

# Full Abstraction for Non-Deterministic and Probabilistic Extensions of PCF

Jean Goubault-Larrecq



ANR Blanc CPP

Domains X - September 2011

# Outline

- 1 Introduction
- 2 Call-by-Name
  - Syntax
  - Operational Semantics
  - Denotational Semantics
- 3 The Full Abstraction Problem
  - Full Abstraction
  - Definability
  - The Need for Termination Testers
- 4 Call-by-Value
  - Syntax
  - Semantics
  - The Need for Statistical Termination Testers
  - Full Abstraction in Angelic Cases
- 5 Conclusion

# Outline

- 1 Introduction
- 2 Call-by-Name
  - Syntax
  - Operational Semantics
  - Denotational Semantics
- 3 The Full Abstraction Problem
  - Full Abstraction
  - Definability
  - The Need for Termination Testers
- 4 Call-by-Value
  - Syntax
  - Semantics
  - The Need for Statistical Termination Testers
  - Full Abstraction in Angelic Cases
- 5 Conclusion

# PCF, Full Abstraction

PCF [Plotkin77]:

- a call-by-name, simply-typed, higher-order **functional language**
- **no side-effects**
- has **computational adequacy**
- **fails full abstraction**... except with additional **por**

# PCF, Full Abstraction

PCF [Plotkin77]:

- a call-by-name, simply-typed, higher-order **functional language**
- **no side-effects**
- has **computational adequacy**
- **fails full abstraction**. . . except with additional **por**

Here, PCF plus specific **choice** effects:

- **probabilistic** choice
- **angelic/demonic/erratic** non-deterministic choice
- + mixtures

Only partial results for now

— with a stress on call-by-value, and angelic non-determinism

# Outline

- 1 Introduction
- 2 Call-by-Name
  - Syntax
  - Operational Semantics
  - Denotational Semantics
- 3 The Full Abstraction Problem
  - Full Abstraction
  - Definability
  - The Need for Termination Testers
- 4 Call-by-Value
  - Syntax
  - Semantics
  - The Need for Statistical Termination Testers
  - Full Abstraction in Angelic Cases
- 5 Conclusion

# Types

$$\begin{array}{ll} \gamma ::= \text{Nat} \mid \text{S} & \text{Ground types} \\ \sigma, \tau ::= \gamma \mid \sigma \rightarrow \tau \mid \mathbf{T}\tau & \text{Types} \end{array}$$

Notes:

- S has only one (non-bottom) value  
= unit type, **termination type**

Not required in principle, but practical

- $\mathbf{T}\tau$  type of **processes** computing value of type  $\tau$

à la [Moggi91]

# PCF( $S$ ) Terms

Language parameterized by set  $S \subseteq \{A, D, P\}$   
 (angelic non-det., demonic non-det., probabilistic choice).

- PCF terms

( $\lambda$ -calculus + basic arithmetic + ifz + fixpoint  $Y$ )

- At  $S$  type:

- $\underline{\perp} : S$

- for every  $M : \text{Nat}$ ,      ignore  $M : S$

- for all  $M : S$ ,  $N : \sigma$ , sequencing  $M; N : \sigma$

- At  $T\tau$  types:

- for each  $M : \tau$ ,      val  $M : T\tau$

- for all  $M : \sigma$ ,  $N : T\tau$ ,      let  $x \leftarrow M$  in  $N : T\tau$

- Non-det. choice       $\bigotimes : T\tau \rightarrow T\tau \rightarrow T\tau$       (if  $A \in S$  or  $D \in S$ )

- Prob. choice       $\bigoplus : T\tau \rightarrow T\tau \rightarrow T\tau$       (if  $P \in S$ )



# Operational Semantics

As a **machine** (a **transition system**)  
working on **configurations**  $E \cdot M$

- $M : \sigma$  is PCF( $S$ ) term
- **Contexts**  $E : (\sigma \vdash \text{TS}) =$  **stacks** of pending operations:

$$\begin{array}{l}
 E := \_ \\
 | E[_M] \\
 | E[\text{succ } \_] \mid E[\text{pred } \_] \\
 | E[\text{ifz } \_ N P] \mid E[; N] \\
 | E[\text{ignore } \_] \\
 | \text{val } \_ \\
 | E[\text{let } x \leftarrow \_ \text{ in } N]
 \end{array}$$

# The PCF(S) Machine: 1. Redex Discovery Rules

Purpose: move top of  $M$  into context  $E$ , until **redex** appears

$$\begin{aligned}
 E \cdot MN &\rightarrow E[_N] \cdot M \\
 E[_N] \cdot \text{pred } \_ &\rightarrow E[\text{pred } \_] \cdot N \\
 E[_N] \cdot \text{succ } \_ &\rightarrow E[\text{succ } \_] \cdot N \\
 E[_MNP] \cdot \text{ifz } \_ &\rightarrow E[\text{ifz } \_ N P] \cdot M \\
 E \cdot M; N &\rightarrow E[_; N] \cdot M \\
 E[_N] \cdot \text{ignore } \_ &\rightarrow E[\text{ignore } \_] \cdot N \\
 \_ \cdot \text{val } M &\rightarrow \text{val } \_ \cdot M \\
 E \cdot \text{let } x \leftarrow M \text{ in } N &\rightarrow E[\text{let } x \leftarrow \_ \text{ in } N] \cdot M
 \end{aligned}$$

# The PCF(S) Machine: 2. Computation

**Redex** = interaction between top of  $M$  and bottom of  $E$

$$E[_N] \cdot \lambda x \cdot P \rightarrow E \cdot P[x := N]$$

$$E[\text{pred } \_] \cdot \underline{n+1} \rightarrow E \cdot \underline{n}$$

$$E[\text{succ } \_] \cdot \underline{n} \rightarrow E \cdot \underline{n+1}$$

$$E[\text{ifz } \_ N P] \cdot \underline{0} \rightarrow E \cdot N$$

$$E[\text{ifz } \_ N P] \cdot \underline{n+1} \rightarrow E \cdot P$$

$$E[; N] \cdot \underline{\top} \rightarrow E \cdot N$$

$$E[\text{ignore } \_] \cdot \underline{n} \rightarrow E \cdot \underline{\top}$$

$$E[_N] \cdot Y \rightarrow E \cdot N(YN)$$

$$E[\text{let } x \leftarrow \_ \text{ in } P] \cdot \text{val } N \rightarrow E \cdot P[x := N]$$

**Termination state:**  $\text{val } \_ \cdot \underline{\top}$

# The PCF(S) Machine: 3. Choice

The **choice states** are:

- (non-deterministic)  $E \cdot \heartsuit$  (if  $A \in S$  or  $D \in S$ )
- (probabilistic)  $E \cdot \oplus$  (if  $P \in S$ )

The rules are pretty non-committal (to the kind of choice):

$$E[_MN] \cdot \heartsuit \rightarrow M$$

$$E[_MN] \cdot \heartsuit \rightarrow N$$

$$E[_MN] \cdot \oplus \rightarrow M$$

$$E[_MN] \cdot \oplus \rightarrow N$$

# Reachability Objectives

$S = \emptyset$  **reachability**: does  $E \cdot M \rightarrow^* \text{val } \_ \cdot \underline{\top}$ ?

$S = \{\mathbf{P}\}$  **probabilistic testing**:  $\Pr[E \cdot M \rightarrow^* \text{val } \_ \cdot \underline{\top}] > r$   
 where  $E[_MN] \cdot \oplus$  goes to  $M$  or  $N$  with prob.  $1/2$

$S = \{\mathbf{A}\}$  **may testing**:  $\exists$  terminating path  $E \cdot M \rightarrow^* \text{val } \_ \cdot \underline{\top}$ ?

$S = \{\mathbf{D}\}$  **must testing**:  $\forall$  paths terminate?

