ICTAC 2017

VNU Hanoi, Vietnam 25-27 October 2017

Logical Characterisation of Parameterised Bisimulations

Divyanshu Bagga and S. Arun-Kumar

{divyanshu.bagga, sak}@cse.iitd.ac.in

Department of Computer Science and Engineering

I. I. T. Delhi, Hauz Khas, New Delhi 110 016.

October 29, 2017

Contents

1 **Background** 4

2 **Parameterised HML** 13

3 **Contribution** 20

4 **Distinguishing Formulae** 24

5 **Characteristic Formulae** 28

6 **Conclusions and Future Work** 39

Background

LTS

Definition 1 *A* **Labelled Transition System (LTS)** *is a structure*

$$\mathfrak{L} = \langle \mathcal{P}, \mathcal{O}, \longrightarrow \rangle$$

where

- $\mathcal{P}$ *is a set of* states *or* processes,
- $\mathcal{O}$ *is a set of* observables,
- $\longrightarrow \subseteq \mathcal{P} \times \mathcal{O} \times \mathcal{P}$ *is the* transition relation.

Parameterised Bisimulations

- A small generalisation of the notion of bisimulations on LTSs [1].
- Let $\mathfrak{L}$ be any LTS and $\rho, \sigma \subseteq \mathcal{O} \times \mathcal{O}$. $R \subseteq \mathcal{P} \times \mathcal{P}$ is a (ρ, σ)**-bisimulation** if pRq implies the following conditions for all $a, b \in \mathcal{O}$.

$$p \xrightarrow{a} p' \Rightarrow \exists b, q'[a\rho b \wedge q \xrightarrow{b} q' \wedge p'Rq']$$

$$q \xrightarrow{b} q' \Rightarrow \exists a, p'[a\sigma b \wedge p \xrightarrow{a} p' \wedge p'Rq']$$

- The largest (ρ, σ)-bisimulation (under set containment) is called (ρ, σ)**-bisimilarity** and denoted $\sqsubseteq_{(\rho,\sigma)}$.

What does it generalise?

- **Strong bisimilarity**[8]: $\sim\, = \sqsubseteq_{(\equiv,\equiv)}$
- **Efficiency Preorder**[2]: $\precsim\, = \sqsubseteq_{(\preceq,\preceq)}$
- **Elaboration Preorder**[3]: $\precapprox\, = \sqsubseteq_{(\preceq,\widehat{=})}$
- **Weak bisimilarity**[8]: $\approx\, = \sqsubseteq_{(\widehat{=},\widehat{=})}$

where

$$\begin{aligned}
\equiv &= \text{the identity relation on } Act \text{ or } Act^* \\
\preceq &= \{(\tau^k a \tau^l, \tau^m a \tau^n) \mid k + l \geq m + n, a \in Act\} \\
\widehat{=} &= \{(s, t) \mid \hat{s} = \hat{t}, s, t \in Act^*\}
\end{aligned}$$

Other (Pre-)bisimilarities

- Simulation preorder[8]
- Dynamic and static location pre-bisimilarity[4]
- Bisimulation on speed[7]
- Amortised bisimilarity[5]

may be represented as $\sqsubseteq_{(\rho,\sigma)}$

1. for appropriately chosen ρ and σ
2. after transforming the LTS obtained from the operational semantics.

Some Properties

Many of the nice algebraic properties of bisimularities are induced by the relations ρ and σ. In fact we have [1]

- **Monotonicity.** $(\rho, \sigma) \subseteq (\rho', \sigma') \Rightarrow \sqsubseteq_{(\rho,\sigma)} \subseteq \sqsubseteq_{(\rho',\sigma')}$.
- **Reflexivity.** If ρ, σ are reflexive then $\sqsubseteq_{(\rho,\sigma)}$ is reflexive.
- **Symmetry.**
  1. If ρ is symmetric then $\sqsubseteq_{(\rho,\rho)}$ is symmetric.
  2. For any ρ, $\sqsubseteq_{(\rho,\rho^{-1})}$ is symmetric.
- **Transitivity.** If ρ,σ are transitive then $\sqsubseteq_{(\rho,\sigma)}$ is transitive.

Some Properties (Contd.)

- **Preorders.** $\sqsubseteq_{(\rho,\sigma)}$ is a preorder iff ρ and σ are both preorders.
- **Equivalences.** $\sqsubseteq_{(\rho,\sigma)}$ is an equivalence iff $\sigma = \rho^{-1}$ and ρ (equivalently σ) is a preorder.
- Consequently, $\sqsubseteq_{(\rho,\sigma)}$ is an equivalence if ρ is an equivalence and $\sigma = \rho$.

