A Generic Approach to Quantitative Verification

Uli Fahrenberg

EPITA

Paris-Saclay 10 May 2022

ÉCOLE D'INGÉNIEURS EN INFORMATIQUE

Nice People

Coauthors:

- Sebastian S. Bauer, Nikola Beneš, Line Juhl, Jan Křetínský, Claus Thrane, Louis-Marie Traonouez

Shoulders:

- Lisbeth Fajstrup, Martin Raussen, Kim G. Larsen, Eric Goubault, Axel Legay, Zoltán Ésik, Georg Struth

Model Checking

model		specification
Mod	$\models$	Spec

Quantitative Model Checking

quantitative model		quantitative specification
Mod	$\models$	Spec

Quantitative Model Checking

quantitative model quantitative specification

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

↑

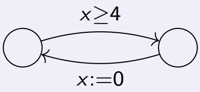
not sufficient

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 $\forall \phi : s \models \phi \Leftrightarrow t \models \phi$	$d_B(s,t) = \sup_\phi d([\![\phi]\!](s), [\![\phi]\!](t))$

Compositional Verification

model specification

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

- $\mathrm{Mod} \models \mathrm{Spec}_1$ & $\mathrm{Spec}_1 \le \mathrm{Spec}_2 \implies \mathrm{Mod} \models \mathrm{Spec}_2$
- $\mathrm{Mod} \models \mathrm{Spec}_1$ & $\mathrm{Mod} \models \mathrm{Spec}_2 \implies \mathrm{Mod} \models \mathrm{Spec}_1 \wedge \mathrm{Spec}_2$
- $\mathrm{Mod}_1 \models \mathrm{Spec}_1$ & $\mathrm{Mod}_2 \models \mathrm{Spec}_2 \implies \mathrm{Mod}_1 \| \mathrm{Mod}_2 \models \mathrm{Spec}_1 \| \mathrm{Spec}_2$
- $\mathrm{Mod}_1 \models \mathrm{Spec}_1$ & $\mathrm{Mod}_2 \models \mathrm{Spec} / \mathrm{Spec}_1 \implies \mathrm{Mod}_1 \| \mathrm{Mod}_2 \models \mathrm{Spec}$

- bottom-up and top-down

Quantitative Compositional Verification?

quantitative model quantitative specification

$$\text{Mod} \quad \models_\varepsilon \quad \text{Spec}$$

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

- surely not the same ε everywhere!?

User Stories

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

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

Challenge (*ca.* 2009)

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

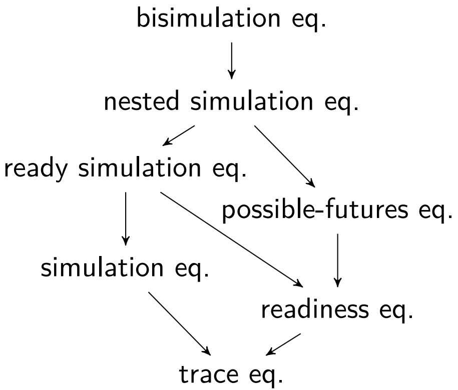
⇒ The Quantitative Linear-Time–Branching-Time Spectrum
  - QAPL 2011, FSTTCS 2011, TCS 2014

Challenge (*ca.* 2012):

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

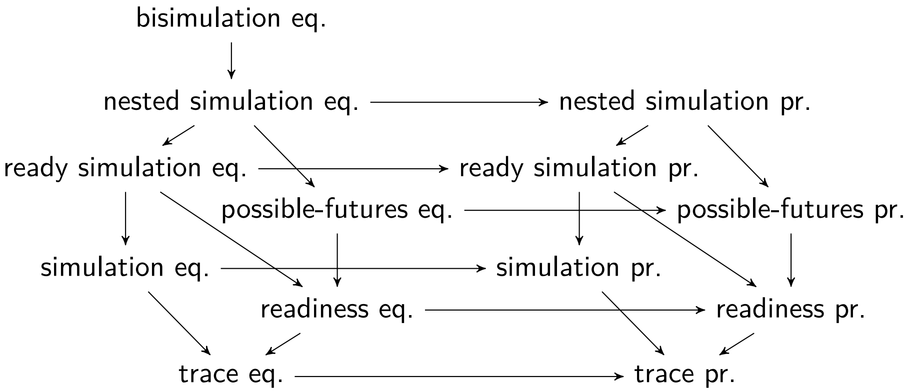
The Linear-Time–Branching-Time Spectrum

van Glabbeek, 2001 (excerpt):



