Ichiro Hasuo
Tracing Anonymity with Coalgebras
The ultimate aim

Better mathematical understanding of computer systems

Computer systems

- pervasive, important
- fail easily
- ...
- we don't quite understand them!
Coalgebras

Our mathematical presentation of systems

Good balance:

- mathematical simplicity
- (potential) applicability

In this thesis:

- more applications are found
- further mathematical theory is developed
### Coalgebras

<table>
<thead>
<tr>
<th>System</th>
<th>Coalgebraically</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>$FX \xrightarrow{c} X$</td>
</tr>
<tr>
<td></td>
<td>$FX \xrightarrow{d} FY$</td>
</tr>
<tr>
<td></td>
<td>$FX \xrightarrow{f} Y$</td>
</tr>
<tr>
<td></td>
<td>$FX \xrightarrow{Ff} FY$</td>
</tr>
<tr>
<td>Behavior-preserving map</td>
<td>Morphism of coalgebras</td>
</tr>
<tr>
<td></td>
<td>$FX \xrightarrow{f} Y$</td>
</tr>
<tr>
<td></td>
<td>$FX \xrightarrow{Ff} FY$</td>
</tr>
<tr>
<td></td>
<td>$FX \xrightarrow{d} FY$</td>
</tr>
<tr>
<td>Behavior</td>
<td>By final coalgebra</td>
</tr>
<tr>
<td></td>
<td>$FX \xrightarrow{c} X$</td>
</tr>
<tr>
<td></td>
<td>$FX \xrightarrow{Ff} FY$</td>
</tr>
<tr>
<td></td>
<td>$FX \xrightarrow{d} FY$</td>
</tr>
<tr>
<td></td>
<td>$FX \xrightarrow{final} Z$</td>
</tr>
</tbody>
</table>

**Hasuo and Coalgbras**

Ichiro Hasuo, Tracing Anonymity with Coalgebras
Overview

**Coalgebraic theory of traces and simulations** (Ch. 2-3)
- via coalgebras in a Kleisli category
- apply to both
  - non-determinism
  - probability
- case study: probabilistic anonymity (Ch. 4)

**Concurrency** in coalgebras (Ch. 5)
- the microcosm principle appears
In $\text{Sets}$: bisimilarity

- what they mean exactly depends on **which category** they're in

- they are in the category $\text{Sets}$
- “behavior” captures **bisimilarity**
Bisimilarity vs. trace semantics

Also captured by final coalgebra?

Bisimilarity

When do we decide or ?

Trace semantics

Anyway we get or
Coalgebraic trace semantics

Behavior by final coalgebra

```
FX --------→ FZ
  c↑        ↑final
X beh(c) → Z
```

captures...

“Kleisli category”

- a category where branching is implicit
  - \( X \to Y \): “branching function” from \( X \) to \( Y \)
  - \( T \): parameter for branching-type

in \( \text{Sets} \)

bisimilarity (standard)

\[ \neq \]

in \( \text{Kl}(T) \)

trace semantics (Ch. 2)

\[ = \]
Different “branching-types”

\[ F \xrightarrow{X} \overset{c}{\longrightarrow} FZ \]

in \( K1(T) \) captures trace semantics

- **Trace Semantics:** \( a \rightarrow b \)
- **Trace Semantics:** \( a \rightarrow c \)

\( T \) : parameter for “branching-types”

- **Trace Semantics:** \( a \rightarrow b : 1/3 \)
- **Trace Semantics:** \( a \rightarrow c : 2/3 \)

**Non-deterministic branching**

- **Trace Semantics:** \( a \rightarrow b \)
- **Trace Semantics:** \( a \rightarrow c \)

**Probabilistic branching**

- **Trace Semantics:** \( a \rightarrow b : 1/3 \)
- **Trace Semantics:** \( a \rightarrow c : 2/3 \)
Coalgebraic simulations (Ch. 3)

- **Morphism of coalgebras** in \( \text{Sets} \)
- **Functional bisimulation (standard)**
- **Genericity again**: both for
  - \( T = \mathcal{P} \) (non-determinism)
  - \( T = \mathcal{D} \) (probability)

**Observation**

- Lax morphism = forward simulation

**Theorem (Soundness)**

- \( \exists \) fwd/bwd simulation \( \Rightarrow \) trace inclusion
**Summary**

<table>
<thead>
<tr>
<th></th>
<th>in Sets</th>
<th>in $\mathbf{Kl}(T)$</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>coalgebra</strong></td>
<td>system</td>
<td>system</td>
</tr>
<tr>
<td><strong>morphism of coalgebra</strong></td>
<td>functional bisimilarity</td>
<td>forward simulation (lax)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>backward simulation (oplax)</td>
</tr>
<tr>
<td><strong>by final coalgebra</strong></td>
<td>bisimilarity</td>
<td>trace semantics</td>
</tr>
</tbody>
</table>

- **genericity**: both for $T = \mathcal{P}$ (non-determinism)
- $T = \mathcal{D}$ (probability)

---

**Functional Bisimilarity**

- $\mathcal{F}X \xrightarrow{f} \mathcal{F}Y$
- $\mathcal{X} \xrightarrow{f} \mathcal{Y}$

---

**Trace Semantics**

- $\mathcal{F}X \xrightarrow{\text{final}} \mathcal{F}Z$
- $\mathcal{X} \xrightarrow{\text{beh}(c)} \mathcal{Z}$

---

**Ch. 2** Theory of Bisimilarity

**Ch. 3** Theory of Traces and Simulations
Case study: probabilistic anonymity (Ch. 4)

Simulation-based proof method for non-deterministic anonymity
[KeawabeMST06]

generic, coalgebraic theory of traces and simulations
[Ch. 2-3]

Simulation-based proof method for probabilistic anonymity

$T = \mathcal{P}$

$T = \mathcal{D}$
Concurrency

“concurrency”, “behavior”

running $C$ and $D$ in parallel

2-dimensional, nested algebraic structure

$\text{Coalg}_F \times \text{Coalg}_F \rightarrow \text{Coalg}_F$

$Z \times Z \rightarrow Z$

the microcosm principle
Concurrency and the microcosm principle (Ch. 5)

The Microcosm Principle and Concurrency in Coalgebra
IH, Bart Jacobs & Ana Sokolova
To appear in Proc. FoSSaCS 2008
LNCS
## Summary

<table>
<thead>
<tr>
<th>Coalgebraic theory of traces and simulations (Ch. 2-3)</th>
</tr>
</thead>
<tbody>
<tr>
<td>• via coalgebras in a Kleisli category</td>
</tr>
<tr>
<td>• apply to both</td>
</tr>
<tr>
<td>• non-determinism</td>
</tr>
<tr>
<td>• probability</td>
</tr>
<tr>
<td>• case study:</td>
</tr>
<tr>
<td>probabilistic anonymity (Ch. 4)</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Concurrency in coalgebras (Ch. 5)</th>
</tr>
</thead>
<tbody>
<tr>
<td>• the microcosm principle appears</td>
</tr>
</tbody>
</table>

Summary

- Coalgebraic theory of traces and simulations (Ch. 2-3):
  - via coalgebras in a Kleisli category
  - apply to both
    - non-determinism
    - probability
  - case study: probabilistic anonymity (Ch. 4)

- Concurrency in coalgebras (Ch. 5):
  - the microcosm principle appears