The Quantitative Linear-Time–Branching-Time Spectrum

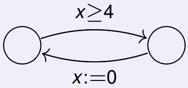
Uli Fahrenberg Axel Legay Claus Thrane

IRISA/INRIA Rennes, France / Aalborg University, Denmark

CEA April 2012

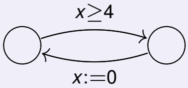
Quantitative Analysis

Quantitative *Models*



Quantitative Quantitative Analysis

Quantitative *Models*

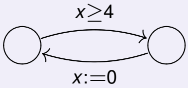


Quantitative *Logics*

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

Quantitative Quantitative Quantitative Analysis

Quantitative *Models*



Quantitative *Logics*

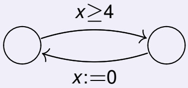
$$\Pr_{\leq .1}(\Diamond \mathit{error})$$

Quantitative *Verification*

$$[\![\varphi]\!](s) = 3.14$$
$$d(s, t) = 42$$

Quantitative Quantitative Quantitative Analysis

Quantitative *Models*



Quantitative *Logics*

$\mathrm{Pr}_{\leq .1}(\Diamond \mathit{error})$

Quantitative *Verification*

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

$d(s,t) = 42$

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

Quantitative Quantitative Quantitative Analysis

Problem: For processes with quantities, lots of different ways to measure distance

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

Upshot

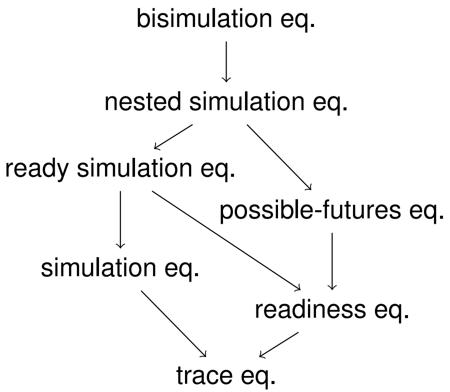
Two ideas:

- For an application, it is easiest to define distance between system traces (executions)
- Use games to convert this *linear* distance to *branching* distances

  Or:
- **If you give us a distance between strings, we give you back a bunch of distances between systems.**

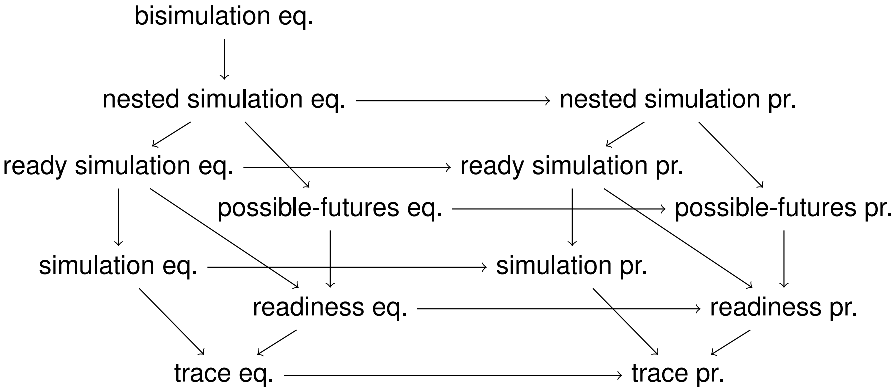
The Linear-Time–Branching-Time Spectrum

van Glabbeek, 2001 (excerpt):