$S = \{\mathbf{A}, \mathbf{P}\}$   $\exists$  **scheduler**  $\varsigma$  /  $\Pr[E \cdot M \rightarrow_{\varsigma}^* \text{val } \_ \cdot \underline{\top}] > r$   
 (pure, memoryless) schedulers map  $E \cdot \oplus$  to left/right

$S = \{\mathbf{D}, \mathbf{P}\}$   $\min_{\varsigma \text{ scheduler}} \Pr[E \cdot M \rightarrow_{\varsigma}^* \text{val } \_ \cdot \underline{\top}] > r$ ?

$\{\mathbf{A}, \mathbf{D}\} \subseteq S$  **erratic cases**: ask both **angelic** and **demonic** questions  
 (I will exclude the erratic cases from this talk)

# Termination Semantics (1/2)

Use **judgments**  $E \cdot M \downarrow^m a$ ,  $m \in \{\text{may}, \text{must}\}$ ,  $a \in \mathbb{Q} \cap [0, 1]$ .

“The probability that  $E \cdot M$  (may, must) terminate is  $> a$ ”

- For every redex discovery (1.) or computation (2.) rule  $C \rightarrow C'$ :

$$\frac{C' \downarrow^m a}{C \downarrow^m a} \quad \left( \text{e.g., } \frac{E \cdot P[x := N] \downarrow^m a}{E[_N] \cdot \lambda x \cdot P \downarrow^m a} \right)$$

- Final state  $\text{val } \_ \cdot \underline{\top}$ :

$$\frac{}{\text{val } \_ \cdot \underline{\top} \downarrow^m a} \quad (a \in \mathbb{Q} \cap [0, 1])$$

- Choice: see next slide (obviously the most important part)

## Termination Semantics (2/2)

Choice:

$$\frac{E \cdot M \downarrow^{\text{may}} a}{E[_{MN}] \cdot \textcircled{\vee} \downarrow^{\text{may}} a} \quad \frac{E \cdot N \downarrow^{\text{may}} a}{E[_{MN}] \cdot \textcircled{\vee} \downarrow^{\text{may}} a} \quad \frac{E \cdot M \downarrow^{\text{must}} a \quad E \cdot N \downarrow^{\text{must}} a}{E[_{MN}] \cdot \textcircled{\vee} \downarrow^{\text{must}} a}$$

$$\frac{E \cdot M \downarrow^m a \quad E \cdot N \downarrow^m b}{E[_{MN}] \cdot \textcircled{\oplus} \downarrow^m \frac{1}{2}(a+b)} (\oplus) \quad (m \in \{\text{may}, \text{must}\})$$

## Definition

$$\Pr(E \cdot M \downarrow^m) = \sup\{a \in \mathbb{Q} \in [0, 1] \mid E \cdot M \downarrow^m a \text{ derivable}\}$$

- $\Pr(\text{val } \_ \cdot \underline{\top} \downarrow^m) = 1$
- $\Pr(E[_{MN}] \cdot \textcircled{\oplus} \downarrow^m) = \frac{1}{2}(\Pr(E \cdot M \downarrow^m) + \Pr(E \cdot N \downarrow^m))$
- $\Pr(E[_{MN}] \cdot \textcircled{\vee} \downarrow^{\text{may}}) = \max(\Pr(E \cdot M \downarrow^{\text{may}}), \Pr(E \cdot N \downarrow^{\text{may}}))$
- $\Pr(E[_{MN}] \cdot \textcircled{\vee} \downarrow^{\text{must}}) = \min(\Pr(E \cdot M \downarrow^{\text{must}}), \Pr(E \cdot N \downarrow^{\text{must}}))$ .

# Denotational Semantics: Previsions

Let  $\llbracket T\tau \rrbracket_S$  as spaces of **previsions** over  $\llbracket \tau \rrbracket_S$  [JGL-CSL07]

## Definition (Prevision on $X$ )

Let  $I = [0, 1]$ , as a dcpo. A Scott-continuous functional  $F : [X \rightarrow I] \rightarrow I$  is a prevision iff:

- $F(ah) = aF(h)$  for every  $a \in I$
- $F(\frac{a+h}{2}) = \frac{1}{2}(a + F(h))$  (total mass = 1)
- $F(\frac{h+h'}{2}) \leq \frac{1}{2}(F(h) + F(h'))$  (if  $S \subseteq \{A, P\}$ )
- $F(\frac{h+h'}{2}) \geq \frac{1}{2}(F(h) + F(h'))$  (if  $S \subseteq \{D, P\}$ )
- $F(h) \in \{0, 1\}$  for every  $h : X \rightarrow \{0, 1\}$  (if  $P \notin S$ )

(Again, not dealing with the erratic cases here.)

**Note:** by representation theorems [JGL08], match the usual Hoare/Smyth powerdomains, as well as [MOW03, TKP05].



## Denotational Semantics

$$\begin{aligned}
\llbracket x \rrbracket_S &= x & \llbracket \top \rrbracket_S &= \top & \llbracket n \rrbracket_S &= n \in \mathbb{N} \\
\llbracket \lambda x \cdot M \rrbracket_S &= (x \mapsto \llbracket M \rrbracket_S) & \llbracket MN \rrbracket_S(\rho) &= \llbracket M \rrbracket_S(\llbracket N \rrbracket_S) \\
\llbracket Y \rrbracket_S &= (f \mapsto \bigcup_{n \in \mathbb{N}} f^n(\perp)) \\
\llbracket \text{pred} \rrbracket_S &= (v \in \mathbb{N} \setminus \{0\} \mapsto v - 1 \mid 0, \perp \mapsto \perp) \\
\llbracket \text{succ} \rrbracket_S &= (v \in \mathbb{N} \mapsto v + 1 \mid \perp \mapsto \perp) \\
\llbracket \text{ifz} \rrbracket_S &= (0, t, e \mapsto t \mid n \in \mathbb{N} \setminus \{0\}, t, e \mapsto e \mid \perp \mapsto \perp) \\
\llbracket M; N \rrbracket_S &= \llbracket N \rrbracket_S \text{ if } \llbracket M \rrbracket_S \neq \perp, \text{ else } \perp \\
\llbracket \text{ignore} \rrbracket_S &= (n \in \mathbb{N} \mapsto \top \mid \perp \mapsto \perp) \\
\llbracket \text{val } M : T\sigma \rrbracket_S &= (h \mapsto h(\llbracket M \rrbracket_S)) \\
\llbracket \text{let } x \Leftarrow M \text{ in } N \rrbracket_S &= (h \mapsto \llbracket M \rrbracket_S(x \mapsto \llbracket N \rrbracket_S(h))) \\
\llbracket \bigvee \rrbracket_S &= (F_1, F_2, h \mapsto \max(F_1(h), F_2(h)) && \text{(if } \mathbf{A} \in S) \\
\llbracket \bigwedge \rrbracket_S &= (F_1, F_2, h \mapsto \min(F_1(h), F_2(h)) && \text{(if } \mathbf{D} \in S) \\
\llbracket \oplus \rrbracket_S &= (F_1, F_2, h \mapsto \frac{1}{2}(F_1(h) + F_2(h)) && \text{(if } \mathbf{P} \in S)
\end{aligned}$$

# Soundness

In usual PCF, **soundness** states that if  $M \rightarrow^* V$  then  $\llbracket M \rrbracket = \llbracket V \rrbracket$ .

## Theorem (Soundness)

Let  $\diamond = \chi_{\{\top\}} : \llbracket S \rrbracket \rightarrow I$  map  $\perp$  to 0,  $\top$  to 1.

- If  $E \cdot M \downarrow^{\text{may}} a$  then  $\llbracket E[M] \rrbracket_S(\diamond) > a$  (if  $S \subseteq \{A, P\}$ )
- If  $E \cdot M \downarrow^{\text{must}} a$  then  $\llbracket E[M] \rrbracket_S(\diamond) > a$  (if  $S \subseteq \{D, P\}$ )

**Proof:** induction. □

# Soundness

In usual PCF, **soundness** states that if  $M \rightarrow^* V$  then  $\llbracket M \rrbracket = \llbracket V \rrbracket$ .

