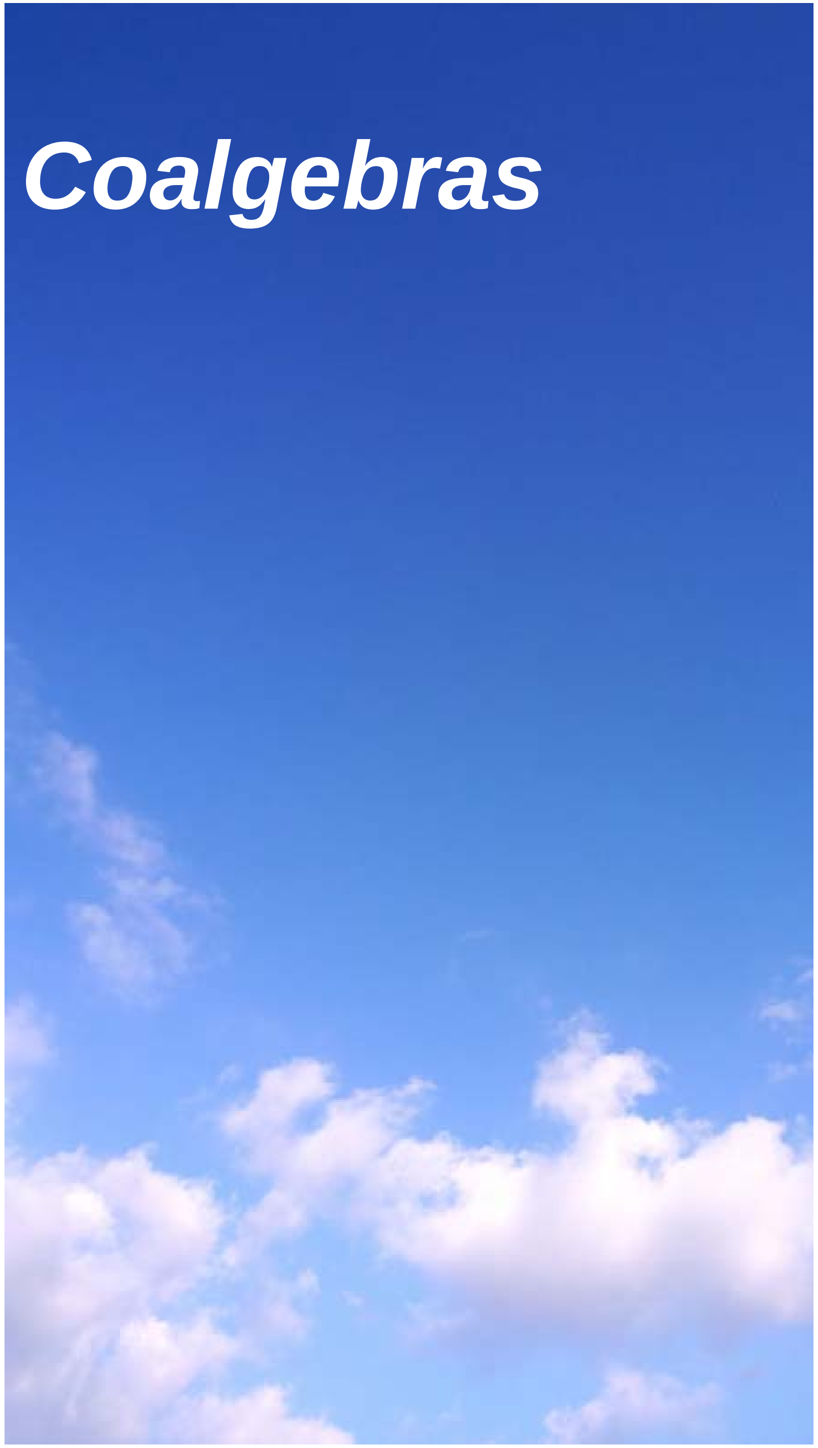
Ichiro Hasuo

Tracing Anonymity with Coalgebras

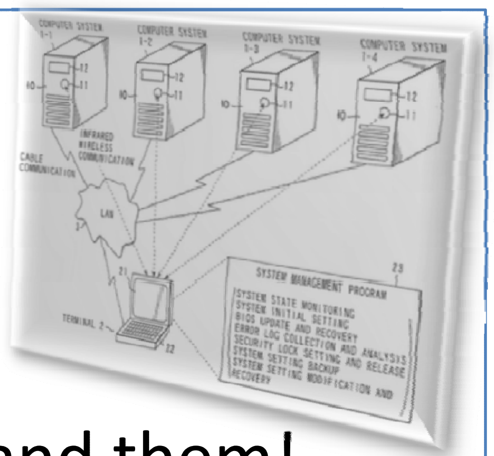


The ultimate aim

Better mathematical understanding of computer systems

Computer systems

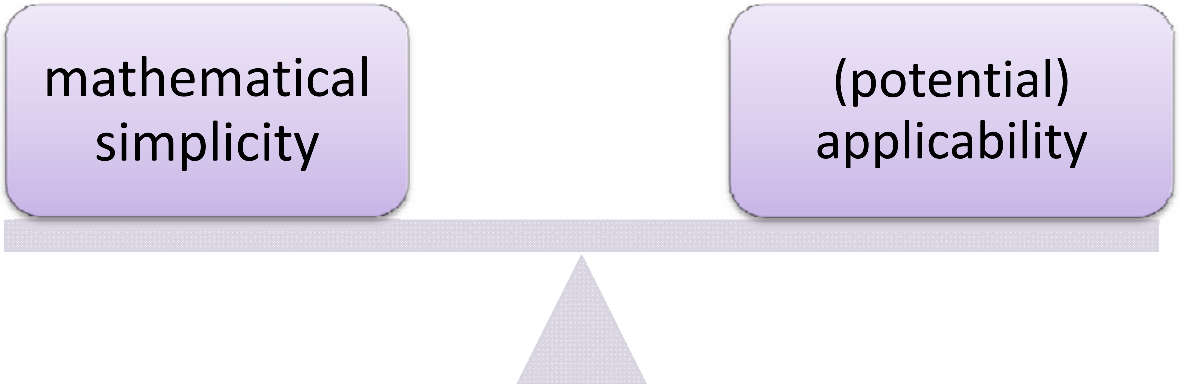
- pervasive, important
- fail easily
- …
- we don't quite understand them!



Coalgebras

Our mathematical presentation of systems

Good balance:



In this thesis:

- more applications are found
- further mathematical theory is developed

Coalgebras

	coalgebraically	
system	coalgebra	$\begin{array}{c} FX \\ \uparrow \\ X \end{array}$
behavior-preserving map	morphism of coalgebras	$\begin{array}{ccc} FX & \xrightarrow{Ff} & FY \\ {\scriptstyle c}\uparrow & & \uparrow{\scriptstyle d} \\ X & \xrightarrow[f]{} & Y \end{array}$
behavior	by final coalgebra	$\begin{array}{ccc} FX & \dashrightarrow & FZ \\ {\scriptstyle c}\uparrow & & \uparrow\text{final} \\ X & \underset{\mathsf{beh}(c)}{\dashrightarrow} & Z \end{array}$

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 Sets*: bisimilarity*

system as coalgebra	behavior by final coalgebra
$\begin{array}{c} FX \\ \uparrow \\ X \end{array}$	$\begin{tikzcd} FX \arrow[r, dashed] & FZ \\ X \arrow[u, "c"] \arrow[r, dashed, "\mathsf{beh}(c)"'] & Z \arrow[u, "\text{final}"'] \end{tikzcd}$

