ULTraS at Work: Compositionality Metaresults for Bisimulation and Trace Semantics

Marco Bernardo
University of Urbino – Italy

© October 2017
Objectives of Behavioral Metamodels

- **Unifying theories**: offering a uniform view of behavioral models that have already appeared in the literature.
- **Reuse facilities**: providing general methodologies, results, and tools that can be applied to a wide range of specific behavioral models.
- Beneficial for the development of *new* theories, models, calculi, or languages accounting for certain behavioral aspects.
- A behavioral metamodel should *reduce* the effort needed for:
  - defining syntax, semantics, and behavioral relations;
  - investigating compositionality properties;
  - studying equational and logical characterizations;
  - designing verification algorithms;
  - ...
Certain frameworks can be viewed to some extent as metamodels:

- SOS rule formats.
- Probabilistic automata.
- Markov automata.
- Weighted automata.
- ...

However, they were not developed with the explicit purpose of paving the way to unifying theories and reuse facilities.

More a matter of ensuring given properties in a general setting or achieving a higher level of expressivity, rather than metamodelling.

Need for something less abstract and easier to use than categorical representations based on coalgebras and bialgebras.
Some Recent Proposals

- The **WLTS** metamodel by Klin (no internal nondeterminism):
  - *commutative monoids* to express and combine weights attached to transition labels under a *weight determinacy condition*;
  - is equipped with a notion of *weighted bisimilarity* and a *rule format* guaranteeing the compositionality of bisimulation semantics.

- The **FuTS** metamodel by De Nicola, Massink, Latella & Loreti:
  - *commutative semirings* for a compositional and compact definition of the *operational semantics*, useful for a precise understanding of similarities and differences among process calculi of the same class;
  - notion of bisimilarity addressed from a *coalgebraic* viewpoint (De Vink).

- The **ULTrAS** metamodel by Bernardo, De Nicola & Loreti:
  - *preordered sets equipped with minimum* to describe reachability;
  - emphasis on bisimulation/testing/trace *metaequivalences*;
  - *rule format* and *coalgebraic* characterization by Miculan & Peressotti;
  - handling of *deterministically timed* models by Bernardo & Tesei.
Definition of the ULTRA$S$ Metamodel

- $(D, \sqsubseteq D, \bot_D)$ is a preordered set equipped with minimum $\bot_D$, where each value represents a degree of one-step reachability and $\bot_D$ denotes unreachability.

- $\Delta \in (S \to D)_{\text{nrefs}}$ is a reachability distribution such that $0 < |\text{supp}(\Delta)| < \omega$ where $\text{supp}(\Delta) = \{s \in S \mid \Delta(s) \neq \bot_D\}$.

- A uniform labeled transition system, ULTRA$S$, on $(D, \sqsubseteq D, \bot_D)$ is a triple $(S, A, \rightarrow)$ where:
  - $S$ is a nonempty, at most countable set of states.
  - $A$ is a countable set of transition-labeling actions.
  - $\rightarrow \subseteq S \times A \times (S \to D)_{\text{nefs}}$ is a transition relation.

- Given a transition $s \xrightarrow{a} \Delta$:
  - Distribution $\Delta$ associates a reachability degree with every $s' \in S$.
  - The set of states reachable via that $a$-transition is $\text{supp}(\Delta)$.
Generality of the ULTRA$S$ Metamodel

- The ULTRA$S$ metamodel is general enough to encompass:
  - Purely nondeterministic models (LTS).
  - Probabilistic models (ADTMC, MDP, PA).
  - Stochastically timed models (ACTMC, CTMDP, MA).
  - Deterministically timed models (TA, PTA).

- We should use:
  - $\langle B, \sqsubseteq_B, \bot \rangle$, where $\bot \sqsubseteq_B \top$, for capturing LTS and TA.
  - $\langle R_{[0,1]}, \leq, 0 \rangle$ for capturing ADTMC, MDP, PA, PTA, MA.
  - $\langle R_{\geq 0}, \leq, 0 \rangle$ for capturing ACTMC and CTMDP.

