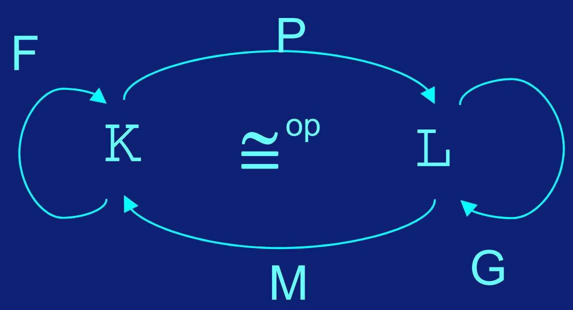
Braga, 12 October 2006



Coalgebraic logic for name-passing processes

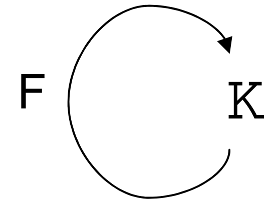
Marcello Bonsangue

Leiden Institute of Advanced Computer Science
Research & Education

Overview

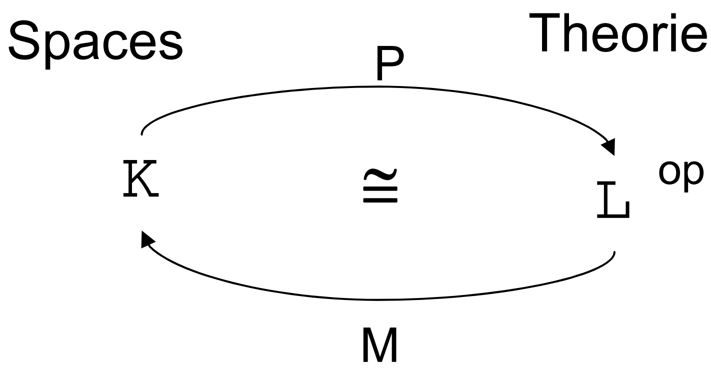
- Coalgebras and their logics
- Coalgebras for names-passing processes
- Modal logic for name-passing processes

Dynamic systems via coalgebras



FX	X → FX
A x X	Streams
2 x X^A	Deterministic automata
H(X)	Kripke structures
H(A x X)	Labelled transition systems

