Quantitative Verification

The Good, The Bad and The Ugly

Uli Fahrenberg

LRE & EPITA Rennes, France

68nqrt 4 April 2024

Nice People

Sebastian S. Bauer, Nikola Beneš, Zoltán Ésik, Lisbeth Fajstrup, Eric Goubault, Line Juhl, Jan Křetínský, Kim G. Larsen, Martin Raussen, Georg Struth, Claus Thrane, Louis-Marie Traonouez

Model Checking

model specification

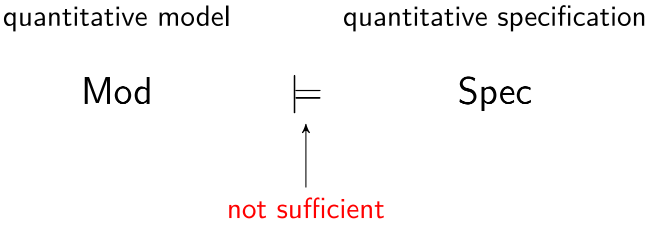
$$\text{Mod} \quad \models \quad \text{Spec}$$

Quantitative Model Checking

quantitative model   quantitative specification

$$\mathsf{Mod} \models \mathsf{Spec}$$

Quantitative Model Checking



quantitative model quantitative specification

$$\mathrm{Mod} \models \mathrm{Spec}$$

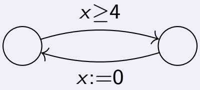
not sufficient

replace by

$$\models_\varepsilon$$

Claus T: Quantitative Quantitative Quantitative Analysis

Quantitative *Models*



Quantitative *Logics*

$$\Pr_{\leq .1}(\Diamond \mathit{error})$$

Quantitative *Verification*

$$[\![\phi]\!](s) = 3.14$$

$$d(s,t) = 42$$

Boolean world	**“Quantification”**
Trace equivalence $\equiv$	Linear distances d_L
Bisimilarity $\sim$	Branching distances d_B
$s \sim t$ implies $s \equiv t$	$d_L(s,t) \leq d_B(s,t)$
$s \models \phi$ or $s \not\models \phi$	$[\![\phi]\!](s)$ is a quantity
$s \sim t$ iff $\forall \phi : s \models \phi \Leftrightarrow t \models \phi$	$d_B(s,t) = \sup_\phi d\big([\![\phi]\!](s), [\![\phi]\!](t)\big)$

Compositional Verification

model		specification
Mod	$\models$	Spec

- $\text{Mod} \models \text{Spec}_1$ & $\text{Spec}_1 \leq \text{Spec}_2 \implies \text{Mod} \models \text{Spec}_2$
- $\text{Mod} \models \text{Spec}_1$ & $\text{Mod} \models \text{Spec}_2 \implies \text{Mod} \models \text{Spec}_1 \wedge \text{Spec}_2$
- $\text{Mod}_1 \models \text{Spec}_1$ & $\text{Mod}_2 \models \text{Spec}_2 \implies \text{Mod}_1 \| \text{Mod}_2 \models \text{Spec}_1 \| \text{Spec}_2$
- $\text{Mod}_1 \models \text{Spec}_1$ & $\text{Mod}_2 \models \text{Spec}/\text{Spec}_1 \implies \text{Mod}_1 \| \text{Mod}_2 \models \text{Spec}$

- bottom-up and top-down

Quantitative Compositional Verification?

quantitative model quantitative specification

$$\mathsf{Mod} \qquad \models_\varepsilon \qquad \mathsf{Spec}$$

- $\mathsf{Mod} \models_\varepsilon \mathsf{Spec}_1$ & $\mathsf{Spec}_1 \le_\varepsilon \mathsf{Spec}_2 \implies \mathsf{Mod} \models_\varepsilon \mathsf{Spec}_2$
- $\mathsf{Mod} \models_\varepsilon \mathsf{Spec}_1$ & $\mathsf{Mod} \models_\varepsilon \mathsf{Spec}_2 \implies \mathsf{Mod} \models_\varepsilon \mathsf{Spec}_1 \wedge \mathsf{Spec}_2$
- $\mathsf{Mod}_1 \models_\varepsilon \mathsf{Spec}_1$ & $\mathsf{Mod}_2 \models_\varepsilon \mathsf{Spec}_2 \implies \mathsf{Mod}_1 \| \mathsf{Mod}_2 \models_\varepsilon \mathsf{Spec}_1 \| \mathsf{Spec}_2$
- $\mathsf{Mod}_1 \models_\varepsilon \mathsf{Spec}_1$ & $\mathsf{Mod}_2 \models_\varepsilon \mathsf{Spec}/\mathsf{Spec}_1 \implies \mathsf{Mod}_1 \| \mathsf{Mod}_2 \models_\varepsilon \mathsf{Spec}$

- surely not the same ε everywhere!?

User Stories

“In your quantitative verification, what type of distances do you use?”

- point-wise	$D(\sigma,\tau) = \sup_i \lvert\sigma_i - \tau_i\rvert$
- accumulating	$D(\sigma,\tau) = \sum_i \lvert\sigma_i - \tau_i\rvert$
- limit-average	$D(\sigma,\tau) = \limsup_N \frac{1}{N}\sum_{i=0}^N \lvert\sigma_i - \tau_i\rvert$
- discounted	$D(\sigma,\tau) = \sum_i \lambda^i \lvert\sigma_i - \tau_i\rvert$
- maximum-lead	$D(\sigma,\tau) = \sup_N \lvert\sum_{i=0}^N (\sigma_i - \tau_i)\rvert$
- Cantor	$D(\sigma,\tau) = 1/(1+\inf\{j \mid \sigma_j \neq \tau_j\})$
- discrete	$D(\sigma,\tau) = 0$ if $\sigma = \tau$; ∞ otherwise

Asarin-Basset-Degorre 2018

$$D(\sigma, \tau) = \max \left\{ \begin{array}{l} \sup_i \inf_j \{ |t_i - s_j| \mid a_i = b_j \} \\ \sup_j \inf_i \{ |t_i - s_j| \mid a_i = b_j \} \end{array} \right.$$

Challenge (*ca.* 2009)

- In quantitative verification, lots of different distances
- Develop theory to cover all/most of them
    - idea: use bisimulation games

⇒ The Quantitative Linear-Time–Branching-Time Spectrum

- QAPL 2011, FSTTCS 2011, TCS 2014

Challenge (*ca.* 2012):

- How to make this compositional?
- Still not satisfied!

1. Introduction

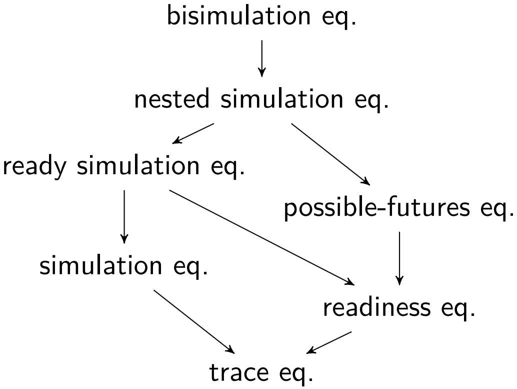
2. The Quantitative Linear-Time–Branching-Time Spectrum

3. Compositional Verification

4. Conclusion

The Linear-Time–Branching-Time Spectrum

van Glabbeek 1990 (excerpt):



bisimulation eq.

nested simulation eq.

ready simulation eq.

possible-futures eq.

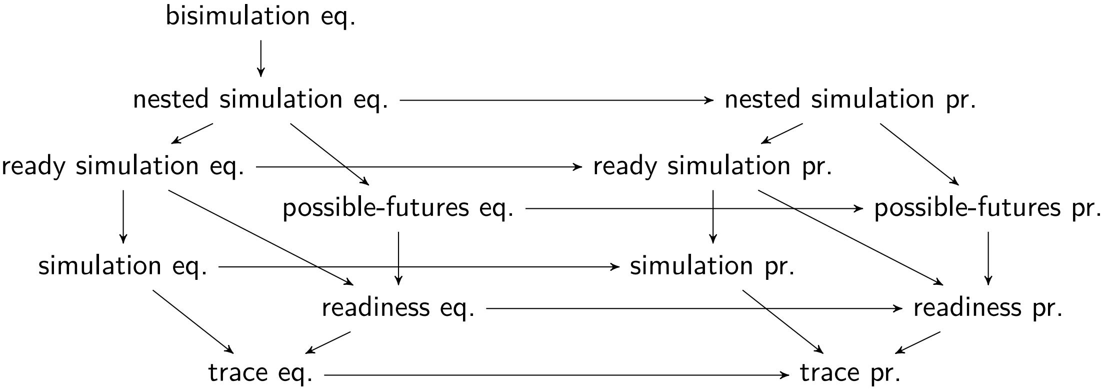
simulation eq.

readiness eq.

trace eq.

