Noninterference Analysis of Reversible Probabilistic Systems

Andrea Esposito, Alessandro Aldini, and Marco Bernardo

Dipartimento di Scienze Pure e Applicate, Università di Urbino, Urbino, Italy

Abstract. Noninterference theory supports the analysis of secure computations in multi-level security systems. In the nondeterministic setting, the approach to noninterefence based on weak bisimilarity has turned out to be inadequate for reversible systems. This drawback can be overcome by employing a more expressive semantics, which has been recently proven to be branching bisimilarity. In this paper we extend the result to reversible systems that feature both nondeterminism and probabilities. We recast noninterference properties by adopting probabilistic variants of weak and branching bisimilarities. Then we investigate a taxonomy of those properties as well as their preservation and compositionality aspects, along with a comparison with the nondeterministic taxonomy. The adequacy of the resulting noninterference theory for reversible systems is illustrated via a probabilistic smart contract example.

1 Introduction

The notion of noninterference was introduced in [22] 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 to extend the approach to a variety of more expressive domains, such as nondeterministic systems, systems in which quantitative aspects – like time and probability – play a central role, and reversible systems; see, e.g., [16,1,31,24,47,39,5,2,25,15].

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 [19] 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. A natural framework in which to study system behavior is given by process algebra [32]. In this setting, weak bisimilarity has been employed in [16] both to reason formally about covert channels and illegitimate information flows and to study a classification of noninterference properties for nondeterministic systems.

In [15] we have extended noninterference analysis to reversible systems. Reversibility has started to gain attention in computing since it has been shown that reversible computations may achieve lower levels of energy consumption [27,6]. The applications of reversibility range from biochemical reaction modeling [37,38] and parallel discrete-event simulation [34,41] to robotics [30], wireless communications [45], fault-tolerant systems [13,48,28,46], and program debugging [18,29].

As shown in [15], weak bisimilarity is not adequate to study noninterference in a reversible context. A more appropriate semantics turns out to be branching bisimilarity [21] because it coincides with weak back-and-forth bisimilarity [14]. The latter behavioral equivalence requires processes to be able to mimic each other's behavior stepwise not only when performing actions in the standard forward direction, but also when undoing those actions in the backward direction.

In this paper we extend the approach of [15] to a probabilistic setting, so as to address noninterference properties in a framework featuring nondeterministic, probabilistic, and reversible behaviors. The starting point for our study is given by the probabilistic noninterference properties developed in [2] over a probabilistic process calculus based on the generative and reactive models of [20]. In addition to probabilistic choice, in [2] 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 considered behavioral equivalence is akin to the weak probabilistic bisimilarity of [4], which is known to coincide with probabilistic branching bisimilarity over fully probabilistic processes.

Here we move to a more expressive model, combining nondeterminism and probabilities, called the strictly alternating model [23]. 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 [35], allows for action transitions also between two nondeterministic states.

Following [23] we build a process calculus that, unlike the one in [2], does not need probabilistic parameters for operators other than probabilistic choice. As for behavioral equivalences, we introduce a weak probabilistic bisimilarity inspired by the one in [35] and adopt the probabilistic branching bisimilarity developed in [3] for the non-strictly alternating model. By using these two equivalences, we recast the noninterference properties of [16,17,15] to study their preservation and compositionality aspects, as well as to provide a taxonomy similar to those in [16,15]. Unlike [2], the resulting noninterference properties do not need additional universal quantifications over probabilistic parameters. Reversibility then comes into play by extending some results of [14] to the strictly alternating model. In particular, a probabilistic variant of weak back-and-forth bisimilarity is shown to coincide with the probabilistic branching bisimilarity of [3].

This paper is organized as follows. In Section 2 we recall the strictly alternating model, various notions of bisimilarity for it, and a process calculus based on it. In Section 3 we recast in our probabilistic framework a selection of noninterference properties. In Section 4 we study their characteristics as well as their taxonomy and relate it to the nondeterministic one of [15]. In Section 5 we show that weak probabilistic back-and-forth bisimilarity coincides with probabilistic branching bisimilarity. In Section 6 we discuss the example of a lottery implemented through a probabilistic smart contract. Section 7 concludes the paper.

2 Background Definitions and Results

In this section, we recall the strict alternating model of [23] (Section 2.1) along with weak probabilistic bisimilarity and probabilistic branching bisimilarity (Section 2.2). Then we introduce a probabilistic process language inspired by [23] through which we will express bisimulation-based information-flow security properties accounting for nondeterminism and probabilities (Section 2.3).

2.1 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 [26] whose transitions are labeled with actions or probabilities. Since we adopt the strictly alternating model of [23], 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. The action set $\mathcal{A}_\tau$ contains a set $\mathcal{A}$ of visible actions and a single action τ representing unobservable actions.

Definition 1. *A* probabilistic labeled transition system (PLTS) *is a triple* $(\mathcal{S}, \mathcal{A}_\tau, \longrightarrow)$ *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,* $\mathcal{A}_\tau = \mathcal{A} \cup \{\tau\}$ *is a countable set of actions, and* $\longrightarrow = \longrightarrow_{\rm a} \cup \longrightarrow_{\rm p}$ *is the transition relation, where* $\longrightarrow_{\rm a} \subseteq \mathcal{S}_{\rm n} \times \mathcal{A}_\tau \times \mathcal{S}_{\rm p}$ *is the action transition relation whilst* $\longrightarrow_{\rm p} \subseteq \mathcal{S}_{\rm p} \times \mathbb{R}_{]0,1]} \times \mathcal{S}_{\rm n}$ *is 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 transition being s and the target of the last one being s'.

2.2 Bisimulation Equivalences

Bisimilarity [33,32] identifies processes that are able to mimic each other's behavior stepwise. In the strictly alternating model, this extends to probabilistic behavior [23]. Let $\mu(s, C) = \sum_{s \xrightarrow{p}_{\rm p} s', s' \in C} p$ be the cumulative probability with which state s reaches a state in C; note that $\mu(s, C) = 0$ when s is not a probabilistic state or C does not contain any nondeterministic state.

Definition 2. *Let* $(\mathcal{S}, \mathcal{A}_\tau, \longrightarrow)$ *be a PLTS. We say that* $s_1, s_2 \in \mathcal{S}$ *are* strongly probabilistic bisimilar*, written* $s_1 \sim_{\rm p} s_2$*, iff* $(s_1, s_2) \in \mathcal{B}$ *for some strong probabilistic bisimulation* $\mathcal{B}$*. An equivalence relation* $\mathcal{B} \subseteq (\mathcal{S}_{\rm n} \times \mathcal{S}_{\rm n}) \cup (\mathcal{S}_{\rm p} \times \mathcal{S}_{\rm p})$ *is a* strong probabilistic bisimulation *iff, whenever* $(s_1, s_2) \in \mathcal{B}$*, then:*

– *For each* $s_1 \xrightarrow{a}_{\rm a} s_1'$ *there exists* $s_2 \xrightarrow{a}_{\rm a} s_2'$ *with* $(s_1', s_2') \in \mathcal{B}$.
– $\mu(s_1, C) = \mu(s_2, C)$ *for all equivalence classes* $C \in \mathcal{S}_{\rm n}/\mathcal{B}$. ■

In [35] a strong probabilistic bisimilarity more liberal than the one in [23] 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 [35]:

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

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

Definition 3. *Let* $(\mathcal{S}, \mathcal{A}_\tau, \longrightarrow)$ *be a PLTS. We say that* $s_1, s_2 \in \mathcal{S}$ *are* strongly mix-probabilistic bisimilar*, written* $s_1 \sim_{\rm mp} s_2$*, 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* $s_1, s_2 \in \mathcal{S}_{\rm n}$*, for each* $s_1 \xrightarrow{a}_{\rm a} s_1'$ *there exists* $s_2 \xrightarrow{a}_{\rm a} s_2'$ *with* $(s_1', s_2') \in \mathcal{B}$.
– $prob(s_1, C) = prob(s_2, C)$ *for all equivalence classes* $C \in \mathcal{S}/\mathcal{B}$. ■

Weak bisimilarity [32] 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 $\stackrel{\hat{a}}{\Longrightarrow}$ stands for $\Longrightarrow$ if $a = \tau$ or $\Longrightarrow \xrightarrow{a}_{\rm a} \Longrightarrow$ if $a \neq \tau$. The weak probabilistic bisimilarity below is inspired by the one in [35]. The constraint $s_1, s_2 \in \mathcal{S}_{\rm n}$ is no longer necessary in the first clause due to the use of $\Longrightarrow$.

Definition 4. *Let* $(\mathcal{S}, \mathcal{A}_\tau, \longrightarrow)$ *be a PLTS. We say that* $s_1, s_2 \in \mathcal{S}$ *are* weakly probabilistic bisimilar*, written* $s_1 \approx_{\rm p} s_2$*, 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:*

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

Branching bisimilarity [21] is finer than weak bisimilarity as it preserves the branching structure of processes even when abstracting from τ-actions – see the condition $(s_1, \bar{s}_2) \in \mathcal{B}$ in the definition below. We adopt the probabilistic branching bisimilarity developed in [3] for the non-strictly alternating model.

Definition 5. *Let* $(\mathcal{S}, \mathcal{A}_\tau, \longrightarrow)$ *be a PLTS. We say that* $s_1, s_2 \in \mathcal{S}$ *are* probabilistic branching bisimilar*, written* $s_1 \approx_{\rm pb} s_2$*, 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:*

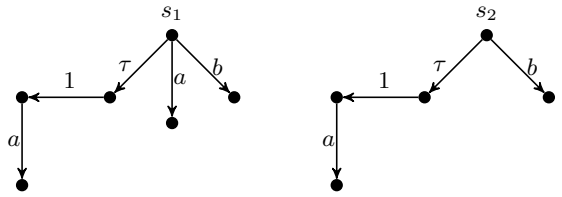

Fig. 1. States s_1 and s_2 are related by $\approx_{\rm p}$ but distinguished by $\approx_{\rm pb}$

- *For each* $s_1 \xrightarrow{a}_{\rm a} s_1'$*:*
  - *either* $a = \tau$ *and* $(s_1', s_2) \in \mathcal{B}$*;*
  - *or there exists* $s_2 \Longrightarrow \bar{s}_2 \xrightarrow{a}_{\rm a} s_2'$ *with* $(s_1, \bar{s}_2) \in \mathcal{B}$ *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 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. The only transition that distinguishes s_1 and s_2 is the a-transition of s_1, which can be mimicked by s_2 according to weak probabilistic bisimilarity by performing the τ-transition, the 1-transition, and lastly the a-transition. However, s_2 cannot respond in the same way according to probabilistic branching bisimilarity. The reason is that the state reached after the τ-transition and the 1-transition should be probabilistic branching bisimilar to s_1, which is not the case because of the b-transition departing from s_1.

2.3 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, actions are divided into high and low. We partition the set of visible actions as $\mathcal{A} = \mathcal{A}_{\mathcal{H}} \cup \mathcal{A}_{\mathcal{L}}$, 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. We recall that $\mathcal{A}_\tau = \mathcal{A} \cup \{\tau\}$.

The overall set of process terms is denoted by $\mathbb{P} = \mathbb{P}_{\rm n} \cup \mathbb{P}_{\rm p}$, ranged over by E. The set $\mathbb{P}_{\rm n}$ of nondeterministic process terms, ranged over by N, is obtained by considering typical operators from [32,9]. The set $\mathbb{P}_{\rm p}$ of probabilistic process terms, ranged over by P, is obtained by taking a probabilistic choice operator similar to the one in [23]. In addition to the usual operators for sequential, alternative, and parallel compositions – with the last one taken from [9] so as not to hide the synchronization between high-level actions – we include restriction [32] and hiding [9] as they are necessary to formalize noninterference properties.

The syntax for $\mathbb{P}$ is:

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

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	$\dfrac{N_1 \xrightarrow{a}_{\mathrm{a}} P_1 \quad a \notin L}{N_1 \parallel_L N_2 \xrightarrow{a}_{\mathrm{a}} P_1 \parallel_L [1]N_2} \qquad \dfrac{N_2 \xrightarrow{a}_{\mathrm{a}} P_2 \quad a \notin L}{N_1 \parallel_L N_2 \xrightarrow{a}_{\mathrm{a}} [1]N_1 \parallel_L P_2}$
Sync	$\dfrac{N_1 \xrightarrow{a}_{\mathrm{a}} P_1 \quad N_2 \xrightarrow{a}_{\mathrm{a}} P_2 \quad a \in L}{N_1 \parallel_L N_2 \xrightarrow{a}_{\mathrm{a}} P_1 \parallel_L P_2}$
Restriction	$\dfrac{N \xrightarrow{a}_{\mathrm{a}} P \quad a \notin L}{N \setminus L \xrightarrow{a}_{\mathrm{a}} P \setminus L}$
Hiding	$\dfrac{N \xrightarrow{a}_{\mathrm{a}} P \quad a \in L}{N \,/\, L \xrightarrow{\tau}_{\mathrm{a}} P \,/\, L} \qquad \dfrac{N \xrightarrow{a}_{\mathrm{a}} P \quad a \notin L}{N \,/\, L \xrightarrow{a}_{\mathrm{a}} P \,/\, L}$

Table 1. Operational semantic rules for nondeterministic processes

where:

- $\underline{0}$ is the terminated process.
- $a \,.\, \_$, for $a \in \mathcal{A}_\tau$, is the action prefix operator describing a process that initially performs action a.
- $\_ + \_$ is the alternative composition operator expressing a nondeterministic choice between two processes based on their initially executable actions.
- $\bigoplus_{i \in I} [p_i] \_$, 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 we will often omit the probability prefix when it is equal to 1.
- $\_ \parallel_L \_$, for $L \subseteq \mathcal{A}$, 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 probabilistic transitions [23].
- $\_ \setminus L$, for $L \subseteq \mathcal{A}$, is the restriction operator, which prevents the execution of actions belonging to L.
- $\_ / L$, for $L \subseteq \mathcal{A}$, is the hiding operator, which turns all the executed actions belonging to L into the unobservable action τ.

The operational semantic rules for the process language are shown in Tables 1 and 2 for nondeterministic and probabilistic processes respectively. Together they produce the PLTS $(\mathbb{P}, \mathcal{A}_\tau, \longrightarrow)$ where $\longrightarrow = \longrightarrow_{\mathrm{a}} \cup \longrightarrow_{\mathrm{p}}$, $\longrightarrow_{\mathrm{a}} \subseteq \mathbb{P}_{\mathrm{n}} \times \mathcal{A}_\tau \times \mathbb{P}_{\mathrm{p}}$, and $\longrightarrow_{\mathrm{p}} \subseteq \mathbb{P}_{\mathrm{p}} \times \mathbb{R}_{]0,1]} \times \mathbb{P}_{\mathrm{n}}$, to which the bisimulation equivalences defined in Section 2.2 are applicable. Note that in the rules *Parallel* the nondeterministic subprocess that does not move has to be prefixed by [1] to make it probabilistic within the overall target process [23].

$$\textit{ProbChoice}\quad \frac{j \in I}{\bigoplus_{i \in I}[p_i]N_i \xrightarrow{p_j}_{\mathrm{p}} N_j}$$

$$\textit{ProbSync}\quad \frac{P_1 \xrightarrow{p_1}_{\mathrm{p}} N_1 \quad P_2 \xrightarrow{p_2}_{\mathrm{p}} N_2}{P_1 \parallel_L P_2 \xrightarrow{p_1 \cdot p_2}_{\mathrm{p}} N_1 \parallel_L N_2}$$

$$\textit{ProbRestriction}\quad \frac{P \xrightarrow{p}_{\mathrm{p}} N}{P \setminus L \xrightarrow{p}_{\mathrm{p}} N \setminus L}$$

$$\textit{ProbHiding}\quad \frac{P \xrightarrow{p}_{\mathrm{p}} N}{P \,/\, L \xrightarrow{p}_{\mathrm{p}} N \,/\, L}$$

Table 2. Operational semantic rules for probabilistic processes

3 Probabilistic Information-Flow Security Properties

In this section we recast the definitions of noninteference properties of [16,17,15] – *Nondeterministic Non-Interference* (NNI) and *Non-Deducibility on Composition* (NDC) – by taking as behavioral equivalence each of the two weak bisimilarities of Section 2.2. The intuition behind noninterference in a two-level security system is that, if a group of agents at the high security level performs some actions, the effect of those actions should not be seen by any agent at the low security level. To formalize this, the restriction and hiding operators play a central role.

Definition 6. *Let $E \in \mathbb{P}$ and $\approx \in \{\approx_{\mathrm{p}}, \approx_{\mathrm{pb}}\}$:*

- $E \in \mathrm{BSNNI}_{\approx} \iff E \setminus \mathcal{A}_{\mathcal{H}} \approx E \,/\, \mathcal{A}_{\mathcal{H}}$.
- $E \in \mathrm{BNDC}_{\approx} \iff$ *for all* $F \in \mathbb{P}$ *such that every* $F' \in \mathit{reach}(F)$ *can execute only actions in* $\mathcal{A}_{\mathcal{H}}$ *and for all* $L \subseteq \mathcal{A}_{\mathcal{H}}$, $E \setminus \mathcal{A}_{\mathcal{H}} \approx ((E \parallel_L F) \,/\, L) \setminus \mathcal{A}_{\mathcal{H}}$.
- $E \in \mathrm{SBSNNI}_{\approx} \iff$ *for all* $E' \in \mathit{reach}(E)$, $E' \in \mathrm{BSNNI}_{\approx}$.
- $E \in \mathrm{P\_BNDC}_{\approx} \iff$ *for all* $E' \in \mathit{reach}(E)$, $E' \in \mathrm{BNDC}_{\approx}$.
- $E \in \mathrm{SBNDC}_{\approx} \iff$ *for all* $E' \in \mathit{reach}(E)$ *and for all* E'' *such that* $E' \xrightarrow{a}_{\mathrm{a}} E''$ *for some* $a \in \mathcal{A}_{\mathcal{H}}$, $E' \setminus \mathcal{A}_{\mathcal{H}} \approx E'' \setminus \mathcal{A}_{\mathcal{H}}$. ■

Historically, one of the first and most intuitive proposals has been the *Bisimulation-based Strong Nondeterministic Non-Interference* (BSNNI). Basically, it is satisfied by any process E that behaves the same when its high-level actions are prevented (as modeled by $E \setminus \mathcal{A}_{\mathcal{H}}$) or when they are considered as hidden, unobservable actions (as modeled by $E \,/\, \mathcal{A}_{\mathcal{H}}$). The equivalence between these two low-level views of E states that a low-level agent cannot distinguish the high-level behavior of the system. For instance, in our probabilistic setting, a low-level agent that observes the execution of l in $E = l \,.\, \underline{0} + l \,.\, ([0.5]h \,.\, l_1 \,.\, \underline{0} \oplus [0.5]h \,.\, l_2 \,.\, \underline{0}) + l \,.\, ([0.5]l_1 \,.\, \underline{0} \oplus [0.5]l_2 \,.\, \underline{0})$ cannot infer anything about the execution of h. Indeed, after the execution of l, what the low-level agent observes is either a deadlocked state or the execution of either l_1 or l_2, both with probability 0.5. Formally, $E \setminus \{h\} \approx E \,/\, \{h\}$ because $l \,.\, \underline{0} + l \,.\, \underline{0} + l \,.\, ([0.5]l_1 \,.\, \underline{0} \oplus [0.5]l_2 \,.\, \underline{0}) \approx l \,.\, \underline{0} + l \,.\, ([0.5]\tau \,.\, l_1 \,.\, \underline{0} \oplus [0.5]\tau \,.\, l_2 \,.\, \underline{0}) + l \,.\, ([0.5]l_1 \,.\, \underline{0} \oplus [0.5]l_2 \,.\, \underline{0})$.

$\text{BSNNI}_{\approx}$ is not powerful enough to capture covert channels that derive from the behavior of the high-level agent interacting with the system. For instance, $l\,.\,\underline{0}+l\,.\,([0.5]h_1\,.\,l_1\,.\,\underline{0}\oplus[0.5]h_2\,.\,l_2\,.\,\underline{0})+l\,.\,([0.5]l_1\,.\,\underline{0}\oplus[0.5]l_2\,.\,\underline{0})$ is $\text{BSNNI}_{\approx}$ for the same reason discussed above. However, a high-level agent could decide to enable only h_1, thus turning the low-level view of the system into $l\,.\,\underline{0}+l\,.\,([0.5]\tau\,.\,l_1\,.\,\underline{0}\oplus [0.5]\underline{0})+l\,.\,([0.5]l_1\,.\,\underline{0}\oplus[0.5]l_2\,.\,\underline{0})$, which is clearly distinguishable from $l\,.\,\underline{0}+l\,.\,\underline{0}+ l\,.\,([0.5]l_1\,.\,\underline{0}\oplus[0.5]l_2\,.\,\underline{0})$, as in the former after the execution of l the low-level agent can never observe l_2. To overcome such a limitation, the most obvious solution consists of checking explicitly the interaction between the system and every possible high-level agent F. The resulting property is the *Bisimulation-based Non-Deducibility on Composition* (BNDC), which features a universal quantification over F executing 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 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. In the nondeterministic case, P_BNDC and SBSNNI have been proven to be equivalent in [17], for the weak bisimilarity variants, and in [15], for the branching bisimilarity variants. In the next section we will see that this is the case also in our probabilistic setting.

4 Characteristics of Probabilistic Security Properties

In this section we investigate preservation and compositionality characteristics of the noninterference properties introduced in the previous section (Section 4.1) as well as the inclusion relationships between the ones based on $\approx_{\text{p}}$ and the ones based on $\approx_{\text{pb}}$ (Section 4.2). Then we relate the resulting probabilistic taxonomy with the nondeterministic one of [15] (Section 4.3).

4.1 Preservation and Compositionality

All the probabilistic noninterference properties turn out to be preserved by the bisimilarity employed in their definition. This means that, whenever a process E_1 is secure under any of such properties, then every other equivalent process E_2 is secure too, provided that the considered equivalence is the one in the definition of the 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. These results immediately follow from the next lemma, which states that $\approx_{\text{p}}$ and $\approx_{\text{pb}}$ are congruences with respect to action prefix, parallel

composition, restriction, and hiding (similar results are present in [35,3] for the non-strictly alternating model).

Lemma 1. *Let $E, E_1, E_2 \in \mathbb{P}$, $\approx \in \{\approx_{\rm p}, \approx_{\rm pb}\}$, and $L \subseteq \mathcal{A}$. If $E_1 \approx E_2$, then:*

- $a\,.\,E_1 \approx a\,.\,E_2$ *when* $E_1, E_2 \in \mathbb{P}_{\rm p}$.
- $E_1 \parallel_L E \approx E_2 \parallel_L E$ *when* $E_1, E_2, E \in \mathbb{P}_{\rm n}$ *or* $E_1, E_2, E \in \mathbb{P}_{\rm p}$.
- $E_1 \setminus L \approx E_2 \setminus L$.
- $E_1 / L \approx E_2 / L$. ■

Theorem 1. *Let E_1,$E_2 \in \mathbb{P}$, $\approx \in \{\approx_{\rm p}, \approx_{\rm pb}\}$, and $\mathcal{P} \in \{{\rm BSNNI}_\approx, {\rm BNDC}_\approx, {\rm SBSNNI}_\approx, {\rm P\_BNDC}_\approx, {\rm SBNDC}_\approx\}$. If $E_1 \approx E_2$, then $E_1 \in \mathcal{P} \iff E_2 \in \mathcal{P}$.* ■

As far as modular verification is concerned, like in the nondeterministic case [16,15] only the local properties ${\rm SBSNNI}_\approx$, ${\rm P\_BNDC}_\approx$, and ${\rm SBNDC}_\approx$ are compositional, i.e., are preserved by some operators of the calculus in certain circumstances. Compositionality with respect to parallel composition is limited, for ${\rm SBSNNI}_{\approx_{\rm pb}}$ and ${\rm P\_BNDC}_{\approx_{\rm pb}}$, to the case in which no synchronization can take place among high-level actions. This is analogous to the nondeterministic case [15], where the same limitation holds for the branching bisimulation-based SBSNNI and P_BNDC. A similar limitation applies to hiding.

Theorem 2. *Let $E, E_1, E_2 \in \mathbb{P}$, $\approx \in \{\approx_{\rm p}, \approx_{\rm pb}\}$, $\mathcal{P} \in \{{\rm SBSNNI}_\approx, {\rm P\_BNDC}_\approx, {\rm SBNDC}_\approx\}$. Then:*

1. $E \in \mathcal{P} \Longrightarrow a\,.\,E \in \mathcal{P}$ *for all* $a \in \mathcal{A}_\mathcal{L} \cup \{\tau\}$ *when* $E \in \mathbb{P}_{\rm p}$.
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* $\mathcal{P} \in \{{\rm SBSNNI}_{\approx_{\rm pb}}, {\rm P\_BNDC}_{\approx_{\rm pb}}\}$ *or* $L \subseteq \mathcal{A}$ *if* $\mathcal{P} \in \{{\rm SBSNNI}_{\approx_{\rm p}}, {\rm P\_BNDC}_{\approx_{\rm p}}, {\rm SBNDC}_{\approx_{\rm p}}, {\rm SBNDC}_{\approx_{\rm pb}}\}$, *when* $E_1, E_2 \in \mathbb{P}_{\rm n}$ *or* $E_1, E_2 \in \mathbb{P}_{\rm p}$.
3. $E \in \mathcal{P} \Longrightarrow E \setminus L \in \mathcal{P}$ *for all* $L \subseteq \mathcal{A}$.
4. $E \in \mathcal{P} \Longrightarrow E / L \in \mathcal{P}$ *for all* $L \subseteq \mathcal{A}_\mathcal{L}$. ■

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 example, both $E_1 := h\,.\,[1]\underline{0} + l_1\,.\,[1]\underline{0} + \tau\,.\,[1]\underline{0}$ and $E_2 := h\,.\,[1]\underline{0} + l_2\,.\,[1]\underline{0} + \tau\,.\,[1]\underline{0}$ 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 $(E_1 \parallel_{\{h\}} E_2) \setminus \mathcal{A}_\mathcal{H} \Longrightarrow (E_1 \parallel_{\{h\}} E_2) \setminus \mathcal{A}_\mathcal{H} \xrightarrow{\tau}_{\rm a} ([1]\underline{0} \parallel_{\{h\}} [1]E_2) \setminus \mathcal{A}_\mathcal{H} \xrightarrow{1}_{\rm p} (\underline{0} \parallel_{\{h\}} E_2) \setminus \mathcal{A}_\mathcal{H} \xrightarrow{\tau}_{\rm a} ([1]\underline{0} \parallel_{\{h\}} [1]\underline{0}) \setminus \mathcal{A}_\mathcal{H}$ as well as $(E_1 \parallel_{\{h\}} E_2) \setminus \mathcal{A}_\mathcal{H} \Longrightarrow (E_1 \parallel_{\{h\}} E_2) \setminus \mathcal{A}_\mathcal{H} \xrightarrow{\tau}_{\rm a} ([1]E_1 \parallel_{\{h\}} [1]\underline{0}) \setminus \mathcal{A}_\mathcal{H} \xrightarrow{1}_{\rm p} (E_1 \parallel_{\{h\}} \underline{0}) \setminus \mathcal{A}_\mathcal{H} \xrightarrow{\tau}_{\rm a} ([1]\underline{0} \parallel_{\{h\}} [1]\underline{0}) \setminus \mathcal{A}_\mathcal{H}$ 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 probabilistic branching bisimilar to $(E_1 \parallel_{\{h\}} E_2) \setminus \mathcal{A}_\mathcal{H}$ when $l_1 \neq l_2$. Note that $(E_1 \parallel_{\{h\}} E_2) / \mathcal{A}_\mathcal{H} \approx (E_1 \parallel_{\{h\}} E_2) \setminus \mathcal{A}_\mathcal{H}$ 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 $(E_1 \parallel_{\{h\}} E_2) \setminus \mathcal{A}_\mathcal{H} \Longrightarrow ([1]\underline{0} \parallel_{\{h\}} [1]\underline{0}) \setminus \mathcal{A}_\mathcal{H}$. As noted in [15], it is not only a matter of the higher

discriminating power of $\approx_{\rm pb}$ with respect to $\approx_p$. If we used the parallel composition operator of [32], which turns into τ the synchronization of two actions 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 with a single τ-transition reaching the parallel composition of $\underline{0}$ and $\underline{0}$ with restriction on $\mathcal{A}_{\mathcal{H}}$.

Like for the nondeterministic case [16,15], none of the considered noninterference properties is compositional with respect to alternative composition. As an example, let us consider the processes $E_1 := l\,.\,\underline{0}$ and $E_2 := h\,.\,\underline{0}$, where we omit [1] before $\underline{0}$. Assuming $\approx \in \{\approx_{\rm p}, \approx_{\rm pb}\}$, both are BSNNI$_\approx$, as $l\,.\,\underline{0}\backslash\{h\} \approx l\,.\,\underline{0}\,/\,\{h\}$ and $h\,.\,\underline{0}\setminus\{h\} \approx h\,.\,\underline{0}\,/\,\{h\}$, but $E_1 + E_2 \notin$ BSNNI$_\approx$ because $(l\,.\,\underline{0} + h\,.\,\underline{0})\setminus\{h\} \approx l\,.\,\underline{0} \not\approx l\,.\,\underline{0} + \tau\,.\,\underline{0} \approx (l\,.\,\underline{0} + h\,.\,\underline{0})\,/\,\{h\}$. It can be easily checked that $E_1 + E_2 \notin \mathcal{P}$ for $\mathcal{P} = \{\text{BNDC}_\approx, \text{SBSNNI}_\approx, \text{SBNDC}_\approx\}$.

4.2 Taxonomy of Security Properties

First of all, as in the nondeterministic case the properties listed in Section 3 are increasingly finer. This result holds for both the $\approx_{\rm p}$-based and $\approx_{\rm pb}$-based noninterference properties.

Theorem 3. *Let $\approx \in \{\approx_{\rm p}, \approx_{\rm pb}\}$. Then:*

$$\text{SBNDC}_\approx \subset \text{SBSNNI}_\approx = \text{P\_BNDC}_\approx \subset \text{BNDC}_\approx \subset \text{BSNNI}_\approx$$ ■

All the inclusions are strict as we now show (we omit every occurrence of [1]):

- The process $\tau\,.\,l\,.\,\underline{0} + l\,.\,l\,.\,\underline{0} + h\,.\,l\,.\,\underline{0}$ is SBSNNI$_\approx$ (resp. P_BDNC$_\approx$) because $(\tau\,.\,l\,.\,\underline{0} + l\,.\,l\,.\,\underline{0} + h\,.\,l\,.\,\underline{0}) \setminus \{h\} \approx (\tau\,.\,l\,.\,\underline{0} + l\,.\,l\,.\,\underline{0} + h\,.\,l\,.\,\underline{0})/\{h\}$ and action h is enabled only by the initial process so every derivative is BSNNI$_\approx$ (resp. BNDC$_\approx$). It is not SBNDC$_\approx$ because the low-level view of the process reached after action h, i.e., $(l\,.\,\underline{0})\setminus\{h\}$, is neither weak probabilistic nor probabilistic branching bisimilar 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 BNDC$_\approx$ 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. The process is not SBSNNI$_\approx$ (resp. P_BNDC$_\approx$) because the reachable process $h\,.\,l\,.\,\underline{0}$ is not BSNNI$_\approx$ (resp. BNDC$_\approx$).
- The process $l\,.\,\underline{0} + h\,.\,h\,.\,l\,.\,\underline{0}$ is BSNNI$_\approx$ due to $(l\,.\,\underline{0} + h\,.\,h\,.\,l\,.\,\underline{0})\setminus\{h\} \approx (l\,.\,\underline{0} + h\,.\,h\,.\,l\,.\,\underline{0})/\{h\}$, but is not BNDC$_\approx$ due to $(((l\,.\,\underline{0} + h\,.\,h\,.\,l\,.\,\underline{0}) \parallel_{\{h\}} (h\,.\,\underline{0}))/\{h\}) \setminus \{h\} \not\approx (l\,.\,\underline{0} + h\,.\,h\,.\,l\,.\,\underline{0}) \setminus \{h\}$ as $(l\,.\,\underline{0} + h\,.\,h\,.\,l\,.\,\underline{0}) \setminus \{h\}$ behaves as $l\,.\,\underline{0}$.

