcal{A}_\mathcal{H}$ and $P_2'' \setminus \mathcal{A}_\mathcal{H} \approx_{\rm mb} P_2'' / \mathcal{A}_\mathcal{H}$, so that $P_2' \setminus \mathcal{A}_\mathcal{H} \xrightarrow{\tau}_{\rm a} P_2'' \setminus \mathcal{A}_\mathcal{H}$ and $P_2' \setminus \mathcal{A}_\mathcal{H} \approx_{\rm mb} P_2' / \mathcal{A}_\mathcal{H} \approx_{\rm mb} P_1' \setminus \mathcal{A}_\mathcal{H}$, i.e., $P_2' \setminus \mathcal{A}_\mathcal{H} \approx_{\rm mb} P_1' \setminus \mathcal{A}_\mathcal{H}$, as $\approx_{\rm mb}$ is symmetric and transitive. There are two subcases:
  - If $P_2'' \backslash \mathcal{A}_\mathcal{H} \approx_{\rm mb} P_1' \backslash \mathcal{A}_\mathcal{H}$ then $P_1' \backslash \mathcal{A}_\mathcal{H}$ is allowed to stay idle with $(((P_2'' \parallel_L Q') / L) \backslash \mathcal{A}_\mathcal{H}, P_1' \backslash \mathcal{A}_\mathcal{H}) \in \mathcal{B}$ because $P_1' \in \mathit{reach}(P_1)$, $P_2'' \in \mathit{reach}(P_2)$, and $P_1' \setminus \mathcal{A}_\mathcal{H} \approx_{\rm mb} P_2'' / \mathcal{A}_\mathcal{H}$ as $P_2 \in {\rm SBSNNI}_{\approx_{\rm mb}}$.
  - If $P_2'' \setminus \mathcal{A}_\mathcal{H} \not\approx_{\rm mb} P_1' \setminus \mathcal{A}_\mathcal{H}$ then there exists $P_1' \setminus \mathcal{A}_\mathcal{H} \xRightarrow{\tau^*}_{\rm a} \bar{P}_1' \setminus \mathcal{A}_\mathcal{H} \xrightarrow{\tau}_{\rm a} P_1'' \setminus \mathcal{A}_\mathcal{H}$ such that $P_2' \setminus \mathcal{A}_\mathcal{H} \approx_{\rm mb} \bar{P}_1' \setminus \mathcal{A}_\mathcal{H}$ and $P_2'' \setminus \mathcal{A}_\mathcal{H} \approx_{\rm mb} P_1'' \setminus \mathcal{A}_\mathcal{H}$. Thus $(((P_2' \parallel_L Q) / L) \setminus \mathcal{A}_\mathcal{H}, \bar{P}_1' \setminus \mathcal{A}_\mathcal{H}) \in \mathcal{B}$ – because $\bar{P}_1' \in \mathit{reach}(P_1)$, $P_2' \in \mathit{reach}(P_2)$, and $\bar{P}_1' \setminus \mathcal{A}_\mathcal{H} \approx_{\rm mb} P_2' / \mathcal{A}_\mathcal{H}$ as $P_2 \in {\rm SBSNNI}_{\approx_{\rm mb}}$ – and $(((P_2'' \parallel_L Q') / L) \setminus \mathcal{A}_\mathcal{H}, P_1'' \setminus \mathcal{A}_\mathcal{H}) \in \mathcal{B}$ – because $P_1'' \in \mathit{reach}(P_1)$, $P_2'' \in \mathit{reach}(P_2)$, and $P_1'' \setminus \mathcal{A}_\mathcal{H} \approx_{\rm mb} P_2'' / \mathcal{A}_\mathcal{H}$ as $P_2 \in {\rm SBSNNI}_{\approx_{\rm mb}}$.

As for rates, we reason like in the proof of the corresponding result for $\approx_{\rm mw}$. ∎

Theorem 10.3. *Let* $\approx \in \{\approx_{\rm mw}, \approx_{\rm mb}\}$. *Then over* $\mathbb{P}_{\rm mk,nhc}$*:*

$$ {\rm SBNDC}_\approx \subsetneq {\rm SBSNNI}_\approx = {\rm P\_BNDC}_\approx \subsetneq {\rm BNDC}_\approx \subsetneq {\rm BSNNI}_\approx $$

Proof. We first prove the results for the $\approx_{\rm mw}$-based properties. Let us examine each relationship separately:

- ${\rm SBNDC}_{\approx_{\rm mw}} \subseteq {\rm SBSNNI}_{\approx_{\rm mw}}$. Given $P \in {\rm SBNDC}_{\approx_{\rm mw}}$, the result follows by proving that the relation $\mathcal{B} = \{(P' \setminus \mathcal{A}_\mathcal{H}, P' / \mathcal{A}_\mathcal{H}) \mid P' \in \mathit{reach}(P)\}$ is a weak Markovian bisimulation up to $\approx_{\rm mw}$. Starting from $(P' \setminus \mathcal{A}_\mathcal{H}, P' / \mathcal{A}_\mathcal{H}) \in \mathcal{B}$, there are three cases for action transitions based on the operational semantic rules in Table 10.1. In the first case, it is $P' \setminus \mathcal{A}_\mathcal{H}$ to move first:

  - If $P' \setminus \mathcal{A}_\mathcal{H} \xRightarrow{a}_{\rm a} P'' \setminus \mathcal{A}_\mathcal{H}$ with $a \in \mathcal{A}_\mathcal{L} \cup \{\tau\}$, then $P' / \mathcal{A}_\mathcal{H} \xRightarrow{\hat{a}}_{\rm a} P'' / \mathcal{A}_\mathcal{H}$ as $a, \tau \notin \mathcal{A}_\mathcal{H}$, with $(P'' \setminus \mathcal{A}_\mathcal{H}, P'' / \mathcal{A}_\mathcal{H}) \in \mathcal{B}$ as $P'' \in \mathit{reach}(P)$. Thus $(P'' \setminus \mathcal{A}_\mathcal{H}, P'' / \mathcal{A}_\mathcal{H}) \in (\mathcal{B} \cup \mathcal{B}^{-1} \cup \approx_{\rm mw})^+$.

  In the other two cases, instead, it is $P' / \mathcal{A}_\mathcal{H}$ to move first (note that possible τ-transitions along $\xRightarrow{\tau^*}_{\rm a}$ arising from high actions in P' can no longer be executed when responding from $P' \setminus \mathcal{A}_\mathcal{H}$, but for them we exploit $P \in {\rm SBNDC}_{\approx_{\rm mw}}$ and Lemma 10.3(1)):

– If $P' \,/\, \mathcal{A}_\mathcal{H} \stackrel{a}{\Longrightarrow}_\mathrm{a} P'' \,/\, \mathcal{A}_\mathcal{H}$ with $a \in \mathcal{A}_\mathcal{L} \cup \{\tau\}$, then there exist two processes $\bar{P}', \bar{P}'' \in \mathit{reach}(P')$ such that $P' \,/\, \mathcal{A}_\mathcal{H} \stackrel{\tau^*}{\Longrightarrow}_\mathrm{a} \bar{P}' / \mathcal{A}_\mathcal{H} \stackrel{a}{\longrightarrow}_\mathrm{a} \bar{P}'' \,/\, \mathcal{A}_\mathcal{H} \stackrel{\tau^*}{\Longrightarrow}_\mathrm{a} P'' \,/\, \mathcal{A}_\mathcal{H}$. From $P' \,/\, \mathcal{A}_\mathcal{H} \stackrel{\tau^*}{\Longrightarrow}_\mathrm{a} \bar{P}' \,/\, \mathcal{A}_\mathcal{H}$ and Lemma 10.3(1) it follows that $P' \setminus \mathcal{A}_\mathcal{H} \stackrel{\tau^*}{\Longrightarrow}_\mathrm{a} \hat{P}' \setminus \mathcal{A}_\mathcal{H}$ with $\bar{P}' \setminus \mathcal{A}_\mathcal{H} \approx_\mathrm{mw} \hat{P}' \setminus \mathcal{A}_\mathcal{H}$. From $\bar{P}' \,/\, \mathcal{A}_\mathcal{H} \stackrel{a}{\longrightarrow}_\mathrm{a} \bar{P}'' \,/\, \mathcal{A}_\mathcal{H}$ it follows that $\bar{P}' \setminus \mathcal{A}_\mathcal{H} \stackrel{a}{\longrightarrow}_\mathrm{a} \bar{P}'' \setminus \mathcal{A}_\mathcal{H}$ as $a \notin \mathcal{A}_\mathcal{H}$, hence $\hat{P}' \setminus \mathcal{A}_\mathcal{H} \stackrel{\hat{a}}{\Longrightarrow}_\mathrm{a} \hat{P}'' \setminus \mathcal{A}_\mathcal{H}$ with $\bar{P}'' \setminus \mathcal{A}_\mathcal{H} \approx_\mathrm{mw} \hat{P}'' \setminus \mathcal{A}_\mathcal{H}$ as $\bar{P}' \setminus \mathcal{A}_\mathcal{H} \approx_\mathrm{mw} \hat{P}' \setminus \mathcal{A}_\mathcal{H}$. From $\bar{P}'' \,/\, \mathcal{A}_\mathcal{H} \stackrel{\tau^*}{\Longrightarrow}_\mathrm{a} P'' / \mathcal{A}_\mathcal{H}$ and Lemma 10.3(1) it follows that $\bar{P}'' \setminus \mathcal{A}_\mathcal{H} \stackrel{\tau^*}{\Longrightarrow}_\mathrm{a} \hat{P}''' \setminus \mathcal{A}_\mathcal{H}$ with $P'' \setminus \mathcal{A}_\mathcal{H} \approx_\mathrm{mw} \hat{P}''' \setminus \mathcal{A}_\mathcal{H}$, hence $\hat{P}'' \setminus \mathcal{A}_\mathcal{H} \stackrel{\tau^*}{\Longrightarrow}_\mathrm{a} \hat{P}'''' \setminus \mathcal{A}_\mathcal{H}$ with $\hat{P}''' \setminus \mathcal{A}_\mathcal{H} \approx_\mathrm{mw} \hat{P}'''' \setminus \mathcal{A}_\mathcal{H}$ as $\bar{P}'' \setminus \mathcal{A}_\mathcal{H} \approx_\mathrm{mw} \hat{P}'' \setminus \mathcal{A}_\mathcal{H}$. Note that $P'' \setminus \mathcal{A}_\mathcal{H} \approx_\mathrm{mw} \hat{P}'''' \setminus \mathcal{A}_\mathcal{H}$ as $\approx_\mathrm{mw}$ is transitive. Summing up, we have that $P' \setminus \mathcal{A}_\mathcal{H} \stackrel{\hat{a}}{\Longrightarrow}_\mathrm{a} \hat{P}'''' \setminus \mathcal{A}_\mathcal{H}$ with $P'' \,/\, \mathcal{A}_\mathcal{H} \;\mathcal{B}\; P'' \setminus \mathcal{A}_\mathcal{H} \approx_\mathrm{mw} \hat{P}'''' \setminus \mathcal{A}_\mathcal{H}$, as $P'' \in \mathit{reach}(P)$, and hence $(P'' \,/\, \mathcal{A}_\mathcal{H}, \hat{P}'''' \setminus \mathcal{A}_\mathcal{H}) \in (\mathcal{B} \cup \mathcal{B}^{-1} \cup \approx_\mathrm{mw})^+$.

– If $P' \,/\, \mathcal{A}_\mathcal{H} \stackrel{\tau}{\Longrightarrow}_\mathrm{a} P'' \,/\, \mathcal{A}_\mathcal{H}$ stems from $\bar{P}' \stackrel{h}{\longrightarrow}_\mathrm{a} \bar{P}''$ for some $\bar{P}', \bar{P}'' \in \mathit{reach}(P')$, then from Lemma 10.3(1) it follows that $P' \setminus \mathcal{A}_\mathcal{H} \stackrel{\tau^*}{\Longrightarrow}_\mathrm{a} \hat{P}'' \setminus \mathcal{A}_\mathcal{H}$ with $P'' \setminus \mathcal{A}_\mathcal{H} \approx_\mathrm{mw} \hat{P}'' \setminus \mathcal{A}_\mathcal{H}$. Since $P'' \,/\, \mathcal{A}_\mathcal{H} \;\mathcal{B}^{-1}\; P'' \setminus \mathcal{A}_\mathcal{H} \approx_\mathrm{mw} \hat{P}'' \setminus \mathcal{A}_\mathcal{H}$ as $P'' \in \mathit{reach}(P)$, we have that $(P'' \,/\, \mathcal{A}_\mathcal{H}, \hat{P}'' \setminus \mathcal{A}_\mathcal{H}) \in (\mathcal{B} \cup \mathcal{B}^{-1} \cup \approx_\mathrm{mw})^+$.

As for rates, suppose that $P' \setminus \mathcal{A}_\mathcal{H} \stackrel{\tau}{\not\longrightarrow}_\mathrm{a}$ so that $P' \stackrel{\tau}{\not\longrightarrow}_\mathrm{a}$ too. There are two cases depending on whether P' performs a high action or not:

– If $P' \stackrel{h}{\longrightarrow}_\mathrm{a} P''$ then $P' \,/\, \mathcal{A}_\mathcal{H} \stackrel{\tau}{\longrightarrow}_\mathrm{a} P'' \,/\, \mathcal{A}_\mathcal{H}$. From Lemma 10.3(1) it follows that there exists $P' \setminus \mathcal{A}_\mathcal{H} \stackrel{\tau^*}{\Longrightarrow}_\mathrm{a} \hat{P}' \setminus \mathcal{A}_\mathcal{H}$ such that $P'' \,/\, \mathcal{A}_\mathcal{H} \approx_\mathrm{mw} \hat{P}' \setminus \mathcal{A}_\mathcal{H}$, but since $P' \setminus \mathcal{A}_\mathcal{H} \stackrel{\tau}{\not\longrightarrow}_\mathrm{a}$ it holds that $\hat{P}' \setminus \mathcal{A}_\mathcal{H}$ must be $P' \setminus \mathcal{A}_\mathcal{H}$ and hence $P'' \,/\, \mathcal{A}_\mathcal{H} \approx_\mathrm{mw} P' \setminus \mathcal{A}_\mathcal{H}$. By repeatedly applying this procedure we will reach a process $\bar{P}' \,/\, \mathcal{A}_\mathcal{H} \stackrel{\tau}{\not\longrightarrow}_\mathrm{a}$, which is guaranteed by the fact that $P \in \mathbb{P}_\mathrm{mk,nhc}$. By Lemma 10.3(1) we thus obtain that $\bar{P}' \,/\, \mathcal{A}_\mathcal{H} \approx_\mathrm{mw} P' \setminus \mathcal{A}_\mathcal{H}$ and hence $(\bar{P}' \,/\, \mathcal{A}_\mathcal{H}, P' \setminus \mathcal{A}_\mathcal{H}) \in (\mathcal{B} \cup \mathcal{B}^{-1} \cup \approx_\mathrm{mw})^+$ with $\mathit{rate}(\bar{P}' \,/\, \mathcal{A}_\mathcal{H}, C) = \mathit{rate}(P' \setminus \mathcal{A}_\mathcal{H}, C)$ for all $C \in \mathbb{P}_\mathrm{mk}/(\mathcal{B} \cup \mathcal{B}^{-1} \cup \approx_\mathrm{mw})^+$.

– If P' cannot perform any high action, then $P' \,/\, \mathcal{A}_\mathcal{H} \stackrel{\tau}{\not\longrightarrow}_\mathrm{a}$ and, since the hiding and restriction operators do not apply to rate transitions, we have that $\mathit{rate}(P' \setminus \mathcal{A}_\mathcal{H}, C) = \mathit{rate}(P' \,/\, \mathcal{A}_\mathcal{H}, C)$ for all $C \in \mathbb{P}_\mathrm{mk}/(\mathcal{B} \cup \mathcal{B}^{-1} \cup \approx_\mathrm{mw})^+$.

If we start from $P' \,/\, \mathcal{A}_\mathcal{H} \stackrel{\tau}{\not\longrightarrow}_\mathrm{a}$, then the proof is like the one of the second case as P' cannot perform any high action.

- $\mathrm{SBSNNI}_{\approx_\mathrm{mw}} = \mathrm{P\_BNDC}_{\approx_\mathrm{mw}}$. $\mathrm{SBSNNI}_{\approx_\mathrm{w}} \subseteq \mathrm{P\_BNDC}_{\approx_\mathrm{mw}}$ follows from Lemma 10.3(3) by taking P_1' identical to P_2' and both reachable from $P \in \mathrm{SBSNNI}_{\approx_\mathrm{mw}}$.
  On the other hand, if $P \in \mathrm{P\_BNDC}_{\approx_\mathrm{mw}}$ then $P' \in \mathrm{BNDC}_{\approx_\mathrm{mw}}$ for every $P' \in \mathit{reach}(P)$. Since $\mathrm{BNDC}_{\approx_\mathrm{mw}} \subseteq \mathrm{BSNNI}_{\approx_\mathrm{mw}}$ as will be shown in the last case of the proof of this part of the theorem, $P' \in \mathrm{BSNNI}_{\approx_\mathrm{mw}}$ for every $P' \in \mathit{reach}(P)$, i.e., $P \in \mathrm{SBSNNI}_{\approx_\mathrm{mw}}$.

- $\mathrm{SBSNNI}_{\approx_\mathrm{mw}} \subseteq \mathrm{BNDC}_{\approx_\mathrm{mw}}$. If $P \in \mathrm{SBSNNI}_{\approx_\mathrm{mw}} = \mathrm{P\_BNDC}_{\approx_\mathrm{mw}}$ then it immediately follows that $P \in \mathrm{BNDC}_{\approx_\mathrm{mw}}$.