Logical Characterisations

Definition 2 *A logic $\mathcal{L}$ characterises*

- **preorder** $\sqsubseteq$ *on processes provided* $\mathcal{L}(p) \subseteq \mathcal{L}(q)$ *iff* $p \sqsubseteq q$
- **equivalence** $\simeq$ *on processes provided* $\mathcal{L}(p) = \mathcal{L}(q)$ *iff* $p \simeq q$

Parameterised HML: Syntax

The language $\mathcal{L}_{(\rho,\sigma)}$ is given by the following BNF

$$\varphi, \psi \ := \ \bot \mid \top \mid \langle a \rangle_{\rho} \varphi \mid [a]^{\sigma^{-1}} \varphi \mid \varphi \wedge \psi \mid \varphi \vee \psi$$

where $a \in \mathcal{O}$.

Notice that this is a negation-free logic.

Parameterised HML: Semantics

Definition 3 $p \vDash \varphi$, *iff* $p \in \|\varphi\|^{\mathcal{P}}$ *where*

$$
\begin{array}{rclcrcl}
\|\top\|^{\mathcal{P}} & = & \mathcal{P} & \quad & \|\varphi_1 \vee \varphi_2\|^{\mathcal{P}} & = & \|\varphi_1\|^{\mathcal{P}} \cup \|\varphi_2\|^{\mathcal{P}} \\
\|\bot\|^{\mathcal{P}} & = & \emptyset & \quad & \|\varphi_1 \wedge \varphi_2\|^{\mathcal{P}} & = & \|\varphi_1\|^{\mathcal{P}} \cap \|\varphi_2\|^{\mathcal{P}}
\end{array}
$$

$$
\begin{array}{rcl}
\|\langle a\rangle_{\rho}\varphi\|^{\mathcal{P}} & = & \{p \mid \exists b, p'[a\rho b \wedge p \xrightarrow{b} p' \wedge p' \in \|\varphi\|^{\mathcal{P}}]\} \\
\|[a]^{\sigma^{-1}}\varphi\|^{\mathcal{P}} & = & \{p \mid \forall b, p'[b\sigma a \wedge p \xrightarrow{b} p' \Rightarrow p' \in \|\varphi\|^{\mathcal{P}}]\}
\end{array}
$$

Definition 4

- $\mathcal{L}_{(\rho,\sigma)}(p) = \{\varphi \in \mathcal{L}_{(\rho,\sigma)} \mid p \vDash \varphi\}$ *for* $p \in \mathcal{P}$.
- $p \preceq_{(\rho,\sigma)} q$ *iff* $\mathcal{L}_{(\rho,\sigma)}(p) \subseteq \mathcal{L}_{(\rho,\sigma)}(q)$.

PHML: Characterisation

Proposition 5 *If* ρ, σ *are both transitive, then* $p \sqsubseteq_{(\rho,\sigma)} q$ *implies* $p \preceq_{(\rho,\sigma)} q$.

Proof by induction on the structure of $\varphi \in \mathcal{L}_{(\rho,\sigma)}(p)$

Proposition 6 *If* ρ, σ *are both reflexive then* $\preceq_{(\rho,\sigma)}$ *is a* (ρ, σ)*-bisimulation.*

Proof by contradiction.

Theorem 7 *If* ρ, σ *are both preorders then* $\preceq_{(\rho,\sigma)} = \sqsubseteq_{(\rho,\sigma)}$.

PHML: Equivalences

From the equivalence characterisations we get

Corollary 8 *If* $\sigma = \rho^{-1}$ *and* ρ *(equivalently* σ*) is a preorder, then* $\preceq_{(\rho,\sigma)}$ *is an equivalence.*

Corollary 9 *If* $\sigma = \rho$ *and* ρ *(equivalently* σ*) is symmetric then* $\preceq_{(\rho,\sigma)}$ *is an equivalence.*

PHML: Negation

If

- $\sigma = \rho^{-1}$ and ρ (equivalently σ) is a preorder or
- $\sigma = \rho$ and ρ (equivalently σ) is symmetric

then

1. $[a]^{\sigma^{-1}} = [a]^{\rho}$ and we have a modal logic parameterised on ρ (equivalently σ),
2. negation may be defined; $\neg\langle a\rangle_{\rho}\varphi = [a]^{\rho}\neg\varphi$