Secondly, we observe that all the $\approx_{\rm pb}$-based noninterference properties imply the corresponding $\approx_{\rm p}$-based ones, due to the fact that $\approx_{\rm pb}$ is finer than $\approx_{\rm p}$.

Theorem 4. *The following inclusions hold:*

1. BSNNI$_{\approx_{\rm pb}} \subset$ BSNNI$_{\approx_{\rm p}}$.
2. BNDC$_{\approx_{\rm pb}} \subset$ BNDC$_{\approx_{\rm p}}$.
3. SBSNNI$_{\approx_{\rm pb}} \subset$ SBSNNI$_{\approx_{\rm p}}$.
4. P_BNDC$_{\approx_{\rm pb}} \subset$ P_BNDC$_{\approx_{\rm p}}$.
5. SBNDC$_{\approx_{\rm pb}} \subset$ SBNDC$_{\approx_{\rm p}}$. ■

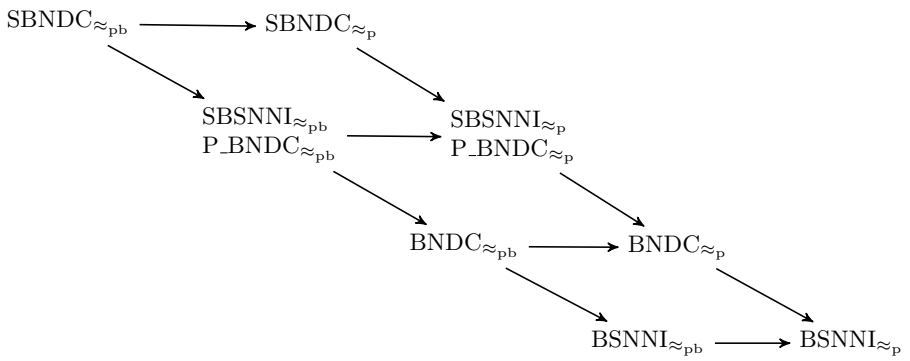

Fig. 2. Taxonomy of security properties based on probabilistic bisimilarities

All the inclusions above are strict due to the following result; for an example of E_1 and E_2 below, see Figure 1.

Theorem 5. *Let $E_1, E_2 \in \mathbb{P}_{\rm n}$ be such that $E_1 \approx_{\rm p} E_2$ but $E_1 \not\approx_{\rm pb} E_2$. 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. *$F \in \text{BSNNI}_{\approx_{\rm p}}$ but $F \notin \text{BSNNI}_{\approx_{\rm pb}}$.*
2. *$F \in \text{BNDC}_{\approx_{\rm p}}$ but $F \notin \text{BNDC}_{\approx_{\rm pb}}$.*
3. *$F \in \text{SBSNNI}_{\approx_{\rm p}}$ but $F \notin \text{SBSNNI}_{\approx_{\rm pb}}$.*
4. *$F \in \text{P\_BNDC}_{\approx_{\rm p}}$ but $F \notin \text{P\_BNDC}_{\approx_{\rm pb}}$.*
5. *$F \in \text{SBNDC}_{\approx_{\rm p}}$ but $F \notin \text{SBNDC}_{\approx_{\rm pb}}$.* ■

Based on the results in Theorems 3 and 4, the diagram in Figure 2 summarizes the inclusions among the various noninterference properties, 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 case [15]. The missing arrows in the diagram, witnessing incomparability, are justified by the following counterexamples:

- SBNDC$_{\approx_{\rm p}}$ vs. SBSNNI$_{\approx_{\rm pb}}$. The process $\tau\,.\,l\,.\,\underline{0}+l\,.\,l\,.\,\underline{0}+h\,.\,l\,.\,\underline{0}$ is BSNNI$_{\approx_{\rm pb}}$ as $\tau\,.\,l\,.\,\underline{0}+l\,.\,l\,.\,\underline{0} \approx_{\rm pb} \tau\,.\,l\,.\,\underline{0}+l\,.\,l\,.\,\underline{0}+\tau\,.\,l\,.\,\underline{0}$. It is also SBSNNI$_{\approx_{\rm pb}}$ because every reachable process does not enable any more high-level actions. However, it is not SBNDC$_{\approx_{\rm p}}$, because after executing the high-level action h it can perform a single action l, while the original process with the restriction on high-level actions can go along a path where it performs two l-actions. On the other hand, the process F mentioned in Theorem 5 is SBNDC$_{\approx_{\rm p}}$ but neither BSNNI$_{\approx_{\rm pb}}$ nor SBSNNI$_{\approx_{\rm pb}}$.
- SBSNNI$_{\approx_{\rm p}}$ vs. BNDC$_{\approx_{\rm pb}}$. The process $l\,.\,h\,.\,l\,.\,\underline{0}+l\,.\,\underline{0}+l\,.\,l\,.\,\underline{0}$ is BSNNI$_{\approx_{\rm pb}}$ as $l\,.\,\underline{0}+l\,.\,\underline{0}+l\,.\,l\,.\,\underline{0} \approx_{\rm pb} l\,.\,\tau\,.\,l\,.\,\underline{0}+l\,.\,\underline{0}+l\,.\,l\,.\,\underline{0}$. The same process is BNDC$_{\approx_{\rm pb}}$ too as it includes only one high-level action, hence the only possible high-level strategy coincides with the check conducted by BSNNI$_{\approx_{\rm pb}}$. However,

the process is not $\text{SBSNNI}_{\approx_\text{p}}$ because of the reachable process $h\,.\,l\,.\,\underline{0}$, which is not $\text{BSNNI}_{\approx_\text{p}}$. On the other hand, the process F mentioned in Theorem 5 is $\text{SBSNNI}_{\approx_\text{p}}$ but not $\text{BSNNI}_{\approx_\text{pb}}$ and, therefore, cannot be $\text{BNDC}_{\approx_\text{pb}}$.
- $\text{BNDC}_{\approx_\text{p}}$ vs. $\text{BSNNI}_{\approx_\text{pb}}$. 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 $\text{BSNNI}_{\approx_\text{pb}}$ as discussed in Section 3, but it is not $\text{BNDC}_{\approx_\text{p}}$. In contrast, the process F mentioned in Theorem 5 is both $\text{BSNNI}_{\approx_\text{p}}$ and $\text{BNDC}_{\approx_\text{p}}$, but not $\text{BSNNI}_{\approx_\text{pb}}$.

As for the nondeterministic case [15], the strongest property based on weak probabilistic bisimilarity ($\text{SBNDC}_{\approx_\text{p}}$) and the weakest property based on probabilistic branching bisimilarity ($\text{BSNNI}_{\approx_\text{pb}}$) 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 5, it is very easy to construct processes that are secure under properties based on $\approx_\text{p}$ but not on $\approx_\text{pb}$, due to the minimal number of high-level actions in F.

4.3 Relating Nondeterministic and Probabilistic Taxonomies

We now compare our probabilistic taxonomy to the nondeterministic one of [15]. In the following, we assume that $\approx$ denotes the weak bisimilarity of [32] and $\approx_\text{b}$ the branching bisimilarity of [21]. These can be obtained by restricting the definitions in Section 2.2 to nondeterministic states and by ignoring the clause involving the *prob* function. Since we are considering probabilistic choices as internal, given a process $E \in \mathbb{P}$ we can obtain its nondeterministic variant, denoted by $nd(E)$, by replacing each probability prefix by τ and each probabilistic choice operator by a nondeterministic choice operator. The next proposition states that if two processes are equivalent according to any of the weak bisimilarities in Section 2.2, then their nondeterministic variants are equivalent according to the corresponding nondeterministic bisimilarity.

Proposition 1. *Let $E_1, E_2 \in \mathbb{P}$. Then:*

- $E_1 \approx_\text{p} E_2 \Longrightarrow nd(E_1) \approx nd(E_2)$.
- $E_1 \approx_\text{pb} E_2 \Longrightarrow nd(E_1) \approx_\text{b} nd(E_2)$. ■

The inverse does not hold. Consider, e.g., the processes E_1 and E_2 defined as $[0.5]l_1\,.\,\underline{0} \oplus [0.5]l_2\,.\,\underline{0}$ and $[0.8]l_1\,.\,\underline{0} \oplus [0.2]l_2\,.\,\underline{0}$ respectively. Clearly, $E_1 \not\approx_\text{p} E_2$ (resp. $E_1 \not\approx_\text{pb} E_2$) but their nondeterministic counterparts are identical: $\tau\,.\,l_1\,.\,\underline{0} + \tau\,.\,l_2\,.\,\underline{0}$. An immediate consequence is that if a process is secure under any of the probabilistic noninterference properties in Section 3, then its nondeterministic variant is secure under the corresponding nondeterministic property. Therefore, the taxonomy in Figure 2 extends to the left the one in [15], as each of the property in Section 3 is finer than its nondeterministic counterpart.

Corollary 1. *Let $E \in \mathbb{P}, \approx_\text{pr} \in \{\approx_\text{p}, \approx_\text{pb}\}, \approx_\text{nd} \in \{\approx, \approx_\text{b}\}$, $\mathcal{P}_\text{pr} \in \{\text{BSNNI}_{\approx_\text{pr}}, \text{BNDC}_{\approx_\text{pr}}, \text{SBSNNI}_{\approx_\text{pr}}, \text{P\_BNDC}_{\approx_\text{pr}}, \text{SBNDC}_{\approx_\text{pr}}\}$, and $\mathcal{P}_\text{nd} \in \{\text{BSNNI}_{\approx_\text{nd}}, \text{BNDC}_{\approx_\text{nd}}, \text{SBSNNI}_{\approx_\text{nd}}, \text{P\_BNDC}_{\approx_\text{nd}}, \text{SBNDC}_{\approx_\text{nd}}\}$. Then:*

$$E \in \mathcal{P}_\text{pr} \Longrightarrow nd(E) \in \mathcal{P}_\text{nd}$$ ■

5 Weak Probabilistic Back-and-Forth Bisimilarity

In [14] it was shown that, for nodeterministic processes, weak back-and-forth bisimilarity coincides with branching bisimilarity. In this section we extend that result to probabilistic processes, so that probabilistic branching bisimilarity can be employed in the noninterference analysis of reversible processes.

A PLTS $(\mathcal{S}, \mathcal{A}_\tau, \longrightarrow)$ 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 [14] 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 [14] to our strictly alternating probabilistic setting. We use ℓ for a label in $\mathcal{A}_\tau \cup \mathbb{R}_{]0,1[}$.

Definition 7. *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 8. *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 $\rho \xrightarrow{\ell} \rho'$ 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 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 [14], given a run ρ we distinguish between *outgoing* and *incoming* action transitions of ρ during the weak bisimulation game. Like in [8], 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. Even a simpler clause requiring for any two related states that they both have incoming probabilistic transitions, or neither has, would distinguish the two states exemplified before.

Definition 9. *Let $(\mathcal{S}, \mathcal{A}_\tau, \longrightarrow)$ 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* $\rho_1 \xrightarrow{a}_{\mathrm{a}} \rho_1'$ *there exists* $\rho_2 \stackrel{\hat{a}}{\Longrightarrow} \rho_2'$ *with* $(\rho_1', \rho_2') \in \mathcal{B}$.
- *For each* $\rho_1' \xrightarrow{a}_{\mathrm{a}} \rho_1$ *there exists* $\rho_2' \stackrel{\hat{a}}{\Longrightarrow} \rho_2$ *with* $(\rho_1', \rho_2') \in \mathcal{B}$.
- $prob(\rho_1, C) = prob(\rho_2, C)$ *for all equivalence classes* $C \in \mathcal{U}/\mathcal{B}$. ■

We show that weak probabilistic back-and-forth bisimilarity over runs coincides with the forward-only probabilistic branching bisimilarity over states of [3] recalled in Section 2.2. We proceed by adopting the proof strategy followed in [14] to show that their weak back-and-forth bisimilarity over runs coincides with the forward-only branching bisimilarity over states of [21]. Therefore we start by proving that $\approx_{\mathrm{pbf}}$ satisfies the *cross property*. This means that, whenever two runs of two $\approx_{\mathrm{pbf}}$-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 $\approx_{\mathrm{pbf}}$-equivalent to the source run of the other sequence, then the two target runs are $\approx_{\mathrm{pbf}}$-equivalent to each other as well.

Lemma 2. *Let* $s_1, s_2 \in \mathcal{S}$ *with* $s_1 \approx_{\mathrm{pbf}} s_2$. *For all* $\rho_1', \rho_1'' \in run(s_1)$ *such that* $\rho_1' \Longrightarrow \rho_1''$ *with* $last(\rho_1'') \in \mathcal{S}_{\mathrm{n}}$ *and for all* $\rho_2', \rho_2'' \in run(s_2)$ *such that* $\rho_2' \Longrightarrow \rho_2''$ *with* $last(\rho_2'') \in \mathcal{S}_{\mathrm{n}}$, *if* $\rho_1' \approx_{\mathrm{pbf}} \rho_2''$ *and* $\rho_1'' \approx_{\mathrm{pbf}} \rho_2'$ *then* $\rho_1'' \approx_{\mathrm{pbf}} \rho_2''$. ■

Theorem 6. *Let* $s_1, s_2 \in \mathcal{S}$. *Then* $s_1 \approx_{\mathrm{pbf}} s_2 \iff s_1 \approx_{\mathrm{pb}} s_2$. ■

Therefore the properties $\mathrm{BSNNI}_{\approx_{\mathrm{pb}}}$, $\mathrm{BNDC}_{\approx_{\mathrm{pb}}}$, $\mathrm{SBSNNI}_{\approx_{\mathrm{pb}}}$, $\mathrm{P\_BNDC}_{\approx_{\mathrm{pb}}}$, and $\mathrm{SBNDC}_{\approx_{\mathrm{pb}}}$ do not change if $\approx_{\mathrm{pb}}$ is replaced by $\approx_{\mathrm{pbf}}$. This allows us to study noninterference properties for reversible probabilistic systems by using $\approx_{\mathrm{pb}}$ in a probabilistic process calculus like the one of Section 2.3, without having to resort to external memories [12] of communication keys [36].

6 Use Case: Probabilistic Smart Contracts

Consider a lottery implemented through a probabilistic smart contract [11] based on a public blockchain, like, e.g., Ethereum. Initially, anyone can buy a ticket by invoking a dedicated smart contract function that allows the user 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.

In this setting, we model and verify two known vulnerabilities discussed in [11]. The former will allow us to emphasize the need for passing from the nondeterministic noninterference analysis to the probabilistic one. Indeed, the critical point is the randomization process of the 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 an adversary that buys a ticket and succeeds in mining the block above by using a timestamp that allows the adversary to win the lottery.

Since both honest users and the adversary employ the same functionalities of the smart contract, we consider the invocations of the smart contract functions as publicly observable low-level actions. To distinguish the interactions of the adversary from those of honest users, such actions are guarded by a high-level action h whenever they refer to the adversary. 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 malicious behaviors of the adversary.

For simplicity, we assume there are only two users buying one ticket each, where the adversary buys ticket 0 while the honest user buys ticket 1. This scenario can be modeled in our probabilistic framework as follows:

$$\begin{array}{l}\tau \,.\, \mathit{draw} \,.\, ([0.5]\mathit{address}_0 \,.\, \mathit{win}_0 \,.\, \underline{0} \oplus [0.5]\mathit{address}_1 \,.\, \mathit{win}_1 \,.\, \underline{0}) + \\ h \,.\, \mathit{draw} \,.\, ([1-\varepsilon]\mathit{address}_0 \,.\, \mathit{win}_0 \,.\, \underline{0} \oplus [\varepsilon]\mathit{address}_1 \,.\, \mathit{win}_1 \,.\, \underline{0})\end{array}$$

The extraction procedure is conducted either by the honest user (action τ) or by the adversary (see the unique high-level action h). In both cases, the action *draw*, modeling the invocation of function draw(), leads to the probabilistic extraction of the ticket, the determination of the winner (actions $\mathit{address}_i$), and the notification to the winner (actions win_i).

By comparing the two branches, we note that in the former the probabilistic extraction is fair, while in the latter the adversary is able to pilot the extraction at will ($\varepsilon > 0$ is considered to be negligible). However, it is easy to see that this interfering behavior cannot be detected in a purely nondeterministic setting, as the two branches are identical if we abstract away from probabilities (after the initial choice, they are both mapped to the nondeterministic process $\mathit{address}_0 \,.\, \mathit{win}_0 \,.\, \underline{0} + \mathit{address}_1 \,.\, \mathit{win}_1 \,.\, \underline{0}$). As a consequence, all the nondeterministic security properties are satisfied for both bisimilarities. In the probabilistic setting, the interference is captured by the $\mathrm{BSNNI}_{\approx_{\mathrm{pr}}}$ property, for $\approx_{\mathrm{pr}} \in \{\approx_{\mathrm{p}}, \approx_{\mathrm{pb}}\}$, in analogy with the counterexample discussed after Proposition 1.

While this example confirms that the detection of probabilistic covert channels requires probabilistic security properties, the second vulnerability we present emphasizes the difference between the two probabilistic bisimilarities. The critical point is the mining procedure. Even assuming that the seed governing the probabilistic extraction cannot be manipulated, if the miner invoking the function draw() is malicious and is going to lose the lottery, that miner can ignore the related block and force the mining failure. Hence, with respect to the previous example, we use additional low-level actions denoting the mining process (action *mine*) and the successful writing to the blockchain (action *success*) or its failure (action *failure*). We model the described behavior through the following process:

$$\begin{array}{l}\mathit{draw} \,.\, ([0.5]\mathit{address}_0 \,.\, \mathit{win}_0 \,.\, \mathit{mine} \,.\, (\mathit{success} \,.\, \underline{0} + \tau \,.\, \mathit{failure} \,.\, \underline{0}) \oplus \\ \qquad [0.5]\mathit{address}_1 \,.\, \mathit{win}_1 \,. \\ \qquad\qquad (\mathit{mine} \,.\, (\mathit{success} \,.\, \underline{0} + \tau \,.\, \mathit{failure} \,.\, \underline{0}) + \\ \qquad\qquad\; h \,.\, (\mathit{mine} \,.\, (\mathit{success} \,.\, \underline{0} + \tau \,.\, \mathit{failure} \,.\, \underline{0}) + \\ \qquad\qquad\qquad \mathit{mine} \,.\, \mathit{failure} \,.\, \underline{0})))\end{array}$$

As mentioned before, the adversary cannot manipulate the seed to affect the extraction. Hence, the probabilistic extraction is fair in any case. However, the adversary can try to interfere if the result of the extraction makes him lose (i.e.,

it is different from ticket 0). On the one hand, consider the behavior after action win_0, which models the block mining procedure. The action *mine* expresses that the mining process is initiated by a honest miner, as no high-level interaction occurred. 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 such a failure (e.g., a wrong transaction in the block or a fork in the blockchain).

On the other hand, in the behavior after action win_1, the adversary decides to compete in the mining procedure (see the choice between the action *mine*, leading to the same behavior surveyed above, and the high-level action h, modeling that the mining procedure may be governed by the adversary). If h is chosen, the race between a honest miner and the adversary is solved nondeterministically through a choice between two actions *mine*. In fact, such a nondeterministic choice models a real-world scenario in which all the potential miners try to solve the cryptographic puzzle needed to add a block to the blockchain. The former branch leads to the behavior of the honest miner, while the latter enables the malicious behavior by leading immediately to the action *failure*.

Formally, the process is $\text{SBNDC}_{\approx_{\text{p}}}$. In particular, it is sufficient to observe that we have only one occurrence of the high-level action h and that the subprocess $mine\,.\,(success\,.\,\underline{0} + \tau\,.\,failure\,.\,\underline{0})$ – denoting the low-level view before executing h – is weakly probabilistic bisimilar to the subprocess $mine\,.\,(success\,.\,\underline{0} + \tau\,.\,failure\,.\,\underline{0}) + mine\,.\,failure\,.\,\underline{0}$ – denoting the low-level view after executing h.

However, the process is not $\text{BSNNI}_{\approx_{\text{pb}}}$. The reason is that the subprocess $mine\,.\,(success\,.\,\underline{0} + \tau\,.\,failure\,.\,\underline{0})$ is not probabilistic branching bisimilar to the subprocess:

$$mine\,.\,(success\,.\,\underline{0} + \tau\,.\,failure\,.\,\underline{0}) + \tau\,.\,(mine\,.\,(success\,.\,\underline{0} + \tau\,.\,failure\,.\,\underline{0}) + mine\,.\,failure\,.\,\underline{0})$$

This depends on the fact that $mine\,.\,(success\,.\,\underline{0} + \tau\,.\,failure\,.\,\underline{0})$ is not probabilistic branching bisimilar to $mine\,.\,(success\,.\,\underline{0} + \tau\,.\,failure\,.\,\underline{0}) + mine\,.\,failure\,.\,\underline{0}$, while they are equated by $\approx_{\text{p}}$. Indeed, the former process cannot respond whenever the latter executes the right-hand action *mine* leading to a state where only the action *failure* is possible.

We employ also the back-and-forth interpretation of the $\text{BSNNI}_{\approx_{\text{pb}}}$ check to show the result above in the setting of reversible systems. In the subprocess including the hidden high-level action h, notice that undoing the action *failure* of the branch $mine\,.\,failure\,.\,\underline{0}$ reveals that the failure has been forced by the adversary. If, instead, we consider the subprocess $mine\,.\,(success\,.\,\underline{0} + \tau\,.\,failure\,.\,\underline{0})$, we observe that undoing the action *failure* reveals that the failure has been the consequence of a choice involving also the action *success*. Hence, it was not deliberately caused by the miner. This is sufficient to expose the behavior of the adversary. In other words, in a reversible system allowing for execution flow debugging, it is possible to capture the malicious behavior of the adversary.

To conclude, the noninterference analysis based on the strongest $\approx_{\text{p}}$-based property of Figure 2 fails to reveal the covert channel caused by the adversary, while the weakest $\approx_{\text{pb}}$-based property of Figure 2 can detect it.

7 Conclusions

In this paper we have investigated a taxonomy of noninterference properties for processes featuring both nondeterminism and probabilities, along with the preservation and compositionality aspects of such properties. The two behavioral equivalences that we have considered for those noninterference properties are a weak probabilistic bisimilarity inspired by the one in [35] and the probabilistic branching bisimilarity of [3].

Since we have shown that the latter coincides with a probabilistic variant of the weak back-and-forth bisimilarity of [14], the noninterference properties based on the latter can be applied to reversible probabilistic systems, thereby extending our previous results in [15] for reversible systems that are fully nondeterministic. Our work also extends the one of [2], where generative-reactive probabilistic systems are considered, in a way that avoids additional universal quantifications over probabilistic parameters in the formalization of noninterference properties.

The nondeterministic and probabilistic model that we have employed is the strictly alternating one of [23], where states are divided into nondeterministic and probabilistic. Each of the former may have action-labeled transitions to probabilistic states, while each of the latter may have probability-labeled transitions to nondeterministic states (in the non-strictly alternating variant of [35] action transitions are admitted also between two nondeterministic states). An alternative model is the non-alternating one given by Segala simple probabilistic automata [42], where every transition is labeled with an action and goes from a state to a probability distribution over states. Regardless of the adopted model, it is worth observing that some characteristics seem to be independent from probabilities, as witnessed by almost all the counterexamples in Section 4.

Both the alternating model and the non-alternating one – whose relationships have been studied in [44] – encompass nondeterministic models, generative models, and reactive models as special cases. Since branching bisimulation semantics plays a fundamental role in reversible systems [14,7], in this paper we have adopted the alternating model because of the probabilistic branching bisimulation congruence developed for it in [3] 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 [43], 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 not to be decidable in polynomial time [10].

As far as future extensions are concerned, we would like to include recursion in the considered process language. This requires identifying a suitable probabilistic variant of the up-to technique for weak bisimilarity [40], to be used in the proof of certain results in place of proceeding by induction on the depth of the tree-like PLTS underlying the considered process term.

Acknowledgment. This research has been supported by the PRIN 2020 project *NiRvAna – Noninterference and Reversibility Analysis in Private Blockchains.*

References

1. Aldini, A.: Classification of security properties in a Linda-like process algebra. Science of Computer Programming **63**, 16–38 (2006)
2. Aldini, A., Bravetti, M., Gorrieri, R.: A process-algebraic approach for the analysis of probabilistic noninterference. Journal of Computer Security **12**, 191–245 (2004)
3. Andova, S., Georgievska, S., Trcka, N.: Branching bisimulation congruence for probabilistic systems. Theoretical Computer Science **413**, 58–72 (2012)
4. Baier, C., Hermanns, H.: Weak bisimulation for fully probabilistic processes. In: Proc. of the 9th Int. Conf. on Computer Aided Verification (CAV 1997). LNCS, vol. 1254, pp. 119–130. Springer (1997)
5. Barbuti, R., Tesei, L.: A decidable notion of timed non-interference. Fundamenta Informaticae **54**, 137–150 (2003)
6. Bennett, C.H.: Logical reversibility of computation. IBM Journal of Research and Development **17**, 525–532 (1973)
7. Bernardo, M., Esposito, A.: 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). EPTCS, vol. 390, pp. 67–81 (2023)
8. Bernardo, M., Mezzina, C.A.: Bridging causal reversibility and time reversibility: A stochastic process algebraic approach. Logical Methods in Computer Science **19(2:6)**, 1–27 (2023)
9. Brookes, S., Hoare, C., Roscoe, A.: A theory of communicating sequential processes. Journal of the ACM **31**, 560–599 (1984)
10. Cattani, S., Segala, R.: Decision algorithms for probabilistic bisimulation. In: Proc. of the 13th Int. Conf. on Concurrency Theory (CONCUR 2002). LNCS, vol. 2421, pp. 371–385. Springer (2002)
11. Chatterjee, K., Goharshady, A.K., Pourdamghani, A.: Probabilistic smart contracts: Secure randomness on the blockchain. In: Proc. of the 1st IEEE Int. Conf. on Blockchain and Cryptocurrency (ICBC 2019). pp. 403–412. IEEE-CS Press (2019)
12. Danos, V., Krivine, J.: Reversible communicating systems. In: Proc. of the 15th Int. Conf. on Concurrency Theory (CONCUR 2004). LNCS, vol. 3170, pp. 292–307. Springer (2004)
13. Danos, V., Krivine, J.: Transactions in RCCS. In: Proc. of the 16th Int. Conf. on Concurrency Theory (CONCUR 2005). LNCS, vol. 3653, pp. 398–412. Springer (2005)
14. De Nicola, R., Montanari, U., Vaandrager, F.: Back and forth bisimulations. In: Proc. of the 1st Int. Conf. on Concurrency Theory (CONCUR 1990). LNCS, vol. 458, pp. 152–165. Springer (1990)
15. Esposito, A., Aldini, A., Bernardo, M.: 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). LNCS, vol. 13910, pp. 57–74. Springer (2023)
16. Focardi, R., Gorrieri, R.: Classification of security properties. In: Proc. of the 1st Int. School on Foundations of Security Analysis and Design (FOSAD 2000). LNCS, vol. 2171, pp. 331–396. Springer (2001)
17. Focardi, R., Rossi, S.: Information flow security in dynamic contexts. Journal of Computer Security **14**, 65–110 (2006)

18. Giachino, E., Lanese, I., Mezzina, C.A.: Causal-consistent reversible debugging. In: Proc. of the 17th Int. Conf. on Fundamental Approaches to Software Engineering (FASE 2014). LNCS, vol. 8411, pp. 370–384. Springer (2014)
19. van Glabbeek, R.J.: The linear time – branching time spectrum I. In: Handbook of Process Algebra. pp. 3–99. Elsevier (2001)
20. van Glabbeek, R.J., Smolka, S.A., Steffen, B.: Reactive, generative and stratified models of probabilistic processes. Information and Computation **121**, 59–80 (1995)
21. van Glabbeek, R.J., Weijland, W.P.: Branching time and abstraction in bisimulation semantics. Journal of the ACM **43**, 555–600 (1996)
22. Goguen, J.A., Meseguer, J.: Security policies and security models. In: Proc. of the 2nd IEEE Symp. on Security and Privacy (SSP 1982). pp. 11–20. IEEE-CS Press (1982)
23. Hansson, H., Jonsson, B.: A calculus for communicating systems with time and probabilities. In: Proc. of the 11th IEEE Real-Time Systems Symp. (RTSS 1990). pp. 278–287. IEEE-CS Press (1990)
24. Hedin, D., Sabelfeld, A.: A perspective on information-flow control. In: Software Safety and Security – Tools for Analysis and Verification. pp. 319–347. IOS Press (2012)
25. Hillston, J., Marin, A., Piazza, C., Rossi, S.: Persistent stochastic non-interference. Fundamenta Informaticae **181**, 1–35 (2021)
26. Keller, R.M.: Formal verification of parallel programs. Communications of the ACM **19**, 371–384 (1976)
27. Landauer, R.: Irreversibility and heat generation in the computing process. IBM Journal of Research and Development **5**, 183–191 (1961)
28. Lanese, I., Lienhardt, M., Mezzina, C.A., Schmitt, A., Stefani, J.B.: Concurrent flexible reversibility. In: Proc. of the 22nd European Symp. on Programming (ESOP 2013). LNCS, vol. 7792, pp. 370–390. Springer (2013)
29. Lanese, I., Nishida, N., Palacios, A., Vidal, G.: CauDEr: A causal-consistent reversible debugger for Erlang. In: Proc. of the 14th Int. Symp. on Functional and Logic Programming (FLOPS 2018). LNCS, vol. 10818, pp. 247–263. Springer (2018)
30. Laursen, J., Ellekilde, L.P., Schultz, U.: Modelling reversible execution of robotic assembly. Robotica **36**, 625–654 (2018)
31. Mantel, H.: Information flow and noninterference. In: Encyclopedia of Cryptography and Security. pp. 605–607. Springer (2011)
32. Milner, R.: Communication and Concurrency. Prentice Hall (1989)
33. Park, D.: Concurrency and automata on infinite sequences. In: Proc. of the 5th GI Conf. on Theoretical Computer Science. LNCS, vol. 104, pp. 167–183. Springer (1981)
34. Perumalla, K., Park, A.: Reverse computation for rollback-based fault tolerance in large parallel systems – Evaluating the potential gains and systems effects. Cluster Computing **17**, 303–313 (2014)
35. Philippou, A., Lee, I., Sokolsky, O.: Weak bisimulation for probabilistic systems. In: Proc. of the 11th Int. Conf. on Concurrency Theory (CONCUR 2000). LNCS, vol. 1877, pp. 334–349. Springer (2000)
36. Phillips, I., Ulidowski, I.: Reversing algebraic process calculi. Journal of Logic and Algebraic Programming **73**, 70–96 (2007)
37. Phillips, I., Ulidowski, I., Yuen, S.: A reversible process calculus and the modelling of the ERK signalling pathway. In: Proc. of the 4th Int. Workshop on Reversible Computation (RC 2012). LNCS, vol. 7581, pp. 218–232. Springer (2012)

38. Pinna, G.M.: Reversing steps in membrane systems computations. In: Proc. of the 18th Int. Conf. on Membrane Computing (CMC 2017). LNCS, vol. 10725, pp. 245–261. Springer (2017)
39. Sabelfeld, A., Sands, D.: Probabilistic noninterference for multi-threaded programs. In: Proc. of the 13th IEEE Computer Security Foundations Workshop (CSF 2000). pp. 200–214 (2000)
40. Sangiorgi, D., Milner, R.: The problem of "weak bisimulation up to". In: Proc. of the 3rd Int. Conf. on Concurrency Theory (CONCUR 1992). LNCS, vol. 630, pp. 32–46. Springer (1992)
41. Schordan, M., Oppelstrup, T., Jefferson, D., Barnes Jr., P.: Generation of reversible C++ code for optimistic parallel discrete event simulation. New Generation Computing **36**, 257–280 (2018)
42. Segala, R.: Modeling and Verification of Randomized Distributed Real-Time Systems. PhD Thesis (1995)
43. Segala, R., Lynch, N.A.: Probabilistic simulations for probabilistic processes. In: Proc. of the 5th Int. Conf. on Concurrency Theory (CONCUR 1994). LNCS, vol. 836, pp. 481–496. Springer (1994)
44. Segala, R., Turrini, A.: 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). pp. 44–53. IEEE-CS Press (2005)
45. Siljak, H., Psara, K., Philippou, A.: Distributed antenna selection for massive MIMO using reversing Petri nets. IEEE Wireless Communication Letters **8**, 1427–1430 (2019)
46. Vassor, M., Stefani, J.B.: Checkpoint/rollback vs causally-consistent reversibility. In: Proc. of the 10th Int. Conf. on Reversible Computation (RC 2018). LNCS, vol. 11106, pp. 286–303. Springer (2018)
47. Volpano, D., Smith, G.: Probabilistic noninterference in a concurrent language. In: Proc. of the 11th IEEE Computer Security Foundations Workshop (CSF 1998). pp. 34–43. IEEE-CS Press (1998)
48. Vries, E., Koutavas, V., Hennessy, M.: Communicating transactions. In: Proc. of the 21st Int. Conf. on Concurrency Theory (CONCUR 2010). LNCS, vol. 6269, pp. 569–583. Springer (2010)

A Proofs of Results

Proof of Lemma 1. We first prove the result for the $\approx_{\rm p}$-based properties. Let $\mathcal{B}$ be a weak probabilistic bisimulation witnessing $E_1 \approx_{\rm p} E_2$:

- The symmetric relation $\mathcal{B}' = \{(a\,.\,F_1, a\,.\,F_2) \mid (F_1, F_2) \in \mathcal{B}\}$ is a weak probabilistic bisimulation too. The result immediately follows from the fact that if $a\,.\,F_1 \stackrel{a}{\longrightarrow}_{\rm a} F_1$ then $a\,.\,F_2 \Longrightarrow \stackrel{a}{\longrightarrow}_{\rm a} \Longrightarrow F_2$ and $(F_1, F_2) \in \mathcal{B}$. Since $a\,.\,F_1$ and $a\,.\,F_2$ are nondeterministic processes and $(F_1, F_2) \in \mathcal{B}$, it follows that for all equivalence classes $C \in \mathbb{P}/\mathcal{B}'$, $prob(a\,.\,F_1, C) = prob(a\,.\,F_2, C)$.
- The symmetric relation $\mathcal{B}' = \{(F_1 \parallel_L F, F_2 \parallel_L F) \mid (F_1, F_2) \in \mathcal{B} \wedge F \in \mathbb{P}\}$ is a weak probabilistic bisimulation too. There are three cases:
  - If $F_1 \parallel_L F \stackrel{a}{\longrightarrow}_{\rm a} F_1' \parallel_L F'$ with $a \in L$, then $F_1 \stackrel{a}{\longrightarrow}_{\rm a} F_1'$ (and $F \stackrel{a}{\longrightarrow}_{\rm a} F'$) and hence there exists a process F_2' such that $F_2 \Longrightarrow \stackrel{a}{\longrightarrow}_{\rm a} \Longrightarrow F_2'$ with $(F_1', F_2') \in \mathcal{B}$. Therefore $F_2 \parallel_L F \Longrightarrow \stackrel{a}{\longrightarrow}_{\rm a} \Longrightarrow F_2' \parallel_L F'$ with $(F_1' \parallel_L F', F_2' \parallel_L F') \in \mathcal{B}'$.
  - If $F_1 \parallel_L F \stackrel{a}{\longrightarrow}_{\rm a} F_1' \parallel_L [1]F$ with $a \notin L$, then $F_1 \stackrel{a}{\longrightarrow}_{\rm a} F_1'$ and hence there exists a process F_2' such that $F_2 \Longrightarrow \stackrel{a}{\longrightarrow}_{\rm a} \Longrightarrow F_2'$ (or $F_2 \Longrightarrow F_2'$ when $a = \tau$) with $(F_1', F_2') \in \mathcal{B}$. Therefore $F_2 \parallel_L F \Longrightarrow \stackrel{a}{\longrightarrow}_{\rm a} \Longrightarrow F_2' \parallel_L [1]F$ with $(F_1' \parallel_L [1]F, F_2' \parallel_L [1]F) \in \mathcal{B}'$.
  - The case $F_1 \parallel_L F \stackrel{a}{\longrightarrow}_{\rm a} [1]F_1 \parallel_L F'$ with $a \notin L$ is trivial.