- $\mathrm{BNDC}_{\approx_\mathrm{mw}} \subseteq \mathrm{BSNNI}_{\approx_\mathrm{mw}}$. If $P \in \mathrm{BNDC}_{\approx_\mathrm{mw}}$, i.e., $P \setminus \mathcal{A}_\mathcal{H} \approx_\mathrm{mw} (P \parallel_L Q) \,/\, L) \setminus \mathcal{A}_\mathcal{H}$ for all $Q \in \mathbb{P}_\mathrm{mk,nhc}$ such that each of its prefixes belongs to $\mathcal{A}_\mathcal{H}$ and for all $L \subseteq \mathcal{A}_\mathcal{H}$, then we can consider in particular $\hat{Q}$ capable of stepwise mimicking the high-level behavior of P, in the sense that $\hat{Q}$ is able to synchronize with all the high-level actions executed by P and its reachable processes, along with $\hat{L} = \mathcal{A}_\mathcal{H}$. As a consequence $(P \parallel_{\hat{L}} \hat{Q}) \,/\, \hat{L}) \setminus \mathcal{A}_\mathcal{H}$

is isomorphic to $P \,/\, \mathcal{A}_\mathcal{H}$, hence $P \setminus \mathcal{A}_\mathcal{H} \approx_{\rm mw} (P \parallel_{\hat{L}} \hat{Q}) \,/\, \hat{L}) \setminus \mathcal{A}_\mathcal{H} \approx_{\rm mw} P \,/\, \mathcal{A}_\mathcal{H}$, i.e., $P \in {\rm BSNNI}_{\approx_{\rm mw}}$, as $\approx_{\rm mw}$ is transitive.

We then prove the results for the $\approx_{\rm mb}$-based properties. Let us examine each relationship separately:

- ${\rm SBNDC}_{\approx_{\rm mb}} \subseteq {\rm SBSNNI}_{\approx_{\rm mb}}$. Given $P \in {\rm SBNDC}_{\approx_{\rm mb}}$, the result follows by proving that the relation $\mathcal{B} = \{(P' \setminus \mathcal{A}_\mathcal{H}, P' \,/\, \mathcal{A}_\mathcal{H}) \mid P' \in \mathit{reach}(P)\}$ is a Markovian branching bisimulation up to $\approx_{\rm mb}$. Starting from $(P' \setminus \mathcal{A}_\mathcal{H}, P' \,/\, \mathcal{A}_\mathcal{H}) \in \mathcal{B}$, there are three cases for action transitions based on the operational semantic rules in Table 10.1. In the first case, it is $P' \setminus \mathcal{A}_\mathcal{H}$ to move first:

  - If $P' \setminus \mathcal{A}_\mathcal{H} \stackrel{\tau^*}{\Longrightarrow}_{\rm a} \bar{P}' \setminus \mathcal{A}_\mathcal{H} \stackrel{a}{\longrightarrow}_{\rm a} P'' \setminus \mathcal{A}_\mathcal{H}$ with $a \in \mathcal{A}_\mathcal{L} \cup \{\tau\}$, then $P' \,/\, \mathcal{A}_\mathcal{H} \stackrel{\tau^*}{\Longrightarrow}_{\rm a} \bar{P}' \,/\, \mathcal{A}_\mathcal{H} \stackrel{a}{\longrightarrow}_{\rm a} P'' \,/\, \mathcal{A}_\mathcal{H}$ as $a, \tau \notin \mathcal{A}_\mathcal{H}$, with $(\bar{P}' \setminus \mathcal{A}_\mathcal{H}, \bar{P}' \,/\, \mathcal{A}_\mathcal{H}) \in \mathcal{B}$ and $(P'' \setminus \mathcal{A}_\mathcal{H}, P'' \,/\, \mathcal{A}_\mathcal{H}) \in \mathcal{B}$ as $\bar{P}', P'' \in \mathit{reach}(P)$. Thus $(\bar{P}' \setminus \mathcal{A}_\mathcal{H}, \bar{P}' \,/\, \mathcal{A}_\mathcal{H}) \in (\mathcal{B} \cup \mathcal{B}^{-1} \cup \approx_{\rm mb})^+$ and $(P'' \setminus \mathcal{A}_\mathcal{H}, P'' \,/\, \mathcal{A}_\mathcal{H}) \in (\mathcal{B} \cup \mathcal{B}^{-1} \cup \approx_{\rm mb})^+$.

  In the other two cases, instead, it is $P' \,/\, \mathcal{A}_\mathcal{H}$ to move first (note that possible τ-transitions along $\stackrel{\tau^*}{\Longrightarrow}_{\rm a}$ arising from high actions in P' can no longer be executed when responding from $P' \setminus \mathcal{A}_\mathcal{H}$, but for them we exploit $P \in {\rm SBNDC}_{\approx_{\rm mb}}$ and Lemma 10.3(1)):

  - Let $P' \,/\, \mathcal{A}_\mathcal{H} \stackrel{\tau^*}{\Longrightarrow}_{\rm a} \bar{P}' \,/\, \mathcal{A}_\mathcal{H} \stackrel{a}{\longrightarrow}_{\rm a} P'' \,/\, \mathcal{A}_\mathcal{H}$ with $a \in \mathcal{A}_\mathcal{L} \cup \{\tau\}$. From $P' \,/\, \mathcal{A}_\mathcal{H} \stackrel{\tau^*}{\Longrightarrow}_{\rm a} \bar{P}' \,/\, \mathcal{A}_\mathcal{H}$ and Lemma 10.3(1) it follows that $P' \setminus \mathcal{A}_\mathcal{H} \stackrel{\tau^*}{\Longrightarrow}_{\rm a} \hat{P}' \setminus \mathcal{A}_\mathcal{H}$ with $\bar{P}' \setminus \mathcal{A}_\mathcal{H} \approx_{\rm mb} \hat{P}' \setminus \mathcal{A}_\mathcal{H}$. From $\bar{P}' \,/\, \mathcal{A}_\mathcal{H} \stackrel{a}{\longrightarrow}_{\rm a} P'' \,/\, \mathcal{A}_\mathcal{H}$ it follows that $\bar{P}' \setminus \mathcal{A}_\mathcal{H} \stackrel{a}{\longrightarrow}_{\rm a} P'' \setminus \mathcal{A}_\mathcal{H}$ as $a \notin \mathcal{A}_\mathcal{H}$. Since $\bar{P}' \setminus \mathcal{A}_\mathcal{H} \approx_{\rm mb} \hat{P}' \setminus \mathcal{A}_\mathcal{H}$ there are two subcases:
    - If $a = \tau$ and $P'' \setminus \mathcal{A}_\mathcal{H} \approx_{\rm mb} \hat{P}' \setminus \mathcal{A}_\mathcal{H}$, then $\bar{P}' \setminus \mathcal{A}_\mathcal{H} \approx_{\rm mb} P'' \setminus \mathcal{A}_\mathcal{H}$ as $\approx_{\rm mb}$ is symmetric and transitive. From $\bar{P}', P'' \in {\rm SBNDC}_{\approx_{\rm mb}}$ and Lemma 10.3(2) it follows that $\bar{P}' \,/\, \mathcal{A}_\mathcal{H} \approx_{\rm mb} P'' \,/\, \mathcal{A}_\mathcal{H}$. Thus $P' \setminus \mathcal{A}_\mathcal{H}$ is allowed to stay idle.
    - Otherwise there exists $\hat{P}' \setminus \mathcal{A}_\mathcal{H} \stackrel{\tau^*}{\Longrightarrow}_{\rm a} \hat{P}'' \setminus \mathcal{A}_\mathcal{H} \stackrel{a}{\longrightarrow}_{\rm a} \hat{P}''' \setminus \mathcal{A}_\mathcal{H}$ such that $\bar{P}' \,/\, \mathcal{A}_\mathcal{H} \approx_{\rm mb} \hat{P}'' \setminus \mathcal{A}_\mathcal{H}$ and $P'' \,/\, \mathcal{A}_\mathcal{H} \approx_{\rm mb} \hat{P}''' \setminus \mathcal{A}_\mathcal{H}$. Summing up, we have that $P' \setminus \mathcal{A}_\mathcal{H} \stackrel{\tau^*}{\Longrightarrow}_{\rm a} \hat{P}'' \setminus \mathcal{A}_\mathcal{H} \stackrel{a}{\longrightarrow}_{\rm a} \hat{P}''' \setminus \mathcal{A}_\mathcal{H}$ with $\bar{P}' \,/\, \mathcal{A}_\mathcal{H} \; \mathcal{B} \; \bar{P}' \setminus \mathcal{A}_\mathcal{H} \approx_{\rm mb} \hat{P}'' \setminus \mathcal{A}_\mathcal{H}$ and $P'' \,/\, \mathcal{A}_\mathcal{H} \; \mathcal{B} \; P'' \setminus \mathcal{A}_\mathcal{H} \approx_{\rm mb} \hat{P}''' \setminus \mathcal{A}_\mathcal{H}$, as $\bar{P}', P'' \in \mathit{reach}(P)$, and hence $(\bar{P}' \,/\, \mathcal{A}_\mathcal{H}, \hat{P}'' \setminus \mathcal{A}_\mathcal{H}) \in (\mathcal{B} \cup \mathcal{B}^{-1} \cup \approx_{\rm mb})^+$ and $(P'' \,/\, \mathcal{A}_\mathcal{H}, \hat{P}''' \setminus \mathcal{A}_\mathcal{H}) \in (\mathcal{B} \cup \mathcal{B}^{-1} \cup \approx_{\rm mb})^+$.
  - Let $P' \,/\, \mathcal{A}_\mathcal{H} \stackrel{\tau^*}{\Longrightarrow}_{\rm a} \bar{P}' \,/\, \mathcal{A}_\mathcal{H} \stackrel{\tau}{\longrightarrow}_{\rm a} P'' \,/\, \mathcal{A}_\mathcal{H}$ with $\bar{P}' \stackrel{h}{\longrightarrow}_{\rm a} P''$. From $\bar{P}' \in \mathit{reach}(P)$ and $P \in {\rm SBNDC}_{\approx_{\rm mb}}$ it follows that $\bar{P}' \setminus \mathcal{A}_\mathcal{H} \approx_{\rm mb} P'' \setminus \mathcal{A}_\mathcal{H}$, hence $\bar{P}' \,/\, \mathcal{A}_\mathcal{H} \approx_{\rm mb} P'' \,/\, \mathcal{A}_\mathcal{H}$ by virtue of Lemma 10.3(2) as $\bar{P}', P'' \in {\rm SBNDC}_{\approx_{\rm mb}}$. Thus $P' \setminus \mathcal{A}_\mathcal{H}$ is allowed to stay idle.

  As for rates, the proof is like the one of the corresponding result for $\approx_{\rm mw}$.

- ${\rm SBSNNI}_{\approx_{\rm mb}} = {\rm P\_BNDC}_{\approx_{\rm mb}}$. The proof is like the one of the corresponding result for $\approx_{\rm mw}$.
- ${\rm SBSNNI}_{\approx_{\rm mb}} \subseteq {\rm BNDC}_{\approx_{\rm mb}}$. The proof is like the one of the corresponding result for $\approx_{\rm mw}$.
- ${\rm BNDC}_{\approx_{\rm mb}} \subseteq {\rm BSNNI}_{\approx_{\rm mb}}$. The proof is like the one of the corresponding result for $\approx_{\rm mw}$. ■

All the inclusions in the previous theorem are strict by virtue of the same counterexamples as those after Theorem 8.4.

We further observe that each of the $\approx_{\rm mb}$-based noninterference properties implies the corresponding $\approx_{\rm mw}$-based one, due to the fact that $\approx_{\rm mb}$ is finer than $\approx_{\rm mw}$.

Theorem 10.4. *The following inclusions hold:*

1. $\text{BSNNI}_{\approx_{\rm mb}} \subsetneq \text{BSNNI}_{\approx_{\rm mw}}$.
2. $\text{BNDC}_{\approx_{\rm mb}} \subsetneq \text{BNDC}_{\approx_{\rm mw}}$.
3. $\text{SBSNNI}_{\approx_{\rm mb}} \subsetneq \text{SBSNNI}_{\approx_{\rm mw}}$.
4. $\text{P\_BNDC}_{\approx_{\rm mb}} \subsetneq \text{P\_BNDC}_{\approx_{\rm mw}}$.
5. $\text{SBNDC}_{\approx_{\rm mb}} \subsetneq \text{SBNDC}_{\approx_{\rm mw}}$. ■

All the inclusions above are strict by virtue of the following result; for an example of P_1 and P_2 below, see Figure 10.1.

Theorem 10.5. *Let $P_1, P_2 \in \mathbb{P}_{\rm mk,nhc}$ be such that $P_1 \approx_{\rm mw} P_2$ but $P_1 \not\approx_{\rm mb} P_2$. If no high-level actions occur in P_1 and P_2, then $Q \in \{P_1 + h\,.\,P_2, P_2 + h\,.\,P_1\}$ is such that:*

1. $Q \in \text{BSNNI}_{\approx_{\rm mw}}$ *but* $Q \notin \text{BSNNI}_{\approx_{\rm mb}}$.
2. $Q \in \text{BNDC}_{\approx_{\rm mw}}$ *but* $Q \notin \text{BNDC}_{\approx_{\rm mb}}$.
3. $Q \in \text{SBSNNI}_{\approx_{\rm mw}}$ *but* $Q \notin \text{SBSNNI}_{\approx_{\rm mb}}$.
4. $Q \in \text{P\_BNDC}_{\approx_{\rm mw}}$ *but* $Q \notin \text{P\_BNDC}_{\approx_{\rm mb}}$.
5. $Q \in \text{SBNDC}_{\approx_{\rm mw}}$ *but* $Q \notin \text{SBNDC}_{\approx_{\rm mb}}$.

Proof. Let Q be $P_1 + h\,.\,P_2$ (the proof is similar for Q equal to $P_2 + h\,.\,P_1$) and observe that no high-level actions occur in every process reachable from Q except Q itself:

1. Since the only high-level action occurring in Q is h, in the proof of $Q \in \text{BSNNI}_{\approx_{\rm mw}}$ the only interesting case is the transition $Q \,/\, \mathcal{A}_{\mathcal{H}} \xrightarrow{\tau}_{\rm a} P_2 \,/\, \mathcal{A}_{\mathcal{H}}$, to which $Q \setminus \mathcal{A}_{\mathcal{H}}$ responds by staying idle because $P_2 \,/\, \mathcal{A}_{\mathcal{H}} \approx_{\rm mw} P_2 \approx_{\rm mw} P_1 \approx_{\rm mw} Q \setminus \mathcal{A}_{\mathcal{H}}$, i.e., $P_2 \,/\, \mathcal{A}_{\mathcal{H}} \approx_{\rm mw} Q \setminus \mathcal{A}_{\mathcal{H}}$ as $\approx_{\rm mw}$ is symmetric and transitive.
   On the other hand, $Q \notin \text{BSNNI}_{\approx_{\rm mb}}$ because $P_2 \not\approx_{\rm mb} P_1$ in the same situation as before.
2. Since $Q \in \text{BSNNI}_{\approx_{\rm mw}}$ by the previous result and no high-level actions occur in every process reachable from Q other than Q, it holds that $Q \in \text{SBSNNI}_{\approx_{\rm mw}}$ and hence $Q \in \text{BNDC}_{\approx_{\rm mw}}$ by virtue of Theorem 10.3.
   On the other hand, from $Q \notin \text{BSNNI}_{\approx_{\rm mb}}$ by the previous result it follows that $Q \notin \text{BNDC}_{\approx_{\rm mb}}$ by virtue of Theorem 10.3.
3. We already know from the proof of the previous result that $Q \in \text{SBSNNI}_{\approx_{\rm mw}}$.
   On the other hand, from $Q \notin \text{BSNNI}_{\approx_{\rm mb}}$ by the first result it follows that $Q \notin \text{SBSNNI}_{\approx_{\rm mb}}$ by virtue of Theorem 10.3.
4. An immediate consequence of $\text{P\_BNDC}_{\approx_{\rm mw}} = \text{SBSNNI}_{\approx_{\rm mw}}$ and $\text{P\_BNDC}_{\approx_{\rm mb}} = \text{SBSNNI}_{\approx_{\rm mb}}$ as established by Theorem 10.3.

