Full Abstraction for Non-Deterministic and Probabilistic Extensions of PCF

Jean Goubault-Larrecq

ANR Blanc CPP

Domains X - September 2011

Outline

Outline

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

Types

$$\begin{array}{rcll} \gamma & ::= & \mathtt{Nat} \mid \mathtt{S} & \text{Ground types} \\ \sigma, \tau & ::= & \gamma \mid \sigma \to \tau \mid \mathtt{T}\tau & \text{Types} \end{array}$$

Notes:

- $\mathtt{S}$ has only one (non-bottom) value
  $=$ `unit` type, termination type

  Not required in principle, but practical
- $\mathtt{T}\tau$ type of processes computing value of type τ

  à la [Moggi91]

PCF(S) Terms

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

- PCF terms
  (λ-calculus + basic arithmetic + $\mathtt{ifz}$ + fixpoint Y)
- At $\mathtt{S}$ type:
  - $\underline{\top} : \mathtt{S}$
  - for every $M : \mathtt{Nat}$, $\quad \mathtt{ignore}\, M : \mathtt{S}$
  - for all $M : \mathtt{S}$, $N : \sigma$, sequencing $M; N : \sigma$
- At $\mathtt{T}\tau$ types:
  - for each $M : \tau$, $\quad \mathtt{val}\, M : \mathtt{T}\tau$
  - for all $M : \sigma$, $N : \mathtt{T}\tau$, $\quad \mathtt{let}\, x \Leftarrow M\, \mathtt{in}\, N : \mathtt{T}\tau$
  - Non-det. choice $\bigtriangledown : \mathtt{T}\tau \to \mathtt{T}\tau \to \mathtt{T}\tau$ $\quad$ (if $\mathtt{A} \in S$ or $\mathtt{D} \in S$)
  - Prob. choice $\bigoplus : \mathtt{T}\tau \to \mathtt{T}\tau \to \mathtt{T}\tau$ $\quad$ (if $\mathtt{P} \in S$)

Operational Semantics

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

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

$$
\begin{array}{rcl}
E & := & \_ \\
& | & E[\_N] \\
& | & E[\mathtt{succ}\ \_] \mid E[\mathtt{pred}\ \_] \\
& | & E[\mathtt{ifz}\ \_\ N\ P] \mid E[\_; N] \\
& | & E[\mathtt{ignore}\ \_] \\
& | & \mathtt{val}\ \_ \\
& | & E[\mathtt{let}\ x \Leftarrow \_\ \mathtt{in}\ N]
\end{array}
$$

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

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

$$E \cdot MN \to E[\_N] \cdot M$$
$$E[\_N] \cdot \mathtt{pred} \to E[\mathtt{pred}\ \_] \cdot N$$
$$E[\_N] \cdot \mathtt{succ} \to E[\mathtt{succ}\ \_] \cdot N$$
$$E[\_MNP] \cdot \mathtt{ifz} \to E[\mathtt{ifz}\ \_\ N\ P] \cdot M$$
$$E \cdot M; N \to E[\_; N] \cdot M$$
$$E[\_N] \cdot \mathtt{ignore} \to E[\mathtt{ignore}\ \_] \cdot N$$
$$\_ \cdot \mathtt{val}\ M \to \mathtt{val}\ \_ \cdot M$$
$$E \cdot \mathtt{let}\ x \Leftarrow M\ \mathtt{in}\ N \to E[\mathtt{let}\ x \Leftarrow \_\ \mathtt{in}\ N] \cdot M$$

The PCF(S) Machine: 2. Computation

Redex = interaction between top of M and bottom of E

$$E[\_N] \cdot \lambda x \cdot P \to E \cdot P[x := N]$$
$$E[\mathtt{pred}\ \_] \cdot \underline{n+1} \to E \cdot \underline{n}$$
$$E[\mathtt{succ}\ \_] \cdot \underline{n} \to E \cdot \underline{n+1}$$
$$E[\mathtt{ifz}\ \_\ N\ P] \cdot \underline{0} \to E \cdot N$$
$$E[\mathtt{ifz}\ \_\ N\ P] \cdot \underline{n+1} \to E \cdot P$$
$$E[\_; N] \cdot \underline{\top} \to E \cdot N$$
$$E[\mathtt{ignore}\ \_] \cdot \underline{n} \to E \cdot \underline{\top}$$
$$E[\_N] \cdot Y \to E \cdot N(YN)$$
$$E[\mathtt{let}\ x \Leftarrow \_\ \mathtt{in}\ P] \cdot \mathtt{val}\ N \to E \cdot P[x := N]$$

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

The PCF(S) Machine: 3. Choice

The choice states are:

- (non-deterministic) $E \cdot \bigtriangledown$ (if $\mathtt{A} \in S$ or $\mathtt{D} \in S$)
- (probabilistic) $E \cdot \bigoplus$ (if $\mathtt{P} \in S$)