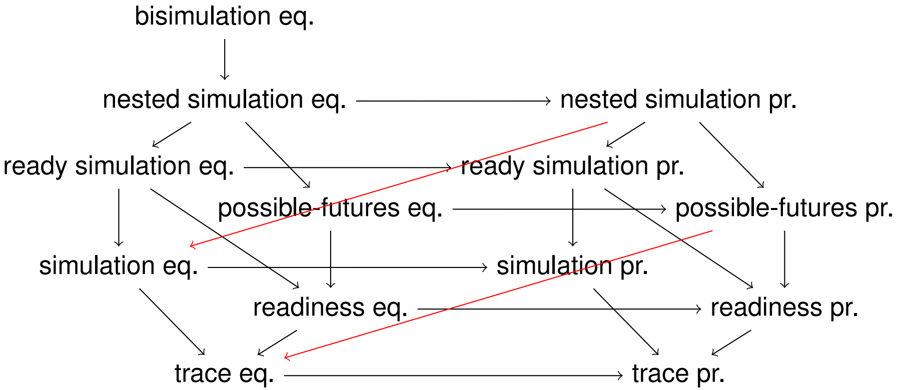
The Linear-Time–Branching-Time Spectrum

van Glabbeek, 2001 (excerpt):

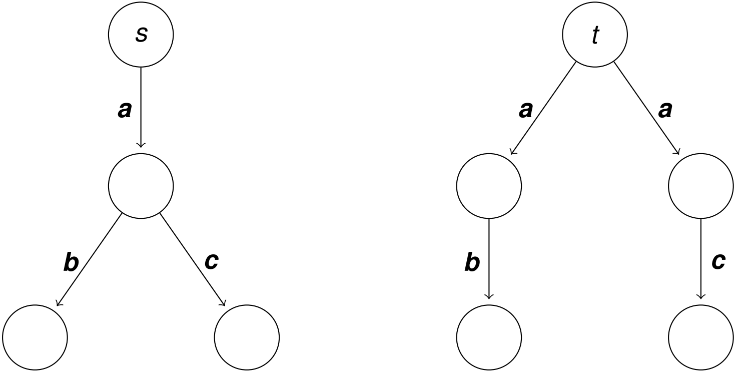


The Linear-Time–Branching-Time Spectrum

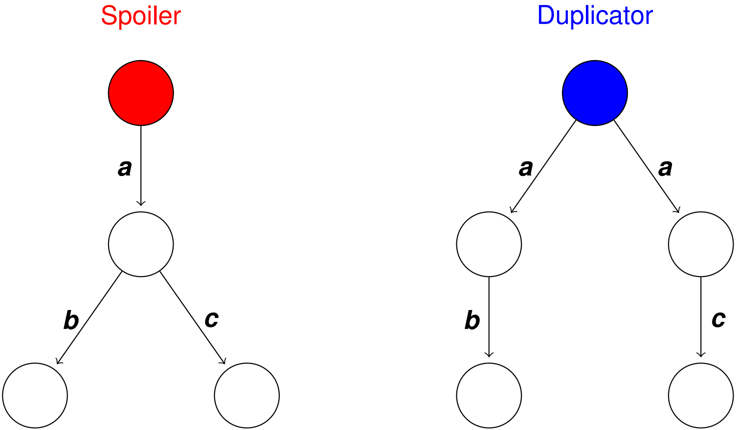
van Glabbeek, 2001 (excerpt):