## Theorem (Soundness)

Let  $\diamond = \chi_{\{\top\}} : \llbracket S \rrbracket \rightarrow I$  map  $\perp$  to 0,  $\top$  to 1.

- If  $E \cdot M \downarrow^{\text{may}} a$  then  $\llbracket E[M] \rrbracket_S(\diamond) > a$  (if  $S \subseteq \{A, P\}$ )
- If  $E \cdot M \downarrow^{\text{must}} a$  then  $\llbracket E[M] \rrbracket_S(\diamond) > a$  (if  $S \subseteq \{D, P\}$ )

**Proof:** induction. □

## Corollary

- $\llbracket E[M] \rrbracket_S(\diamond) \geq \Pr(E \cdot M \downarrow^{\text{may}})$  (if  $S \subseteq \{A, P\}$ )
- $\llbracket E[M] \rrbracket_S(\diamond) \geq \Pr(E \cdot M \downarrow^{\text{must}})$  (if  $S \subseteq \{D, P\}$ )

# Computational Adequacy

In usual PCF,  $M \rightarrow^* V$  iff  $\llbracket M \rrbracket = \llbracket V \rrbracket$ , at ground types.

Here, use  $E = \_$  (empty context, of type  $TS \vdash TS$ )

## Theorem (Computational Adequacy)

- $\llbracket M \rrbracket_S(\diamond) = Pr(\_ \cdot M \downarrow^{\text{may}})$  (if  $S \subseteq \{A, P\}$ )
- $\llbracket M \rrbracket_S(\diamond) = Pr(\_ \cdot M \downarrow^{\text{must}})$  (if  $S \subseteq \{D, P\}$ )

**Proof:** Let  $M \lesssim^m N$  iff  $Pr(E \cdot M \downarrow^m) \leq Pr(E \cdot N \downarrow^m)$  for every  $E$ .

- $M[x := N] \lesssim^m (\lambda x \cdot M)N$   $M(YM) \lesssim^m YM$
- $\underline{n} \lesssim^m M \Rightarrow \underline{n+1} \lesssim^m \text{succ } M$   $\underline{n+1} \lesssim^m M \Rightarrow \underline{n} \lesssim^m \text{pred } M$
- $\underline{0} \lesssim^m M \Rightarrow N \lesssim^m \text{ifz } M \ N \ P$   $\underline{n+1} \lesssim^m M \Rightarrow P \lesssim^m \text{ifz } M \ N \ P$
- $\perp \lesssim^m M \Rightarrow N \lesssim^m M; N$   $\underline{n} \lesssim^m M \Rightarrow \perp \lesssim^m \text{ignore } M$

# Computational Adequacy

In usual PCF,  $M \rightarrow^* V$  iff  $\llbracket M \rrbracket = \llbracket V \rrbracket$ , at ground types.

Here, use  $E = \_$  (empty context, of type  $TS \vdash TS$ )

## Theorem (Computational Adequacy)

- $\llbracket M \rrbracket_S(\diamond) = Pr(\_ \cdot M \downarrow^{\text{may}})$  (if  $S \subseteq \{A, P\}$ )
- $\llbracket M \rrbracket_S(\diamond) = Pr(\_ \cdot M \downarrow^{\text{must}})$  (if  $S \subseteq \{D, P\}$ )

**Proof:** Let  $M \lesssim^m N$  iff  $Pr(E \cdot M \downarrow^m) \leq Pr(E \cdot N \downarrow^m)$  for every  $E$ .

Define a logical relation  $R_\sigma$ :

- $M R_S u$  iff  $u = \perp$ , or  $u = \top$  and  $\perp \lesssim^m M$
- $M R_{\text{Nat}} n$  iff  $n = \perp$ , or  $n \in \mathbb{N}$  and  $\underline{n} \lesssim^m M$
- $M R_{\sigma \rightarrow \tau} f$  iff for all  $N R_\sigma v$ ,  $M N R_\tau f(v)$
- $M R_{T\sigma} F$  iff for all  $E R_\sigma^\perp h$ ,  $Pr(E \cdot M \downarrow^m) \geq F(h)$
- $E R_\sigma^\perp h$  iff for all  $Q R_\sigma v$ ,  $Pr(E \cdot \text{val } Q \downarrow^m) \geq h(v)$

# Computational Adequacy

In usual PCF,  $M \rightarrow^* V$  iff  $\llbracket M \rrbracket = \llbracket V \rrbracket$ , at ground types.

Here, use  $E = \_$  (empty context, of type  $TS \vdash TS$ )

## Theorem (Computational Adequacy)

- $\llbracket M \rrbracket_S(\blacklozenge) = Pr(\_ \cdot M \downarrow^{\text{may}})$  (if  $S \subseteq \{A, P\}$ )
- $\llbracket M \rrbracket_S(\blacklozenge) = Pr(\_ \cdot M \downarrow^{\text{must}})$  (if  $S \subseteq \{D, P\}$ )

**Proof:** Let  $M \lesssim^m N$  iff  $Pr(E \cdot M \downarrow^m) \leq Pr(E \cdot N \downarrow^m)$  for every  $E$ .

Define a logical relation  $R_\sigma$ :

$$M R_{T\sigma} F \quad \text{iff} \quad \text{for all } E R_\sigma^\perp h, Pr(E \cdot M \downarrow^m) \geq F(h)$$

$$E R_\sigma^\perp h \quad \text{iff} \quad \text{for all } Q R_\sigma v, Pr(E \cdot \text{val } Q \downarrow^m) \geq h(v)$$

By definition,  $\_ R_S^\perp \blacklozenge$

Basic Lemma:  $M R_\tau \llbracket M \rrbracket_S$  for every  $M : \tau$

For all  $E R_\tau^\perp h$ ,  $Pr(E \cdot M \downarrow^m) \geq \llbracket M \rrbracket_S(h)$

Conclude by taking  $E = \_$ ,  $h = \blacklozenge$ .

# Outline

- 1 Introduction
- 2 Call-by-Name
  - Syntax
  - Operational Semantics
  - Denotational Semantics
- 3 The Full Abstraction Problem
  - Full Abstraction
  - Definability
  - The Need for Termination Testers
- 4 Call-by-Value
  - Syntax
  - Semantics
  - The Need for Statistical Termination Testers
  - Full Abstraction in Angelic Cases
- 5 Conclusion

# Full Abstraction

## Definition (Full Abstraction)

$M \approx^m N$  iff  $\llbracket M \rrbracket_S \leq \llbracket N \rrbracket_S$ , **at all types**.

- Easy direction: If  $\llbracket M \rrbracket_S \leq \llbracket N \rrbracket_S$  at type  $\tau$ , then
  - $\llbracket E[M] \rrbracket_S \leq \llbracket E[N] \rrbracket_S$  for every context  $E : \tau \vdash \text{TS}$
  - By computational adequacy,  $\Pr(- \cdot E[M] \downarrow^m) \leq \Pr(- \cdot E[N] \downarrow^m)$
  - So  $\Pr(E \cdot M \downarrow^m) \leq \Pr(E \cdot N \downarrow^m)$
  - This is the definition of  $M \approx^m N$ .



# Full Abstraction

## Definition (Full Abstraction)

$M \approx^m N$  iff  $\llbracket M \rrbracket_S \leq \llbracket N \rrbracket_S$ , **at all types**.

- Easy direction: If  $\llbracket M \rrbracket_S \leq \llbracket N \rrbracket_S$  at type  $\tau$ , then  $\llbracket E[M] \rrbracket_S \leq \llbracket E[N] \rrbracket_S$  for every context  $E : \tau \vdash \text{TS}$   
 By computational adequacy,  $\Pr(- \cdot E[M] \downarrow^m) \leq \Pr(- \cdot E[N] \downarrow^m)$   
 So  $\Pr(E \cdot M \downarrow^m) \leq \Pr(E \cdot N \downarrow^m)$   
 This is the definition of  $M \approx^m N$ .
- Hard direction: assume  $\llbracket M \rrbracket_S \not\leq \llbracket N \rrbracket_S$ , **find  $E$**  such that  $\Pr(E \cdot M \downarrow^m) > \Pr(E \cdot N \downarrow^m)$

# Full Abstraction

## Definition (Full Abstraction)

$M \approx^m N$  iff  $\llbracket M \rrbracket_S \leq \llbracket N \rrbracket_S$ , **at all types**.