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

$$E[\_MN] \cdot \bigtriangledown \to M \qquad E[\_MN] \cdot \bigtriangledown \to N$$

$$E[\_MN] \cdot \bigoplus \to M \qquad E[\_MN] \cdot \bigoplus \to N$$

Reachability Objectives

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

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

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

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

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

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

$\{\mathtt{A}, \mathtt{D}\} \subseteq S$ 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 $C \to C'$:

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

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

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

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

Termination Semantics (2/2)

Choice:

$$\frac{E \cdot M \downarrow^{\text{may}} a}{E[\_MN] \cdot \mathbin{\textcircled{\scriptsize\vee}} \downarrow^{\text{may}} a} \qquad \frac{E \cdot N \downarrow^{\text{may}} a}{E[\_MN] \cdot \mathbin{\textcircled{\scriptsize\vee}} \downarrow^{\text{may}} a} \qquad \frac{E \cdot M \downarrow^{\text{must}} a \quad E \cdot N \downarrow^{\text{must}} a}{E[\_MN] \cdot \mathbin{\textcircled{\scriptsize\vee}} \downarrow^{\text{must}} a}$$

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

Definition

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

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

Denotational Semantics: Previsions

Let $[\![\mathrm{T}\tau]\!]_S$ 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 $a \in I$
- $F(\frac{a+h}{2}) = \frac{1}{2}(a + F(h))$ (total mass $= 1$)
- $F(\frac{h+h'}{2}) \leq \frac{1}{2}(F(h) + F(h'))$ (if $S \subseteq \{\mathtt{A}, \mathtt{P}\}$)
- $F(\frac{h+h'}{2}) \geq \frac{1}{2}(F(h) + F(h'))$ (if $S \subseteq \{\mathtt{D}, \mathtt{P}\}$)
- $F(h) \in \{0,1\}$ for every $h : X \to \{0,1\}$ (if $\mathtt{P} \notin S$)

(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

$$[\![x]\!]_S = x \quad [\![\underline{\top}]\!]_S = \top \quad [\![\underline{n}]\!]_S = n \in \mathbb{N}$$
$$[\![\lambda x \cdot M]\!]_S = (x \mapsto [\![M]\!]_S) \qquad [\![MN]\!]_S(\rho) = [\![M]\!]_S([\![N]\!]_S)$$

$$\begin{aligned}
[\![Y]\!]_S &= (f \mapsto \bigcup_{n\in\mathbb{N}} f^n(\bot)) \\
[\![\mathtt{pred}]\!]_S &= (v \in \mathbb{N} \setminus \{0\} \mapsto v-1 \mid 0, \bot \mapsto \bot) \\
[\![\mathtt{succ}]\!]_S &= (v \in \mathbb{N} \mapsto v+1 \mid \bot \mapsto \bot) \\
[\![\mathtt{ifz}]\!]_S &= (0, t, e \mapsto t \mid n \in \mathbb{N} \setminus \{0\}, t, e \mapsto e \mid \bot \mapsto \bot) \\
[\![M; N]\!]_S &= [\![N]\!]_S \text{ if } [\![M]\!]_S \neq \bot, \text{ else } \bot \\
[\![\mathtt{ignore}]\!]_S &= (n \in \mathbb{N} \mapsto \top \mid \bot \to \bot) \\
[\![\mathtt{val}\, M : \mathtt{T}\sigma]\!]_S &= (h \mapsto h([\![M]\!]_S)) \\
[\![\mathtt{let}\, x \Leftarrow M \,\mathtt{in}\, N]\!]_S &= (h \mapsto [\![M]\!]_S(x \mapsto [\![N]\!]_S(h)) \\
[\![\mathbin{\mathbb{V}}]\!]_S &= (F_1, F_2, h \mapsto \max(F_1(h), F_2(h)) && (\text{if } \mathtt{A} \in S) \\
[\![\mathbin{\mathbb{V}}]\!]_S &= (F_1, F_2, h \mapsto \min(F_1(h), F_2(h)) && (\text{if } \mathtt{D} \in S) \\
[\![\oplus]\!]_S &= (F_1, F_2, h \mapsto \tfrac{1}{2}(F_1(h) + F_2(h)) && (\text{if } \mathtt{P} \in S)
\end{aligned}$$

Soundness

In usual PCF, soundness states that if $M \to^* V$ then $[\![M]\!] = [\![V]\!]$.

Theorem (Soundness)

Let $\blacklozenge = \chi_{\{\top\}} : [\![\mathbb{S}]\!] \to I$ *map* $\bot$ *to* 0, $\top$ *to* 1.

