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 \textit{por}

Here, PCF plus specific \textit{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

\[
\begin{align*}
\gamma & ::= \text{Nat} \mid S & \text{Ground types} \\
\sigma, \tau & ::= \gamma \mid \sigma \rightarrow \tau \mid T\tau & \text{Types} 
\end{align*}
\]

Notes:
- \(S\) has only one (non-bottom) value
  - \(=\) \textit{unit type}, \textit{termination type}
  - Not required in principle, but practical
- \(T\tau\) type of \textit{processes} computing value of type \(\tau\)

\(\text{à la [Moggi91]}\)
PCF(S) Terms

Language parameterized by set $S \subseteq \{A, D, P\}$

(angelic non-det., demonic non-det., probabilistic choice).

- PCF terms
  \[
  (\lambda\text{-calculus} + \text{basic arithmetic} + \text{ifz} + \text{fixpoint } Y)
  \]

- At $S$ type:
  - $\top : S$
  - for every $M : \text{Nat}$, ignore $M : S$
  - for all $M : S, N : \sigma$, sequencing $M; N : \sigma$

- At $T_\tau$ types:
  - for each $M : \tau$, $\text{val } M : T_\tau$
  - for all $M : \sigma, N : T_\tau$, let $x \leftarrow M$ in $N : T_\tau$
  - Non-det. choice $\text{\bigvee} : T_\tau \rightarrow T_\tau \rightarrow T_\tau$ (if $A \in S$ or $D \in S$)
  - Prob. choice $\text{\bigoplus} : T_\tau \rightarrow T_\tau \rightarrow T_\tau$ (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 $E : (\sigma \vdash TS) =$ stacks of pending operations:

\[
E \quad ::= \\- E[N] \quad | \quad E[\text{succ } \_] \mid E[\text{pred } \_] \\
| \quad E[\text{ifz } N P] \mid E[\_ ; N] \\
| \quad E[\text{ignore } \_] \\
| \quad \text{val } \_ \\
| \quad E[\text{let } x \leftarrow \_ \text{ in } N]
\]
The PCF(S) Machine: 1. Redex Discovery Rules

Purpose: move top of \( M \) into context \( E \), until redex appears

\[
E \cdot MN \rightarrow E[_N] \cdot M \\
E[_N] \cdot \text{pred} \rightarrow E[\text{pred }_] \cdot N \\
E[_N] \cdot \text{succ} \rightarrow E[\text{succ }_] \cdot N \\
E[_MNP] \cdot \text{ifz} \rightarrow E[\text{ifz } N P] \cdot M \\
E \cdot M; N \rightarrow E[_; N] \cdot M \\
E[_N] \cdot \text{ignore} \rightarrow E[\text{ignore }_] \cdot N \\
_\cdot \text{val } M \rightarrow \text{val }_ \cdot M \\
E \cdot \text{let } x \leftarrow M \text{ in } N \rightarrow E[\text{let } x \leftarrow _\text{in } N] \cdot M
\]
The PCF(S) Machine: 2. Computation

**Redex** = interaction between top of \( M \) and bottom of \( E \)

\[
\begin{align*}
E[N] \cdot \lambda x \cdot P & \rightarrow E \cdot P[x := N] \\
E[pred \_ \_] \cdot n + 1 & \rightarrow E \cdot n \\
E[succ \_ \_] \cdot n & \rightarrow E \cdot n + 1 \\
E[ifz \_ \_ N P] \cdot 0 & \rightarrow E \cdot N \\
E[ifz \_ \_ N P] \cdot n + 1 & \rightarrow E \cdot P \\
E[\_; N] \cdot \top & \rightarrow E \cdot N \\
E[ignore \_ \_ \_] \cdot n & \rightarrow E \cdot \top \\
E[\_N] \cdot Y & \rightarrow E \cdot N(YN) \\
E[let x \_ := \_ \_ in P] \cdot \text{val} N & \rightarrow E \cdot P[x := N]
\end{align*}
\]

**Termination state:** \( \text{val} \_ \cdot \top \)
The choice states are:

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

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

$$E[MN] \cdot \bigcirc \rightarrow M \quad E[MN] \cdot \bigcirc \rightarrow N$$

$$E[MN] \cdot \bigoplus \rightarrow M \quad E[MN] \cdot \bigoplus \rightarrow N$$
Reachability Objectives

\[ S = \emptyset \] reachability: does \( E \cdot M \rightarrow^* \text{val} \cdot \top \)?