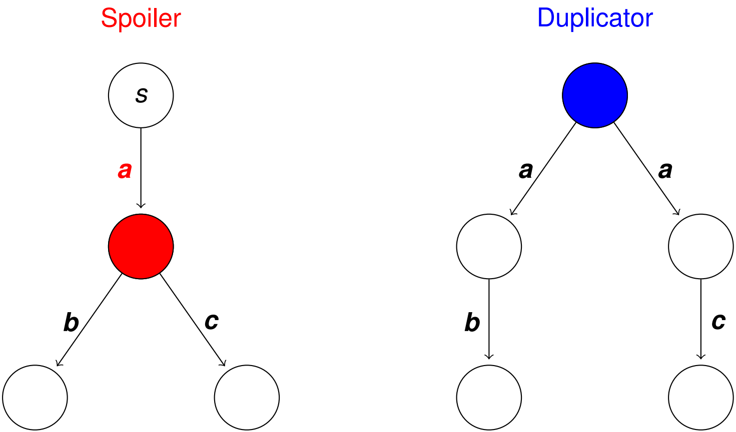
The Simulation Game



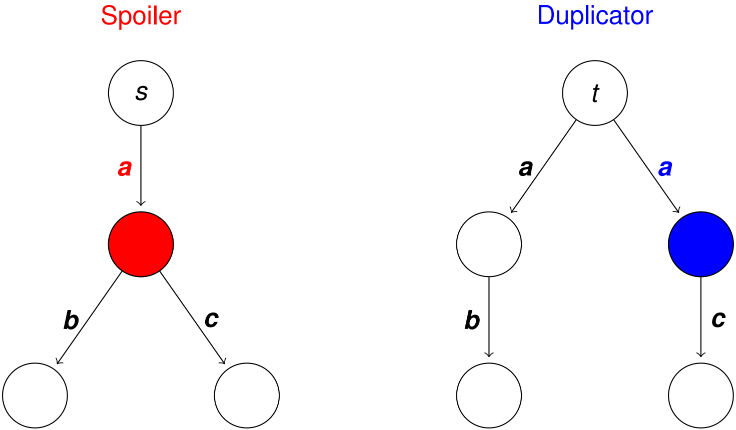
The Simulation Game



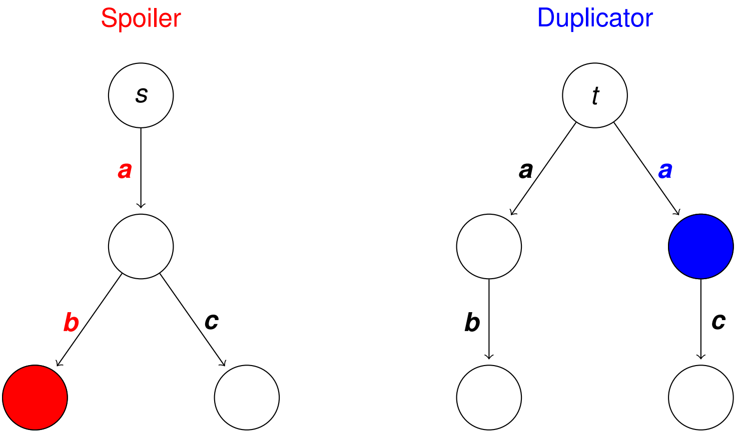
The Simulation Game



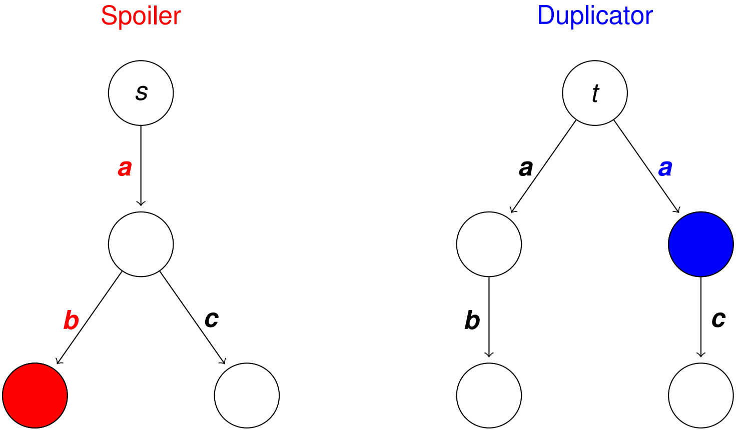
The Simulation Game



The Simulation Game



The Simulation Game



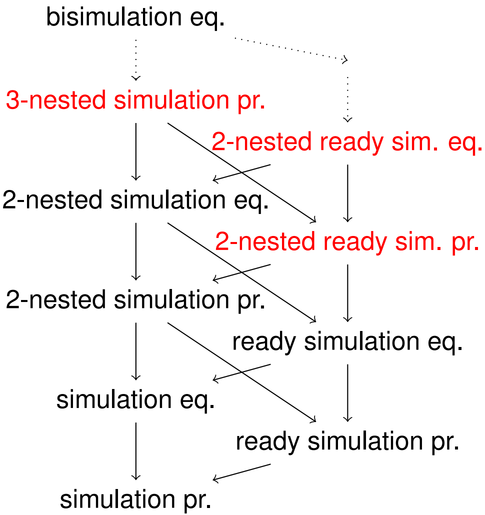
Spoiler wins

The Simulation Game

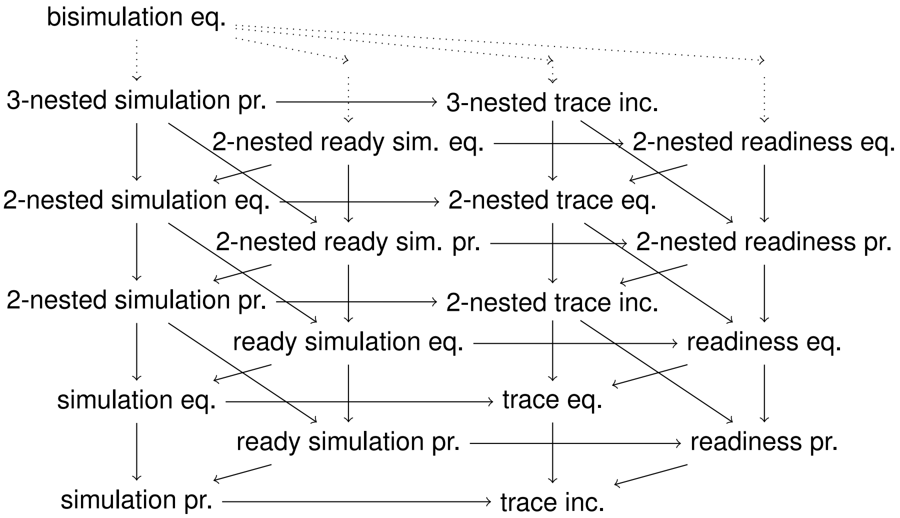
1. Player 1 (“Spoiler”) chooses edge from s (leading to s')
2. Player 2 (“Duplicator”) chooses matching edge from t (leading to t')
3. Game continues from configuration s', t'

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

The Linear-Time–Branching-Time Spectrum, Reordered



The Linear-Time–Branching-Time Spectrum, Reordered



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:

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
- Hence a (hemi)metric $d_T : (\sigma, \tau) \mapsto d_T(\sigma, \tau) \in \mathbb{R}_{\geq 0} \cup \{\infty\}$

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 $d_T(\sigma, \tau)$

This can be done for all the games in the LTBT spectrum.

Quantitative EF Games: The Gory Details – 1

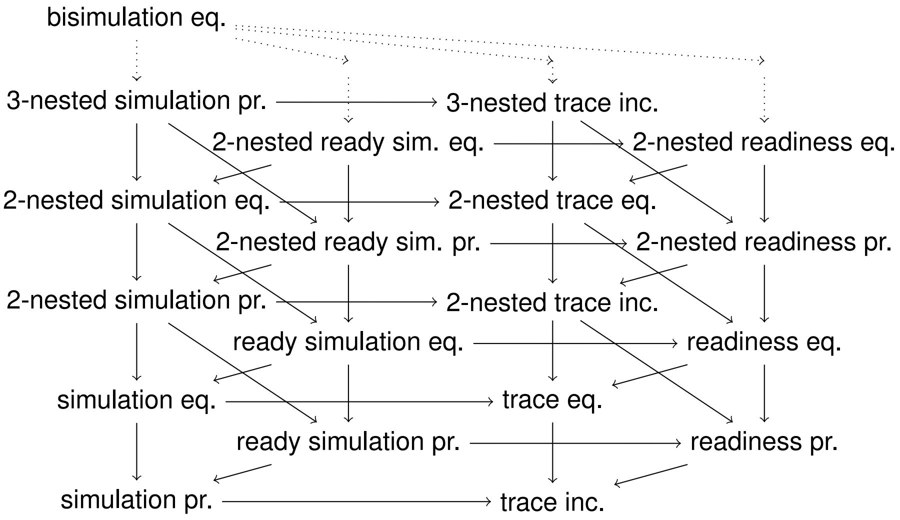
- Configuration of the game: (π, ρ): π the Player-1 choices up to now; ρ the Player-2 choices
- Strategy: mapping from configurations to next moves
  - Θ_i: set of Player-i strategies
- Simulation strategy: Player-1 moves allowed from end of π
- Bisimulation strategy: Player-1 moves allowed from end 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: The Gory Details – 2

