Queen Mary / Imperial College
Joint Theory Seminar
10 December 2003

# Free-Algebra Models for the $\pi$-Calculus

Ian Stark

Laboratory for Foundations of Computer Science
School of Informatics
University of Edinburgh

# Summary

The finite $\pi$-calculus has an explicit set-theoretic functor-category model that is known to be fully-abstract for bisimulation congruence [Fiore, Moggi, Sangiorgi]

We can characterise this as the free algebra for certain operations and equations in the setting of Power and Plotkin's enriched Lawvere theories.

This combines separate theories of nondeterminism, I/O and name creation in a modular fashion. As a bonus, we get a modal logic and a computational monad. The tricky part is that everything has to happen inside the functor category $\mathcal{S}et^{\mathcal{I}}$.

# Overview

- Equational theories for different features of computation.
- Enrichment over the functor category $\mathcal{S}et^{\mathcal{I}}$.
- A theory of $\pi$.
- Free-algebra models; full abstraction; modal logic.

# Nondeterministic computation

## Operations

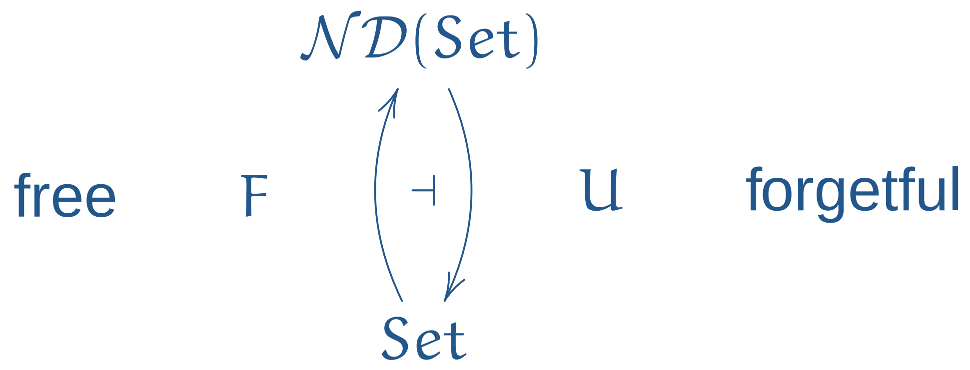
$$\mathrm{choice} : A^2 \longrightarrow A$$
$$\mathrm{nil} : 1 \longrightarrow A$$

## Equations

$$\mathrm{choice}(P, Q) = \mathrm{choice}(Q, P)$$
$$\mathrm{choice}(\mathrm{nil}, P) = \mathrm{choice}(P, P) = P$$
$$\mathrm{choice}(P, (\mathrm{choice}(Q, R)) = \mathrm{choice}(\mathrm{choice}(P, Q), R)$$

# Algebras for nondeterminism

For any Cartesian category $\mathcal{C}$ we can form the category $\mathcal{ND}(\mathcal{C})$ of models $(A, \mathsf{choice}, \mathsf{nil})$ for the theory. In particular, there is:




In fact $(U \circ F)$ is finite powerset and the adjunction is monadic: $\mathcal{ND}(\mathcal{S}et)$ is isomorphic to the category of $\mathcal{P}_{\mathrm{fin}}$-algebras.

# Computational monad for nondeterminism

$$\mathcal{ND}(Set)$$

free $\quad F \uparrow \dashv \downarrow U \quad$ forgetful

$$Set$$

The composition $T = (U \circ F) = \mathcal{P}_{\mathrm{fin}}$ is the computational monad for finite nondeterminism. Operations $choice$ and $nil$ then induce generic effects in the Kleisli category:

from $\quad choice : A^2 \longrightarrow A^1 \qquad$ we get $\quad arb : 1 \longrightarrow T\,2$

$\qquad nil : A^0 \longrightarrow A^1 \qquad\qquad dead : 1 \longrightarrow T\,0$

[Plotkin, Power: Algebraic Operations and Generic Effects]

# I/O computation

Operations

$$\mathrm{in} : A^V \longrightarrow A$$
$$\mathrm{out} : \ A \ \longrightarrow A^V$$

Equations

none

From any Cartesian $\mathcal{C}$ we form the category $\mathcal{IO}(\mathcal{C})$ of models $(A, \mathrm{in}, \mathrm{out})$ for I/O computation over $\mathcal{C}$.