Logics via algebras

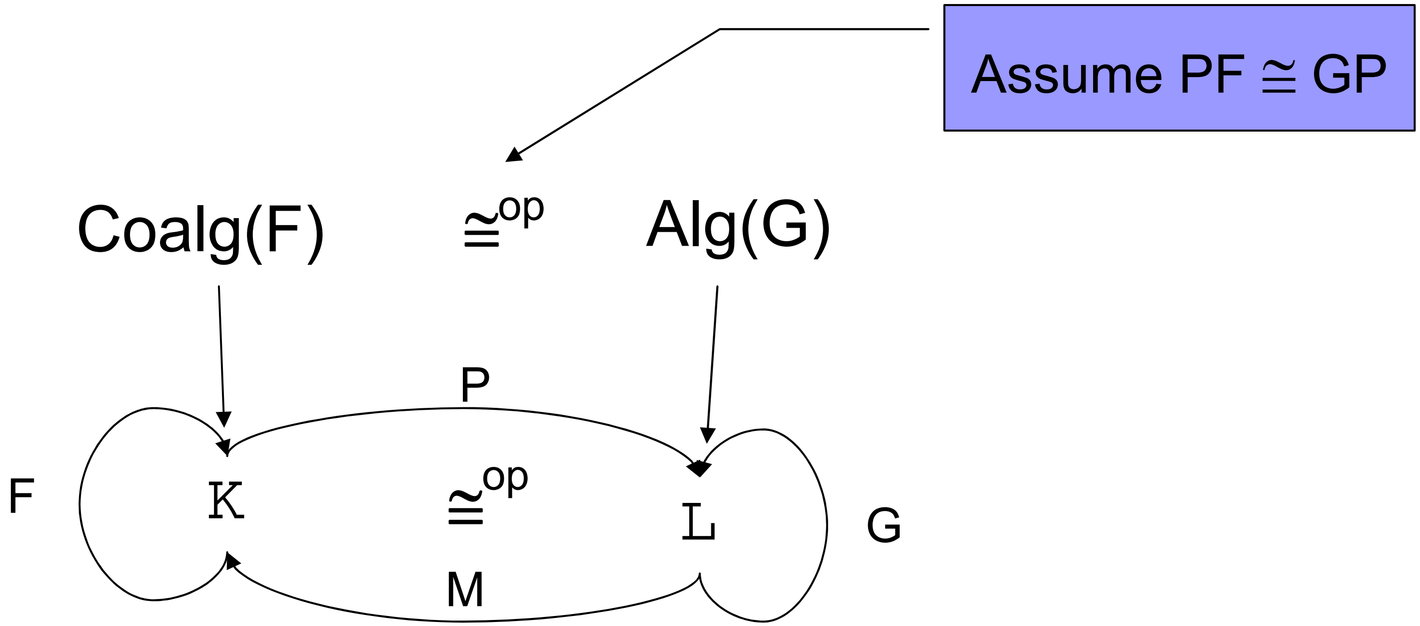


- PX = predicates over X
- MA = models of A

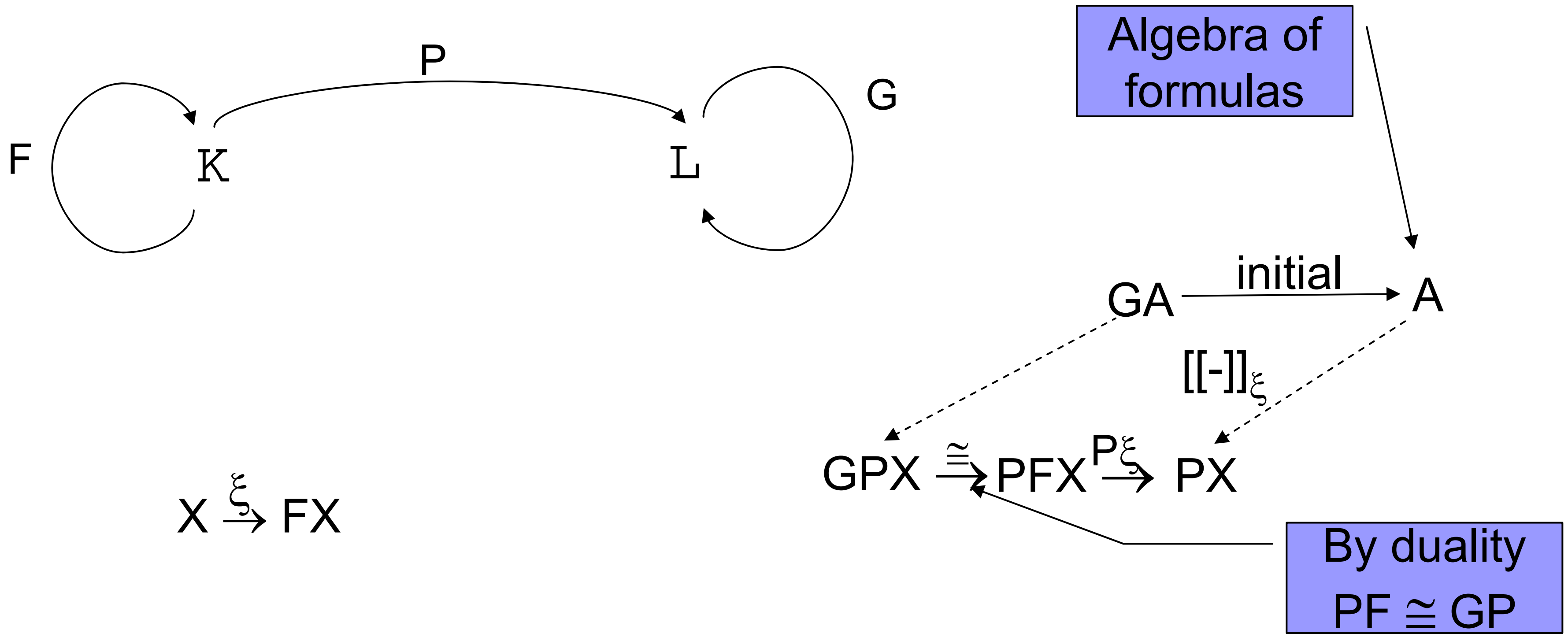
K	L	Logic
Stone	BA	Propositional logic
Spec	DL	Intuitionist propositional logic
Set	CABA	Infinitary propositional logic

Coalgebraic logic

- Coalgebraic logic = study of logical systems associated with coalgebraic structures

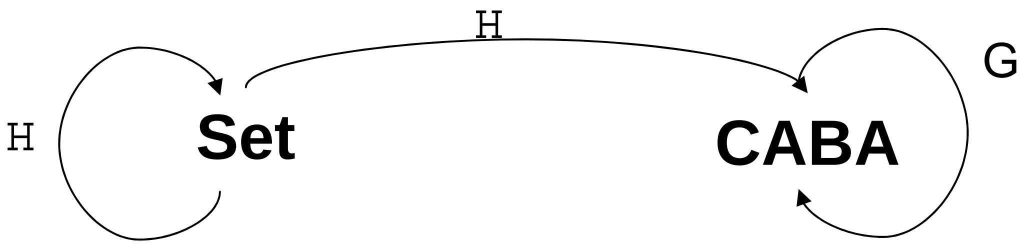


Abstract coalgebraic logic



- $\phi =_A \psi$ iff $[[\phi]]_\xi = [[\psi]]_\xi$ for all coalgebras $\xi : X \to FX$
- The logic is expressive w.r.t. F-bisimulation

