Generic Forward and Backward Simulations

Ichiro Hasuo

Radboud Universiteit Nijmegen

The Netherlands

Radboud University Nijmegen

IN·DEI·NOMINE·FELICITER

Slogan, almost [Vardi]

Everything you can do

I can do “better” with **coalgebras**

- More genericity
- More abstraction
- More fun (for me)

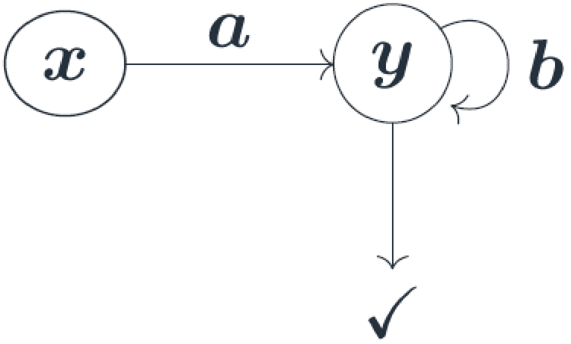
- This work aims at a **generic, coalgebraic** version of

N. Lynch & F. Vaandrager.
Forward and Backward Simulations I. Untimed Systems.
Information and Computation, 1995

Contents

1. Theory of traces and simulations, conventionally
2. Generic theory
   - Forward simulation as
     $$\begin{tikzcd} FX \arrow[r] & FY \\ X \arrow[u] \arrow[r] \arrow[ur, phantom, "\sqsupseteq"] & Y \arrow[u] \end{tikzcd}$$
     - Uniformly for non-determinism and probability
   - Main result: general soundness theorem
3. Illustration of generic theory
4. New application field of coalgebras

Traces, conventionally

- Let's focus on labelled transition systems (LTS)
- Trace = **set of possible linear-time behavior**
- 

$$\mathbf{trace}(x) = \{a\checkmark, ab\checkmark, abb\checkmark, \ldots\}$$

better captured by our coalgebraic framework

- Disclaimer:

  In this work we only work with **finite** traces

Simulations, conventionally

- Two systems: $\mathcal{S}$ and $\mathcal{T}$
- R : a relation between state spaces
  - R is a **forward simulation** if

$$\begin{tikzcd} x \arrow[r, "a"] \arrow[d, dash, dashed, "R"'] & x' \\ y & \end{tikzcd} \quad \text{implies} \quad \begin{tikzcd} x \arrow[r, "a"] \arrow[d, dash, dashed, "R"'] & x' \arrow[d, dash, dashed, "R"] \\ y \arrow[r, "a"] & \exists y' \end{tikzcd}$$

  - R is a **backward simulation** if

$$\begin{tikzcd} x \arrow[r, "a"] & x' \arrow[d, dash, dashed, "R"] \\ & y' \end{tikzcd} \quad \text{implies} \quad \begin{tikzcd} x \arrow[r, "a"] \arrow[d, dash, dashed, "R"'] & x' \arrow[d, dash, dashed, "R"] \\ \exists y \arrow[r, "a"] & y' \end{tikzcd}$$

Soundness theorem

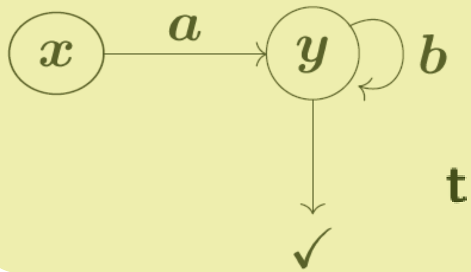
$\exists$ forward/backward simulation

$\Rightarrow$ trace inclusion

Summary:
theory of traces and simulations

We have reviewed:

- Traces



$$\mathsf{trace}(x) = \{a\checkmark,\ ab\checkmark,\ abb\checkmark,\ \dots\}$$

- Forward/backward simulations

$$\begin{tikzcd} x \arrow[r, "a"] \arrow[d, dash, dashed, "R"'] & x' \\ y & \end{tikzcd} \quad \Rightarrow \quad \begin{tikzcd} x \arrow[r, "a"] \arrow[d, dash, dashed, "R"'] & x' \arrow[d, dash, dashed, "R"] \\ y \arrow[r, "a"] & \exists y' \end{tikzcd}$$

- Soundness theorem

Contents

1. Theory of traces and simulations, conventionally
2. Generic theory
   - Forward simulation as

$$\begin{tikzcd} FX \arrow[r] & FY \\ X \arrow[u] \arrow[r] \arrow[ur, phantom, "\sqsupseteq"] & Y \arrow[u] \end{tikzcd}$$

     - Uniformly for non-determinism and probability
   - Main result: general soundness theorem
3. Illustration of generic theory
4. New application field of coalgebras

Traces and simulations, coalgebraically

System	$\begin{tikzcd} FX \\ X \arrow[u] \end{tikzcd}$
Trace semantics	$\begin{tikzcd} FX \arrow[r, dashed] & FZ \\ X \arrow[u] \arrow[r, dashed, "\textbf{trace}"'] \arrow[ur, phantom, "="] & Z \arrow[u, "\cong"', "\text{final}"] \end{tikzcd}$
Contribution! Simulations	$\begin{tikzcd} FX \arrow[r] & FY \\ X \arrow[u] \arrow[r] \arrow[ur, phantom, "\sqsupseteq"] & Y \arrow[u] \end{tikzcd}$ Contribution! $\begin{tikzcd} FX \arrow[r] & FY \\ X \arrow[u] \arrow[r] \arrow[ur, phantom, "\sqsubseteq"] & Y \arrow[u] \end{tikzcd}$ **backward** sim.

in $\mathcal{K}\ell(T)$

Main result: General soundness theorem

Systems, coalgebraically

A system is $\begin{array}{c} FX \\ \uparrow \\ X \end{array}$ in $\mathcal{K}\ell(T)$

coalgebra!

“Kleisli” category

- Such as
  - LTS
  - Generative probabilistic systems
  - etc.
- [Power&Turi CTCS’99] [Jacobs CMCS’04]

Traces, coalgebraically

Trace semantics is by **coinduction**

$$\begin{tikzcd}
FX \arrow[r, dashed] & FZ \\
X \arrow[u] \arrow[r, dashed, "\mathsf{trace}"'] \arrow[ur, phantom, "="] & Z \arrow[u, "\cong"', "\mathsf{final}"]
\end{tikzcd}$$

in $\mathcal{K}\ell(T)$

- [IH, Jacobs & Sokolova, CMCS'06]

Simulations, coalgebraically [This work]

- A **forward simulation** is
$$\begin{tikzcd} FX \arrow[r, "FR"] & FY \\ X \arrow[u] \arrow[r, "R"'] \arrow[ur, phantom, "\sqsupseteq"] & Y \arrow[u] \end{tikzcd}$$
in $\mathcal{K}\ell(T)$

lax morphism of coalgebras

- A **backward simulation** is
$$\begin{tikzcd} FX \arrow[r, "FR"] & FY \\ X \arrow[u] \arrow[r, "R"'] \arrow[ur, phantom, "\sqsubseteq"] & Y \arrow[u] \end{tikzcd}$$
in $\mathcal{K}\ell(T)$

oplax morphism of coalgebras

Cf.

$$\begin{tikzcd} \bullet \arrow[r] & \bullet \\ \bullet \arrow[u] \arrow[r] \arrow[ur, phantom, "="] & \bullet \arrow[u] \end{tikzcd}$$
morphism

$$\begin{tikzcd} \bullet \arrow[r] & \bullet \\ \bullet \arrow[u] \arrow[r] \arrow[ur, phantom, "\sqsupseteq"] & \bullet \arrow[u] \end{tikzcd}$$
lax morphism

$$\begin{tikzcd} \bullet \arrow[r] & \bullet \\ \bullet \arrow[u] \arrow[r] \arrow[ur, phantom, "\sqsubseteq"] & \bullet \arrow[u] \end{tikzcd}$$
oplax morphism