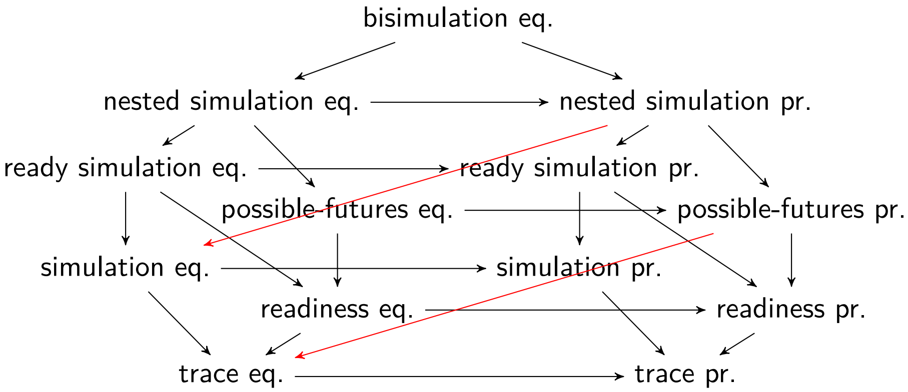
The Linear-Time–Branching-Time Spectrum

van Glabbeek, 2001 (excerpt):

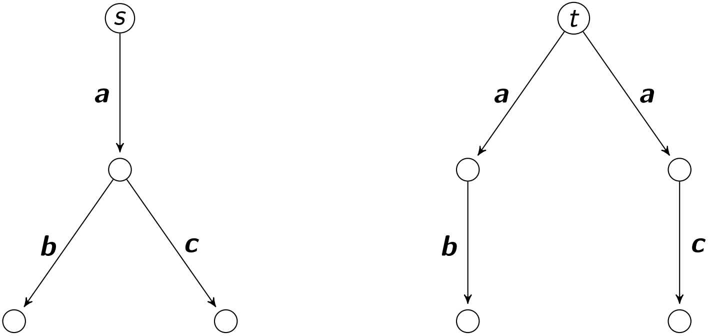


The Linear-Time–Branching-Time Spectrum

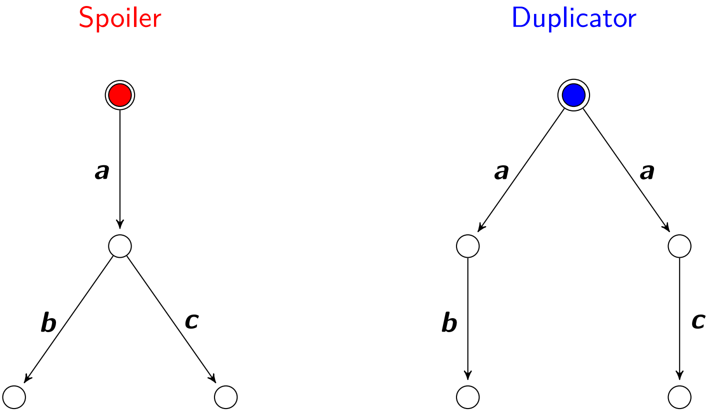
van Glabbeek, 2001 (excerpt):