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

\[ S = \{ A \} \] may testing: \( \exists \) terminating path \( E \cdot M \rightarrow^* \text{val} \cdot \top \) ?

\[ S = \{ D \} \] must testing: \( \forall \) paths terminate?

\[ S = \{ A, P \} \] \( \exists \) scheduler \( \varsigma \) / \( \Pr[E \cdot M \rightarrow^*_\varsigma \text{val} \cdot \top] > r \)?

(pure, memoryless) schedulers map \( E \cdot \emptyset \) to left/right

\[ S = \{ D, P \} \] min\( \varsigma \) scheduler \( \Pr[E \cdot M \rightarrow^*_\varsigma \text{val} \cdot \top] > r \)?

\( \{ A, D \} \subseteq S \) 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 $C \rightarrow C'$:

  $\frac{C' \downarrow^m a}{C \downarrow^m a}$

  (e.g., $E \cdot P[x := N] \downarrow^m a$

  $E[N] \cdot \lambda x \cdot P \downarrow^m a$)

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

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

- Choice: see next slide (obviously the most important part)
Termination Semantics (2/2)

Choice:

\[
\begin{align*}
E \cdot M \downarrow^\text{may} a & \quad \Rightarrow \quad E[\_MN] \cdot \bigvee \downarrow^\text{may} a \\
E[\_MN] \cdot \bigvee \downarrow^\text{may} a & \quad \Rightarrow \quad E \cdot N \downarrow^\text{may} a
\end{align*}
\]

\[
E \cdot M \downarrow^\text{must} a \quad E \cdot N \downarrow^\text{must} a
\]

\[
E \cdot M \downarrow^m a \quad E \cdot N \downarrow^m b
\]

\[
E[\_MN] \cdot \bigoplus \downarrow^m \frac{1}{2}(a+b)
\]

\[
(m \in \{\text{may, must}\})
\]

Definition

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

- \[
\Pr(\text{val } \cdot \top \downarrow^m) = 1
\]
- \[
\Pr(E[\_MN] \cdot \bigoplus \downarrow^m) = \frac{1}{2}(\Pr(E \cdot M \downarrow^m) + \Pr(E \cdot N \downarrow^m))
\]
- \[
\Pr(E[\_MN] \cdot \bigvee \downarrow^\text{may}) = \max(\Pr(E \cdot M \downarrow^\text{may}), \Pr(E \cdot N \downarrow^\text{may}))
\]
- \[
\Pr(E[\_MN] \cdot \bigvee \downarrow^\text{must}) = \min(\Pr(E \cdot M \downarrow^\text{must}), \Pr(E \cdot N \downarrow^\text{must})).
\]
Denotational Semantics: Previsions

Let $[[T \tau]]_S$ as spaces of previsions over $[[\tau]]_S$ [JGL-CSL07]

Definition (Prevision on $X$)

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

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

\[
\begin{align*}
[x]_S &= x & [\top]_S &= \top & [n]_S &= n \in \mathbb{N} \\
[\lambda x \cdot M]_S &= (x \mapsto [M]_S) & [MN]_S(\rho) &= [M]_S([N]_S) \\
[Y]_S &= (f \mapsto \bigcup_{n \in \mathbb{N}} f^n(\bot)) \\
[pred]_S &= (\nu \in \mathbb{N} \setminus \{0\} \mapsto \nu - 1 \mid 0, \bot \mapsto \bot) \\
[succ]_S &= (\nu \in \mathbb{N} \mapsto \nu + 1 \mid \bot \mapsto \bot) \\
[ifz]_S &= (0, t, e \mapsto t \mid n \in \mathbb{N} \setminus \{0\}, t, e \mapsto e \mid \bot \mapsto \bot) \\
[M; N]_S &= [N]_S \text{ if } [M]_S \neq \bot, \text{ else } \bot \\
[ignore]_S &= (n \in \mathbb{N} \mapsto \top \mid \bot \mapsto \bot) \\
[val \ M : T]_S &= (h \mapsto h([M]_S)) \\
[let \ x \leftarrow M \ in N]_S &= (h \mapsto [M]_S(x \mapsto [N]_S(h))) \\
[S]_S &= (F_1, F_2, h \mapsto \max(F_1(h), F_2(h))) \quad \text{(if } A \in S) \\
[S]_S &= (F_1, F_2, h \mapsto \min(F_1(h), F_2(h))) \quad \text{(if } D \in S) \\
[S]_S &= (F_1, F_2, h \mapsto \frac{1}{2}(F_1(h) + F_2(h))) \quad \text{(if } P \in S) 
\end{align*}
\]
In usual PCF, **soundness** states that if $M \rightarrow^* V$ then $\llbracket M \rrbracket = \llbracket V \rrbracket$.