- Preordered sets with minimum are enough to represent reachability, hence ULTRA$S$ is more parsimonious than WLTS and FU$T$S.
Open Problems in the ULTraS Setting

- Bisimulation/testing/trace metaequivalences on ULTraS capture most behavioral equivalences on specific models, but *not* all of them!
- *New* equivalences arise when instantiating ULTraS to specific models with probabilities and internal nondeterminism:
  - New bisimilarity for PA logically characterized by PML.
  - New trace equivalence for PA compositional w.r.t. parallel operator.
- The widely accepted equivalences for PA are left out:
  - Segala & Lynch bisimilarity.
  - Segala trace-distribution equivalence.
- How to capture both the existing equivalences and the new ones?
- General properties of the ULTraS behavioral metaequivalences?
Summary of Results

- Introduction of *resolutions* in the ULTrAS setting instrumental to the redefinition of bisimulation and trace metaequivalences by distinguishing between *pre-* and *post-*metaequivalences, so to capture *also* the specific equivalences that were left out.
- Elicitation of a *semiring structure* as in the FuTS setting, thereby reconciling the two metamodels (+ reachability consistency).
- *General congruence results* for bisimulation and trace semantics, which confirm a *duality* with respect to parallel composition that shows up in the presence of internal nondeterminism:
  - for bisimulation, only the post-metaequivalence is always compositional;
  - for trace, only the pre-metaequivalence is always compositional.
A resolution of a state $s$ belonging to an ULTraS $U = (S, A, \rightarrow)$ is the result of a possible way of resolving choices starting from $s$.

As if a deterministic scheduler were applied that, at each step, selects one of the outgoing transitions or no transitions at all.

Tree whose branching points correspond to target distributions of transitions, obtained by unfolding the graph structure of $U$.

Formalized as an acyclic deterministic ULTraS $Z = (Z, A, \rightarrow_Z)$ hence akin to a special case of WLTS.

Defined through locally injective functions as inspired by testing theories for probabilistic and nondeterministic processes.

$Res(s)$ is the set of resolutions of $s$.

$k$-$Res(s)$ is the set of $k$-resolutions of $s$ (for bisimulation semantics).
Formal Definition of Resolution

- Given an ULTRaS $U = (S, A, \rightarrow)$, a **resolution** of $s \in S$ is an ULTRaS $Z = (Z, A, \rightarrow_Z)$, with no cycles and $Z$ disjoint from $S$, for which there exists a state correspondence function $corr_Z : Z \rightarrow S$ such that $s = corr_Z(z_s)$ for some $z_s \in Z$, and for all $z \in Z$:
  - If $z \xrightarrow{a}_Z \Delta$, then $corr_Z(z) \xrightarrow{a} \Delta'$ with $corr_Z$ injective over $supp(\Delta)$ and $\Delta(z') = \Delta'(corr_Z(z'))$ for all $z' \in supp(\Delta)$.
  - State $z$ has at most one outgoing transition.

- In the case of a $k$-resolution for $k \in \mathbb{N}_{\geq 1}$, if $z$ is reachable from $z_s$ with a sequence of less than $k$ transitions, then:
  - $z \notin S$;
  - $z$ cannot be part of a cycle;
  - $z$ has at most one outgoing transition;

otherwise $z$ is equal to $corr_Z(z) \in S$ and has the same outgoing transitions that it has in $U$. 
ULTRA\textsuperscript{S} metaequivalences were parameterized with respect to a measure function expressing degrees of multi-step reachability (for trace and testing semantics), not necessarily taken from \((D, \sqsubseteq, \bot_D)\).

It returns sets of values in the presence of internal nondeterminism, but always returns single values in \(D\) when applied to resolutions!