The Linear-Time–Branching-Time Spectrum

van Glabbeek 1990 (excerpt):



bisimulation eq.

nested simulation eq.

nested simulation pr.

ready simulation eq.

ready simulation pr.

possible-futures eq.

possible-futures pr.

simulation eq.

simulation pr.

readiness eq.

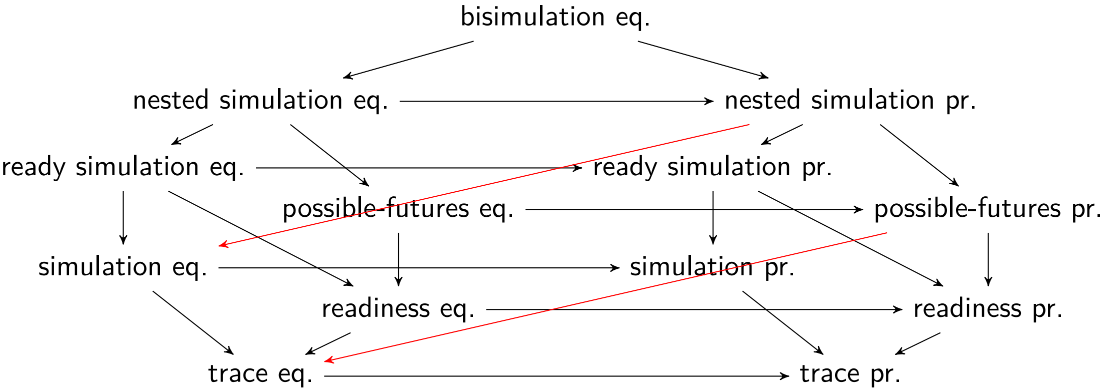
readiness pr.

trace eq.

trace pr.

The Linear-Time–Branching-Time Spectrum

van Glabbeek 1990 (excerpt):



bisimulation eq.

nested simulation eq.

nested simulation pr.

ready simulation eq.

ready simulation pr.

possible-futures eq.

possible-futures pr.

simulation eq.

simulation pr.

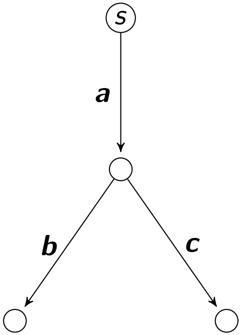
readiness eq.

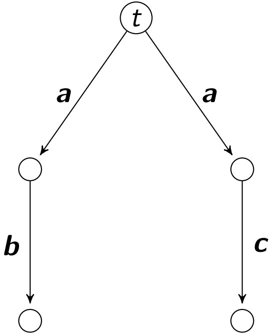
readiness pr.

trace eq.

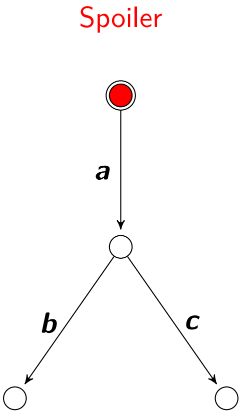
trace pr.

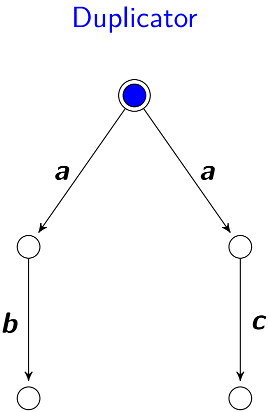
The Simulation Game



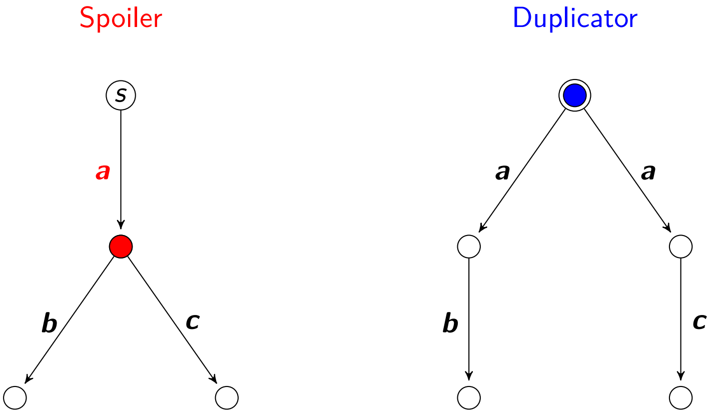


The Simulation Game

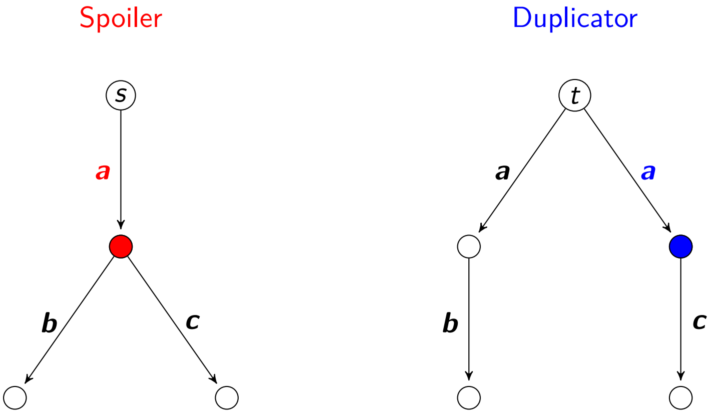




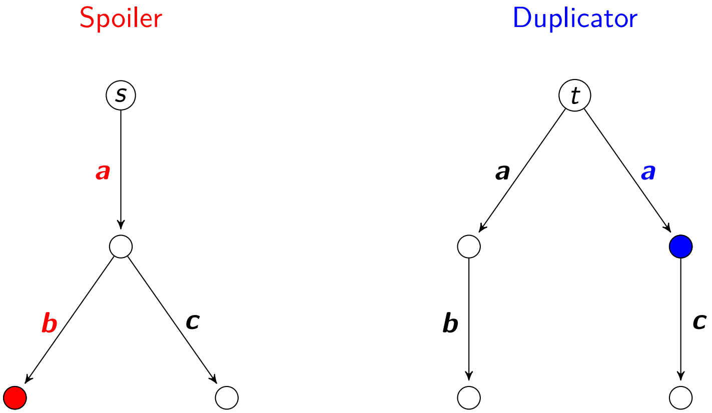
The Simulation Game



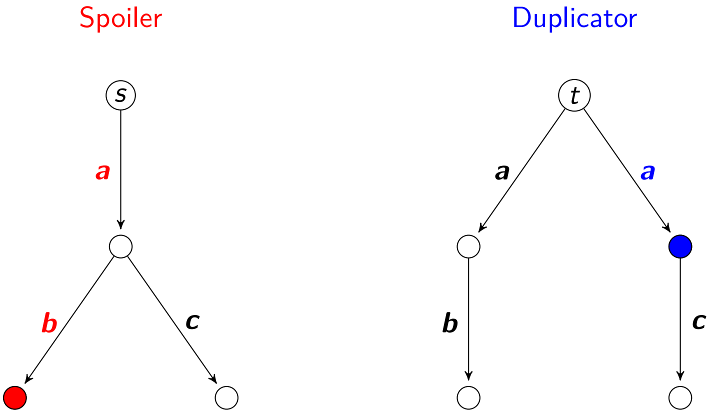
The Simulation Game



The Simulation Game

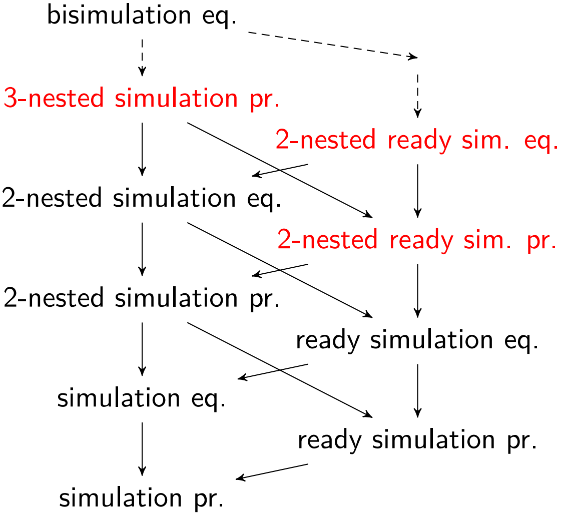


The Simulation Game



Spoiler wins

The LTBT Spectrum, Game Version



bisimulation eq.