Contribution

Contribution of this paper

1. PHML is a logical characterisation of all bisimilarities (preorders and equivalences) for processes expressed in the framework of parameterised bisimulations
2. Conditions required to ensure that distinguishing formulae are always finite
3. Logical characterisation extended with fixed-point operators to derive characteristic formulae

Distinguishing Formulae

Image Finiteness

Definition 10 *An LTS* $\mathfrak{L} = \langle \mathcal{P}, \mathcal{A}ct, \longrightarrow \rangle$ *is* (ρ, σ)*-image-finite iff for any* $p \in \mathcal{P}$ *and* $a \in \mathcal{A}ct$*, the sets,* $\{q \mid p \xrightarrow{b} q \wedge a\rho b\}$ *and* $\{q \mid p \xrightarrow{b} q \wedge b\sigma a\}$*, are finite. An LTS* $\mathfrak{L}$ *is image-finite upto* (ρ, σ)*-bisimilarity if* $\mathfrak{L}_p^\dagger$ *is* (ρ, σ)*-image-finite for every* $p \in \mathcal{P}$*.*

Definition 11

$$\mathfrak{L}_p^\dagger = \langle Reach(p), \mathcal{A}ct, \longrightarrow_p^\dagger \rangle$$

where

$$Reach(p) = \{p\} \cup \bigcup_{p' \in TI(p)} Reach(p')$$

where $TI(p) = \bigcup_{a \in \mathcal{A}ct} [(a\rho\text{-Succ}(p))^{\mathfrak{t}} \cup (\sigma a\text{-Succ}(p))^{\mathfrak{i}}]$

Distinguishing Formulae

Data: $p, q \in \mathfrak{L} = \langle \mathcal{P}, \mathcal{A}ct, \longrightarrow \rangle$

Result: if $p \sqsubseteq_{(\rho,\sigma)} q$ then *ff* else φ s.t. ($p \models \varphi$ and $q \not\models \varphi$) or ($p \not\models \varphi$ and $q \models \varphi$)

$\texttt{DisL}\,(p, q) = (a, p') : \nexists (b, q')[a\rho b \wedge q \xrightarrow{b} q' \wedge p' \sqsubseteq^{i-1}_{(\rho,\sigma)} q']$

$\texttt{DisR}\,(p, q) = (b, q') : \nexists (a, p')[a\sigma b \wedge p \xrightarrow{b} p' \wedge p' \sqsubseteq^{i-1}_{(\rho,\sigma)} q']$

$\texttt{Dis}\,(p, q) = \texttt{DisL}\,(p, q)$ or $\texttt{DisR}\,(p, q)$

$\texttt{GenForm}\,(p, q) =$ **if** $p \sqsubseteq_{(\rho,\sigma)} q$ **then return** *ff*

else switch $\texttt{Dis}\,(p, q)$ **do**

case (a, p'): **return** $\langle a \rangle [\rho] \bigwedge_{\{q' \mid q \xrightarrow{b} q' \wedge a\rho b\}^{\mathtt{t}}} \texttt{GenForm}\,(p', q')$

case (b, q'): **return** $[b]^{\sigma^{-1}} \bigvee_{\{p' \mid p \xrightarrow{a} p' \wedge a\sigma b\}^{\mathtt{i}}} \texttt{GenForm}\,(p', q')$

endsw

Characteristic Formulae

Fixpoint Operators

Definition 12 *The syntax of the logic* $\mathcal{L}^{\mathcal{X}}_{(\rho,\sigma)}$ *is given by the BNF*

$$\varphi, \psi \;:=\; \top \mid \bot \mid X \mid \langle a \rangle_{\rho} \varphi \mid [a]^{\sigma^{-1}} \varphi \mid \varphi \wedge \psi \mid \varphi \vee \psi \mid \nu X.\varphi \mid \mu X.\varphi$$

where $X \in \mathcal{X}$ *ranges over a countable set of variables.*

- Since formulae may have free variables we require a *valuation*

$$\mathcal{V} : \mathcal{X} \longrightarrow 2^{\mathcal{P}}$$

- The semantics $\|.\|^{\mathcal{P}}_{\mathcal{V}}$ is defined relative to the valuation $\mathcal{V}$.
- $cf(\mathcal{L}^{\mathcal{X}}_{(\rho,\sigma)})$ is the set of *closed formulae*.