**Theorem (Soundness)**

Let $\diamondsuit = \chi\{\top\} : \llbracket S \rrbracket \rightarrow l$ map $\bot$ to 0, $\top$ to 1.

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

**Proof:** induction.  

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

**Theorem (Soundness)**

Let $\diamond = \chi_{\{T\}} : [S] \rightarrow I$ map $\bot$ to 0, $T$ 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 \( \text{TS} \vdash \text{TS} \)).

**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 \( M \preceq^m N \) iff \( \Pr(E \cdot M \downarrow^m) \leq \Pr(E \cdot N \downarrow^m) \) for every \( E \).

- \( M[x := N] \preceq^m (\lambda x \cdot M)N \)
- \( n \preceq^m M \Rightarrow n + 1 \preceq^m \text{succ} M \)
- \( 0 \preceq^m M \Rightarrow N \preceq^m \text{ifz} M \cdot N \cdot P \)
- \( \top \preceq^m M \Rightarrow N \preceq^m M; N \)
- \( n \preceq^m M \Rightarrow \top \preceq^m \text{ignore} M \)
- \( n + 1 \preceq^m M \Rightarrow n \preceq^m \text{pred} M \)
- \( n + 1 \preceq^m M \Rightarrow P \preceq^m \text{ifz} M \cdot N \cdot P \)
In usual PCF, $M \rightarrow^\ast V$ iff $\llbracket M \rrbracket = \llbracket V \rrbracket$, at ground types.

Theorem (Computational Adequacy)

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

**Proof:** Let $M \preceq^m N$ 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 $u = \bot$, or $u = \top$ and $\top \preceq^m M$
- $M R_{\text{Nat}} n$ iff $n = \bot$, or $n \in \mathbb{N}$ and $n \preceq^m M$
- $M R_{\tau \rightarrow^\tau} f$ iff for all $N R_\sigma v$, $MN R_\tau f(v)$
- $M R_{T\sigma} F$ iff for all $E R_\sigma h$, $\Pr(E \cdot M\downarrow^m) \geq F(h)$
- $E R_\sigma h$ 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 \([M] = [V]\), at ground types.
Here, use \( E = \_\) (empty context, of type \( TS \vdash TS \))

Theorem (Computational Adequacy)

- \([M]_S (\Diamond) = \Pr(\_ \cdot M \downarrow^\text{may}) \quad (if \ S \subseteq \{A, P\})
- \([M]_S (\Diamond) = \Pr(\_ \cdot M \downarrow^\text{must}) \quad (if \ S \subseteq \{D, P\})

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

Define a logical relation \( R_\sigma: \)
- \( M R_{T \sigma} F \) 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 \( Q R_\sigma v, \Pr(E \cdot \text{val} Q \downarrow^m) \geq h(v) \)

By definition, \( \_ R_S^\perp \Diamond \)

Basic Lemma: \( M R_\tau [M]_S \) for every \( M : \tau \)
For all \( E R_\tau^\perp h, \Pr(E \cdot M \downarrow^m) \geq [M]_S (h) \)
Conclude by taking \( E = \_, h = \Diamond\).
Full Abstraction for PCF with Choice

The Full Abstraction Problem

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
Definition (Full Abstraction)

\[ M \lesssim^m N \text{ iff } \llbracket M \rrbracket_S \leq \llbracket N \rrbracket_S, \text{ at all types.} \]

- 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 \( E : \tau \vdash TS \)
  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 \( M \lesssim^m N \).
Full Abstraction for PCF with Choice

Full Abstraction

Definition (Full Abstraction)

\[ M \sim^m N \iff \llbracket M \rrbracket_S \leq \llbracket N \rrbracket_S, \text{ at all types.} \]

- **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 \( E : \tau \vdash TS \)
  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 \( M \sim^m N \).

- **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
Full Abstraction

Definition (Full Abstraction)

\[ M \sim^m N \text{ iff } \llbracket M \rrbracket_S \leq \llbracket N \rrbracket_S \text{, at all types.} \]

- 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 \( E : \tau \vdash TS \)
  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 \( M \sim^m N \).

- 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)
  \[ \ldots \text{so one should do something about this} \]
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 $\text{PCF} + \text{por}$, the finite elements of $[\tau]$ are exactly those of the form $[M]$, $M : \tau$.