3-nested simulation pr.

2-nested ready sim. eq.

2-nested simulation eq.

2-nested ready sim. pr.

2-nested simulation pr.

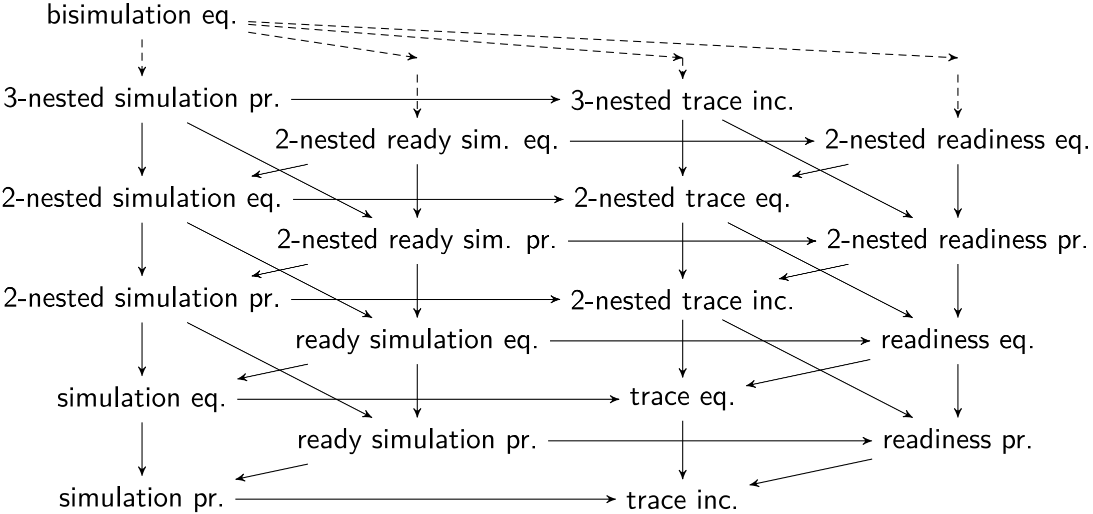
ready simulation eq.

simulation eq.

ready simulation pr.

simulation pr.

The LTBT Spectrum, Game Version



bisimulation eq.

3-nested simulation pr.

3-nested trace inc.

2-nested ready sim. eq.

2-nested readiness eq.

2-nested simulation eq.

2-nested trace eq.

2-nested ready sim. pr.

2-nested readiness pr.

2-nested simulation pr.

2-nested trace inc.

ready simulation eq.

readiness eq.

simulation eq.

trace eq.

ready simulation pr.

readiness pr.

simulation pr.

trace inc.

The Simulation Game, Revisited

1. Player 1 chooses edge from s (leading to s')
2. Player 2 chooses matching edge from t (leading to t')
3. Game continues from configuration s', t'

ω. If Player 2 can always answer: YES, t simulates s.
Otherwise: NO

Or, as an Ehrenfeucht-Fraïssé game (“delayed evaluation”):

1. Player 1 chooses edge from s (leading to s')
2. Player 2 chooses edge from t (leading to t')
3. Game continues from new configuration s', t'

ω. At the end (maybe after infinitely many rounds!), compare the chosen traces:
If the trace chosen by t matches the one chosen by s: YES
Otherwise: NO

Quantitative Ehrenfeucht-Fraïssé Games

The quantitative setting:

- Assume we have a way, possibly application-determined, to measure distances of (finite or infinite) traces
- a hemimetric $D : (\sigma, \tau) \mapsto D(\sigma, \tau) \in \mathbb{R}_{\ge 0} \cup \{\infty\}$

The quantitative Ehrenfeucht-Fraïssé game:

1. Player 1 chooses edge from s (leading to s')
2. Player 2 chooses edge from t (leading to t')
3. Game continues from new configuration s', t'

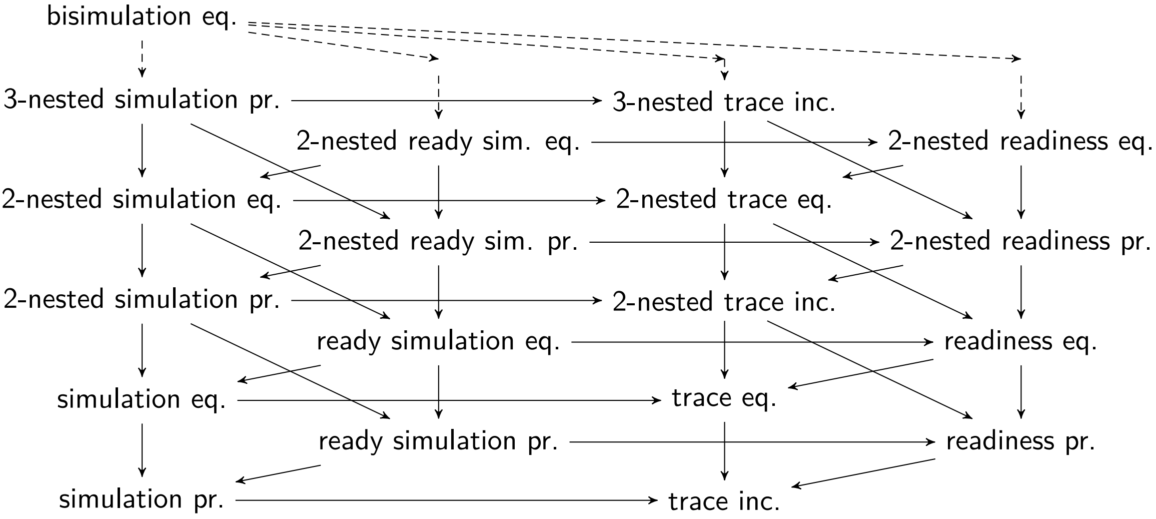
ω. At the end, compare the chosen traces σ, τ:
The simulation distance from s to t is defined to be $D(\sigma, \tau)$

- Player 1 plays to maximize $D(\sigma, \tau)$; Player 2 plays to minimize

This can be generalized to all the games in the LTBT spectrum.

The Quantitative Linear-Time–Branching-Time Spectrum

For any trace distance $D : (\sigma, \tau) \mapsto D(\sigma, \tau) \in \mathbb{R}_{\geq 0} \cup \{\infty\}$:



bisimulation eq.

3-nested simulation pr.

3-nested trace inc.

2-nested ready sim. eq.

2-nested readiness eq.

2-nested simulation eq.

2-nested trace eq.

2-nested ready sim. pr.

2-nested readiness pr.

2-nested simulation pr.

2-nested trace inc.

ready simulation eq.

readiness eq.

simulation eq.

trace eq.

ready simulation pr.

readiness pr.

simulation pr.

trace inc.