# I/O adjunction and monad

$$\mathcal{IO}(\mathit{Set})$$

$$\text{free} \quad F \;\uparrow\; \dashv \;\downarrow\; U \quad \text{forgetful}$$

$$\mathit{Set}$$

The adjunction is monadic: $\mathcal{IO}(\mathit{Set}) \cong T\text{-}\mathcal{A}lg$ for the resumptions monad, the computational monad for I/O:

$$T(X) = \mu Y.(X + Y^V + Y \times V) \; .$$

The operations induce suitable effects in its Kleisli category:

$$\text{from} \quad \mathrm{in} : A^V \longrightarrow A^1 \qquad \text{we get} \quad \mathit{read} : 1 \longrightarrow T\,V$$

$$\mathrm{out} : A^1 \longrightarrow A^V \qquad\qquad \mathit{write} : V \longrightarrow T\,1$$

# Notions of computation determine monads

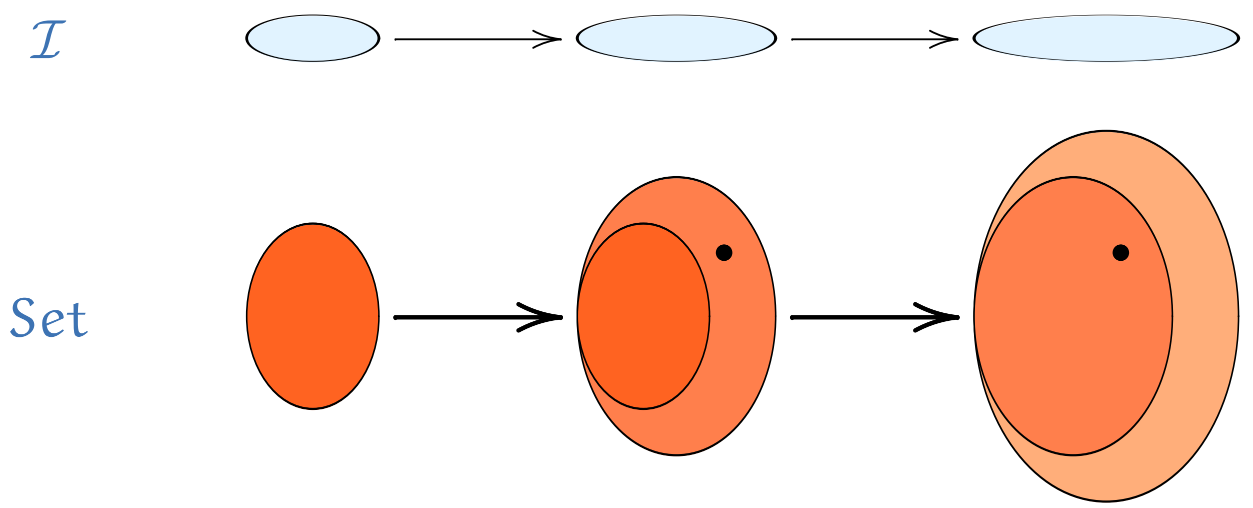
Operations + Equations $\longrightarrow$ Free-algebra models of computational features

$\longrightarrow$ Monads + generic effects

- Characterise known computational monads *and* effects.
- Simple and flexible combination of theories.
- Enriched models and arities: countably infinite, posets, $\omega\mathrm{Cpo}$.

# The functor category $\mathcal{S}et^{\mathcal{I}}$

To account for names, we work with structures that vary according to the names available.




An object $B \in \mathcal{S}et^{\mathcal{I}}$ is a varying set: it specifies for any finite set of names $s$ the set $B(s)$ of values using names from $s$, together with information about how these values change with renaming.

# Structure within $\mathcal{S}et^{\mathcal{I}}$

We use $\mathcal{S}et^{\mathcal{I}}$ both as the arena for building name-aware algebras and monads, and as the source of arities for operations.

Relevant structure includes:

- Pairs $A \times B$ and function space $A \rightarrow B$;
- Separated pairs $A \otimes B$ and fresh function space $A \multimap B$;
- The object of names $N$;
- The shift endofunctor $\delta A = A(\_ + 1)$, with $\delta A = N \multimap A$.

In particular, the object $N$ serves as a varying arity.