This is bound to fail here:
if $P \in S$, then $[\tau]$ is a continuous, not an algebraic domain.
Strategies for Proving Full Abstraction

Plotkin showed full abstraction using definitability (needed anyway)

**Theorem (Plotkin77)**

In $PCF^{\text{por}}$, 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 definitability result, of both

- elements
- and opens

Find a basis of definable elements of $\llbracket \tau \rrbracket_S$ (terms $M : \tau$)
Find a subbase $B_\tau$ of definable opens of $\llbracket \tau \rrbracket_S$ (contexts $E : \tau \vdash S$)
Opens are More Important than Elements

Find a basis of definable elements of $[\tau]_S$ (terms $M : \tau$)

Then if $[M]_S \not\subseteq [N]_S$,
for some $U \in \mathcal{B}_\tau$, $[M]_S \in U$ and $[N]_S \not\in U$,
i.e., for some $E$, $[E[M]]_S = \top$ and $[E[N]]_S = \bot$.

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 $\tau S$ is given by $\uparrow^\nu$

Would require us to find term defining $\ll$ (seems hard)
The canonical (sub)base in the continuous dcpo $\llbracket \tau \rrbracket_S$ is given by $\uparrow \nu$

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

<table>
<thead>
<tr>
<th>Basis of elements</th>
<th>Subbase of opens</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Nat</strong></td>
<td>$n, \bot$</td>
</tr>
<tr>
<td><strong>$S$</strong></td>
<td>$\top, \bot$</td>
</tr>
<tr>
<td><strong>$T \tau$</strong></td>
<td>Definable from $\delta_a = \lambda h \cdot h(a), 0$ $\sup$ (if $A \in S$) $\inf$ (if $D \in S$) $\frac{1}{2} (- + -)$ (if $P \in S$)</td>
</tr>
<tr>
<td><strong>$\sigma \rightarrow \tau$</strong></td>
<td>Step functions $\sup_{i=1}^{m} (\bigcap_{j=1}^{ni} U_{ij}) \downarrow y_i$ $U_{ij}$ in $\mathcal{B}_\sigma$</td>
</tr>
</tbody>
</table>
Subbases

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

Theorem

*The Scott and weak topologies *coincide* on \([T\tau]_S\).*

Theorem

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

In general, Scott is finer. But here \([\tau]_S\) 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 $A = \{ a_1, \ldots, a_n \}$. 

\[ \square \]
Scott = Weak

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

**Theorem**

*The Scott and weak topologies coincide on $[T\tau]_S$.***

**Proof:**

- $S = \{A\}$ weak=lower Vietoris (subbasic $\Diamond U$) = Scott (since every closed subset is directed union of $\downarrow E$, $E$ finite)
- $S = \{D\}$ weak=upper Vietoris (subbasic $\Box U$) = Scott (since every $Q$ is $\bigcap_{E} \uparrow E$)
- $S = \{P\}$ proved by [Kirch93], see also [Tix95,Jung04]
- $S = \{A,P\}$ by [JGL08], Hoare previsions = retract (closed convex hull) of Hoare powerdomain on valuations, then apply previous results ($S = \{A\}, S = \{P\}$)
- $S = \{D,P\}$ by [JGL08], similarly.
### Definability

<table>
<thead>
<tr>
<th>Basis of elements</th>
<th>Subbase of opens</th>
</tr>
</thead>
<tbody>
<tr>
<td>( \mathbb{T} )</td>
<td>( h &gt; r ) = ( { F \mid F(h) &gt; r } )</td>
</tr>
<tr>
<td>( \delta_a )</td>
<td>( \text{val } a )</td>
</tr>
<tr>
<td>0</td>
<td>( Y(\lambda F_{\mathbb{T}} \cdot F) )</td>
</tr>
<tr>
<td>( \sup )</td>
<td>( \bigvee ) (( A \in S ))</td>
</tr>
<tr>
<td>( \inf )</td>
<td>( \bigvee ) (( D \in S ))</td>
</tr>
<tr>
<td>( \frac{1}{2} (_ + _) )</td>
<td>( \bigoplus ) (( P \in S ))</td>
</tr>
</tbody>
</table>

**Step functions**

\[
\left( \sup_{i=1}^{m} \left( \bigcap_{j=1}^{n_i} U_{ij} \right) \right) \downarrow y_i
\]

\[
\bigcap_{j=1}^{n_i} U_{ij} \quad \bigwedge_{j=1}^{n_i} \chi U_{ij}
\]

\[
\sup_{i=1}^{m}
\]

... \( \text{a nuisance} \)

---

**Needs statistical tester**

\[
[a \in V] \ldots E[-N]
\]

where \( E \) defines \( V \), and \( N \) defines \( a \)
We must show definability of two kinds of things:

- **statistical testers** \([h > r]\)
- finite sups of step functions in \(\sigma \rightarrow \tau\)

Both of them **fail**.