Quantitative EF Games: Some Details

- Configuration of the game: (π, ρ): π the Player-1 choices up to now; ρ the Player-2 choices
- Strategy: mapping from configurations to next moves
  - Θ_i: set of Player-i strategies
- Simulation strategy: Player-1 moves allowed from end of π
- Bisimulation strategy: Player-1 moves allowed from end of π or end of ρ
  - (hence π and ρ are generally not paths – "mingled paths")
- Pair of strategies $\Longrightarrow$ (possibly infinite) sequence of configurations
- Take the limit; unmingle $\Longrightarrow$ pair of (possibly infinite) traces (σ, τ)
- Bisimulation distance: $\sup_{\theta_1 \in \Theta_1} \inf_{\theta_2 \in \Theta_2} d_T(\sigma, \tau)$
- Simulation distance: $\sup_{\theta_1 \in \Theta_1^0} \inf_{\theta_2 \in \Theta_2} d_T(\sigma, \tau)$ (restricting Player 1's capabilities)

Quantitative EF Games: Some Details – II

- Blind Player-1 strategies: depend only on the end of ρ
  - ("cannot see Player-2 moves")
  - $\tilde\Theta_1$: set of blind Player-1 strategies
- Trace inclusion distance: $\sup_{\theta_1\in\tilde\Theta_1^0} \inf_{\theta_2\in\Theta_2} d_T(\sigma,\tau)$
- For nesting: count the number of times Player 1 switches between end of π and end of ρ
  - Θ_1^k: k switches allowed
- Nested simulation distance: $\sup_{\theta_1\in\Theta_1^1} \inf_{\theta_2\in\Theta_2} d_T(\sigma,\tau)$
- Nested trace inclusion distance: $\sup_{\theta_1\in\tilde\Theta_1^1} \inf_{\theta_2\in\Theta_2} d_T(\sigma,\tau)$ (!)
- For ready: allow extra "I'll see you" Player-1 transition from end of ρ

Transfer Theorem

Theorem

If two equivalences or preorders are inequivalent in the qualitative setting, and the trace distance D is separating, then the corresponding QLTBT distances are topologically inequivalent.

Recursive Characterization

Theorem

If the trace distance $D : (\sigma, \tau) \mapsto d(\sigma, \tau)$ has a decomposition $d = g \circ f : \mathrm{Tr} \times \mathrm{Tr} \to L \to \mathbb{R}_{\geq 0} \cup \{\infty\}$ through a complete lattice L, and f has a recursive characterization, i.e., such that $f(a.\sigma, b.\tau) = F(a, b, f(\sigma, \tau))$ for some $F : \Sigma \times \Sigma \times L \to L$ which is monotone in the third coordinate, then all distances in the corresponding QLTBT spectrum are given as least fixed points of some functionals using F.

All trace distances I know can be expressed recursively like this.

- Example: simulation distance:

$$d_{\mathrm{sim}}(s, t) = \sup_{s \xrightarrow{a} s'} \inf_{t \xrightarrow{b} t'} F(a, b, d_{\mathrm{sim}}(s', t')) \qquad \text{(l.f.p.)}$$

- L is “memory”
- also gives relation family characterization

1. Introduction
2. The Quantitative Linear-Time–Branching-Time Spectrum
3. Compositional Verification
4. Conclusion

Specification Theories

Let Mod be a set of models with an equivalence $\sim$.

Definition

A complete specification theory for $(\mathrm{Mod}, \sim)$ is $(\mathrm{Spec}, \leq, \|, \chi)$ such that

- $\leq$ is a refinement preorder on Spec
- $\chi : \mathrm{Mod} \to \mathrm{Spec}$ picks out characteristic specifications
  - *i.e.*, $\forall \mathcal{M}_1, \mathcal{M}_2 \in \mathrm{Mod} : \mathcal{M}_1 \sim \mathcal{M}_2 \iff \chi(\mathcal{M}_1) \leq \chi(\mathcal{M}_2)$
- $(\mathrm{Spec}, \leq, \|)$ forms a bounded commutative distributive residuated lattice up to $\leq \cap \geq$

$\Rightarrow$ $\vee$ and $\wedge$ on Spec; double distributivity; $\bot, \top \in \mathrm{Spec}$

- everything up to modal equivalence $\equiv \, = \, \leq \cap \geq$

$\Rightarrow$ $\|$ distributes over $\vee$, has unit U, has residual $/$ (up to $\equiv$)

- $\mathcal{S}_1 \| \mathcal{S}_2 \leq \mathcal{S}_3 \iff \mathcal{S}_2 \leq \mathcal{S}_3 / \mathcal{S}_1$

Examples

- Disjunctive modal transition systems
- Acceptance automata
- Hennessy-Milner logic with maximal fixed points

- CONCUR 2013, ICTAC 2014, I&C 2020 (all with bisimulation as model equivalence $\sim$)

Acceptance Automata

Let Σ be a finite alphabet.

Definition

A (nondeterministic) acceptance automaton (AA) is a structure $\mathcal{A} = (S, S^0, \text{Tran})$, with $S \supseteq S^0$ finite sets of states and initial states and $\text{Tran} : S \to 2^{2^{\Sigma \times S}}$ an assignment of *transition constraints*.

- standard labeled transition system (LTS): $\text{Tran} : S \to 2^{\Sigma \times S}$ (coalgebraic view)
- (for AA:) $\text{Tran}(s) = \{M_1, M_2, \dots\}$: provide M_1 or M_2 or …
- a disjunctive choice of conjunctive constraints
- J.-B. Raclet 2008 (but deterministic); see also H. H. Hansen 2003
- note multiple initial states

Refinement

Definition

Let $\mathcal{A}_1 = (S_1, S_1^0, \mathrm{Tran}_1)$ and $\mathcal{A}_2 = (S_2, S_2^0, \mathrm{Tran}_2)$ be AA.
A relation $R \subseteq S_1 \times S_2$ is a modal refinement if:

1. $\forall s_1^0 \in S_1^0 : \exists s_2^0 \in S_2^0 : (s_1^0, s_2^0) \in R$ (init)
2. $\forall (s_1, s_2) \in R : \forall M_1 \in \mathrm{Tran}_1(s_1) : \exists M_2 \in \mathrm{Tran}_2(s_2) :$ (tran)
    1. $\forall (a, t_1) \in M_1 : \exists (a, t_2) \in M_2 : (t_1, t_2) \in R$
    2. $\forall (a, t_2) \in M_2 : \exists (a, t_1) \in M_1 : (t_1, t_2) \in R$

Write $\mathcal{A}_1 \le \mathcal{A}_2$ if there exists such a modal refinement.

- for any constraint choice M_1 there is a bisimilar choice M_2
- $\mathcal{A}_1$ has fewer choices than $\mathcal{A}_2$
- no more choices $\triangleq$ only one $M \in \mathrm{Tran}(s)$ $\triangleq$ LTS
- formally: an embedding $\chi : \mathrm{LTS} \hookrightarrow \mathrm{AA}$
  such that $\chi(\mathcal{L}_1) \le \chi(\mathcal{L}_2)$ iff $\mathcal{L}_1$ and $\mathcal{L}_2$ are bisimilar

Logical Operations

Let $\mathcal{A}_1 = (S_1, S_1^0, \mathrm{Tran}_1)$ and $\mathcal{A}_2 = (S_2, S_2^0, \mathrm{Tran}_2)$ be AA.

Disjunction: $\mathcal{A}_1 \vee \mathcal{A}_2 = (S_1 \overset{+}{\cup} S_2, S_1^0 \overset{+}{\cup} S_2^0, \mathrm{Tran}_1 \overset{+}{\cup} \mathrm{Tran}_2)$

Conjunction: define $\pi_i : 2^{\Sigma \times S_1 \times S_2} \to 2^{\Sigma \times S_i}$ by

$$\begin{aligned} \pi_1(M) &= \{(a, s_1) \mid \exists s_2 \in S_2 : (a, s_1, s_2) \in M\} \\ \pi_2(M) &= \{(a, s_2) \mid \exists s_1 \in S_1 : (a, s_1, s_2) \in M\} \end{aligned}$$

Let $\mathcal{A}_1 \wedge \mathcal{A}_2 = (S_1 \times S_2, S_1^0 \times S_2^0, \mathrm{Tran})$ with

$$\mathrm{Tran}((s_1, s_2)) = \{M \subseteq \Sigma \times S_1 \times S_2 \mid \pi_1(M) \in \mathrm{Tran}_1(s_1), \pi_2(M) \in \mathrm{Tran}_2(s_2)\}$$

Theorem

For all LTS $\mathcal{L}$ and AA $\mathcal{A}_1, \mathcal{A}_2$:

$$\begin{aligned} \mathcal{L} \models \mathcal{A}_1 \vee \mathcal{A}_2 &\iff \mathcal{L} \models \mathcal{A}_1 \text{ or } \mathcal{L} \models \mathcal{A}_2 \\ \mathcal{L} \models \mathcal{A}_1 \wedge \mathcal{A}_2 &\iff \mathcal{L} \models \mathcal{A}_1 \;\&\; \mathcal{L} \models \mathcal{A}_2 \end{aligned}$$

Structural Operations: Composition

Let $\mathcal{A}_1 = (S_1, S_1^0, \text{Tran}_1)$ and $\mathcal{A}_2 = (S_2, S_2^0, \text{Tran}_2)$ be AA.