Semantics of Recursion

$$
\begin{aligned}
\|X\|^{\mathcal{P}}_{\mathcal{V}} &= \mathcal{V}(X)\\
\|\varphi_1 \vee \varphi_2\|^{\mathcal{P}}_{\mathcal{V}} &= \|\varphi_1\|^{\mathcal{P}}_{\mathcal{V}} \cup \|\varphi_1\|^{\mathcal{P}}_{\mathcal{V}}\\
\|\varphi_1 \wedge \varphi_2\|^{\mathcal{P}}_{\mathcal{V}} &= \|\varphi_1\|^{\mathcal{P}}_{\mathcal{V}} \cap \|\varphi_1\|^{\mathcal{P}}_{\mathcal{V}}\\
\|\langle a\rangle[\rho]\varphi\|^{\mathcal{P}}_{\mathcal{V}} &= \{p \mid \exists b, p'[a\rho b \wedge p \xrightarrow{b} p' \wedge p' \in \|\varphi\|^{\mathcal{P}}_{\mathcal{V}}]\}\\
\|[a]^{\sigma^{-1}}\varphi\|^{\mathcal{P}}_{\mathcal{V}} &= \{p \mid \forall b, p'[b\sigma a \wedge p \xrightarrow{b} p' \Rightarrow p' \in \|\varphi\|^{\mathcal{P}}_{\mathcal{V}}]\}\\
\|\nu X.\varphi\|^{\mathcal{P}}_{\mathcal{V}} &= \bigcup\{\mathcal{E} \subseteq \mathcal{P} \mid \mathcal{E} \subseteq \|\varphi\|^{\mathcal{P}}_{\mathcal{V}[\mathcal{E}/X]}\}\\
\|\mu X.\varphi\|^{\mathcal{P}}_{\mathcal{V}} &= \bigcap\{\mathcal{E} \subseteq \mathcal{P} \mid \|\varphi\|^{\mathcal{P}}_{\mathcal{V}[\mathcal{E}/X]} \subseteq \mathcal{E}\}
\end{aligned}
$$

where $\mathcal{V}[\mathcal{E}/X](Y) = \mathcal{V}(Y)$ for all $Y \neq X$ and $\mathcal{V}[\mathcal{E}/X](X) = \mathcal{E}$.

Valuations and Satisfaction

The semantics of any formula depends upon the valuation supplied. Consequently, the satisfaction relation needs to be redefined.

Definition 13

- $p \models_{\mathcal{V}} \varphi$, *iff* $p \in \|\varphi\|^{\mathcal{P}}_{\mathcal{V}}$
- $p \models \varphi$ *iff* $p \in \|\varphi\|^{\mathcal{P}}_{\mathcal{V}}$ *for all valuations* $\mathcal{V}$.

Partial Ordering on Valuations

Definition 14

$$\mathcal{V}_1 \leq \mathcal{V}_2 \Leftrightarrow \forall X \in \mathcal{X}[\mathcal{V}_1(X) \subseteq \mathcal{V}_2(X)]$$

The $\leq$ *ordering yields a complete lattice,* $(\mathcal{X} \rightarrow 2^{\mathcal{P}}, \leq)$*, over valuations.*

Lemma 15 (Monotonicity)

- *If* $\mathcal{V}_1 \leq \mathcal{V}_2$ *then* $\|\varphi\|^{\mathcal{P}}_{\mathcal{V}_1} \subseteq \|\varphi\|^{\mathcal{P}}_{\mathcal{V}_2}$.
- $\mathcal{O}_\varphi(\mathcal{V}) = \mathcal{V}[\|\varphi\|^{\mathcal{P}}_{\mathcal{V}}/X]$*, is monotonic over the complete lattice* $(\mathcal{X} \rightarrow 2^{\mathcal{P}}, \leq)$.