Already in PCF, \(\text{por}\) is missing:

- In 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 \(h = ♦\)
just at type \(S\): termination testers

**Theorem**

\[
PCF(S) + \text{por} \text{ is not fully abstract} \quad (\text{for any } S)
\]

**Proof.** Key Lemma: every definable function : \(Tγ \rightarrow γ\) is constant.
(Proof: logical relation \(R_γ = \text{equality of values, } R_{TT} \text{ always true.})

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

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

But \([M]_S \not\preceq [N]_S\) since

\[
[M]_S ([♦ > 1/2]) = ⊤ \quad [N]_S ([♦ > 1/2]) = ⊥
\]
Termination Testers

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

\[
\frac{M \downarrow^m b \quad E \cdot \bot \downarrow^m a \quad (Pr)}{E \cdot \Pr(M > b) \downarrow^m a}
\]

\[
[\Pr(M > b)]_s = \begin{cases} 
\top & \text{if } [M]_s (\Diamond) > b \\
\bot & \text{otherwise}
\end{cases}
\]

Computational adequacy: still OK.

Fully abstract now? I don’t know (I don’t think so.)
(Even redefining $\sim^m$ using extended contexts $E := \ldots | \Pr(\_ > b)$)
Let us restrict to semantic domains with a top (continuous lattices)

- Involves switching to call-by-value
  ... so all domains are of the form $[T\tau]$

- Make sure all domains of the form $[T\tau]$ 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
Syntax changes: no let/val, constants turned into operators, \( Y/\lambda \) merged as \( \text{rec } f \cdot \lambda x \cdot M \), ignore /; omitted (definable)

\[
M ::= x \mid \top \mid n \\
| \text{rec } f \cdot \lambda x \cdot M \\
| MN \\
| \text{pred } M \mid \text{succ } M \\
| \text{ifz } M \; N \; P \\
| M \otimes N \quad (\text{if } A \in S \text{ or } D \in S) \\
| M \oplus N \quad (\text{if } P \in S)
\]
**Call-by-Value PCF(S): Denotational Semantics**

Types $\tau ::= \gamma \mid \sigma \Rightarrow \tau$ \hspace{1cm} (no $T$ type; but $\sigma \Rightarrow \tau \defeq \sigma \to T\tau$)

<table>
<thead>
<tr>
<th>Semantics</th>
<th>if $M : \tau$ then $\llbracket M \rrbracket^*_S \in \llbracket T\tau \rrbracket_S$</th>
</tr>
</thead>
<tbody>
<tr>
<td>$\llbracket x \rrbracket^*_S = \text{val } x$</td>
<td></td>
</tr>
<tr>
<td>$\llbracket \top \rrbracket^*_S = \text{val } \top$</td>
<td></td>
</tr>
<tr>
<td>$\llbracket n \rrbracket^*_S = \text{val } n$</td>
<td></td>
</tr>
<tr>
<td>$\llbracket \text{rec } f \cdot \lambda x \cdot M \rrbracket^*_S$</td>
<td>$\text{val } (\text{lfp}(f, x \mapsto \llbracket M \rrbracket^*_S))$</td>
</tr>
<tr>
<td>$\llbracket MN \rrbracket^*_S$</td>
<td>$\text{let } f \leftarrow \llbracket M \rrbracket^<em>_S \text{ in let } v \leftarrow \llbracket N \rrbracket^</em>_S \text{ in } f(v)$</td>
</tr>
<tr>
<td>$\llbracket \text{pred } M \rrbracket^*_S$</td>
<td>$\text{let } h \mapsto \llbracket M \rrbracket^*_S (n \neq 0 \mapsto h(n-1) \mid 0 \mapsto 0)$</td>
</tr>
<tr>
<td>$\llbracket \text{succ } M \rrbracket^*_S$</td>
<td>$\text{let } n \leftarrow \llbracket M \rrbracket^*_S \text{ in } n+1$</td>
</tr>
<tr>
<td>$\llbracket \text{ifz } M N P \rrbracket^*_S$</td>
<td>$\text{let } n \leftarrow \llbracket M \rrbracket^<em>_S \text{ in } (\llbracket N \rrbracket^</em>_S \text{ if } n = 0, \llbracket P \rrbracket^*_S \text{ else})$</td>
</tr>
<tr>
<td>$\llbracket M \otimes N \rrbracket^*_S$</td>
<td>$\llbracket M \rrbracket^<em>_S(\llbracket M \rrbracket^</em>_S)(\llbracket N \rrbracket^*_S)$</td>
</tr>
<tr>
<td>$\llbracket M + N \rrbracket^*_S$</td>
<td>$\llbracket M \rrbracket^<em>_S(\llbracket M \rrbracket^</em>_S)(\llbracket N \rrbracket^*_S)$</td>
</tr>
</tbody>
</table>

where $\text{val } a = (h \mapsto h(a))$

$\text{let } v \leftarrow F \text{ in } G(v) = (h \mapsto F(v \mapsto G(v)(h)))$

... we now need subnormalized previsions $(F(a + h) \leq \frac{1}{2}(a + F(h)))$

+ no $\bot$ in base types: $\llbracket \text{Nat} \rrbracket_S = \mathbb{N}$, $\llbracket S \rrbracket_S = \{\top\}$
New notion: values $V = \text{rec } f \cdot \lambda x \cdot M \mid \top \mid n$