For $M_1 \subseteq \Sigma \times S_1$ and $M_2 \subseteq \Sigma \times S_2$, define

$$M_1 \| M_2 = \{(a, (t_1, t_2)) \mid (a, t_1) \in M_1, (a, t_2) \in M_2\}$$

(assumes CSP synchronization, but can be generalized)

Let $\mathcal{A}_1 \| \mathcal{A}_2 = (S_1 \times S_2, S_1^0 \times S_2^0, \text{Tran})$ with

$$\text{Tran}((s_1, s_2)) = \{M_1 \| M_2 \mid M_1 \in \text{Tran}_1(s_1), M_2 \in \text{Tran}_2(s_2)\}$$

Theorem (independent implementability)

For all AA $\mathcal{A}_1$, $\mathcal{A}_2$, $\mathcal{A}_3$, $\mathcal{A}_4$:

$$\mathcal{A}_1 \leq \mathcal{A}_3 \;\&\; \mathcal{A}_2 \leq \mathcal{A}_4 \implies \mathcal{A}_1 \| \mathcal{A}_2 \leq \mathcal{A}_3 \| \mathcal{A}_4$$

Structural Operations: Quotient

Let $\mathcal{A}_1 = (S_1, S_1^0, \text{Tran}_1)$ and $\mathcal{A}_2 = (S_2, S_2^0, \text{Tran}_2)$ be AA.

Define $\mathcal{A}_1 / \mathcal{A}_2 = (S, S^0, \text{Tran})$:

- $S = 2^{S_1 \times S_2}$
- write $S_2^0 = \{s_2^{0,1}, \dots, s_2^{0,p}\}$ and let $S^0 = \{\{(s_1^{0,q}, s_2^{0,q}) \mid q \in \{1, \dots, p\}\} \mid \forall q : s_1^{0,q} \in S_1^0\}$
- $\text{Tran} =$

Structural Operations: Quotient

Let $\mathcal{A}_1 = (S_1, S_1^0, \mathrm{Tran}_1)$ and $\mathcal{A}_2 = (S_2, S_2^0, \mathrm{Tran}_2)$ be AA.

Define $\mathcal{A}_1 / \mathcal{A}_2 = (S, S^0, \mathrm{Tran})$:

- $S = 2^{S_1 \times S_2}$
- write $S_2^0 = \{s_2^{0,1}, \dots, s_2^{0,p}\}$ and let $S^0 = \{\{(s_1^{0,q}, s_2^{0,q}) \mid q \in \{1, \dots, p\}\} \mid \forall q : s_1^{0,q} \in S_1^0\}$
- $\mathrm{Tran} =$

Structural Operations: Quotient

Let $\mathcal{A}_1 = (S_1, S_1^0, \mathrm{Tran}_1)$ and $\mathcal{A}_2 = (S_2, S_2^0, \mathrm{Tran}_2)$ be AA.

Define $\mathcal{A}_1 / \mathcal{A}_2 = (S, S^0, \mathrm{Tran})$:

- $S = 2^{S_1 \times S_2}$
- write $S_2^0 = \{s_2^{0,1}, \dots, s_2^{0,p}\}$ and let $S^0 = \{\{(s_1^{0,q}, s_2^{0,q}) \mid q \in \{1, \dots, p\}\} \mid \forall q : s_1^{0,q} \in S_1^0\}$
- $\mathrm{Tran} = \quad \dots$

Theorem

For all AA $\mathcal{A}_1$, $\mathcal{A}_2$, $\mathcal{A}_3$:

$$\mathcal{A}_1 \| \mathcal{A}_2 \le \mathcal{A}_3 \iff \mathcal{A}_2 \le \mathcal{A}_3 / \mathcal{A}_1$$

- up to $\equiv$, $/$ is the adjoint (or residual) of $\|$

Quantitative Specification Theories?

Definition (recall)

A complete specification theory for $(\mathsf{Mod}, \sim)$ is $(\mathsf{Spec}, \leq, \|, \chi)$ such that

- $\leq$ is a refinement preorder on Spec
- $\mathcal{M}_1 \sim \mathcal{M}_2 \iff \chi(\mathcal{M}_1) \leq \chi(\mathcal{M}_2)$
- $(\mathsf{Spec}, \leq, \|)$ forms a b.c.d. residuated lattice up to $\equiv$

- generalize $\sim$ by pseudometric d_{Mod}
  - $d_{\mathsf{Mod}}(\mathcal{M}_1, \mathcal{M}_2) = 0$ iff $\mathcal{M}_1 \sim \mathcal{M}_2$
- generalize $\leq$ by hemimetric d
  - $d_{\mathsf{Mod}}(\mathcal{M}_1, \mathcal{M}_2) = d(\chi(\mathcal{M}_1), \chi(\mathcal{M}_2))$
  - $d(\mathcal{M}, \mathcal{S}) = d(\chi(\mathcal{M}), \mathcal{S})$
- still want $(\mathsf{Spec}, \leq, \|)$ to be a b.c.d. residuated lattice up to $\equiv$

Acceptance Automata

For DMTS/AA/HML$_{\text{max}}$:

- d_{Mod}: any bisimulation distance
- d: corresponding modal refinement distance
- transitivity $\rightsquigarrow$ triangle ineq.: $d(\mathcal{S}_1, \mathcal{S}_2) + d(\mathcal{S}_2, \mathcal{S}_3) \geq d(\mathcal{S}_1, \mathcal{S}_3)$
- $d(\mathcal{S}, \mathcal{S}_1 \wedge \mathcal{S}_2) = \max(d(\mathcal{S}, \mathcal{S}_1), d(\mathcal{S}, \mathcal{S}_2))$ or ∞
- $d(\mathcal{S}_1 \vee \mathcal{S}_2, \mathcal{S}) = \max(d(\mathcal{S}_1, \mathcal{S}), d(\mathcal{S}_2, \mathcal{S}))$ or ∞
- quotient is quantitative residual: $d(\mathcal{S}_1 \| \mathcal{S}_2, \mathcal{S}_3) = d(\mathcal{S}_2, \mathcal{S}_3 / \mathcal{S}_1)$
- for $\|$ itself, uniform continuity: a function $P : \mathbb{R}_{\geq 0} \times \mathbb{R}_{\geq 0} \to \mathbb{R}_{\geq 0}$ such that $d(\mathcal{S}_1 \| \mathcal{S}_2, \mathcal{S}_3 \| \mathcal{S}_4) \leq P(d(\mathcal{S}_1, \mathcal{S}_3), d(\mathcal{S}_2, \mathcal{S}_4))$

The Bad
and/or
Ugly

Silent Moves in QLTBT?