- Easy direction: If  $\llbracket M \rrbracket_S \leq \llbracket N \rrbracket_S$  at type  $\tau$ , then  $\llbracket E[M] \rrbracket_S \leq \llbracket E[N] \rrbracket_S$  for every context  $E : \tau \vdash \text{TS}$   
 By computational adequacy,  $\Pr(- \cdot E[M] \downarrow^m) \leq \Pr(- \cdot E[N] \downarrow^m)$   
 So  $\Pr(E \cdot M \downarrow^m) \leq \Pr(E \cdot N \downarrow^m)$   
 This is the definition of  $M \approx^m N$ .
- Hard direction: assume  $\llbracket M \rrbracket_S \not\leq \llbracket N \rrbracket_S$ , **find**  $E$  such that  $\Pr(E \cdot M \downarrow^m) > \Pr(E \cdot N \downarrow^m)$
- So hard that it is **wrong** for PCF, and for PCF(S)  
 ... so one should do something about this

# The Failure of Full Abstraction

Full abstraction **fails** for PCF [Plotkin77].

Source: parallel or (`por`) should be definable, is not.

## Cures:

- 1 Change the **model**

e.g., game semantics:

[AJM93,HO03] (no choice), [HarmerMcCusker99] (non-det.),  
[DanosHarmer01] (prob.)

- 2 Restrict the denotations to some **invariant**

Kripke logical (Sieber-) relations [JungTiuryn93]  
of variable arity [O'HearnRiecke94]

- 3 Change the **syntax**

Add `por` [Plotkin77]

I will attempt to do something similar.

Meanwhile, let us adopt a proof strategy, and see what is missing for this to work.

# Strategies for Proving Full Abstraction

Plotkin showed full abstraction using **definability** (needed anyway)

## Theorem (Plotkin77)

*In  $PCF_{+por}$ , the finite elements of  $[[\tau]]$  are exactly those of the form  $[[M]]$ ,  $M : \tau$ .*

This is bound to fail here:

if  $\mathbf{P} \in S$ , then  $[[\tau]]$  is a **continuous**, not an algebraic domain.

# Strategies for Proving Full Abstraction

Plotkin showed full abstraction using **definability** (needed anyway)

## Theorem (Plotkin77)

*In  $PCF_{+por}$ , the finite elements of  $\llbracket \tau \rrbracket$  are exactly those of the form  $\llbracket M \rrbracket$ ,  $M : \tau$ .*

This is bound to fail here:

if  $P \in S$ , then  $\llbracket \tau \rrbracket$  is a **continuous**, not an algebraic domain.

**Cure:** show a weaker definability result, of both

**elements**

and **opens**

Find a **basis**  
of definable elements of  $\llbracket \tau \rrbracket_S$   
(terms  $M : \tau$ )

Find a **subbase**  $\mathcal{B}_\tau$   
of definable opens of  $\llbracket \tau \rrbracket_S$   
(contexts  $E : \tau \vdash S$ )

# Opens are More Important than Elements

elements

Find a basis  
of definable elements of  $\llbracket \tau \rrbracket_S$   
(terms  $M : \tau$ )

opens

Find a **subbase**  $\mathcal{B}_\tau$   
of definable opens of  $\llbracket \tau \rrbracket_S$   
(contexts  $E : \tau \vdash S$ )

Then if  $\llbracket M \rrbracket_S \not\leq \llbracket N \rrbracket_S$ ,  
for some  $U \in \mathcal{B}_\tau$ ,  $\llbracket M \rrbracket_S \in U$  and  $\llbracket N \rrbracket_S \notin U$ ,  
i.e., for some  $E$ ,  $\llbracket E[M] \rrbracket_S = \top$  and  $\llbracket E[N] \rrbracket_S = \perp$ .

By computational adequacy,  
 $\Pr(\text{val } E \cdot M \downarrow^m) = 1 > 0 = \Pr(\text{val } E \cdot N \downarrow^m)$ ,  
so **full abstraction** will hold.

# Candidates for Subbases

The canonical (sub)base in the continuous dcpo  $\llbracket \tau \rrbracket_S$  is given by  $\uparrow v$

Would require us to find term defining  $\ll$  (seems hard)

## Candidates for Subbases

The canonical (sub)base in the continuous dcpo  $\llbracket \tau \rrbracket_S$  is given by  $\uparrow v$

Would require us to find term defining  $\ll$  (seems hard). Instead:

	Basis of elements	Subbase of opens
Nat	$n, \perp$	$\uparrow n$
S	$\top, \perp$	$\uparrow \top$
$\mathbb{T}\tau$	Definable from $\delta_a = \lambda h \cdot h(a), 0$ sup (if $\mathbf{A} \in S$ ) inf (if $\mathbf{D} \in S$ ) $\frac{1}{2}(- + -)$ (if $\mathbf{P} \in S$ )	$[h > r] = \{F \mid F(h) > r\}$ (weak/Vietoris topology) where $h$ in basis of $\tau \rightarrow I$ $r \in \mathbb{Q} \cap [0, 1)$
$\sigma \rightarrow \tau$	Step functions $\sup_{i=1}^m (\bigcap_{j=1}^{n_i} U_{ij}) \searrow y_i$ $U_{ij}$ in $\mathcal{B}_\sigma$	$[a \in V] = \{f \mid f(a) \in V\}$ (pointwise convergence) $V \in \mathcal{B}_\tau$



# Subbases

This is allowed because of:  $(S \text{ among } \{A\}, \{A, P\}, \{D\}, \{D, P\})$

## Theorem

*The Scott and weak topologies coincide on  $\llbracket T\tau \rrbracket_S$ .*

## Theorem

*The Scott and pointwise conv. topologies coincide on  $\llbracket \sigma \rightarrow \tau \rrbracket_S$ .*

In general, Scott is finer. But here  $\llbracket \tau \rrbracket_S$  is a **bc-domain** for every  $\tau$ .  
(Remember we don't deal with erratic cases here, where this fails.)

**Note:** exclude **purely probabilistic** case  $S = \{P\}$ , where this fails.  
(Anyway, full abstraction seems unlikely in this case.)

## Scott = Pointwise

## Theorem

The Scott and pointwise conv. topologies *coincide* on  $[[\sigma \rightarrow \tau]]_S$ .

**Proof:** On  $\sigma \rightarrow \tau$ , Scott = compact-open topology (follows e.g. from characterization of  $\ll$  through co-step functions [EEK98])

Has subbasic opens  $[Q \subseteq V] = \{f \mid f \langle Q \rangle \subseteq V\}$ ,  
 $Q$  compact saturated,  $V$  open

Since  $Q = \bigcap_{A \text{ finite}} \uparrow A$ ,  $[Q \subseteq V] = \bigcup_{A \text{ finite}} [\uparrow A \subseteq V]$ .

And  $[\uparrow A \subseteq V] = \bigcap_{i=1}^n [a_i \in V]$ , where  $A = \{a_1, \dots, a_n\}$ . □

# Scott = Weak

Remember weak subbasic opens  $[h > r] = \{F \mid F(h) > r\}$ .

## Theorem

The Scott and weak topologies *coincide* on  $\llbracket \text{T}\tau \rrbracket_S$ .