...if $f$ not free in $M$, $\text{rec } f \cdot \lambda x \cdot M$ written $\lambda x \cdot M$

Semantically, $\llbracket V \rrbracket^*_S = \text{val}(\llbracket V \rrbracket^*_S)$ where

$\llbracket \text{rec } f \cdot \lambda x \cdot M \rrbracket^*_S = \text{lfp}(f, x \mapsto \llbracket M \rrbracket^*_S)$, $\llbracket \top \rrbracket^*_S = \top$, $\llbracket n \rrbracket^*_S = n$

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

$$
E : \sigma \vdash S := \\
\begin{align*}
E & : \sigma \vdash S \\
\text{or} & \quad E[\_N] \\
\text{or} & \quad E[(\text{rec } f \cdot \lambda x \cdot M)_\_] \quad \text{(new)} \\
\text{or} & \quad E[\text{succ } \_] | E[\text{pred } \_] \\
\text{or} & \quad E[\text{ifz } N P]
\end{align*}
$$
The CBV PCF(S) Machine

1. Redex Discovery Rules

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

2. Computation

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

3. Choice states are now
\[ E \cdot M \Join N, \ E \cdot M \Join N \]

4. Termination state:
\[ \_ \cdot \top \]
Essentially the same as before:

\[
\begin{align*}
C' \downarrow^m a & \quad (C \to C') \\
C \downarrow^m a & \quad (a \in \mathbb{Q} \cap [0, 1)) \\
E \cdot M \downarrow^{\text{may}} a & \quad E \cdot N \downarrow^{\text{may}} a \\
E \cdot M \oplus N \downarrow^{\text{may}} a & \quad E \cdot M \oplus N \downarrow^{\text{may}} a \\
E \cdot M \downarrow^m a & \quad E \cdot N \downarrow^m b \\
E \cdot M \oplus N \downarrow^m \frac{1}{2} (a + b) & \quad (a \in \mathbb{Q} \cap [0, 1)) \\
E \cdot M \oplus N \downarrow^{\text{must}} a & \quad E \cdot M \oplus N \downarrow^{\text{must}} a
\end{align*}
\]
Full Abstraction for PCF with Choice

Call-by-Value

Semantics

Soundness

Theorem (Soundness)

1. \([E[M]]_S^* (\diamond) \geq \text{Pr}(E \cdot M \downarrow \text{may})\) (if \(S \subseteq \{A, P\}\))
2. \([E[M]]_S^* (\diamond) \geq \text{Pr}(E \cdot M \downarrow \text{must})\) (if \(S \subseteq \{D, P\}\))

Proof: induction, using \([E[M]]_S^* (\diamond) = [M]^*_S (h)\) for some \(h\) depending on \(E\) only.
Theorem (Computational Adequacy)

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

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

- $M R_\sigma^* F$ 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 $V R_\sigma^\circ v$, $Pr(E \cdot V \downarrow^m) \geq h(v)$
- $V_f R_\sigma^\circ \Rightarrow_\tau \varphi$ iff for all $V R_\sigma^\circ v$, $E R_\tau^\perp h$, $Pr(E[V_f] \cdot V \downarrow^m) \geq \varphi(v)(h)$
- $m R_\text{Nat}^\circ n$ iff $m = n$ and $\top R_S^\circ \top$

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

Finally take $E = \_$, $h = \diamondsuit$ at $\tau = S$. \qed
Statistical Termination Testers

Do we still need termination testers?