- *If* $E \cdot M \downarrow^{\text{may}} a$ *then* $[\![E[M]]\!]_S(\blacklozenge) > a$ *(if* $S \subseteq \{\mathtt{A}, \mathtt{P}\}$*)*
- *If* $E \cdot M \downarrow^{\text{must}} a$ *then* $[\![E[M]]\!]_S(\blacklozenge) > a$ *(if* $S \subseteq \{\mathtt{D}, \mathtt{P}\}$*)*

Proof: induction. □

Soundness

In usual PCF, soundness states that if $M \to^* V$ then $[\![M]\!] = [\![V]\!]$.

Theorem (Soundness)

Let $\blacklozenge = \chi_{\{\top\}} : [\![\mathbb{S}]\!] \to I$ *map* $\bot$ *to* 0, $\top$ *to* 1.

- *If* $E \cdot M \downarrow^{\text{may}} a$ *then* $[\![E[M]]\!]_S(\blacklozenge) > a$ *(if* $S \subseteq \{\mathtt{A}, \mathtt{P}\}$*)*
- *If* $E \cdot M \downarrow^{\text{must}} a$ *then* $[\![E[M]]\!]_S(\blacklozenge) > a$ *(if* $S \subseteq \{\mathtt{D}, \mathtt{P}\}$*)*

Proof: induction. □

Corollary

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

Computational Adequacy

In usual PCF, $M \to^* V$ iff $[\![M]\!] = [\![V]\!]$, at ground types.
Here, use $E = \_$ (empty context, of type $\mathtt{TS} \vdash \mathtt{TS}$)

Theorem (Computational Adequacy)

- $[\![M]\!]_S(\blacklozenge) = Pr(\_ \cdot M{\downarrow}^{\mathsf{may}})$ *(if $S \subseteq \{\mathtt{A}, \mathtt{P}\}$)*
- $[\![M]\!]_S(\blacklozenge) = Pr(\_ \cdot M{\downarrow}^{\mathsf{must}})$ *(if $S \subseteq \{\mathtt{D}, \mathtt{P}\}$)*

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

- $M[x := N] \precsim^m (\lambda x \cdot M)N$ $\quad M(YM) \precsim^m YM$
- $\underline{n} \precsim^m M \Rightarrow \underline{n+1} \precsim^m \mathtt{succ}\, M$ $\quad \underline{n+1} \precsim^m M \Rightarrow \underline{n} \precsim^m \mathtt{pred}\, M$
- $\underline{0} \precsim^m M \Rightarrow N \precsim^m \mathtt{ifz}\, M\, N\, P$ $\quad \underline{n+1} \precsim^m M \Rightarrow P \precsim^m \mathtt{ifz}\, M\, N\, P$
- $\underline{\top} \precsim^m M \Rightarrow N \precsim^m M; N$ $\quad \underline{n} \precsim^m M \Rightarrow \underline{\top} \precsim^m \mathtt{ignore}\, M$

Computational Adequacy

In usual PCF, $M \to^* V$ iff $[\![M]\!] = [\![V]\!]$, at ground types.
Here, use $E = \_$ (empty context, of type $\mathtt{TS} \vdash \mathtt{TS}$)

Theorem (Computational Adequacy)

- $[\![M]\!]_S(\blacklozenge) = Pr(\_ \cdot M{\downarrow}^{\mathsf{may}})$ *(if $S \subseteq \{\mathtt{A}, \mathtt{P}\}$)*
- $[\![M]\!]_S(\blacklozenge) = Pr(\_ \cdot M{\downarrow}^{\mathsf{must}})$ *(if $S \subseteq \{\mathtt{D}, \mathtt{P}\}$)*

Proof: Let $M \precsim^m N$ iff $\Pr(E \cdot M{\downarrow}^m) \leq \Pr(E \cdot N{\downarrow}^m)$ for every E.
Define a logical relation R_σ:

$$
\begin{array}{rll}
M\, R_{\mathtt{S}}\, u & \text{iff} & u = \bot, \text{ or } u = \top \text{ and } \underline{\top} \precsim^m M \\
M\, R_{\mathtt{Nat}}\, n & \text{iff} & n = \bot, \text{ or } n \in \mathbb{N} \text{ and } \underline{n} \precsim^m M \\
M\, R_{\sigma\to\tau}\, f & \text{iff} & \text{for all } N\, R_\sigma\, v,\ MN\, R_\tau\, f(v) \\
M\, R_{\mathtt{T}\sigma}\, F & \text{iff} & \text{for all } E\, R_\sigma^\perp\, h,\ \Pr(E \cdot M{\downarrow}^m) \geq F(h) \\
E\, R_\sigma^\perp\, h & \text{iff} & \text{for all } Q\, R_\sigma\, v,\ \Pr(E \cdot \mathtt{val}\, Q{\downarrow}^m) \geq h(v)
\end{array}
$$