- Any serious spectrographer needs to think about silent moves
- (van Glabbeek 1993: LTBT II)
- Bisping, Jansen 2023: Energy games for the weak spectrum
  - but uses power set for linear part (recall: we use blindness instead)
  - difficult to reconcile power set with quantitative setting
- otherwise, some coalgebra approaches:
  - Sprunger, Katsumata, Dubut, Hasuo 2021: Fibrational bisimulations and quantitative reasoning
  - Ford, Milius, Schröder, Beohar, König 2022: Graded monads and behavioural equivalence games
  - Beohar, Gurke, König, Messing 2023: Hennessy-Milner theorems via Galois connections
  - again, power set seems very popular . . .
- status: IT'S COMPLICATED

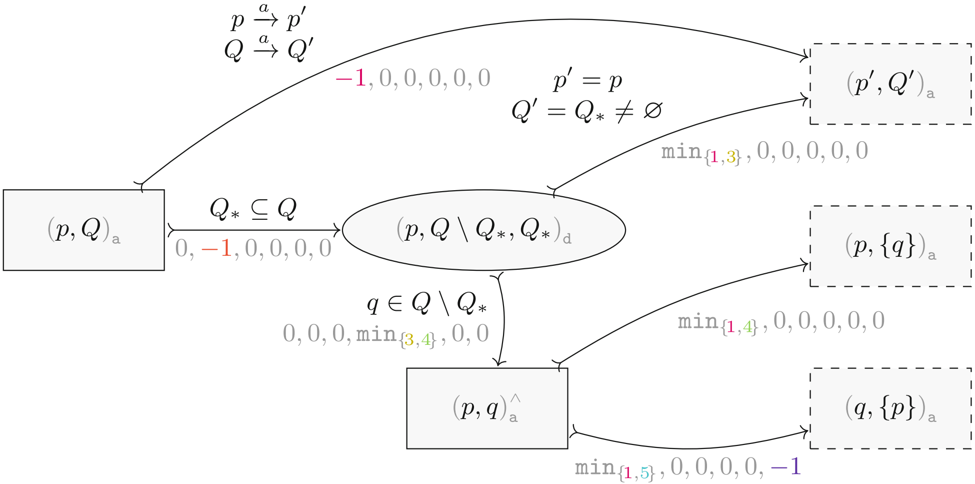

$p \xrightarrow{a} p'$
$Q \xrightarrow{a} Q'$
$-1, 0, 0, 0, 0, 0$
$p' = p$
$Q' = Q_* \neq \varnothing$
$(p', Q')_{\mathtt{a}}$
$\mathtt{min}_{\{1,3\}}, 0, 0, 0, 0, 0$
$(p, Q)_{\mathtt{a}}$
$Q_* \subseteq Q$
$0, -1, 0, 0, 0, 0$
$(p, Q \setminus Q_*, Q_*)_{\mathtt{d}}$
$(p, \{q\})_{\mathtt{a}}$
$q \in Q \setminus Q_*$
$0, 0, 0, \mathtt{min}_{\{3,4\}}, 0, 0$
$\mathtt{min}_{\{1,4\}}, 0, 0, 0, 0, 0$
$(p, q)^{\wedge}_{\mathtt{a}}$
$(q, \{p\})_{\mathtt{a}}$
$\mathtt{min}_{\{1,5\}}, 0, 0, 0, 0, -1$

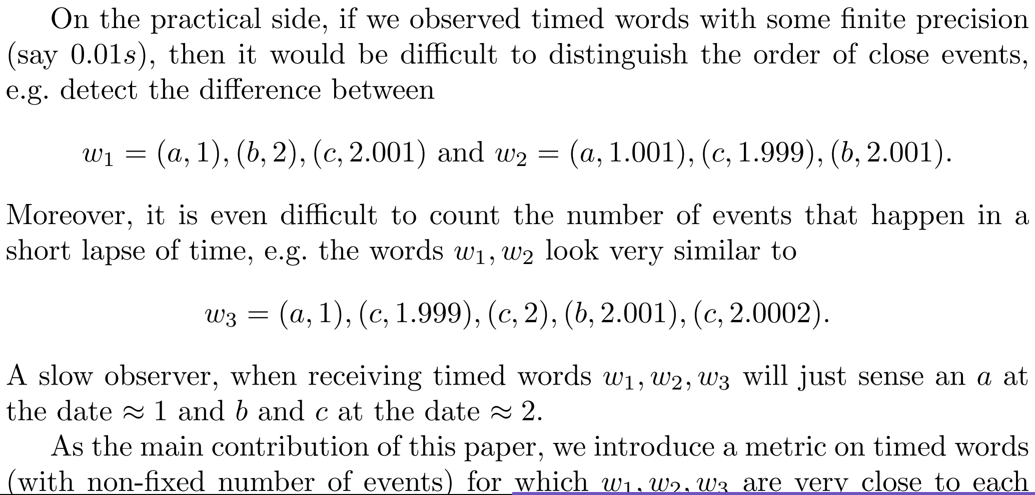
Fig. 7. Schematic spectroscopy game $\mathcal{G}_{\triangle}$ of Definition 10.

Asarin-Basset-Degorre Distance

Recall:

$$D(\sigma,\tau) = \max \begin{cases} \sup_i \inf_j \{|t_i - s_j| \mid a_i = b_j\} \\ \sup_j \inf_i \{|t_i - s_j| \mid a_i = b_j\} \end{cases}$$

Asarin-Basset-Degorre Distance



On the practical side, if we observed timed words with some finite precision (say $0.01s$), then it would be difficult to distinguish the order of close events, e.g. detect the difference between

$$w_1 = (a, 1), (b, 2), (c, 2.001) \text{ and } w_2 = (a, 1.001), (c, 1.999), (b, 2.001).$$

Moreover, it is even difficult to count the number of events that happen in a short lapse of time, e.g. the words w_1, w_2 look very similar to

$$w_3 = (a, 1), (c, 1.999), (c, 2), (b, 2.001), (c, 2.0002).$$

A slow observer, when receiving timed words w_1, w_2, w_3 will just sense an a at the date ≈ 1 and b and c at the date ≈ 2.

As the main contribution of this paper, we introduce a metric on timed words (with non-fixed number of events) for which w_1, w_2, w_3 are very close to each

Asarin-Basset-Degorre Distance

Recall:

$$D(\sigma, \tau) = \max \begin{cases} \sup_i \inf_j \{|t_i - s_j| \mid a_i = b_j\} \\ \sup_j \inf_i \{|t_i - s_j| \mid a_i = b_j\} \end{cases}$$

- takes into account permutations of symbols which are close in timing
- but in a way which may lose symbols
- relation to timed pomsets? Amrane, Bazille, Clement, UF 2024: Languages of HDTA
- status: HOPEFUL

Robustness

A quantitative system is robust if

$$\left.\begin{array}{c}\text{small changes in inputs}\\ \text{small environment perturbations}\\ \text{small measuring errors}\end{array}\right\} \implies \text{small changes in behavior}$$

Formulate using uniform continuity: there is a constant K such that

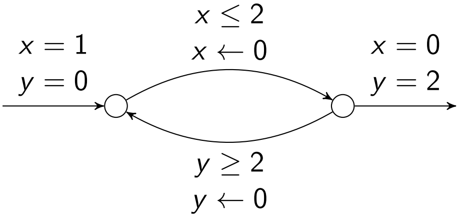
$$d_{\text{behavior}}(S, S') \le K\, d_{\text{syntax}}(S, S')$$

for all perturbations S' of S.

- Standard formulation in control theory
- Generally want systems to be robust

Robustness, lack of

Our quantitative models are not robust: (Merci, Nico)



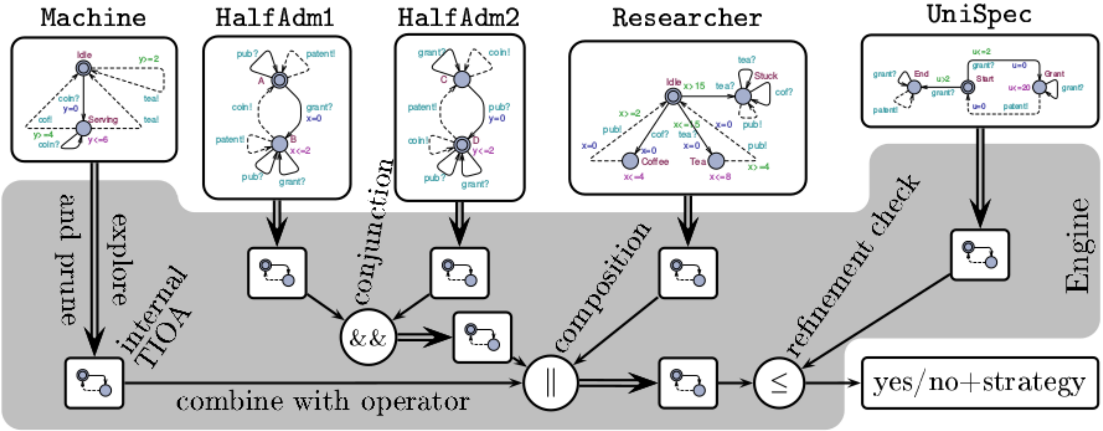
- restrict to robust models?
- quantify robustness?
- use different models?
- . . .