Model Checking Finite State Systems

- To compute $\|\nu X.\varphi\|^{\mathcal{P}}$, apply $\mathcal{O}_\varphi$ repeatedly, starting from $\mathcal{P}$
- To compute $\|\mu X.\varphi\|^{\mathcal{P}}$, apply $\mathcal{O}_\varphi$ repeatedly, starting from $\emptyset$

Theorem 16 *Given a finite $\mathfrak{L}_p^{\dagger}$, for any $\varphi \in cf(\mathcal{L}^{\mathcal{X}}_{(\rho,\sigma)})$, $p \models \varphi$ is decidable.*

Recursion: Logical Characterisation

Under a definition of (ρ, σ)-bisimilarity closure it turns out

Theorem 17 *Given preorders* ρ, σ, $cf(\mathcal{L}^{\mathcal{X}}_{(\rho,\sigma)})$ *is a logical characterisation of* $\sqsubseteq_{(\rho,\sigma)}$ *for all* (ρ, σ)*-image-finite processes, i.e.*

$$p \sqsubseteq_{(\rho,\sigma)} q \textit{ iff } p \preceq_{cf(\mathcal{L}^{\mathcal{X}}_{(\rho,\sigma)})} q$$

Characteristic Formulae

Definition 18 *A closed formula $\varphi_p \in \mathcal{L}^{\mathcal{X}}_{(\rho,\sigma)}$ is characteristic of a process p, if for every $q \in \mathcal{P}$, we have $p \sqsubseteq_{(\rho,\sigma)} q$ iff $q \in \|\varphi_p\|^{\mathcal{P}}$.*

Given a process $p \in \mathcal{P}$, we define an equational system $E^{\mathcal{P}}$ of mutually recursive equations $X_p = \varphi_p$ where $\varphi_p \in \mathcal{L}^{\mathcal{X}}_{(\rho,\sigma)}$ which by standard techniques yields

$$X_p = \Big(\bigwedge_{a,p' : p \xrightarrow{a} p'} \langle a \rangle_{\rho} X_{p'} \Big) \wedge \Big(\bigwedge_{b} [b]^{\sigma^{-1}} \big(\bigvee_{a,p' : a \sigma b \wedge p \xrightarrow{a} p'} X_{p'} \big) \Big)$$

Characterising Characteristic Formulae

Theorem 19 *A process p has a finite characteristic formula in $\mathcal{L}^{\mathcal{X}}_{(\rho,\sigma)}$, if ρ and σ are preorders with finitely many maximal elements and every action being less than some maximal element, and $\mathfrak{L}^{\dagger}_{p}$ is finite with $p_{\mathfrak{L}^{\dagger}_{p}} \sqsupseteq_{(\rho,\sigma)} p_{\mathfrak{L}}$.*

Conclusions and Future Work

Concluding Remarks

- PHML is *some* logic but not necessarily modal unless $\rho = \sigma^{-1}$.
- It is negation-free and deliberately so to retain certain monotonicity properties.
- The notion of logical characterisation of preorders is in principle what was done in [6] for efficiency preorders, but it is more general.

Future Work

- The notion of abstracted LTS (11) could be useful in various kinds of infinite state systems such as timed systems with durations
- Other kinds of abstractions may be used to get over-approximations or under-approximations of bisimilarities *à la* abstract interpretations in the domain of infinitely branching infinite state systems.

References

[1] S. Arun-Kumar. On bisimilarities induced by relations on actions. In *Proceedings 4th IEEE International Conference on Software Engineering and Formal Methods, Pune, India*. IEEE Computer Society Press, 2006.

[2] S. Arun-Kumar and M. Hennessy. An efficiency preorder for processes. *Acta Informatica*, 29:737–760, 1992.

[3] S. Arun-Kumar and V. Natarajan. Conformance: A precongruence close to bisimilarity. In *STRICT, Berlin 1995*, number 526 in Workshops in Computing Series, pages 55–68. Springer-Verlag, 1995.

[4] I. Castellani. Process algebras with localities. In J. Bergstra, A. Ponse, and S. Smolka, editors, *Handbook of Process Algebra*, pages 945–1045. North-Holland, Amsterdam, 2001.

[5] Astrid Kiehn and S. Arun-Kumar. Amortised bisimulations. In *Formal Techniques for Networked and Distributed Systems*, volume 3731, pages 320–334. Lecture Notes in Computer Science, 2005.

[6] Neelesh Korade and S. Arun-Kumar. A logical characterization of efficiency preorders. In *International Colloquium on Theoretical Aspects of Computing*, volume 3407, pages 99–112. Lecture Notes in Computer Science, 2004.

[7] G. Lüttgen and W. Vogler. Bisimulation on speed: a unified approach. In *Proceedings of FOSSACS 2005*, number 3441 in Lecture Notes in Computer Science, pages 79–94. Springer-Verlag, 2005.

[8] R. Milner. *Communication and Concurrency*. Prentice-Hall International, 1989.

Thank You!

Any Questions?