Computational Adequacy

In usual PCF, $M \to^* V$ iff $[\![M]\!] = [\![V]\!]$, at ground types.
Here, use $E = \_$ (empty context, of type $\mathtt{TS} \vdash \mathtt{TS}$)

Theorem (Computational Adequacy)

- $[\![M]\!]_S(\blacklozenge) = Pr(\_ \cdot M{\downarrow}^{\text{may}})$ *(if $S \subseteq \{\mathtt{A}, \mathtt{P}\}$)*
- $[\![M]\!]_S(\blacklozenge) = Pr(\_ \cdot M{\downarrow}^{\text{must}})$ *(if $S \subseteq \{\mathtt{D}, \mathtt{P}\}$)*

Proof: Let $M \precsim^m N$ iff $\Pr(E \cdot M{\downarrow}^m) \leq \Pr(E \cdot N{\downarrow}^m)$ for every E.
Define a logical relation R_σ:

$M\, R_{\mathtt{T}\sigma}\, F$ 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 $Q\, R_\sigma\, v$, $\Pr(E \cdot \mathtt{val}\, Q{\downarrow}^m) \geq h(v)$

By definition, $\_\, R_{\mathtt{S}}^\perp\, \blacklozenge$
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 $E = \_$, $h = \blacklozenge$.

Outline

Full Abstraction

Definition (Full Abstraction)

$M \precsim^m N$ iff $[\![M]\!]_S \leq [\![N]\!]_S$, at all types.

- Easy direction: If $[\![M]\!]_S \leq [\![N]\!]_S$ at type τ, then
  $[\![E[M]]\!]_S \leq [\![E[N]]\!]_S$ for every context $E : \tau \vdash \mathtt{TS}$
  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 $M \precsim^m N$.

Full Abstraction

Definition (Full Abstraction)

$M \precsim^m N$ iff $[\![M]\!]_S \leq [\![N]\!]_S$, at all types.

- Easy direction: If $[\![M]\!]_S \leq [\![N]\!]_S$ at type τ, then
  $[\![E[M]]\!]_S \leq [\![E[N]]\!]_S$ for every context $E : \tau \vdash \mathtt{TS}$
  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 $M \precsim^m N$.
- Hard direction: assume $[\![M]\!]_S \not\leq [\![N]\!]_S$, find E such that
  $\Pr(E \cdot M{\downarrow^m}) > \Pr(E \cdot N{\downarrow^m})$

Full Abstraction

Definition (Full Abstraction)

$M \precsim^m N$ iff $[\![M]\!]_S \leq [\![N]\!]_S$, at all types.

- Easy direction: If $[\![M]\!]_S \leq [\![N]\!]_S$ at type τ, then
  $[\![E[M]]\!]_S \leq [\![E[N]]\!]_S$ for every context $E : \tau \vdash \mathtt{TS}$
  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 $M \precsim^m N$.
- Hard direction: assume $[\![M]\!]_S \not\leq [\![N]\!]_S$, 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+$\mathtt{por}$*, the finite elements of* $[\![\tau]\!]$ *are exactly those of the form* $[\![M]\!]$, $M : \tau$.

This is bound to fail here:
if $\mathtt{P} \in S$, 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* $[\![\tau]\!]$ *are exactly those of the form* $[\![M]\!]$, $M : \tau$.

This is bound to fail here:
if $\mathtt{P} \in S$, then $[\![\tau]\!]$ 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 $[\![\tau]\!]_S$ (terms $M : \tau$)

Find a subbase $\mathcal{B}_\tau$ of definable opens of $[\![\tau]\!]_S$ (contexts $E : \tau \vdash \mathtt{S}$)

Opens are More Important than Elements

elements	opens
Find a basis of definable elements of $[\![\tau]\!]_S$ (terms $M : \tau$)	Find a subbase $\mathcal{B}_\tau$ of definable opens of $[\![\tau]\!]_S$ (contexts $E : \tau \vdash \mathbb{S}$)

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

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

Candidates for Subbases

The canonical (sub)base in the continuous dcpo $[\![\tau]\!]_S$ is given by $\Uparrow v$

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

Candidates for Subbases

The canonical (sub)base in the continuous dcpo $[\![\tau]\!]_S$ is given by $\Uparrow v$

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

	Basis of elements	Subbase of opens
Nat	n, $\bot$	$\uparrow n$
S	$\top$, $\bot$	$\uparrow \top$
Tτ	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 $\in S$)	$[h > r] = \{F \mid F(h) > r\}$ (weak/Vietoris topology) where h in basis of $\tau \to l$ $r \in \mathbb{Q} \cap [0, 1)$
$\sigma \to \tau$	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 among $\{\mathtt{A}\}$, $\{\mathtt{A},\mathtt{P}\}$, $\{\mathtt{D}\}$, $\{\mathtt{D},\mathtt{P}\}$)

Theorem

The Scott and weak topologies coincide on $[\![\mathtt{T}\tau]\!]_S$.