# Theory of $\pi$: operations

## Nondeterminism

| | | | |
|---|---|---|---|
| $\mathit{nil} : 1 \longrightarrow A$ | inactive process | $0$ |
| $\mathit{choice} : A^2 \longrightarrow A$ | process sum | $P + Q$ |

## I/O

| | | |
|---|---|---|
| $\mathit{out} : A \longrightarrow A^{N \times N}$ | output prefix | $\bar{x}y.P$ |
| $\mathit{in} : A^N \longrightarrow A^N$ | input prefix | $x(y).P$ |
| $\mathit{tau} : A \longrightarrow A$ | silent prefix | $\tau.P$ |

## Dynamic name creation

| | | |
|---|---|---|
| $\mathit{new} : \delta A \longrightarrow A$ | restriction | $\nu x.P$ |

# Theory of $\pi$: interlude

Each operation induces a corresponding effect:

$$\begin{aligned} send &: N \times N \longrightarrow T\,1 & dead &: 1 \longrightarrow T\,0 \\ recv &: N \longrightarrow T\,N & arb &: 1 \longrightarrow T2 \\ skip &: 1 \longrightarrow T\,1 & gensym &: 1 \longrightarrow T\,N \end{aligned}$$

Other possible operations:

- $par$ is not algebraic (because $(P \mid Q); R \neq (P; R) \mid (Q; R)$ )
- $eq, neq : A \longrightarrow A^{N \times N}$ definable from $N \times N \cong N \otimes N + N$
- $bout : \delta A \longrightarrow A^{N}$ can be defined from $new$ and $out$

# Theory of $\pi$: operations

## Nondeterminism

| | | |
|---|---|---|
| $nil : 1 \longrightarrow A$ | inactive process | $0$ |
| $choice : A^2 \longrightarrow A$ | process sum | $P + Q$ |

## I/O

| | | |
|---|---|---|
| $out : A \longrightarrow A^{N \times N}$ | output prefix | $\bar{x}y.P$ |
| $in : A^N \longrightarrow A^N$ | input prefix | $x(y).P$ |
| $tau : A \longrightarrow A$ | silent prefix | $\tau.P$ |

## Dynamic name creation

| | | |
|---|---|---|
| $new : \delta A \longrightarrow A$ | restriction | $\nu x.P$ |

# Theory of $\pi$: component equations

## Nondeterminism

$choice$ is associative, commutative and idempotent, with identity $nil$.

## I/O

None.

## Dynamic name creation

$$new(x.P) = P$$

$$new(x.new(y.P)) = new(y.new(x.P))$$

# Theory of $\pi$: combining equations

## Commuting

$$\mathit{new}(x.\mathit{choice}(P, Q)) = \mathit{choice}(\mathit{new}(x.P), \mathit{new}(x.Q))$$

$$\mathit{new}(z.\mathit{out}_{x,y}(P)) = \mathit{out}_{x,y}(\mathit{new}(z.P)) \qquad z \notin \{x, y\}$$

$$\mathit{new}(z.\mathit{in}_x(\lambda y.P)) = \mathit{in}_x(\lambda y.\mathit{new}(z.P)) \qquad z \notin \{x, y\}$$

$$\mathit{new}(z.\mathit{tau}(P)) = \mathit{tau}(\mathit{new}(z.P))$$

## Interaction

$$\mathit{new}(x.\mathit{out}_{x,y}(P)) = \mathit{nil}$$

$$\mathit{new}(x.\mathit{in}_x(\lambda y.P)) = \mathit{nil}$$

# Models of the theory of $\pi$

The category $\mathcal{PI}(\mathit{Set}^{\mathcal{I}})$ of $\pi$ models has objects of the form $(A \in \mathit{Set}^{\mathcal{I}}; \mathit{in}, \mathit{out}, \ldots, \mathit{new})$ satisfying the equations given.

$$\begin{array}{c} \mathcal{PI}(\mathit{Set}^{\mathcal{I}}) \\ \Big\downarrow U \quad \text{forgetful} \\ \mathit{Set}^{\mathcal{I}} \end{array}$$

Naturally, we now look for a free model left adjoint to $U$, and its accompanying monad.

As it happens, using both closed structures at the same time means that general results don't immediately apply.

# Free models for $\pi$

Each component theory has a standard monad:

| | |
|---|---|
| **Nondeterminism** | $\mathcal{P}_{fin}(X)$ |
| **I/O** | $\mu Y.(X + N \times N \times Y + N \times Y^N + Y)$ |
| **Name creation** | $Dyn(X) = \int^k X(\_ + k)$ |

Weaving these together as monad transformers gives

$$\mu Y.\mathcal{P}_{fin}(Dyn(X + N \times N \times Y + N \times Y^N + Y)) \ldots$$

# Free models for $\pi$

Each component theory has a standard monad:

| | |
|---|---|
| **Nondeterminism** | $\mathcal{P}_{\mathrm{fin}}(X)$ |
| **I/O** | $\mu Y.(X + N \times N \times Y + N \times Y^N + Y)$ |
| **Name creation** | $\mathrm{Dyn}(X) = \int^k X(\_ + k)$ |

Weaving these together as monad transformers gives

$$\mu Y.\mathcal{P}_{\mathrm{fin}}(\mathrm{Dyn}(X + N \times N \times Y + N \times Y^N + Y))$$

. . . but the algebras for this do not satisfy the interaction equations between $\mathit{new}$ and $\mathrm{in}/\mathrm{out}$.