**Theorem (Yes, in Probabilistic Cases ($P \in S$))**

CBV PCF(S) without termination testers is not fully abstract

**Proof.** Define logical relation $R^*_T$, $R^\perp_T$, $R^\circ_T$:

- $\top R^\circ_T \top$ $n_1 R^\circ_{\text{Nat}} n_2$ iff $n_1 = n_2$
- $f_1 R^\circ_{\sigma \Rightarrow \tau} f_2$ iff for all $v_1 R^\circ_\sigma v_2$, $f_1(v_1) R^*_T f_2(v_2)$
- $F_1 R^*_T F_2$ iff for all $h_1 R^\perp_T h_2$, $F_1(h_1) \sim_0 F_2(h_2)$
- $h_1 R^\perp_T h_2$ iff for all $v_1 R^\circ_\tau v_2$, $h_1(v_1) \sim_0 h_2(v_2)$
- $a_1 \sim_0 a_2$ iff $a_1 = a_2 = 0$ or ($a_1 \neq 0$ and $a_2 \neq 0$)

Then $[\text{\textcolor{red}{\textbullet}} > r] = (h \mapsto \begin{cases} \text{val } \top & \text{if } h(\top)(\text{\textcolor{red}{\textbullet}}) > r \\ 0 & \text{else} \end{cases})$ is not in relation with itself, hence not definable (of type $(S \Rightarrow S) \Rightarrow S \sim TS \Rightarrow TS)$
Statistical Termination Testers

Do we still need termination testers?

**Theorem (Yes, in Probabilistic Cases \((P \in S)\))**

**CBV PCF(S) without termination testers is not fully abstract**

**Proof.** Define logical relation \(R^*, R^\perp, R^\circ\):

\[
\begin{align*}
\top &\ R^\circ_S \top &\ n_1 \ R^\circ_{\text{Nat}} \ n_2 \ \text{iff} \ n_1 = n_2 \\
 f_1 \ R^\circ_{\sigma \Rightarrow \tau} \ f_2 &\ \text{iff} \ \text{for all} \ v_1 \ R^\circ_{\sigma} \ v_2, \ f_1(v_1) \ R^* \ f_2(v_2) \\
 F_1 \ R^* \ F_2 &\ \text{iff} \ \text{for all} \ h_1 \ R^\perp_{\tau} \ h_2, \ F_1(h_1) \sim_0 F_2(h_2) \\
h_1 \ R^\perp_{\tau} \ h_2 &\ \text{iff} \ \text{for all} \ v_1 \ R^\circ_{\tau} \ v_2, \ h_1(v_1) \sim_0 h_2(v_2) \\
a_1 \sim_0 a_2 &\ \text{iff} \ a_1 = a_2 = 0 \ \text{or} \ (a_1 \neq 0 \ \text{and} \ a_2 \neq 0)
\end{align*}
\]

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

**Fact (No, in Non-Probabilistic Cases \((P \notin S)\))**

Can define \(\Pr(M > r)\) as \(M\) if \(r \in [0, 1)\)
Add termination testers $\Pr(M > b)$ to the language $(M : S)$.

\[
\frac{\_ \cdot M \Downarrow^m b \quad E \cdot \top \Downarrow^m a}{E \cdot \Pr(M > b) \Downarrow^m a} \qquad (Pr)
\]

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

Computational adequacy: still OK.
The Angelic+Probabilistic Case

Let $M \sim^m N$ iff $\Pr(\_ \cdot E'[M] \downarrow^m) \leq \Pr(\_ \cdot E'[N] \downarrow^m)$ for every extended context $E'$.

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

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

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

**Proof.**

- Open subbase $[a \mapsto h > r] = \{f \in \llbracket \sigma \Rightarrow \tau \rrbracket_S \mid f(a)(h) > r\}$
  definable by $E[\Pr(\_ > r)][V_{h-}][V_a]

- Basis of values definable from $\ominus, \oplus, \text{val}, \Omega (0)$
  The “nuisance” $\sup_{i=1}^m$ is definable through $\bigvee (= \sup)$.  

**Note:** no need for $\text{por}$.  

The Purely Angelic Case

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

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

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

\[
M \sim^{\text{may}} N \iff M \sim^{\text{may}} N \iff [M]_A \leq [N]_A
\]

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

**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 $\preceq$ Hoare powerdomain (with $\emptyset$)

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

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

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

- Call-by-value PCF(\{A\}) is **fully abstract**
- Call-by-value 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: \([\tau]_S\) not a bc-domain

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

- **Purely probabilistic** case hopeless (valuations/lin. previsions) \([\tau]_S\) 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 \((D \in S)\), \([T\tau]_S\) has no top

**Cure:** add one.

Let \(X^{err}\) be \(X\) with a fresh top element \(err\) (abnormal termination)

(not really the space we shall work with)

Previsions on \(X^{err}\) are the same as lax previsions on \(X\):

**Definition (Lax Prevision)**

Let \(lax\) map previsions \(F\) on \(X^{err}\) to \((h \in [X \rightarrow I] \mapsto F(\hat{h}))\),

where \(\hat{h}(x) = h(x)\ (x \in X)\) and \(\hat{h}(err) = 1\).