Theorem

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

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

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

Scott = Pointwise

Theorem

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

Proof: On $\sigma \to \tau$, 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 $Q = \bigcap^{\downarrow}_{A \text{ finite}} \uparrow A$, $[Q \subseteq V] = \bigcup_{A \text{ finite}} [\uparrow A \subseteq V]$.

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

Scott = Weak

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

Theorem

The Scott and weak topologies coincide on $[\![\mathtt{T}\tau]\!]_S$.

Proof:

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

$S = \{\mathtt{D}\}$ weak=upper Vietoris (subbasic $\Box U$) = Scott (since every Q is $\bigcap_E^{\downarrow} \uparrow E$)

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

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

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

Definability

	Basis of elements			Subbase of opens
$\mathtt{T}\tau$	δ_a	$\mathtt{val}\, a$		$[h > r] = \{F \mid F(h) > r\}$
	0	$Y(\lambda F_{\mathtt{T}\tau} \cdot F)$		
	sup	$\bigtriangledown$	$(\mathtt{A} \in S)$	Needs statistical tester
	inf	$\bigtriangledown$	$(\mathtt{D} \in S)$	
	$\frac{1}{2}(\_ + \_)$	$\oplus$	$(\mathtt{P} \in S)$	
$\sigma \to \tau$	Step functions			$[a \in V] \ldots E[\_N]$
	$\sup_{i=1}^{m}(\bigcap_{j=1}^{n_i} U_{ij}) \searrow y_i$			where E defines V,
	$\bigcap_{j=1}^{n_i} U_{ij}$	$\bigwedge_{j=1}^{n_i} \chi_{U_{ij}}$		and N defines a
	$\wedge$	;		
	$\sup_{i=1}^{m}$	a nuisance		

Return to PCF

We must show definability of two kinds of things:

- statistical testers $[h > r]$
- finite sups of step functions in $\sigma \to \tau$

Both of them fail.

Already in PCF, `por` is missing:

- In PCF+`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 $\mathtt{S}$: termination testers

Theorem

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

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

Let $M = \lambda g \cdot g(\mathtt{val}\,\bot)$, $N = \lambda g \cdot g(\mathtt{val}\,\Omega)$ $(g : \mathtt{TS} \to \mathtt{S})$.

The only definable g are constant, so $M \precsim^m N$ (and $N \precsim^m M$)
But $[\![M]\!]_S \not\leq [\![N]\!]_S$ since

$$[\![M]\!]_S([\blacklozenge > 1/2]) = \top \quad [\![N]\!]_S([\blacklozenge > 1/2]) = \bot$$

Termination Testers

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

$$\frac{\_ \cdot M \downarrow^m b \quad E \cdot \top \downarrow^m a}{E \cdot \mathtt{Pr}(M > b) \downarrow^m a}\,(\mathtt{Pr}) \qquad [\![\mathtt{Pr}(M > b)]\!]_S = \begin{cases} \top & \text{if } [\![M]\!]_S(\blacklozenge) > b \\ \bot & \text{otherwise} \end{cases}$$

Computational adequacy: still OK.

Fully abstract now? I don't know (I don't think so.)
(Even redefining $\precsim^m$ using *extended* contexts $E := \ldots \mid \mathrm{Pr}(\_ > b)$)

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 $[\![\mathtt{T}\tau]\!]$
- Make sure all domains of the form $[\![\mathtt{T}\tau]\!]$ have a top:
  We shall eventually concentrate on the angelic cases

  (S among $\{\mathtt{A}\}$, $\{\mathtt{A}, \mathtt{P}\}$)

Outline

Call-by-Value PCF(S): Syntax

Syntax changes: no `let`/`val`,
constants turned into operators,
Y/λ merged as $\mathtt{rec}\, f \cdot \lambda x \cdot M$,
`ignore` /; omitted (definable)

$$
\begin{array}{rcll}
M & ::= & x \mid \underline{\top} \mid \underline{n} & \\
& \mid & \mathtt{rec}\, f \cdot \lambda x \cdot M & \\
& \mid & MN & \\
& \mid & \mathtt{pred}\, M \mid \mathtt{succ}\, M & \\
& \mid & \mathtt{ifz}\ M\ N\ P & \\
& \mid & M \mathbin{\textcircled{\scriptsize \vee}} N & (\text{if } \mathtt{A} \in S \text{ or } \mathtt{D} \in S) \\
& \mid & M \oplus N & (\text{if } \mathtt{P} \in S)
\end{array}
$$