## Free models for $\pi$

Each component theory has a standard monad:

| | |
|---|---|
| **Nondeterminism** | $\mathcal{P}_{\mathrm{fin}}(X)$ |
| **I/O** | $\mu Y.(X + N \times N \times Y + N \times Y^N + Y)$ |
| **Name creation** | $\mathrm{Dyn}(X) = \int^k X(\_ + k)$ |

The correct monad for the combined theory is

$$\mathrm{Pi}(X) = \mu Y.\mathcal{P}_{\mathrm{fin}}(\mathrm{Dyn}(X) + N \times N \times Y + N \times \delta Y + N \times Y^N + Y)$$

which adds bound output but otherwise does little with name creation.

# Results

There is an adjunction making the category of $\pi$ models monadic over $\mathit{Set}^{\mathcal{I}}$.

$$\text{free} \quad \mathsf{Pi} \; \dashv \; \mathsf{U} \quad \text{forgetful} \qquad \mathsf{Pi} : \mathit{Set}^{\mathcal{I}} \rightleftarrows \mathcal{PI}(\mathit{Set}^{\mathcal{I}}) : \mathsf{U}$$

$\mathsf{Pi}(0)$ is the known fully abstract model of the finite $\pi$-calculus.

# Modal logic

Each theory gives rise to a modal logic over its algebras, with possibility and necessity modalities for every operation.

$$P \models \Diamond \mathrm{out}_{x,y}(\phi) \iff \exists Q.\ P \sim \bar{x}y.Q \ \wedge\ Q \models \phi$$

$$P \models \Box \mathrm{out}_{x,y}(\phi) \iff \forall Q.\ P \sim \bar{x}y.Q \ \Rightarrow\ Q \models \phi$$

$$P \models \Diamond \mathrm{choice}(\phi, \psi) \iff \exists Q, R.\ P \sim Q + R \ \wedge\ Q \models \phi \ \wedge\ R \models \psi$$

HML is definable:

$$\langle \bar{x}y \rangle \phi \ = \ \Diamond \mathrm{choice}(\Diamond \mathrm{out}_{x,y}(\phi), \mathrm{true})$$

We could also take other algebraic operations and define modalities. However, in no case is there a $\phi \mid \psi$ modality.

# Review

Operations and equations with enriched arities can give algebraic models for features of computation.

Taking $\mathcal{S}et^{\mathcal{I}}$ for both arities and algebras, we can give a modular theory for the $\pi$-calculus:

$$\pi = (\text{Nondeterminism} + \text{I/O} + \text{Name creation}) \;/\; new \leftrightarrow i/o$$

The free algebra over $0$ is fully abstract for bisimilarity.

The induced computational monad is almost, but not quite, the combination of its three components.

# What next?

- Use $\omega\mathcal{C}po$ for the full $\pi$-calculus.
- Use partial order arities to constrain choice to the upper or lower powerdomain. [Hennessy]

- Build a proper theory of arities over two closed structures.

OR

- Exhibit $\mathcal{S}et^{\mathcal{I}}$ as the category of algebras for a theory of equality testing in $\mathcal{S}et^{\mathcal{F}}$, and then redo everything in the single Cartesian closed structure of $\mathcal{S}et^{\mathcal{F}}$.

# Constructions in $\mathcal{S}et^{\mathcal{I}}$

Cartesian closed

$$(A \times B)(k) = A(k) \times B(k)$$
$$B^{A}(k) = [A(k + \_), B(k + \_)]$$

Monoidal closed

$$(A \otimes B)(k) = \int^{k' + k'' \hookrightarrow k} A(k') \times B(k'')$$
$$(A \multimap B)(k) = [A(\_), B(k + \_)]$$

# More constructions in $\mathcal{S}et^{\mathcal{I}}$

## Object of names, shift operator

$$\mathrm{N}(k) = k$$

$$\delta A(k) = A(k+1)$$

## Connections

$$A \otimes B \hookrightarrow A \times B$$

$$(A \to B) \twoheadrightarrow (A \multimap B)$$

$$\delta A = \mathrm{N} \multimap A$$