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 \((= lax(\delta_{err}))\)
- Lax prev. closed under \(\frac{\_ + \_}{2}\) \((P \in S)\), \(\text{min} (D \in S)\), \(\text{max} (A \in S)\)
CBV PCF(S) + irq

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

New operational rules

\[
\begin{align*}
E \cdot M \downarrow^m a & \quad \vdash E \cdot M \text{ irq } N \downarrow^m a \\
\vdash E \cdot M \text{ irq } N \downarrow^m a & \quad \vdash _\cdot N \downarrow^m a \\
\vdash E \cdot M \text{ irq } N \downarrow^m a & \quad \vdash E \cdot M \text{ irq } N \downarrow^m a
\end{align*}
\]

Run \( M \) with \( N \) in background: if \( N \) terminates, kill \( M \) and abort

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

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

Soundness, computational adequacy: still OK.
The Demonic+Probabilistic Case

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

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

\[ M \sim_{\text{must}} N \iff \llbracket M \rrbracket_{D, P} \leq \llbracket N \rrbracket_{D, P} \]

**Proof.**

- Open subbase $[a \mapsto h > r] = \{ f \in \llbracket \sigma \Rightarrow \tau \rrbracket_S | f(a)(h) > r \}$
  defensible by $E[\Pr(\cdot > r)\llbracket V_h \rrbracket\llbracket_- V_a \rrbracket]$
  Note that Scott=weak again on lax previsions

- Basis of values defensible from $\lor$, $\oplus$, $\text{val}$, $\Omega$, and abort.
  “Nuisance” $\sup_{i=1}^{m}$: use “sup-as-inf” trick:

\[
\sup_{i=1}^{m} (U_i \downarrow F_i)(x) = \min_{I \subseteq \{1, \ldots, m\}} F_I \text{ irq } \chi_{\bigcup_{i \in I} u_i(x)}
\]

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

\[ F \text{ irq } \top = (h \mapsto 1), \ F \text{ irq } \bot = F \ldots \text{definable through irq} \]

and $\min$ definable through $\lor$. 
The Purely Demonic Case

Again, termination testers are definable when \( P \notin S \)

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

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

\[
M \prec_{\text{must}} N \iff M \prec_{\text{must}} N \iff [M]_{\{D\}} \leq [N]_{\{D\}}
\]
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 $PCF(\{A\}) + irq$:

$$M \preceq_{\text{may}} N \iff M \preceq_{\text{may}} N \iff [M]_{\{A\}} \leq [N]_{\{A\}}$$

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

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

$$M \preceq_{\text{may}} N \iff [M]_{\{A, P\}} \leq [N]_{\{A, P\}}$$
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:

\[
F^-(\frac{h + h'}{2}) \leq \frac{F^-(h) + F^+(h')}{2} \leq F^+(\frac{h + h'}{2})
\]

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**

\[
[M]_S^* = ([M]_S^-)^*, ([M]_S^+)^*
\]

...merely ignoring Walley’s condition

Now, if \( [M]_S^* \not\cong [N]_S^* \), either:

- \( [M]_S^-^* \not\cong [N]_S^-^* \): since demonic cases are fully abstract, there is an \( E \) such that \( \Pr(\_ \cdot E[M]_\downarrow^{\text{must}}) \not\cong \Prob(\_ \cdot E[M]_\downarrow^{\text{must}}) \)

- or \( [M]_S^+^* \not\cong [N]_S^+^* \): since angelic cases are fully abstract, there is an \( E \) such that \( \Pr(\_ \cdot E[M]_\downarrow^{\text{may}}) \not\cong \Prob(\_ \cdot E[M]_\downarrow^{\text{may}}) \)
Full Abstraction in the Erratic Cases

For \( \{A, D\} \subseteq S \), let \( M \preceq N \) iff \( M \preceq_{\text{may}} N \) and \( M \preceq_{\text{must}} N \)
(i.e., with extended contexts, including \( E[\Pr(\_ > b)] \))
(and similarly for \( \preceq \), with ordinary contexts)

We therefore obtain:

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

*Full abstraction holds for PCF(\( \{A, D\} \)) + irq:*
\[
M \preceq N \text{ iff } M \preceq_{\text{may}} N \text{ iff } [M]_{\{A,D\}} \leq [N]_{\{A,D\}}
\]

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

*Full abstraction holds for PCF(\( \{A, D, P\} \)) + irq + statistical testers:*
\[
M \preceq N \text{ iff } [M]_{\{A,D,P\}} \leq [N]_{\{A,D,P\}}
\]