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

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

Semantics if $M : \tau$ then $[\![M]\!]^*_S \in [\![\mathtt{T}\tau]\!]_S$

$$[\![x]\!]^*_S = \mathit{val}\, x \qquad [\![\top]\!]^*_S = \mathit{val}\, \top \qquad [\![\underline{n}]\!]^*_S = \mathit{val}\, n$$

$$\begin{aligned}
[\![\mathtt{rec}\, f \cdot \lambda x \cdot M]\!]^*_S &= \mathit{val}\,(\mathit{lfp}(f, x \mapsto [\![M]\!]^*_S)) \\
[\![MN]\!]^*_S &= \mathit{let}\, f \Leftarrow [\![M]\!]^*_S\ \mathit{in}\ \mathit{let}\, v \Leftarrow [\![N]\!]^*_S\ \mathit{in}\ f(v) \\
[\![\mathtt{pred}\, M]\!]^*_S &= (h \mapsto [\![M]\!]^*_S\,(n \neq 0 \mapsto h(n-1) \mid 0 \mapsto 0)) \\
[\![\mathtt{succ}\, M]\!]^*_S &= \mathit{let}\, n \Leftarrow [\![M]\!]^*_S\ \mathit{in}\ n+1 \\
[\![\mathtt{ifz}\ M\ N\ P]\!]^*_S &= \mathit{let}\, n \Leftarrow [\![M]\!]^*_S\ \mathit{in}\ ([\![N]\!]^*_S \text{ if } n = 0, [\![P]\!]^*_S \text{ else})
\end{aligned}$$

$$[\![M \mathbin{\textcircled{\scriptsize \vee}} N]\!]^*_S = [\![\mathbin{\textcircled{\scriptsize \vee}}]\!]_S\,([\![M]\!]^*_S)([\![N]\!]^*_S) \qquad [\![M \oplus N]\!]^*_S = [\![\oplus]\!]_S\,([\![M]\!]^*_S)([\![N]\!]^*_S)$$

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

$\mathit{let}\, v \Leftarrow F\ \mathit{in}\ G(v) = (h \mapsto F(v \mapsto G(v)(h)))$

. . . we now need *sub*normalized previsions ($F(\frac{a+h}{2}) \leq \frac{1}{2}(a + F(h))$)
+ no $\bot$ in base types: $[\![\mathtt{Nat}]\!]_S = \mathbb{N}$, $[\![\mathtt{S}]\!]_S = \{\top\}$

Operational Semantics

New notion: values $V = \mathtt{rec}\, f \cdot \lambda x \cdot M \mid \underline{\top} \mid \underline{n}$

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

Semantically, $[\![V]\!]^*_S = \mathit{val}([\![V]\!]^\circ_S)$ where

$[\![\mathtt{rec}\, f \cdot \lambda x \cdot M]\!]^\circ_S = \mathit{lfp}(f, x \mapsto [\![M]\!]^*_S)$, $[\![\underline{\top}]\!]^\circ_S = \top$, $[\![\underline{n}]\!]^\circ_S = n$

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

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

The CBV PCF(S) Machine

1. Redex Discovery Rules

$$E \cdot MN \to E[\_N] \cdot M$$
$$E[\_N] \cdot \mathtt{rec}\, f \cdot \lambda x \cdot M \to E[(\mathtt{rec}\, f \cdot \lambda x \cdot M)\_] \cdot N \qquad \text{(new)}$$
$$E \cdot \mathtt{pred}\, M \to E[\mathtt{pred}\, \_] \cdot M \qquad E \cdot \mathtt{succ}\, M \to E[\mathtt{succ}\, \_] \cdot M$$
$$E \cdot \mathtt{ifz}\, M\, N\, P \to E[\mathtt{ifz}\, \_\, N\, P] \cdot M$$

2. Computation

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

3. Choice states are now $E \cdot M \mathbin{\bigcirc\!\!\!\!\vee} N$, $E \cdot M \oplus N$
4. Termination state: $\_ \cdot \underline{\top}$

Termination Semantics

Essentially the same as before:

$$\frac{C' \downarrow^m a}{C \downarrow^m a}\,(C \to C') \qquad \frac{}{\_ \cdot \top \downarrow^m a}\,(a \in \mathbb{Q} \cap [0,1))$$

$$\frac{E \cdot M \downarrow^{\text{may}} a}{E \cdot M \mathbin{\textcircled{\scriptsize$\vee$}} N \downarrow^{\text{may}} a} \qquad \frac{E \cdot N \downarrow^{\text{may}} a}{E \cdot M \mathbin{\textcircled{\scriptsize$\vee$}} N \downarrow^{\text{may}} a} \qquad \frac{E \cdot M \downarrow^{\text{must}} a \quad E \cdot N \downarrow^{\text{must}} a}{E \cdot M \mathbin{\textcircled{\scriptsize$\vee$}} N \downarrow^{\text{must}} a}$$

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

Soundness

Theorem (Soundness)

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

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

Computational Adequacy

Theorem (Computational Adequacy)