Compositionality?

Timed input-output automata:

- David, Larsen, Legay, Nyman, Traonouez, Wąsowski 2015: Real-time specifications
- Goorden, Larsen, Legay, Lorber, Nyman, Wąsowski 2023: Timed I/O Automata: It is never too late to complete your timed specification theory
- complete, with quotient, but without disjunction
- only deterministic specifications
- tool support: ECDAR / Uppaal TiGa (Aalborg)
- some work on robustness and implementability: Larsen, Legay, Traonouez, Wąsowski 2014: Robust synthesis for real-time systems

Timed Input-Output Automata



Specification Theories for Real-Time Systems, contd.

Modal event-clock specifications:

- Bertrand, Legay, Pinchinat, Raclet 2012: Modal event-clock specifications for timed component-based design
- complete, with quotient, but without disjunction
- only deterministic specifications
- some work on robustness: UF, Legay 2012: A robust specification theory for modal event-clock automata

Synchronous time-triggered interface theories:

- Delahaye, UF, Henzinger, Legay, Ničković 2012: Synchronous interface theories and time triggered scheduling
- no quotient, dubious conjunction, no implementation
- relation to BIP

Specification Theories for Hybrid Systems

Specification Theories for Hybrid Systems

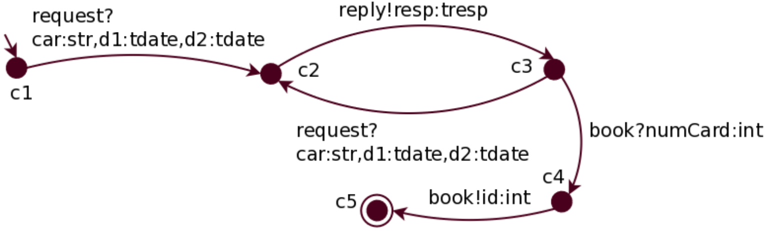
- Quesel, Fränzle, Damm 2011: Crossing the bridge between similar games

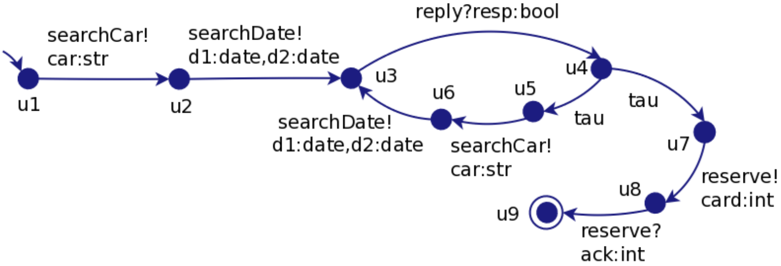
Conclusion

- general theory of quantitative verification ✓
- general theory of compositional quantitative verification ¯_(ツ)_/¯
    - algebraic properties ✓
    - quantitative algebraic properties ✗
    - silent moves ✗
- for real-time systems ¯_(ツ)_/¯
    - robustness ¯_(ツ)_/¯
    - compositionality ¯_(ツ)_/¯
    - robust compositionality ✗
- for hybrid systems ✗

5 Applications

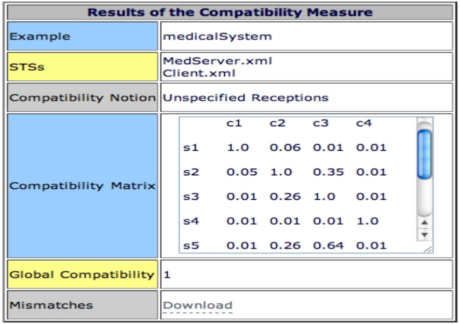
Interface Compatibility





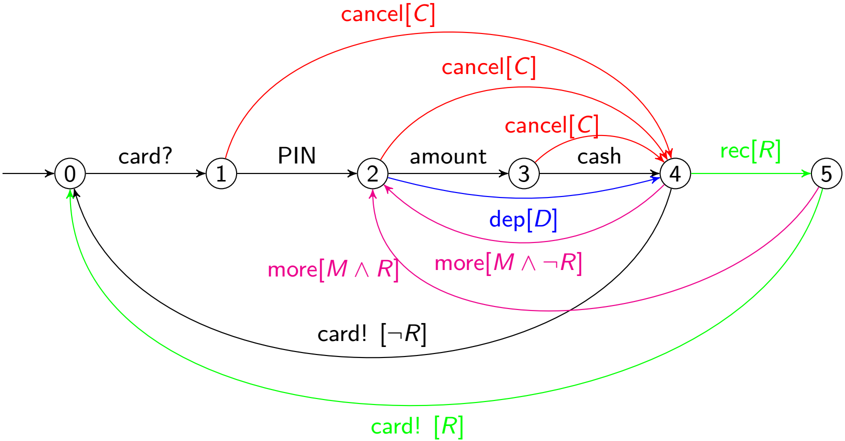
Interface Compatibility

- Use discounted (bi)simulation distances for measuring interface compatibility
- With A. Legay, M. Ouederni, G. Salaün
  - bisimulation d. for symmetric compatibility
  - ready simulation d. for asymmetric compatibility
- With tool support:



<table>
<tr><th colspan="2">Results of the Compatibility Measure</th></tr>
<tr><td>Example</td><td>medicalSystem</td></tr>
<tr><td>STSs</td><td>MedServer.xml
Client.xml</td></tr>
<tr><td>Compatibility Notion</td><td>Unspecified Receptions</td></tr>
<tr><td>Compatibility Matrix</td><td>
<table>
<tr><th></th><th>c1</th><th>c2</th><th>c3</th><th>c4</th></tr>
<tr><td>s1</td><td>1.0</td><td>0.06</td><td>0.01</td><td>0.01</td></tr>
<tr><td>s2</td><td>0.05</td><td>1.0</td><td>0.35</td><td>0.01</td></tr>
<tr><td>s3</td><td>0.01</td><td>0.26</td><td>1.0</td><td>0.01</td></tr>
<tr><td>s4</td><td>0.01</td><td>0.01</td><td>0.01</td><td>1.0</td></tr>
<tr><td>s5</td><td>0.01</td><td>0.26</td><td>0.64</td><td>0.01</td></tr>
</table>
</td></tr>
<tr><td>Global Compatibility</td><td>1</td></tr>
<tr><td>Mismatches</td><td>Download</td></tr>
</table>

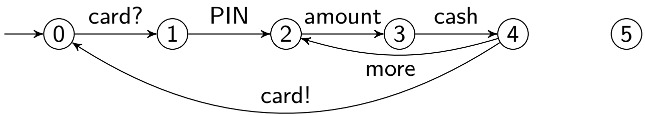
Behaviour Interactions in Product Lines



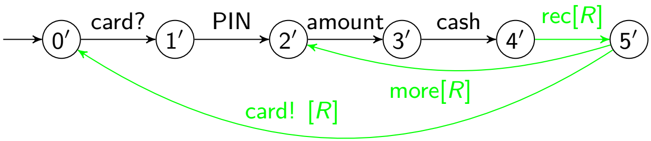
Behaviour Interactions in Product Lines

- Use a variant of Cantor bisimulation distance for counting the number of behaviour interactions in feature transition systems
- With J. Atlee, S. Beidu, A. Legay
- Use projections to products and compute Cantor bisimulation distance without repetitions:

$\pi_M(F)$:



$\pi_{M+R}(F)$:



Inter-Textual Distances in Statistical NLP

- Use discounted bisimulation distance to measure differences between texts
- With F. Biondi, S. Kongshøj, A. Legay
  - texts are very simple transition systems!
- Implementation
- Works better for some cases than standard distances used in statistical natural language processing
- New collaboration with NLP people in Grenoble

Inter-Textual Distances in Statistical NLP

- Let $A = (a_1, a_2, \dots, a_{N_A})$ and $B = (b_1, b_2, \dots, b_{N_B})$ be texts
- Write $\delta_{i,j} = [\,\text{if } a_i = b_j \text{ then } 0 \text{ else } 1\,]$ (word match indicator)
- position match (λ: discounting factor, $0 \le \lambda < 1$):

$$d_{\text{pm}}(i,j) = \delta_{i,j} + \lambda\delta_{i+1,j+1} + \lambda^2\delta_{i+2,j+2} + \lambda^3\delta_{i+3,j+3} + \cdots$$