One preordered set suffices & semiring \((D, \oplus, \otimes, 0_D, 1_D)\) emerges:

- \(\otimes\) is useful for calculating multi-step reachability from values of consecutive single-step reachability along the same trajectory;
- \(\oplus\) is useful for aggregating values of multi-step reachability along different trajectories starting from the same state;

The semiring must be consistent with the notion of reachability:

- \(0_D = \bot_D\);
- \(d_1 \otimes d_2 \neq 0_D\) whenever \(d_1 \neq 0_D \neq d_2\) (consecutive steps cannot yield unreachability);
- characteristic zero: finitely many values \(1_D\) sum up to \(\neq 0_D\) (no \(\mathbb{Z}_n\)).
A measure schema $\mathcal{M}$ for an ULTRAS $\mathcal{U} = (S, A, \rightarrow)$ on a reachability-consistent semiring $(D, \oplus, \otimes, 0_D, 1_D)$ is a set of measure functions $\mathcal{M}_Z : Z \times A^* \times 2^Z \rightarrow D$, one for each $Z = (Z, A, \rightarrow_Z) \in \text{Res}(s)$ and $s \in S$:

$$
\mathcal{M}_Z(z, \alpha, Z') = \begin{cases} 
  f_Z(\bigoplus_{z' \in \text{supp}(\Delta)} (\Delta(z') \otimes \mathcal{M}_Z(z', \alpha', Z'))), z, a, \Delta \\
  1_D & \text{if } \alpha = a \alpha' \text{ and } z \xrightarrow{a} z \Delta \\
  1_D & \text{if } \alpha = \epsilon \text{ and } z \in Z' \\
  0_D & \text{otherwise}
\end{cases}
$$

$f_Z : D \times Z \times A \times (Z \rightarrow D)_{\text{nefs}} \rightarrow D$ provides some flexibility.

The definition applies to $Z \in k-\text{Res}(s)$ by restricting to traces $\alpha \in A^*$ such that $|\alpha| \leq k$.

$\mathcal{M}_{\text{nd}}$ denotes the measure schema for $(\mathbb{B}, \lor, \land, \perp, \top)$.

$\mathcal{M}_{\text{pb}}$ denotes the measure schema for $(\mathbb{R}_{\geq 0}, +, \times, 0, 1)$.

$\mathcal{M}_{\text{ete}}$ and $\mathcal{M}_{\text{sbs}}$, developed for the stochastic case, exploit $f_Z$. 
Measure Schemata for the Stochastic Case

- The *end-to-end* option originates a measure schema $\mathcal{M}_{\text{ete}}(t)$ that expresses the probability of performing within $t \in \mathbb{R}_{\geq 0}$ time units a computation from state $z$ labeled with trace $\alpha$ to a state in $Z'$ (convolution of two probability distributions when $\alpha = a \alpha'$ and $t > 0$ built by taking $x \in \mathbb{R}_{[0, t]}$):

  $$\mathcal{M}_{\text{ete}}(z, \alpha, Z')(t) = f_{\text{ete}} \left( \sum_{z' \in \text{supp}(\Delta)} (\Delta(z') \times \mathcal{M}_{\text{ete}}(z', \alpha', Z')(t - x)), z, a, \Delta \right)(t)$$
  $$f_{\text{ete}}(d, z, a, \Delta)(t) = \int_{0}^{t} e^{-E(z) \times x} \times d \, dx$$

- The *step-by-step* option originates a measure schema $\mathcal{M}_{\text{sbs}}(\theta)$ that expresses the prob. of perf. within a sequence of time units $\theta \in (\mathbb{R}_{\geq 0})^*$ a computation from state $z$ labeled with trace $\alpha$ to a state in $Z'$ (product of two probability distributions when $\alpha = a \alpha'$ and $\theta = t \theta'$ with $t > 0$):

  $$\mathcal{M}_{\text{sbs}}(z, \alpha, Z')(\theta) = f_{\text{sbs}} \left( \sum_{z' \in \text{supp}(\Delta)} (\Delta(z') \times \mathcal{M}_{\text{sbs}}(z', \alpha', Z')(\theta')), z, a, \Delta \right)(t)$$
  $$f_{\text{sbs}}(d, z, a, \Delta)(t) = \frac{1 - e^{-E(z) \times t}}{E(z)} \times d$$
Resolution-Based Bisimulation Metaequivalences