Main result: general soundness theorem

$$\begin{tikzcd} FX \arrow[r] & FY \\ X \arrow[u] \arrow[r] \arrow[ur, phantom, "\sqsupseteq"] & Y \arrow[u] \end{tikzcd}$$

$\exists$ forward/backward simulation

$\Rightarrow$ trace inclusion

- Also completeness result:

  trace inclusion $\Rightarrow$ $\exists$ a hybrid simulation

Traces and simulations coalgebraically

Parameter F :
for **transition-type**

System	$\begin{array}{c} FX \\ \uparrow \\ X \end{array}$
Trace semantics	$\begin{array}{ccc} FX & \dashrightarrow & FZ \\ \uparrow & = & \cong \uparrow \text{final} \\ X & \underset{\textbf{trace}}{\dashrightarrow} & Z \end{array}$
Simulations	$\begin{array}{ccc} FX & \longrightarrow & FY \\ \uparrow & \sqsupseteq & \uparrow \\ X & \longrightarrow & Y \end{array}$ **forward** sim. $\quad \begin{array}{ccc} FX & \longrightarrow & \\ \uparrow & & \\ X & \longrightarrow & \end{array}$ **backward** sim.

in $\mathcal{K}\ell(T)$

Parameter T :
for **branching-type**

Main result: General soundness theorem

Genericity

T and F

By changing parameters, the framework covers

- different **branching-types** by different T
  - non-determinism
  - probabilistic branching
- different **transition-types** by different F
  - LTS: $x \mapsto (a, x')$
  - Context-free grammar: $x \mapsto \langle \text{“}\neg\text{”}, x \rangle$

    $x \mapsto \langle x, \text{“}\wedge\text{”}, x \rangle$

Significance of soundness thm

Scenario: verification by finding a simulation

$\mathcal{S}$ **Specification** automaton
- Simple
- Known to satisfy desired properties

$\mathcal{I}$ **Implementation** automaton
- Complex
- Questioned to satisfy desired properties

Goal: $\mathcal{I}$ satisfies a **safety** property $\boldsymbol{P}$

- $\mathcal{S}$ satisfies $\boldsymbol{P}$
- **trace(** $\mathcal{I}$ **)** $\subseteq$ **trace(** $\mathcal{S}$ **)**

Soundness theorem

$\exists$ forward/backward simulation from $\mathcal{I}$ to $\mathcal{S}$

Practical implication, an envisaged scenario

- Given an (exotic) kind of systems,
  - Whether non-deterministic or probabilistic
  - No idea what is an appropriate def. of simulations
- Instantiate $$\begin{tikzcd} FX \arrow[r] & FY \\ X \arrow[u] \arrow[r] \arrow[ur, phantom, "\sqsupseteq"] & Y \arrow[u] \end{tikzcd}$$ in $\mathcal{K}\ell(T)$
  - We obtain def. of fwd/bwd simulations

Soundness thm. comes **for free**

- In particular, a move: non-det. $\Rightarrow$ prob.

  is trivial by changing a parameter.

Contents

1. Theory of traces and simulations, conventionally
2. Generic theory
   - Forward simulation as

$$\begin{tikzcd} FX \arrow[r] & FY \\ X \arrow[u] \arrow[r] \arrow[ur, phantom, "\sqsupseteq"] & Y \arrow[u] \end{tikzcd}$$

     - Uniformly for non-determinism and probability
   - Main result: general soundness theorem
3. Illustration of generic theory
4. New application field of coalgebras

Parameters

F: a functor
for **transition-type**

A system is: $\begin{array}{c} FX \\ \uparrow \\ X \end{array}$ in $\mathcal{K}\ell(T)$