  As far as probabilities are concerned, we start by observing that that for all $R_1, R_2, R_1', R_2' \in \mathbb{P}$ and for all $L \subseteq \mathcal{A}$, $prob(R_1 \parallel_L R_2, R_1' \parallel_L R_2') = prob(R_1, R_1') \cdot prob(R_2, R_2')$. If R_1 and R_2 are nondeterministic processes, then $prob(R_1, R_1') \cdot prob(R_2, R_2') = 1$ if $R_1 = R_1'$ and $R_2 = R_2'$ and $prob(R_1, R_1') \cdot prob(R_2, R_2') = 0$ otherwise. From this fact it follows that $prob(R_1 \parallel_L R_2, R_1' \parallel_L R_2') = 1$ if $R_1 \parallel_L R_2 = R_1' \parallel_L R_2'$, i.e., $R_1 = R_1'$ and $R_2 = R_2'$, and $prob(R_1 \parallel_L R_2, R_1' \parallel_L R_2') = 0$ otherwise. If R_1 and R_2 are both probabilistic processes, we have that $prob(R_1, R_1') = \sum_{R_1 \stackrel{p}{\longrightarrow}_{\rm p} R_1'} p$ and $prob(R_2, R_2') = \sum_{R_2 \stackrel{q}{\longrightarrow}_{\rm p} R_2'} q$ and hence $prob(R_1, R_1') \cdot prob(R_2, R_2') = \sum_{R_1 \stackrel{p}{\longrightarrow}_{\rm p} R_1'} p \cdot \sum_{R_2 \stackrel{q}{\longrightarrow}_{\rm p} R_2'} q = \sum_{R_1 \stackrel{p}{\longrightarrow}_{\rm p} R_1'} \sum_{R_2 \stackrel{q}{\longrightarrow}_{\rm p} R_2'} p \cdot q$, which, according to the rules in Table 2, is equal to $prob(R_1 \parallel_L R_2, R_1' \parallel_L R_2')$. With this result we observe that given an arbitrary equivalence class $D = [S \parallel_L F']_{\mathcal{B}}$, for $S \in \mathbb{P}_{\rm n}$, $prob(F_1 \parallel_L F, D) = \sum_{\bar{S} \parallel_L \bar{F'} \in D} prob(F_1 \parallel_L F, \bar{S} \parallel_L \bar{F'}) =$ $\sum_{\bar{S} \parallel_L \bar{F'} \in D} prob(F_1, \bar{S}) \cdot prob(\bar{F}, \bar{F'})$ (note that in this case F_1, F_2 and F are probabilistic processes, we consider only this as the case in which they are nondeterministic is straightforward). This in turn implies that $\sum_{\bar{S} \parallel_L \bar{F'} \in D} prob(F_1, \bar{S}) \cdot prob(\bar{F}, \bar{F'}) = \sum_{\bar{S} \approx_{\rm p} S, \bar{F'} \approx_{\rm p} F'} prob(F_1, \bar{S}) \cdot prob(F, \bar{F'})$ $= (\sum_{\bar{S} \approx_{\rm p} S} prob(F_1, \bar{S})) \cdot (\sum_{\bar{F'} \approx_{\rm p} F'} prob(F, \bar{F'}))$. By the same reasoning $prob(F_2 \parallel_L F, D) = (\sum_{\bar{S} \approx_{\rm p} S} prob(F_2, \bar{S})) \cdot (\sum_{\bar{F'} \approx_{\rm p} F'} prob(F, \bar{F'}))$. Lastly, from $F_1 \approx_{\rm p} F_2$ and $F \approx_{\rm p} F$ we obtain $(\sum_{\bar{S} \approx_{\rm p} S} prob(F_1, \bar{S})) \cdot (\sum_{\bar{F'} \approx_{\rm p} F'} prob(F, \bar{F'}))$ $= (\sum_{\bar{S} \approx_{\rm p} S} prob(F_2, \bar{S})) \cdot (\sum_{\bar{F'} \approx_{\rm p} F'} prob(F, \bar{F'}))$, and hence $prob(F_1 \parallel_L F, D) = prob(F_2 \parallel_L F, D)$.

– The symmetric relation $\mathcal{B}' = \{(F_1 \setminus L, F_2 \setminus L) \mid (F_1, F_2) \in \mathcal{B}\}$ is a weak probabilistic bisimulation too. There are two cases:

  - If $F_1 \setminus L \xrightarrow{\tau}_{\rm a} F_1' \setminus L$, then $F_1 \xrightarrow{\tau}_{\rm a} F_1'$ and hence there exists a process F_2' such that $F_2 \Longrightarrow F_2'$ with $(F_1', F_2') \in \mathcal{B}$. Since the restriction operator does not apply to τ nor to probabilistic transitions, it follows 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 $a \notin L \cup \{\tau\}$, then $F_1 \xrightarrow{a}_{\rm a} F_1'$ and hence there exists a process F_2' such that $F_2 \Longrightarrow \xrightarrow{a}_{\rm a} \Longrightarrow F_2'$ with $(F_1', F_2') \in \mathcal{B}$. Since the restriction operator does not apply to τ nor to probabilistic transitions and $a \notin L$, it follows 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 far as probabilities are concerned, from the fact that $(F_1, F_2) \in \mathcal{B}$ it follows that for all equivalence classes $C \in \mathbb{P}/\mathcal{B}$, $prob(F_1, C) = prob(F_2, C)$, and from the fact that the restriction operator does not apply to probabilistic transitions, it follows that for all equivalence classes $C \in \mathbb{P}/\mathcal{B}'$, $prob(F_1 \setminus L, C) = prob(F_2 \setminus L, C)$.

– The symmetric relation $\mathcal{B}' = \{(F_1 \,/\, L, F_2 \,/\, L) \mid (F_1, F_2) \in \mathcal{B}\}$ is a weak probabilistic bisimulation too. There are two cases:

  - 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 a process F_2' such that $F_2 \Longrightarrow \xrightarrow{b}_{\rm a} \Longrightarrow F_2'$ with $(F_1', F_2') \in \mathcal{B}$. Since the hiding operator does not apply to τ, it follows that $F_2 \,/\, L \Longrightarrow \xrightarrow{a}_{\rm a} \Longrightarrow F_2' \,/\, L$ with $(F_1' \,/\, L, F_2' \,/\, L) \in \mathcal{B}'$.
  - If $F_1 \,/\, L \xrightarrow{\tau}_{\rm a} F_1' \,/\, L$ with $F_1 \xrightarrow{\tau}_{\rm a} F_1'$, then there exists a process F_2' such that $F_2 \Longrightarrow F_2'$ with $(F_1', F_2') \in \mathcal{B}$. Since the hiding operator does not apply to τ nor to probabilistic transitions, it follows that $F_2 \,/\, L \Longrightarrow F_2' \,/\, L$ with $(F_1' \,/\, L, F_2' \,/\, L) \in \mathcal{B}'$.

  As far as probabilities are concerned, from the fact that $(F_1, F_2) \in \mathcal{B}$ it follows that for all equivalence classes $C \in \mathbb{P}/\mathcal{B}$, $prob(F_1, C) = prob(F_2, C)$, and from the fact that the hiding operator does not apply to probabilistic transitions, it follows that for all equivalence classes $C \in \mathcal{B}$, $prob(F_1 \,/\, L, C) = prob(F_2 \,/\, L, C)$.

We now prove the same result for $\approx_{\rm pb}$. Let $\mathcal{B}$ be a probabilistic branching bisimulation witnessing $E_1 \approx_{\rm pb} E_2$:

– The symmetric relation $\mathcal{B}' = \{(a \,.\, F_1, a \,.\, F_2) \mid (F_1, F_2) \in \mathcal{B}\}$ is a probabilistic branching bisimulation too. The result immediately follow from the fact that if $a \,.\, F_1 \xrightarrow{a}_{\rm a} F_1$ then $a \,.\, F_2 \Longrightarrow a \,.\, F_2 \xrightarrow{a}_{\rm a} F_2$, $(a \,.\, F_1, a \,.\, F_2) \in \mathcal{B}'$ and $(F_1, F_2) \in \mathcal{B}$. Since $a \,.\, F_1$ and $a \,.\, F_2$ are nondeterministic processes and $(F_1, F_2) \in \mathcal{B}$, it follows that for all equivalence classes $C \in \mathbb{P}/\mathcal{B}'$, $prob(a \,.\, F_1, C) = prob(a \,.\, F_2, C)$.
– The symmetric relation $\mathcal{B}' = \{(F_1 \parallel_L F, F_2 \parallel_L F) \mid (F_1, F_2) \in \mathcal{B} \wedge F \in \mathbb{P}\}$ is a probabilistic branching bisimulation too. There are three cases:

- If $F_1 \parallel_L F \xrightarrow{a}_{\rm a} F_1' \parallel_L F'$ with $a \in L$, then $F_1 \xrightarrow{a}_{\rm a} F_1'$ (and $F \xrightarrow{a}_{\rm a} F'$) and hence there exist $\bar{F}_2$ and F_2' such that $F_2 \Longrightarrow \bar{F}_2 \xrightarrow{a}_{\rm a} F_2'$ with $(F_1, \bar{F}_2) \in \mathcal{B}$ and $(F_1', F_2') \in \mathcal{B}$. Therefore $F_2 \parallel_L F \Longrightarrow \bar{F}_2 \parallel_L F \xrightarrow{a}_{\rm a} F_2' \parallel_L F'$ with $(F_1 \parallel_L F, \bar{F}_2 \parallel_L F) \in \mathcal{B}'$ and $(F_1' \parallel_L F', F_2' \parallel_L F') \in \mathcal{B}'$.
- If $F_1 \parallel_L F \xrightarrow{a}_{\rm a} F_1' \parallel_L [1]F$ with $a \notin L$, then $F_1 \xrightarrow{a}_{\rm a} F_1'$ and hence either $(F_1', F_2) \in \mathcal{B}$ when $a = \tau$, or there exist $\bar{F}_2$ and F_2' such that $F_2 \Longrightarrow \bar{F}_2 \xrightarrow{a}_{\rm a} F_2'$ with $(F_1, \bar{F}_2) \in \mathcal{B}$ and $(F_1', F_2') \in \mathcal{B}$. 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 $F_2 \parallel_L F \Longrightarrow \bar{F}_2 \parallel_L F \xrightarrow{a}_{\rm a} F_2' \parallel_L [1]F$ with $(F_1 \parallel_L F, \bar{F}_2 \parallel_L F) \in \mathcal{B}'$ and $(F_1' \parallel_L [1]F, F_2' \parallel_L [1]F) \in \mathcal{B}'$.
- The case $F_1 \parallel_L F \xrightarrow{a}_{\rm a} F_1 \parallel_L F'$ with $a \notin L$ is trivial.

As far as probabilites are concerned, the reasoning is the same as in the case of the compositionality of $\approx_{\rm p}$ with respect to the parallel operator (see the fourth case in the first part of the proof).

– The symmetric relation $\mathcal{B}' = \{(F_1 \backslash L, F_2 \backslash L) \mid (F_1, F_2) \in \mathcal{B}\}$ is a probabilistic branching bisimulation too. There are two cases:
  - If $F_1 \setminus L \xrightarrow{\tau}_{\rm a} F_1' \setminus L$, then $F_1 \xrightarrow{\tau}_{\rm a} F_1'$ and hence either $(F_1', F_2) \in \mathcal{B}$, or there exist $\bar{F}_2$ and F_2' such that $F_2 \Longrightarrow \bar{F}_2 \xrightarrow{\tau}_{\rm a} F_2'$ with $(F_1, \bar{F}_2) \in \mathcal{B}$ and $(F_1', F_2') \in \mathcal{B}$. Since the restriction operator does not apply to τ nor to 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 $F_2 \setminus L \Longrightarrow \bar{F}_2 \setminus L \xrightarrow{\tau}_{\rm a} F_2' \setminus L$, 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 $F_1 \backslash L \xrightarrow{a}_{\rm a} F_1' \backslash L$ with $a \notin L \cup \{\tau\}$, then $F_1 \xrightarrow{a}_{\rm a} F_1'$ and hence there exist $\bar{F}_2$ and F_2' such that $F_2 \Longrightarrow \bar{F}_2 \xrightarrow{a}_{\rm a} F_2'$ with $(F_1, \bar{F}_2) \in \mathcal{B}$ and $(F_1', F_2') \in \mathcal{B}$. Since the restriction operator does not apply to τ nor to probabilistic transitions and $a \notin L$, it follows that $F_2 \setminus L \Longrightarrow \bar{F}_2 \setminus L \xrightarrow{a}_{\rm a} F_2' \setminus L$ 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 far as probabilities are concerned, from the fact that $(F_1, F_2) \in \mathcal{B}$ it follows that for all equivalence classes $C \in \mathbb{P}/\mathcal{B}$, $prob(F_1, C) = prob(F_2, C)$, and from the fact that the restriction operator does not apply to probabilistic transitions, it follows that for all equivalence classes $C \in \mathbb{P}/\mathcal{B}'$, $prob(F_1 \setminus L, C) = prob(F_2 \setminus L, C)$. The same reasoning applies to the other pairs of processes mentioned in the proof.

– The symmetric relation $\mathcal{B}' = \{(F_1 \,/\, L, F_2 \,/\, L) \mid (F_1, F_2) \in \mathcal{B}\}$ is a probabilistic branching bisimulation too. There are two cases:
  - 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 exist $\bar{F}_2$ and F_2' such that $F_2 \Longrightarrow \bar{F}_2 \xrightarrow{b}_{\rm a} F_2'$ with $(F_1, \bar{F}_2) \in \mathcal{B}$ and $(F_1', F_2') \in \mathcal{B}$. Since the hiding operator does not apply to τ nor to probabilistic transitions, it follows that $F_2 \,/\, L \Longrightarrow \bar{F}_2 \,/\, L \xrightarrow{a}_{\rm a} F_2' \,/\, L$, with $(F_1 \,/\, L, \bar{F}_2 \,/\, L) \in \mathcal{B}'$ and $(F_1' \,/\, L, F_2' \,/\, L) \in \mathcal{B}'$.
  - If $F_1 \,/\, L \xrightarrow{\tau}_{\rm a} F_1' \,/\, L$ with $F_1 \xrightarrow{\tau}_{\rm a} F_1'$, then either $(F_1', F_2) \in \mathcal{B}$, or there exist $\bar{F}_2$ and F_2' such that $F_2 \Longrightarrow \bar{F}_2 \xrightarrow{\tau}_{\rm a} F_2'$ with $(F_1, \bar{F}_2) \in \mathcal{B}$ and $(F_1', F_2') \in \mathcal{B}$. Since the hiding operator does not apply to τ nor to 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 $F_2 \,/\, L \Longrightarrow \bar{F}_2 \,/\, L \xrightarrow{\tau}_{\rm a} F_2' \,/\, L$ with $(F_1 \,/\, L, \bar{F}_2 \,/\, L) \in \mathcal{B}'$ and $(F_1' \,/\, L, F_2' \,/\, L) \in \mathcal{B}'$. As far as probabilities are concerned, from the fact that $(F_1, F_2) \in \mathcal{B}$ it follows that for all equivalence classes $C \in \mathbb{P}/\mathcal{B}$, $prob(F_1, C) = prob(F_2, C)$, and from the fact that the hiding operator does not apply to probabilistic transitions, it follows that for all equivalence classes $C \in \mathbb{P}/\mathcal{B}'$, $prob(F_1 \,/\, L, C) = prob(F_2 \,/\, L, C)$. The same reasoning applies to the other pairs of processes mentioned in the proof. ■

Proof of Theorem 1. The results immediately follow from the fact that $\approx_{\rm p}$ and $\approx_{\rm pb}$ are congruences with respect to the parallel, restriction and hiding operators (see the proof of the Lemma 1). ■

Proof of Theorem 2. We divide the proof into two parts. In the first part we prove the theorem for the $\approx_{\rm p}$-based properties, and in the second part we do the same for the $\approx_{\rm pb}$-based properties. We first prove the results for $\text{SBSNNI}_{\approx_{\rm p}}$, and hence for $\text{P\_BNDC}_{\approx_{\rm p}}$ too by virtue of the forthcoming Theorem 3:

1. Given an arbitrary $E \in \text{SBSNNI}_{\approx_{\rm p}}$ and an arbitrary $a \in \mathcal{A}_{\mathcal{L}} \cup \{\tau\}$, from $E \setminus \mathcal{A}_{\mathcal{H}} \approx_{\rm p} E \,/\, \mathcal{A}_{\mathcal{H}}$ we derive that $a \,.\, (E \setminus \mathcal{A}_{\mathcal{H}}) \approx_{\rm p} a \,.\, (E \,/\, \mathcal{A}_{\mathcal{H}})$ because $\approx_{\rm p}$ is a congruence with respect to action prefix (see proof of Lemma 1), from which it follows that $(a \,.\, E) \setminus \mathcal{A}_{\mathcal{H}} \approx_{\rm p} (a \,.\, E) \,/\, \mathcal{A}_{\mathcal{H}}$, i.e., $a \,.\, E \in \text{BSNNI}_{\approx_{\rm p}}$, 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 $\text{BSNNI}_{\approx_{\rm p}}$.
2. Given two arbitrary $E_1, E_2 \in \text{SBSNNI}_{\approx_{\rm p}}$ and an arbitrary $L \subseteq \mathcal{A}$, the result follows by proving that the symmetric relation $\mathcal{B} = \{((E_{1,1} \parallel_L E_{2,1}) \setminus \mathcal{A}_{\mathcal{H}}, (E_{1,2} \parallel_L E_{2,2}) \,/\, \mathcal{A}_{\mathcal{H}}), ((E_{1,2} \parallel_L E_{2,2}) \,/\, \mathcal{A}_{\mathcal{H}}, (E_{1,1} \parallel_L E_{2,1}) \setminus \mathcal{A}_{\mathcal{H}}) \mid E_{1,1} \parallel_L E_{2,1}, E_{1,2} \parallel_L E_{2,2} \in \mathit{reach}(E_1 \parallel_L E_2) \wedge E_{1,1} \setminus \mathcal{A}_{\mathcal{H}} \approx_{\rm p} E_{1,2} \,/\, \mathcal{A}_{\mathcal{H}} \wedge E_{2,1} \setminus \mathcal{A}_{\mathcal{H}} \approx_{\rm p} E_{2,2} \,/\, \mathcal{A}_{\mathcal{H}}\}$ is a weak probabilistic bisimulation, as can be seen by taking $E_{1,1}$ identical to $E_{1,2}$ as well as $E_{2,1}$ identical to $E_{2,2}$. Assuming that $(E_{1,1} \parallel_L E_{2,1}) \setminus \mathcal{A}_{\mathcal{H}}$ and $(E_{1,2} \parallel_L E_{2,2}) \,/\, \mathcal{A}_{\mathcal{H}}$ are related by $\mathcal{B}$, there are thirteen cases (in the first five it is the former process to move first, while in the last eight it is the latter):
   - If $(E_{1,1} \parallel_L E_{2,1}) \setminus \mathcal{A}_{\mathcal{H}} \xrightarrow{l}_{\rm a} (E_{1,1}' \parallel_L [1]E_{2,1}) \setminus \mathcal{A}_{\mathcal{H}}$ with $E_{1,1} \xrightarrow{l}_{\rm a} E_{1,1}'$ and $l \notin L$, then $E_{1,1} \setminus \mathcal{A}_{\mathcal{H}} \xrightarrow{l}_{\rm a} E_{1,1}' \setminus \mathcal{A}_{\mathcal{H}}$ as $l \notin \mathcal{A}_{\mathcal{H}}$. From $E_{1,1} \setminus \mathcal{A}_{\mathcal{H}} \approx_{\rm p} E_{1,2} \,/\, \mathcal{A}_{\mathcal{H}}$ it follows that there exists a process $E_{1,2}'$ such that $E_{1,2} \,/\, \mathcal{A}_{\mathcal{H}} \Longrightarrow \xrightarrow{l}_{\rm a} \Longrightarrow E_{1,2}' \,/\, \mathcal{A}_{\mathcal{H}}$ with $E_{1,1}' \setminus \mathcal{A}_{\mathcal{H}} \approx_{\rm p} E_{1,2}' \,/\, \mathcal{A}_{\mathcal{H}}$. Since synchronization does not apply to τ nor to l, it follows that $(E_{1,2} \parallel_L E_{2,2}) \,/\, \mathcal{A}_{\mathcal{H}} \Longrightarrow \xrightarrow{l}_{\rm a} \Longrightarrow (E_{1,2}' \parallel_L [1]E_{2,2}) \,/\, \mathcal{A}_{\mathcal{H}}$ with $((E_{1,1}' \parallel_L [1]E_{2,1}) \setminus \mathcal{A}_{\mathcal{H}}, (E_{1,2}' \parallel_L [1]E_{2,2}) \,/\, \mathcal{A}_{\mathcal{H}}) \in \mathcal{B}$.
   - If $(E_{1,1} \parallel_L E_{2,1}) \setminus \mathcal{A}_{\mathcal{H}} \xrightarrow{l}_{\rm a} ([1]E_{1,1} \parallel_L E_{2,1}') \setminus \mathcal{A}_{\mathcal{H}}$ with $E_{2,1} \xrightarrow{l}_{\rm a} E_{2,1}'$ and $l \notin L$, then the proof is similar to the one of the previous case.
   - If $(E_{1,1} \parallel_L E_{2,1}) \setminus \mathcal{A}_{\mathcal{H}} \xrightarrow{l}_{\rm a} (E_{1,1}' \parallel_L E_{2,1}') \setminus \mathcal{A}_{\mathcal{H}}$ with $E_{i,1} \xrightarrow{l}_{\rm a} E_{i,1}'$ for $i \in \{1,2\}$ and $l \in L$, then $E_{i,1} \setminus \mathcal{A}_{\mathcal{H}} \xrightarrow{l}_{\rm a} E_{i,1}' \setminus \mathcal{A}_{\mathcal{H}}$ as $l \notin \mathcal{A}_{\mathcal{H}}$. From

$E_{i,1} \setminus \mathcal{A}_{\mathcal{H}} \approx_{\mathrm{p}} E_{i,2} / \mathcal{A}_{\mathcal{H}}$ it follows that there exists a process $E'_{i,2}$ such that $E_{i,2} / \mathcal{A}_{\mathcal{H}} \Longrightarrow \xrightarrow{l}_{\mathrm{a}} \Longrightarrow E'_{i,2} / \mathcal{A}_{\mathcal{H}}$ with $E'_{i,1} \setminus \mathcal{A}_{\mathcal{H}} \approx_{\mathrm{p}} E'_{i,2} / \mathcal{A}_{\mathcal{H}}$. Since synchronization does not apply to τ, it follows that $(E_{1,2} \parallel_L E_{2,2}) / \mathcal{A}_{\mathcal{H}} \Longrightarrow \xrightarrow{l}_{\mathrm{a}} \Longrightarrow (E'_{1,2} \parallel_L E'_{2,2}) / \mathcal{A}_{\mathcal{H}}$ with $((E'_{1,1} \parallel_L E'_{2,1}) \setminus \mathcal{A}_{\mathcal{H}}, (E'_{1,2} \parallel_L E'_{2,2}) / \mathcal{A}_{\mathcal{H}}) \in \mathcal{B}$.