- $[\![M]\!]^*_S(\blacklozenge) = Pr(\_ \cdot M{\downarrow}^{\mathsf{may}})$ *(if* $S \subseteq \{\mathtt{A}, \mathtt{P}\}$*)*
- $[\![M]\!]^*_S(\blacklozenge) = Pr(\_ \cdot M{\downarrow}^{\mathsf{must}})$ *(if* $S \subseteq \{\mathtt{D}, \mathtt{P}\}$*)*

Proof: Define logical relation R^*_τ (terms), $R^\perp_\tau$ (contexts), R°_τ (values):

$$\begin{array}{rll} M\, R^*_\sigma\, F & \text{iff} & \text{for all } E\, R^\perp_\sigma\, h,\ \Pr(E \cdot M{\downarrow}^m) \geq F(h) \\ E\, R^\perp_\sigma\, h & \text{iff} & \text{for all } V\, R^\circ_\sigma\, v,\ \Pr(E \cdot V{\downarrow}^m) \geq h(v) \\ V_f\, R^\circ_{\sigma\Rightarrow\tau}\, \varphi & \text{iff} & \text{for all } V\, R^\circ_\sigma\, v,\ E\, R^\perp_\tau\, h,\ \Pr(E[V_f\,\_] \cdot V{\downarrow}^m) \geq \varphi(v)(h) \end{array}$$

$$\underline{m}\, R^\circ_{\mathtt{Nat}}\, n \text{ iff } m = n \qquad \underline{\top}\, R^\circ_{\mathtt{S}}\, \top$$

Show $V\, R^\circ_\tau\, [\![V^\circ]\!]_S$ and $M\, R^*_\tau\, [\![M^*]\!]_S$.
Finally take $E = \_$, $h = \blacklozenge$ at $\tau = \mathtt{S}$. □

Statistical Termination Testers

Do we still need termination testers?

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

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

Proof. Define logical relation R^*_τ, $R^\perp_\tau$, R°_τ:

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

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

Statistical Termination Testers

Do we still need termination testers?

Theorem (Yes, in Probabilistic Cases ($\mathtt{P} \in S$))

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

Proof. Define logical relation R^*_τ, $R^\perp_\tau$, R°_τ:

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

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

Fact (No, in Non-Probabilistic Cases ($\mathtt{P} \notin S$))

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

Statistical Termination Testers

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

$$\frac{\_ \cdot M \downarrow^m b \quad E \cdot \top \downarrow^m a}{E \cdot \mathtt{Pr}(M > b) \downarrow^m a}\,(\mathtt{Pr})$$

$$[\![\mathtt{Pr}(M > b)]\!]^*_S = \begin{cases} val\,\top & \text{if } [\![M]\!]^*_S(\blacklozenge) > b \\ 0 & \text{otherwise} \end{cases}$$

Computational adequacy: still OK.

The Angelic+Probabilistic Case

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

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

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

$$M \lesssim^{\text{may}} N \text{ iff } [\![M]\!]_{\{\mathtt{A},\mathtt{P}\}} \leq [\![N]\!]_{\{\mathtt{A},\mathtt{P}\}}$$

Proof.

- Open subbase $[a \mapsto h > r] = \{f \in [\![\sigma \Rightarrow \tau]\!]_S \mid f(a)(h) > r\}$
  definable by $E[\mathtt{Pr}(\_ > r)][V_h\_][\_V_a]$
- Basis of values definable from $\bigtriangledown$, $\oplus$, $\mathtt{val}$, Ω (0)
  The "nuisance" $\sup_{i=1}^m$ is definable through $\bigtriangledown$ $(= \sup)$. □

Note: no need for $\mathtt{por}$.

The Purely Angelic Case

Let $M \lesssim^{m} N$ 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 $S = \{\mathtt{A}\}$)

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

$$M \lesssim^{\text{may}} N \text{ iff } M \precsim^{\text{may}} N \text{ iff } [\![M]\!]_{\{\mathtt{A}\}} \leq [\![N]\!]_{\{\mathtt{A}\}}$$

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

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

Fully abstract, as is!

The Purely Angelic Case: Standard Semantics

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

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

$$[\![x]\!]^*_S = \downarrow x \qquad [\![\underline{\top}]\!]^*_S = \{\top\} \qquad [\![\underline{n}]\!]^*_S = \{n\}$$

$$[\![\mathtt{rec}\, f \cdot \lambda x \cdot M]\!]^*_S = \downarrow(\mathit{lfp}(f, x \mapsto [\![M]\!]^*_S))$$