NB

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

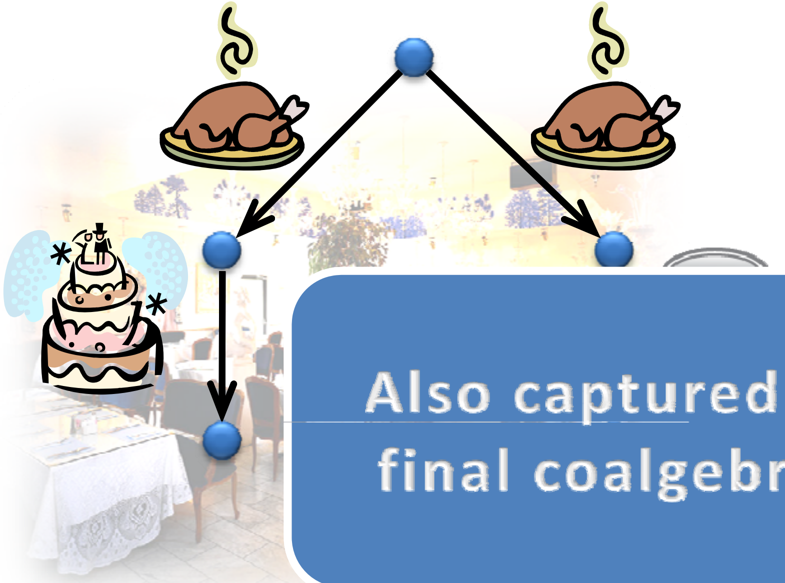
category = "universe"
Sets, Top, Stone, Vect, CLat, …

standard

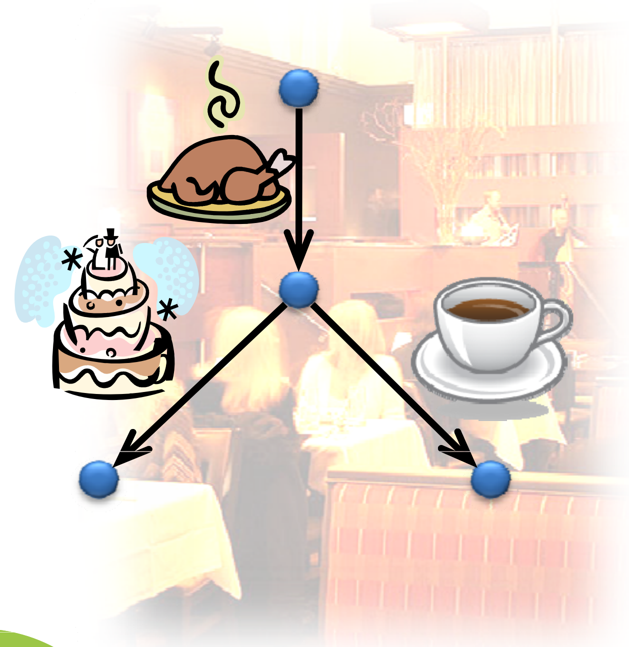
- they are in the category Sets
- "behavior" captures **bisimilarity**

$X, FX, FZ, \ldots$	sets
$X \to Y$	function

Bisimilarity vs. trace semantics



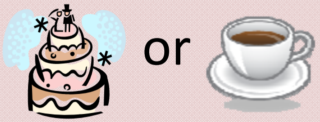
$\neq$



Also captured by final coalgebra?

Bisimilarity

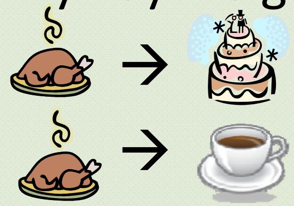
When do we decide



or ?

Trace semantics

Anyway we get



or

Coalgebraic trace semantics

Behavior by final coalgebra

$$\begin{array}{ccc} FX & \dashrightarrow & FZ \\ c\uparrow & & \uparrow\text{final} \\ X & \underset{\mathbf{beh}(c)}{\dashrightarrow} & Z \end{array}$$

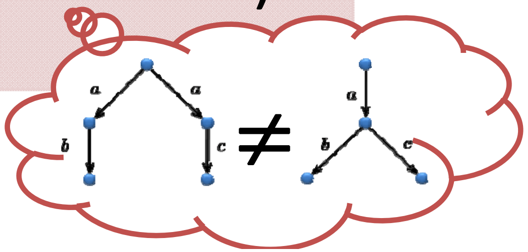
captures…

“**Kleisli category**”

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

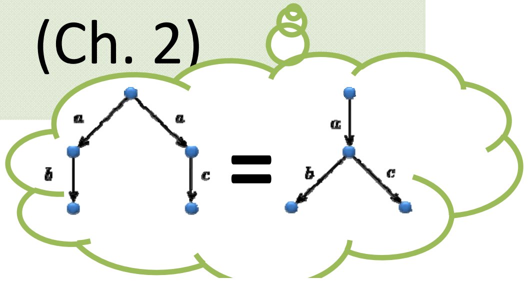
in $\mathbf{Sets}$

bisimilarity (standard)



in $\mathrm{Kl}(T)$

trace semantics (Ch. 2)