- If $(E_{1,1} \parallel_L E_{2,1}) \setminus \mathcal{A}_{\mathcal{H}} \xrightarrow{\tau}_{\mathrm{a}} (E'_{1,1} \parallel_L [1]E_{2,1}) \setminus \mathcal{A}_{\mathcal{H}}$ with $E_{1,1} \xrightarrow{\tau}_{\mathrm{a}} E'_{1,1}$, then $E_{1,1} \setminus \mathcal{A}_{\mathcal{H}} \xrightarrow{\tau}_{\mathrm{a}} E'_{1,1} \setminus \mathcal{A}_{\mathcal{H}}$ as $\tau \notin \mathcal{A}_{\mathcal{H}}$. From $E_{1,1} \setminus \mathcal{A}_{\mathcal{H}} \approx_{\mathrm{p}} E_{1,2} / \mathcal{A}_{\mathcal{H}}$ it follows that there exists a process $E'_{1,2}$ such that $E_{1,2} / \mathcal{A}_{\mathcal{H}} \Longrightarrow E'_{1,2} / \mathcal{A}_{\mathcal{H}}$ with $E'_{1,1} \setminus \mathcal{A}_{\mathcal{H}} \approx_{\mathrm{p}} E'_{1,2} / \mathcal{A}_{\mathcal{H}}$. Since synchronization does not apply to τ, it follows that $(E_{1,2} \parallel_L E_{2,2}) / \mathcal{A}_{\mathcal{H}} \Longrightarrow (E'_{1,2} \parallel_L [1]E_{2,2}) / \mathcal{A}_{\mathcal{H}}$ with $((E'_{1,1} \parallel_L [1]E_{2,1}) \setminus \mathcal{A}_{\mathcal{H}}, (E'_{1,2} \parallel_L [1]E_{2,2}) / \mathcal{A}_{\mathcal{H}}) \in \mathcal{B}$.
- If $(E_{1,1} \parallel_L E_{2,1}) \setminus \mathcal{A}_{\mathcal{H}} \xrightarrow{\tau}_{\mathrm{a}} ([1]E_{1,1} \parallel_L E'_{2,1}) \setminus \mathcal{A}_{\mathcal{H}}$ with $E_{2,1} \xrightarrow{\tau}_{\mathrm{a}} E'_{2,1}$, then the proof is similar to the one of the previous case.
- If $(E_{1,2} \parallel_L E_{2,2}) / \mathcal{A}_{\mathcal{H}} \xrightarrow{l}_{\mathrm{a}} (E'_{1,2} \parallel_L [1]E_{2,2}) / \mathcal{A}_{\mathcal{H}}$ with $E_{1,2} \xrightarrow{l}_{\mathrm{a}} E'_{1,2}$ and $l \notin L$, then $E_{1,2} / \mathcal{A}_{\mathcal{H}} \xrightarrow{l}_{\mathrm{a}} E'_{1,2} / \mathcal{A}_{\mathcal{H}}$ as $l \notin \mathcal{A}_{\mathcal{H}}$. From $E_{1,2} / \mathcal{A}_{\mathcal{H}} \approx_{\mathrm{p}} E_{1,1} \setminus \mathcal{A}_{\mathcal{H}}$ it follows that there exists a process $E'_{1,1}$ such that $E_{1,1} \setminus \mathcal{A}_{\mathcal{H}} \Longrightarrow \xrightarrow{l}_{\mathrm{a}} \Longrightarrow E'_{1,1} \setminus \mathcal{A}_{\mathcal{H}}$ with $E_{1,2} / \mathcal{A}_{\mathcal{H}} \approx_{\mathrm{p}} \bar{E}_{1,1} \setminus \mathcal{A}_{\mathcal{H}}$ and $E'_{1,2} / \mathcal{A}_{\mathcal{H}} \approx_{\mathrm{p}} E'_{1,1} \setminus \mathcal{A}_{\mathcal{H}}$. Since synchronization does not apply to τ nor to l, it follows that $(E_{1,1} \parallel_L E_{2,1}) \setminus \mathcal{A}_{\mathcal{H}} \Longrightarrow \xrightarrow{l}_{\mathrm{a}} \Longrightarrow (E'_{1,1} \parallel_L [1]E_{2,1}) \setminus \mathcal{A}_{\mathcal{H}}$ with $((E'_{1,2} \parallel_L [1]E_{2,2}) / \mathcal{A}_{\mathcal{H}}, (E'_{1,1} \parallel_L [1]E_{2,1}) \setminus \mathcal{A}_{\mathcal{H}}) \in \mathcal{B}$.
- If $(E_{1,2} \parallel_L E_{2,2}) / \mathcal{A}_{\mathcal{H}} \xrightarrow{l}_{\mathrm{a}} ([1]E_{1,2} \parallel_L E'_{2,2}) / \mathcal{A}_{\mathcal{H}}$ with $E_{2,2} \xrightarrow{l}_{\mathrm{a}} E'_{2,2}$ and $l \notin L$, then the proof is similar to the one of the previous case.
- If $(E_{1,2} \parallel_L E_{2,2}) / \mathcal{A}_{\mathcal{H}} \xrightarrow{l}_{\mathrm{a}} (E'_{1,2} \parallel_L E'_{2,2}) / \mathcal{A}_{\mathcal{H}}$ with $E_{i,2} \xrightarrow{l}_{\mathrm{a}} E'_{i,2}$ for $i \in \{1, 2\}$ and $l \in L$, then $E_{i,2} / \mathcal{A}_{\mathcal{H}} \xrightarrow{l}_{\mathrm{a}} E'_{i,2} / \mathcal{A}_{\mathcal{H}}$ as $l \notin \mathcal{A}_{\mathcal{H}}$. From $E_{i,2} / \mathcal{A}_{\mathcal{H}} \approx_{\mathrm{p}} E_{i,1} \setminus \mathcal{A}_{\mathcal{H}}$ it follows that there exists a process $E'_{i,1}$ such that $E_{i,1} \setminus \mathcal{A}_{\mathcal{H}} \Longrightarrow \xrightarrow{l}_{\mathrm{a}} \Longrightarrow E'_{i,1} \setminus \mathcal{A}_{\mathcal{H}}$ with $E'_{i,2} / \mathcal{A}_{\mathcal{H}} \approx_{\mathrm{p}} E'_{1,1} \setminus \mathcal{A}_{\mathcal{H}}$. Since synchronization does not apply to τ, it follows that $(E_{1,1} \parallel_L E_{2,1}) \setminus \mathcal{A}_{\mathcal{H}} \Longrightarrow \xrightarrow{l}_{\mathrm{a}} \Longrightarrow (E'_{1,1} \parallel_L E'_{2,1}) \setminus \mathcal{A}_{\mathcal{H}}$ with $((E'_{1,2} \parallel_L E'_{2,2}) / \mathcal{A}_{\mathcal{H}}, (E'_{1,1} \parallel_L E'_{2,1}) \setminus \mathcal{A}_{\mathcal{H}}) \in \mathcal{B}$.
- If $(E_{1,2} \parallel_L E_{2,2}) / \mathcal{A}_{\mathcal{H}} \xrightarrow{\tau}_{\mathrm{a}} (E'_{1,2} \parallel_L [1]E_{2,2}) / \mathcal{A}_{\mathcal{H}}$ with $E_{1,2} \xrightarrow{\tau}_{\mathrm{a}} E'_{1,2}$, then $E_{1,2} / \mathcal{A}_{\mathcal{H}} \xrightarrow{\tau}_{\mathrm{a}} E'_{1,2} / \mathcal{A}_{\mathcal{H}}$ as $\tau \notin \mathcal{A}_{\mathcal{H}}$. From $E_{1,2} / \mathcal{A}_{\mathcal{H}} \approx_{\mathrm{p}} E_{1,1} \setminus \mathcal{A}_{\mathcal{H}}$ it follows that there exists a process $E'_{1,1}$ such that $E_{1,1} \setminus \mathcal{A}_{\mathcal{H}} \Longrightarrow E'_{1,1} \setminus \mathcal{A}_{\mathcal{H}}$ with $E'_{1,2} / \mathcal{A}_{\mathcal{H}} \approx_{\mathrm{p}} E'_{1,1} \setminus \mathcal{A}_{\mathcal{H}}$. Since synchronization does not apply to τ, it follows that $(E_{1,1} \parallel_L E_{2,1}) \setminus \mathcal{A}_{\mathcal{H}} \Longrightarrow (E'_{1,1} \parallel_L [1]E_{2,1}) \setminus \mathcal{A}_{\mathcal{H}}$ with $((E'_{1,2} \parallel_L [1]E_{2,2}) / \mathcal{A}_{\mathcal{H}}, (E'_{1,1} \parallel_L [1]E_{2,1}) \setminus \mathcal{A}_{\mathcal{H}}) \in \mathcal{B}$.
- If $(E_{1,2} \parallel_L E_{2,2}) / \mathcal{A}_{\mathcal{H}} \xrightarrow{\tau}_{\mathrm{a}} (E_{1,2} \parallel_L E'_{2,2}) / \mathcal{A}_{\mathcal{H}}$ with $E_{2,2} \xrightarrow{\tau}_{\mathrm{a}} E'_{2,2}$, then the proof is similar to the one of the previous case.
- If $(E_{1,2} \parallel_L E_{2,2}) / \mathcal{A}_{\mathcal{H}} \xrightarrow{\tau}_{\mathrm{a}} (E'_{1,2} \parallel_L [1]E_{2,2}) / \mathcal{A}_{\mathcal{H}}$ with $E_{1,2} \xrightarrow{h}_{\mathrm{a}} E'_{1,2}$ and $h \notin L$, then $E_{1,2} / \mathcal{A}_{\mathcal{H}} \xrightarrow{\tau}_{\mathrm{a}} E'_{1,2} / \mathcal{A}_{\mathcal{H}}$ as $h \in \mathcal{A}_{\mathcal{H}}$. From $E_{1,2} / \mathcal{A}_{\mathcal{H}} \approx_{\mathrm{p}} E_{1,1} \setminus \mathcal{A}_{\mathcal{H}}$ it follows that there exists a process $E'_{1,1}$ such that $E_{1,1} \setminus \mathcal{A}_{\mathcal{H}} \Longrightarrow E'_{1,1} \setminus \mathcal{A}_{\mathcal{H}}$ with $E'_{1,2} / \mathcal{A}_{\mathcal{H}} \approx_{\mathrm{p}} E'_{1,1} \setminus \mathcal{A}_{\mathcal{H}}$. Since synchronization

does not apply to τ, it follows that $(E_{1,1} \parallel_L E_{2,1}) \setminus \mathcal{A}_\mathcal{H} \Longrightarrow (E'_{1,1} \parallel_L [1]E_{2,1}) \setminus \mathcal{A}_\mathcal{H}$ with $((E'_{1,2} \parallel_L [1]E_{2,2}) / \mathcal{A}_\mathcal{H}, (E'_{1,1} \parallel_L [1]E_{2,1}) \setminus \mathcal{A}_\mathcal{H}) \in \mathcal{B}$.

- If $(E_{1,2} \parallel_L E_{2,2}) / \mathcal{A}_\mathcal{H} \stackrel{\tau}{\longrightarrow}_\mathrm{a} ([1]E_{1,2} \parallel_L E'_{2,2}) / \mathcal{A}_\mathcal{H}$ with $E_{2,2} \stackrel{h}{\longrightarrow}_\mathrm{a} E'_{2,2}$ and $h \notin L$, then the proof is similar to the one of the previous case.
- If $(E_{1,2} \parallel_L E_{2,2}) / \mathcal{A}_\mathcal{H} \stackrel{\tau}{\longrightarrow}_\mathrm{a} (E'_{1,2} \parallel_L E'_{2,2}) / \mathcal{A}_\mathcal{H}$ with $E_{i,2} \stackrel{h}{\longrightarrow}_\mathrm{a} E'_{i,2}$ for $i \in \{1,2\}$ and $h \in L$, then $E_{i,2} / \mathcal{A}_\mathcal{H} \stackrel{\tau}{\longrightarrow}_\mathrm{a} E'_{i,2} / \mathcal{A}_\mathcal{H}$. From $E_{i,2} / \mathcal{A}_\mathcal{H} \approx_\mathrm{p} E_{i,1} \setminus \mathcal{A}_\mathcal{H}$ it follows that there exist $E'_{i,1}$ such that $E_{i,1} \setminus \mathcal{A}_\mathcal{H} \Longrightarrow E'_{i,1} \setminus \mathcal{A}_\mathcal{H}$ with $E'_{i,2} / \mathcal{A}_\mathcal{H} \approx_\mathrm{p} E'_{i,1} \setminus \mathcal{A}_\mathcal{H}$. Since synchronization does not apply to τ, it follows that $(E_{1,1} \parallel_L E_{2,1}) \setminus \mathcal{A}_\mathcal{H} \Longrightarrow (E'_{1,1} \parallel_L E'_{2,1}) \setminus \mathcal{A}_\mathcal{H}$ with $((E'_{1,2} \parallel_L E'_{2,2}) / \mathcal{A}_\mathcal{H}, (E'_{1,1} \parallel_L E'_{2,1}) \setminus \mathcal{A}_\mathcal{H}) \in \mathcal{B}$.

As far as probability are concerned, given two arbitrary processes $F_1, F_2 \in \mathbb{P}_\mathrm{p}$ we observe that $prob((E_{1,1} \setminus \mathcal{A}_\mathcal{H}) \parallel_L (E_{2,1} \setminus \mathcal{A}_\mathcal{H}), [F_1 \parallel_L F_2]_\mathcal{B}) = prob(E_{1,1} \setminus \mathcal{A}_\mathcal{H}, [F_1]_\mathcal{B}) \cdot prob(E_{1,2} \setminus \mathcal{A}_\mathcal{H}, [F_2]_\mathcal{B})$ and $prob((E_{1,2} / \mathcal{A}_\mathcal{H}) \parallel_L (E_{2,2} / \mathcal{A}_\mathcal{H}), [F_1 \parallel_L F_2]_\mathcal{B}) = prob(E_{1,2} / \mathcal{A}_\mathcal{H}, [F_1]_\mathcal{B}) \cdot prob(E_{2,2} / \mathcal{A}_\mathcal{H}, [F_2]_\mathcal{B})$ (see the proof of Lemma 1). Now, from the fact that $E_{i,1} \setminus \mathcal{A}_\mathcal{H} \approx_\mathrm{p} E_{i,2} / \mathcal{A}_\mathcal{H}$, for $i \in \{1,2\}$, it follows that for all equivalence classes $C \in \mathbb{P}/\mathcal{B}$, $prob(E_{i,1} \setminus \mathcal{A}_\mathcal{H}, C) = prob(E_{i,2} / \mathcal{A}_\mathcal{H}, C)$, which in turn implies that $prob((E_{1,1} \setminus \mathcal{A}_\mathcal{H}) \parallel_L (E_{2,1} \setminus \mathcal{A}_\mathcal{H}), [F_1 \parallel_L F_2]_\mathcal{B}) = prob((E_{1,2} / \mathcal{A}_\mathcal{H}) \parallel_L (E_{2,2} / \mathcal{A}_\mathcal{H}), [F_1 \parallel_L F_2]_\mathcal{B})$. Finally from the fact that the hiding and restriction operators do not apply to probabilistic transitions we conclude that $prob((E_{1,1} \parallel_L E_{2,1}) \setminus \mathcal{A}_\mathcal{H}, [F_1 \parallel_L F_2]_\mathcal{B}) = prob(E_{1,2} \parallel_L E_{2,2}) / \mathcal{A}_\mathcal{H}, [F_1 \parallel_L F_2]_\mathcal{B})$.

3. Given an arbitrary $E \in \mathrm{SBSNNI}_{\approx_\mathrm{p}}$ and an arbitrary $L \subseteq \mathcal{A}$, the result follows by proving that the symmetric relation $\mathcal{B} = \{((E_1 / \mathcal{A}_\mathcal{H}) \setminus L, (E_2 \setminus L) / \mathcal{A}_\mathcal{H}), ((E_2 \setminus L) / \mathcal{A}_\mathcal{H}, (E_1 / \mathcal{A}_\mathcal{H}) \setminus L) \mid E_1, E_2 \in reach(E) \wedge E_1 / \mathcal{A}_\mathcal{H} \approx_\mathrm{p} E_2 \setminus \mathcal{A}_\mathcal{H}\}$ is a weak probabilistic bisimulation, as can be seen by taking E_1 identical to E_2 – which will be denoted by E' – because:
   - $(E' \setminus L) \setminus \mathcal{A}_\mathcal{H} \approx_\mathrm{p} (E' \setminus \mathcal{A}_\mathcal{H}) \setminus L$ as the order in which restriction sets are considered is unimportant.
   - $(E' \setminus \mathcal{A}_\mathcal{H}) \setminus L \approx_\mathrm{p} (E' / \mathcal{A}_\mathcal{H}) \setminus L$ due to $E' \setminus \mathcal{A}_\mathcal{H} \approx_\mathrm{p} E' / \mathcal{A}_\mathcal{H}$ – as $E \in \mathrm{SBSNNI}_{\approx_\mathrm{p}}$ and $E' \in reach(E)$ – and $\approx_\mathrm{p}$ being a congruence with respect to the restriction operator (see the proof of Lemma 1).
   - $(E' / \mathcal{A}_\mathcal{H}) \setminus L \approx_\mathrm{p} (E' \setminus L) / \mathcal{A}_\mathcal{H}$ as $((E' / \mathcal{A}_\mathcal{H}) \setminus L, (E' \setminus L) / \mathcal{A}_\mathcal{H}) \in \mathcal{B}$.
   - From the transitivity of $\approx_\mathrm{p}$ it follows that $(E' \setminus L) \setminus \mathcal{A}_\mathcal{H} \approx_\mathrm{p} (E' \setminus L) / \mathcal{A}_\mathcal{H}$.

   Assuming that $(E_1 / \mathcal{A}_\mathcal{H}) \setminus L$ and $(E_2 \setminus L) / \mathcal{A}_\mathcal{H}$ are related by $\mathcal{B}$, there are six cases:
   - If $(E_1 / \mathcal{A}_\mathcal{H}) \setminus L \stackrel{l}{\longrightarrow}_\mathrm{a} (E'_1 / \mathcal{A}_\mathcal{H}) \setminus L$ with $E_1 \stackrel{l}{\longrightarrow}_\mathrm{a} E'_1$ and $l \notin L$, then $E_1 / \mathcal{A}_\mathcal{H} \stackrel{l}{\longrightarrow}_\mathrm{a} E'_1 / \mathcal{A}_\mathcal{H}$ as $l \notin \mathcal{A}_\mathcal{H}$. From $E_1 / \mathcal{A}_\mathcal{H} \approx_\mathrm{p} E_2 \setminus \mathcal{A}_\mathcal{H}$ it follows that there exists a process E'_2 such that $E_2 \setminus \mathcal{A}_\mathcal{H} \Longrightarrow \stackrel{l}{\longrightarrow}_\mathrm{a} \Longrightarrow E'_2 \setminus \mathcal{A}_\mathcal{H}$ with $E'_1 / \mathcal{A}_\mathcal{H} \approx_\mathrm{p} E'_2 \setminus \mathcal{A}_\mathcal{H}$. Since neither the restriction operator nor the hiding operator applies to τ, l, and probabilistic transitions, it follows that $(E_2 \setminus L) / \mathcal{A}_\mathcal{H} \Longrightarrow \stackrel{l}{\longrightarrow}_\mathrm{a} \Longrightarrow (E'_2 \setminus L) / \mathcal{A}_\mathcal{H}$ with $((E'_1 / \mathcal{A}_\mathcal{H}) \setminus L, (E'_2 \setminus L) / \mathcal{A}_\mathcal{H}) \in \mathcal{B}$.
   - If $(E_1 / \mathcal{A}_\mathcal{H}) \setminus L \stackrel{\tau}{\longrightarrow}_\mathrm{a} (E'_1 / \mathcal{A}_\mathcal{H}) \setminus L$ with $E_1 \stackrel{\tau}{\longrightarrow}_\mathrm{a} E'_1$, then $E_1 / \mathcal{A}_\mathcal{H} \stackrel{\tau}{\longrightarrow}_\mathrm{a} E'_1 / \mathcal{A}_\mathcal{H}$ as $\tau \notin \mathcal{A}_\mathcal{H}$. From $E_1 / \mathcal{A}_\mathcal{H} \approx_\mathrm{p} E_2 \setminus \mathcal{A}_\mathcal{H}$ it follows that there

exists a process E_2' such that $E_2 \setminus \mathcal{A}_\mathcal{H} \Longrightarrow E_2' \setminus \mathcal{A}_\mathcal{H}$ with $E_1' / \mathcal{A}_\mathcal{H} \approx_\mathrm{p} E_2' \setminus \mathcal{A}_\mathcal{H}$. Since neither the restriction operator nor the hiding operator applies to τ and probabilistic transitions, it follows that $(E_2 \setminus L) / \mathcal{A}_\mathcal{H} \Longrightarrow (E_2' \setminus L) / \mathcal{A}_\mathcal{H}$ with and $((E_1' / \mathcal{A}_\mathcal{H}) \setminus L, (E_2' \setminus L) / \mathcal{A}_\mathcal{H}) \in \mathcal{B}$.
- If $(E_1 / \mathcal{A}_\mathcal{H}) \setminus L \xrightarrow{\tau}_\mathrm{a} (E_1' / \mathcal{A}_\mathcal{H}) \setminus L$ with $E_1 \xrightarrow{h}_\mathrm{a} E_1'$ and $h \in \mathcal{A}_\mathcal{H}$, then $E_1 / \mathcal{A}_\mathcal{H} \xrightarrow{\tau}_\mathrm{a} E_1' / \mathcal{A}_\mathcal{H}$ as $h \in \mathcal{A}_\mathcal{H}$ and the rest the proof is similar to the one of the previous case.
- If $(E_2 \setminus L) / \mathcal{A}_\mathcal{H} \xrightarrow{l}_\mathrm{a} (E_2' \setminus L) / \mathcal{A}_\mathcal{H}$ with $E_2 \xrightarrow{l}_\mathrm{a} E_2'$ and $l \notin L$, then $E_2 \setminus \mathcal{A}_\mathcal{H} \xrightarrow{l}_\mathrm{a} E_2' \setminus \mathcal{A}_\mathcal{H}$ as $l \notin \mathcal{A}_\mathcal{H}$. From $E_2 \setminus \mathcal{A}_\mathcal{H} \approx_\mathrm{p} E_1 / \mathcal{A}_\mathcal{H}$ it follows that there exists a process E_1' such that $E_1 / \mathcal{A}_\mathcal{H} \Longrightarrow \xrightarrow{l}_\mathrm{a} \Longrightarrow E_1' / \mathcal{A}_\mathcal{H}$ with $E_2' \setminus \mathcal{A}_\mathcal{H} \approx_\mathrm{p} E_1' / \mathcal{A}_\mathcal{H}$. Since the restriction operator does not apply to τ, l, and probabilistic transitions it follows that $(E_1 / \mathcal{A}_\mathcal{H}) \setminus L \Longrightarrow \xrightarrow{l}_\mathrm{a} \Longrightarrow (E_1' / \mathcal{A}_\mathcal{H}) \setminus L$ with $((E_2' \setminus L) / \mathcal{A}_\mathcal{H}, (E_1' / \mathcal{A}_\mathcal{H}) \setminus L) \in \mathcal{B}$.
- If $(E_2 \setminus L) / \mathcal{A}_\mathcal{H} \xrightarrow{\tau}_\mathrm{a} (E_2' \setminus L) / \mathcal{A}_\mathcal{H}$ with $E_2 \xrightarrow{\tau}_\mathrm{a} E_2'$, then $E_2 \setminus \mathcal{A}_\mathcal{H} \xrightarrow{\tau}_\mathrm{a} E_2' \setminus \mathcal{A}_\mathcal{H}$ as $\tau \notin \mathcal{A}_\mathcal{H}$. From $E_2 \setminus \mathcal{A}_\mathcal{H} \approx_\mathrm{p} E_1 / \mathcal{A}_\mathcal{H}$ it follows that there exists a process E_1' such that $E_1 / \mathcal{A}_\mathcal{H} \Longrightarrow E_1' / \mathcal{A}_\mathcal{H}$ with $E_2' \setminus \mathcal{A}_\mathcal{H} \approx_\mathrm{p} E_1' / \mathcal{A}_\mathcal{H}$. Since the restriction operator does not apply to τ nor to probabilistic transitions, it follows that $(E_1 / \mathcal{A}_\mathcal{H}) \setminus L \Longrightarrow (E_1' / \mathcal{A}_\mathcal{H}) \setminus L$ with and $((E_2' \setminus L) / \mathcal{A}_\mathcal{H}, (E_1' / \mathcal{A}_\mathcal{H}) \setminus L) \in \mathcal{B}$.
- If $(E_2 \setminus L) / \mathcal{A}_\mathcal{H} \xrightarrow{\tau}_\mathrm{a} (E_2' \setminus L) / \mathcal{A}_\mathcal{H}$ with $E_2 \xrightarrow{h}_\mathrm{a} E_2'$ and $h \notin L$, then $E_2 / \mathcal{A}_\mathcal{H} \xrightarrow{\tau}_\mathrm{a} E_2' / \mathcal{A}_\mathcal{H}$ as $h \in \mathcal{A}_\mathcal{H}$ (note that $E_2 \setminus \mathcal{A}_\mathcal{H}$ cannot perform h). From $E_2 / \mathcal{A}_\mathcal{H} \approx_\mathrm{p} E_2 \setminus \mathcal{A}_\mathcal{H}$ – as $E \in \mathrm{SBSNNI}_{\approx_\mathrm{p}}$ and $E_2 \in \mathit{reach}(E)$ – and $E_2 \setminus \mathcal{A}_\mathcal{H} \approx_\mathrm{p} E_1 / \mathcal{A}_\mathcal{H}$ it follows that there exists a process E_1' such that $E_1 / \mathcal{A}_\mathcal{H} \Longrightarrow E_1' / \mathcal{A}_\mathcal{H}$ with $E_2' / \mathcal{A}_\mathcal{H} \approx_\mathrm{b} E_1' / \mathcal{A}_\mathcal{H}$ and hence $E_2' \setminus \mathcal{A}_\mathcal{H} \approx_\mathrm{p} E_1' / \mathcal{A}_\mathcal{H}$. Since the restriction operator does not apply to τ, it follows that $(E_1 / \mathcal{A}_\mathcal{H}) \setminus L \Longrightarrow (E_1' / \mathcal{A}_\mathcal{H}) \setminus L$ with $((E_2' \setminus L) / \mathcal{A}_\mathcal{H}, (E_1' / \mathcal{A}_\mathcal{H}) \setminus L) \in \mathcal{B}$.

As far as probabilities are concerned, from the fact that $E_1 / \mathcal{A}_\mathcal{H} \approx_\mathrm{p} E_2 \setminus \mathcal{A}_\mathcal{H}$ it follows that for all equivalence classes $C \in \mathbb{P}/\mathcal{B}$, $\mathit{prob}(E_1 / \mathcal{A}_\mathcal{H}, C) = \mathit{prob}(E_2 \setminus \mathcal{A}_\mathcal{H}, C)$, and from the fact that the hiding operator and the restriction do not apply to probabilistic transitions, it follows that for all equivalence classes $C \in \mathcal{B}$, $\mathit{prob}((E_1 / \mathcal{A}_\mathcal{H}) \setminus L, C) = \mathit{prob}((E_2 \setminus L) / \mathcal{A}_\mathcal{H}), C)$.

4. Given an arbitrary $E \in \mathrm{SBSNNI}_{\approx_\mathrm{p}}$ and an arbitrary $L \subseteq \mathcal{A}_\mathcal{L}$, for every $E' \in \mathit{reach}(E)$ it holds that $E' \setminus \mathcal{A}_\mathcal{H} \approx_\mathrm{p} E' / \mathcal{A}_\mathcal{H}$, from which we derive that $(E' \setminus \mathcal{A}_\mathcal{H}) / L \approx_\mathrm{p} (E' / \mathcal{A}_\mathcal{H}) / L$ because $\approx_\mathrm{p}$ is a congruence with respect to the hiding operator (see the proof of Lemma 1). 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 $(E' / L) \setminus \mathcal{A}_\mathcal{H} \approx_\mathrm{p} (E' / L) / \mathcal{A}_\mathcal{H}$, i.e., E' / L is $\mathrm{BSNNI}_{\approx_\mathrm{p}}$.

We now prove the results for $\mathrm{SBNDC}_{\approx_\mathrm{p}}$:

1. Given an arbitrary $E \in \mathrm{SBNDC}_{\approx_\mathrm{p}}$ and an arbitrary $a \in \mathcal{A}_\tau \setminus \mathcal{A}_\mathcal{H}$, it trivially holds that $a \,.\, E \in \mathrm{SBNDC}_{\approx_\mathrm{p}}$.
2. Given two arbitrary $E_1, E_2 \in \mathrm{SBNDC}_{\approx_\mathrm{p}}$ and an arbitrary $L \subseteq \mathcal{A}$, the result follows by proving that the symmetric relation $\mathcal{B} = \{((F_1 \parallel_L F_2) \setminus$

$\mathcal{A}_{\mathcal{H}}, (R_1 \parallel_L R_2) \setminus \mathcal{A}_{\mathcal{H}}), ((R_1 \parallel_L R_2) \setminus \mathcal{A}_{\mathcal{H}}, (F_1 \parallel_L F_2) \setminus \mathcal{A}_{\mathcal{H}}) \mid F_1 \parallel_L F_2, R_1 \parallel_L R_2 \in \mathit{reach}(E_1 \parallel_L E_2) \wedge F_1 \setminus \mathcal{A}_{\mathcal{H}} \approx_{\mathrm{p}} R_1 \setminus \mathcal{A}_{\mathcal{H}} \wedge F_2 \setminus \mathcal{A}_{\mathcal{H}} \approx_{\mathrm{p}} R_2 \setminus \mathcal{A}_{\mathcal{H}}\}$ is a weak probabilistic bisimulation, as can be seen by observing that whenever $E'_1 \parallel_L E'_2 \xrightarrow{h}_{\mathrm{a}} E''_1 \parallel_L E''_2$ for $E'_1 \parallel_L E'_2 \in \mathit{reach}(E_1 \parallel_L E_2)$:

- If $E'_1 \xrightarrow{h}_{\mathrm{a}} E''_1$, $E''_2 = E'_2$, and $h \notin L$, then from $E_1 \in \mathrm{SBNDC}_{\approx_{\mathrm{p}}}$ it follows that $E'_1 \setminus \mathcal{A}_{\mathcal{H}} \approx_{\mathrm{p}} E''_1 \setminus \mathcal{A}_{\mathcal{H}}$ and hence $((E'_1 \parallel_L E'_2) \setminus \mathcal{A}_{\mathcal{H}}, ((E''_1 \parallel_L E''_2) \setminus \mathcal{A}_{\mathcal{H}}) \in \mathcal{B}$ as $E'_2 \setminus \mathcal{A}_{\mathcal{H}} \approx_{\mathrm{p}} E''_2 \setminus \mathcal{A}_{\mathcal{H}}$.
- If $E'_2 \xrightarrow{h}_{\mathrm{a}} E''_2$, $E''_1 = E'_1$, and $h \notin L$, then from $E_2 \in \mathrm{SBNDC}_{\approx_{\mathrm{p}}}$ it follows that $E'_2 \setminus \mathcal{A}_{\mathcal{H}} \approx_{\mathrm{p}} E''_2 \setminus \mathcal{A}_{\mathcal{H}}$ and hence $((E'_1 \parallel_L E'_2) \setminus \mathcal{A}_{\mathcal{H}}, ((E''_1 \parallel_L E''_2) \setminus \mathcal{A}_{\mathcal{H}}) \in \mathcal{B}$ as $E'_1 \setminus \mathcal{A}_{\mathcal{H}} \approx_{\mathrm{p}} E''_1 \setminus \mathcal{A}_{\mathcal{H}}$.
- If $E'_1 \xrightarrow{h}_{\mathrm{a}} E''_1$, $E'_2 \xrightarrow{h}_{\mathrm{a}} E''_2$, and $h \in L$, then from $E_1, E_2 \in \mathrm{SBNDC}_{\approx_{\mathrm{p}}}$ it follows that $E'_1 \setminus \mathcal{A}_{\mathcal{H}} \approx_{\mathrm{p}} E''_1 \setminus \mathcal{A}_{\mathcal{H}}$ and $E'_2 \setminus \mathcal{A}_{\mathcal{H}} \approx_{\mathrm{p}} E''_2 \setminus \mathcal{A}_{\mathcal{H}}$, which in turn entail that $((E'_1 \parallel_L E'_2) \setminus \mathcal{A}_{\mathcal{H}}, ((E''_1 \parallel_L E''_2) \setminus \mathcal{A}_{\mathcal{H}}) \in \mathcal{B}$.

Assuming that $((F_1 \parallel_L F_2) \setminus \mathcal{A}_{\mathcal{H}}, (R_1 \parallel_L R_2) \setminus \mathcal{A}_{\mathcal{H}}) \in \mathcal{B}$, there are five cases:

- 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 $F_1 \setminus \mathcal{A}_{\mathcal{H}} \approx_{\mathrm{p}} R_1 \setminus \mathcal{A}_{\mathcal{H}}$ it follows that there exists a process R'_1 such that $R_1 \setminus \mathcal{A}_{\mathcal{H}} \Longrightarrow \xrightarrow{l}_{\mathrm{a}} \Longrightarrow R'_1 \setminus \mathcal{A}_{\mathcal{H}}$ with $F'_1 \setminus \mathcal{A}_{\mathcal{H}} \approx_{\mathrm{p}} R'_1 \setminus \mathcal{A}_{\mathcal{H}}$. Since synchronization does not apply to τ, it follows that $(R_1 \parallel_L R_2) \setminus \mathcal{A}_{\mathcal{H}} \Longrightarrow \xrightarrow{l}_{\mathrm{a}} \Longrightarrow (R'_1 \parallel_L [1]R_2) \setminus \mathcal{A}_{\mathcal{H}}$ with and $((F'_1 \parallel_L [1]F_2) \setminus \mathcal{A}_{\mathcal{H}}, (R'_1 \parallel_L [1]R_2) \setminus \mathcal{A}_{\mathcal{H}}) \in \mathcal{B}$.
- 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 $F_i \setminus \mathcal{A}_{\mathcal{H}} \approx_{\mathrm{p}} R_i \setminus \mathcal{A}_{\mathcal{H}}$ it follows that there exists a process R'_i such that $R_i \setminus \mathcal{A}_{\mathcal{H}} \Longrightarrow \xrightarrow{l}_{\mathrm{a}} \Longrightarrow R'_i \setminus \mathcal{A}_{\mathcal{H}}$ with $F'_i \setminus \mathcal{A}_{\mathcal{H}} \approx_{\mathrm{p}} R'_i \setminus \mathcal{A}_{\mathcal{H}}$. Since synchronization does not apply to τ, it follows that $(R_1 \parallel_L R_2) \setminus \mathcal{A}_{\mathcal{H}} \Longrightarrow \xrightarrow{l}_{\mathrm{a}} \Longrightarrow (R'_1 \parallel_L R'_2) \setminus \mathcal{A}_{\mathcal{H}}$ with $((F'_1 \parallel_L F'_2) \setminus \mathcal{A}_{\mathcal{H}}, (R'_1 \parallel_L R'_2) \setminus \mathcal{A}_{\mathcal{H}}) \in \mathcal{B}$.
- 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 $F_1 \setminus \mathcal{A}_{\mathcal{H}} \xrightarrow{\tau}_{\mathrm{a}} F'_1 \setminus \mathcal{A}_{\mathcal{H}}$. From $F_1 \setminus \mathcal{A}_{\mathcal{H}} \approx_{\mathrm{p}} R_1 \setminus \mathcal{A}_{\mathcal{H}}$ it follows that there exists a process R'_1 such that $R_1 \setminus \mathcal{A}_{\mathcal{H}} \Longrightarrow R'_1 \setminus \mathcal{A}_{\mathcal{H}}$ with $F'_1 \setminus \mathcal{A}_{\mathcal{H}} \approx_{\mathrm{p}} R'_1 \setminus \mathcal{A}_{\mathcal{H}}$. Since synchronization does not apply to τ, it follows that $(R_1 \parallel_L R_2) \setminus \mathcal{A}_{\mathcal{H}} \Longrightarrow (R'_1 \parallel_L R_2) \setminus \mathcal{A}_{\mathcal{H}}$ with $((F'_1 \parallel_L [1]F_2) \setminus \mathcal{A}_{\mathcal{H}}, (R'_1 \parallel_L [1]R_2) \setminus \mathcal{A}_{\mathcal{H}}) \in \mathcal{B}$.
- 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 far as probability are concerned, given two arbitrary probabilistic processes $S_1, S_2 \in \mathbb{P}$, we observe that $\mathit{prob}((F_1 \setminus \mathcal{A}_{\mathcal{H}}) \parallel_L (F_2 \setminus \mathcal{A}_{\mathcal{H}}), [S_1 \parallel_L S_2]_{\mathcal{B}}) = \mathit{prob}(F_1 \setminus \mathcal{A}_{\mathcal{H}}, [S_1]_{\mathcal{B}}) \cdot \mathit{prob}(F_2 \setminus \mathcal{A}_{\mathcal{H}}, [S_2]_{\mathcal{B}})$ and $\mathit{prob}((R_1 \setminus \mathcal{A}_{\mathcal{H}}) \parallel_L R_2 \setminus \mathcal{A}_{\mathcal{H}}), [S_1 \parallel_L S_2]_{\mathcal{B}}) = \mathit{prob}(R_1 \,/\, \mathcal{A}_{\mathcal{H}}, [S_1]_{\mathcal{B}}) \cdot \mathit{prob}(R_2 \,/\, \mathcal{A}_{\mathcal{H}}, [S_2]_{\mathcal{B}})$ (see the proof of Lemma 1). Now, from the fact that $F_i \setminus \mathcal{A}_{\mathcal{H}} \approx_{\mathrm{p}} R_i \setminus \mathcal{A}_{\mathcal{H}}$, for $i \in \{1, 2\}$, it follows that for all equivalence classes $C \in \mathbb{P}/\mathcal{B}$, $\mathit{prob}(F_i \setminus \mathcal{A}_{\mathcal{H}}, C) = \mathit{prob}(R_i \setminus \mathcal{A}_{\mathcal{H}}, C)$, which in turn implies that $\mathit{prob}((F_1 \setminus \mathcal{A}_{\mathcal{H}}) \parallel_L (F_2 \setminus \mathcal{A}_{\mathcal{H}}), [S_1 \parallel_L S_2]_{\mathcal{B}}) =$

$prob((R_1 \setminus \mathcal{A}_\mathcal{H}) \parallel_L (R_2 \setminus \mathcal{A}_\mathcal{H}), [S_1 \parallel_L S_2]_\mathcal{B})$. Lastly, from the fact that the restriction operator does not apply to probabilistic transitions we conclude that $prob((F_1 \parallel_L F_2) \setminus \mathcal{A}_\mathcal{H}, [S_1 \parallel_L S_2]_\mathcal{B}) = prob((R_1 \parallel_L R_2) \setminus \mathcal{A}_\mathcal{H}, [S_1 \parallel_L S_2]_\mathcal{B})$.