### Proof:

$S = \{\mathbf{A}\}$  weak=lower Vietoris (subbasic  $\diamond U$ ) = Scott (since every closed subset is directed union of  $\downarrow E$ ,  $E$  finite)

$S = \{\mathbf{D}\}$  weak=upper Vietoris (subbasic  $\square U$ ) = Scott (since every  $Q$  is  $\bigcap_E \uparrow E$ )

$S = \{\mathbf{P}\}$  proved by [Kirch93], see also [Tix95, Jung04]

$S = \{\mathbf{A}, \mathbf{P}\}$  by [JGL08], Hoare previsions = retract (closed convex hull) of Hoare powerdomain on valuations, then apply previous results ( $S = \{\mathbf{A}\}$ ,  $S = \{\mathbf{P}\}$ )

$S = \{\mathbf{D}, \mathbf{P}\}$  by [JGL08], similarly.

## Definability

	Basis of elements		Subbase of opens
$\mathbb{T}\tau$	$\delta_a$ 0 sup inf $\frac{1}{2}(- + -)$	val $a$ $Y(\lambda F_{\mathbb{T}\tau} \cdot F)$ $\bigvee$ $\bigvee$ $\bigoplus$	$\{A \in S\}$ $\{D \in S\}$ $\{P \in S\}$ $[h > r] = \{F \mid F(h) > r\}$ Needs <u>statistical tester</u>
$\sigma \rightarrow \tau$	Step functions $\sup_{i=1}^m (\bigcap_{j=1}^{n_i} U_{ij}) \searrow y_i$ $\bigcap_{j=1}^{n_i} U_{ij}$ $\bigwedge_{j=1}^{n_i} \chi U_{ij}$ $\wedge$ ; $\sup_{i=1}^m$ <u>a nuisance</u>		$[a \in V] \dots E[-N]$ where $E$ defines $V$ , and $N$ defines $a$

# Return to PCF

We must show definability of two kinds of things:

- **statistical testers**  $[h > r]$
- finite **sup**s of step functions in  $\sigma \rightarrow \tau$

Both of them **fail**.

Already in PCF, `por` is missing:

- In  $\text{PCF}_{+\text{por}}$ , one can define parallel if, hence finite sups of step functions (through a convoluted trick)

# The Need for Termination Testers

We need (statistical) testers  $[h > r]$ , for  $h = \blacklozenge$   
 just at type  $S$ : **termination** testers

## Theorem

$PCF(S) + \text{por}$  is **not** fully abstract (for any  $S$ )

**Proof.** Key Lemma: every definable function  $: T\gamma \rightarrow \gamma$  is **constant**.  
 (Proof: logical relation  $R_\gamma =$  equality of values,  $R_{T\tau}$  always true.)

Let  $M = \lambda g \cdot g(\text{val } \perp)$ ,  $N = \lambda g \cdot g(\text{val } \Omega)$  ( $g : TS \rightarrow S$ ).

The only definable  $g$  are constant, so  $M \simeq^m N$  (and  $N \simeq^m M$ )

But  $\llbracket M \rrbracket_S \not\leq \llbracket N \rrbracket_S$  since

$$\llbracket M \rrbracket_S ([\blacklozenge > 1/2]) = \top \quad \llbracket N \rrbracket_S ([\blacklozenge > 1/2]) = \perp$$

# Termination Testers

Add **termination testers**  $\text{Pr}(M > b)$  to the language  $(M : \text{TS})$

$$\frac{- \cdot M \downarrow^m b \quad E \cdot \perp \downarrow^m a}{E \cdot \text{Pr}(M > b) \downarrow^m a} (\text{Pr}) \quad \llbracket \text{Pr}(M > b) \rrbracket_S = \begin{cases} \top & \text{if } \llbracket M \rrbracket_S(\blacklozenge) > b \\ \perp & \text{otherwise} \end{cases}$$

Computational adequacy: still OK.

Fully abstract now? I don't know (I don't think so.)

(Even redefining  $\approx^m$  using *extended* contexts  $E := \dots \mid \text{Pr}(\_ > b)$ )

# Searching Under the Lamppost

Let us restrict to semantic domains with a **top**  
(continuous lattices)

- Involves switching to **call-by-value**  
... so all domains are of the form  $\llbracket T\tau \rrbracket$
- Make sure all domains of the form  $\llbracket T\tau \rrbracket$  have a top:  
We shall eventually concentrate on the angelic cases  
( $S$  among  $\{A\}$ ,  $\{A, P\}$ )



# Outline

- 1 Introduction
- 2 Call-by-Name
  - Syntax
  - Operational Semantics
  - Denotational Semantics
- 3 The Full Abstraction Problem
  - Full Abstraction
  - Definability
  - The Need for Termination Testers
- 4 Call-by-Value
  - Syntax
  - Semantics
  - The Need for Statistical Termination Testers
  - Full Abstraction in Angelic Cases
- 5 Conclusion

# Call-by-Value PCF(S): Syntax

Syntax changes:

no `let/val`,  
 constants turned into operators,  
 $Y/\lambda$  merged as `rec  $f \cdot \lambda x \cdot M$` ,  
`ignore /;` omitted (definable)

$$\begin{array}{l}
 M ::= x \mid \underline{\perp} \mid \underline{n} \\
 \quad | \text{rec } f \cdot \lambda x \cdot M \\
 \quad | MN \\
 \quad | \text{pred } M \mid \text{succ } M \\
 \quad | \text{ifz } M \ N \ P \\
 \quad | M \oplus N \quad (\text{if } A \in S \text{ or } D \in S) \\
 \quad | M \oplus N \quad (\text{if } P \in S)
 \end{array}$$

## Call-by-Value PCF(S): Denotational Semantics

Types  $\tau ::= \gamma \mid \sigma \Rightarrow \tau$  (no  $\top$  type; but  $\sigma \Rightarrow \tau \stackrel{\text{def}}{=} \sigma \rightarrow \top\tau$ )

Semantics

if  $M : \tau$  then  $\llbracket M \rrbracket_S^* \in \llbracket \top\tau \rrbracket_S$ 

$$\begin{aligned}
 \llbracket x \rrbracket_S^* &= \text{val } x & \llbracket \top \rrbracket_S^* &= \text{val } \top & \llbracket n \rrbracket_S^* &= \text{val } n \\
 \llbracket \text{rec } f \cdot \lambda x \cdot M \rrbracket_S^* &= \text{val } (\text{lfp}(f, x \mapsto \llbracket M \rrbracket_S^*)) \\
 \llbracket MN \rrbracket_S^* &= \text{let } f \leftarrow \llbracket M \rrbracket_S^* \text{ in let } v \leftarrow \llbracket N \rrbracket_S^* \text{ in } f(v) \\
 \llbracket \text{pred } M \rrbracket_S^* &= (h \mapsto \llbracket M \rrbracket_S^* (n \neq 0 \mapsto h(n-1) \mid 0 \mapsto 0)) \\
 \llbracket \text{succ } M \rrbracket_S^* &= \text{let } n \leftarrow \llbracket M \rrbracket_S^* \text{ in } n + 1 \\
 \llbracket \text{ifz } M \ N \ P \rrbracket_S^* &= \text{let } n \leftarrow \llbracket M \rrbracket_S^* \text{ in } (\llbracket N \rrbracket_S^* \text{ if } n = 0, \llbracket P \rrbracket_S^* \text{ else}) \\
 \llbracket M \otimes N \rrbracket_S^* &= \llbracket \otimes \rrbracket_S (\llbracket M \rrbracket_S^*) (\llbracket N \rrbracket_S^*) & \llbracket M \oplus N \rrbracket_S^* &= \llbracket \oplus \rrbracket_S (\llbracket M \rrbracket_S^*) (\llbracket N \rrbracket_S^*) \\
 \text{where} & \text{val } a &= (h \mapsto h(a)) \\
 & \text{let } v \leftarrow F \text{ in } G(v) &= (h \mapsto F(v \mapsto G(v)(h)))
 \end{aligned}$$

... we now need *subnormalized* previsions ( $F(\frac{a+h}{2}) \leq \frac{1}{2}(a + F(h))$ )  
 + no  $\perp$  in base types:  $\llbracket \text{Nat} \rrbracket_S = \mathbb{N}$ ,  $\llbracket \text{S} \rrbracket_S = \{\top\}$