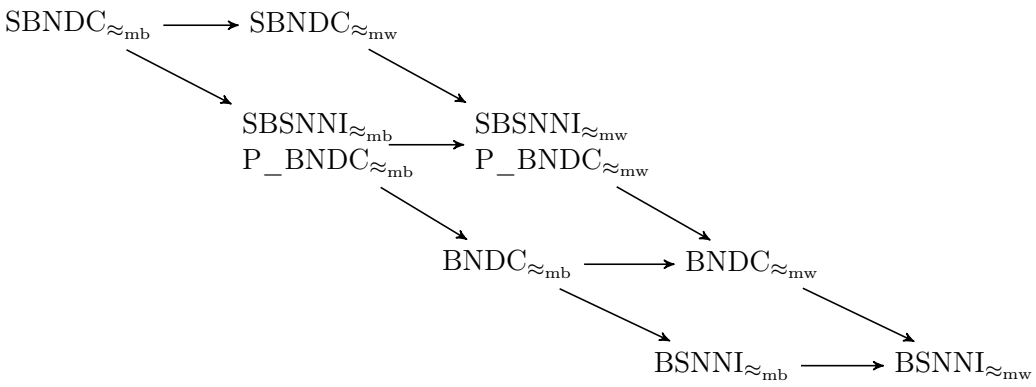


Figure 10.2: Taxonomy of security properties based on Markovian weak and branching bisimilarities

5. Since the only high-level action occurring in Q is h, in the proof of $Q \in \text{SBNDC}_{\approx_{\rm mw}}$ the only interesting case is the transition $Q \xrightarrow{h}_{\rm a} P_2$, for which it holds that $Q \setminus \mathcal{A}_{\mathcal{H}} \approx_{\rm mw} P_1 \approx_{\rm mw} P_2 \approx_{\rm mw} P_2 \setminus \mathcal{A}_{\mathcal{H}}$, i.e., $Q \setminus \mathcal{A}_{\mathcal{H}} \approx_{\rm mw} P_2 \setminus \mathcal{A}_{\mathcal{H}}$ as $\approx_{\rm mw}$ is transitive.
On the other hand, $Q \notin \text{SBNDC}_{\approx_{\rm mb}}$ because $P_1 \not\approx_{\rm mb} P_2$ in the same situation as before. ■

The diagram in Figure 10.2 summarizes the inclusions among the various noninterference properties based on the results in Theorems 10.3 and 10.4, where $\mathcal{P} \to \mathcal{Q}$ means that $\mathcal{P}$ is strictly included in $\mathcal{Q}$. These inclusions follow the same pattern as the nondeterministic and probabilistic settings in Figures 8.4 and 9.2. The arrows missing in the diagram, witnessing incomparability, are justified by the same counterexamples as those after Proposition 8.3. As an additional counterexample, for BNDC$_{\approx_{\rm mw}}$ vs. BSNNI$_{\approx_{\rm mb}}$ we have that the process $l\,.\,(2{\cdot}\lambda)\,.\,\underline{0}{+}l\,.\,((\lambda)\,.\,h_1\,.\,l_1\,.\,\underline{0}{+}(\lambda)\,.\,h_2\,.\,l_2\,.\,\underline{0}) + l\,.\,((\lambda)\,.\,l_1\,.\,\underline{0} + (\lambda)\,.\,l_2\,.\,\underline{0})$ is BSNNI$_{\approx_{\rm mb}}$ but not BNDC$_{\approx_{\rm mw}}$ as discussed in Section 10.2, while the process Q mentioned in Theorem 10.5 is both BSNNI$_{\approx_{\rm mw}}$ and BNDC$_{\approx_{\rm mw}}$ but not BSNNI$_{\approx_{\rm mb}}$.

Like in the nondeterministic and probabilistic settings of the two previous chapters, the strongest property based on weak Markovian bisimilarity (SBNDC$_{\approx_{\rm mw}}$) and the weakest property based on Markovian branching bisimilarity (BSNNI$_{\approx_{\rm mb}}$) are incomparable too. The former is a very restrictive property because it requires a local check every time a high-level action is performed, while the latter requires a check only on the initial state. On the other hand, as shown in Theorem 10.5, it is very easy to construct processes that are secure under properties based on $\approx_{\rm mw}$ but not on $\approx_{\rm mb}$, due to the minimal number of high-level actions in Q.

10.2.3 Relating Nondeterministic, Probabilistic, and Markovian Taxonomies

Let us compare our Markovian taxonomy with the nondeterministic and probabilistic ones of the two previous chapters. In the following, we assume that $\approx_{\rm w}$ denotes the weak nondeterministic bisimilarity of [112] and $\approx_{\rm b}$ denotes the nondeterministic branching bisimilarity of [80], which we have used in Chapter 8. These can also be obtained from the corresponding definitions in Section 10.1.2 by ignoring the clause involving the *rate* function. Since we are abstracting from time, given a process $P \in \mathbb{P}_{\rm mk}$ we can obtain its nondeterministic variant, denoted by $nd(P)$, by replacing every occurrence of $(\lambda)\,.\,P'$ with $\tau\,.\,P'$. However, to respect maximal progress, first we

have to eliminate every subprocess starting with a rate prefix that is alternative to a subprocess starting with a τ-prefix. To accomplish this transformation syntactically, we focus on the set $\mathbb{P}_{\rm mk,seq}$ of sequential processes, i.e., without parallel composition; this is not too restrictive because, in the absence of recursion, parallel composition can be eliminated by repeatedly applying a Markovian variant of the expansion law [90].

The next proposition states that if two sequential processes are equivalent according to any of the weak bisimilarities in Section 10.1.2, then their nondeterministic variants are equivalent according to the corresponding nondeterministic weak bisimilarity. The inverse does not hold; e.g., processes $P_1 = (1) \,.\, a \,.\, \underline{0}$ and $P_2 = (2) \,.\, a \,.\, \underline{0}$ are such that $P_1 \not\approx_{\rm mw} P_2$ and $P_1 \not\approx_{\rm mb} P_2$, but their nondeterministic counterparts coincide as both of them are equal to $\tau \,.\, a \,.\, \underline{0}$.

Proposition 10.3. *Let $P_1, P_2 \in \mathbb{P}_{\rm mk,seq}$. Then:*

- $P_1 \approx_{\rm mw} P_2 \Longrightarrow nd(P_1) \approx_{\rm w} nd(P_2)$.
- $P_1 \approx_{\rm mb} P_2 \Longrightarrow nd(P_1) \approx_{\rm b} nd(P_2)$.

Proof. We prove the two results separately:

- We need to prove that the symmetric relation $\mathcal{B} = \{(nd(P_1), nd(P_2)) \mid P_1 \approx_{\rm mw} P_2\}$ is a weak bisimulation. We start by observing that from $P_1 \approx_{\rm mw} P_2$ it follows that for each $P_1 \stackrel{a}{\longrightarrow}_{\rm a} P_1'$ there exists $P_2 \stackrel{\hat{a}}{\Longrightarrow}_{\rm a} P_2'$ such that $P_1' \approx_{\rm mw} P_2'$. Since $nd(P_1)$ and $nd(P_2)$ are obtained by eliminating every rate transition that is alternative to a τ-transition and replacing each remaining rate transition with a τ-transition, for each $nd(P_1) \stackrel{a}{\longrightarrow}_{\rm a} nd(P_1')$ there exists $nd(P_2) \stackrel{\hat{a}}{\Longrightarrow}_{\rm a} nd(P_2')$ such that $(nd(P_1'), nd(P_2')) \in \mathcal{B}$.
- We need to prove that the symmetric relation $\mathcal{B} = \{nd(P_1), nd(P_2)) \mid P_1 \approx_{\rm mb} P_2\}$ is a branching bisimulation. We start by observing that from $P_1 \approx_{\rm mb} P_2$ it follows that for each $P_1 \stackrel{a}{\longrightarrow}_{\rm a} P_1'$ either $a = \tau$ and $P_1' \approx_{\rm mb} P_2$, or there exists $P_2 \stackrel{\tau^*}{\Longrightarrow}_{\rm a} \bar{P}_2 \stackrel{a}{\longrightarrow}_{\rm a} P_2'$ such that $P_1 \approx_{\rm mb} \bar{P}_2$ and $P_1' \approx_{\rm mb} P_2'$. Since $nd(P_1)$ and $nd(P_2)$ are obtained by eliminating every rate transition that is alternative to a τ-transition and replacing each remaining rate transition with a τ-transition, for each $nd(P_1) \stackrel{a}{\longrightarrow}_{\rm a} nd(P_1')$ either $a = \tau$ and $(nd(P_1'), nd(P_2)) \in \mathcal{B}$, or there exists $nd(P_2) \stackrel{\tau^*}{\Longrightarrow}_{\rm a} nd(\bar{P}_2) \stackrel{a}{\longrightarrow}_{\rm a} nd(P_2')$ such that $(nd(P_1), nd(\bar{P}_2)) \in \mathcal{B}$ and $(nd(P_1'), nd(P_2')) \in \mathcal{B}$. ∎

An immediate consequence is that if a sequential process is secure under any of the Markovian noninterference properties of Section 10.2, then its nondeterministic variant is secure under the corresponding nondeterministic property. The taxonomy of Figure 10.2 thus extends to the left the one in Figure 8.4, as each of the properties of Section 10.2 is finer than its nondeterministic counterpart.

Corollary 10.1. *Let $\mathcal{P}_{\rm mk} \in \{{\rm BSNNI}_{\approx_{\rm mk}}, {\rm BNDC}_{\approx_{\rm mk}}, {\rm SBSNNI}_{\approx_{\rm mk}}, {\rm P\_BNDC}_{\approx_{\rm mk}}, {\rm SBNDC}_{\approx_{\rm mk}}\}$ and $\mathcal{P}_{\rm nd} \in \{{\rm BSNNI}_{\approx_{\rm nd}}, {\rm BNDC}_{\approx_{\rm nd}}, {\rm SBSNNI}_{\approx_{\rm nd}}, {\rm P\_BNDC}_{\approx_{\rm nd}}, {\rm SBNDC}_{\approx_{\rm nd}}\}$ for $\approx_{\rm mk} \in \{\approx_{\rm mw}, \approx_{\rm mb}\}$ and $\approx_{\rm nd} \in \{\approx_{\rm w}, \approx_{\rm b}\}$, where $\mathcal{P}_{\rm nd}$ is meant to be the nondeterministic variant of $\mathcal{P}_{\rm mk}$. Then $P \in \mathcal{P}_{\rm mk} \Longrightarrow nd(P) \in \mathcal{P}_{\rm nd}$ for all $P \in \mathbb{P}_{\rm mk,seq}$.*

Proof. The result directly follows from Proposition 10.1. ∎

We now compare our Markovian taxonomy with the probabilistic one of the previous chapter, which relies on the weak probabilistic bisimilarity $\approx_{\rm pw}$ of [120] and the probabilistic branching bisimilarity $\approx_{\rm pb}$ of [8], also obtainable from the corresponding definitions in Section 10.1.2 by replacing the clause involving the *rate* function with the clause involving the *prob* function. We focus on the set $\mathbb{P}_{\rm mk,alt,seq}$ of processes in which action prefixes and rate prefixes alternate – to comply with the strictly alternating model of [86] adopted for probabilistic processes – that are sequential – as rate transitions, as opposed to probabilistic ones, do not synchronize. Since we are abstracting from time, given a process $P \in \mathbb{P}_{\rm mk,alt,seq}$ we can obtain its probabilistic variant, denoted by $pr(P)$, by replacing every occurrence of $\sum_{i\in I}(\lambda_i) \,.\, P_i$ with $\bigoplus_{i\in I}[p_i]pr(P_i)$ where $p_i = \lambda_i / \sum_{j\in I} \lambda_j$. It is worth noting that over $\mathbb{P}_{\rm mk,alt,seq}$ the weak bisimilarities $\approx_{\rm mw}$ and $\approx_{\rm mb}$ boil down to the strong bisimilarity $\sim_{\rm m}$ of Definition 10.2. This is due to the strict alternation between action prefixes and rate prefixes and the fact that the two weak bisimilarities do not abstract from rate transitions ($\approx_{\rm pw}$ and $\approx_{\rm pb}$ can abstract from probabilistic transitions).

The next proposition states that if two sequential alternating processes are equivalent according to any of the weak bisimilarities in Section 10.1.2, then their probabilistic variants are equivalent according to the corresponding probabilistic weak bisimilarity. The inverse does not hold; e.g., the probabilistic counterparts of the two inequivalent processes $(1) \,.\, a \,.\, \underline{0}$ and $(2) \,.\, a \,.\, \underline{0}$ coincide as both of them are equal to $[1]a \,.\, \underline{0}$.

Proposition 10.4. *Let $P_1, P_2 \in \mathbb{P}_{\rm mk,alt,seq}$. Then:*

- $P_1 \approx_{\rm mw} P_2 \Longrightarrow pr(P_1) \approx_{\rm pw} pr(P_2)$.
- $P_1 \approx_{\rm mb} P_2 \Longrightarrow pr(P_1) \approx_{\rm pb} pr(P_2)$.

Proof. We prove the two results separately:

- We need to prove that the equivalence relation $\mathcal{B} = \{(pr(P_1), pr(P_2)) \mid P_1 \approx_{\rm mw} P_2\}$ is a weak probabilistic bisimulation.
  As for action transitions, we start by observing that from $P_1 \approx_{\rm mw} P_2$ it follows that for each $P_1 \xrightarrow{a}_{\rm a} P_1'$ there exists $P_2 \xrightarrow{a}_{\rm a} P_2'$ – due to the strict alternation – such that $P_1' \approx_{\rm mw} P_2'$. Since $pr(P_1)$ and $pr(P_2)$ are obtained by replacing each rate transition with a probabilistic one, for each $pr(P_1) \xrightarrow{a}_{\rm a} pr(P_1')$ there exists $pr(P_2) \xrightarrow{a}_{\rm a} pr(P_2')$ such that $(pr(P_1'), pr(P_2')) \in \mathcal{B}$.
  As for probabilities, for each $P \xrightarrow{\gamma}_{\rm r} P'$ there exists $pr(P) \xrightarrow{p}_{\rm p} pr(P')$ with $p = \gamma / \sum_{P \xrightarrow{\delta}_{\rm r} Q} \delta$. Due to the strict alternation, from $P_1 \approx_{\rm mw} P_2$ it follows that $\sum_{P_1 \xrightarrow{\lambda}_{\rm r} P_1', P_1' \in C} \lambda = \sum_{P_2 \xrightarrow{\mu}_{\rm r} P_2', P_2' \in C} \mu$ for each $C \in \mathbb{P}_{\rm mk} / \approx_{\rm mw}$ and hence $\sum_{P_1 \xrightarrow{\lambda}_{\rm r} P_1'} \lambda = \sum_{P_2 \xrightarrow{\mu}_{\rm r} P_2'} \mu$. Since every equivalence class $C' \in \mathbb{P}_{\rm pr,seq} / \mathcal{B}$ is of the form $[pr(Q)]_{\mathcal{B}} = \{pr(Q') \mid Q \approx_{\rm mw} Q'\}$, we have that $\sum_{pr(P_1) \xrightarrow{p}_{\rm p} pr(P_1'), pr(P_1') \in C'} p = \sum_{pr(P_2) \xrightarrow{q}_{\rm p} pr(P_2'), pr(P_2') \in C'} q$ where every p and every q is obtained from the corresponding rate ratios respectively involving λ and μ.
- We need to prove that the equivalence relation $\mathcal{B} = \{(pr(P_1), pr(P_2)) \mid P_1 \approx_{\rm mb} P_2\}$ is a probabilistic branching bisimulation.
  As for action transitions, we start by observing that from $P_1 \approx_{\rm mb} P_2$ it follows that for each $P_1 \xrightarrow{a}_{\rm a} P_1'$ either $a = \tau$ and $P_1' \approx_{\rm mb} P_2$, or there exists $P_2 \xRightarrow{\tau^*}_{\rm a} P_2 \xrightarrow{a}_{\rm a} P_2'$ – due to the strict alternation – such that $P_1' \approx_{\rm mb} P_2'$. Since $pr(P_1)$ and $pr(P_2)$ are obtained by replacing each rate transition with a probabilistic one, for each $pr(P_1) \xrightarrow{a}_{\rm a} pr(P_1')$ either $a = \tau$ and $(pr(P_1'), pr(P_2)) \in \mathcal{B}$, or there exists $pr(P_2) \xRightarrow{\tau^*}_{\rm a} pr(P_2) \xrightarrow{a}_{\rm a} pr(P_2')$ such that $(pr(P_1'), pr(P_2')) \in \mathcal{B}$.
  As for probabilities, we reason like in the proof of the corresponding result for $\approx_{\rm pw}$. ∎

An immediate consequence is that if a sequential alternating process is secure under any of the Markovian noninterference properties of Section 10.2, then its probabilistic variant is secure under the corresponding probabilistic property. The taxonomy of Figure 10.2 thus extends to the left also the one in Figure 9.2, as each of the properties of Section 10.2 is finer than its probabilistic counterpart.

Corollary 10.2. *Let* $\mathcal{P}_{\rm mk} \in \{\mathrm{BSNNI}_{\approx_{\rm mk}}, \mathrm{BNDC}_{\approx_{\rm mk}}, \mathrm{SBSNNI}_{\approx_{\rm mk}}, \mathrm{P\_BNDC}_{\approx_{\rm mk}}, \mathrm{SBNDC}_{\approx_{\rm mk}}\}$ *and* $\mathcal{P}_{\rm pr} \in \{\mathrm{BSNNI}_{\approx_{\rm pr}}, \mathrm{BNDC}_{\approx_{\rm pr}}, \mathrm{SBSNNI}_{\approx_{\rm pr}}, \mathrm{P\_BNDC}_{\approx_{\rm pr}}, \mathrm{SBNDC}_{\approx_{\rm pr}}\}$ *for* $\approx_{\rm mk} \in \{\approx_{\rm mw}, \approx_{\rm mb}\}$ *and* $\approx_{\rm pr} \in \{\approx_{\rm pw}, \approx_{\rm pb}\}$*, where* $\mathcal{P}_{\rm pr}$ *is meant to be the probabilistic variant of* $\mathcal{P}_{\rm mk}$*. Then* $P \in \mathcal{P}_{\rm mk} \Longrightarrow pr(P) \in \mathcal{P}_{\rm pr}$ *for all* $P \in \mathbb{P}_{\rm mk,alt,seq}$*.*

Proof. The result directly follows from Proposition 10.2. ∎

10.3 Reversibility via Weak Markovian Back-and-Forth Bisimilarity

As recalled in the two previous chapters, weak back-and-forth bisimilarity coincides with branching bisimilarity over nodeterministic processes [57]. In this section we extend that result so that Markovian branching bisimilarity can be employed in the noninterference analysis of reversible processes featuring nondeterminism and stochastic time.