3. Given an arbitrary $E \in \mathrm{SBNDC}_{\approx_\mathrm{p}}$ and an arbitrary $L \subseteq \mathcal{A}$, for every $E' \in reach(E)$ and for every E'' such that $E' \xrightarrow{h}_\mathrm{a} E''$ it holds that $E' \setminus \mathcal{A}_\mathcal{H} \approx_\mathrm{p} E'' \setminus \mathcal{A}_\mathcal{H}$, from which we derive that $(E' \setminus \mathcal{A}_\mathcal{H}) \setminus L \approx_\mathrm{p} (E'' \setminus \mathcal{A}_\mathcal{H}) \setminus L$ because $\approx_\mathrm{p}$ is a congruence with respect to the restriction operator (see the proof of Lemma 1). 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 $(E' \setminus L) \setminus \mathcal{A}_\mathcal{H} \approx_\mathrm{p} (E'' \setminus L) \setminus \mathcal{A}_\mathcal{H}$.
4. Given an arbitrary $E \in \mathrm{SBNDC}_{\approx_\mathrm{p}}$ and an arbitrary $L \subseteq \mathcal{A}_\mathcal{L}$, for every $E' \in reach(E)$ and for every E'' such that $E' \xrightarrow{h}_\mathrm{a} E''$ it holds that $E' \setminus \mathcal{A}_\mathcal{H} \approx_\mathrm{p} E'' \setminus \mathcal{A}_\mathcal{H}$, from which we derive that $(E' \setminus \mathcal{A}_\mathcal{H}) / L \approx_\mathrm{p} (E'' \setminus \mathcal{A}_\mathcal{H}) / L$ because $\approx_\mathrm{p}$ is a congruence with respect to the hiding operator (see the proof of Lemma 1). 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 $(E' / L) \setminus \mathcal{A}_\mathcal{H} \approx_\mathrm{p} (E'' / L) \setminus \mathcal{A}_\mathcal{H}$.

We now prove the same result for the $\approx_\mathrm{pb}$-based properties. As for the first part of the proof, we first prove the results for $\mathrm{SBSNNI}_{\approx_\mathrm{pb}}$, and hence for $\mathrm{P\_BNDC}_{\approx_\mathrm{pb}}$ too by virtue of the forthcoming Theorem 3:

1. Given an arbitrary $E \in \mathrm{SBSNNI}_{\approx_\mathrm{pb}}$ and an arbitrary $a \in \mathcal{A}_\mathcal{L} \cup \{\tau\}$, from $E \setminus \mathcal{A}_\mathcal{H} \approx_\mathrm{pb} E / \mathcal{A}_\mathcal{H}$ we derive that $a\,.\,(E \setminus \mathcal{A}_\mathcal{H}) \approx_\mathrm{pb} a\,.\,(E / \mathcal{A}_\mathcal{H})$ because $\approx_\mathrm{pb}$ is a congruence with respect to action prefix (see Lemma 1), from which it follows that $(a\,.\,E) \setminus \mathcal{A}_\mathcal{H} \approx_\mathrm{pb} (a\,.\,E) / \mathcal{A}_\mathcal{H}$, i.e., $a\,.\,E \in \mathrm{BSNNI}_{\approx_\mathrm{pb}}$, 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 $\mathrm{BSNNI}_{\approx_\mathrm{pb}}$.
2. Given two arbitrary $E_1, E_2 \in \mathrm{SBSNNI}_{\approx_\mathrm{pb}}$ and an arbitrary $L \subseteq \mathcal{A}_\mathcal{L}$, the result follows by proving that the symmetric relation $\mathcal{B} = \{((E_{1,1} \parallel_L E_{2,1}) \setminus \mathcal{A}_\mathcal{H}, (E_{1,2} \parallel_L E_{2,2}) / \mathcal{A}_\mathcal{H}), ((E_{1,2} \parallel_L E_{2,2}) / \mathcal{A}_\mathcal{H}, (E_{1,1} \parallel_L E_{2,1}) \setminus \mathcal{A}_\mathcal{H}) \mid E_{1,1} \parallel_L E_{2,1}, E_{1,2} \parallel_L E_{2,2} \in reach(E_1 \parallel_L E_2) \wedge E_{1,1} \setminus \mathcal{A}_\mathcal{H} \approx_\mathrm{pb} E_{1,2} / \mathcal{A}_\mathcal{H} \wedge E_{2,1} \setminus \mathcal{A}_\mathcal{H} \approx_\mathrm{pb} E_{2,2} / \mathcal{A}_\mathcal{H}\}$ is a probabilistic branching bisimulation, as can be seen by taking $E_{1,1}$ identical to $E_{1,2}$ as well as $E_{2,1}$ identical to $E_{2,2}$. Assuming that $(E_{1,1} \parallel_L E_{2,1}) \setminus \mathcal{A}_\mathcal{H}$ and $(E_{1,2} \parallel_L E_{2,2}) / \mathcal{A}_\mathcal{H}$ are related by $\mathcal{B}$, there are twelve cases (in the first five it is the former process to move first, while in the last seven it is the latter):
   - If $(E_{1,1} \parallel_L E_{2,1}) \setminus \mathcal{A}_\mathcal{H} \xrightarrow{l}_\mathrm{a} (E'_{1,1} \parallel_L [1]E_{2,1}) \setminus \mathcal{A}_\mathcal{H}$ with $E_{1,1} \xrightarrow{l}_\mathrm{a} E'_{1,1}$ and $l \notin L$, then $E_{1,1} \setminus \mathcal{A}_\mathcal{H} \xrightarrow{l}_\mathrm{a} E'_{1,1} \setminus \mathcal{A}_\mathcal{H}$ as $l \notin \mathcal{A}_\mathcal{H}$. From $E_{1,1} \setminus \mathcal{A}_\mathcal{H} \approx_\mathrm{pb} E_{1,2} / \mathcal{A}_\mathcal{H}$ it follows that there exist $\bar{E}_{1,2}$ and $E'_{1,2}$ such that $E_{1,2} / \mathcal{A}_\mathcal{H} \Longrightarrow \bar{E}_{1,2} / \mathcal{A}_\mathcal{H} \xrightarrow{l}_\mathrm{a} E'_{1,2} / \mathcal{A}_\mathcal{H}$ with $E_{1,1} \setminus \mathcal{A}_\mathcal{H} \approx_\mathrm{pb} \bar{E}_{1,2} / \mathcal{A}_\mathcal{H}$ and $E'_{1,1} \setminus \mathcal{A}_\mathcal{H} \approx_\mathrm{pb} E'_{1,2} / \mathcal{A}_\mathcal{H}$. Since synchronization does not apply to τ and l, it follows that $(E_{1,2} \parallel_L E_{2,2}) / \mathcal{A}_\mathcal{H} \Longrightarrow (\bar{E}_{1,2} \parallel_L E_{2,2}) / \mathcal{A}_\mathcal{H} \xrightarrow{l}_\mathrm{a} (E'_{1,2} \parallel_L [1]E_{2,2}) / \mathcal{A}_\mathcal{H}$ with $((E_{1,1} \parallel_L E_{2,1}) \setminus \mathcal{A}_\mathcal{H}, (\bar{E}_{1,2} \parallel_L E_{2,2}) / \mathcal{A}_\mathcal{H}) \in \mathcal{B}$ and $((E'_{1,1} \parallel_L E_{2,1}) \setminus \mathcal{A}_\mathcal{H}, (E'_{1,2} \parallel_L E_{2,2}) / \mathcal{A}_\mathcal{H}) \in \mathcal{B}$.

- If $(E_{1,1} \parallel_L E_{2,1}) \setminus \mathcal{A}_\mathcal{H} \xrightarrow{l}_{\rm a} ([1]E_{1,1} \parallel_L E'_{2,1}) \setminus \mathcal{A}_\mathcal{H}$ with $E_{2,1} \xrightarrow{l}_{\rm a} E'_{2,1}$ and $l \notin L$, then the proof is similar to the one of the previous case.
- If $(E_{1,1} \parallel_L E_{2,1}) \setminus \mathcal{A}_\mathcal{H} \xrightarrow{l}_{\rm a} (E'_{1,1} \parallel_L E'_{2,1}) \setminus \mathcal{A}_\mathcal{H}$ with $E_{i,1} \xrightarrow{l}_{\rm a} E'_{i,1}$ for $i \in \{1,2\}$ and $l \in L$, then $E_{i,1} \setminus \mathcal{A}_\mathcal{H} \xrightarrow{l}_{\rm a} E'_{i,1} \setminus \mathcal{A}_\mathcal{H}$ as $l \notin \mathcal{A}_\mathcal{H}$. From $E_{i,1} \setminus \mathcal{A}_\mathcal{H} \approx_{\rm pb} E_{i,2} / \mathcal{A}_\mathcal{H}$ it follows that there exist $\bar{E}_{i,2}$ and $E'_{i,2}$ such that $E_{i,2} / \mathcal{A}_\mathcal{H} \Longrightarrow \bar{E}_{i,2} / \mathcal{A}_\mathcal{H} \xrightarrow{l}_{\rm a} E'_{i,2} / \mathcal{A}_\mathcal{H}$ with $E_{i,1} \setminus \mathcal{A}_\mathcal{H} \approx_{\rm pb} \bar{E}_{i,2} / \mathcal{A}_\mathcal{H}$ and $E'_{i,1} \setminus \mathcal{A}_\mathcal{H} \approx_{\rm pb} E'_{i,2} / \mathcal{A}_\mathcal{H}$. Since synchronization does not apply to τ, it follows that $(E_{1,2} \parallel_L E_{2,2}) / \mathcal{A}_\mathcal{H} \Longrightarrow (\bar{E}_{1,2} \parallel_L \bar{E}_{2,2}) / \mathcal{A}_\mathcal{H} \xrightarrow{l}_{\rm a} (E'_{1,2} \parallel_L E'_{2,2}) / \mathcal{A}_\mathcal{H}$ with $((E_{1,1} \parallel_L E_{2,1}) \setminus \mathcal{A}_\mathcal{H}, (\bar{E}_{1,2} \parallel_L \bar{E}_{2,2}) / \mathcal{A}_\mathcal{H}) \in \mathcal{B}$ and $((E'_{1,1} \parallel_L E'_{2,1}) \setminus \mathcal{A}_\mathcal{H}, (E'_{1,2} \parallel_L E'_{2,2}) / \mathcal{A}_\mathcal{H}) \in \mathcal{B}$.
- If $(E_{1,1} \parallel_L E_{2,1}) \setminus \mathcal{A}_\mathcal{H} \xrightarrow{\tau}_{\rm a} (E'_{1,1} \parallel_L [1]E_{2,1}) \setminus \mathcal{A}_\mathcal{H}$ with $E_{1,1} \xrightarrow{\tau}_{\rm a} E'_{1,1}$, then $E_{1,1} \setminus \mathcal{A}_\mathcal{H} \xrightarrow{\tau}_{\rm a} E'_{1,1} \setminus \mathcal{A}_\mathcal{H}$ as $\tau \notin \mathcal{A}_\mathcal{H}$. From $E_{1,1} \setminus \mathcal{A}_\mathcal{H} \approx_{\rm pb} E_{1,2} / \mathcal{A}_\mathcal{H}$ it follows that either $E'_{1,1} \setminus \mathcal{A}_\mathcal{H} \approx_{\rm pb} E_{1,2} / \mathcal{A}_\mathcal{H}$, or there exist $\bar{E}_{1,2}$ and $E'_{1,2}$ such that $E_{1,2} / \mathcal{A}_\mathcal{H} \Longrightarrow \bar{E}_{1,2} / \mathcal{A}_\mathcal{H} \xrightarrow{\tau}_{\rm a} E'_{1,2} / \mathcal{A}_\mathcal{H}$ with $E_{1,1} \setminus \mathcal{A}_\mathcal{H} \approx_{\rm pb} \bar{E}_{1,2} / \mathcal{A}_\mathcal{H}$ and $E'_{1,1} \setminus \mathcal{A}_\mathcal{H} \approx_{\rm pb} E'_{1,2} / \mathcal{A}_\mathcal{H}$. In the former subcase $(E_{1,2} \parallel_L E_{2,2}) / \mathcal{A}_\mathcal{H}$ is allowed to stay idle with $((E'_{1,1} \parallel_L E_{2,1}) \setminus \mathcal{A}_\mathcal{H}, (E_{1,2} \parallel_L E_{2,2}) / \mathcal{A}_\mathcal{H}) \in \mathcal{B}$, while in the latter subcase, since synchronization does not apply to τ, it follows that $(E_{1,2} \parallel_L E_{2,2}) / \mathcal{A}_\mathcal{H} \Longrightarrow (\bar{E}_{1,2} \parallel_L E_{2,2}) / \mathcal{A}_\mathcal{H} \xrightarrow{\tau}_{\rm a} (E'_{1,2} \parallel_L E_{2,2}) / \mathcal{A}_\mathcal{H}$ with $((E_{1,1} \parallel_L E_{2,1}) \setminus \mathcal{A}_\mathcal{H}, (\bar{E}_{1,2} \parallel_L E_{2,2}) / \mathcal{A}_\mathcal{H}) \in \mathcal{B}$ and $((E'_{1,1} \parallel_L E_{2,1}) \setminus \mathcal{A}_\mathcal{H}, (E'_{1,2} \parallel_L E_{2,2}) / \mathcal{A}_\mathcal{H}) \in \mathcal{B}$.
- If $(E_{1,1} \parallel_L E_{2,1}) \setminus \mathcal{A}_\mathcal{H} \xrightarrow{\tau}_{\rm a} ([1]E_{1,1} \parallel_L E'_{2,1}) \setminus \mathcal{A}_\mathcal{H}$ with $E_{2,1} \xrightarrow{\tau}_{\rm a} E'_{2,1}$, then the proof is similar to the one of the previous case.
- If $(E_{1,2} \parallel_L E_{2,2}) / \mathcal{A}_\mathcal{H} \xrightarrow{l}_{\rm a} (E'_{1,2} \parallel_L [1]E_{2,2}) / \mathcal{A}_\mathcal{H}$ with $E_{1,2} \xrightarrow{l}_{\rm a} E'_{1,2}$ and $l \notin L$, then $E_{1,2} / \mathcal{A}_\mathcal{H} \xrightarrow{l}_{\rm a} E'_{1,2} / \mathcal{A}_\mathcal{H}$ as $l \notin \mathcal{A}_\mathcal{H}$. From $E_{1,2} / \mathcal{A}_\mathcal{H} \approx_{\rm pb} E_{1,1} \setminus \mathcal{A}_\mathcal{H}$ it follows that there exist $\bar{E}_{1,1}$ and $E'_{1,1}$ such that $E_{1,1} \setminus \mathcal{A}_\mathcal{H} \Longrightarrow \bar{E}_{1,1} \setminus \mathcal{A}_\mathcal{H} \xrightarrow{l}_{\rm a} E'_{1,1} \setminus \mathcal{A}_\mathcal{H}$ with $E_{1,2} / \mathcal{A}_\mathcal{H} \approx_{\rm pb} \bar{E}_{1,1} \setminus \mathcal{A}_\mathcal{H}$ and $E'_{1,2} / \mathcal{A}_\mathcal{H} \approx_{\rm pb} E'_{1,1} \setminus \mathcal{A}_\mathcal{H}$. Since synchronization does not apply to τ and l, it follows that $(E_{1,1} \parallel_L E_{2,1}) \setminus \mathcal{A}_\mathcal{H} \Longrightarrow (\bar{E}_{1,1} \parallel_L E_{2,1}) \setminus \mathcal{A}_\mathcal{H} \xrightarrow{l}_{\rm a} (E'_{1,1} \parallel_L [1]E_{2,1}) \setminus \mathcal{A}_\mathcal{H}$ with $((E_{1,2} \parallel_L E_{2,2}) / \mathcal{A}_\mathcal{H}, (\bar{E}_{1,1} \parallel_L E_{2,1}) \setminus \mathcal{A}_\mathcal{H}) \in \mathcal{B}$ and $((E'_{1,2} \parallel_L [1]E_{2,2}) / \mathcal{A}_\mathcal{H}, (E'_{1,1} \parallel_L [1]E_{2,1}) \setminus \mathcal{A}_\mathcal{H}) \in \mathcal{B}$.
- If $(E_{1,2} \parallel_L E_{2,2}) / \mathcal{A}_\mathcal{H} \xrightarrow{l}_{\rm a} ([1]E_{1,2} \parallel_L E'_{2,2}) / \mathcal{A}_\mathcal{H}$ with $E_{2,2} \xrightarrow{l}_{\rm a} E'_{2,2}$ and $l \notin L$, then the proof is similar to the one of the previous case.
- If $(E_{1,2} \parallel_L E_{2,2}) / \mathcal{A}_\mathcal{H} \xrightarrow{l}_{\rm a} (E'_{1,2} \parallel_L E'_{2,2}) / \mathcal{A}_\mathcal{H}$ with $E_{i,2} \xrightarrow{l}_{\rm a} E'_{i,2}$ for $i \in \{1,2\}$ and $l \in L$, then $E_{i,2} / \mathcal{A}_\mathcal{H} \xrightarrow{l}_{\rm a} E'_{i,2} / \mathcal{A}_\mathcal{H}$ as $l \notin \mathcal{A}_\mathcal{H}$.
  From $E_{i,2} / \mathcal{A}_\mathcal{H} \approx_{\rm pb} E_{i,1} \setminus \mathcal{A}_\mathcal{H}$ it follows that there exist $\bar{E}_{i,1}$ and $E'_{i,1}$ such that $E_{i,1} \setminus \mathcal{A}_\mathcal{H} \Longrightarrow \bar{E}_{i,1} \setminus \mathcal{A}_\mathcal{H} \xrightarrow{l}_{\rm a} E'_{i,1} \setminus \mathcal{A}_\mathcal{H}$ with $E_{i,2} / \mathcal{A}_\mathcal{H} \approx_{\rm pb} \bar{E}_{i,1} \setminus \mathcal{A}_\mathcal{H}$ and $E'_{i,2} / \mathcal{A}_\mathcal{H} \approx_{\rm pb} E'_{i,1} \setminus \mathcal{A}_\mathcal{H}$. Since synchronization does not apply to τ, it follows that $(E_{1,1} \parallel_L E_{2,1}) \setminus \mathcal{A}_\mathcal{H} \Longrightarrow (\bar{E}_{1,1} \parallel_L \bar{E}_{2,1}) \setminus \mathcal{A}_\mathcal{H} \xrightarrow{l}_{\rm a}$

$(E'_{1,1} \parallel_L E'_{2,1}) \backslash \mathcal{A}_\mathcal{H}$ with $((E_{1,2} \parallel_L E_{2,2}) / \mathcal{A}_\mathcal{H}, (\bar{E}_{1,1} \parallel_L \bar{E}_{2,1}) \backslash \mathcal{A}_\mathcal{H}) \in \mathcal{B}$ and $((E'_{1,2} \parallel_L E'_{2,2}) / \mathcal{A}_\mathcal{H}, (E'_{1,1} \parallel_L E'_{2,1}) \setminus \mathcal{A}_\mathcal{H}) \in \mathcal{B}$.

- If $(E_{1,2} \parallel_L E_{2,2}) / \mathcal{A}_\mathcal{H} \xrightarrow{\tau}_{\rm a} (E'_{1,2} \parallel_L [1]E_{2,2}) / \mathcal{A}_\mathcal{H}$ with $E_{1,2} \xrightarrow{\tau}_{\rm a} E'_{1,2}$, then $E_{1,2} / \mathcal{A}_\mathcal{H} \xrightarrow{\tau}_{\rm a} E'_{1,2} / \mathcal{A}_\mathcal{H}$ as $\tau \notin \mathcal{A}_\mathcal{H}$. From $E_{1,2} / \mathcal{A}_\mathcal{H} \approx_{\rm pb} E_{1,1} \setminus \mathcal{A}_\mathcal{H}$ it follows that either $E'_{1,2} / \mathcal{A}_\mathcal{H} \approx_{\rm pb} E_{1,1} \setminus \mathcal{A}_\mathcal{H}$, or there exist $\bar{E}_{1,1}$ and $E'_{1,1}$ such that $E_{1,1} \setminus \mathcal{A}_\mathcal{H} \Longrightarrow \bar{E}_{1,1} \setminus \mathcal{A}_\mathcal{H} \xrightarrow{\tau}_{\rm a} E'_{1,1} \setminus \mathcal{A}_\mathcal{H}$ with $E_{1,2} / \mathcal{A}_\mathcal{H} \approx_{\rm pb} \bar{E}_{1,1} \setminus \mathcal{A}_\mathcal{H}$ and $E'_{1,2} / \mathcal{A}_\mathcal{H} \approx_{\rm pb} E'_{1,1} \setminus \mathcal{A}_\mathcal{H}$.
  In the former subcase $(E_{1,1} \parallel_L E_{2,1}) \setminus \mathcal{A}_\mathcal{H}$ is allowed to stay idle with $((E'_{1,2} \parallel_L E_{2,2}) / \mathcal{A}_\mathcal{H}, (E_{1,1} \parallel_L E_{2,1}) \setminus \mathcal{A}_\mathcal{H}) \in \mathcal{B}$, while in the latter subcase, since synchronization does not apply to τ, it follows that $(E_{1,1} \parallel_L E_{2,1}) \setminus \mathcal{A}_\mathcal{H} \Longrightarrow (\bar{E}_{1,1} \parallel_L E_{2,1}) \setminus \mathcal{A}_\mathcal{H} \xrightarrow{\tau}_{\rm a} (E'_{1,1} \parallel_L [1]E_{2,1}) \setminus \mathcal{A}_\mathcal{H}$ with $((E_{1,2} \parallel_L E_{2,2}) / \mathcal{A}_\mathcal{H}, (\bar{E}_{1,1} \parallel_L E_{2,1}) \setminus \mathcal{A}_\mathcal{H}) \in \mathcal{B}$ and $((E'_{1,2} \parallel_L [1]E_{2,2}) / \mathcal{A}_\mathcal{H}, (E'_{1,1} \parallel_L [1]E_{2,1}) \setminus \mathcal{A}_\mathcal{H}) \in \mathcal{B}$.
- If $(E_{1,2} \parallel_L E_{2,2}) / \mathcal{A}_\mathcal{H} \xrightarrow{\tau}_{\rm a} ([1]E_{1,2} \parallel_L E'_{2,2}) / \mathcal{A}_\mathcal{H}$ with $E_{2,2} \xrightarrow{\tau}_{\rm a} E'_{2,2}$, then the proof is similar to the one of the previous case.
- If $(E_{1,2} \parallel_L E_{2,2}) / \mathcal{A}_\mathcal{H} \xrightarrow{\tau}_{\rm a} (E'_{1,2} \parallel_L E_{2,2}) / \mathcal{A}_\mathcal{H}$ with $E_{1,2} \xrightarrow{h}_{\rm a} E'_{1,2}$ and $h \notin L$, then $E_{1,2} / \mathcal{A}_\mathcal{H} \xrightarrow{\tau}_{\rm a} E'_{1,2} / \mathcal{A}_\mathcal{H}$ as $h \in \mathcal{A}_\mathcal{H}$. From $E_{1,2} / \mathcal{A}_\mathcal{H} \approx_{\rm pb} E_{1,1} \setminus \mathcal{A}_\mathcal{H}$ it follows that either $E'_{1,2} / \mathcal{A}_\mathcal{H} \approx_{\rm pb} E_{1,1} \setminus \mathcal{A}_\mathcal{H}$, or there exist $\bar{E}_{1,1}$ and $E'_{1,1}$ such that $E_{1,1} \setminus \mathcal{A}_\mathcal{H} \Longrightarrow \bar{E}_{1,1} \setminus \mathcal{A}_\mathcal{H} \xrightarrow{\tau}_{\rm a} E'_{1,1} \setminus \mathcal{A}_\mathcal{H}$ with $E_{1,2} / \mathcal{A}_\mathcal{H} \approx_{\rm pb} \bar{E}_{1,1} \setminus \mathcal{A}_\mathcal{H}$ and $E'_{1,2} / \mathcal{A}_\mathcal{H} \approx_{\rm pb} E'_{1,1} \setminus \mathcal{A}_\mathcal{H}$.
  In the former subcase $(E_{1,1} \parallel_L E_{2,1}) \setminus \mathcal{A}_\mathcal{H}$ is allowed to stay idle with $((E'_{1,2} \parallel_L E_{2,2}) / \mathcal{A}_\mathcal{H}, (E_{1,1} \parallel_L E_{2,1}) \setminus \mathcal{A}_\mathcal{H}) \in \mathcal{B}$, while in the latter subcase, since synchronization does not apply to τ, it follows that $(E_{1,1} \parallel_L E_{2,1}) \setminus \mathcal{A}_\mathcal{H} \Longrightarrow (\bar{E}_{1,1} \parallel_L E_{2,1}) \setminus \mathcal{A}_\mathcal{H} \xrightarrow{\tau}_{\rm a} (E'_{1,1} \parallel_L E_{2,1}) \setminus \mathcal{A}_\mathcal{H}$ with $((E_{1,2} \parallel_L E_{2,2}) / \mathcal{A}_\mathcal{H}, (\bar{E}_{1,1} \parallel_L E_{2,1}) \setminus \mathcal{A}_\mathcal{H}) \in \mathcal{B}$ and $((E'_{1,2} \parallel_L E_{2,2}) / \mathcal{A}_\mathcal{H}, (E'_{1,1} \parallel_L E_{2,1}) \setminus \mathcal{A}_\mathcal{H}) \in \mathcal{B}$.
- If $(E_{1,2} \parallel_L E_{2,2}) / \mathcal{A}_\mathcal{H} \xrightarrow{\tau}_{\rm a} ([1]E_{1,2} \parallel_L E'_{2,2}) / \mathcal{A}_\mathcal{H}$ with $E_{2,2} \xrightarrow{h}_{\rm a} E'_{2,2}$ and $h \notin L$, then the proof is similar to the one of the previous case.

As far as probability are concerned, given two arbitrary processes processes $F_1, F_2 \in \mathbb{P}$, we observe that $prob((E_{1,1} \setminus \mathcal{A}_\mathcal{H}) \parallel_L (E_{2,1} \setminus \mathcal{A}_\mathcal{H}), [F_1 \parallel_L F_2]_\mathcal{B}) = prob(E_{1,1} \setminus \mathcal{A}_\mathcal{H}, [F_1]_\mathcal{B}) \cdot prob(E_{1,2} \setminus \mathcal{A}_\mathcal{H}, [F_2]_\mathcal{B})$ and $prob((E_{1,2} / \mathcal{A}_\mathcal{H}) \parallel_L (E_{2,2} / \mathcal{A}_\mathcal{H}), [F_1 \parallel_L F_2]_\mathcal{B}) = prob(E_{1,2} / \mathcal{A}_\mathcal{H}, [F_1]_\mathcal{B}) \cdot prob(E_{2,2} / \mathcal{A}_\mathcal{H}, [F_2]_\mathcal{B})$ (see the proof of Lemma 1). Now, from the fact that $E_{i,1} \setminus \mathcal{A}_\mathcal{H} \approx_{\rm pb} E_{i,2} / \mathcal{A}_\mathcal{H}$, for $i \in \{1, 2\}$, it follows that for all equivalence classes $C \in \mathbb{P}/\mathcal{B}$, $prob(E_{i,1} \setminus \mathcal{A}_\mathcal{H}, C) = prob(E_{i,2} / \mathcal{A}_\mathcal{H}, C)$, which in turn implies that $prob((E_{1,1} \setminus \mathcal{A}_\mathcal{H}) \parallel_L (E_{2,1} \setminus \mathcal{A}_\mathcal{H}), [F_1 \parallel_L F_2]_\mathcal{B}) =$ $prob((E_{1,2} / \mathcal{A}_\mathcal{H}) \parallel_L (E_{2,2} / \mathcal{A}_\mathcal{H}), [F_1 \parallel_L F_2]_\mathcal{B})$. Finally from the fact that the hiding and restriction operators do not apply to probabilistic transitions we conclude that $prob((E_{1,1} \parallel_L E_{2,1}) \setminus \mathcal{A}_\mathcal{H}, [F_1 \parallel_L F_2]_\mathcal{B}) =$ $prob((E_{1,2} \parallel_L E_{2,2}) / \mathcal{A}_\mathcal{H}, [F_1 \parallel_L F_2]_\mathcal{B})$.