- "try to match n-grams for n as high as possible, but don't be too sad if very long phrases don't match"
- global distance:

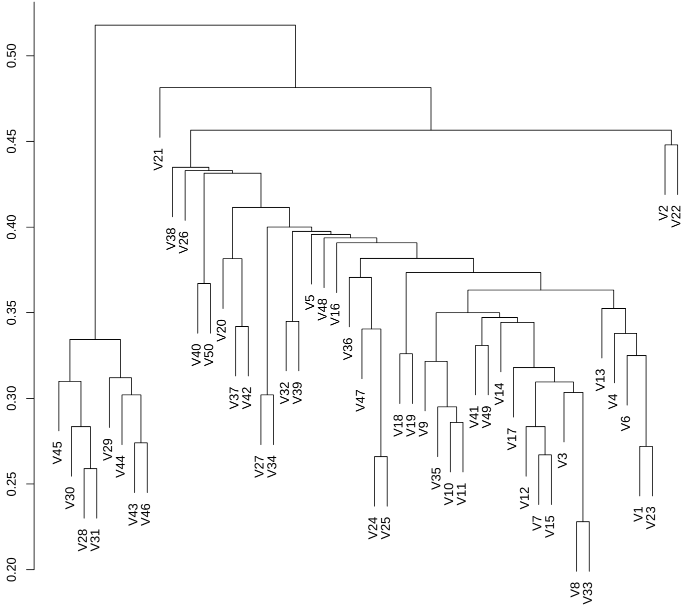
$$d_3(A,B) = \frac{1-\lambda}{N_A}\sum_{i=1}^{N_A} \min_{j=1,\dots,N_B} d_{\text{pm}}(i,j)$$

- find best possible match for each position in A, average, and scale
- and symmetrize: $d_4(A,B) = \max(d_3(A,B), d_3(B,A))$

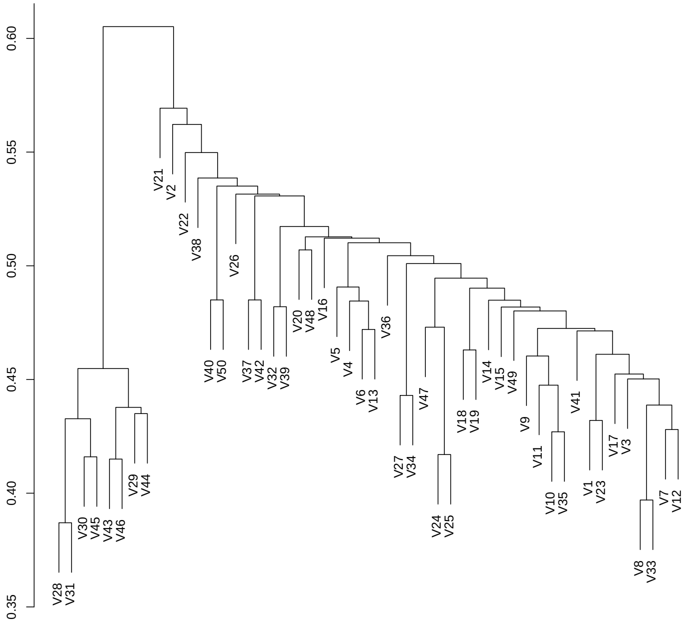
Inter-Textual Distances in Statistical NLP

Experiment:

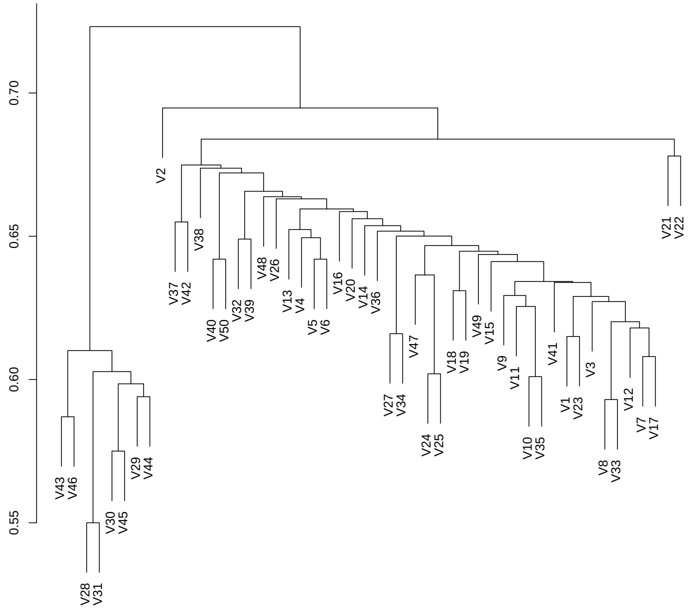
- 42 genuine scientific papers, all about modeling and verification
- 8 automatically generated “fake” papers (“SciGen”)


0.50
0.45
0.40
0.35
0.30
0.25
0.20
V45
V30
V28
V31
V29
V44
V43
V46
V21
V38
V26
V40
V50
V20
V37
V42
V27
V34
V32
V39
V5
V48
V16
V36
V47
V24
V25
V18
V19
V9
V35
V10
V11
V41
V49
V14
V17
V12
V7
V15
V3
V8
V33
V13
V4
V6
V1
V23
V2
V22

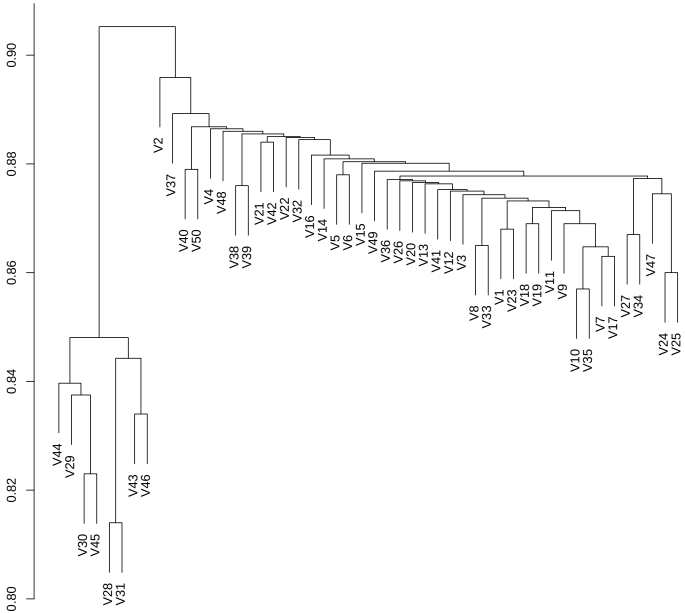
$\lambda = 0$


0.35
0.40
0.45
0.50
0.55
0.60
V28
V31
V30
V45
V43
V46
V29
V44
V21
V2
V22
V38
V40
V50
V26
V37
V42
V32
V39
V20
V48
V16
V5
V4
V6
V13
V36
V27
V34
V47
V24
V25
V18
V19
V14
V15
V49
V9
V11
V10
V35
V41
V1
V23
V17
V3
V8
V33
V7
V12

$\lambda = .4$


0.70
0.65
0.60
0.55
V43
V46
V28
V31
V30
V45
V29
V44
V2
V37
V42
V38
V40
V50
V32
V39
V48
V26
V13
V4
V5
V6
V16
V20
V14
V36
V27
V34
V47
V24
V25
V18
V19
V49
V15
V9
V11
V10
V35
V41
V1
V23
V3
V8
V33
V12
V7
V17
V21
V22

$\lambda = .7$


0.80
0.82
0.84
0.86
0.88
0.90
V44
V29
V30
V45
V28
V31
V43
V46
V2
V37
V40
V50
V4
V48
V38
V39
V21
V42
V22
V32
V16
V14
V5
V6
V15
V49
V36
V26
V20
V13
V41
V12
V3
V8
V33
V1
V23
V18
V19
V11
V9
V10
V35
V7
V17
V27
V34
V47
V24
V25

$\lambda = .95$