T: a monad
for **branching-type**

- T is a **monad**, for branching-type. Examples:
  - $\mathcal{P}$, powerset monad
    - for non-determinism
  - $\mathcal{D}$, subdistribution monad
    - for (generative) probabilistic branching

$$\begin{aligned} \mathcal{D}X &= \{\text{probability subdistributions on } X\} \\ &= \{d : X \to [0,1] \mid \sum_{x \in X} d(x) \le 1\} \end{aligned}$$

Parameters

A system is: $\begin{array}{c} FX \\ \uparrow \\ X \end{array}$ in $\mathcal{K}\ell(T)$

$$\frac{\begin{array}{c} FX \\ \uparrow \\ X \end{array} \text{ in } \mathcal{K}\ell(T)}{\begin{array}{c} TFX \\ \uparrow \\ X \end{array}\text{, a function}}$$

A category where **branching** is implicit

$\mathcal{K}\ell(T)$: the **Kleisli** category for T

- Main point: for T = $\mathcal{P}$,

$$\frac{X \longrightarrow Y \text{ in } \mathcal{K}\ell(\mathcal{P})}{X \longrightarrow \mathcal{P}Y\text{, a function}}$$

$$x \longmapsto \{y_1, y_2, \ldots\}$$

Parameters

A system is: $\begin{array}{c} FX \\ \big\uparrow \\ X \end{array}$ in $\mathcal{K}\ell(T)$

$$\overline{\overline{\qquad\qquad\qquad\qquad}}$$

$\begin{array}{c} TFX \\ \big\uparrow \\ X \end{array}$, a function

branching-type:
non-determinism

- T = $\mathcal{P}$, F = 1 + Σ × -

transition-type:
terminate or (output, next)

$\begin{array}{c} \mathcal{P}(1 + \Sigma \times X) \\ \big\uparrow \\ X \end{array}$ such as $\begin{array}{c} \{\checkmark,\ (a_1, x_1),\ (a_2, x_2)\} \\ \big\uparrow \\ x \end{array}$

$x \rightarrow \checkmark$
$x \xrightarrow{a_1} x_1$
$x \xrightarrow{a_2} x_2$

LTS with explicit termination

Parameters

A system is: $\dfrac{\boldsymbol{X} \to \boldsymbol{FX} \text{ in } \mathcal{K}\ell(\boldsymbol{T})}{\boldsymbol{X} \to \boldsymbol{TFX}\text{, a function}}$

- T = $\mathcal{P}$, F = 1 + Σ × -

  LTS with explicit termination
- T = $\mathcal{D}$, F = 1 + Σ × -

  Generative probabilistic system
- T = $\mathcal{P}$, F = (Σ + -)*

  Context-free grammar

Trace semantics [IH, Jacobs, Sokolova. CMCS'06]

1. $\exists$ final coalgebra $\begin{array}{c} FZ \\ \cong\uparrow \\ Z \end{array}$ in $\mathcal{K}\ell(T)$

For any system $\begin{array}{c} FX \\ \uparrow \\ X \end{array}$, $\exists! f$ such that

$$\begin{tikzcd} FX \arrow[r, dashed, "Ff"] & FZ \\ X \arrow[u] \arrow[r, dashed, "f"'] \arrow[ur, phantom, "="] & Z \arrow[u, "\cong"] \end{tikzcd}$$

domain of traces, e.g. Σ^*

2. This f "induced by coinduction" gives finite trace semantics

Forward simulation

$$\begin{tikzcd} FX \arrow[r, "FR"] & FY \\ X \arrow[u, "c"] \arrow[r, "R"'] \arrow[ur, phantom, "\sqsupseteq"] & Y \arrow[u, "d"'] \end{tikzcd}$$