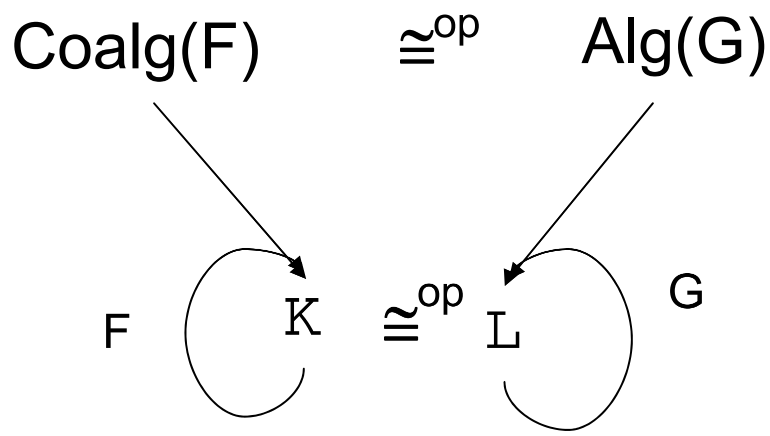
Example: modal logic



- Coalgebras $\xi : X \to \mathtt{H}X$ are transition systems
  - $x \to y$ iff $y \in \xi(x)$

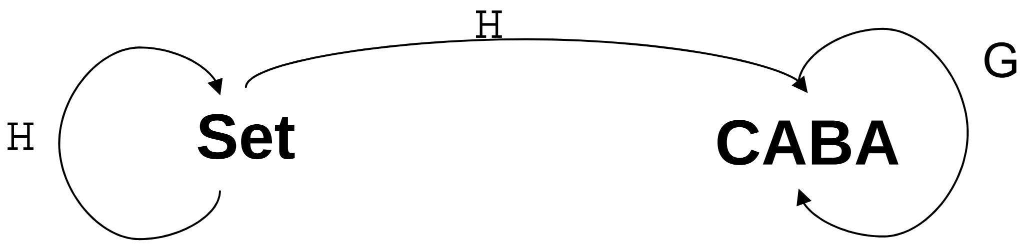
- GA generated by relations
  - a, $a \in A$
  - preserves all meets

Concrete coalgebraic logic



- If L = Alg(Σ,E) and Alg(G) = Alg(Σ+ Ω,E+I) then
  - We have terms for the initial G-algebra (formulae)
  - We can inherit a concrete proof system from the equations of the initial G-algebra

Example: modal logic – II



- Coalgebras $\xi : X \to \mathtt{H}X$ are transition systems
  - $x \to y$ iff $y \in \xi(x)$

- GA generated by relations: $- a$, $a \in A$; $-$ preserves all meets

- Formulae: ϕ ::= $\mathtt{f}$ | $\neg\phi$ | $\Lambda_I \phi_i$ | $- \phi$
- Semantics e.g.: $x \,\mathtt{b}\, - \phi$ iff $\forall x \to y.\ y \,\mathtt{b}\, \phi$
- Proof system e.g.: if $\mathtt{a}\ \phi_1 = \phi_2$ then $\mathtt{a}\ - \phi_1 = - \phi_2$

Overview

- Coalgebras and their logics
- Coalgebras for names-passing processes
- Modal logic for name-passing processes

Communicating processes

- Communication by synchronization on channel names
  - Input: a?
  - Output: a!
- Internal activity τ

Value passing processes

- Communication by exchanging values on channels
  - Input: a?x
  - Output: a!v
- Internal activity τ

Name passing processes

- Communication by exchanging channel names
  - Input: a?b
  - Output: a!b
- Names are private, but may be shared by communicating it
  - Bound output: a!νb
- Internal activity τ