- $\sim_{B,\mathcal{M}}^{\text{pre}}$ and $\sim_{B,\mathcal{M}}^{\text{post}}$, defined in the style of Larsen & Skou, differing for the position of the univ. quantif. over sets of equivalence classes.
- Sets avoid generating a pre-metaequivalence that is too coarse (and would ensure transitivity of bisimilarity over continuous state spaces).
- An equivalence relation $\mathcal{B}$ over $S$ is an $\mathcal{M}$-pre-bisimulation iff, whenever $(s_1, s_2) \in \mathcal{B}$, then for all $a \in A$ and $\mathcal{G} \in 2^{S/\mathcal{B}}$ it holds that for each $\mathcal{Z}_1 \in 1-\text{Res}(s_1)$ there exists $\mathcal{Z}_2 \in 1-\text{Res}(s_2)$ such that:
  \[ \mathcal{M}(z_{s_1}, a, \bigcup \mathcal{G}) = \mathcal{M}(z_{s_2}, a, \bigcup \mathcal{G}) \]
- An equivalence relation $\mathcal{B}$ over $S$ is an $\mathcal{M}$-post-bisimulation iff, whenever $(s_1, s_2) \in \mathcal{B}$, then for all $a \in A$ it holds that for each $\mathcal{Z}_1 \in 1-\text{Res}(s_1)$ there is $\mathcal{Z}_2 \in 1-\text{Res}(s_2)$ s.t. f.a. $\mathcal{G} \in 2^{S/\mathcal{B}}$:
  \[ \mathcal{M}(z_{s_1}, a, \bigcup \mathcal{G}) = \mathcal{M}(z_{s_2}, a, \bigcup \mathcal{G}) \]
Resolution-Based Trace Metaequivalences

- \( \sim_{T,M}^{\text{pre}} \) and \( \sim_{T,M}^{\text{post}} \), differing for the position of the univ. quantif. over traces.

- \( s_1 \sim_{T,M}^{\text{pre}} s_2 \) iff
  for all \( \alpha \in A^* \) it holds that
  for each \( Z_1 \in \text{Res}(s_1) \) there exists \( Z_2 \in \text{Res}(s_2) \) such that:
  \[ M(z_{s_1}, \alpha, Z_1) = M(z_{s_2}, \alpha, Z_2) \]

- \( s_1 \sim_{T,M}^{\text{post}} s_2 \) iff
  for each \( Z_1 \in \text{Res}(s_1) \) there exists \( Z_2 \in \text{Res}(s_2) \) such that for all \( \alpha \in A^* \):
  \[ M(z_{s_1}, \alpha, Z_1) = M(z_{s_2}, \alpha, Z_2) \]

- Symmetrically, ... for each \( Z_2 \in \text{Res}(s_2) \) there exists \( Z_1 \in \text{Res}(s_1) \) ...
Discriminating Power of the Metaequivalences

- $\sim_{\text{post} B, M}$ is finer than $\sim_{\text{pre} B, M}$.
- $\sim_{\text{post} B, M}$ and $\sim_{\text{pre} B, M}$ coincide if there is no internal nondeterminism in $U$.
- $\sim_{\text{post} T, M}$ is finer than $\sim_{\text{pre} T, M}$.
- $\sim_{\text{post} T, M}$ and $\sim_{\text{pre} T, M}$ may not coincide even if there is no internal nondet.
- $\sim_{\text{post} B, M}$ is finer than $\sim_{\text{post} T, M}$.
- $\sim_{\text{pre} B, M}$ and $\sim_{\text{pre} T, M}$ are incomparable if there is internal nondeterminism.

Weighted bisimilarity for WLTS coincides with both $\sim_{\text{pre} B, M}$ and $\sim_{\text{post} B, M}$ when the same commutative monoid is considered.