in $\mathcal{K}\ell(T)$

Take T=$\mathcal{P}$

R : a **relation**, because

$\longrightarrow Y$ in $\mathcal{K}\ell(\mathcal{P})$

$\longrightarrow \mathcal{P}Y$, a function

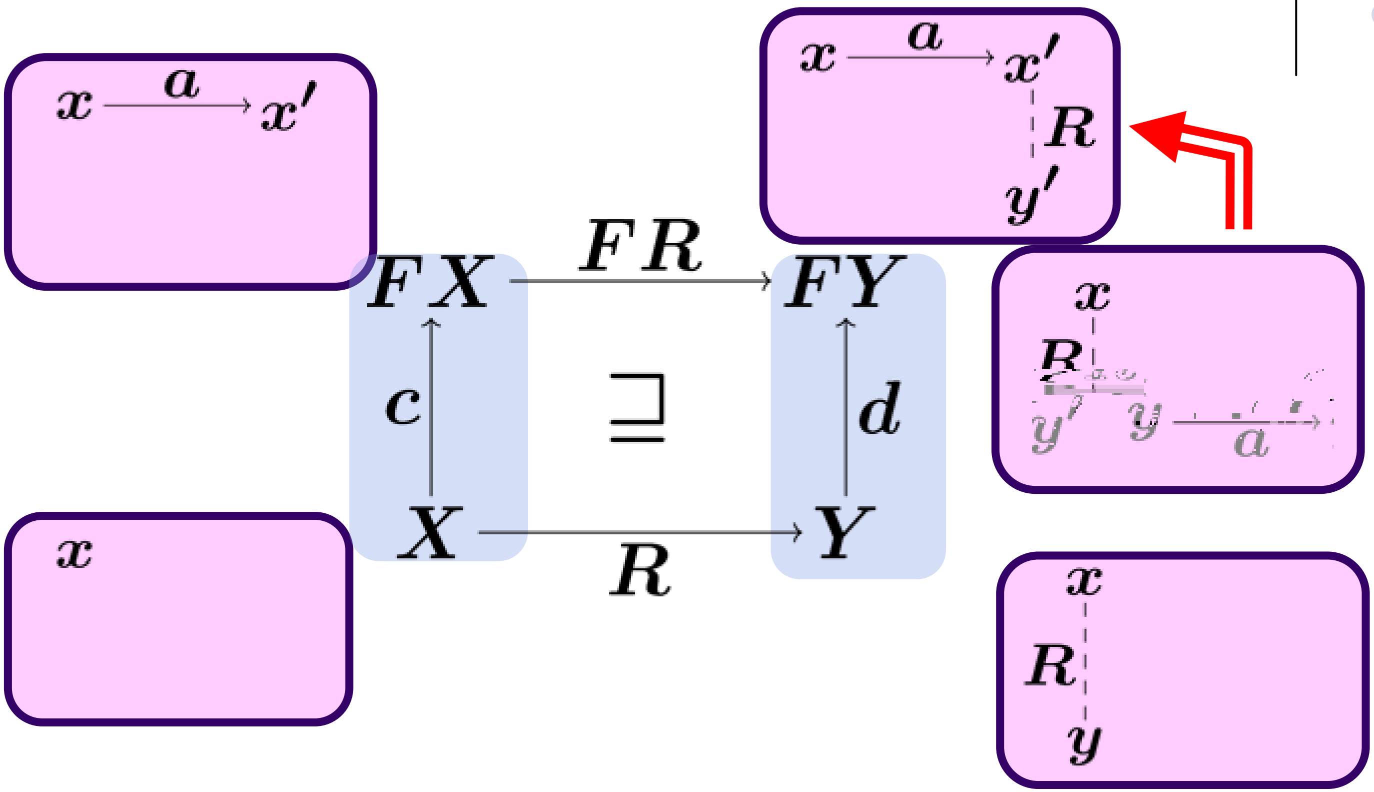
$X \times Y$, a relation

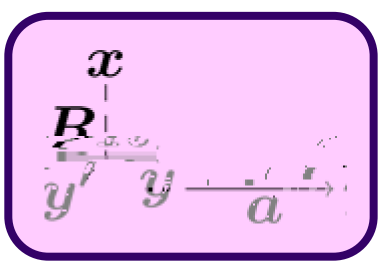
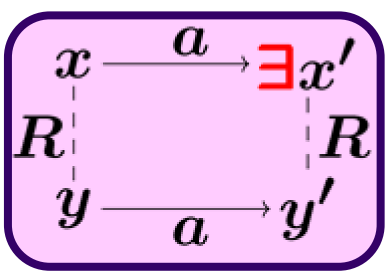