# Operational Semantics

New notion: **values**  $V = \text{rec } f \cdot \lambda x \cdot M \mid \underline{\top} \mid \underline{n}$   
 ... if  $f$  not free in  $M$ ,  $\text{rec } f \cdot \lambda x \cdot M$  written  $\lambda x \cdot M$

Semantically,  $\llbracket V \rrbracket_S^* = \text{val}(\llbracket V \rrbracket_S^\circ)$  where  
 $\llbracket \text{rec } f \cdot \lambda x \cdot M \rrbracket_S^\circ = \text{lfp}(f, x \mapsto \llbracket M \rrbracket_S^*)$ ,  $\llbracket \underline{\top} \rrbracket_S^\circ = \top$ ,  $\llbracket \underline{n} \rrbracket_S^\circ = n$

**Contexts**  $E : \sigma \vdash S$  (rather  $\sigma \vdash \text{TS}$ ) are now:

$$\begin{array}{l}
 E := \_ \\
 | \quad E[_N] \\
 | \quad E[(\text{rec } f \cdot \lambda x \cdot M)\_] \quad (\text{new}) \\
 | \quad E[\text{succ } \_] \mid E[\text{pred } \_] \\
 | \quad E[\text{ifz } \_ N P]
 \end{array}$$

# The CBV PCF(S) Machine

## 1 Redex Discovery Rules

$$\begin{aligned}
 E \cdot MN &\rightarrow E[_N] \cdot M \\
 E[_N] \cdot \text{rec } f \cdot \lambda x \cdot M &\rightarrow E[(\text{rec } f \cdot \lambda x \cdot M)_] \cdot N \quad (\text{new}) \\
 E \cdot \text{pred } M &\rightarrow E[\text{pred } _] \cdot M & E \cdot \text{succ } M &\rightarrow E[\text{succ } _] \cdot M \\
 E \cdot \text{ifz } M N P &\rightarrow E[\text{ifz } _ N P] \cdot M
 \end{aligned}$$

## 2 Computation

$$\begin{aligned}
 E[V_f _] \cdot V &\rightarrow E.M[f := V_f, x := V] \quad \text{where } V_f = \text{rec } f \cdot \lambda x \cdot M \\
 E[\text{pred } _] \cdot \underline{n+1} &\rightarrow E \cdot \underline{n} & E[\text{succ } _] \cdot \underline{n} &\rightarrow E \cdot \underline{n+1} \\
 E[\text{ifz } _ N P] \cdot \underline{0} &\rightarrow E \cdot N & E[\text{ifz } _ N P] \cdot \underline{n+1} &\rightarrow E \cdot P
 \end{aligned}$$

3 Choice states are now  $E \cdot M \otimes N, E \cdot M \oplus N$

4 Termination state:  $_ \cdot \underline{\top}$

# Termination Semantics

Essentially the same as before:

$$\frac{C' \downarrow^m a}{C \downarrow^m a} (C \rightarrow C') \quad \frac{}{- \cdot \perp \downarrow^m a} (a \in \mathbb{Q} \cap [0, 1))$$

$$\frac{E \cdot M \downarrow^{\text{may}} a}{E \cdot M \otimes N \downarrow^{\text{may}} a} \quad \frac{E \cdot N \downarrow^{\text{may}} a}{E \cdot M \otimes N \downarrow^{\text{may}} a} \quad \frac{E \cdot M \downarrow^{\text{must}} a \quad E \cdot N \downarrow^{\text{must}} a}{E \cdot M \otimes N \downarrow^{\text{must}} a}$$

$$\frac{E \cdot M \downarrow^m a \quad E \cdot N \downarrow^m b}{E \cdot M \oplus N \downarrow^m \frac{1}{2}(a+b)} (\oplus) \quad (m \in \{\text{may}, \text{must}\})$$

# Soundness

## Theorem (Soundness)

- $\llbracket E[M] \rrbracket_S^* (\blacklozenge) \geq Pr(E \cdot M \downarrow^{\text{may}})$  (if  $S \subseteq \{A, P\}$ )
- $\llbracket E[M] \rrbracket_S^* (\blacklozenge) \geq Pr(E \cdot M \downarrow^{\text{must}})$  (if  $S \subseteq \{D, P\}$ )

**Proof:** induction, using  $\llbracket E[M] \rrbracket_S^* (\blacklozenge) = \llbracket M \rrbracket_S^* (h)$  for some  $h$  depending on  $E$  only. □

# Computational Adequacy

## Theorem (Computational Adequacy)

- $\llbracket M \rrbracket_S^* (\blacklozenge) = Pr(- \cdot M \downarrow^{\text{may}})$  (if  $S \subseteq \{A, P\}$ )
- $\llbracket M \rrbracket_S^* (\blacklozenge) = Pr(- \cdot M \downarrow^{\text{must}})$  (if  $S \subseteq \{D, P\}$ )

**Proof:** Define logical relation  $R_\tau^*$  (terms),  $R_\tau^\perp$  (contexts),  $R_\tau^\circ$  (values):

$$M R_\sigma^* F \quad \text{iff} \quad \text{for all } E R_\sigma^\perp h, Pr(E \cdot M \downarrow^m) \geq F(h)$$

$$E R_\sigma^\perp h \quad \text{iff} \quad \text{for all } V R_\sigma^\circ v, Pr(E \cdot V \downarrow^m) \geq h(v)$$

$$V_f R_{\sigma \Rightarrow \tau}^\circ \varphi \quad \text{iff} \quad \text{for all } V R_\sigma^\circ v, E R_\tau^\perp h, Pr(E[V_f \_ ] \cdot V \downarrow^m) \geq \varphi(v)(h)$$

$$\underline{m} R_{\text{Nat}}^\circ n \quad \text{iff} \quad m = n \quad \quad \underline{\top} R_S^\circ \top$$

Show  $V R_\tau^\circ \llbracket V^\circ \rrbracket_S$  and  $M R_\tau^* \llbracket M^* \rrbracket_S$ .

Finally take  $E = \_$ ,  $h = \blacklozenge$  at  $\tau = S$ . □



# Statistical Termination Testers

Do we still need **termination testers**?

Theorem (Yes, in Probabilistic Cases

( $\mathbb{P} \in \mathcal{S}$ ))

*CBV PCF( $\mathcal{S}$ ) without termination testers is **not** fully abstract*

**Proof.** Define logical relation  $R_{\tau}^*$ ,  $R_{\tau}^{\perp}$ ,  $R_{\tau}^{\circ}$ :

$$\begin{aligned} \top R_{\mathcal{S}}^{\circ} \top & \quad n_1 R_{\text{Nat}}^{\circ} n_2 \text{ iff } n_1 = n_2 \\ f_1 R_{\sigma \Rightarrow \tau}^{\circ} f_2 & \quad \text{iff for all } v_1 R_{\sigma}^{\circ} v_2, f_1(v_1) R_{\tau}^* f_2(v_2) \\ F_1 R_{\tau}^* F_2 & \quad \text{iff for all } h_1 R_{\tau}^{\perp} h_2, F_1(h_1) \sim_0 F_2(h_2) \\ h_1 R_{\tau}^{\perp} h_2 & \quad \text{iff for all } v_1 R_{\tau}^{\circ} v_2, h_1(v_1) \sim_0 h_2(v_2) \\ a_1 \sim_0 a_2 & \quad \text{iff } a_1 = a_2 = 0 \text{ or } (a_1 \neq 0 \text{ and } a_2 \neq 0) \end{aligned}$$

Then  $[\blacklozenge > r] = (h \mapsto \begin{cases} \text{val } \top & \text{if } h(\top)(\blacklozenge) > r \\ 0 & \text{else} \end{cases})$  is not in relation with itself, hence not definable (of type  $(\mathcal{S} \Rightarrow \mathcal{S}) \Rightarrow \mathcal{S} \sim \text{TS} \rightarrow \text{TS}$ )  $\square$

# Statistical Termination Testers

Do we still need **termination testers**?