- 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 choses edge from end of ρ
  - Θ_1^k: k choices from end of ρ 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

The Quantitative Linear-Time–Branching-Time Spectrum

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



Transfer Principle

- Given two equivalences or preorders in the *qualitative* setting for which there is a *counter-example* which separates them, then the two corresponding distances are topologically inequivalent
- (under certain mild conditions for the trace distance)
- (And the proof uses precisely the same counter-example!)

Recursive Characterization

- 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 formula
- *i.e.* such that $f(\sigma, \tau) = F(\sigma_0, \tau_0, f(\sigma^1, \tau^1))$ for some $F : \Sigma \times \Sigma \times L \to L$ (which is *monotone* in the third coordinate)
- (where $\sigma = \sigma_0 \cdot \sigma^1$ is a split of σ into first element and tail)
- then all distances in the QLTBT are given as least fixed points of some functionals using F

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

Recursive Characterization: Theorem

The endofunction I on $(\mathbb{N}_+ \cup \{\infty\}) \times \{1,2\} \to L^{S\times S}$ defined by

$$I(h_{m,p})(s,t) = \begin{cases} \max\begin{cases} \sup\limits_{s\xrightarrow{x}s'} \inf\limits_{t\xrightarrow{y}t'} F(x,y,h_{m,1}(s',t')) \\ \sup\limits_{t\xrightarrow{y}t'} \inf\limits_{s\xrightarrow{x}s'} F(x,y,h_{m-1,2}(s',t')) \end{cases} & \text{if } m \geq 2, p = 1 \\ \sup\limits_{s\xrightarrow{x}s'} \inf\limits_{t\xrightarrow{y}t'} F(x,y,h_{m,1}(s',t')) & \text{if } m = 1, p = 1 \\ \max\begin{cases} \sup\limits_{t\xrightarrow{y}t'} \inf\limits_{s\xrightarrow{x}s'} F(x,y,h_{m,2}(s',t')) \\ \sup\limits_{s\xrightarrow{x}s'} \inf\limits_{t\xrightarrow{y}t'} F(x,y,h_{m-1,1}(s',t')) \end{cases} & \text{if } m \geq 2, p = 2 \\ \sup\limits_{t\xrightarrow{y}t'} \inf\limits_{st\xrightarrow{x}s'} F(x,y,h_{m,2}(s',t')) & \text{if } m = 1, p = 2 \end{cases}$$

has a least fixed point $h^* : (\mathbb{N}_+ \cup \{\infty\}) \times \{1,2\} \to L^{S\times S}$, and if the LTS (S,T) is finitely branching, then $d^{k\text{-sim}} = g \circ h^*_{k,1}$ for all $k \in \mathbb{N}_+ \cup \{\infty\}$.

Conclusion & Further Work

- We show how to convert any (typically application-given) distance on system traces to (almost) any type of branching distance in the LTBT spectrum
- "Adding an extra dimension to the LTBT spectrum"

- Application to different scenarios (How does it work in concrete cases? Do we get sensible algorithms? Approximations?)
- Application to real-time and hybrid systems
  - Replace "finitely branching" by "compactly branching"?
- Quantitative LTBT with silent moves?
- What about probabilistic systems?