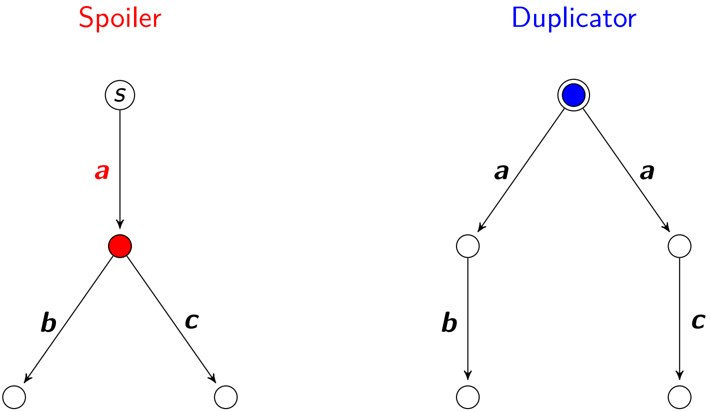
The Simulation Game



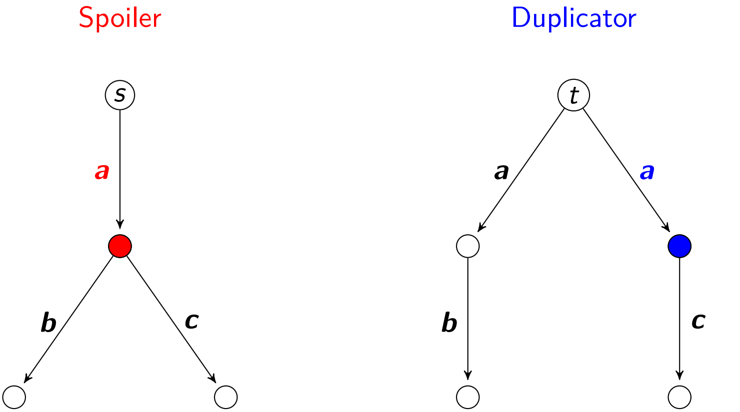
The Simulation Game



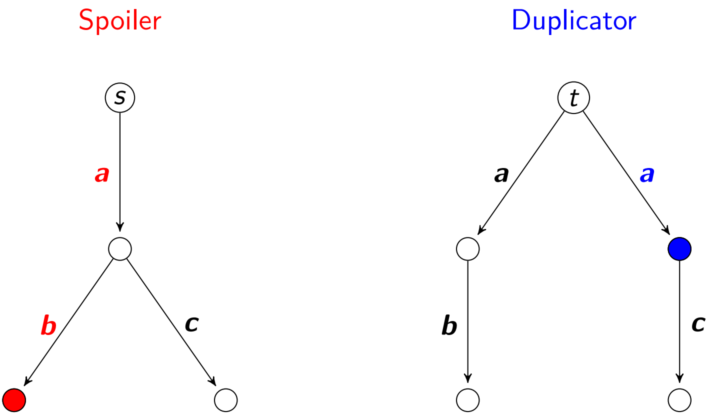
The Simulation Game



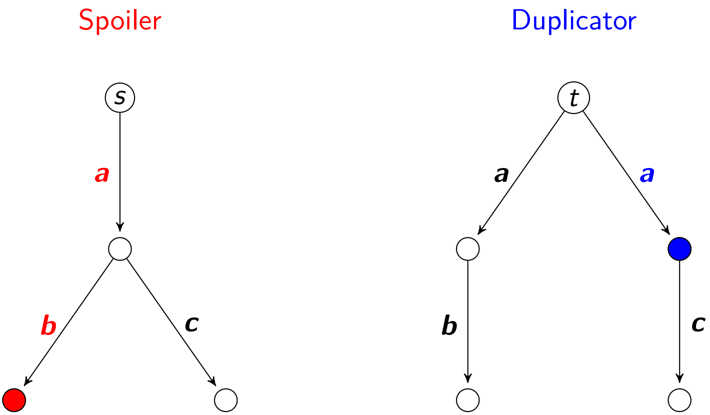
The Simulation Game



The Simulation Game

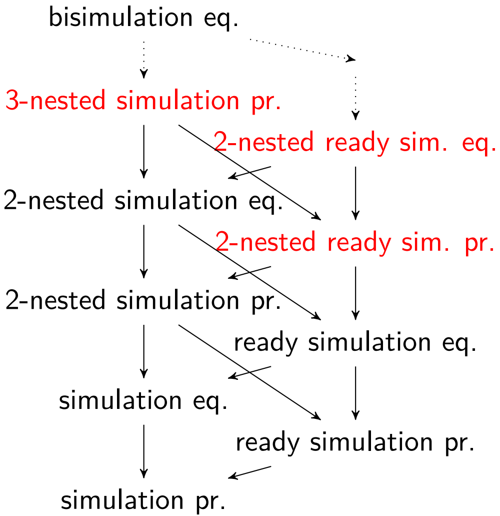


The Simulation Game

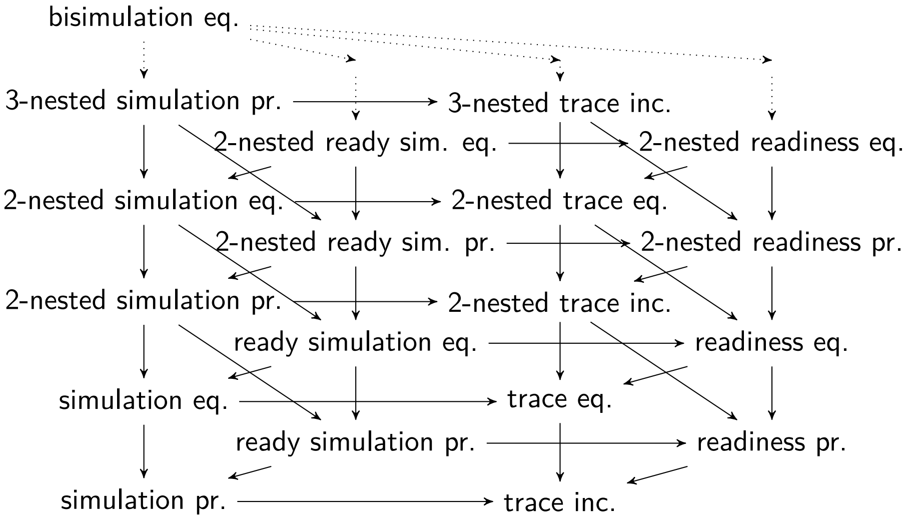


Spoiler wins

The LTBT Spectrum, Game Version



The LTBT Spectrum, Game Version



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

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'