$\sqsupseteq$ refers to “pointwise inclusion”:

$$\begin{tikzcd} X \arrow[r, bend left, "FR \circ c"] \arrow[r, bend right, "d \circ R"'] \arrow[r, phantom, "\sqsupseteq"] & \mathcal{P}FY \end{tikzcd} \quad \text{in } \mathbf{Sets}$$

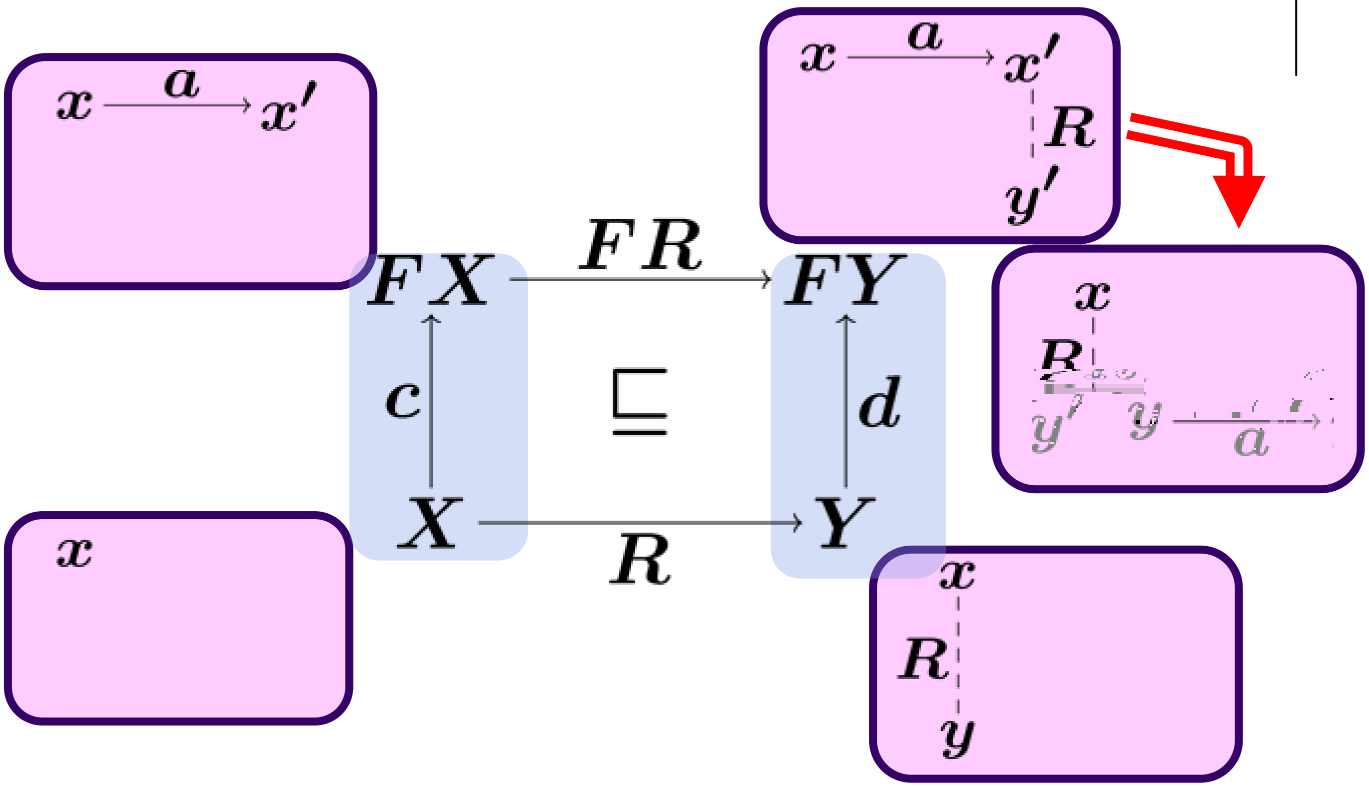
(cf. **Dcpo**-enriched structure of $\mathcal{K}\ell(T)$)