An MLTS $(\mathcal{S}, \mathcal{A}, \longrightarrow)$ represents a reversible process if each of its transitions is seen as bidirectional. When going backward, it is of paramount importance to respect causality, i.e., the last performed transition must be the first one to be undone. Following [57] we set up an equivalence that enforces not only causality but also history preservation. This means that, when going backward, a process can only move along the path representing the history that brought the process to the current state even in the presence of concurrency. To accomplish this, the equivalence has to be defined over computations, not over states, and the notion of transition has to be suitably revised. We start by adapting the notation of the nondeterministic setting of [57] to our nondeterministic and stochastically timed setting. We use ℓ for a label in $\mathcal{A} \cup \mathbb{R}_{>0}$.

Definition 10.8. *A sequence* $\xi = (s_0, \ell_1, s_1)(s_1, \ell_2, s_2) \ldots (s_{n-1}, \ell_n, s_n) \in \longrightarrow^*$ *is a* path *of length* n *from state* s_0*. We let* $first(\xi) = s_0$ *and* $last(\xi) = s_n$*; the empty path is indicated with* ε*. We denote by* $path(s)$ *the set of paths from* s*.* ∎

Definition 10.9. *A pair* $\rho = (s, \xi)$ *is called a* run *from state* s *iff* $\xi \in path(s)$*, in which case we let* $path(\rho) = \xi$*,* $first(\rho) = first(\xi) = s$*,* $last(\rho) = last(\xi)$*, with* $first(\rho) = last(\rho) = s$ *when* $\xi = \varepsilon$*. We denote by* $run(s)$ *the set of runs from state* s*. Given* $\rho = (s, \xi) \in run(s)$ *and* $\rho' = (s', \xi') \in run(s')$*, their composition* $\rho\rho' = (s, \xi\xi') \in run(s)$ *is defined iff* $last(\rho) = first(\rho') = s'$*. We write* $\rho \stackrel{\ell}{\longrightarrow} \rho'$ *iff there exists* $\rho'' = (\bar{s}, (\bar{s}, \ell, s'))$ *with* $\bar{s} = last(\rho)$ *such that* $\rho' = \rho\rho''$*; note that* $first(\rho) = first(\rho')$*. Moreover rate is lifted in the expected way.* ∎

In the considered MLTS we work with the set $\mathcal{U}$ of runs in lieu of $\mathcal{S}$. Following [57], given a run ρ, we distinguish between outgoing and incoming action transitions of ρ during the weak bisimulation game. Like in [32], this does not apply to rate transitions, in the sense that the cumulative rates of incoming rate transitions are not compared. It this were not the case, states like $(\lambda_1) \,.\, (\underline{0} \setminus \emptyset) + (\lambda_2) \,.\, (\underline{0} \,/\, \emptyset)$ and $(\lambda_1 + \lambda_2) \,.\, \underline{0}$ – which are indistinguishable in the forward direction – would be told apart because the incoming cumulative rate from the class formed by those two states is λ_1, λ_2, or $\lambda_1 + \lambda_2$ depending on whether $\underline{0} \setminus \emptyset$, $\underline{0} \,/\, \emptyset$, or $\underline{0}$ is considered. When comparing the cumulative rates of outgoing transitions, we slightly deviate from the corresponding clause in Definition 10.4 to set up a more

symmetric clause inspired by an alternative characterization of $\approx_{\rm mw}$ in [90] that is helpful to prove the forthcoming Lemma 10.4.

Definition 10.10. *Let $(\mathcal{S}, \mathcal{A}, \longrightarrow)$ be an MLTS. We say that $s_1, s_2 \in \mathcal{S}$ are* weakly Markovian back-and-forth bisimilar*, written $s_1 \approx_{\rm mbf} s_2$, iff $((s_1, \varepsilon), (s_2, \varepsilon)) \in \mathcal{B}$ for some weak Markovian back-and-forth bisimulation $\mathcal{B}$. An equivalence relation $\mathcal{B}$ over $\mathcal{U}$ is a* weak Markovian back-and-forth bisimulation *iff, whenever $(\rho_1, \rho_2) \in \mathcal{B}$, then:*

- *For each $\rho_1 \xrightarrow{a}_{\rm a} \rho_1'$ there exists $\rho_2 \stackrel{\hat{a}}{\Longrightarrow}_{\rm a} \rho_2'$ such that $(\rho_1', \rho_2') \in \mathcal{B}$.*
- *For each $\rho_1' \xrightarrow{a}_{\rm a} \rho_1$ there exists $\rho_2' \stackrel{\hat{a}}{\Longrightarrow}_{\rm a} \rho_2$ such that $(\rho_1', \rho_2') \in \mathcal{B}$.*
- *For each $\rho_1 \stackrel{\tau^*}{\Longrightarrow}_{\rm a} \rho_1'$ with $\rho_1' \stackrel{\tau}{\not\longrightarrow}_{\rm a}$ there exists $\rho_2 \stackrel{\tau^*}{\Longrightarrow}_{\rm a} \rho_2'$ with $\rho_2' \stackrel{\tau}{\not\longrightarrow}_{\rm a}$ such that $(\rho_1', \rho_2') \in \mathcal{B}$ and $rate(\rho_1', C) = rate(\rho_2', C)$ for all equivalence classes $C \in \mathcal{U}/\mathcal{B}$.*
- *For each $\rho_1' \xrightarrow{\lambda_1}_{\rm r} \rho_1$ with $\rho_1' \stackrel{\tau}{\not\longrightarrow}_{\rm a}$ there exists $\rho_2' \stackrel{\tau^*}{\Longrightarrow}_{\rm a} \bar{\rho}_2' \xrightarrow{\lambda_2}_{\rm r} \bar{\rho}_2 \stackrel{\tau^*}{\Longrightarrow}_{\rm a} \rho_2$ with $\bar{\rho}_2' \stackrel{\tau}{\not\longrightarrow}_{\rm a}$ such that $(\rho_1, \bar{\rho}_2) \in \mathcal{B}$, $(\rho_1', \bar{\rho}_2') \in \mathcal{B}$, and $(\rho_1', \rho_2') \in \mathcal{B}$.* ■

We show that weak Markovian back-and-forth bisimilarity over runs coincides with $\approx_{\rm mb}$, the forward-only Markovian branching bisimilarity over states. Like in the previous chapter, we proceed by adopting the proof strategy followed in [57] to show that their weak back-and-forth bisimilarity over runs coincides with the forward-only branching bisimilarity over states of [80]. Therefore we start by proving that $\approx_{\rm mbf}$ satisfies the *cross property*. This means that, whenever two runs of two $\approx_{\rm mbf}$-equivalent states can perform a sequence of finitely many τ-transitions such that each of the two target runs is $\approx_{\rm mbf}$-equivalent to the source run of the other sequence, then the two target runs are $\approx_{\rm mbf}$-equivalent to each other as well.

Lemma 10.4. *Let $s_1, s_2 \in \mathcal{S}$ with $s_1 \approx_{\rm mbf} s_2$. For all $\rho_1', \rho_1'' \in run(s_1)$ such that $\rho_1' \stackrel{\tau^*}{\Longrightarrow}_{\rm a} \rho_1''$ and for all $\rho_2', \rho_2'' \in run(s_2)$ such that $\rho_2' \stackrel{\tau^*}{\Longrightarrow}_{\rm a} \rho_2''$, if $\rho_1' \approx_{\rm mbf} \rho_2''$ and $\rho_1'' \approx_{\rm mbf} \rho_2'$ then $\rho_1'' \approx_{\rm mbf} \rho_2''$.*

Proof. Given $s_1, s_2 \in \mathcal{S}$ with $s_1 \approx_{\rm mbf} s_2$, consider the transitive closure $\mathcal{B}^+$ of the reflexive and symmetric relation $\mathcal{B} = \approx_{\rm mbf} \cup \{(\rho_1'', \rho_2''), (\rho_2'', \rho_1'') \in (run(s_1) \times run(s_2)) \cup (run(s_2) \times run(s_1)) \mid \exists \rho_1' \in run(s_1), \rho_2' \in run(s_2).\ \rho_1' \stackrel{\tau^*}{\Longrightarrow}_{\rm a} \rho_1'' \wedge \rho_2' \stackrel{\tau^*}{\Longrightarrow}_{\rm a} \rho_2'' \wedge \rho_1' \approx_{\rm mbf} \rho_2'' \wedge \rho_1'' \approx_{\rm mbf} \rho_2'\}$. The result will follow by proving that $\mathcal{B}^+$ is a weak Markovian back-and-forth bisimulation, because this implies that $\rho_1'' \approx_{\rm mbf} \rho_2''$ for every additional pair – i.e., $\mathcal{B}^+$ satisfies the cross property – as well as $\mathcal{B}^+ = \approx_{\rm mbf}$ – hence $\approx_{\rm mbf}$ satisfies the cross property too.
Let $(\rho_1'', \rho_2'') \in \mathcal{B} \setminus \approx_{\rm mbf}$ to avoid trivial cases. Then there exist $\rho_1' \in run(s_1)$ and $\rho_2' \in run(s_2)$ such that $\rho_1' \stackrel{\tau^*}{\Longrightarrow}_{\rm a} \rho_1''$, $\rho_2' \stackrel{\tau^*}{\Longrightarrow}_{\rm a} \rho_2''$, $\rho_1' \approx_{\rm mbf} \rho_2''$, and $\rho_1'' \approx_{\rm mbf} \rho_2'$. There are two cases for action transitions:

- In the forward case, assume that $\rho_1'' \xrightarrow{a}_{\rm a} \rho_1'''$, from which we derive $\rho_1' \stackrel{\tau^*}{\Longrightarrow}_{\rm a} \rho_1'' \xrightarrow{a}_{\rm a} \rho_1'''$. From $\rho_1' \approx_{\rm mbf} \rho_2''$ it follows that there exists $\rho_2'' \stackrel{\tau^*}{\Longrightarrow}_{\rm a} \rho_2'''$ if $a = \tau$ or $\rho_2'' \stackrel{\tau^*}{\Longrightarrow}_{\rm a} \xrightarrow{a}_{\rm a} \stackrel{\tau^*}{\Longrightarrow}_{\rm a} \rho_2'''$ if $a \neq \tau$, such that $\rho_1''' \approx_{\rm mbf} \rho_2'''$ and hence $(\rho_1''', \rho_2''') \in \mathcal{B}$.
  When starting from $\rho_2'' \xrightarrow{a}_{\rm a} \rho_2'''$, we exploit $\rho_2' \stackrel{\tau^*}{\Longrightarrow}_{\rm a} \rho_2''$ and $\rho_1'' \approx_{\rm mbf} \rho_2'$ instead.
- In the backward case, assume that $\rho_1''' \xrightarrow{a}_{\rm a} \rho_1''$. From $\rho_1'' \approx_{\rm mbf} \rho_2'$ it follows that there exists $\rho_2''' \stackrel{\tau^*}{\Longrightarrow}_{\rm a} \rho_2'$ if $a = \tau$, so that $\rho_2''' \stackrel{\tau^*}{\Longrightarrow}_{\rm a} \rho_2''$, or $\rho_2''' \stackrel{\tau^*}{\Longrightarrow}_{\rm a} \xrightarrow{a} \stackrel{\tau^*}{\Longrightarrow}_{\rm a} \rho_2'$ if $a \neq \tau$, so that $\rho_2''' \stackrel{\tau^*}{\Longrightarrow}_{\rm a} \xrightarrow{a}_{\rm a} \stackrel{\tau^*}{\Longrightarrow}_{\rm a} \rho_2''$, such that $\rho_1''' \approx_{\rm mbf} \rho_2'''$ and hence $(\rho_1''', \rho_2''') \in \mathcal{B}$.
  When starting from $\rho_2''' \xrightarrow{a}_{\rm a} \rho_2''$, we exploit $\rho_1' \approx_{\rm mbf} \rho_2''$ and $\rho_1' \stackrel{\tau^*}{\Longrightarrow}_{\rm a} \rho_1''$ instead.

Likewise, there are two cases for rate transitions:

- In the forward case, assume that $\rho_1'' \stackrel{\tau^*}{\Longrightarrow}_{\rm a} \rho_1'''$ with $\rho_1''' \stackrel{\tau}{\not\longrightarrow}_{\rm a}$, from which we derive $\rho_1' \stackrel{\tau^*}{\Longrightarrow}_{\rm a} \rho_1'''$. From $\rho_1' \approx_{\rm mbf} \rho_2''$ it follows that there exists $\rho_2'' \stackrel{\tau^*}{\Longrightarrow}_{\rm a} \rho_2'''$ with $\rho_2''' \stackrel{\tau}{\not\longrightarrow}_{\rm a}$ such that $\rho_1''' \approx_{\rm mbf} \rho_2'''$ and $rate(\rho_1''', C) = rate(\rho_2''', C)$ for all $C \in \mathcal{U}/\!\approx_{\rm mbf}$. Since every equivalence class $C' \in \mathcal{U}/\mathcal{B}^+$ is the union of equivalence classes with respect to $\approx_{\rm mbf}$, it holds that $rate(\rho_1''', C') = rate(\rho_2''', C')$.
  When starting from $\rho_2'' \stackrel{\tau^*}{\Longrightarrow}_{\rm a} \rho_2'''$ with $\rho_2''' \stackrel{\tau}{\not\longrightarrow}_{\rm a}$, we exploit $\rho_2' \stackrel{\tau^*}{\Longrightarrow}_{\rm a} \rho_2''$ and $\rho_1'' \approx_{\rm mbf} \rho_2'$ instead.

- In the backward case, assume that $\rho_1''' \stackrel{\lambda_1}{\longrightarrow}_{\rm r} \rho_1''$ with $\rho_1''' \stackrel{\tau}{\not\longrightarrow}_{\rm a}$. From $\rho_1'' \approx_{\rm mbf} \rho_2'$ it follows that there exists $\rho_2''' \stackrel{\tau^*}{\Longrightarrow}_{\rm a} \bar\rho_2''' \stackrel{\lambda_2}{\longrightarrow}_{\rm r} \bar\rho_2' \stackrel{\tau^*}{\Longrightarrow}_{\rm a} \rho_2'$ with $\bar\rho_2''' \stackrel{\tau}{\not\longrightarrow}_{\rm a}$, so $\rho_2''' \stackrel{\tau^*}{\Longrightarrow}_{\rm a} \bar\rho_2''' \stackrel{\lambda_2}{\longrightarrow}_{\rm r} \bar\rho_2' \stackrel{\tau^*}{\Longrightarrow}_{\rm a} \rho_2''$ with $\bar\rho_2''' \stackrel{\tau}{\not\longrightarrow}_{\rm a}$, such that $\rho_1'' \approx_{\rm mbf} \bar\rho_2'$, $\rho_1''' \approx_{\rm mbf} \bar\rho_2'''$, and $\rho_1''' \approx_{\rm mbf} \rho_2'''$, hence $(\rho_1'', \bar\rho_2') \in \mathcal{B}$, $(\rho_1''', \bar\rho_2''') \in \mathcal{B}$, and $(\rho_1''', \rho_2''') \in \mathcal{B}$.
  When starting from $\rho_2''' \stackrel{\lambda_2}{\longrightarrow}_{\rm r} \rho_2''$ with $\rho_2''' \stackrel{\tau}{\not\longrightarrow}_{\rm a}$, we exploit $\rho_1' \approx_{\rm mbf} \rho_2''$ and $\rho_1' \stackrel{\tau^*}{\Longrightarrow}_{\rm a} \rho_1''$ instead. ∎

Theorem 10.6. *Let $s_1, s_2 \in \mathcal{S}$. Then $s_1 \approx_{\rm mbf} s_2 \iff s_1 \approx_{\rm mb} s_2$.*

Proof. The proof is divided into two parts:

- Suppose that $s_1 \approx_{\rm mbf} s_2$ and let $\mathcal{B}$ be a weak Markovian back-and-forth bisimulation over $\mathcal{U}$ such that $((s_1, \varepsilon), (s_2, \varepsilon)) \in \mathcal{B}$. Assume that $\mathcal{B}$ only contains all the pairs of $\approx_{\rm mbf}$-equivalent runs from s_1 and s_2, so that Lemma 10.4 is applicable to $\mathcal{B}$. We show that $\mathcal{B}' = \{(last(\rho_1), last(\rho_2)) \mid (\rho_1, \rho_2) \in \mathcal{B}\}$ is a Markovian branching bisimulation over the states in $\mathcal{S}$ reachable from s_1 and s_2, from which $s_1 \approx_{\rm mb} s_2$ will follow. Note that $\mathcal{B}'$ is an equivalence relation because so is $\mathcal{B}$.
  Given $(last(\rho_1), last(\rho_2)) \in \mathcal{B}'$, by definition of $\mathcal{B}'$ we have that $(\rho_1, \rho_2) \in \mathcal{B}$. Let $r_k = last(\rho_k)$ for $k \in \{1, 2\}$, so that $(r_1, r_2) \in \mathcal{B}'$. Suppose that $r_1 \stackrel{a}{\longrightarrow}_{\rm a} r_1'$, i.e., $\rho_1 \stackrel{a}{\longrightarrow}_{\rm a} \rho_1'$ where $last(\rho_1') = r_1'$. There are two cases:

  - If $a = \tau$ then from $(\rho_1, \rho_2) \in \mathcal{B}$ it follows that there exists $\rho_2 \stackrel{\tau^*}{\Longrightarrow}_{\rm a} \rho_2'$ such that $(\rho_1', \rho_2') \in \mathcal{B}$. This means that we have a sequence of $n \geq 0$ transitions of the form $\rho_{2,i} \stackrel{\tau}{\longrightarrow}_{\rm a} \rho_{2,i+1}$ for all $0 \leq i \leq n-1$ where $\rho_{2,0}$ is ρ_2 while $\rho_{2,n}$ is ρ_2' so that $(\rho_1', \rho_{2,n}) \in \mathcal{B}$ as $(\rho_1', \rho_2') \in \mathcal{B}$.
    If $n = 0$ then we are done because ρ_2' is ρ_2 and hence $(\rho_1', \rho_2) \in \mathcal{B}$ as $(\rho_1', \rho_2') \in \mathcal{B}$ – thus $(r_1', r_2) \in \mathcal{B}'$ – otherwise from $\rho_{2,n}$ we go back to $\rho_{2,n-1}$ via $\rho_{2,n-1} \stackrel{\tau}{\longrightarrow}_{\rm a} \rho_{2,n}$. Recalling that $(\rho_1', \rho_{2,n}) \in \mathcal{B}$, if ρ_1' can respond by staying idle, so that $(\rho_1', \rho_{2,n-1}) \in \mathcal{B}$, and $n = 1$, then we are done because $\rho_{2,n-1}$ is ρ_2 and hence $(\rho_1', \rho_2) \in \mathcal{B}$ as $(\rho_1', \rho_{2,n-1}) \in \mathcal{B}$ – thus $(r_1', r_2) \in \mathcal{B}'$ – otherwise we go further back to $\rho_{2,n-2}$ via $\rho_{2,n-2} \stackrel{\tau}{\longrightarrow}_{\rm a} \rho_{2,n-1}$. If ρ_1' can respond by staying idle, so that $(\rho_1', \rho_{2,n-2}) \in \mathcal{B}$, and $n = 2$, then we are done because $\rho_{2,n-2}$ is ρ_2 and hence $(\rho_1', \rho_2) \in \mathcal{B}$ as $(\rho_1', \rho_{2,n-2}) \in \mathcal{B}$ – thus $(r_1', r_2) \in \mathcal{B}'$ – otherwise we keep going backward.
    By repeating this procedure, since $(\rho_1', \rho_{2,n}) \in \mathcal{B}$ either we get to $(\rho_1', \rho_{2,n-n}) \in \mathcal{B}$ and we are done because this implies that $(\rho_1', \rho_2) \in \mathcal{B}$ – thus $(r_1', r_2) \in \mathcal{B}'$ – or for some $0 < m \leq n$ such that $(\rho_1', \rho_{2,m}) \in \mathcal{B}$ the incoming transition $\rho_{2,m-1} \stackrel{\tau}{\longrightarrow}_{\rm a} \rho_{2,m}$ is matched by $\bar\rho_1 \stackrel{\tau^*}{\Longrightarrow}_{\rm a} \rho_1 \stackrel{\tau}{\longrightarrow}_{\rm a} \rho_1'$ with $(\bar\rho_1, \rho_{2,m-1}) \in \mathcal{B}$. In the latter case, since $\bar\rho_1 \stackrel{\tau^*}{\Longrightarrow}_{\rm a} \rho_1$, $\rho_2 \stackrel{\tau^*}{\Longrightarrow}_{\rm a} \rho_{2,m-1}$, $(\bar\rho_1, \rho_{2,m-1}) \in \mathcal{B}$, and $(\rho_1, \rho_2) \in \mathcal{B}$, from Lemma 10.4 we derive that $(\rho_1, \rho_{2,m-1}) \in \mathcal{B}$. Consequently $\rho_2 \stackrel{\tau^*}{\Longrightarrow}_{\rm a} \rho_{2,m-1} \stackrel{\tau}{\longrightarrow}_{\rm a} \rho_{2,m}$ with $(\rho_1, \rho_{2,m-1}) \in \mathcal{B}$ and $(\rho_1', \rho_{2,m}) \in \mathcal{B}$, thus $r_2 \stackrel{\tau^*}{\Longrightarrow}_{\rm a} last(\rho_{2,m-1}) \stackrel{\tau}{\longrightarrow}_{\rm a} last(\rho_{2,m})$ with $(r_1, last(\rho_{2,m-1})) \in \mathcal{B}'$ and $(r_1', last(\rho_{2,m})) \in \mathcal{B}'$.

– If $a \neq \tau$ then from $(\rho_1, \rho_2) \in \mathcal{B}$ it follows that there exists $\rho_2 \stackrel{\tau^*}{\Longrightarrow}_{\rm a} \bar{\rho}_2 \stackrel{a}{\longrightarrow}_{\rm a} \bar{\rho}_2' \stackrel{\tau^*}{\Longrightarrow}_{\rm a} \rho_2'$ such that $(\rho_1', \rho_2') \in \mathcal{B}$.
From $(\rho_1', \rho_2') \in \mathcal{B}$ and $\bar{\rho}_2' \stackrel{\tau^*}{\Longrightarrow}_{\rm a} \rho_2'$ it follows that there exists $\bar{\rho}_1' \stackrel{\tau^*}{\Longrightarrow}_{\rm a} \rho_1'$ such that $(\bar{\rho}_1', \bar{\rho}_2') \in \mathcal{B}$. Since $\rho_1 \stackrel{a}{\longrightarrow}_{\rm a} \rho_1'$ and hence the last transition in ρ_1' is labeled with a, we derive that $\bar{\rho}_1'$ is ρ_1' and hence $(\rho_1', \bar{\rho}_2') \in \mathcal{B}$.
From $(\rho_1', \bar{\rho}_2') \in \mathcal{B}$ and $\bar{\rho}_2 \stackrel{a}{\longrightarrow}_{\rm a} \bar{\rho}_2'$ it follows that there exists $\bar{\rho}_1 \stackrel{\tau^*}{\Longrightarrow}_{\rm a} \rho_1 \stackrel{a}{\longrightarrow}_{\rm a} \rho_1'$ such that $(\bar{\rho}_1, \bar{\rho}_2) \in \mathcal{B}$. Since $\bar{\rho}_1 \stackrel{\tau^*}{\Longrightarrow}_{\rm a} \rho_1$, $\rho_2 \stackrel{\tau^*}{\Longrightarrow}_{\rm a} \bar{\rho}_2$, $(\bar{\rho}_1, \bar{\rho}_2) \in \mathcal{B}$, and $(\rho_1, \rho_2) \in \mathcal{B}$, from Lemma 10.4 we derive that $(\rho_1, \bar{\rho}_2) \in \mathcal{B}$. Consequently $\rho_2 \stackrel{\tau^*}{\Longrightarrow}_{\rm a} \bar{\rho}_2 \stackrel{a}{\longrightarrow}_{\rm a} \bar{\rho}_2'$ with $(\rho_1, \bar{\rho}_2) \in \mathcal{B}$ and $(\rho_1', \bar{\rho}_2') \in \mathcal{B}$, thus $r_2 \stackrel{\tau^*}{\Longrightarrow}_{\rm a} \mathit{last}(\bar{\rho}_2) \stackrel{a}{\longrightarrow}_{\rm a} \mathit{last}(\bar{\rho}_2')$ with $(r_1, \mathit{last}(\bar{\rho}_2)) \in \mathcal{B}'$ and $(r_1', \mathit{last}(\bar{\rho}_2')) \in \mathcal{B}'$.

As for rates, given $\rho \in \mathit{run}(s_1) \cup \mathit{run}(s_2)$, the equivalence class C_ρ' with respect to $\mathcal{B}'$ is of the form $[\mathit{last}(\rho)]_{\mathcal{B}'} = \{\mathit{last}(\rho') \mid (\mathit{last}(\rho), \mathit{last}(\rho')) \in \mathcal{B}'\} = \mathit{last}(\{\rho' \mid (\rho, \rho') \in \mathcal{B}\}) = \mathit{last}([\rho]_{\mathcal{B}})$, i.e., $C_\rho' = \mathit{last}(C_\rho)$ for some equivalence class C_ρ with respect to $\mathcal{B}$, provided that function last is lifted from runs to sets of runs. Suppose that $r_1 \stackrel{\tau}{\not\longrightarrow}_{\rm a}$ so that $\rho_1 \stackrel{\tau^*}{\Longrightarrow}_{\rm a} \rho_1$ with $\rho_1 \stackrel{\tau}{\not\longrightarrow}_{\rm a}$. From $(\rho_1, \rho_2) \in \mathcal{B}$ it follows that there exists $\rho_2 \stackrel{\tau^*}{\Longrightarrow}_{\rm a} \rho_2'$ with $\rho_2' \stackrel{\tau}{\not\longrightarrow}_{\rm a}$ such that $(\rho_1, \rho_2') \in \mathcal{B}$ and $\mathit{rate}(\rho_1, C) = \mathit{rate}(\rho_2', C)$ for all $C \in \mathcal{U}/\mathcal{B}$. Thus there exists $r_2 \stackrel{\tau^*}{\Longrightarrow}_{\rm a} r_2'$ with $r_2' = \mathit{last}(\rho_2')$ and $r_2' \stackrel{\tau}{\not\longrightarrow}_{\rm a}$ such that $(r_1, r_2') \in \mathcal{B}'$ and $\mathit{rate}(r_1, C_\rho') = \mathit{rate}(\rho_1, C_\rho) = \mathit{rate}(\rho_2', C_\rho) = \mathit{rate}(r_2', C_\rho')$ for all equivalence classes C_ρ' with respect to $\mathcal{B}'$ such that $C_\rho' = \mathit{last}(C_\rho)$ for some equivalence class C_ρ with respect to $\mathcal{B}$.

- Suppose that $s_1 \approx_{\rm mb} s_2$ and let $\mathcal{B}$ be a Markovian branching bisimulation over $\mathcal{S}$ such that $(s_1, s_2) \in \mathcal{B}$. Assume that $\mathcal{B}$ only contains all the pairs of $\approx_{\rm mb}$-equivalent states reachable from s_1 and s_2. We show that the reflexive and transitive closure $\mathcal{B}'^*$ of $\mathcal{B}' = \{(\rho_1, \rho_2), (\rho_2, \rho_1) \in (\mathit{run}(s_1) \times \mathit{run}(s_2)) \cup (\mathit{run}(s_2) \times \mathit{run}(s_1)) \mid (\mathit{last}(\rho_1), \mathit{last}(\rho_2)) \in \mathcal{B}\}$ is a weak Markovian back-and-forth bisimulation over the runs in $\mathcal{U}$ from s_1 and s_2, from which $(s_1, \varepsilon) \approx_{\rm mbf} (s_2, \varepsilon)$, i.e., $s_1 \approx_{\rm mbf} s_2$, will follow.
Given $(\rho_1, \rho_2) \in \mathcal{B}'$, by definition of $\mathcal{B}'$ we have that $(\mathit{last}(\rho_1), \mathit{last}(\rho_2)) \in \mathcal{B}$. Let $r_k = \mathit{last}(\rho_k)$ for $k \in \{1, 2\}$, so that $(r_1, r_2) \in \mathcal{B}$. There are two cases for action transitions:

  – If $\rho_1 \stackrel{a}{\longrightarrow}_{\rm a} \rho_1'$, i.e., $r_1 \stackrel{a}{\longrightarrow}_{\rm a} r_1'$ where $r_1' = \mathit{last}(\rho_1')$, then either $a = \tau$ and $(r_1', r_2') \in \mathcal{B}$ where $r_2' = r_2$, or there exists $r_2 \stackrel{\tau^*}{\Longrightarrow}_{\rm a} \bar{r}_2 \stackrel{a}{\longrightarrow}_{\rm a} r_2'$ such that $(r_1, \bar{r}_2) \in \mathcal{B}$ and $(r_1', r_2') \in \mathcal{B}$. In both cases $\rho_2 \stackrel{\hat{a}}{\Longrightarrow}_{\rm a} \rho_2'$ where $\mathit{last}(\rho_2') = r_2'$, so that $(\rho_1', \rho_2') \in \mathcal{B}'$.
  – If $\rho_1' \stackrel{a}{\longrightarrow}_{\rm a} \rho_1$, i.e., $r_1' \stackrel{a}{\longrightarrow}_{\rm a} r_1$ where $r_1' = \mathit{last}(\rho_1')$, there are two subcases:
    * If ρ_1' is (s_1, ε), i.e., $r_1' \stackrel{a}{\longrightarrow}_{\rm a} r_1$ is $s_1 \stackrel{a}{\longrightarrow}_{\rm a} r_1$ and $\mathit{last}(\rho_1') = s_1$, then from $(s_1, s_2) \in \mathcal{B}$ it follows that either $a = \tau$ and $(r_1, r_2) \in \mathcal{B}$ where $r_2 = s_2$, or there exists $s_2 \stackrel{\tau^*}{\Longrightarrow}_{\rm a} \bar{r}_2 \stackrel{a}{\longrightarrow}_{\rm a} r_2$ such that $(s_1, \bar{r}_2) \in \mathcal{B}$ and $(r_1, r_2) \in \mathcal{B}$. In both cases $\rho_2' \stackrel{\hat{a}}{\Longrightarrow}_{\rm a} \rho_2$ where $\mathit{last}(\rho_2') = s_2$, so that $(\rho_1', \rho_2') \in \mathcal{B}'$.
    * If ρ_1' is not (s_1, ε) then from $(s_1, s_2) \in \mathcal{B}$ it follows that s_1 reaches r_1' with a sequence of moves that are $\mathcal{B}$-compatible with those with which s_2 reaches some r_2' such that $(r_1', r_2') \in \mathcal{B}$ as $\mathcal{B}$ only contains all the states reachable from s_1 and s_2. Therefore either $a = \tau$ and $(r_1, r_2') \in \mathcal{B}$ where $r_2' = r_2$, or there exists $r_2' \stackrel{\tau^*}{\Longrightarrow}_{\rm a} \bar{r}_2 \stackrel{a}{\longrightarrow}_{\rm a} r_2$ such that $(r_1', \bar{r}_2) \in \mathcal{B}$ and $(r_1, r_2) \in \mathcal{B}$. In both cases $\rho_2' \stackrel{\hat{a}}{\Longrightarrow}_{\rm a} \rho_2$ where $\mathit{last}(\rho_2') = r_2'$, so that $(\rho_1', \rho_2') \in \mathcal{B}'$.

Likewise, there are two cases for rate transitions:

- Given $\rho \in \mathit{run}(s_1) \cup \mathit{run}(s_2)$, the equivalence class C'_ρ with respect to $\mathcal{B}'^*$ is of the form $[\rho]_{\mathcal{B}'^*} = \{\rho' \in \mathit{run}(s_1) \cup \mathit{run}(s_2) \mid \mathit{last}(\rho') \in [\mathit{last}(\rho)]_{\mathcal{B}}\}$, i.e., C'_ρ corresponds to some equivalence class C_ρ with respect to $\mathcal{B}$. Suppose that $\rho_1 \stackrel{\tau^*}{\Longrightarrow}_{\mathrm{a}} \rho'_1$ with $\rho'_1 \stackrel{\tau}{\not\longrightarrow}_{\mathrm{a}}$ so that $r_1 \stackrel{\tau^*}{\Longrightarrow}_{\mathrm{a}} r'_1$ with $r'_1 = \mathit{last}(\rho'_1) \stackrel{\tau}{\not\longrightarrow}_{\mathrm{a}}$. From $(r_1, r_2) \in \mathcal{B}$ it follows that there exists $r_2 \stackrel{\tau^*}{\Longrightarrow}_{\mathrm{a}} \bar{r}_2$ such that $(r'_1, \bar{r}_2) \in \mathcal{B}$ and, since $r'_1 \stackrel{\tau}{\not\longrightarrow}_{\mathrm{a}}$, there exists $\bar{r}_2 \stackrel{\tau^*}{\Longrightarrow}_{\mathrm{a}} r'_2$ with $r'_2 \stackrel{\tau}{\not\longrightarrow}_{\mathrm{a}}$ such that $(r'_1, r'_2) \in \mathcal{B}$ and $\mathit{rate}(r'_1, C) = \mathit{rate}(r'_2, C)$ for all $C \in \mathcal{S}/\mathcal{B}$. Thus there exists $\rho_2 \stackrel{\tau^*}{\Longrightarrow}_{\mathrm{a}} \rho'_2$ with $\mathit{last}(\rho'_2) = r'_2$ and $\rho'_2 \stackrel{\tau}{\not\longrightarrow}_{\mathrm{a}}$ such that $(\rho'_1, \rho'_2) \in \mathcal{B}$ and $\mathit{rate}(\rho'_1, C'_\rho) = \mathit{rate}(\mathit{last}(\rho'_1), C_\rho) = \mathit{rate}(\mathit{last}(\rho'_2), C_\rho) = \mathit{rate}(\rho'_2, C'_\rho)$ for all equivalence classes C'_ρ with respect to $\mathcal{B}'^*$.
- If $\rho'_1 \stackrel{\lambda_1}{\longrightarrow}_{\mathrm{r}} \rho_1$ with $\rho'_1 \stackrel{\tau}{\not\longrightarrow}_{\mathrm{a}}$, i.e., $r'_1 \stackrel{\lambda_1}{\longrightarrow}_{\mathrm{r}} r_1$ where $r'_1 = \mathit{last}(\rho'_1) \stackrel{\tau}{\not\longrightarrow}_{\mathrm{a}}$, there are two subcases:
  - If ρ'_1 is (s_1, ε), i.e., $r'_1 \stackrel{\lambda_1}{\longrightarrow}_{\mathrm{r}} r_1$ is $s_1 \stackrel{\lambda_1}{\longrightarrow}_{\mathrm{r}} r_1$ and $\mathit{last}(\rho'_1) = s_1$, then from $(s_1, s_2) \in \mathcal{B}$ and $s_1 \stackrel{\tau}{\not\longrightarrow}_{\mathrm{a}}$ it follows that there exists $s_2 \stackrel{\tau^*}{\Longrightarrow}_{\mathrm{a}} \bar{r}'_2$ with $\bar{r}'_2 \stackrel{\tau}{\not\longrightarrow}_{\mathrm{a}}$ and $r_2 \in \mathit{reach}(\bar{r}'_2)$ such that $(r'_1, \bar{r}'_2) \in \mathcal{B}$, which in turn implies that there exists $\bar{r}'_2 \stackrel{\lambda_2}{\longrightarrow}_{\mathrm{r}} \bar{r}_2$ such that $(r_1, \bar{r}_2) \in \mathcal{B}$, hence $(r_2, \bar{r}_2) \in \mathcal{B}$ as $\approx_{\mathrm{mb}}$ is symmetric and transitive. If r_2 and $\bar{r}_2$ coincide then we are done because $\rho'_2 \stackrel{\tau^*}{\Longrightarrow}_{\mathrm{a}} \bar{\rho}'_2 \stackrel{\lambda_2}{\longrightarrow}_{\mathrm{r}} \rho_2 \stackrel{\tau^*}{\Longrightarrow}_{\mathrm{a}} \rho_2$, where $\mathit{last}(\rho'_2) = s_2$ and $\mathit{last}(\bar{\rho}'_2) = \bar{r}'_2$, and $(\rho'_1, \bar{\rho}'_2) \in \mathcal{B}'$ and $(\rho'_1, \rho'_2) \in \mathcal{B}'$. Otherwise, from $r_2 \in \mathit{reach}(\bar{r}_2)$ and $(r_2, \bar{r}_2) \in \mathcal{B}$ it follows that there must exists $\bar{r}_2 \stackrel{\tau^*}{\Longrightarrow}_{\mathrm{a}} r_2$ and hence we are done because $\rho'_2 \stackrel{\tau^*}{\Longrightarrow}_{\mathrm{a}} \bar{\rho}'_2 \stackrel{\lambda_2}{\longrightarrow}_{\mathrm{r}} \bar{\rho}_2 \stackrel{\tau^*}{\Longrightarrow}_{\mathrm{a}} \rho_2$, where $\mathit{last}(\bar{\rho}_2) = \bar{r}_2$, and $(\rho_1, \bar{\rho}_2) \in \mathcal{B}'$, $(\rho'_1, \bar{\rho}'_2) \in \mathcal{B}'$, and $(\rho'_1, \rho'_2) \in \mathcal{B}'$.
  - If ρ'_1 is not (s_1, ε) then from $(s_1, s_2) \in \mathcal{B}$ it follows that s_1 reaches r'_1 with a sequence of moves that are $\mathcal{B}$-compatible with those with which s_2 reaches some r'_2 such that $(r'_1, r'_2) \in \mathcal{B}$ as $\mathcal{B}$ only contains all the states reachable from s_1 and s_2. From $(r'_1, r'_2) \in \mathcal{B}$ and $r'_1 \stackrel{\tau}{\not\longrightarrow}_{\mathrm{a}}$ it follows that there exists $r'_2 \stackrel{\tau^*}{\Longrightarrow}_{\mathrm{a}} \bar{r}'_2$ with $\bar{r}'_2 \stackrel{\tau}{\not\longrightarrow}_{\mathrm{a}}$ and $r_2 \in \mathit{reach}(\bar{r}'_2)$ such that $(r'_1, \bar{r}'_2) \in \mathcal{B}$, at which points the proof continues like the one of the previous subcase. ■

Therefore the properties $\mathrm{BSNNI}_{\approx_{\mathrm{mb}}}$, $\mathrm{BNDC}_{\approx_{\mathrm{mb}}}$, $\mathrm{SBSNNI}_{\approx_{\mathrm{mb}}}$, $\mathrm{P\_BNDC}_{\approx_{\mathrm{mb}}}$, and $\mathrm{SBNDC}_{\approx_{\mathrm{mb}}}$ do not change if $\approx_{\mathrm{mb}}$ is replaced by $\approx_{\mathrm{mbf}}$. This allows us to study noninterference properties for reversible systems featuring nondeterminism and stochastic time by using $\approx_{\mathrm{mb}}$ in a standard Markovian process calculus like the one of Section 10.1.3.

10.4 Use Case: DBMS Obfuscation and Permission Mechanisms

In Sections 8.2 and 8.5 we have modeled the authentication mechanism of a database management system (DBMS) in which the database can be used to feed a machine learning (ML) module for training purposes, where reversible transactions are supported [60]. Due to privacy issues, DBMS users are not allowed to know which data are actually chosen to train the ML module [12]. Hence, for analysis purposes, the interactions between users and the DBMS are considered to be low level, while the interactions between the DBMS and the ML module are considered to be high level. The aim of the noninterference analysis is thus to check whether users can infer the utilization of their data in the ML dataset. In this section we present two novel examples for this scenario, which show

(i) the nature of the interferences emerging in a stochastically timed setting and (ii) the greater expressive power of branching bisimulation semantics in this setting.

Let $l_{\rm w}$ be a low-level action expressing the execution of a write transaction and $l_{\rm ow}$ be an analogous action that includes also the additional application of an obfuscation mechanism over written data for privacy purposes [3]. We assume that only obfuscated data can feed the ML module. Given the high-level actions h and h' denoting interactions between the DBMS and the ML module, consider the following process:

$$\begin{array}{rcl} DBMS & \triangleq & h\,.\,\tau\,.\,(l_{\rm w}\,.\,\underline{0} + l_{\rm ow}\,.\,h'\,.\,\underline{0}) + \\ & & \tau\,.\,(\tau\,.\,(l_{\rm w}\,.\,\underline{0} + l_{\rm ow}\,.\,\underline{0}) + l_{\rm w}\,.\,\underline{0}) \end{array}$$

The subprocess guarded by the high-level action h represents the behavior of the DBMS whenever the ML module is activated through the h-based interaction. After an internal activity, the DBMS offers a choice between the two available transaction mechanisms, by assuming that only in the second case the transaction data will feed the ML module (through the h'-based interaction). The alternative subprocess guarded by a τ-action describes the behavior of the DBMS whenever the ML module is not involved. Note that this subprocess replicates the behavior above to simulate the presence of the ML module and, thus, makes it transparent from the viewpoint of users. In addition, the subprocess immediately enables also action $l_{\rm w}$ for efficiency reasons and because, in any case, the transaction data will not feed the ML module.

Since the two low views $\tau\,.\,(l_{\rm w}\,.\,\underline{0}+l_{\rm ow}\,.\,\tau\,.\,\underline{0})$ and $\tau\,.\,(l_{\rm w}\,.\,\underline{0}+l_{\rm ow}\,.\,\underline{0})+l_{\rm w}\,.\,\underline{0}$ are both weakly bisimilar and branching bisimilar, we immediately derive that all the noninterference properties of the nondeterministic taxonomy are satisfied. In particular, note that $DBMS\setminus\{h,h'\}$ and $DBMS\,/\,\{h,h'\}$ enable weakly/branching bisimilar behaviors by virtue of the observation above. However, if we add to the model the time spent by the DBMS in the internal activity before the choice about the possible obfuscation, we obtain:

$$\begin{array}{rcl} DBMS_{\rm stoch\_timed} & \triangleq & h\,.\,(\lambda_1)\,.\,(l_{\rm w}\,.\,\underline{0} + l_{\rm ow}\,.\,h'\,.\,\underline{0}) + \\ & & \tau\,.\,((\lambda_2)\,.\,(l_{\rm w}\,.\,\underline{0} + l_{\rm ow}\,.\,\underline{0}) + l_{\rm w}\,.\,\underline{0}) \end{array}$$

where the rates λ_1 and λ_2 govern the delays discussed above for the ML module being involved or not respectively (note that $DBMS$ is the nondeterministic version of $DBMS_{\rm stoch\_timed}$). In this enriched process, the equivalence between the two low views $(\lambda_1)\,.\,(l_{\rm w}\,.\,\underline{0}+l_{\rm ow}\,.\,\tau\,.\,\underline{0})$ and $(\lambda_2)\,.\,(l_{\rm w}\,.\,\underline{0}+l_{\rm ow}\,.\,\underline{0})+l_{\rm w}\,.\,\underline{0}$ does not hold for the Markovian versions of the two bisimilarities. This means that no noninterference property of the Markovian taxonomy is satisfied. Note that this negative result holds also in the case $\lambda_1=\lambda_2$, because only in the second subprocess it is possible to observe action $l_{\rm w}$ with no delay.

Let us consider a more sophisticated variant of the system above, including an explicit permission mechanism involving users. Let $l_{\rm no\_auth}$ be a low-level action expressing that users do not authorize the DBMS to feed the ML module with the data of their transaction, $l_{\rm no\_auth\_o}$ be a low-level action expressing that users do not authorize the obfuscation of the data of their transaction, and $l_{\rm commit}$ be a low-level action expressing the execution of the transaction. Then in the following process:

$$\begin{array}{rcl} DBMS' & \triangleq & h\,.\,(l_{\rm no\_auth}\,.\,l_{\rm commit}\,.\,\underline{0} + \tau\,.\,(l_{\rm no\_auth\_o}\,.\,l_{\rm commit}\,.\,\underline{0} + \tau\,.\,l_{\rm commit}\,.\,h'\,.\,\underline{0})) + \\ & & \tau\,.\,((l_{\rm no\_auth}\,.\,l_{\rm commit}\,.\,\underline{0} + \tau\,.\,(l_{\rm no\_auth\_o}\,.\,l_{\rm commit}\,.\,\underline{0} + \tau\,.\,l_{\rm commit}\,.\,\underline{0})) + \\ & & \quad \tau\,.\,l_{\rm commit}\,.\,\underline{0}) \end{array}$$

the subprocess guarded by the high-level action h – call it P – expresses the behavior of the system whenever the ML module is active. In particular, in such a case, once that no authorization has been forbidden, the committed data are transferred to the training set (through the h'-based interaction). Now, consider the alternative subprocess guarded by a τ-action and modeling the absence of the ML module – call it Q. This subprocess simulates the same behavior as P in the absence of the ML module and, in addition, enables the branch $\tau\,.\,l_{\rm commit}\,.\,\underline{0}$ expressing the immediate execution of the transaction, which does not require any authorization because the ML module is not active. The two subprocesses $P\,/\,\{h'\}$ and Q are weakly bisimilar but not branching bisimilar. In fact, $P\,/\,\{h'\}$

cannot respond to the τ-action of Q leading to $l_{\mathrm{commit}} \,.\, \underline{0}$ in a way that complies with the branching bisimulation semantics.

From the back-and-forth perspective, consider executing the run $\tau \,.\, l_{\mathrm{commit}} \,.\, \underline{0}$ of Q and the run $\tau \,.\, \tau \,.\, l_{\mathrm{commit}} \,.\, \tau \,.\, \underline{0}$ of $P \,/\, \{h'\}$. By undoing the actions of the Q-run it is not possible to go back to a state enabling action $l_{\mathrm{no\_auth\_o}}$ before enabling action $l_{\mathrm{no\_auth}}$. Instead, this is possible by undoing the other run. This is enough to distinguish $P \,/\, \{h'\}$ and Q in the setting of reversible transactions. Therefore, by following the same observations as the previous example, it turns out that the weak-bisimilarity-based noninterference properties are satisfied, while those based on branching bisimilarity are not. Finally, if we add the same rate λ just before the execution of any action l_{commit} – thus yielding $DBMS'_{\mathrm{stoch\_timed}}$ – the same considerations continue to hold, thereby confirming the greater expressive power of the branching bisimulation semantics even in the Markovian setting.

Chapter 11

Conclusions

We conclude the thesis by summarizing our findings (Section 11.1) and indicating future work (Section 11.2).

11.1 Summary of Results

In the first part of the thesis, we have presented a fully fledged process algebraic theory of reversible concurrent systems, which encompasses on the one hand interleaving and truly concurrent equivalences and on the other hand branching-time and linear-time semantics.

We have started by defining a calculus including typical operators such as action prefix, nondeterministic choice, parallel composition, and renaming/hiding. Although inspired by CCSK [121] and RCCS [53, 100], our calculus PRPC is lighter because there are neither communication keys nor stack-based memories. This has been achieved by generating a single transition relation that is deemed to be symmetric as in [57], so that it is sufficient to decorate in the syntax all executed actions with the same symbol † like in [42]. The operational semantics is proved in the sense of [59] so as to pave the way to uniform derivation of expansion laws for parallel composition (Table 2.1). The labeled transition system turns out to be a tree in the case of sequential processes (Proposition 2.1). In particular, the model underlying $a \,.\, b \,.\, \underline{0} + b \,.\, a \,.\, \underline{0}$, which is the interleaving expansion of $a \,.\, \underline{0} \parallel_\emptyset b \,.\, \underline{0}$, is no longer diamond-shaped as it would be in a forward-only calculus (Figure 1.1).

The systematic study of $\sim_{\rm FB}$, $\sim_{\rm RB}$, $\sim_{\rm FRB}$, $\approx_{\rm FB}$, $\approx_{\rm RB}$, $\approx_{\rm FRB}$ has revealed that forward-reverse bisimilarity is strictly included in the intersection of forward bisimilarity and reverse bisimilarity, with the last two being incomparable as the former can identify processes with a different past while the latter can identify processes with a different future. In addition to necessary conditions based on forward ready sets and backward ready sets (Propositions 3.2 and 3.7) and alternative definitions of the three weak bisimilarities (Propositions 3.3, 3.4, 3.5), we have established that all the six bisimilarities are congruences with respect to the operators of PRPC apart from $\sim_{\rm FRB}$, $\approx_{\rm FB}$, $\approx_{\rm FRB}$. These three are not compositional with respect to nondeterministic choice, but for them we have found out the coarsest congruences $\sim_{\rm FRB:ps}$, $\approx_{\rm FB:ps}$, $\approx_{\rm FRB:ps}$ by further requiring past sensitivity, i.e., by imposing that an initial process and a non-initial one cannot be identified (Theorems 4.1 and 4.2). This construction is different from the one used in [112] to build a weak bisimulation congruence on top of weak bisimilarity over forward-only processes.

We have then investigated logical and equational characterizations. The modal logics for the nine bisimilarities are fragments (Table 5.1) of Hennessy-Milner logic [88] extended with a proposition for initiality, which is needed by past-sensitive bisimilarities, and strong and weak backward modalities (Theorems 5.1 and 5.2).

We have employed the proved trees approach of [59] to uniformly derive expansion laws of parallel composition for the two interleaving bisimulation congruences $\sim_{FB}$ and $\approx_{FB:ps}$ and the four truly concurrent bisimulation congruences $\sim_{RB}$, $\approx_{RB}$, $\sim_{FRB:ps}$, $\approx_{FRB:ps}$. In the interleaving case we have the usual associativity, commutativity, idempotency, and neutral element axioms of nondeterministic choice as well as an expansion law that is a past-sensitive variant of the forward-only one [112], with further specific axioms establishing that the presence of the past cannot be ignored, but the specific past and previously non-selected alternatives can be neglected when moving only forward (Table 6.1); for the weak variant the τ-axioms are akin to the forward-only ones [112] (Table 6.2) but the saturation normal form is more complex to express (Lemma 6.3). In the truly concurrent case we have discovered that backward ready sets constitute the additional discriminating information to be inserted into action prefixes via suitable encodings to derive correct expansion laws (Corollaries 6.1 and 6.2). In the reverse subcase the specific axioms establish that, when moving only backward, the future can be completely canceled and previously non-selected alternatives can be discarded (Table 6.4); for the weak variant the only τ-axiom is akin to the one not valid in the forward-only setting for weak bisimulation congruence [112] (Table 6.5). In the forward-reverse subcase we confirm a specific form of idempotency appeared in [106] (Table 6.6); for the weak variant the τ-axioms are akin to the one of branching bisimilarity over forward-only processes [80] (Table 6.7).

As far as alternative characterizations are concerned, we have shown that strong and weak reverse bisimilarities boil down to a linear-time semantics over sequential processes as they coincide with strong and weak reverse trace equivalences [45] (Theorems 7.1 and 7.2), while the former are strictly finer than the latter in general (Corollaries 7.1 and 7.2). Then we have confirmed the connection between branching bisimilarity [80] and reversibility, established in [57], through the notion of weak back-and-forth bisimilarity in a setting in which any backward computation amounts to backtracking, i.e., it is constrained to follow the same path as the corresponding forward computation even in the presence of concurrency. More precisely, weak forward-reverse bisimilarity coincides with branching bisimilarity over sequential initial processes (Theorem 7.3), while they are incomparable in general. Furthermore, weak forward-reverse bisimilarity coincides with forward-reverse branching bisimilarity over sequential processes (Theorem 7.4), while the latter is strictly finer than the former in general (Corollary 7.3). Finally, we have proven that hereditary history-preserving bisimilarity [16] corresponds to forward-reverse bisimilarity extended with backward ready multisets equality, thus providing a simpler solution to a long-standing problem (Theorem 7.5).

In the second part of the thesis, we have developed a comprehensive information flow theory based on the five noninterference properties BSNNI, BNDC, SBSNNI, P_BNDC, SBNDC for multi-level security systems of different nature, where weak bisimilarity and branching bisimilarity – due to the aforementioned results involving the latter – are respectively used as the common thread of the investigation for irreversible and reversible systems.