Theorem (Yes, in Probabilistic Cases

( $\mathbb{P} \in \mathcal{S}$ ))

*CBV PCF( $\mathcal{S}$ ) without termination testers is **not** fully abstract*

**Proof.** Define logical relation  $R_{\tau}^*$ ,  $R_{\tau}^{\perp}$ ,  $R_{\tau}^{\circ}$ :

$$\begin{aligned} \top R_{\mathcal{S}}^{\circ} \top & \quad n_1 R_{\text{Nat}}^{\circ} n_2 \text{ iff } n_1 = n_2 \\ f_1 R_{\sigma \Rightarrow \tau}^{\circ} f_2 & \quad \text{iff for all } v_1 R_{\sigma}^{\circ} v_2, f_1(v_1) R_{\tau}^* f_2(v_2) \\ F_1 R_{\tau}^* F_2 & \quad \text{iff for all } h_1 R_{\tau}^{\perp} h_2, F_1(h_1) \sim_0 F_2(h_2) \\ h_1 R_{\tau}^{\perp} h_2 & \quad \text{iff for all } v_1 R_{\tau}^{\circ} v_2, h_1(v_1) \sim_0 h_2(v_2) \\ a_1 \sim_0 a_2 & \quad \text{iff } a_1 = a_2 = 0 \text{ or } (a_1 \neq 0 \text{ and } a_2 \neq 0) \end{aligned}$$

Then  $[\blacklozenge > r] = (h \mapsto \begin{cases} \text{val } \top & \text{if } h(\top)(\blacklozenge) > r \\ 0 & \text{else} \end{cases})$  is not in relation with itself, hence not definable (of type  $(\mathcal{S} \Rightarrow \mathcal{S}) \Rightarrow \mathcal{S} \sim \text{TS} \rightarrow \text{TS}$ )  $\square$

Fact (No, in Non-Probabilistic Cases

( $\mathbb{P} \notin \mathcal{S}$ ))

Can define  $\text{Pr}(M > r)$  as  $M$  if  $r \in [0, 1]$

# Statistical Termination Testers

Add **termination testers**  $\Pr(M > b)$  to the language  $(M : S)$

$$\frac{- \cdot M \downarrow^m b \quad E \cdot \top \downarrow^m a}{E \cdot \Pr(M > b) \downarrow^m a} (\text{Pr})$$

$$\llbracket \Pr(M > b) \rrbracket_S^* = \begin{cases} \text{val } \top & \text{if } \llbracket M \rrbracket_S^*(\blacklozenge) > b \\ 0 & \text{otherwise} \end{cases}$$

Computational adequacy: still OK.

# The Angelic+Probabilistic Case

Let  $M \lesssim^m N$  iff  $\Pr(\cdot \cdot E'[M] \downarrow^m) \leq \Pr(\cdot \cdot E'[N] \downarrow^m)$   
 for every **extended** context  $E'$   $E' ::= \dots \mid \Pr(\cdot > b)$

Theorem (Case  $S = \{A, P\}$ )

Full abstraction holds for  $PCF(\{A, P\})$  + statistical testers:

$$M \lesssim^{\text{may}} N \text{ iff } \llbracket M \rrbracket_{\{A, P\}} \leq \llbracket N \rrbracket_{\{A, P\}}$$

## Proof.

- Open subbase  $[a \mapsto h > r] = \{f \in \llbracket \sigma \Rightarrow \tau \rrbracket_S \mid f(a)(h) > r\}$   
 definable by  $E[\Pr(\cdot > r)][V_{h-}][V_a]$
- Basis of values definable from  $\odot, \oplus, \text{val}, \Omega$  (0)  
 The “nuisance”  $\sup_{i=1}^m$  is definable through  $\odot$  (= sup). □

**Note:** no need for por.

# The Purely Angelic Case

Let  $M \lesssim^m N$  iff  $\Pr(\cdot \cdot E[M] \downarrow^m) \leq \Pr(\cdot \cdot E[N] \downarrow^m)$   
 for every **ordinary** context  $E$  (no need for  $\Pr(\cdot > b)$ )

Theorem (Case  $S = \{A\}$ )

Full abstraction holds for  $PCF(\{A\})$ :

$$M \lesssim^{\text{may}} N \text{ iff } M \lesssim^{\text{may}} N \text{ iff } \llbracket M \rrbracket_{\{A\}} \leq \llbracket N \rrbracket_{\{A\}}$$

**Proof.** Same argument, except termination testers are definable  
 ( $\Pr(M > b) = M$  if  $b \in [0, 1)$ ) □

**Note:** no need for  $\text{por}$ , no need for  $\Pr(M > b)$

Fully abstract, as is!

# The Purely Angelic Case: Standard Semantics

If  $S = \{A\}$ , note that previsions  $\cong$  Hoare powerdomain (with  $\emptyset$ )

We obtain a **standard** call-by-value semantics for non-determinism

$$\begin{aligned}
 \llbracket x \rrbracket_S^* &= \downarrow x & \llbracket \top \rrbracket_S^* &= \{\top\} & \llbracket n \rrbracket_S^* &= \{n\} \\
 \llbracket \text{rec } f \cdot \lambda x \cdot M \rrbracket_S^* &= \downarrow (\text{lfp}(f, x \mapsto \llbracket M \rrbracket_S^*)) \\
 \llbracket MN \rrbracket_S^* &= \bigcup_{f \in \llbracket M \rrbracket_S^*, v \in \llbracket N \rrbracket_S^*} f(v) \\
 \llbracket \text{pred } M \rrbracket_S^* &= \{n-1 \mid n \in \llbracket M \rrbracket_S^*, n \neq 0\} \\
 \llbracket \text{succ } M \rrbracket_S^* &= \{n+1 \mid n \in \llbracket M \rrbracket_S^*\} \\
 \llbracket \text{ifz } M N P \rrbracket_S^* &= \begin{cases} \emptyset & \text{if } \llbracket M \rrbracket_S^* = \emptyset \\ \llbracket N \rrbracket_S^* & \text{if } \llbracket M \rrbracket_S^* = \{0\} \\ \llbracket P \rrbracket_S^* & \text{if } \llbracket M \rrbracket_S^* \neq \emptyset, \text{ does not contain } 0 \\ \llbracket M \rrbracket_S^* \cup \llbracket P \rrbracket_S^* & \text{if } \llbracket M \rrbracket_S^* \text{ contains } 0 \text{ and some } n \neq 0 \end{cases} \\
 \llbracket M \odot N \rrbracket_S^* &= \llbracket M \rrbracket_S^* \cup \llbracket N \rrbracket_S^*
 \end{aligned}$$

... and we have shown this was fully abstract.

# Outline

- 1 Introduction
- 2 Call-by-Name
  - Syntax
  - Operational Semantics
  - Denotational Semantics
- 3 The Full Abstraction Problem
  - Full Abstraction
  - Definability
  - The Need for Termination Testers
- 4 Call-by-Value
  - Syntax
  - Semantics
  - The Need for Statistical Termination Testers
  - Full Abstraction in Angelic Cases
- 5 Conclusion

# Conclusion

The **angelic** cases ... are angelic:

- Call-by-value  $\text{PCF}(\{A\})$  is **fully abstract**
- Call-by-value  $\text{PCF}(\{A, P\})$  + **statistical termination testers**  
is **fully abstract**

- Similar results for **demonic** cases + new primitive “irq”

- **Erratic** cases easy consequences of the above

Difficulty:  $\llbracket \tau \rrbracket_S$  not a bc-domain

... but semantics is pair of angelic/demonic semantics

- Purely **probabilistic** case hopeless (valuations/lin. previsions)

$\llbracket \tau \rrbracket_S$  not a bc-domain, no known cure [JungTix98]

... even FS-domains would not help (see “nuisance”)

- What about using **random variables** [JGLVaracca11] instead?

form bc-domains again, but should require extra testers

- Call-by-name cases seem hard.