3. Given an arbitrary $E \in {\rm SBSNNI}_{\approx_{\rm pb}}$ and an arbitrary $L \subseteq \mathcal{A}$, the result follows by proving that the symmetric relation $\mathcal{B} = \{((E_1 / \mathcal{A}_\mathcal{H}) \setminus L, (E_2 \setminus L) / \mathcal{A}_\mathcal{H}), ((E_2 \setminus L) / \mathcal{A}_\mathcal{H}, (E_1 / \mathcal{A}_\mathcal{H}) \setminus L) \mid E_1, E_2 \in reach(E) \wedge E_1 / \mathcal{A}_\mathcal{H} \approx_{\rm pb}$

$E_2 \setminus \mathcal{A}_\mathcal{H}\}$ is a probabilistic branching bisimulation, as can be seen by taking E_1 identical to E_2 – which will be denoted by E' – because:

- $(E' \setminus L) \setminus \mathcal{A}_\mathcal{H} \approx_{\rm pb} (E' \setminus \mathcal{A}_\mathcal{H}) \setminus L$ as the order in which restriction sets are considered is unimportant.
- $(E' \setminus \mathcal{A}_\mathcal{H}) \setminus L \approx_{\rm pb} (E' / \mathcal{A}_\mathcal{H}) \setminus L$ due to $E' \setminus \mathcal{A}_\mathcal{H} \approx_{\rm pb} E' / \mathcal{A}_\mathcal{H}$ – as $E \in {\rm SBSNNI}_{\approx_{\rm pb}}$ and $E' \in \mathit{reach}(E)$ – and $\approx_{\rm pb}$ being a congruence with respect to the restriction operator (see the proof of Lemma 1).
- $(E' / \mathcal{A}_\mathcal{H}) \setminus L \approx_{\rm pb} (E' \setminus L) / \mathcal{A}_\mathcal{H}$ as $((E' / \mathcal{A}_\mathcal{H}) \setminus L, (E' \setminus L) / \mathcal{A}_\mathcal{H}) \in \mathcal{B}$.
- From the transitivity of $\approx_{\rm pb}$ it follows that $(E' \setminus L) \setminus \mathcal{A}_\mathcal{H} \approx_{\rm pb} (E' \setminus L) / \mathcal{A}_\mathcal{H}$.

Assuming that $(E_1 / \mathcal{A}_\mathcal{H}) \setminus L$ and $(E_2 \setminus L) / \mathcal{A}_\mathcal{H}$ are related by $\mathcal{B}$, there are six cases:

- If $(E_1 / \mathcal{A}_\mathcal{H}) \setminus L \stackrel{l}{\longrightarrow}_{\rm a} (E_1' / \mathcal{A}_\mathcal{H}) \setminus L$ with $E_1 \stackrel{l}{\longrightarrow}_{\rm a} E_1'$ and $l \notin L$, then $E_1 / \mathcal{A}_\mathcal{H} \stackrel{l}{\longrightarrow}_{\rm a} E_1' / \mathcal{A}_\mathcal{H}$ as $l \notin \mathcal{A}_\mathcal{H}$. From $E_1 / \mathcal{A}_\mathcal{H} \approx_{\rm pb} E_2 \setminus \mathcal{A}_\mathcal{H}$ it follows that there exist $\bar{E}_2$ and E_2' such that $E_2 \setminus \mathcal{A}_\mathcal{H} \Longrightarrow \bar{E}_2 \setminus \mathcal{A}_\mathcal{H} \stackrel{l}{\longrightarrow}_{\rm a} E_2' \setminus \mathcal{A}_\mathcal{H}$ with $E_1 / \mathcal{A}_\mathcal{H} \approx_{\rm pb} \bar{E}_2 \setminus \mathcal{A}_\mathcal{H}$ and $E_1' / \mathcal{A}_\mathcal{H} \approx_{\rm pb} E_2' \setminus \mathcal{A}_\mathcal{H}$. Since neither the restriction operator nor the hiding operator applies to τ, l, and to probabilistic transitions, it follows that $(E_2 \setminus L) / \mathcal{A}_\mathcal{H} \Longrightarrow (\bar{E}_2 \setminus L) / \mathcal{A}_\mathcal{H} \stackrel{l}{\longrightarrow}_{\rm a} (E_2' \setminus L) / \mathcal{A}_\mathcal{H}$ with $((E_1 / \mathcal{A}_\mathcal{H}) \setminus L, (\bar{E}_2 \setminus L) / \mathcal{A}_\mathcal{H}) \in \mathcal{B}$ and $((E_1' / \mathcal{A}_\mathcal{H}) \setminus L, (E_2' \setminus L) / \mathcal{A}_\mathcal{H}) \in \mathcal{B}$.
- If $(E_1 / \mathcal{A}_\mathcal{H}) \setminus L \stackrel{\tau}{\longrightarrow}_{\rm a} (E_1' / \mathcal{A}_\mathcal{H}) \setminus L$ with $E_1 \stackrel{\tau}{\longrightarrow}_{\rm a} E_1'$, then $E_1 / \mathcal{A}_\mathcal{H} \stackrel{\tau}{\longrightarrow}_{\rm a} E_1' / \mathcal{A}_\mathcal{H}$ as $\tau \notin \mathcal{A}_\mathcal{H}$. From $E_1 / \mathcal{A}_\mathcal{H} \approx_{\rm pb} E_2 \setminus \mathcal{A}_\mathcal{H}$ it follows that either $E_1' / \mathcal{A}_\mathcal{H} \approx_{\rm pb} E_2 \setminus \mathcal{A}_\mathcal{H}$, or there exist $\bar{E}_2$ and E_2' such that $E_2 \setminus \mathcal{A}_\mathcal{H} \Longrightarrow \bar{E}_2 \setminus \mathcal{A}_\mathcal{H} \stackrel{\tau}{\longrightarrow}_{\rm a} E_2' \setminus \mathcal{A}_\mathcal{H}$ with $E_1 / \mathcal{A}_\mathcal{H} \approx_{\rm pb} \bar{E}_2 \setminus \mathcal{A}_\mathcal{H}$ and $E_1' / \mathcal{A}_\mathcal{H} \approx_{\rm pb} E_2' \setminus \mathcal{A}_\mathcal{H}$. In the former subcase $(E_2 \setminus L) / \mathcal{A}_\mathcal{H}$ is allowed to stay idle with $((E_1' / \mathcal{A}_\mathcal{H}) \setminus L, (E_2 \setminus L) / \mathcal{A}_\mathcal{H}) \in \mathcal{B}$, while in the latter subcase, since neither the restriction operator nor the hiding operator applies to τ and to probabilistic transitions, it follows that $(E_2 \setminus L) / \mathcal{A}_\mathcal{H} \Longrightarrow (\bar{E}_2 \setminus L) / \mathcal{A}_\mathcal{H} \stackrel{\tau}{\longrightarrow}_{\rm a} (E_2' \setminus L) / \mathcal{A}_\mathcal{H}$ with $((E_1 / \mathcal{A}_\mathcal{H}) \setminus L, (\bar{E}_2 \setminus L) / \mathcal{A}_\mathcal{H}) \in \mathcal{B}$ and $((E_1' / \mathcal{A}_\mathcal{H}) \setminus L, (E_2' \setminus L) / \mathcal{A}_\mathcal{H}) \in \mathcal{B}$.
- If $(E_1 / \mathcal{A}_\mathcal{H}) \setminus L \stackrel{\tau}{\longrightarrow}_{\rm a} (E_1' / \mathcal{A}_\mathcal{H}) \setminus L$ with $E_1 \stackrel{h}{\longrightarrow}_{\rm a} E_1'$, then $E_1 / \mathcal{A}_\mathcal{H} \stackrel{\tau}{\longrightarrow}_{\rm a} E_1' / \mathcal{A}_\mathcal{H}$ as $h \in \mathcal{A}_\mathcal{H}$ and the rest of the proof is similar to the one of the previous case.
- If $(E_2 \setminus L) / \mathcal{A}_\mathcal{H} \stackrel{l}{\longrightarrow}_{\rm a} (E_2' \setminus L) / \mathcal{A}_\mathcal{H}$ with $E_2 \stackrel{l}{\longrightarrow}_{\rm a} E_2'$ and $l \notin L$, then $E_2 \setminus \mathcal{A}_\mathcal{H} \stackrel{l}{\longrightarrow}_{\rm a} E_2' \setminus \mathcal{A}_\mathcal{H}$ as $l \notin \mathcal{A}_\mathcal{H}$. From $E_2 \setminus \mathcal{A}_\mathcal{H} \approx_{\rm pb} E_1 / \mathcal{A}_\mathcal{H}$ it follows that there exist $\bar{E}_1$ and E_1' such that $E_1 / \mathcal{A}_\mathcal{H} \Longrightarrow \bar{E}_1 / \mathcal{A}_\mathcal{H} \stackrel{l}{\longrightarrow}_{\rm a} E_1' / \mathcal{A}_\mathcal{H}$ with $E_2 \setminus \mathcal{A}_\mathcal{H} \approx_{\rm pb} \bar{E}_1 / \mathcal{A}_\mathcal{H}$ and $E_2' \setminus \mathcal{A}_\mathcal{H} \approx_{\rm pb} E_1' / \mathcal{A}_\mathcal{H}$. Since the restriction operator does not apply to τ, l, and probabilistic transitions, it follows that $(E_1 / \mathcal{A}_\mathcal{H}) \setminus L \Longrightarrow (\bar{E}_1 / \mathcal{A}_\mathcal{H}) \setminus L \stackrel{l}{\longrightarrow}_{\rm a} (E_1' / \mathcal{A}_\mathcal{H}) \setminus L$ with $((E_2 \setminus L) / \mathcal{A}_\mathcal{H}, (\bar{E}_1 / \mathcal{A}_\mathcal{H}) \setminus L) \in \mathcal{B}$ and $((E_2' \setminus L) / \mathcal{A}_\mathcal{H}, (E_1' / \mathcal{A}_\mathcal{H}) \setminus L) \in \mathcal{B}$.
- If $(E_2 \setminus L) / \mathcal{A}_\mathcal{H} \stackrel{\tau}{\longrightarrow}_{\rm a} (E_2' \setminus L) / \mathcal{A}_\mathcal{H}$ with $E_2 \stackrel{\tau}{\longrightarrow}_{\rm a} E_2'$, then $E_2 \setminus \mathcal{A}_\mathcal{H} \stackrel{\tau}{\longrightarrow}_{\rm a} E_2' \setminus \mathcal{A}_\mathcal{H}$ as $\tau \notin \mathcal{A}_\mathcal{H}$. From $E_2 \setminus \mathcal{A}_\mathcal{H} \approx_{\rm pb} E_1 / \mathcal{A}_\mathcal{H}$ it follows that either $E_2' \setminus \mathcal{A}_\mathcal{H} \approx_{\rm pb} E_1 / \mathcal{A}_\mathcal{H}$, or there exist $\bar{E}_1$ and E_1' such that $E_1 / \mathcal{A}_\mathcal{H} \Longrightarrow \bar{E}_1 / \mathcal{A}_\mathcal{H} \stackrel{\tau}{\longrightarrow}_{\rm a} E_1' / \mathcal{A}_\mathcal{H}$ with $E_2 \setminus \mathcal{A}_\mathcal{H} \approx_{\rm pb} \bar{E}_1 / \mathcal{A}_\mathcal{H}$ and $E_2' \setminus \mathcal{A}_\mathcal{H} \approx_{\rm pb}$

$E_1' \,/\, \mathcal{A}_\mathcal{H}$. In the former subcase $(E_1 \,/\, \mathcal{A}_\mathcal{H}) \setminus L$ is allowed to stay idle with $((E_2' \setminus L) \,/\, \mathcal{A}_\mathcal{H}, (E_1 \,/\, \mathcal{A}_\mathcal{H}) \setminus L) \in \mathcal{B}$, while in the latter subcase, since the restriction operator does not apply to τ nor to probabilistic transitions, it follows that $(E_1 \,/\, \mathcal{A}_\mathcal{H}) \setminus L \Longrightarrow (\bar{E}_1 \,/\, \mathcal{A}_\mathcal{H}) \setminus L \xrightarrow{\tau}_\mathrm{a} (E_1' \,/\, \mathcal{A}_\mathcal{H}) \setminus L$ with $((E_2 \setminus L) \,/\, \mathcal{A}_\mathcal{H}, (\bar{E}_1 \,/\, \mathcal{A}_\mathcal{H}) \setminus L) \in \mathcal{B}$ and $((E_2' \setminus L) \,/\, \mathcal{A}_\mathcal{H}, (E_1' \,/\, \mathcal{A}_\mathcal{H}) \setminus L) \in \mathcal{B}$.

- If $(E_2 \setminus L) \,/\, \mathcal{A}_\mathcal{H} \xrightarrow{\tau}_\mathrm{a} (E_2' \setminus L) \,/\, \mathcal{A}_\mathcal{H}$ with $E_2 \xrightarrow{h}_\mathrm{a} E_2'$ and $h \notin L$, then $E_2 \,/\, \mathcal{A}_\mathcal{H} \xrightarrow{\tau}_\mathrm{a} E_2' \,/\, \mathcal{A}_\mathcal{H}$ as $h \in \mathcal{A}_\mathcal{H}$ (note that $E_2 \setminus \mathcal{A}_\mathcal{H}$ cannot perform h). From $E_2 \,/\, \mathcal{A}_\mathcal{H} \approx_\mathrm{pb} E_2 \setminus \mathcal{A}_\mathcal{H}$ – as $E \in \mathrm{SBSNNI}_{\approx_\mathrm{pb}}$ and $E_2 \in \mathit{reach}(E)$ – and $E_2 \setminus \mathcal{A}_\mathcal{H} \approx_\mathrm{pb} E_1 \,/\, \mathcal{A}_\mathcal{H}$ it follows that either $E_2' \,/\, \mathcal{A}_\mathcal{H} \approx_\mathrm{pb} E_1 \,/\, \mathcal{A}_\mathcal{H}$ and hence $E_2' \setminus \mathcal{A}_\mathcal{H} \approx_\mathrm{pb} E_1 \,/\, \mathcal{A}_\mathcal{H}$, or there exist $\bar{E}_1$ and E_1' such that $E_1 \,/\, \mathcal{A}_\mathcal{H} \Longrightarrow \bar{E}_1 \,/\, \mathcal{A}_\mathcal{H} \xrightarrow{\tau}_\mathrm{a} E_1' \,/\, \mathcal{A}_\mathcal{H}$ with $E_2 \,/\, \mathcal{A}_\mathcal{H} \approx_\mathrm{pb} \bar{E}_1 \,/\, \mathcal{A}_\mathcal{H}$ and $E_2' \,/\, \mathcal{A}_\mathcal{H} \approx_\mathrm{pb} E_1' \,/\, \mathcal{A}_\mathcal{H}$ and hence $E_2 \setminus \mathcal{A}_\mathcal{H} \approx_\mathrm{pb} \bar{E}_1 \,/\, \mathcal{A}_\mathcal{H}$ and $E_2' \setminus \mathcal{A}_\mathcal{H} \approx_\mathrm{pb} E_1' \,/\, \mathcal{A}_\mathcal{H}$. In the former subcase $(E_1 \,/\, \mathcal{A}_\mathcal{H}) \setminus L$ is allowed to stay idle with $((E_2' \setminus L) \,/\, \mathcal{A}_\mathcal{H}, (E_1 \,/\, \mathcal{A}_\mathcal{H}) \setminus L) \in \mathcal{B}$, while in the latter subcase, since the restriction operator does not apply to τ and to probabilistic transitions, it follows that $(E_1 \,/\, \mathcal{A}_\mathcal{H}) \setminus L \Longrightarrow (\bar{E}_1 \,/\, \mathcal{A}_\mathcal{H}) \setminus L \xrightarrow{\tau}_\mathrm{a} (E_1' \,/\, \mathcal{A}_\mathcal{H}) \setminus L$ with $((E_2 \setminus L) \,/\, \mathcal{A}_\mathcal{H}, (\bar{E}_1 \,/\, \mathcal{A}_\mathcal{H}) \setminus L) \in \mathcal{B}$ and $((E_2' \setminus L) \,/\, \mathcal{A}_\mathcal{H}, (E_1' \,/\, \mathcal{A}_\mathcal{H}) \setminus L) \in \mathcal{B}$.

As far as probabilities are concerned, from the fact that $E_1 \,/\, \mathcal{A}_\mathcal{H} \approx_\mathrm{p} E_2 \setminus \mathcal{A}_\mathcal{H}$ it follows that for all equivalence classes $C \in \mathbb{P}/\mathcal{B}$, $\mathit{prob}(E_1 \,/\, \mathcal{A}_\mathcal{H}, C) = \mathit{prob}(E_2 \setminus \mathcal{A}_\mathcal{H}, C)$, and from the fact that the hiding operator and the restriction do not apply to probabilistic transitions, it follows that for all equivalence classes $C \in \mathcal{B}$, $\mathit{prob}((E_1 \,/\, \mathcal{A}_\mathcal{H}) \setminus L, C) = \mathit{prob}((E_2 \setminus L) \,/\, \mathcal{A}_\mathcal{H}), C)$. The same reasoning applies to the other pairs of processes mentioned in the proof.

4. Given an arbitrary $E \in \mathrm{SBSNNI}_{\approx_\mathrm{pb}}$ and an arbitrary $L \subseteq \mathcal{A}_\mathcal{L}$, for every $E' \in \mathit{reach}(E)$ it holds that $E' \setminus \mathcal{A}_\mathcal{H} \approx_\mathrm{pb} E' \,/\, \mathcal{A}_\mathcal{H}$, from which we derive that $(E' \setminus \mathcal{A}_\mathcal{H}) \,/\, L \approx_\mathrm{pb} (E' / \mathcal{A}_\mathcal{H}) \,/\, L$ because $\approx_\mathrm{pb}$ is a congruence with respect to the hiding operator (see the proof of Lemma 1). 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 $(E' \,/\, L) \setminus \mathcal{A}_\mathcal{H} \approx_\mathrm{pb} (E' \,/\, L) \,/\, \mathcal{A}_\mathcal{H}$, i.e., $E' \,/\, L$ is $\mathrm{BSNNI}_{\approx_\mathrm{pb}}$.

We now prove the results for $\mathrm{SBNDC}_{\approx_\mathrm{pb}}$:

1. Given an arbitrary $E \in \mathrm{SBNDC}_{\approx_\mathrm{pb}}$ and an arbitrary $a \in \mathcal{A}_\tau \setminus \mathcal{A}_\mathcal{H}$, it trivially holds that $a \,.\, E \in \mathrm{SBNDC}_{\approx_\mathrm{pb}}$.
2. Given two arbitrary $E_1, E_2 \in \mathrm{SBNDC}_{\approx_\mathrm{pb}}$ and an arbitrary $L \subseteq \mathcal{A}$, the result follows by proving that the symmetric relation $\mathcal{B} = \{((F_1 \parallel_L F_2) \setminus \mathcal{A}_\mathcal{H}, (R_1 \parallel_L R_2) \setminus \mathcal{A}_\mathcal{H}), ((R_1 \parallel_L R_2) \setminus \mathcal{A}_\mathcal{H}, (F_1 \parallel_L F_2) \setminus \mathcal{A}_\mathcal{H}) \mid F_1 \parallel_L F_2, R_1 \parallel_L R_2 \in \mathit{reach}(E_1 \parallel_L E_2) \wedge F_1 \setminus \mathcal{A}_\mathcal{H} \approx_\mathrm{pb} R_1 \setminus \mathcal{A}_\mathcal{H} \wedge F_2 \setminus \mathcal{A}_\mathcal{H} \approx_\mathrm{pb} R_2 \setminus \mathcal{A}_\mathcal{H}\}$ is a probabilistic branching bisimulation, as can be seen by observing that whenever $E_1' \parallel_L E_2' \xrightarrow{h}_\mathrm{a} E_1'' \parallel_L E_2''$ for $E_1' \parallel_L E_2' \in \mathit{reach}(E_1 \parallel_L E_2)$:
   - If $E_1' \xrightarrow{h}_\mathrm{a} E_1''$, $E_2'' = E_2'$, and $h \notin L$, then from $E_1 \in \mathrm{SBNDC}_{\approx_\mathrm{pb}}$ it follows that $E_1' \setminus \mathcal{A}_\mathcal{H} \approx_\mathrm{pb} E_1'' \setminus \mathcal{A}_\mathcal{H}$ and hence $((E_1' \parallel_L E_2') \setminus \mathcal{A}_\mathcal{H}, ((E_1'' \parallel_L E_2'') \setminus \mathcal{A}_\mathcal{H}) \in \mathcal{B}$ as $E_2' \setminus \mathcal{A}_\mathcal{H} \approx_\mathrm{pb} E_2'' \setminus \mathcal{A}_\mathcal{H}$.

- If $E_2' \xrightarrow{h}_{\rm a} E_2''$, $E_1'' = E_1'$, and $h \notin L$, then from $E_2 \in {\rm SBNDC}_{\approx_{\rm pb}}$ it follows that $E_2' \setminus \mathcal{A}_\mathcal{H} \approx_{\rm pb} E_2'' \setminus \mathcal{A}_\mathcal{H}$ and hence $((E_1' \parallel_L E_2') \setminus \mathcal{A}_\mathcal{H}, ((E_1'' \parallel_L E_2'') \setminus \mathcal{A}_\mathcal{H}) \in \mathcal{B}$ as $E_1' \setminus \mathcal{A}_\mathcal{H} \approx_{\rm pb} E_1'' \setminus \mathcal{A}_\mathcal{H}$.
- If $E_1' \xrightarrow{h}_{\rm a} E_1''$, $E_2' \xrightarrow{h}_{\rm a} E_2''$, and $h \in L$, then from $E_1, E_2 \in {\rm SBNDC}_{\approx_{\rm pb}}$ it follows that $E_1' \setminus \mathcal{A}_\mathcal{H} \approx_{\rm pb} E_1'' \setminus \mathcal{A}_\mathcal{H}$ and $E_2' \setminus \mathcal{A}_\mathcal{H} \approx_{\rm pb} E_2'' \setminus \mathcal{A}_\mathcal{H}$, which in turn entail that $((E_1' \parallel_L E_2') \setminus \mathcal{A}_\mathcal{H}, ((E_1'' \parallel_L E_2'') \setminus \mathcal{A}_\mathcal{H}) \in \mathcal{B}$.

Assuming that $((F_1 \parallel_L F_2) \setminus \mathcal{A}_\mathcal{H}, (R_1 \parallel_L R_2) \setminus \mathcal{A}_\mathcal{H}) \in \mathcal{B}$, there are five cases:

- 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 $F_1 \setminus \mathcal{A}_\mathcal{H} \approx_{\rm pb} R_1 \setminus \mathcal{A}_\mathcal{H}$ it follows that there exist $\bar{R}_1$ and R_1' such that $R_1 \setminus \mathcal{A}_\mathcal{H} \Longrightarrow \bar{R}_1 \setminus \mathcal{A}_\mathcal{H} \xrightarrow{l}_{\rm a} R_1' \setminus \mathcal{A}_\mathcal{H}$ with $F_1 \setminus \mathcal{A}_\mathcal{H} \approx_{\rm pb} \bar{R}_1 \setminus \mathcal{A}_\mathcal{H}$ and $F_1' \setminus \mathcal{A}_\mathcal{H} \approx_{\rm pb} R_1' \setminus \mathcal{A}_\mathcal{H}$. Since synchronization does not apply to τ, it follows that $(R_1 \parallel_L R_2) \setminus \mathcal{A}_\mathcal{H} \Longrightarrow (\bar{R}_1 \parallel_L R_2) \setminus \mathcal{A}_\mathcal{H} \xrightarrow{l}_{\rm a} (R_1' \parallel_L [1]R_2) \setminus \mathcal{A}_\mathcal{H}$ with $((F_1 \parallel_L F_2) \setminus \mathcal{A}_\mathcal{H}, (\bar{R}_1 \parallel_L R_2) \setminus \mathcal{A}_\mathcal{H}) \in \mathcal{B}$ and $((F_1' \parallel_L [1]F_2) \setminus \mathcal{A}_\mathcal{H}, (R_1' \parallel_L [1]R_2) \setminus \mathcal{A}_\mathcal{H}) \in \mathcal{B}$.
- 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 $F_i \setminus \mathcal{A}_\mathcal{H} \approx_{\rm b} R_i \setminus \mathcal{A}_\mathcal{H}$ it follows that there exist $\bar{R}_i$ and R_i' such that $R_i \setminus \mathcal{A}_\mathcal{H} \Longrightarrow \bar{R}_i \setminus \mathcal{A}_\mathcal{H} \xrightarrow{l}_{\rm a} R_i' \setminus \mathcal{A}_\mathcal{H}$ with $F_i \setminus \mathcal{A}_\mathcal{H} \approx_{\rm pb} \bar{R}_i \setminus \mathcal{A}_\mathcal{H}$ and $F_i' \setminus \mathcal{A}_\mathcal{H} \approx_{\rm pb} R_i' \setminus \mathcal{A}_\mathcal{H}$. Since synchronization does not apply to τ, it follows that $(R_1 \parallel_L R_2) \setminus \mathcal{A}_\mathcal{H} \Longrightarrow (\bar{R}_1 \parallel_L \bar{R}_2) \setminus \mathcal{A}_\mathcal{H} \xrightarrow{l}_{\rm a} (R_1' \parallel_L R_2') \setminus \mathcal{A}_\mathcal{H}$ with $((F_1 \parallel_L F_2) \setminus \mathcal{A}_\mathcal{H}, (\bar{R}_1 \parallel_L \bar{R}_2) \setminus \mathcal{A}_\mathcal{H}) \in \mathcal{B}$ and $((F_1' \parallel_L F_2') \setminus \mathcal{A}_\mathcal{H}, (R_1' \parallel_L R_2') \setminus \mathcal{A}_\mathcal{H}) \in \mathcal{B}$.
- 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 $F_1 \setminus \mathcal{A}_\mathcal{H} \xrightarrow{\tau}_{\rm a} F_1' \setminus \mathcal{A}_\mathcal{H}$. From $F_1 \setminus \mathcal{A}_\mathcal{H} \approx_{\rm pb} R_1 \setminus \mathcal{A}_\mathcal{H}$ it follows that either $F_1' \setminus \mathcal{A}_\mathcal{H} \approx_{\rm pb} R_1 \setminus \mathcal{A}_\mathcal{H}$, or there exist $\bar{R}_1$ and R_1' such that $R_1 \setminus \mathcal{A}_\mathcal{H} \Longrightarrow \bar{R}_1 \setminus \mathcal{A}_\mathcal{H} \xrightarrow{\tau}_{\rm a} R_1' \setminus \mathcal{A}_\mathcal{H}$ with $F_1 \setminus \mathcal{A}_\mathcal{H} \approx_{\rm pb} \bar{R}_1 \setminus \mathcal{A}_\mathcal{H}$ and $F_1' \setminus \mathcal{A}_\mathcal{H} \approx_{\rm pb} R_1' \setminus \mathcal{A}_\mathcal{H}$. In the former subcase $(R_1 \parallel_L R_2) \setminus \mathcal{A}_\mathcal{H}$ is allowed to stay idle with $((F_1' \parallel_L F_2) \setminus \mathcal{A}_\mathcal{H}, (R_1 \parallel_L R_2) \setminus \mathcal{A}_\mathcal{H}) \in \mathcal{B}$, while in the latter subcase, since synchronization does not apply to τ, it follows that $(R_1 \parallel_L R_2) \setminus \mathcal{A}_\mathcal{H} \Longrightarrow (\bar{R}_1 \parallel_L R_2) \setminus \mathcal{A}_\mathcal{H} \xrightarrow{\tau}_{\rm a} (R_1' \parallel_L [1]R_2) \setminus \mathcal{A}_\mathcal{H}$ with $((F_1 \parallel_L F_2) \setminus \mathcal{A}_\mathcal{H}, (\bar{R}_1 \parallel_L R_2) \setminus \mathcal{A}_\mathcal{H}) \in \mathcal{B}$ and $((F_1' \parallel_L [1]F_2) \setminus \mathcal{A}_\mathcal{H}, (R_1' \parallel_L [1]R_2) \setminus \mathcal{A}_\mathcal{H}) \in \mathcal{B}$.
- 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 far as probability are concerned, given two arbitrary probabilistic processes $S_1, S_2 \in \mathbb{P}$, we observe that $prob((F_1 \setminus \mathcal{A}_\mathcal{H}) \parallel_L (F_2 \setminus \mathcal{A}_\mathcal{H}), [S_1 \parallel_L S_2]_\mathcal{B}) = prob(F_1 \setminus \mathcal{A}_\mathcal{H}, [S_1]_\mathcal{B}) \cdot prob(F_2 \setminus \mathcal{A}_\mathcal{H}, [S_2]_\mathcal{B})$ and $prob((R_1 \setminus \mathcal{A}_\mathcal{H}) \parallel_L R_2 \setminus \mathcal{A}_\mathcal{H}), [S_1 \parallel_L S_2]_\mathcal{B}) = prob(R_1 \,/\, \mathcal{A}_\mathcal{H}, [S_1]_\mathcal{B}) \cdot prob(R_2 \,/\, \mathcal{A}_\mathcal{H}, [S_2]_\mathcal{B})$ (see the proof of Lemma 1). Now, from the fact that $F_i \setminus \mathcal{A}_\mathcal{H} \approx_{\rm pb} R_i \setminus \mathcal{A}_\mathcal{H}$, for $i \in \{1, 2\}$, it follows that for all equivalence classes $C \in \mathbb{P}/\mathcal{B}$, $prob(F_i \setminus \mathcal{A}_\mathcal{H}, C) = prob(R_i \setminus \mathcal{A}_\mathcal{H}, C)$, which in turn implies that $prob((F_1 \setminus \mathcal{A}_\mathcal{H}) \parallel_L (F_2 \setminus \mathcal{A}_\mathcal{H}), [S_1 \parallel_L S_2]_\mathcal{B}) =$

$prob((R_1 \setminus \mathcal{A}_\mathcal{H}) \parallel_L (R_2 \setminus \mathcal{A}_\mathcal{H}), [S_1 \parallel_L S_2]_\mathcal{B})$. Lastly, from the fact that the restriction operators does not apply to probabilistic transitions we conclude that $prob((F_1 \parallel_L F_2) \setminus \mathcal{A}_\mathcal{H}, [S_1 \parallel_L S_2]_\mathcal{B}) = prob((R_1 \parallel_L R_2) \setminus \mathcal{A}_\mathcal{H}, [S_1 \parallel_L S_2]_\mathcal{B})$.