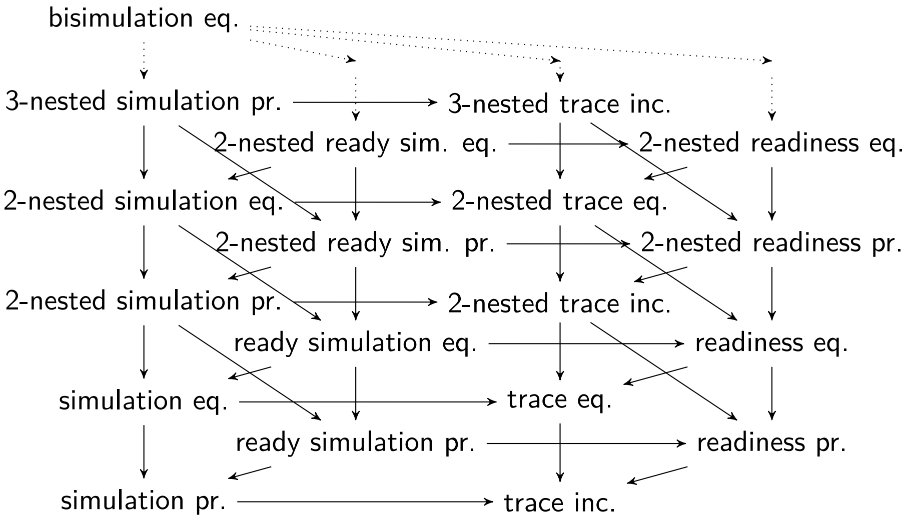
ω. At the end, compare the chosen traces σ, τ:
The simulation distance from s to t is defined to be $D(\sigma, \tau)$

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



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

Given two equivalences or preorders which are inequivalent in the qualitative setting,
and a separating trace distance,
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 are given as least fixed points of some functionals using F.

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

- L is "memory"
- also gives "relation family" characterization

Specification Theories

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

Definition

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

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

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

- 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 $\sim =$ bisimulation)

Quantitative Specification Theories?

Definition (recall)

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

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

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

Example: Disjunctive Modal Transition Systems

For DMTS/AA/HML_{max}:

- d_{Mod}: any bisimulation distance
- d: corresponding modal refinement distance
- transitivity $\Rightarrow$ 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 $d(\mathcal{S}_1 \| \mathcal{S}_2, \mathcal{S}_3 \| \mathcal{S}_4) \leq P(d(\mathcal{S}_1, \mathcal{S}_3), d(\mathcal{S}_2, \mathcal{S}_4))$

Recent Related Work

- Mardare, Panangaden, Plotkin: Quantitative equational logics
- Sprunger, Katsumata, Dubut, Hasuo: Fibrational bisimulations and quantitative reasoning
- Beohar, Ford, König, Milius, Schröder: Graded monads and behavioural equivalence games
- ...

Conclusion

- A general theory of quantitative verification ✓
- A general theory of compositional quantitative verification
  ¯_(ツ)_/¯
    - algebraic properties
        - for bisimulation ✓
        - for LTBT spectrum ✗
    - quantitative algebraic properties ✗

More generally

- All of this is based on transition systems
  - . . . at least all my examples are
- What about real-time systems? probabilistic systems? hybrid systems?
  - lots of work on compositional verification for these
  - . . . and on quantitative verification
  - . . . but on compositional quantitative verification??
  - I don't know how to make the connection to my work
- What about non-interleaving concurrency?!
  - I believe this is necessary
  - higher-dimensional automata to the rescue?
- Coalgebra is nice; but seems to have some the same problems?

Thank you!

Jo Atlee, Sebastian S. Bauer, Nikola Beneš, Patricia Bouyer-Decitre, Benoît Delahaye, Manfred Droste, Jérémy Dubut, Zoltán Ésik, Ignacio Fábregas, Lisbeth Fajstrup, Martin Fränzle, Eric Goubault, Emmanuel Haucourt, Christian Johansen, Jan Křetínský, Alexander Kurz, Kim G. Larsen, Axel Legay, Nicolas Markey, Samuel Mimram, Dejan Ničković, Rafael Olaechea, Karin Quaas, Martin Raussen, Jiří Srba, Georg Struth, Claus Thrane, Louis-Marie Traonouez, Andrzej Wąsowski, Rafał Wisniewski

Aline, Martin & Ionas