Generic Trace Semantics via Coinduction
IH, Bart Jacobs & Ana Sokolova
Logical Method in Comp. Sci. 3(4:11), 2007

Different "branching-types"

$$\begin{tikzcd} FX \arrow[r, dashed] & FZ \\ X \arrow[u, "c"] \arrow[r, dashed, "\mathsf{beh}(c)"'] & Z \arrow[u, "\text{final}"'] \end{tikzcd}$$

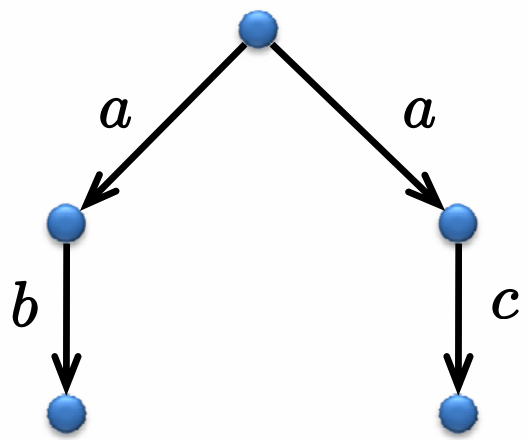
in $\mathrm{Kl}(T)$ captures **trace s antics**

T : parara meter for
"**bran**

$T = \mathcal{P}$

trace semantics:
$\left\{ \begin{array}{l} a \to b \\ a \to c \end{array} \right\}$

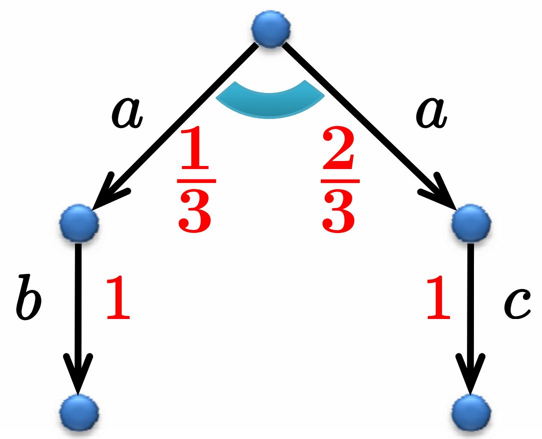
non-deterministic branching



$T = \mathcal{D}$

trace semantics:
$\left(\begin{array}{ll} a \to b & : 1/3 \\ a \to c & : 2/3 \end{array} \right)$

probabilistic branching



Coalgebraic simulations (Ch. 3)

morphism of coalgebras

$$\begin{tikzcd} FX \arrow[r, "Ff"] & FY \\ X \arrow[u, "c"] \arrow[r, "f"'] & Y \arrow[u, "d"'] \end{tikzcd}$$

in Sets: functional bisimulation (standard)

in $\mathbf{Kl}(T)$: ??

observation

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

lax morphism = **forward simulation**

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

theorem (soundness)

fwd/bwd simulation ➔ trace inclusion

Generic Forward and Backward Simulations
IH
Proc. CONCUR 2006
LNCS 4137

Summa

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

	in Sets	in $\mathbf{Kl}(T)$
coalgebra $\begin{array}{c} FX \\ \uparrow \\ X \end{array}$	system	system
morphism of coalgebra $\begin{array}{ccc} FX & \xrightarrow{Ff} & FY \\ {\scriptstyle c}\uparrow & & \uparrow{\scriptstyle d} \\ X & \xrightarrow[f]{} & Y \end{array}$	functional bisimilarity	forward simulation (lax) backward similation (oplax)
by final coalgebra $\begin{array}{ccc} FX & \dashrightarrow & FZ \\ {\scriptstyle c}\uparrow & & \uparrow{\scriptstyle \text{final}} \\ X & \underset{\mathsf{beh}(c)}{\dashrightarrow} & Z \end{array}$	bisimilarity	trace semantics