Forward simulation

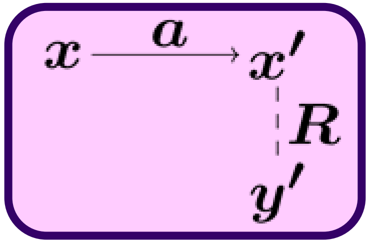


Hence  implies 

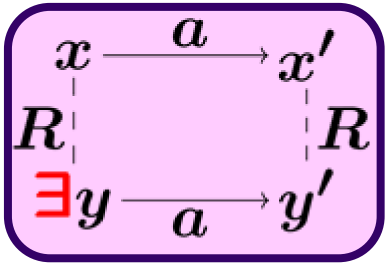
Backward simulation



Hence



implies



Main result: general soundness theorem

$$\begin{tikzcd} FX \arrow[r] \arrow[dr, phantom, "\sqsupseteq"] & FY \\ X \arrow[u] \arrow[r] & Y \arrow[u] \end{tikzcd}$$

$\exists$ forward/backward simulation

$\Longrightarrow$ trace inclusion

Proof.

$$\begin{tikzcd} FX \arrow[r] \arrow[rr, bend left, dashed] \arrow[dr, phantom, "\sqsupseteq"] & FY \arrow[r, dashed] \arrow[dr, phantom, "="] & FZ \\ X \arrow[u] \arrow[r] \arrow[rr, bend right, dashed] & Y \arrow[u] \arrow[r, dashed] & Z \arrow[u, "\cong", "\mathrm{final}"'] \end{tikzcd} \quad \text{in } \mathcal{K}\ell(T)$$

- Also completeness result, as easily

Summary:
we have illustrated

System	$\begin{tikzcd} FX \\ X \arrow[u] \end{tikzcd}$
Trace semantics	$\begin{tikzcd} FX \arrow[r, dashed] & FZ \\ X \arrow[u] \arrow[r, dashed, "\textbf{trace}"'] \arrow[ur, phantom, "="] & Z \arrow[u, "\cong"', "\text{final}"] \end{tikzcd}$
Simulations	$\begin{tikzcd} FX \arrow[r] & FY \\ X \arrow[u] \arrow[r] \arrow[ur, phantom, "\sqsupseteq"] & Y \arrow[u] \end{tikzcd}$ **forward** sim. $\begin{tikzcd} FX \arrow[r] & FY \\ X \arrow[u] \arrow[r] \arrow[ur, phantom, "\sqsubseteq"] & Y \arrow[u] \end{tikzcd}$ **backward** sim.

in $\mathcal{K}\ell(T)$

Main result: General soundness theorem

In the paper, we have

- More details on examples
- More technical details
  - **DCpo**-enriched structure of $\mathcal{K}\ell(T)$

$$\begin{tikzcd} \bullet \arrow[r, bend left, "f"] \arrow[r, bend right, "g"'] \arrow[r, phantom, "\sqsubseteq"] & \bullet \end{tikzcd}$$