For purely nondeterministic systems, we have enriched the classical taxonomy of noninterference properties based on weak bisimilarity [67, 69] by introducing branching-bisimilarity-based properties together with their relationships (Figure 8.4), their preservation aspects (Theorem 8.2), and their compositionality characteristics (Theorem 8.3); we have also recalled their connection with reversibility due to branching bisimilarity coinciding with weak back-and-forth bisimilarity [57]. The adequacy of the resulting noninterference properties has been illustrated on an authentication mechanism for a database management system.

For nondeterministic systems extended with probabilities according to the strictly alternating model of [86], we have produced a taxonomy of noninterference properties based on a weak probabilistic bisimilarity inspired by [120] and a probabilistic branching bisimilarity inspired by [8] (Figure 9.2) and shown their preservation aspects (Theorem 9.1), their compositionality characteristics (Theorem 9.2), their relationships with the nondeterministic taxonomy (Corollary 9.1), and their connection with reversibility due to probabilistic branching bisimilarity coinciding with weak probabilistic back-and-forth bisimilarity (Theorem 9.6). These results extend the work of [7] about probabilistic variants of BSNNI, BNDC, SBNDC for a combination of the generative and reactive probabilistic

models of [79] and have required the introduction of a novel weak probabilistic bisimulation up to weak probabilistic bisimililarity as well as a novel probabilistic branching bisimulation up to probabilistic branching bisimililarity (Definitions 9.7 and 9.8). The adequacy of the resulting noninterference properties based on probabilistic branching bisimilarity has been exemplified through a lottery relying on a probabilistic smart contract.

For nondeterministic systems extended with stochastic time according to the interactive Markov chain model of [90], we have produced a taxonomy of noninterference properties based on weak Markovian bisimilarity [90] and a novel Markovian branching bisimilarity (Figure 10.2) and shown their preservation aspects (Theorem 10.1), their compositionality characteristics (Theorem 10.2), their relationships with the nondeterministic and probabilistic taxonomies (Corollaries 10.1 and 10.2), and their connection with reversibility due to Markovian branching bisimilarity coinciding with weak Markovian back-and-forth bisimilarity (Theorem 10.6). These results extend the work of [5] about stochastic variants of BSNNI and SBNDC and the work of [94] about a stochastic variant of P_BNDC – both conducted in process algebraic frameworks inspired by [93] where every action integrates its rate – and have required the introduction of a novel weak Markovian bisimulation up to weak Markovian bisimililarity as well as a novel Markovian branching bisimulation up to Markovian branching bisimilarity (Definitions 10.6 and 10.7). The adequacy of the resulting noninterference properties based on Markovian branching bisimilarity has been shown through obfuscation and permission mechanisms in a database management system for which also time-related aspects have been modeled.

In all the three types of systems a number of ancillary results about SBSNNI and SBNDC have emerged as general patterns for parallel composition, restriction, and hiding (Lemmas 8.2, 8.3, 9.3, 9.4, 10.2, 10.3).

11.2 Future Work

A useful extension to our calculus PRPC would be the inclusion of irreversible actions, as done for instance in [54], because not all activities can be reverted in reality. Another addition would be recursion, which is usually neglected in reversible process calculi because it leads to an infinite state space even in the very simple case of a process that can repeatedly execute a single action.

As for bisimulation semantics, we plan to investigate further the relationships between backward-ready-multiset forward-reverse bisimilarity and hereditary history-preserving bisimilarity, not only in terms of the class of processes for which our result holds. While the latter inherits a variant of the sound and complete axiomatization in Table 6.6, where backward ready sets are replaced by backward ready multisets, the former inherits the logical characterizations of the latter [124, 14]. Since it is easy to find a modal logic characterizing the former, it is interesting to compare all the involved logics; a preliminary study can be found in [28].

On the noninterference side, we are implementing our nondeterministic, probabilistic, and stochastically timed taxonomies for irreversible and reversible multi-level security systems in CADP [72]. Furthermore, we are studying the taxonomy for deterministically timed systems, in which action execution is separated from time passing according to the model of [113, 114] governed by time determinism and time additivity.

A more general objective is to study connections with other forms of reversibility. For example, in [32] causal reversibility and time reversibility have been jointly investigated in a stochastic process algebraic setting. In [31] it has been shown a condition under which causal reversibility implies time reversibility [98], but it is not known when the inverse implication holds.

A different direction to pursue is the investigation of the relationships with reversible programming languages [81], such as the time-reversible programming language Janus and reversible variants of Erlang. Our theory may be exploited as a semantical underpinning or for program verification.

Finally, we would like to address quantum computing [115], given that unitary transformations are reversible. It is worth mentioning that quantum extensions of process calculi and bisimulation semantics have recently appeared [49, 50] that overcome some limitations of previous proposals.

Bibliography

[1] L. Aceto, R.J. van Glabbeek, W. Fokkink, and A. Ingolfsdottir. Axiomatizing prefix iteration with silent steps. *Information and Computation*, 127:26–40, 1996.

[2] L. Aceto, A. Ingolfsdottir, K.G. Larsen, and J. Srba. *Reactive Systems: Modelling, Specification and Verification*. Cambridge University Press, 2007.

[3] M. Al-Rubaie and J.M. Chang. Privacy-preserving machine learning: Threats and solutions. *IEEE Security & Privacy*, 17:49–58, 2019.

[4] A. Aldini. Classification of security properties in a Linda-like process algebra. *Science of Computer Programming*, 63:16–38, 2006.

[5] A. Aldini and M. Bernardo. A general framework for nondeterministic, probabilistic, and stochastic noninterference. In *Proc. of the 1st Joint Workshop on Automated Reasoning for Security Protocol Analysis and Issues in the Theory of Security (ARSPA/WITS 2009)*, volume 5511 of *LNCS*, pages 18–33. Springer, 2009.

[6] A. Aldini and M. Bernardo. Component-oriented verification of noninterference. *Journal of Systems Architecture*, 57:282–293, 2011.

[7] A. Aldini, M. Bravetti, and R. Gorrieri. A process-algebraic approach for the analysis of probabilistic noninterference. *Journal of Computer Security*, 12:191–245, 2004.

[8] S. Andova, S. Georgievska, and N. Trcka. Branching bisimulation congruence for probabilistic systems. *Theoretical Computer Science*, 413:58–72, 2012.

[9] C. Aubert and I. Cristescu. Contextual equivalences in configuration structures and reversibility. *Journal of Logical and Algebraic Methods in Programming*, 86:77–106, 2017.

[10] C. Aubert and I. Cristescu. How reversibility can solve traditional questions: The example of hereditary history-preserving bisimulation. In *Proc. of the 31st Int. Conf. on Concurrency Theory (CONCUR 2020)*, volume 171 of *LIPIcs*, pages 7:1–7:23, 2020.

[11] D. Azzolini, F. Riguzzi, and E. Lamma. Modeling smart contracts with probabilistic logic programming. In *Proc. of the 23rd Int. Business Information Systems Workshops (BIS 2020)*, volume 394 of *LNBIP*, pages 86–98. Springer, 2020.

[12] Y. Bai, M. Fan, Y. Li, and C. Xie. Privacy risk assessment of training data in machine learning. In *Proc. of the 34th IEEE Int. Conf. on Communications (ICC 2022)*, pages 1015–1015. IEEE-CS Press, 2022.

[13] C. Baier and H. Hermanns. Weak bisimulation for fully probabilistic processes. In *Proc. of the 9th Int. Conf. on Computer Aided Verification (CAV 1997)*, volume 1254 of *LNCS*, pages 119–130. Springer, 1997.

[14] P. Baldan and S. Crafa. A logic for true concurrency. *Journal of the ACM*, 61:24:1–24:36, 2014.

[15] R. Barbuti and L. Tesei. A decidable notion of timed non-interference. *Fundamenta Informaticae*, 54:137–150, 2003.

[16] M.A. Bednarczyk. Hereditary history preserving bisimulations or what is the power of the future perfect in program logics. Technical Report, Polish Academy of Sciences, Gdansk, 1991.

[17] C.H. Bennett. Logical reversibility of computation. *IBM Journal of Research and Development*, 17:525–532, 1973.

[18] J.A. Bergstra and J.W. Klop. Process algebra for synchronous communication. *Information and Control*, 60:109–137, 1984.

[19] J.A. Bergstra, J.W. Klop, and E.-R. Olderog. Readies and failures in the algebra of communicating processes. *SIAM Journal on Computing*, 17:1134–1177, 1988.

[20] J.A. Bergstra, A. Ponse, and S.A. Smolka (editors). *Handbook of Process Algebra*. Elsevier, 2001.

[21] M. Bernardo. A survey of Markovian behavioral equivalences. In *Formal Methods for Performance Evaluation*, volume 4486 of *LNCS*, pages 180–219. Springer, 2007.

[22] M. Bernardo. On the tradeoff between compositionality and exactness in weak bisimilarity for integrated-time Markovian process calculi. *Theoretical Computer Science*, 563:99–143, 2015.

[23] M. Bernardo and M. Bravetti. Performance measure sensitive congruences for Markovian process algebras. *Theoretical Computer Science*, 290:117–160, 2003.

[24] M. Bernardo, F. Corradini, and L. Tesei. Timed process calculi with deterministic or stochastic delays: Commuting between durational and durationless actions. *Theoretical Computer Science*, 629:2–39, 2016.

[25] M. Bernardo and A. Esposito. On the weak continuation of reverse bisimilarity vs. forward bisimilarity. In *Proc. of the 24th Italian Conf. on Theoretical Computer Science (ICTCS 2023)*, volume 3587 of *CEUR-WS*, pages 44–58, 2023.

[26] M. Bernardo and A. Esposito. Modal logic characterizations of forward, reverse, and forward-reverse bisimilarities. In *Proc. of the 14th Int. Symp. on Games, Automata, Logics, and Formal Verification (GANDALF 2023)*, volume 390 of *EPTCS*, pages 67–81, 2023.

[27] M. Bernardo, A. Esposito, and C.A. Mezzina. Expansion laws for forward-reverse, forward, and reverse bisimilarities via proved encodings. In *Proc. of the Combined 31st Int. Workshop on Expressiveness in Concurrency and 21st Workshop on Structural Operational Semantics (EXPRESS/SOS 2024)*, volume 412 of *EPTCS*, pages 51–70, 2024.

[28] M. Bernardo, A. Esposito, and C.A. Mezzina. Alternative characterizations of hereditary history-preserving bisimilarity via backward ready multisets. In *Proc. of the 28th Int. Conf. on Foundations of Software Science and Computation Structures (FOSSACS 2025)*, LNCS. Springer, 2025. To appear.

[29] M. Bernardo, A. Esposito, and C.A. Mezzina. A process algebraic theory of reversible computing. 2025. Submitted to a journal.

[30] M. Bernardo and R. Gorrieri. A tutorial on EMPA: A theory of concurrent processes with nondeterminism, priorities, probabilities and time. *Theoretical Computer Science*, 202:1–54, 1998.

[31] M. Bernardo, I. Lanese, A. Marin, C.A. Mezzina, S. Rossi, and C. Sacerdoti Coen. Causal reversibility implies time reversibility. In *Proc. of the 20th Int. Conf. on the Quantitative Evaluation of Systems (QEST 2023)*, volume 14287 of *LNCS*, pages 270–287. Springer, 2023.

[32] M. Bernardo and C.A. Mezzina. Bridging causal reversibility and time reversibility: A stochastic process algebraic approach. *Logical Methods in Computer Science*, 19(2):6:1–6:27, 2023.

[33] M. Bernardo and C.A. Mezzina. Causal reversibility for timed process calculi with lazy/eager durationless actions and time additivity. In *Proc. of the 21st Int. Conf. on Formal Modeling and Analysis of Timed Systems (FORMATS 2023)*, volume 14138 of *LNCS*, pages 15–32. Springer, 2023.

[34] M. Bernardo and C.A. Mezzina. Reversibility in process calculi with nondeterminism and probabilities. In *Proc. of the 21st Int. Coll. on Theoretical Aspects of Computing (ICTAC 2024)*, volume 15373 of *LNCS*, pages 251–271. Springer, 2024.

[35] M. Bernardo and S. Rossi. Reverse bisimilarity vs. forward bisimilarity. In *Proc. of the 26th Int. Conf. on Foundations of Software Science and Computation Structures (FOSSACS 2023)*, volume 13992 of *LNCS*, pages 265–284. Springer, 2023.

[36] A. Bérut, A. Arakelyan, A. Petrosyan, S. Ciliberto, R. Dillenschneider, and E. Lutz. Experimental verification of Landauer's principle linking information and thermodynamics. *Nature*, 483:187–189, 2012.

[37] L. Bocchi, I. Lanese, C.A. Mezzina, and S. Yuen. revTPL: The reversible temporal process language. *Logical Methods in Computer Science*, 20(1):11:1–11:35, 2024.

[38] T. Bolognesi and E. Brinksma. Introduction to the ISO specification language LOTOS. *Computer Networks and ISDN Systems*, 14:25–59, 1988.

[39] S. Boonkrong. *Authentication and Access Control*. Apress, 2020.

[40] G. Boudol and I. Castellani. Concurrency and atomicity. *Theoretical Computer Science*, 59:25–84, 1988.

[41] G. Boudol and I. Castellani. A non-interleaving semantics for CCS based on proved transitions. *Fundamenta Informaticae*, 11:433–452, 1988.

[42] G. Boudol and I. Castellani. Flow models of distributed computations: Three equivalent semantics for CCS. *Information and Computation*, 114:247–314, 1994.

[43] G. Boudol, I. Castellani, M. Hennessy, and A. Kiehn. A theory of processes with localities. *Formal Aspects of Computing*, 6:165–200, 1994.

[44] M. Bravetti, M. Bernardo, and R. Gorrieri. A note on the congruence proof for recursion in Markovian bisimulation equivalence. In *Proc. of the 6th Int. Workshop on Process Algebra and Performance Modelling (PAPM 1998)*, pages 71–87, 1998.

[45] S.D. Brookes, C.A.R. Hoare, and A.W. Roscoe. A theory of communicating sequential processes. *Journal of the ACM*, 31:560–599, 1984.

[46] M.C. Browne, E.M. Clarke, and O. Grümberg. Characterizing finite Kripke structures in propositional temporal logic. *Theoretical Computer Science*, 59:115–131, 1988.

[47] P. Buchholz. Markovian process algebra: Composition and equivalence. In *Proc. of the 2nd Int. Workshop on Process Algebra and Performance Modelling (PAPM 1994)*, pages 11–30. University of Erlangen, Technical Report 27-4, 1994.

[48] I. Castellani. Observing distribution in processes: Static and dynamic localities. *Foundations of Computer Science*, 6:353–393, 1995.

[49] L. Ceragioli, F. Gadducci, G. Lomurno, and G. Tedeschi. Quantum bisimilarity via barbs and contexts: Curbing the power of non-deterministic observers. *Proc. of the ACM on Programming Languages*, 8:43:1–43:29, 2024.

[50] L. Ceragioli, F. Gadducci, G. Lomurno, and G. Tedeschi. Effect semantics for quantum process calculi. In *Proc. of the 35th Int. Conf. on Concurrency Theory (CONCUR 2024)*, volume 311 of *LIPIcs*, pages 16:1–16:22, 2024.

[51] K. Chatterjee, A.K. Goharshady, and A. Pourdamghani. Probabilistic smart contracts: Secure randomness on the blockchain. In *Proc. of the 1st IEEE Int. Conf. on Blockchain and Cryptocurrency (ICBC 2019)*, pages 403–412. IEEE-CS Press, 2019.

[52] I. Cristescu, J. Krivine, and D. Varacca. A compositional semantics for the reversible p-calculus. In *Proc. of the 28th ACM/IEEE Symp. on Logic in Computer Science (LICS 2013)*, pages 388–397. IEEE-CS Press, 2013.

[53] V. Danos and J. Krivine. Reversible communicating systems. In *Proc. of the 15th Int. Conf. on Concurrency Theory (CONCUR 2004)*, volume 3170 of *LNCS*, pages 292–307. Springer, 2004.

[54] V. Danos and J. Krivine. Transactions in RCCS. In *Proc. of the 16th Int. Conf. on Concurrency Theory (CONCUR 2005)*, volume 3653 of *LNCS*, pages 398–412. Springer, 2005.

[55] Ph. Darondeau and P. Degano. Causal trees. In *Proc. of the 16th Int. Coll. on Automata, Languages and Programming (ICALP 1989)*, volume 372 of *LNCS*, pages 234–248. Springer, 1989.

[56] Ph. Darondeau and P. Degano. Causal trees: Interleaving + causality. In *Proc. of the LITP Spring School on Theoretical Computer Science: Semantics of Systems of Concurrent Processes*, volume 469 of *LNCS*, pages 239–255. Springer, 1990.

[57] R. De Nicola, U. Montanari, and F. Vaandrager. Back and forth bisimulations. In *Proc. of the 1st Int. Conf. on Concurrency Theory (CONCUR 1990)*, volume 458 of *LNCS*, pages 152–165. Springer, 1990.

[58] R. De Nicola and F. Vaandrager. Three logics for branching bisimulation. *Journal of the ACM*, 42:458–487, 1995.

[59] P. Degano and C. Priami. Proved trees. In *Proc. of the 19th Int. Coll. on Automata, Languages and Programming (ICALP 1992)*, volume 623 of *LNCS*, pages 629–640. Springer, 1992.

[60] J. Engblom. A review of reverse debugging. In *Proc. of the 4th System, Software, SoC and Silicon Debug Conf. (S4D 2012)*, pages 1–6. IEEE-CS Press, 2012.