Bisimilarity for FuTS coincides with both $\sim_{\text{pre} B, M}$ and $\sim_{\text{post} B, M}$ when the same semiring is considered (deterministic state spaces).
Strictness of Inclusions and Internal Nondeterminism

- Three B-ULTRAS models and their maximal resolutions:

\[ s_1 \sim_{B, M_{nd}} s_2 \text{ but } s_1 \not\sim_{B, M_{nd}} s_2; \quad s_1 \not\sim_{B, M_{nd}} s_3 \text{ hence } s_1 \not\sim_{B, M_{nd}} s_3 \]

\( s_2 \) and \( s_3 \) have different maximal 1-resolutions.

- \[ s_1 \sim_{T, M_{nd}} s_2 \text{ but } s_1 \not\sim_{T, M_{nd}} s_2; \quad s_1 \sim_{T, M_{nd}} s_3 \text{ but } s_1 \not\sim_{T, M_{nd}} s_3 \]

\( s_1 \) and \( s_3 \) have no internal nondeterminism, \( s_1 \) is not the canonical representation of any LTS.

- \[ s_2 \sim_{T, M_{nd}} s_3 \text{ but } s_2 \not\sim_{B, M_{nd}} s_3. \]
Backward Compatibility of Bisimulation Metaequivalences

- $\sim_{B,M}^{pre}$ instantiates to all the specific bisimulation equivalences captured by the original ULTRAS bisimulation metaequivalence.
- $\sim_{B,M}^{post}$ instantiates to all the specific bisimulation equivalences captured by the original ULTRAS bisimulation metaequivalence if there are no internal nondeterminism & probabilities/stochasticity.
- Common specific bisimulation equivalences for specific models:
  - Milner bisimilarity for LTS.
  - Giacalone, Jou & Smolka bisimilarity for ADTMC.
  - Larsen & Skou bisimilarity for MDP.
  - Hillston bisimilarity for ACTMC.
  - Neuhäuser & Katoen bisimilarity for CTMDP.
- $\sim_{B,M_{pb}}^{post}$ coincides with the strong bisimulation equivalence of Segala & Lynch for PA (not initially captured).
Backward Compatibility of Trace Metaequivalences

- $\sim_{T,M}^{\text{pre}}$ instantiates to all the specific trace equivalences captured by the original ULTRAS trace metaequivalence.
- $\sim_{T,M}^{\text{post}}$ instantiates to all the specific trace equivalences captured by the original ULTRAS trace metaequivalence if there are no internal nondeterminism & probabilities/stochasticity.

Common specific trace equivalences for specific models:

- Brookes, Hoare & Roscoe trace equivalence for LTS.
- Jou & Smolka trace equivalence for ADTMC.
- Seidel trace equivalence for MDP.
- Wolf, Baier & Majster-Cederbaum trace equiv. for ACTMC (ete option).
- Bernardo trace equivalence for ACTMC (sbs option).

- $\sim_{T,M,\text{pb}}^{\text{post}}$ coincides with the strong trace-distribution equivalence of Segala for PA (not initially captured).
Process Algebraic Operators

- Generalized action prefix:
  \[ a \cdot (d_j \triangleright s_j)_{j \in J} \xrightarrow{a} \bigoplus_{j \in J} (d_j \otimes \delta_{s_j}) \]

- Generalized guarded choice:
  \[ \sum_{i \in I} a_i \cdot (d_{i,j} \triangleright s_{i,j})_{j \in J_i} \xrightarrow{a_i} a_k = a_i \bigoplus_{k \in I} \bigoplus_{j \in J_k} (d_{k,j} \otimes \delta_{s_{k,j}}), \quad i \in I \]

- Nondeterministic choice:
  \[
  \begin{align*}
  s_1 & \xrightarrow{a} \Delta \\
  s_1 + s_2 & \xrightarrow{a} \Delta \\
  s_1 + s_2 & \xrightarrow{a} \Delta
  \end{align*}
  \]