: ***g*** yields **more** behavior than ***f***

  - Explicit start states: a system is actually

$$\begin{array}{c} FX \\ \uparrow \\ X \\ \uparrow \\ 1 \end{array}$$

- An extended version is available:

http://www.cs.ru.nl/~ichiro

Contents

1. Theory of traces and simulations, conventionally
2. Generic theory
   - Forward simulation as

$$\begin{tikzcd} FX \arrow[r] \arrow[dr, phantom, "\sqsupseteq"] & FY \\ X \arrow[u] \arrow[r] & Y \arrow[u] \end{tikzcd}$$

     - Uniformly for non-determinism and probability
   - Main result: general soundness theorem
3. Illustration of generic theory
4. New application field of coalgebras

Interpretation of coalgebraic notions

underlying category	in **Sets** e.g.[Rutten'00]	in $\mathcal{K}\ell(T)$
captured process semantics	bisimilarity	trace semantics
coalgebra $\begin{array}{c} FX \\ \uparrow \\ X \end{array}$	a system	a system
by coinduction $\begin{array}{ccc} FX & \dashrightarrow & FZ \\ \uparrow & = & \cong\uparrow\text{final} \\ X & \underset{\text{beh}}{\dashrightarrow} & Z \end{array}$	behavior modulo bisimilarity	trace semantics [Power&Turi'99] [IH,Jacobs,Sokolova'06]
morphism of coalg. $\begin{array}{ccc} FX & \longrightarrow & FY \\ \uparrow & = & \uparrow \\ X & \longrightarrow & Y \end{array}$	functional bisimulation	lax : **forward sim.** oplax : **backward sim.** [current work]

Process theory in categorical/algebraic/coalgebraic terms

• Bisimulation	[Rutten, TCS'02]
• Traces and simulations, as in [Lynch&Vaandrager'95]	[Power&Turi, CTCS'99]
	[IH,Jacobs&Sokolova,CMCS'06]
	[IH, CONCUR'06]
• Modal logic	[Bonsangue&Kurz, FOSSACS'06]
	[Cirstea&Pattinson, CONCUR'04]
	[Schroeder, FOSSACS'06]
• Process algebra and SOS	[Turi&Plotkin, LICS'97]
	[Bartels, CMCS'02]
	[Klin, invited talk at EXPRESS'06]
• Probabilistic system	[Sokolova, VOSS'04]
• Testing semantics, LT-BT spec.	[Klin&Sobocinski, CONCUR'03]
	[Pavlovic,M AMAST'

More fun for us

Everything we can do, we can do "better" with **coalgebras**

Future work: applicational side

- Generalization of simulation-based verification tools such as IOA toolkit [Garland,Lynch&Vaziri'97]
- More examples
  - Now **non-det.** $\Rightarrow$ **prob.** is trivial
  - E.g. probabilistic ver. of **anonymity simulations** [Kawabe,Mano,Sakurada&Tsukada,'06] (Ongoing)

Future work: theoretical side

- Infinite traces
- Internal actions

in [Lynch&Vaandrager'95]

but not in our paper

preliminary results by IH

- Linear-time logic

ongoing by Kurz & IH

- Process algebra and compositionality
- Combination of **both** non-det. and probability
  - A lot of bad things occur

    [Varacca&Winskel,LICS'02]

    [Cheung, PhD Thesis]

preliminary results by Jacobs & Sokolova

Conclusion

- (Part of) [Lynch&Vaandrager'95] is done coalgebraically
  - Forward simulation as

$$\begin{tikzcd} FX \arrow[r, "FR"] & FY \\ X \arrow[u, "c"] \arrow[r, "R"'] \arrow[ur, phantom, "\sqsupseteq"] & Y \arrow[u, "d"'] \end{tikzcd}$$

  - General soundness theorem
- Genericity
  - Non-det. or probabilistic
- Practical implication envisaged
- Lots of topics to be worked out

Thank you for your attention!

Contact: Ichiro Hasuo

http://www.cs.ru.nl/~ichiro

Everything we can do, we can do "better" with **coalgebras**