3. Given an arbitrary $E \in \text{SBNDC}_{\approx_{\text{pb}}}$ and an arbitrary $L \subseteq \mathcal{A}$, for every $E' \in reach(E)$ and for every E'' such that $E' \xrightarrow{h}_{\text{a}} E''$ it holds that $E' \setminus \mathcal{A}_\mathcal{H} \approx_{\text{pb}} E'' \setminus \mathcal{A}_\mathcal{H}$, from which we derive that $(E' \setminus \mathcal{A}_\mathcal{H}) \setminus L \approx_{\text{pb}} (E'' \setminus \mathcal{A}_\mathcal{H}) \setminus L$ because $\approx_{\text{pb}}$ is a congruence with respect to the restriction operator (see the proof of Lemma 1). 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 $(E' \setminus L) \setminus \mathcal{A}_\mathcal{H} \approx_{\text{pb}} (E'' \setminus L) \setminus \mathcal{A}_\mathcal{H}$.
4. Given an arbitrary $E \in \text{SBNDC}_{\approx_{\text{pb}}}$ and an arbitrary $L \subseteq \mathcal{A}_\mathcal{L}$, for every $E' \in reach(E)$ and for every E'' such that $E' \xrightarrow{h}_{\text{a}} E''$ it holds that $E' \setminus \mathcal{A}_\mathcal{H} \approx_{\text{pb}} E'' \setminus \mathcal{A}_\mathcal{H}$, from which we derive that $(E' \setminus \mathcal{A}_\mathcal{H}) / L \approx_{\text{pb}} (E'' \setminus \mathcal{A}_\mathcal{H}) / L$ because $\approx_{\text{pb}}$ is a congruence with respect to the hiding operator (see the proof of Lemma 1). 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 $(E' / L) \setminus \mathcal{A}_\mathcal{H} \approx_{\text{pb}} (E'' / L) \setminus \mathcal{A}_\mathcal{H}$. ■

Proof of Theorem 3. We first prove the results for the $\approx_{\text{p}}$-based properties. Let us examine each relationship separately:

- $\text{SBNDC}_{\approx_{\text{p}}} \subset \text{SBSNNI}_{\approx_{\text{p}}}$. We need to prove that for a given $E \in \mathbb{P}$, if $E \in \text{SBNDC}$, it follows that for every E' reachable from E, $E' \in \text{BSNNI}_{\approx_{\text{p}}}$. Since the processes we are considering are not recursive we can treat them as trees, and hence we can proceed by induction on their depth. In this case we will proceed by induction on the depth of E:
  - If the depth of E is 0 then E has no outgoing transitions and it behaves as $\underline{0}$. This obviously entails that $E \setminus \mathcal{A}_\mathcal{H} \approx_{\text{p}} E / \mathcal{A}_\mathcal{H}$.
  - If the depth of E is $n+1$ with $n \in \mathbb{N}$, then take any E' of depth n such that $E \xrightarrow{a}_{\text{a}} E'$. By hypothesis, $E, E' \in \text{SBNDC}_{\approx_{\text{p}}}$ and by induction hypothesis $E' \in \text{SBSNNI}_{\approx_{\text{p}}}$. Hence, we just need to prove that $E \setminus \mathcal{A}_\mathcal{H} \approx_{\text{p}} E / \mathcal{A}_\mathcal{H}$. There are three cases:
    - If $a \notin \mathcal{A}_\mathcal{H}$ then both $E \setminus \mathcal{A}_\mathcal{H}$ and $E / \mathcal{A}_\mathcal{H}$ can execute a and reach, respectively, $E' \setminus \mathcal{A}_\mathcal{H}$ and $E' / \mathcal{A}_\mathcal{H}$, which are weakly probabilistic bisimilar by induction hypothesis. Thus Definition 4 is respected.
    - If $a \in \mathcal{A}_\mathcal{H}$ we have that $E / \mathcal{A}_\mathcal{H} \xrightarrow{\tau}_{\text{a}} E' / \mathcal{A}_\mathcal{H}$, with $E \xrightarrow{a}_{\text{a}} E'$. By induction hypothesis we have that $E' \setminus \mathcal{A}_\mathcal{H} \approx_{\text{p}} E' / \mathcal{A}_\mathcal{H}$, and since $a \in \mathcal{A}_\mathcal{H}$ and $E \in \text{SBNDC}_{\approx_{\text{p}}}$ we have $E \setminus \mathcal{A}_\mathcal{H} \approx_{\text{p}} E' \setminus \mathcal{A}_\mathcal{H}$. By transitivity it follows that $E \setminus \mathcal{A}_\mathcal{H} \approx_{\text{p}} E' / \mathcal{A}_\mathcal{H}$ which, combined with $E / \mathcal{A}_\mathcal{H} \xrightarrow{\tau}_{\text{a}} E' / \mathcal{A}_\mathcal{H}$, determines the condition required by Definition 4.
    - If $E / \mathcal{A}_\mathcal{H} \xrightarrow{p}_{\text{p}} E' / \mathcal{A}_\mathcal{H}$ then $E \setminus \mathcal{A}_\mathcal{H}$ can perform the same transition, i.e., $E \setminus \mathcal{A}_\mathcal{H} \xrightarrow{p}_{\text{p}} E' \setminus \mathcal{A}_\mathcal{H}$, because the hiding and restriction operators do not apply to probabilistic transitions. The processes $E' / \mathcal{A}_\mathcal{H}$ and $E' \setminus \mathcal{A}_\mathcal{H}$ are weakly probabilistic bisimilar because of the induction hypothesis.

– $\text{SBSNNI}_{\approx_\text{p}} = \text{P\_BNDC}_{\approx_\text{p}}$. We first prove that $\text{P\_BNDC}_{\approx_\text{p}} \subseteq \text{SBSNNI}_{\approx_\text{p}}$. If $E \in \text{P\_BNDC}_{\approx_\text{p}}$, then $E' \in \text{BNDC}_{\approx_\text{p}}$ for every $E' \in \mathit{reach}(E)$. Since $\text{BNDC}_{\approx_\text{p}} \subset \text{BSNNI}_{\approx_\text{p}}$ as will be shown in the last case of the proof of this part of the theorem, $E' \in \text{BSNNI}_{\approx_\text{p}}$ for every $E' \in \mathit{reach}(E)$, i.e., $E \in \text{SBSNNI}_{\approx_\text{p}}$.
The fact that $\text{SBSNNI}_{\approx_\text{p}} \subseteq \text{P\_BNDC}_{\approx_\text{p}}$ will follow by proving that the symmetric relation $\mathcal{B} = \{(E_1' \setminus \mathcal{A}_\mathcal{H}, ((E_2' \parallel_L F) / L) \setminus \mathcal{A}_\mathcal{H}), (((E_2' \parallel_L F) / L) \setminus \mathcal{A}_\mathcal{H}, E_1' \setminus \mathcal{A}_\mathcal{H}) \mid E_1' \in \mathit{reach}(E_1) \wedge E_2' \in \mathit{reach}(E_2) \wedge F$ executing only actions in $\mathcal{A}_\mathcal{H} \wedge L \subseteq \mathcal{A}_\mathcal{H} \wedge E_1' \setminus \mathcal{A}_\mathcal{H} \approx_\text{p} E_2' / \mathcal{A}_\mathcal{H} \wedge E_2 \in \text{SBSNNI}_{\approx_\text{p}}\}$ is a weak probabilistic bisimulation, as can be seen by taking E_1' identical to E_2' and both reachable from $E \in \text{SBSNNI}_{\approx_\text{p}}$. Assuming that $E_1' \setminus \mathcal{A}_\mathcal{H}$ and $((E_2' \parallel_L F) / L) \setminus \mathcal{A}_\mathcal{H}$ are related by $\mathcal{B}$ – so that $E_1' \setminus \mathcal{A}_\mathcal{H} \approx_\text{p} E_2' / \mathcal{A}_\mathcal{H}$ – there are six cases:

- If $E_1' \setminus \mathcal{A}_\mathcal{H} \xrightarrow{l}_\text{a} E_1'' \setminus \mathcal{A}_\mathcal{H}$, we observe that from $E_2' \in \mathit{reach}(E_2)$ and $E_2 \in \text{SBSNNI}_{\approx_\text{p}}$ it follows that $E_2' \setminus \mathcal{A}_\mathcal{H} \approx_\text{p} E_2' / \mathcal{A}_\mathcal{H}$, so that $E_1' \setminus \mathcal{A}_\mathcal{H} \approx_\text{p} E_2' / \mathcal{A}_\mathcal{H} \approx_\text{p} E_2' \setminus \mathcal{A}_\mathcal{H}$, i.e., $E_1' \setminus \mathcal{A}_\mathcal{H} \approx_\text{p} E_2' \setminus \mathcal{A}_\mathcal{H}$. As a consequence, since $l \neq \tau$ there exists a process E_2'' such that $E_2' \setminus \mathcal{A}_\mathcal{H} \Longrightarrow \xrightarrow{l}_\text{a} \Longrightarrow E_2'' \setminus \mathcal{A}_\mathcal{H}$ with $E_1'' \setminus \mathcal{A}_\mathcal{H} \approx_\text{p} E_2'' \setminus \mathcal{A}_\mathcal{H}$. Therefore, $((E_2' \parallel_L F) / L) \setminus \mathcal{A}_\mathcal{H} \Longrightarrow \xrightarrow{l}_\text{a} \Longrightarrow ((E_2'' \parallel_L F) / L) \setminus \mathcal{A}_\mathcal{H}$ with $(E_1'' \setminus \mathcal{A}_\mathcal{H}, ((E_2'' \parallel_L F) / L) \setminus \mathcal{A}_\mathcal{H}) \in \mathcal{B}$ – because $E_1'' \in \mathit{reach}(E_1)$, $E_2'' \in \mathit{reach}(E_2)$, and $E_1'' \setminus \mathcal{A}_\mathcal{H} \approx_\text{p} E_2'' / \mathcal{A}_\mathcal{H}$ as $E_2 \in \text{SBSNNI}_{\approx_\text{p}}$. Note that if $E_2'' \setminus \mathcal{A}_\mathcal{H}$ is a probabilistic process F is prefixed by [1] in the reached process.
- If $E_1' \setminus \mathcal{A}_\mathcal{H} \xrightarrow{\tau}_\text{a} E_1'' \setminus \mathcal{A}_\mathcal{H}$, we observe that from $E_2' \in \mathit{reach}(E_2)$ and $E_2 \in \text{SBSNNI}_{\approx_\text{p}}$ it follows that $E_2' \setminus \mathcal{A}_\mathcal{H} \approx_\text{p} E_2' / \mathcal{A}_\mathcal{H}$, so from $E_1' \setminus \mathcal{A}_\mathcal{H} \approx_\text{p} E_2' / \mathcal{A}_\mathcal{H} \approx_\text{p} E_2' \setminus \mathcal{A}_\mathcal{H}$, i.e., $E_1' \setminus \mathcal{A}_\mathcal{H} \approx_\text{p} E_2' \setminus \mathcal{A}_\mathcal{H}$, it follows that there exists a process E_2'' such that $E_2' \setminus \mathcal{A}_\mathcal{H} \Longrightarrow E_2'' \setminus \mathcal{A}_\mathcal{H}$ with $E_1'' \setminus \mathcal{A}_\mathcal{H} \approx_\text{p} E_2'' \setminus \mathcal{A}_\mathcal{H}$. Therefore, $((E_2' \parallel_L F) / L) \setminus \mathcal{A}_\mathcal{H} \Longrightarrow ((E_2'' \parallel_L F) / L) \setminus \mathcal{A}_\mathcal{H}$ with $E_1' \setminus \mathcal{A}_\mathcal{H} \approx_\text{p} \bar{E}_2' / \mathcal{A}_\mathcal{H}$ as $E_2 \in \text{SBSNNI}_{\approx_\text{p}}$ – 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 $E_1'' \setminus \mathcal{A}_\mathcal{H} \approx_\text{p} E_2'' / \mathcal{A}_\mathcal{H}$ as $E_2 \in \text{SBSNNI}_{\approx_\text{p}}$. Note that if $E_2'' \setminus \mathcal{A}_\mathcal{H}$ is a probabilistic process F is prefixed by [1] in the reached process.
- If $((E_2' \parallel_L F) / L) \setminus \mathcal{A}_\mathcal{H} \xrightarrow{l}_\text{a} ((E_2'' \parallel_L [1]F) / L) \setminus \mathcal{A}_\mathcal{H}$ because $E_2' \xrightarrow{l}_\text{a} E_2''$ so that $E_2' \setminus \mathcal{A}_\mathcal{H} \xrightarrow{l}_\text{a} E_2'' \setminus \mathcal{A}_\mathcal{H}$, we observe that from $E_2' \in \mathit{reach}(E_2)$ and $E_2 \in \text{SBSNNI}_{\approx_\text{p}}$ it follows that $E_2' \setminus \mathcal{A}_\mathcal{H} \approx_\text{p} E_2' / \mathcal{A}_\mathcal{H}$, so that $E_2' \setminus \mathcal{A}_\mathcal{H} \approx_\text{p} E_2' / \mathcal{A}_\mathcal{H} \approx_\text{p} E_1' \setminus \mathcal{A}_\mathcal{H}$, i.e., $E_2' \setminus \mathcal{A}_\mathcal{H} \approx_\text{p} E_1' \setminus \mathcal{A}_\mathcal{H}$. As a consequence, since $l \neq \tau$ there exists a process E_1'' such that $E_1' \setminus \mathcal{A}_\mathcal{H} \Longrightarrow \xrightarrow{l}_\text{a} \Longrightarrow E_1'' \setminus \mathcal{A}_\mathcal{H}$ with $E_2'' \setminus \mathcal{A}_\mathcal{H} \approx_\text{p} E_1'' \setminus \mathcal{A}_\mathcal{H}$. Therefore, $(((E_2'' \parallel_L [1]F) / L) \setminus \mathcal{A}_\mathcal{H}, E_1'' \setminus \mathcal{A}_\mathcal{H}) \in \mathcal{B}$ – because $E_1'' \in \mathit{reach}(E_1)$, $E_2'' \in \mathit{reach}(E_2)$, and $E_1'' \setminus \mathcal{A}_\mathcal{H} \approx_\text{p} E_2'' / \mathcal{A}_\mathcal{H}$ as $E_2 \in \text{SBSNNI}_{\approx_\text{p}}$.
- If $((E_2' \parallel_L F) / L) \setminus \mathcal{A}_\mathcal{H} \xrightarrow{\tau}_\text{a} ((E_2'' \parallel_L [1]F) / L) \setminus \mathcal{A}_\mathcal{H}$ because $E_2' \xrightarrow{\tau}_\text{a} E_2''$ so that $E_2' \setminus \mathcal{A}_\mathcal{H} \xrightarrow{\tau}_\text{a} E_2'' \setminus \mathcal{A}_\mathcal{H}$, we observe that from $E_2' \in \mathit{reach}(E_2)$ and $E_2 \in \text{SBSNNI}_{\approx_\text{p}}$ it follows that $E_2' \setminus \mathcal{A}_\mathcal{H} \approx_\text{p} E_2' / \mathcal{A}_\mathcal{H}$, so that $E_2' \setminus \mathcal{A}_\mathcal{H} \approx_\text{p} E_2' / \mathcal{A}_\mathcal{H} \approx_\text{p} E_1' \setminus \mathcal{A}_\mathcal{H}$, i.e., $E_2' \setminus \mathcal{A}_\mathcal{H} \approx_\text{p} E_1' \setminus \mathcal{A}_\mathcal{H}$. It follows that there exists a process E_1'' such that $E_1' \setminus \mathcal{A}_\mathcal{H} \Longrightarrow E_1'' \setminus \mathcal{A}_\mathcal{H}$ with $E_2'' \setminus \mathcal{A}_\mathcal{H} \approx_\text{p} E_1'' \setminus \mathcal{A}_\mathcal{H}$. Therefore, $(((E_2'' \parallel_L [1]F) / L) \setminus \mathcal{A}_\mathcal{H}, E_1'' \setminus \mathcal{A}_\mathcal{H}) \in \mathcal{B}$

– because $E_1'' \in \mathit{reach}(E_1)$, $E_2'' \in \mathit{reach}(E_2)$, and $E_1'' \setminus \mathcal{A}_\mathcal{H} \approx_\mathrm{p} E_2'' / \mathcal{A}_\mathcal{H}$ as $E_2 \in \mathrm{SBSNNI}_{\approx_\mathrm{p}}$.

- If $((E_2' \parallel_L F) / L) \setminus \mathcal{A}_\mathcal{H} \xrightarrow{\tau}_\mathrm{a} ((E_2' \parallel_L F') / L) \setminus \mathcal{A}_\mathcal{H}$ because $F \xrightarrow{\tau}_\mathrm{a} F'$, then trivially $(((E_2' \parallel_L F') / L) \setminus \mathcal{A}_\mathcal{H}, E_1' \setminus \mathcal{A}_\mathcal{H}) \in \mathcal{B}$.
- If $((E_2' \parallel_L F) / L) \setminus \mathcal{A}_\mathcal{H} \xrightarrow{\tau}_\mathrm{a} ((E_2'' \parallel_L F') / L) \setminus \mathcal{A}_\mathcal{H})$ because $E_2' \xrightarrow{h}_\mathrm{a} E_2''$ – so that $E_2' / \mathcal{A}_\mathcal{H} \xrightarrow{\tau}_\mathrm{a} E_2'' / \mathcal{A}_\mathcal{H}$ – and $F \xrightarrow{h}_\mathrm{a} F'$, we observe that from $E_2', E_2'' \in \mathit{reach}(E_2)$ and $E_2 \in \mathrm{SBSNNI}_{\approx_\mathrm{p}}$ it follows that $E_2' \setminus \mathcal{A}_\mathcal{H} \approx_\mathrm{p} E_2' / \mathcal{A}_\mathcal{H}$ and $E_2'' \setminus \mathcal{A}_\mathcal{H} \approx_\mathrm{p} E_2'' / \mathcal{A}_\mathcal{H}$, so that $E_2' \setminus \mathcal{A}_\mathcal{H} \xrightarrow{\tau}_\mathrm{a} E_2'' \setminus \mathcal{A}_\mathcal{H}$ and $E_2' \setminus \mathcal{A}_\mathcal{H} \approx_\mathrm{p} E_2' / \mathcal{A}_\mathcal{H} \approx_\mathrm{p} E_1' \setminus \mathcal{A}_\mathcal{H}$, i.e., $E_2' \setminus \mathcal{A}_\mathcal{H} \approx_\mathrm{p} E_1' \setminus \mathcal{A}_\mathcal{H}$. It follows that there exists a process E_1'' such that $E_1' \setminus \mathcal{A}_\mathcal{H} \Longrightarrow E_1'' \setminus \mathcal{A}_\mathcal{H}$ with $E_2'' \setminus \mathcal{A}_\mathcal{H} \approx_\mathrm{p} E_1'' \setminus \mathcal{A}_\mathcal{H}$. Therefore, $(((E_2'' \parallel_L F') / L) \setminus \mathcal{A}_\mathcal{H}, E_1'' \setminus \mathcal{A}_\mathcal{H}) \in \mathcal{B}$ – because $E_1'' \in \mathit{reach}(E_1)$, $E_2'' \in \mathit{reach}(E_2)$, and $E_1'' \setminus \mathcal{A}_\mathcal{H} \approx_\mathrm{p} E_2'' / \mathcal{A}_\mathcal{H}$ as $E_2 \in \mathrm{SBSNNI}_{\approx_\mathrm{p}}$.

As far as probabilities are concerned we observe that from the fact that $E_1' \setminus \mathcal{A}_\mathcal{H} \approx_\mathrm{p} E_2' / \mathcal{A}_\mathcal{H}$ it follows that for all equivalence classes $C \in \mathbb{P}/\mathcal{B}$, $\mathit{prob}(E_1' \setminus \mathcal{A}_\mathcal{H}, C) = \mathit{prob}(E_2' / \mathcal{A}_\mathcal{H}, C)$. If we consider $((E_2' \parallel_L F) / L) \setminus \mathcal{A}_\mathcal{H}$ we observe that since F can only perform high level actions, which are later hidden or restricted, the processes that F reaches by performing a probabilistic transition do not change the equivalence class reached by $E_1 \setminus \mathcal{A}_\mathcal{H}$ and $E_2 / \mathcal{A}_\mathcal{H}$ (see the first part of this case). This implies that $\mathit{prob}(E_1 \setminus \mathcal{A}_\mathcal{H}, C) = \mathit{prob}(((E_2 \parallel_L F) / L) \setminus \mathcal{A}_\mathcal{H}, C)$.

– $\mathrm{SBSNNI}_{\approx_\mathrm{p}} \subset \mathrm{BNDC}_{\approx_\mathrm{p}}$. If $E \in \mathrm{SBSNNI}_{\approx_\mathrm{p}} = \mathrm{P\_BNDC}_{\approx_\mathrm{p}}$, then it immediately follows that $E \in \mathrm{BNDC}_{\approx_\mathrm{p}}$.
– $\mathrm{BNDC}_{\approx_\mathrm{p}} \subset \mathrm{BSNNI}_{\approx_\mathrm{p}}$. If $E \in \mathrm{BNDC}_{\approx_\mathrm{p}}$, i.e., $E \setminus \mathcal{A}_\mathcal{H} \approx_\mathrm{p} (E \parallel_L F) / L) \setminus \mathcal{A}_\mathcal{H}$ for all $F \in \mathbb{P}$ such that every $F' \in \mathit{reach}(F)$ executes only actions in $\mathcal{A}_\mathcal{H}$ 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 $E \setminus \mathcal{A}_\mathcal{H} \approx_\mathrm{p} E / \mathcal{A}_\mathcal{H}$, i.e., $E \in \mathrm{BSNNI}_{\approx_\mathrm{p}}$.

We now prove the same results for the $\approx_\mathrm{pb}$-based properties. Let us examine each relationship separately:

– $\mathrm{SBNDC}_{\approx_\mathrm{pb}} \subset \mathrm{SBSNNI}_{\approx_\mathrm{pb}}$. We need to prove that for a given $E \in \mathbb{P}$, if $E \in \mathrm{SBNDC}$, it follows that for every E' reachable from E, $E' \in \mathrm{BSNNI}_{\approx_\mathrm{pb}}$. Since the processes we are considering are not recursive we can treat them as trees, and hence we can proceed by induction on their depth. In this case we will proceed by induction on the depth of E:
  - If the depth of E is 0 then E has no outgoing transitions and it behaves as $\underline{0}$. This obviously entails that $E \setminus \mathcal{A}_\mathcal{H} \approx_\mathrm{pb} E / \mathcal{A}_\mathcal{H}$.
  - If the depth of E is $n+1$ with $n \in \mathbb{N}$, then take any E' of depth n such that $E \xrightarrow{a}_\mathrm{a} E'$. By hypothesis, $E, E' \in \mathrm{SBNDC}_{\approx_\mathrm{pb}}$ and by induction hypothesis $E' \in \mathrm{SBSNNI}_{\approx_\mathrm{pb}}$. Hence, we just need to prove that $E \setminus \mathcal{A}_\mathcal{H} \approx_\mathrm{pb} E / \mathcal{A}_\mathcal{H}$. There are three cases:

  - If $a \notin \mathcal{A}_{\mathcal{H}}$ then both $E \setminus \mathcal{A}_{\mathcal{H}}$ and $E / \mathcal{A}_{\mathcal{H}}$ can execute a and reach, respectively, $E' \setminus \mathcal{A}_{\mathcal{H}}$ and $E' / \mathcal{A}_{\mathcal{H}}$, which are probabilistic branching bisimilar by induction hypothesis. Thus Definition 5 is respected.
  - If $a \in \mathcal{A}_{\mathcal{H}}$ we have that $E / \mathcal{A}_{\mathcal{H}} \xrightarrow{\tau}_{\mathrm{a}} E' / \mathcal{A}_{\mathcal{H}}$, with $E \xrightarrow{a}_{\mathrm{a}} E'$. By induction hypothesis we have that $E' \setminus \mathcal{A}_{\mathcal{H}} \approx_{\mathrm{pb}} E' / \mathcal{A}_{\mathcal{H}}$, and since $a \in \mathcal{A}_{\mathcal{H}}$ and $E \in \mathrm{SBNDC}_{\approx_{\mathrm{pb}}}$ we have $E \setminus \mathcal{A}_{\mathcal{H}} \approx_{\mathrm{pb}} E' \setminus \mathcal{A}_{\mathcal{H}}$. By transitivity it follows that $E \setminus \mathcal{A}_{\mathcal{H}} \approx_{\mathrm{pb}} E' / \mathcal{A}_{\mathcal{H}}$ which, combined with $E / \mathcal{A}_{\mathcal{H}} \xrightarrow{\tau}_{\mathrm{a}} E' / \mathcal{A}_{\mathcal{H}}$, determines the condition required by Definition 5.
  - If $E / \mathcal{A}_{\mathcal{H}} \xrightarrow{p}_{\mathrm{p}} E' / \mathcal{A}_{\mathcal{H}}$ then $E \setminus \mathcal{A}_{\mathcal{H}}$ can perform the same transition, i.e., $E \setminus \mathcal{A}_{\mathcal{H}} \xrightarrow{p}_{\mathrm{p}} E' \setminus \mathcal{A}_{\mathcal{H}}$, because the hiding and restriction operators do not apply to probabilistic transitions. The processes $E' / \mathcal{A}_{\mathcal{H}}$ and $E' \setminus \mathcal{A}_{\mathcal{H}}$ are probabilistic branching bisimilar because of the induction hypothesis.

– $\mathrm{SBSNNI}_{\approx_{\mathrm{pb}}} = \mathrm{P\_BNDC}_{\approx_{\mathrm{pb}}}$. We first prove that $\mathrm{P\_BNDC}_{\approx_{\mathrm{pb}}} \subseteq \mathrm{SBSNNI}_{\approx_{\mathrm{pb}}}$. If $E \in \mathrm{P\_BNDC}_{\approx_{\mathrm{pb}}}$, then $E' \in \mathrm{BNDC}_{\approx_{\mathrm{pb}}}$ for every $E' \in \mathit{reach}(E)$. Since $\mathrm{BNDC}_{\approx_{\mathrm{pb}}} \subset \mathrm{BSNNI}_{\approx_{\mathrm{pb}}}$ as will be shown in the last case of the proof of this theorem, $E' \in \mathrm{BSNNI}_{\approx_{\mathrm{pb}}}$ for every $E' \in \mathit{reach}(E)$, i.e., $E \in \mathrm{SBSNNI}_{\approx_{\mathrm{pb}}}$.
  The fact that $\mathrm{SBSNNI}_{\approx_{\mathrm{pb}}} \subseteq \mathrm{P\_BNDC}_{\approx_{\mathrm{pb}}}$ will follow by proving that the symmetric relation $\mathcal{B} = \{(E'_1 \setminus \mathcal{A}_{\mathcal{H}}, ((E'_2 \parallel_L F) / L) \setminus \mathcal{A}_{\mathcal{H}}), (((E'_2 \parallel_L F) / L) \setminus \mathcal{A}_{\mathcal{H}}, E'_1 \setminus \mathcal{A}_{\mathcal{H}}) \mid E'_1 \in \mathit{reach}(E_1) \wedge E'_2 \in \mathit{reach}(E_2) \wedge F$ executing only actions in $\mathcal{A}_{\mathcal{H}} \wedge L \subseteq \mathcal{A}_{\mathcal{H}} \wedge E'_1 \setminus \mathcal{A}_{\mathcal{H}} \approx_{\mathrm{pb}} E'_2 / \mathcal{A}_{\mathcal{H}} \wedge E_2 \in \mathrm{SBSNNI}_{\approx_{\mathrm{pb}}}\}$ is a probabilistic branching bisimulation, as can be seen by taking E'_1 identical to E'_2 and both reachable from $E \in \mathrm{SBSNNI}_{\approx_{\mathrm{pb}}}$. Assuming that $E'_1 \setminus \mathcal{A}_{\mathcal{H}}$ and $((E'_2 \parallel_L F) / L) \setminus \mathcal{A}_{\mathcal{H}}$ are related by $\mathcal{B}$ – so that $E'_1 \setminus \mathcal{A}_{\mathcal{H}} \approx_{\mathrm{pb}} E'_2 / \mathcal{A}_{\mathcal{H}}$ – there are six cases:
  - If $E'_1 \setminus \mathcal{A}_{\mathcal{H}} \xrightarrow{l}_{\mathrm{p}} E''_1 \setminus \mathcal{A}_{\mathcal{H}}$, we observe that from $E'_2 \in \mathit{reach}(E_2)$ and $E_2 \in \mathrm{SBSNNI}_{\approx_{\mathrm{p}}}$ it follows that $E'_2 \setminus \mathcal{A}_{\mathcal{H}} \approx_{\mathrm{pb}} E'_2 / \mathcal{A}_{\mathcal{H}}$, so that $E'_1 \setminus \mathcal{A}_{\mathcal{H}} \approx_{\mathrm{pb}} E'_2 / \mathcal{A}_{\mathcal{H}} \approx_{\mathrm{pb}} E'_2 \setminus \mathcal{A}_{\mathcal{H}}$, i.e., $E'_1 \setminus \mathcal{A}_{\mathcal{H}} \approx_{\mathrm{pb}} E'_2 \setminus \mathcal{A}_{\mathcal{H}}$. As a consequence, since $l \neq \tau$ there exist $\bar{E}'_2$ and E''_2 such that $E'_2 \setminus \mathcal{A}_{\mathcal{H}} \Longrightarrow \bar{E}'_2 \setminus \mathcal{A}_{\mathcal{H}} \xrightarrow{l}_{\mathrm{a}} E''_2 \setminus \mathcal{A}_{\mathcal{H}}$ with $E'_1 \setminus \mathcal{A}_{\mathcal{H}} \approx_{\mathrm{pb}} \bar{E}'_2 \setminus \mathcal{A}_{\mathcal{H}}$ and $E''_1 \setminus \mathcal{A}_{\mathcal{H}} \approx_{\mathrm{pb}} E''_2 \setminus \mathcal{A}_{\mathcal{H}}$. Therefore, $((E'_2 \parallel_L F) / L) \setminus \mathcal{A}_{\mathcal{H}} \Longrightarrow ((\bar{E}'_2 \parallel_L F) / L) \setminus \mathcal{A}_{\mathcal{H}} \xrightarrow{l}_{\mathrm{a}} ((E''_2 \parallel_L F) / L) \setminus \mathcal{A}_{\mathcal{H}}$ 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 $E'_1 \setminus \mathcal{A}_{\mathcal{H}} \approx_{\mathrm{pb}} \bar{E}'_2 / \mathcal{A}_{\mathcal{H}}$ as $E_2 \in \mathrm{SBSNNI}_{\approx_{\mathrm{pb}}}$ – 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 $E''_1 \setminus \mathcal{A}_{\mathcal{H}} \approx_{\mathrm{pb}} E''_2 / \mathcal{A}_{\mathcal{H}}$ as $E_2 \in \mathrm{SBSNNI}_{\approx_{\mathrm{pb}}}$.
  - 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 $(E''_1 \setminus \mathcal{A}_{\mathcal{H}}, ((E'_2 \parallel_L F) / L) \setminus \mathcal{A}_{\mathcal{H}}) \in \mathcal{B}$ as $E''_1 \in \mathit{reach}(E_1)$, $E'_2 \in \mathit{reach}(E_2)$, and $E_2 \in \mathrm{SBSNNI}_{\approx_{\mathrm{pb}}}$.
    - If $E''_1 \setminus \mathcal{A}_{\mathcal{H}} \not\approx_{\mathrm{pb}} E'_2 / \mathcal{A}_{\mathcal{H}}$, 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 on the one hand $E'_1 \setminus \mathcal{A}_{\mathcal{H}} \approx_{\mathrm{pb}} E'_2 / \mathcal{A}_{\mathcal{H}} \approx_{\mathrm{pb}} E'_2 \setminus \mathcal{A}_{\mathcal{H}}$, i.e., $E'_1 \setminus \mathcal{A}_{\mathcal{H}} \approx_{\mathrm{pb}} E'_2 \setminus \mathcal{A}_{\mathcal{H}}$, while on the other hand $E''_1 \setminus \mathcal{A}_{\mathcal{H}} \not\approx_{\mathrm{pb}} E'_2 / \mathcal{A}_{\mathcal{H}} \approx_{\mathrm{pb}} E'_2 \setminus \mathcal{A}_{\mathcal{H}}$, i.e., $E''_1 \setminus \mathcal{A}_{\mathcal{H}} \not\approx_{\mathrm{pb}} E'_2 \setminus \mathcal{A}_{\mathcal{H}}$. As a consequence, there exist $\bar{E}'_2$ and E''_2 such that $E'_2 \setminus \mathcal{A}_{\mathcal{H}} \Longrightarrow \bar{E}'_2 \setminus \mathcal{A}_{\mathcal{H}} \xrightarrow{\tau}_{\mathrm{a}} E''_2 \setminus \mathcal{A}_{\mathcal{H}}$ with $E'_1 \setminus \mathcal{A}_{\mathcal{H}} \approx_{\mathrm{pb}}$

$\bar{E}_2' \setminus \mathcal{A}_\mathcal{H}$ and $E_1'' \setminus \mathcal{A}_\mathcal{H} \approx_{\rm pb} E_2'' \setminus \mathcal{A}_\mathcal{H}$. Therefore, $((E_2' \parallel_L F) / L) \setminus \mathcal{A}_\mathcal{H} \Longrightarrow ((\bar{E}_2' \parallel_L F) / L) \setminus \mathcal{A}_\mathcal{H} \xrightarrow{\tau}_{\rm a} ((E_2'' \parallel_L F) / L) \setminus \mathcal{A}_\mathcal{H}$ 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 $E_2 \in {\rm SBSNNI}_{\approx_{\rm pb}}$.