[61] A. Esposito, A. Aldini, and M. Bernardo. Branching bisimulation semantics enables noninterference analysis of reversible systems. In *Proc. of the 43rd Int. Conf. on Formal Techniques for Distributed Objects, Components, and Systems (FORTE 2023)*, volume 13910 of *LNCS*, pages 57–74. Springer, 2023.

[62] A. Esposito, A. Aldini, and M. Bernardo. Noninterference analysis of reversible probabilistic systems. In *Proc. of the 44th Int. Conf. on Formal Techniques for Distributed Objects, Components, and Systems (FORTE 2024)*, volume 14678 of *LNCS*, pages 39–59. Springer, 2024.

[63] A. Esposito, A. Aldini, and M. Bernardo. Noninterference analysis of stochastically timed reversible systems. In *Proc. of the 45th Int. Conf. on Formal Techniques for Distributed Objects, Components, and Systems (FORTE 2025)*, 2025. To appear.

[64] A. Esposito, A. Aldini, and M. Bernardo. Noninterference analysis of irreversible or reversible systems with nondeterminism and probabilities. 2025. Invited to a journal.

[65] A. Esposito, A. Aldini, M. Bernardo, and S. Rossi. Noninterference analysis of reversible systems: An approach based on branching bisimilarity. *Logical Methods in Computer Science*, 21(1):6:1–6:28, 2025.

[66] H. Fecher. A completed hierarchy of true concurrent equivalences. *Information Processing Letters*, 89:261–265, 2004.

[67] R. Focardi and R. Gorrieri. Classification of security properties. In *Proc. of the 1st Int. School on Foundations of Security Analysis and Design (FOSAD 2000)*, volume 2171 of *LNCS*, pages 331–396. Springer, 2001.

[68] R. Focardi, C. Piazza, and S. Rossi. Proofs methods for bisimulation based information flow security. In *Proc. of the 3rd Int. Workshop on Verification, Model Checking, and Abstract Interpretation (VMCAI 2002)*, volume 2294 of *LNCS*, pages 16–31. Springer, 2002.

[69] R. Focardi and S. Rossi. Information flow security in dynamic contexts. *Journal of Computer Security*, 14:65–110, 2006.

[70] M.P. Frank. Physical foundations of Landauer's principle. In *Proc. of the 10th Int. Conf. on Reversible Computation (RC 2018)*, volume 11106 of *LNCS*, pages 3–33. Springer, 2018.

[71] S. Fröschle and S. Lasota. Decomposition and complexity of hereditary history preserving bisimulation on BPP. In *Proc. of the 16th Int. Conf. on Concurrency Theory (CONCUR 2005)*, volume 3653 of *LNCS*, pages 263–277. Springer, 2005.

[72] H. Garavel, F. Lang, R. Mateescu, and W. Serve. CADP 2011: A tool for the construction and analysis of distributed processes. *Software Tools for Technology Transfer*, 15:89–107, 2013. `https://cadp.inria.fr/`.

[73] E. Giachino, I. Lanese, and C.A. Mezzina. Causal-consistent reversible debugging. In *Proc. of the 17th Int. Conf. on Fundamental Approaches to Software Engineering (FASE 2014)*, volume 8411 of *LNCS*, pages 370–384. Springer, 2014.

[74] R. Giacobazzi and I. Mastroeni. Abstract non-interference: A unifying framework for weakening information-flow. *ACM Trans. on Privacy and Security*, 21(2):9:1–9:31, 2018.

[75] R.J. van Glabbeek. A complete axiomatization for branching bisimulation congruence of finite-state behaviours. In *Proc. of the 18th Int. Symp. on Mathematical Foundations of Computer Science (MFCS 1993)*, volume 711 of *LNCS*, pages 473–484. Springer, 1993.

[76] R.J. van Glabbeek. The linear time – branching time spectrum I. In *Handbook of Process Algebra*, pages 3–99. Elsevier, 2001.

[77] R.J. van Glabbeek and U. Goltz. Refinement of actions and equivalence notions for concurrent systems. *Acta Informatica*, 37:229–327, 2001.

[78] R.J. van Glabbeek and G.D. Plotkin. Configuration structures, event structures and Petri nets. *Theoretical Computer Science*, 410:4111–4159, 2009.

[79] R.J. van Glabbeek, S.A. Smolka, and B. Steffen. Reactive, generative and stratified models of probabilistic processes. *Information and Computation*, 121:59–80, 1995.

[80] R.J. van Glabbeek and W.P. Weijland. Branching time and abstraction in bisimulation semantics. *Journal of the ACM*, 43:555–600, 1996.

[81] R. Glück and T. Yokoyama. Reversible computing from a programming language perspective. *Theoretical Computer Science*, 953:113429, 2023.

[82] J.A. Goguen and J. Meseguer. Security policies and security models. In *Proc. of the 2nd IEEE Symp. on Security and Privacy (SSP 1982)*, pages 11–20. IEEE-CS Press, 1982.

[83] N. Götz, U. Herzog, and M. Rettelbach. Multiprocessor and distributed systems design: The integration of functional specification and performance analysis using stochastic process algebras. In *Proc. of the 16th Int. Symp. on Computer Performance Modelling, Measurement and Evaluation (PERFORMANCE 1993)*, volume 729 of *LNCS*, pages 121–146. Springer, 1993.

[84] J.F. Groote and M.R. Mousavi. *Modeling and Analysis of Communicating Systems*. MIT Press, 2014. `https://www.mcrl2.org/`.

[85] J.F. Groote and F. Vaandrager. An efficient algorithm for branching bisimulation and stuttering equivalence. In *Proc. of the 17th Int. Coll. on Automata, Languages and Programming (ICALP 1990)*, volume 443 of *LNCS*, pages 626–638. Springer, 1990.

[86] H. Hansson and B. Jonsson. A calculus for communicating systems with time and probabilities. In *Proc. of the 11th IEEE Real-Time Systems Symp. (RTSS 1990)*, pages 278–287. IEEE-CS Press, 1990.

[87] D. Hedin and A. Sabelfeld. A perspective on information-flow control. In *Software Safety and Security – Tools for Analysis and Verification*, pages 319–347. IOS Press, 2012.

[88] M. Hennessy and R. Milner. Algebraic laws for nondeterminism and concurrency. *Journal of the ACM*, 32:137–162, 1985.

[89] M. Hennessy and C. Stirling. The power of the future perfect in program logics. *Information and Control*, 67:23–52, 1985.

[90] H. Hermanns. *Interactive Markov Chains*. Springer, 2002. Volume 2428 of LNCS.

[91] H. Hermanns and M. Lohrey. Observation congruence in a stochastic timed calculus with maximal progress. University of Erlangen, Technical Report IMMD VII-7/97, 1997.

[92] H. Hermanns and M. Rettelbach. Syntax, semantics, equivalences, and axioms for MTIPP. In *Proc. of the 2nd Int. Workshop on Process Algebra and Performance Modelling (PAPM 1994)*, pages 71–87. University of Erlangen, Technical Report 27-4, 1994.

[93] J. Hillston. *A Compositional Approach to Performance Modelling*. Cambridge University Press, 1996.

[94] J. Hillston, A. Marin, C. Piazza, and S. Rossi. Persistent stochastic non-interference. *Fundamenta Informaticae*, 181:1–35, 2021.

[95] D.N. Jansen, J.F. Groote, J.J.A. Keiren, and A. Wijs. An $O(m \log n)$ algorithm for branching bisimilarity on labelled transition systems. In *Proc. of the 26th Int. Conf. on Tools and Algorithms for the Construction and Analysis of Systems (TACAS 2020)*, volume 12079 of *LNCS*, pages 3–20. Springer, 2020.

[96] A. Joyal, M. Nielsen, and G. Winskel. Bisimulation from open maps. *Information and Computation*, 127:164–185, 1996.

[97] R.M. Keller. Formal verification of parallel programs. *Communications of the ACM*, 19:371–384, 1976.

[98] F.P. Kelly. *Reversibility and Stochastic Networks*. John Wiley & Sons, 1979.

[99] L.V. Kovalchuk and A.A. Vykhlo. Estimation of the probability of success of a frontrunning attack on smart contracts. *Cybernetics and Systems Analysis*, 60:881–890, 2024.

[100] J. Krivine. A verification technique for reversible process algebra. In *Proc. of the 4th Int. Workshop on Reversible Computation (RC 2012)*, volume 7581 of *LNCS*, pages 204–217. Springer, 2012.

[101] R. Landauer. Irreversibility and heat generation in the computing process. *IBM Journal of Research and Development*, 5:183–191, 1961.

[102] I. Lanese, M. Lienhardt, C.A. Mezzina, A. Schmitt, and J.-B. Stefani. Concurrent flexible reversibility. In *Proc. of the 22nd European Symp. on Programming (ESOP 2013)*, volume 7792 of *LNCS*, pages 370–390. Springer, 2013.

[103] I. Lanese, D. Medić, and C.A. Mezzina. Static versus dynamic reversibility in CCS. *Acta Informatica*, 58:1–34, 2021.

[104] I. Lanese, C.A. Mezzina, and J.-B. Stefani. Reversing higher-order pi. In *Proc. of the 21st Int. Conf. on Concurrency Theory (CONCUR 2010)*, volume 6269 of *LNCS*, pages 478–493. Springer, 2010.

[105] I. Lanese, N. Nishida, A. Palacios, and G. Vidal. CauDEr: A causal-consistent reversible debugger for Erlang. In *Proc. of the 14th Int. Symp. on Functional and Logic Programming (FLOPS 2018)*, volume 10818 of *LNCS*, pages 247–263. Springer, 2018.

[106] I. Lanese and I. Phillips. Forward-reverse observational equivalences in CCSK. In *Proc. of the 13th Int. Conf. on Reversible Computation (RC 2021)*, volume 12805 of *LNCS*, pages 126–143. Springer, 2021.

[107] I. Lanese, I. Phillips, and I. Ulidowski. An axiomatic theory for reversible computation. *ACM Trans. on Computational Logic*, 25(2):11:1–11:40, 2024.

[108] J.S. Laursen, L.-P. Ellekilde, and U.P. Schultz. Modelling reversible execution of robotic assembly. *Robotica*, 36:625–654, 2018.

[109] O. Lichtenstein, A. Pnueli, and L. Zuck. The glory of the past. In *Proc. of the Conf. on Logics in Programs*, volume 193 of *LNCS*, pages 196–218. Springer, 1985.

[110] H. Mantel. Information flow and noninterference. In *Encyclopedia of Cryptography and Security*, pages 605–607. Springer, 2011.

[111] F. Martinelli. Analysis of security protocols as open systems. *Theoretical Computer Science*, 290:1057–1106, 2003.

[112] R. Milner. *Communication and Concurrency*. Prentice Hall, 1989.

[113] F. Moller and C. Tofts. A temporal calculus of communicating systems. In *Proc. of the 1st Int. Conf. on Concurrency Theory (CONCUR 1990)*, volume 458 of *LNCS*, pages 401–415. Springer, 1990.

[114] F. Moller and C. Tofts. Behavioural abstraction in TCCS. In *Proc. of the 19th Int. Coll. on Automata, Languages and Programming (ICALP 1992)*, volume 623 of *LNCS*, pages 559–570. Springer, 1992.

[115] M.A. Nielsen and I.L. Chuang. *Quantum Computation and Quantum Information: 10th Anniversary Edition*. Cambridge University Press, 2010.

[116] E.-R. Olderog and C.A.R. Hoare. Specification-oriented semantics for communicating processes. *Acta Informatica*, 23:9–66, 1986.

[117] D. Park. Concurrency and automata on infinite sequences. In *Proc. of the 5th GI Conf. on Theoretical Computer Science*, volume 104 of *LNCS*, pages 167–183. Springer, 1981.

[118] N.S. Patel, P. Bhattacharya, S.B. Patel, S. Tanwar, N. Kumar, and H. Song. Blockchain-envisioned trusted random oracles for IoT-enabled probabilistic smart contracts. *IEEE Internet of Things Journal*, 8:14797–14809, 2021.

[119] K.S. Perumalla and A.J. Park. Reverse computation for rollback-based fault tolerance in large parallel systems – Evaluating the potential gains and systems effects. *Cluster Computing*, 17:303–313, 2014.

[120] A. Philippou, I. Lee, and O. Sokolsky. Weak bisimulation for probabilistic systems. In *Proc. of the 11th Int. Conf. on Concurrency Theory (CONCUR 2000)*, volume 1877 of *LNCS*, pages 334–349. Springer, 2000.

[121] I. Phillips and I. Ulidowski. Reversing algebraic process calculi. *Journal of Logic and Algebraic Programming*, 73:70–96, 2007.

[122] I. Phillips and I. Ulidowski. Reversibility and models for concurrency. In *Proc. of the 4th Int. Workshop on Structural Operational Semantics (SOS 2007)*, volume 192(1) of *ENTCS*, pages 93–108. Elsevier, 2007.

[123] I. Phillips and I. Ulidowski. A hierarchy of reverse bisimulations on stable configuration structures. *Mathematical Structures in Computer Science*, 22:333–372, 2012.

[124] I. Phillips and I. Ulidowski. Event identifier logic. *Mathematical Structures in Computer Science*, 24(2):1–51, 2014.

[125] I. Phillips, I. Ulidowski, and S. Yuen. A reversible process calculus and the modelling of the ERK signalling pathway. In *Proc. of the 4th Int. Workshop on Reversible Computation (RC 2012)*, volume 7581 of *LNCS*, pages 218–232. Springer, 2012.

[126] G.M. Pinna. Reversing steps in membrane systems computations. In *Proc. of the 18th Int. Conf. on Membrane Computing (CMC 2017)*, volume 10725 of *LNCS*, pages 245–261. Springer, 2017.

[127] C. Priami. Stochastic π-calculus. *Computer Journal*, 38:578–589, 1995.

[128] P. Qian, J. He, L. Lu, S. Wu, Z. Lu, L. Wu, Y. Zhou, and Q. He. Demystifying random number in Ethereum smart contract: Taxonomy, vulnerability identification, and attack detection. *IEEE Trans. on Software Engineering*, 49:3793–3810, 2023.

[129] A.M. Rabinovich and B.A. Trakhtenbrot. Behavior structures and nets. *Fundamenta Informaticae*, 11:357–404, 1988.

[130] A. Sabelfeld and D. Sands. Probabilistic noninterference for multi-threaded programs. In *Proc. of the 13th IEEE Computer Security Foundations Workshop (CSFW 2000)*, pages 200–214. IEEE-CS Press, 2000.

[131] D. Sangiorgi and R. Milner. The problem of "weak bisimulation up to". In *Proc. of the 3rd Int. Conf. on Concurrency Theory (CONCUR 1992)*, volume 630 of *LNCS*, pages 32–46. Springer, 1992.

[132] M. Schordan, T. Oppelstrup, D.R. Jefferson, and P.D. Barnes Jr. Generation of reversible C++ code for optimistic parallel discrete event simulation. *New Generation Computing*, 36:257–280, 2018.

[133] R. Segala. *Modeling and Verification of Randomized Distributed Real-Time Systems*. PhD Thesis, 1995.

[134] R. Segala and N.A. Lynch. Probabilistic simulations for probabilistic processes. In *Proc. of the 5th Int. Conf. on Concurrency Theory (CONCUR 1994)*, volume 836 of *LNCS*, pages 481–496. Springer, 1994.

[135] R. Segala and A. Turrini. Comparative analysis of bisimulation relations on alternating and non-alternating probabilistic models. In *Proc. of the 2nd Int. Conf. on the Quantitative Evaluation of Systems (QEST 2005)*, pages 44–53. IEEE-CS Press, 2005.

[136] S. Semujju, F. Liu, H. Huang, and Y. Xiang. Enhancing fault detection in smart contract loops through adaptive probabilistic sampling. In *Proc. of the 26th Genetic and Evolutionary Computation Conf. (GECCO 2024)*, pages 731–734. ACM Press, 2024.

[137] H. Siljak, K. Psara, and A. Philippou. Distributed antenna selection for massive MIMO using reversing Petri nets. *IEEE Wireless Communication Letters*, 8:1427–1430, 2019.

[138] A. Turrini and H. Hermanns. Polynomial time decision algorithms for probabilistic automata. *Information and Computation*, 244:134–171, 2015.

[139] M. Vassor and J.-B. Stefani. Checkpoint/rollback vs causally-consistent reversibility. In *Proc. of the 10th Int. Conf. on Reversible Computation (RC 2018)*, volume 11106 of *LNCS*, pages 286–303. Springer, 2018.

[140] D. Volpano and G. Smith. Probabilistic noninterference in a concurrent language. In *Proc. of the 11th IEEE Computer Security Foundations Workshop (CSFW 1998)*, pages 34–43. IEEE-CS Press, 1998.

[141] E. de Vries, V. Koutavas, and M. Hennessy. Communicating transactions. In *Proc. of the 21st Int. Conf. on Concurrency Theory (CONCUR 2010)*, volume 6269 of *LNCS*, pages 569–583. Springer, 2010.

[142] G. Winskel. Event structures. In *Advances in Petri Nets*, volume 255 of *LNCS*, pages 325–392. Springer, 1986.

[143] B. Ycart. The philosophers' process: An ergodic reversible nearest particle system. *Annals of Applied Probability*, 3:356–363, 1993.

[144] L. Zheng and A. Myers. Dynamic security labels and noninterference. In *Proc. of the 2nd IFIP Workshop on Formal Aspects in Security and Trust (FAST 2004)*, volume 173 of *IFIP AICT*, pages 27–40. Springer, 2004.