Some coalgebras

- A coalgebra for communicating processes

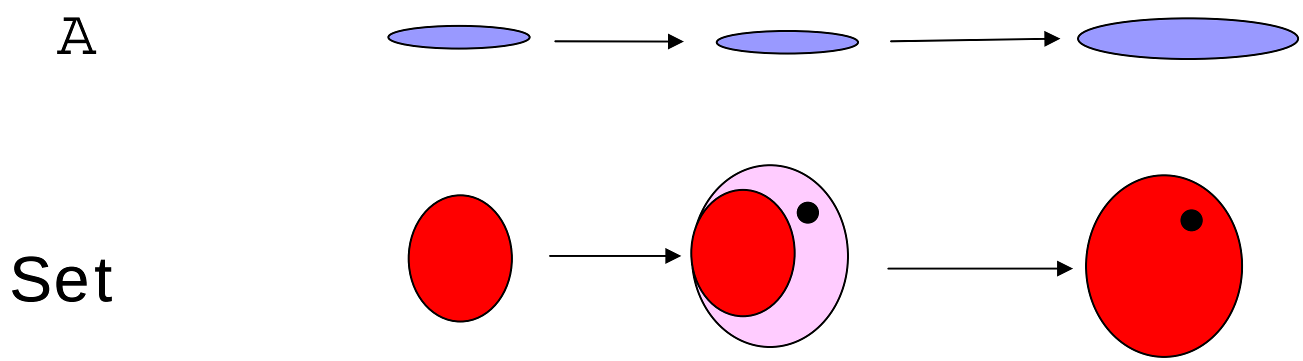
$\xi : X \to \mathtt{H}(X +$	silent step	$x \xrightarrow{\tau} y$
$A \times X +$	input	$x \xrightarrow{a?} y$
$A \times X)$	output	$x \xrightarrow{a!} y$

- A coalgebra for name passing processes

$\xi : X \to \mathtt{H}(X +$	silent step	$x \xrightarrow{\tau} y$
$N \times (N \Rightarrow X) +$	input	$x \xrightarrow{a?} f$
$N \times N \times X +$	output	$x \xrightarrow{a!b} y$
$N \times \delta X)$	bound output	$x \xrightarrow{a!\nu b} y$

The functor category $\mathbb{Set}^{\mathbb{A}}$ [FMS96,Sta96]

- We need a structure that vary according to the free names available for interaction



- A functor $F:\mathbb{A} \to \mathbb{Set}$ specifies for each set of names i a process F(i) using names in i for interaction. It also takes into account possible renaming.

Constuctors on $Set^{\mathbb{A}}$

- Names N
  - The inclusion functor $I \to Set$
- Product × and sum +
  - Defined pointwise
- Powerspace $\mathbb{H}-$
  - Defined pointwise and including the emptyset
- Name exponentiation F^N
  - Defined on objects by $F^N(i) = F(i)^i \times F(i \oplus 1)$
- Dynamic allocation δF
  - Defined by $\delta F(i) = F(i \oplus 1)$

Overview

- Coalgebras and their logics
- Coalgebras for names-passing processes
- Modal logic for name-passing processes

The dual of $\mathtt{Set}^{\mathbb{A}}$

- The duality between Set and CABA can be lifted in a pointwise manner to a duality between $\mathtt{Set}^{\mathbb{A}}$ and $\mathrm{CABA}^{\mathbb{A}^{op}}$
- Its objects are many-sorted algebras with sorts in $\mathbb{A}$ and operators
  - $\mathtt{f}$:i $\neg$:i $\rightarrow$i $\bigwedge_K$:i^K $\rightarrow$i for each i in $\mathbb{A}$
    - obeying the Booleans laws
  - $[\iota]$:j $\rightarrow$i for each ι:i $\rightarrow$j in $\mathbb{A}$
    - obeying the functorial laws and distributing on all finite meets and joins.

A modal logic

- Two tiers logic
  - One tier for processes

$\phi{:}i \;::=\; \pounds{:}i \mid \neg\phi{:}i \mid \bigwedge_K \phi_k{:}i \mid [\iota]\phi{:}j$	structural formulas
$\mid\; -(\psi{:}i)$	necessity

  - and another for capabilities

$\psi{:}i \;::=\; \pounds{:}i \mid \neg\psi{:}i \mid \psi{:}i \wedge \psi{:}i \mid [\iota]\psi{:}j$	structural formulas
$\mid\; \phi{:}i$	silent step
$\mid\; a(b) \rightarrow \phi{:}i$	input old name
$\mid\; a(-) \rightarrow \phi{:}i{+}1$	input new name
$\mid\; ab \leftarrow \phi{:}i$	output
$\mid\; a- \leftarrow \delta\phi{:}i{+}1$	bound output

with $a,b \in i$ and $\iota{:}i \rightarrow j$

Reasoning about names: an example

It is possible that a process receives a fresh name, say b, along the channel a, and if this is the case then it must output the name a on the newly received channel b.

$\Diamond a(\nu b) \rightarrow (- \; ba \leftarrow \mathtt{f}\;):i$ with $a \in i$ but $b \notin i$

This is a shorthand for

$\neg - \neg(a() \rightarrow ([\nu b](- \; ba \leftarrow \mathtt{f}\;))):i$

where $\nu b:i{+}1 \rightarrow i \cup \{b\}$,

Conclusion

- Other equivalences
  - Late bisimulation $H(N \times X^N)$ first choose - then receive

    vs.

    early bisimulation $N \Rightarrow H(X)^N$ first receive - then choose

  - Weak bisimulation

    – – ϕ:i = – ϕ:i silent steps are transitive

  - Trace equivalences: may and must testing
- Other logics
  - Without negation and/or with finite conjunctions
- Model checking?