Ch. 3

Ch. 2

theory of bisimilarity

theory of traces and simulations

Case study: probabilistic anonymity (Ch. 4)

Simulation-based proof method for non-deterministic anonymity
[KawabeMST06]

$\mathcal{T} = \mathcal{P}$

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

$\mathcal{T} = \mathcal{D}$

Simulation-based proof method for probabilistic anonymity

Probabilistic Anonymity via Coalgebraic Simulations
IH & Yoshinobu Kawabe
Proc. ESOP 2007
LNCS 4421

Concurrency

“concurrency” , “behavior”

$\mathcal{C} \parallel \mathcal{D}$

running $\mathcal{C}$ and $\mathcal{D}$ in parallel

2-dimensional , nested algebraic structure

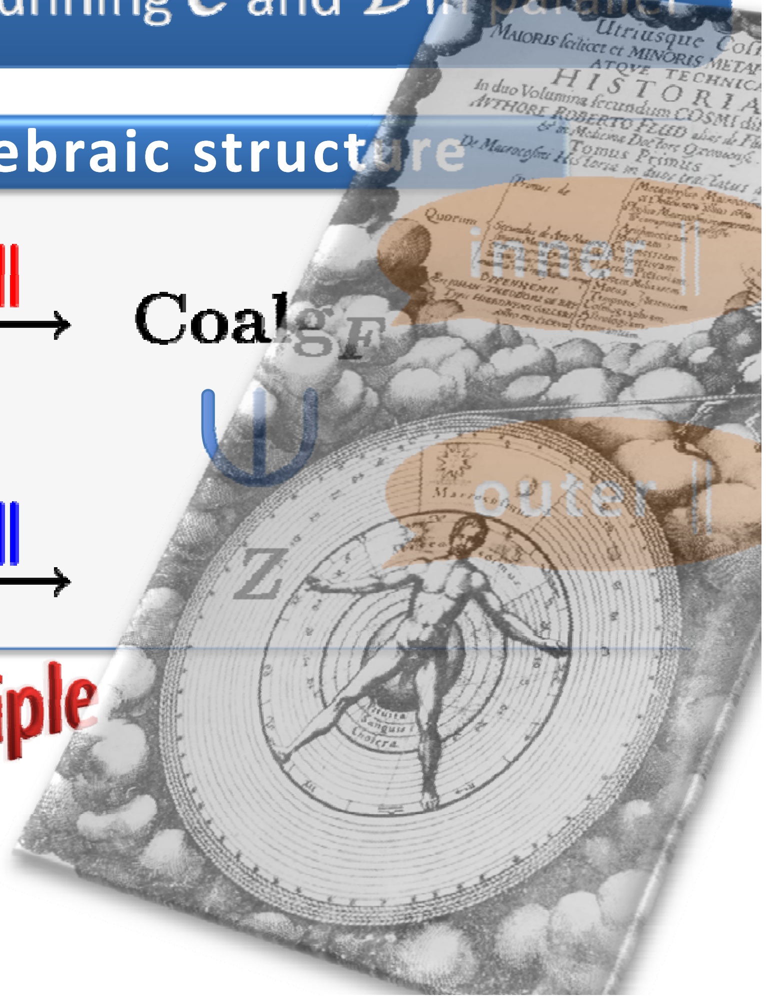
category of coalgebras

final coalgebra

$$
\begin{array}{ccccc}
\mathrm{Coalg}_F & \times & \mathrm{Coalg}_F & \xrightarrow{\parallel} & \mathrm{Coalg}_F \\
 & & & & \cup \\
Z & \times & Z & \xrightarrow{\parallel} & Z
\end{array}
$$

inner ||

outer ||



the microcosm principle

Concurrency and the microcosm principle (Ch. 5)

science of

generic compositionality theorem

concurrency, compositionality, behavior, …

formalization of microcosm principle in 2-categories

$$\begin{tikzcd} \mathbb{L} \arrow[rr, bend left=50, "1"] \arrow[rr, "\mathbb{C}"'] \arrow[rr, phantom, shift left=3, "\Downarrow X"] & & \mathbf{Cat} \end{tikzcd}$$

mathematics

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

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