- Parallel composition:
  \[
  \begin{align*}
  s_1 & \xrightarrow{a} \Delta_1 \quad a \notin L \\
  s_1 \parallel_L s_2 & \xrightarrow{a} \Delta_1 \otimes \delta_{s_2} \\
  s_2 & \xrightarrow{a} \Delta_2 \quad a \notin L \\
  s_1 \parallel_L s_2 & \xrightarrow{a} \delta_{s_1} \otimes \Delta_2 \\
  s_1 & \xrightarrow{a} \Delta_1 \quad a \in L \\
  s_1 \parallel_L s_2 & \xrightarrow{a} \Delta_1 \otimes \Delta_2 \\
  s_2 & \xrightarrow{a} \Delta_2 \quad a \in L \\
  s_1 \parallel_L s_2 & \xrightarrow{a} \Delta_1 \otimes \Delta_2
  \end{align*}
  \]
Compositionality of Bisimulation Metaequivalences

- $\sim_{\text{pre}}^{B,\mathcal{M}}$ and $\sim_{\text{post}}^{B,\mathcal{M}}$ are both congruences with respect to action prefix, guarded choice, and nondeterministic choice.
- $\sim_{\text{post}}^{B,\mathcal{M}}$ is a congruence with respect to parallel composition too, hence so is $\sim_{\text{pre}}^{B,\mathcal{M}}$ in the absence of internal nondeterminism.
- $\sim_{\text{pre}}^{B,\mathcal{M}_{\text{nd}}}$ is a congruence with respect to parallel composition, because in the only reachability-consistent semiring with $|D| = 2$, which is $(\mathbb{B}, \lor, \land, \bot, \top)$, parallel composition cannot generate values different from $\bot$ and $\top$.
- $\sim_{\text{pre}}^{B,\mathcal{M}}$ is not a congruence with respect to parallel composition when $|D| > 2$ and there is internal nondeterminism.
- $\sim_{\text{post}}^{B,\mathcal{M}}$ is the coarsest congruence contained in $\sim_{\text{pre}}^{B,\mathcal{M}}$ w.r.t. parallel composition in the case of an image-finite ULTRAs on a reachability-consistent field (algebraic and topological properties of vector spaces).
Compositionality of Trace Metaequivalences

- $\sim_{\text{pre}}^{T,M}$ and $\sim_{\text{post}}^{T,M}$ are both congruences with respect to action prefix, guarded choice, and nondeterministic choice.
- $\sim_{\text{pre}}^{T,M}$ is a congruence with respect to parallel composition too, hence so is $\sim_{\text{post}}^{T,M}$ in the absence of internal nondeterminism.
- The proof is based on an alternative characterization of $\sim_{\text{pre}}^{T,M}$, which associates with each state the set of traces it can perform in the various resolutions together with their degree of executability.
- $\sim_{\text{post}}^{T,M}$ is not a congruence with respect to parallel composition when there is internal nondeterminism.
- $\sim_{\text{post}}^{T,M_{\text{nd}}}$ is anyway a congruence with respect to parallel composition if we rule out ULTRAS that are not canonical representations of LTS.
- A coarsest congruence result is impossible.
Summary of Results

- Introduction of resolutions in the ULTrAS setting instrumental to the redefinition of bisimulation and trace metaequivalences by distinguishing between pre- and post-metaequivalences, so to capture also the specific equivalences that were left out.

- Elicitation of a semiring structure as in the FuTS setting, thereby reconciling the two metamodels (+ reachability consistency).

- General congruence results for bisimulation and trace semantics, which confirm a duality with respect to parallel composition that shows up in the presence of internal nondeterminism:
  - for bisimulation, only the post-metaequivalence is always compositional;
  - for trace, only the pre-metaequivalence is always compositional.
Future Work

Still putting ULTraS at work on behavioral metaequivalences:

- Equational characterizations of bisimulation and trace pre-metaequivalences and post-metaequivalences.
- Logical characterizations of bisimulation and trace pre-metaequivalences and post-metaequivalences.
- Metaresults for testing metaequivalences.

Also defining and studying:

- Behavioral metapreorders.
- Weak variants of behavioral metarelations.
- Approximate variants of behavioral metarelations.

On the metamodel side, capturing:

- Specific interleaving models with continuous state spaces.
- Specific truly concurrent models (Petri nets, event structures).