# Dealing with the Demonic Cases

**Problem:** in the **demonic** cases ( $\mathbf{D} \in S$ ),  $\llbracket \mathbf{T}\tau \rrbracket_S$  has no top

**Cure:** add one.

Let  $X^{\text{err}}$  be  $X$  with a fresh top element **err** (**abnormal** termination)  
(not really the space we shall work with)

Previsions on  $X^{\text{err}}$  are the same as lax previsions on  $X$ :

## Definition (Lax Prevision)

Let *lax* map previsions  $F$  on  $X^{\text{err}}$  to  $(h \in [X \rightarrow I] \mapsto F(\widehat{h}))$ ,  
where  $\widehat{h}(x) = h(x)$  ( $x \in X$ ) and  $\widehat{h}(\text{err}) = 1$ .

The functionals in the range of *lax* are the **lax previsions** on  $X$

- Every prevision is a lax prevision
- $h \mapsto 1$  is largest (**top**) lax prevision ( $= \text{lax}(\delta_{\text{err}})$ )
- Lax prev. closed under  $\frac{+}{2}$  ( $\mathbf{P} \in S$ ), **min** ( $\mathbf{D} \in S$ ), **max** ( $\mathbf{A} \in S$ )

## CBV PCF(S)+ irq

New syntax:  $M \text{ irq } N : \tau$  (if  $M : \tau$ ,  $N : S$ )  
(at every type  $\tau$ )

New operational rules

$$\frac{E \cdot M \downarrow^m a}{E \cdot M \text{ irq } N \downarrow^m a} \quad \frac{\_ \cdot N \downarrow^m a}{E \cdot M \text{ irq } N \downarrow^m a}$$

Run  $M$  with  $N$  in background: if  $N$  terminates, kill  $M$  and abort

**Note:** abort =  $M \text{ irq } \perp$  **aborts** immediately ( $M$  arbitrary)

Den. semantics:  $\llbracket M \text{ irq } N \rrbracket_S^* (h) = \max(\llbracket M \rrbracket_S^* (h), \llbracket N \rrbracket^* (\blacklozenge))$

Soundness, computational adequacy: still OK.

# The Demonic+Probabilistic Case

## Theorem (Case $S = \{\mathbf{D}, \mathbf{P}\}$ )

Full abstraction holds for  $\text{PCF}(\{\mathbf{D}, \mathbf{P}\}) + \text{irq} + \text{statistical testers}$ :

$$M \underset{\sim}{\lesssim}^{\text{must}} N \text{ iff } \llbracket M \rrbracket_{\{\mathbf{D}, \mathbf{P}\}} \leq \llbracket N \rrbracket_{\{\mathbf{D}, \mathbf{P}\}}$$

### Proof.

- Open subbase  $[a \mapsto h > r] = \{f \in \llbracket \sigma \Rightarrow \tau \rrbracket_S \mid f(a)(h) > r\}$   
 definable by  $E[\text{Pr}(\_ > r)][V_{h-}][\_ - V_a]$   
 Note that Scott=weak again on lax previsions
- Basis of values definable from  $\odot$ ,  $\oplus$ ,  $\text{val}$ ,  $\Omega$ , and  $\text{abort}$ .

“Nuisance”  $\sup_{i=1}^m$ : use “sup-as-inf” trick:

$$\sup_{i=1}^m (U_i \searrow F_i)(x) = \min_{I \subseteq \{1, \dots, m\}} F_I \text{ irq } \chi_{\bigcup_{i \notin I} U_i}(x)$$

where  $F_I = \sup_{i \in I} F_i$  (exists since bc-domain)

$F \text{ irq } \top = (h \mapsto 1)$ ,  $F \text{ irq } \perp = F \dots$  definable through  $\text{irq}$   
 and  $\min$  definable through  $\odot$ .

# The Purely Demonic Case

Again, termination testers are definable when  $P \notin S$

Theorem (Case  $S = \{D\}$ )

Full abstraction holds for  $PCF(\{D\}) + \text{irq}$ :

$$M \lesssim^{\text{must}} N \text{ iff } M \approx^{\text{must}} N \text{ iff } \llbracket M \rrbracket_{\{D\}} \leq \llbracket N \rrbracket_{\{D\}}$$

# Back to the Angelic Cases

Everything works with lax previsions and `irq` as before  
 in **angelic** cases

## Theorem (Case $S = \{A\}$ )

Full abstraction holds for  $PCF(\{A\}) + \text{irq}$ :

$$M \lesssim^{\text{may}} N \text{ iff } M \approx^{\text{may}} N \text{ iff } \llbracket M \rrbracket_{\{A\}} \leq \llbracket N \rrbracket_{\{A\}}$$

## Theorem (Case $S = \{A, P\}$ )

Full abstraction holds for  $PCF(\{A, P\}) + \text{irq} + \text{statistical testers}$ :

$$M \lesssim^{\text{may}} N \text{ iff } \llbracket M \rrbracket_{\{A, P\}} \leq \llbracket N \rrbracket_{\{A, P\}}$$

# The Erratic Cases

When  $\{A, D\} \subseteq S$ , semantics given in terms of forks [JGL-CSL07]

## Definition

A *fork* is a pair  $(F^-, F^+)$  of a Hoare and a Smyth prevision satisfying **Walley's condition**:

$$F^-\left(\frac{h + h'}{2}\right) \leq \frac{F^-(h) + F^+(h')}{2} \leq F^+\left(\frac{h + h'}{2}\right)$$

Ordered componentwise.

(Define lax forks similarly.)

**Difficulty:** (lax) forks do **not** form a bc-domain

... but we don't care here

# Erratic = Angelic + Demonic

Assume  $\{A, D\} \subseteq S$ . Let  $S^- = S \cap \{D, P\}$ ,  $S^+ = S \cap \{A, P\}$ .

We don't care because:

## Lemma

$$\llbracket M \rrbracket_S^* = (\llbracket M \rrbracket_{S^-}^*, \llbracket M \rrbracket_{S^+}^*)$$

... merely **ignoring** Walley's condition

Now, if  $\llbracket M \rrbracket_S^* \not\leq \llbracket N \rrbracket_S^*$ , either:

- $\llbracket M \rrbracket_{S^-}^* \not\leq \llbracket N \rrbracket_{S^-}^*$ : since **demonic** cases are fully abstract, there is an  $E$  such that  $\text{Pr}(- \cdot E[M] \downarrow^{\text{must}}) \not\leq \text{Prob}(- \cdot E[M] \downarrow^{\text{must}})$
- or  $\llbracket M \rrbracket_{S^+}^* \not\leq \llbracket N \rrbracket_{S^+}^*$ : since **angelic** cases are fully abstract, there is an  $E$  such that  $\text{Pr}(- \cdot E[M] \downarrow^{\text{may}}) \not\leq \text{Prob}(- \cdot E[M] \downarrow^{\text{may}})$

# Full Abstraction in the Erratic Cases

For  $\{A, D\} \subseteq S$ , let  $M \lesssim N$  iff  $M \lesssim^{\text{may}} N$  and  $M \lesssim^{\text{must}} N$

(i.e., with *extended* contexts, including  $E[\text{Pr}(\_ > b)]$ )  
(and similarly for  $\lesssim$ , with ordinary contexts)

We therefore obtain:

**Theorem (Case  $S = \{A, D\}$ )**

*Full abstraction holds for  $\text{PCF}(\{A, D\}) + \text{irq}$ :*

$$M \lesssim N \text{ iff } M \approx N \text{ iff } \llbracket M \rrbracket_{\{A, D\}} \leq \llbracket N \rrbracket_{\{A, D\}}$$

**Theorem (Case  $S = \{A, D, P\}$ )**

*Full abstraction holds for  $\text{PCF}(\{A, D, P\}) + \text{irq} + \text{statistical testers}$ :*

$$M \lesssim N \text{ iff } \llbracket M \rrbracket_{\{A, D, P\}} \leq \llbracket N \rrbracket_{\{A, D, P\}}$$