- If $((E_2' \parallel_L F) / L) \setminus \mathcal{A}_\mathcal{H} \xrightarrow{l}_{\rm a} ((E_2'' \parallel_L F) / L) \setminus \mathcal{A}_\mathcal{H}$ because $E_2' \xrightarrow{l}_{\rm a} E_2''$ so that $E_2' \setminus \mathcal{A}_\mathcal{H} \xrightarrow{l}_{\rm a} E_2'' \setminus \mathcal{A}_\mathcal{H}$, 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 $E_2' \setminus \mathcal{A}_\mathcal{H} \approx_{\rm pb} E_2' / \mathcal{A}_\mathcal{H} \approx_{\rm pb} E_1' \setminus \mathcal{A}_\mathcal{H}$, i.e., $E_2' \setminus \mathcal{A}_\mathcal{H} \approx_{\rm pb} E_1' \setminus \mathcal{A}_\mathcal{H}$. As a consequence, since $l \neq \tau$ there exist $\bar{E}_1'$ and E_1'' such that $E_1' \setminus \mathcal{A}_\mathcal{H} \Longrightarrow \bar{E}_1' \setminus \mathcal{A}_\mathcal{H} \xrightarrow{l}_{\rm a} E_1'' \setminus \mathcal{A}_\mathcal{H}$ with $E_2' \setminus \mathcal{A}_\mathcal{H} \approx_{\rm pb} \bar{E}_1' \setminus \mathcal{A}_\mathcal{H}$ and $E_2'' \setminus \mathcal{A}_\mathcal{H} \approx_{\rm pb} E_1'' \setminus \mathcal{A}_\mathcal{H}$. Therefore, $(((E_2' \parallel_L F) / L) \setminus \mathcal{A}_\mathcal{H}, \bar{E}_1' \setminus \mathcal{A}_\mathcal{H}) \in \mathcal{B}$ – because $\bar{E}_1' \in \mathit{reach}(E_1)$, $E_2' \in \mathit{reach}(E_2)$, and $\bar{E}_1' \setminus \mathcal{A}_\mathcal{H} \approx_{\rm pb} E_2' / \mathcal{A}_\mathcal{H}$ as $E_2 \in {\rm SBSNNI}_{\approx_{\rm pb}}$ – 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 $E_1'' \setminus \mathcal{A}_\mathcal{H} \approx_{\rm pb} E_2'' / \mathcal{A}_\mathcal{H}$ as $E_2 \in {\rm SBSNNI}_{\approx_{\rm pb}}$.
- If $((E_2' \parallel_L F) / L) \setminus \mathcal{A}_\mathcal{H} \xrightarrow{\tau}_{\rm a} ((E_2'' \parallel_L F) / L) \setminus \mathcal{A}_\mathcal{H}$ because $E_2' \xrightarrow{\tau}_{\rm a} E_2''$ so that $E_2' \setminus \mathcal{A}_\mathcal{H} \xrightarrow{\tau}_{\rm a} E_2'' \setminus \mathcal{A}_\mathcal{H}$, 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 $E_2' \setminus \mathcal{A}_\mathcal{H} \approx_{\rm pb} E_2' / \mathcal{A}_\mathcal{H} \approx_{\rm pb} E_1' \setminus \mathcal{A}_\mathcal{H}$, i.e., $E_2' \setminus \mathcal{A}_\mathcal{H} \approx_{\rm pb} E_1' \setminus \mathcal{A}_\mathcal{H}$. There are two subcases:
  - If $E_2'' \setminus \mathcal{A}_\mathcal{H} \approx_{\rm pb} E_1' \setminus \mathcal{A}_\mathcal{H}$, then $(((E_2'' \parallel_L F) / L) \setminus \mathcal{A}_\mathcal{H}, E_1' \setminus \mathcal{A}_\mathcal{H}) \in \mathcal{B}$ because $E_1' \in \mathit{reach}(E_1)$, $E_2'' \in \mathit{reach}(E_2)$, and $E_1' \setminus \mathcal{A}_\mathcal{H} \approx_{\rm pb} E_2'' / \mathcal{A}_\mathcal{H}$ as $E_2 \in {\rm SBSNNI}_{\approx_{\rm pb}}$.
  - If $E_2'' \setminus \mathcal{A}_\mathcal{H} \not\approx_{\rm pb} E_1' \setminus \mathcal{A}_\mathcal{H}$, then there exist $\bar{E}_1'$ and E_1'' such that $E_1' \setminus \mathcal{A}_\mathcal{H} \Longrightarrow \bar{E}_1' \setminus \mathcal{A}_\mathcal{H} \xrightarrow{\tau}_{\rm a} E_1'' \setminus \mathcal{A}_\mathcal{H}$ with $E_2' \setminus \mathcal{A}_\mathcal{H} \approx_{\rm pb} \bar{E}_1' \setminus \mathcal{A}_\mathcal{H}$ and $E_2'' \setminus \mathcal{A}_\mathcal{H} \approx_{\rm pb} E_1'' \setminus \mathcal{A}_\mathcal{H}$. Therefore, $(((E_2' \parallel_L F) / L) \setminus \mathcal{A}_\mathcal{H}, \bar{E}_1' \setminus \mathcal{A}_\mathcal{H}) \in \mathcal{B}$ – because $\bar{E}_1' \in \mathit{reach}(E_1)$, $E_2' \in \mathit{reach}(E_2)$, and $\bar{E}_1' \setminus \mathcal{A}_\mathcal{H} \approx_{\rm pb} E_2' / \mathcal{A}_\mathcal{H}$ as $E_2 \in {\rm SBSNNI}_{\approx_{\rm pb}}$ – 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 $E_1'' \setminus \mathcal{A}_\mathcal{H} \approx_{\rm pb} E_2'' / \mathcal{A}_\mathcal{H}$ as $E_2 \in {\rm SBSNNI}_{\approx_{\rm pb}}$.
- If $((E_2' \parallel_L F) / L) \setminus \mathcal{A}_\mathcal{H} \xrightarrow{\tau}_{\rm a} ((E_2' \parallel_L F') / L) \setminus \mathcal{A}_\mathcal{H}$ because $F \xrightarrow{\tau}_{\rm a} F'$, then trivially $(((E_2' \parallel_L F') / L) \setminus \mathcal{A}_\mathcal{H}, E_1' \setminus \mathcal{A}_\mathcal{H}) \in \mathcal{B}$.
- If $((E_2' \parallel_L F) / L) \setminus \mathcal{A}_\mathcal{H} \xrightarrow{\tau}_{\rm a} ((E_2'' \parallel_L F' / L) \setminus \mathcal{A}_\mathcal{H})$ because $E_2' \xrightarrow{h}_{\rm a} E_2''$ – so that $E_2' / \mathcal{A}_\mathcal{H} \xrightarrow{\tau}_{\rm a} E_2'' / \mathcal{A}_\mathcal{H}$ – and $F \xrightarrow{h}_{\rm a} F'$, we observe that from $E_2', E_2'' \in \mathit{reach}(E_2)$ and $E_2 \in {\rm SBSNNI}_{\approx_{\rm pb}}$ it follows that $E_2' \setminus \mathcal{A}_\mathcal{H} \approx_{\rm pb} E_2' / \mathcal{A}_\mathcal{H}$ and $E_2'' \setminus \mathcal{A}_\mathcal{H} \approx_{\rm pb} E_2'' / \mathcal{A}_\mathcal{H}$, so that $E_2' \setminus \mathcal{A}_\mathcal{H} \xrightarrow{\tau}_{\rm a} E_2'' \setminus \mathcal{A}_\mathcal{H}$ and $E_2' \setminus \mathcal{A}_\mathcal{H} \approx_{\rm pb} E_2' / \mathcal{A}_\mathcal{H} \approx_{\rm pb} E_1' \setminus \mathcal{A}_\mathcal{H}$, i.e., $E_2' \setminus \mathcal{A}_\mathcal{H} \approx_{\rm pb} E_1' \setminus \mathcal{A}_\mathcal{H}$. There are two subcases:
  - If $E_2'' \setminus \mathcal{A}_\mathcal{H} \approx_{\rm pb} E_1' \setminus \mathcal{A}_\mathcal{H}$, then $(((E_2'' \parallel_L F') / L) \setminus \mathcal{A}_\mathcal{H}, E_1' \setminus \mathcal{A}_\mathcal{H}) \in \mathcal{B}$ because $E_1' \in \mathit{reach}(E_1)$, $E_2'' \in \mathit{reach}(E_2)$, and $E_1' \setminus \mathcal{A}_\mathcal{H} \approx_{\rm pb} E_2'' / \mathcal{A}_\mathcal{H}$ as $E_2 \in {\rm SBSNNI}_{\approx_{\rm pb}}$.
  - If $E_2'' \setminus \mathcal{A}_\mathcal{H} \not\approx_{\rm pb} E_1' \setminus \mathcal{A}_\mathcal{H}$, then there exist $\bar{E}_1'$ and E_1'' such that $E_1' \setminus \mathcal{A}_\mathcal{H} \Longrightarrow \bar{E}_1' \setminus \mathcal{A}_\mathcal{H} \xrightarrow{\tau}_{\rm a} E_1'' \setminus \mathcal{A}_\mathcal{H}$ with $E_2' \setminus \mathcal{A}_\mathcal{H} \approx_{\rm pb} \bar{E}_1' \setminus \mathcal{A}_\mathcal{H}$ and

$E_2'' \setminus \mathcal{A}_{\mathcal{H}} \approx_{\rm pb} E_1'' \setminus \mathcal{A}_{\mathcal{H}}$. Therefore, $(((E_2' \parallel_L F) / L) \setminus \mathcal{A}_{\mathcal{H}}, \bar{E}_1' \setminus \mathcal{A}_{\mathcal{H}}) \in \mathcal{B}$ – because $\bar{E}_1' \in \mathit{reach}(E_1)$, $E_2' \in \mathit{reach}(E_2)$, and $\bar{E}_1' \setminus \mathcal{A}_{\mathcal{H}} \approx_{\rm pb} E_2' / \mathcal{A}_{\mathcal{H}}$ as $E_2 \in {\rm SBSNNI}_{\approx_{\rm pb}}$ – 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 $E_1'' \setminus \mathcal{A}_{\mathcal{H}} \approx_{\rm pb} E_2'' / \mathcal{A}_{\mathcal{H}}$ as $E_2 \in {\rm SBSNNI}_{\approx_{\rm pb}}$.

As far as probabilities are concerned we observe that from the fact that $E_1' \setminus \mathcal{A}_{\mathcal{H}} \approx_{\rm p} E_2' / \mathcal{A}_{\mathcal{H}}$ it follows that for all equivalence classes $C \in \mathbb{P}/\mathcal{B}$, $\mathit{prob}(E_1' \setminus \mathcal{A}_{\mathcal{H}}, C) = \mathit{prob}(E_2' / \mathcal{A}_{\mathcal{H}}, C)$. If we consider $((E_2 \parallel_L F') / L) \setminus \mathcal{A}_{\mathcal{H}}$ we observe that since F' can only perform high level actions, which are later hidden or restricted, the processes that F' reaches by performing a probabilistic transition do not change the the equivalence class reached by $E_1 \setminus \mathcal{A}_{\mathcal{H}}$ and $E_2 / \mathcal{A}_{\mathcal{H}}$ (see the first part of this case). This implies that $\mathit{prob}(E_1 \setminus \mathcal{A}_{\mathcal{H}}, C) = \mathit{prob}(((E_2 \parallel_L F) / L) \setminus \mathcal{A}_{\mathcal{H}}, C)$.

- ${\rm SBSNNI}_{\approx_{\rm pb}} \subset {\rm BNDC}_{\approx_{\rm pb}}$. If $E \in {\rm SBSNNI}_{\approx_{\rm pb}} = {\rm P\_BNDC}_{\approx_{\rm pb}}$, then it immediately follows that $E \in {\rm BNDC}_{\approx_{\rm pb}}$.
- ${\rm BNDC}_{\approx_{\rm pb}} \subset {\rm BSNNI}_{\approx_{\rm pb}}$. If $E \in {\rm BNDC}_{\approx_{\rm pb}}$, i.e., $E \setminus \mathcal{A}_{\mathcal{H}} \approx_{\rm pb} (E \parallel_L F) / L) \setminus \mathcal{A}_{\mathcal{H}}$ for all $F \in \mathbb{P}$ such that every $F' \in \mathit{reach}(F)$ executes only actions in $\mathcal{A}_{\mathcal{H}}$ 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 $E \setminus \mathcal{A}_{\mathcal{H}} \approx_{\rm pb} E / \mathcal{A}_{\mathcal{H}}$, i.e., $E \in {\rm BSNNI}_{\approx_{\rm pb}}$. ■

Proof of Theorem 5 Let F be $E_1 + h\,.\,[1]E_2$:

1. Let $\mathcal{B}$ be a weak probabilistic bisimulation witnessing $E_1 \approx_{\rm p} E_2$. Then $F \in {\rm BSNNI}_{\approx_{\rm p}}$ because the symmetric relation $\mathcal{B}' = \mathcal{B} \cup \{(F \setminus \mathcal{A}_{\mathcal{H}}, F / \mathcal{A}_{\mathcal{H}}), (F / \mathcal{A}_{\mathcal{H}}, F \setminus \mathcal{A}_{\mathcal{H}})\}$ turns out to be a weak probabilistic bisimulation too. The only interesting case is the one where $F / \mathcal{A}_{\mathcal{H}}$, which is isomorphic to $E_1 + \tau\,.\,[1]E_2$, performs a τ-action toward $[1]E_2 / \mathcal{A}_{\mathcal{H}}$, which is isomorphic to $[1]E_2$. In that case $F \setminus \mathcal{A}_{\mathcal{H}}$, which is isomorphic to E_1, can respond by staying idle, because from $(E_2, E_1) \in \mathcal{B}$ it follows that $([1]E_2, E_1) \in \mathcal{B}$, and hence $([1]E_2, E_1) \in \mathcal{B}'$.
   On the other hand, $F \notin {\rm BSNNI}_{\approx_{\rm pb}}$ because $E_2 \not\approx_{\rm pb} E_1$ in the same situation as before.
2. Since $F \in {\rm BSNNI}_{\approx_{\rm p}}$ and no high-level actions occur in every process reachable from F, it holds that $F \in {\rm SBSNNI}_{\approx_{\rm p}}$ and hence $F \in {\rm BNDC}_{\approx_{\rm p}}$ by virtue of Theorem 3.
   On the other hand, from $F \notin {\rm BSNNI}_{\approx_{\rm pb}}$ it follows that $F \notin {\rm BNDC}_{\approx_{\rm pb}}$ by virtue of Theorem 3.
3. We already know from the previous case that $F \in {\rm SBSNNI}_{\approx_{\rm p}}$.
   On the other hand, from $F \notin {\rm BSNNI}_{\approx_{\rm pb}}$ it follows that $F \notin {\rm SBSNNI}_{\approx_{\rm pb}}$ by virtue of Theorem 3.
4. A straightforward consequence of ${\rm P\_BNDC}_{\approx_{\rm p}} = {\rm SBSNNI}_{\approx_{\rm p}}$ (Theorem 3) and ${\rm P\_BNDC}_{\approx_{\rm pb}} = {\rm SBSNNI}_{\approx_{\rm pb}}$ (Theorem 3).

5. Since the only high-level action occurring in F is h, in the proof of $F \in \mathrm{SBNDC}_{\approx_{\mathrm{p}}}$ the only interesting case is the transition $F \xrightarrow{h}_{\mathrm{a}} [1]E_2$, for which it holds that $F \setminus \mathcal{A}_{\mathcal{H}} \approx_{\mathrm{p}} E_2 \setminus \mathcal{A}_{\mathcal{H}}$ because the former is isomorphic to E_1, the latter is isomorphic to E_2, and $E_1 \approx_{\mathrm{p}} E_2$.
On the other hand, $F \notin \mathrm{SBNDC}_{\approx_{\mathrm{pb}}}$ because $E_1 \not\approx_{\mathrm{pb}} E_2$ in the same situation as before. ■

Proof of Lemma 2. Given $s_1, s_2 \in \mathcal{S}$ with $s_1 \approx_{\mathrm{pbf}} s_2$, consider the reflexive and symmetric relation $\mathcal{B} = \approx_{\mathrm{pbf}} \cup \{(\rho_1'', \rho_2''), (\rho_2'', \rho_1'') \in (\mathit{run}(s_1) \times \mathit{run}(s_2)) \cup (\mathit{run}(s_2) \times \mathit{run}(s_1)) \mid \mathit{last}(\rho_1'') \in \mathcal{S}_{\mathtt{n}} \wedge \mathit{last}(\rho_2'') \in \mathcal{S}_{\mathtt{n}} \wedge \exists \rho_1' \in \mathit{run}(s_1), \rho_2' \in \mathit{run}(s_2). \rho_1' \Longrightarrow \rho_1'' \wedge \rho_2' \Longrightarrow \rho_2'' \wedge \rho_1' \approx_{\mathrm{pbf}} \rho_2'' \wedge \rho_1'' \approx_{\mathrm{pbf}} \rho_2'\}$. The result will follow by proving that $\mathcal{B}$ is a weak probabilistic back-and-forth bisimulation, because this implies that $\rho_1'' \approx_{\mathrm{pbf}} \rho_2''$ for every additional pair – i.e., $\mathcal{B}$ satisfies the cross property – as well as $\mathcal{B} = \approx_{\mathrm{pbf}}$ – hence $\approx_{\mathrm{pbf}}$ satisfies the cross property too.
Let $(\rho_1'', \rho_2'') \in \mathcal{B} \setminus \approx_{\mathrm{pbf}}$ to avoid trivial cases. Then there exist $\rho_1' \in \mathit{run}(s_1)$ and $\rho_2' \in \mathit{run}(s_2)$ such that $\rho_1' \Longrightarrow \rho_1''$, $\rho_2' \Longrightarrow \rho_2''$, $\rho_1' \approx_{\mathrm{pbf}} \rho_2''$, and $\rho_1'' \approx_{\mathrm{pbf}} \rho_2'$. For action transitions we examine the forward and backward directions separately:

- In the forward case, assume that $\rho_1'' \xrightarrow{a}_{\mathrm{a}} \rho_1'''$, from which it follows that $\rho_1' \Longrightarrow \rho_1'' \xrightarrow{a}_{\mathrm{a}} \rho_1'''$. Since $\rho_1' \approx_{\mathrm{pbf}} \rho_2''$, we obtain $\rho_2'' \Longrightarrow \xrightarrow{a}_{\mathrm{a}} \Longrightarrow \rho_2'''$, or $\rho_2'' \Longrightarrow \rho_2'''$ when $a = \tau$, with $\rho_1''' \approx_{\mathrm{pbf}} \rho_2'''$ and hence $(\rho_1''', \rho_2''') \in \mathcal{B}$. Starting from $\rho_2'' \xrightarrow{a}_{\mathrm{a}} \rho_2'''$ one exploits $\rho_2' \Longrightarrow \rho_2''$ and $\rho_1' \approx_{\mathrm{pbf}} \rho_2'$ instead.
- In the backward case, assume that $\rho_1''' \xrightarrow{a}_{\mathrm{a}} \rho_1''$. Since $\rho_1'' \approx_{\mathrm{pbf}} \rho_2'$, we obtain $\rho_2''' \Longrightarrow \xrightarrow{a}_{\mathrm{a}} \Longrightarrow \rho_2'$, so that $\rho_2''' \Longrightarrow \xrightarrow{a}_{\mathrm{a}} \Longrightarrow \rho_2''$, or $\rho_2''' \Longrightarrow \rho_2'$ when $a = \tau$, so that $\rho_2''' \Longrightarrow \rho_2''$, with $\rho_1''' \approx_{\mathrm{pbf}} \rho_2'''$ and hence $(\rho_1''', \rho_2''') \in \mathcal{B}$. Starting from $\rho_2''' \xrightarrow{a}_{\mathrm{a}} \rho_2''$ one exploits $\rho_1' \approx_{\mathrm{pbf}} \rho_2''$ and $\rho_1' \Longrightarrow \rho_1''$ instead.

As for probabilities, since $\mathit{last}(\rho_1'') \in \mathcal{S}_{\mathtt{n}}$ and $\mathit{last}(\rho_2'') \in \mathcal{S}_{\mathtt{n}}$, we have that $\mathit{prob}(\rho_1'', \bar{C}) = 1 = \mathit{prob}(\rho_2'', \bar{C})$ if $\bar{C}$ is the equivalence class containing ρ_1'' and ρ_2'', while $\mathit{prob}(\rho_1'', C) = 0 = \mathit{prob}(\rho_2'', C)$ for any other $C \in \mathcal{U}/\mathcal{B}$. ■

Proof of Theorem 6. The proof is divided into two parts:

- Suppose that $s_1 \approx_{\mathrm{pbf}} s_2$ 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 $\approx_{\mathrm{pbf}}$-equivalent runs in $\mathit{run}(s_1) \cup \mathit{run}(s_2)$, so that Lemma 2 is applicable to $\mathcal{B}$. We show that $\mathcal{B}' = \{(\mathit{last}(\rho_1), \mathit{last}(\rho_2)) \mid (\rho_1, \rho_2) \in \mathcal{B}\}$ is a probabilistic branching bisimulation over $\mathcal{S}$, from which $s_1 \approx_{\mathrm{pb}} s_2$ will follow.
  Given $(\mathit{last}(\rho_1), \mathit{last}(\rho_2)) \in \mathcal{B}'$, by definition of $\mathcal{B}'$ we have that $(\rho_1, \rho_2) \in \mathcal{B}$. Let $r_k = \mathit{last}(\rho_k)$ for $k \in \{1, 2\}$, so that $(r_1, r_2) \in \mathcal{B}'$. Suppose that $r_1 \xrightarrow{a}_{\mathrm{a}} r_1'$, i.e., $\rho_1 \xrightarrow{a}_{\mathrm{a}} \rho_1'$ where $\mathit{last}(\rho_1') = r_1'$. There are two cases:
  - If $a = \tau$, then $\rho_2 \Longrightarrow \rho_2'$ with $(\rho_1', \rho_2') \in \mathcal{B}$. This means that there is a sequence of $n \geq 0$ transitions of the form $\rho_{2,i} \xrightarrow{\tau}_{\mathrm{a}} \rho_{2,i+1}$ or $\rho_{2,i} \xrightarrow{p_i}_{\mathrm{p}} \rho_{2,i+1}$ 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

$(\rho'_1, \rho_{2,n}) \in \mathcal{B}$.
If $n = 0$ then ρ'_2 is ρ_2 and we are done because $(\rho'_1, \rho_2) \in \mathcal{B}$ and hence $r_2 \Longrightarrow r_2 \xrightarrow{\hat{\tau}}_{\mathrm{a}} r_2$ with $(r_1, r_2) \in \mathcal{B}'$ and $(r'_1, r_2) \in \mathcal{B}'$, otherwise within $\rho_{2,n}$ we can go back to $\rho_{2,n-1}$ via $\rho_{2,n-1} \xrightarrow{\tau}_{\mathrm{a}} \rho_{2,n}$ or $\rho_{2,n-1} \xrightarrow{p_{n-1}}_{\mathrm{p}} \rho_{2,n}$. If it is a τ-transition and ρ'_1 can match it by doing nothing, 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 $(\rho'_1, \rho_2) \in \mathcal{B}$ and hence $r_2 \Longrightarrow r_2 \xrightarrow{\hat{\tau}}_{\mathrm{a}} r_2$ with $(r_1, r_2) \in \mathcal{B}'$ and $(r'_1, r_2) \in \mathcal{B}'$, otherwise we can go back to $\rho_{2,n-2}$ via $\rho_{2,n-2} \xrightarrow{\tau}_{\mathtt{a}} \rho_{2,n-1}$ or $\rho_{2,n-2} \xrightarrow{p_{n-2}}_{\mathrm{p}} \rho_{2,n-1}$. By repeating this procedure, either we get to $(\rho'_1, \rho_{2,0}) \in \mathcal{B}$ and we are done because $(\rho'_1, \rho_2) \in \mathcal{B}$ and hence $r_2 \Longrightarrow r_2 \xrightarrow{\hat{\tau}}_{\mathrm{a}} r_2$ with $(r_1, r_2) \in \mathcal{B}'$ and $(r'_1, r_2) \in \mathcal{B}'$, or for some $0 < m \leq n$ such that $(\rho'_1, \rho_{2,m}) \in \mathcal{B}$ we have that the incoming transition $\rho_{2,m-1} \xrightarrow{\tau}_{\mathrm{a}} \rho_{2,m}$ is matched by $\bar{\rho}_1 \Longrightarrow \rho_1 \xrightarrow{\tau}_{\mathrm{a}} \rho'_1$ with $(\bar{\rho}_1, \rho_{2,m-1}) \in \mathcal{B}$.
In the latter case, since $\mathit{last}(\rho_1) \in \mathcal{S}_{\mathtt{n}}$, $\mathit{last}(\rho_{2,m-1}) \in \mathcal{S}_{\mathtt{n}}$, $\bar{\rho}_1 \Longrightarrow \rho_1$, $\rho_2 \Longrightarrow \rho_{2,m-1}$, $(\bar{\rho}_1, \rho_{2,m-1}) \in \mathcal{B}$, and $(\rho_1, \rho_2) \in \mathcal{B}$, from Lemma 2 it follows that $(\rho_1, \rho_{2,m-1}) \in \mathcal{B}$. In conclusion $\rho_2 \Longrightarrow \rho_{2,m-1} \xrightarrow{\tau}_{\mathrm{a}} \rho_{2,m}$ with $(\rho_1, \rho_{2,m-1}) \in \mathcal{B}$ and $(\rho'_1, \rho_{2,m}) \in \mathcal{B}$, so $r_2 \Longrightarrow \mathit{last}(\rho_{2,m-1}) \xrightarrow{\tau}_{\mathrm{a}} \mathit{last}(\rho_{2,m})$ with $(r_1, \mathit{last}(\rho_{2,m-1})) \in \mathcal{B}'$ and $(r'_1, \mathit{last}(\rho_{2,m})) \in \mathcal{B}'$.

- If $a \neq \tau$, then $\rho_2 \Longrightarrow \bar{\rho}_2 \xrightarrow{a}_{\mathrm{a}} \bar{\rho}'_2 \Longrightarrow \rho'_2$ with $(\rho'_1, \rho'_2) \in \mathcal{B}$.
From $\bar{\rho}'_2 \Longrightarrow \rho'_2$ and $(\rho'_1, \rho'_2) \in \mathcal{B}$ it follows that $\bar{\rho}'_1 \Longrightarrow \rho'_1$ with $(\bar{\rho}'_1, \bar{\rho}'_2) \in \mathcal{B}$. Since $\rho_1 \xrightarrow{a}_{\mathrm{a}} \rho'_1$ 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 $\bar{\rho}_2 \xrightarrow{a}_{\mathrm{a}} \bar{\rho}'_2$ and $(\rho'_1, \bar{\rho}'_2) \in \mathcal{B}$ it follows that $\bar{\rho}_1 \Longrightarrow \rho_1 \xrightarrow{a}_{\mathrm{a}} \rho'_1$ with $(\bar{\rho}_1, \bar{\rho}_2) \in \mathcal{B}$. Since $\mathit{last}(\rho_1) \in \mathcal{S}_{\mathtt{n}}$, $\mathit{last}(\bar{\rho}_2) \in \mathcal{S}_{\mathtt{n}}$, $\bar{\rho}_1 \Longrightarrow \rho_1$, $\rho_2 \Longrightarrow \bar{\rho}_2$, $(\bar{\rho}_1, \bar{\rho}_2) \in \mathcal{B}$, and $(\rho_1, \rho_2) \in \mathcal{B}$, from Lemma 2 it follows that $(\rho_1, \bar{\rho}_2) \in \mathcal{B}$. In conclusion $\rho_2 \Longrightarrow \bar{\rho}_2 \xrightarrow{a}_{\mathrm{a}} \bar{\rho}'_2$ with $(\rho_1, \bar{\rho}_2) \in \mathcal{B}$ and $(\rho'_1, \bar{\rho}'_2) \in \mathcal{B}$, hence $r_2 \Longrightarrow \mathit{last}(\bar{\rho}_2) \xrightarrow{a}_{\mathrm{a}} \mathit{last}(\bar{\rho}'_2)$ with $(r_1, \mathit{last}(\bar{\rho}_2)) \in \mathcal{B}'$ and $(r'_1, \mathit{last}(\bar{\rho}'_2)) \in \mathcal{B}'$.

As far as probabilities are concerned, each equivalence class $C' \in \mathcal{S}/\mathcal{B}'$ 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., $C' = \mathit{last}(C)$ for some equivalence class $C \in \mathcal{U}/\mathcal{B}$, provided that function *last* is lifted from runs to sets of runs. Therefore, for all $C' \in \mathcal{S}/\mathcal{B}'$ such that $C' = \mathit{last}(C)$ for some $C \in \mathcal{U}/\mathcal{B}$, $\mathit{prob}(r_1, C') = \mathit{prob}(\rho_1, C) = \mathit{prob}(\rho_2, C) = \mathit{prob}(r_2, C')$.

– Suppose that $s_1 \approx_{\mathrm{pb}} s_2$ 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 $\approx_{\mathrm{pb}}$-equivalent states reachable from s_1 and s_2. We show that $\mathcal{B}' = \{(\rho_1, \rho_2), (\rho_2, \rho_1) \in (\mathit{run}(s_1) \times \mathit{run}(s_2)) \cup (\mathit{run}(s_2) \times \mathit{run}(s_1)) \mid (\mathit{last}(\rho_1), \mathit{last}(\rho_2)) \in \mathcal{B}\}$ is a weak probabilistic back-and-forth bisimulation over $\mathcal{U}$, from which $(s_1, \varepsilon) \approx_{\mathrm{pbf}} (s_2, \varepsilon)$, i.e., $s_1 \approx_{\mathrm{pbf}} s_2$, 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 $(r_1, r_2) \in \mathcal{B}$. For action transitions we examine the forward and backward directions separately:

- If $\rho_1 \xrightarrow{a}_{\mathrm{a}} \rho_1'$, i.e., $r_1 \xrightarrow{a}_{\mathrm{a}} r_1'$ where $r_1' = \mathit{last}(\rho_1')$, then $r_2 \Longrightarrow \bar{r}_2 \xrightarrow{\hat{a}}_{\mathrm{a}} r_2'$ with $(r_1, \bar{r}_2) \in \mathcal{B}$ and $(r_1', r_2') \in \mathcal{B}$, hence $\rho_2 \stackrel{\hat{a}}{\Longrightarrow} \rho_2'$ where $\mathit{last}(\rho_2') = r_2'$ so that $(\rho_1', \rho_2') \in \mathcal{B}'$.
- If $\rho_1' \xrightarrow{a}_{\mathrm{a}} \rho_1$, i.e., $r_1' \xrightarrow{a}_{\mathrm{a}} r_1$ where $r_1' = \mathit{last}(\rho_1')$, there are two cases:
  - If ρ_1' is (s_1, ε) then $r_1' \xrightarrow{a}_{\mathrm{a}} r_1$ is $s_1 \xrightarrow{a}_{\mathrm{a}} r_1$ and $\mathit{last}(\rho_1') = s_1$. Therefore $s_2 \Longrightarrow \bar{r}_2 \xrightarrow{\hat{a}}_{\mathrm{a}} r_2$ with $(s_1, \bar{r}_2) \in \mathcal{B}$ and $(r_1, r_2) \in \mathcal{B}$, hence $\rho_2' \stackrel{\hat{a}}{\Longrightarrow} \rho_2$ 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 s_1 reaches $\mathit{last}(\rho_1')$ with a sequence of moves that are $\mathcal{B}$-compatible with those with which s_2 reaches some $r_2' = \mathit{last}(\rho_2')$ 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 $r_2' \Longrightarrow \bar{r}_2 \xrightarrow{\hat{a}}_{\mathrm{a}} r_2$ with $(r_1', \bar{r}_2) \in \mathcal{B}$ and $(r_1, r_2) \in \mathcal{B}$, hence $\rho_2' \stackrel{\hat{a}}{\Longrightarrow} \rho_2$ with $(\rho_1', \rho_2') \in \mathcal{B}'$.

As far as probabilities are concerned, each equivalence class $C' \in \mathcal{U}/\mathcal{B}'$ is of the form $[\rho]_{\mathcal{B}'} = \{\rho' \mid (\mathit{last}(\rho), \mathit{last}(\rho')) \in \mathcal{B}\} = \{\rho' \mid \mathit{last}(\rho') \in [\mathit{last}(\rho)]_{\mathcal{B}}\}$, i.e., C' corresponds to a precise equivalence class $C_{C'} \in \mathcal{S}/\mathcal{B}$. Therefore, for all $C' \in \mathcal{U}/\mathcal{B}'$, $\mathit{prob}(\rho_1, C') = \mathit{prob}(\mathit{last}(\rho_1), C_{C'}) = \mathit{prob}(\mathit{last}(\rho_2), C_{C'}) = \mathit{prob}(\rho_2, C')$. ■