$$[\![MN]\!]^*_S = \bigcup_{f \in [\![M]\!]^*_S, v \in [\![N]\!]^*_S} f(v)$$

$$[\![\mathtt{pred}\, M]\!]^*_S = \{n - 1 \mid n \in [\![M]\!]^*_S, n \neq 0\}$$

$$[\![\mathtt{succ}\, M]\!]^*_S = \{n + 1 \mid n \in [\![N]\!]^*_S\}$$

$$[\![\mathtt{ifz}\ M\ N\ P]\!]^*_S = \begin{cases} \emptyset & \text{if } [\![M]\!]^*_S = \emptyset \\ [\![N]\!]^*_S & \text{if } [\![M]\!]^*_S = \{0\} \\ [\![P]\!]^*_S & \text{if } [\![M]\!]^*_S \neq \emptyset, \text{ does not contain } 0 \\ [\![N]\!]^*_S \cup [\![P]\!]^*_S & \text{if } [\![M]\!]^*_S \text{ contains } 0 \text{ and some } n \neq 0 \end{cases}$$

$$[\![M \mathbin{\textcircled{\scriptsize V}} N]\!]^*_S = [\![M]\!]^*_S \cup [\![N]\!]^*_S$$

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

Outline

Conclusion

The angelic cases . . . are angelic:

- Call-by-value PCF($\{\mathtt{A}\}$) is fully abstract
- Call-by-value PCF($\{\mathtt{A},\mathtt{P}\}$)+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 ($\mathtt{D} \in S$), $[\![\mathtt{T}\tau]\!]_S$ 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 $(h \in [X \to I] \mapsto F(\widehat{h}))$,
where $\widehat{h}(x) = h(x)$ $(x \in X)$ and $\widehat{h}(\mathrm{err}) = 1$.
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 $(= \mathit{lax}(\delta_{\mathrm{err}}))$
- Lax prev. closed under $\frac{-+-}{2}$ $(\mathtt{P} \in S)$, min $(\mathtt{D} \in S)$, max $(\mathtt{A} \in S)$

CBV PCF(S)+ $\mathtt{irq}$

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

New operational rules

$$\frac{E \cdot M \downarrow^m a}{E \cdot M \ \mathtt{irq} \ N \downarrow^m a} \qquad \frac{\_ \cdot N \downarrow^m a}{E \cdot M \ \mathtt{irq} \ N \downarrow^m a}$$

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

Note: $\mathtt{abort} = M \ \mathtt{irq} \ \bot$ aborts immediately (M arbitrary)

Den. semantics: $[\![M \ \mathtt{irq} \ N]\!]^*_S(h) = \max([\![M]\!]^*_S(h), [\![N]\!]^*(\blacklozenge))$

Soundness, computational adequacy: still OK.

The Demonic+Probabilistic Case

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

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

$$M \overset{\text{must}}{\sim} N \text{ iff } [\![M]\!]_{\{\mathtt{D},\mathtt{P}\}} \leq [\![N]\!]_{\{\mathtt{D},\mathtt{P}\}}$$

Proof.

- Open subbase $[a \mapsto h > r] = \{f \in [\![\sigma \Rightarrow \tau]\!]_S \mid f(a)(h) > r\}$
  definable by $E[\mathtt{Pr}(\_ > r)][V_h \_][\_ V_a]$
  Note that Scott=weak again on lax previsions
- Basis of values definable from $\bigtriangledown$, $\oplus$, $\mathtt{val}$, Ω, and $\mathtt{abort}$.
  "Nuisance" $\sup_{i=1}^m$: use "sup-as-inf" trick:

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

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

$F \; \mathit{irq} \top = (h \mapsto 1)$, $F \; \mathit{irq} \bot = F$ ... definable through $\mathtt{irq}$ and min definable through $\bigtriangledown$.

The Purely Demonic Case

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

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

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

$$M \lesssim^{\text{must}} N \text{ iff } M \precsim^{\text{must}} N \text{ iff } [\![M]\!]_{\{\mathtt{D}\}} \leq [\![N]\!]_{\{\mathtt{D}\}}$$

Back to the Angelic Cases

Everything works with lax previsions and `irq` as before

in angelic cases

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

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

$$M \lesssim^{\text{may}} N \text{ iff } M \precsim^{\text{may}} N \text{ iff } [\![M]\!]_{\{\mathtt{A}\}} \leq [\![N]\!]_{\{\mathtt{A}\}}$$

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

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

$$M \lesssim^{\text{may}} N \text{ iff } [\![M]\!]_{\{\mathtt{A},\mathtt{P}\}} \leq [\![N]\!]_{\{\mathtt{A},\mathtt{P}\}}$$

The Erratic Cases

When $\{\mathtt{A}, \mathtt{D}\} \subseteq S$, 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 $\{\mathtt{A}, \mathtt{D}\} \subseteq S$. Let $S^- = S \cap \{\mathtt{D}, \mathtt{P}\}$, $S^+ = S \cap \{\mathtt{A}, \mathtt{P}\}$.
We don't care because:

Lemma

$$[\![M]\!]^*_S = ([\![M]\!]^*_{S^-}, [\![M]\!]^*_{S^+})$$

. . . merely ignoring Walley's condition

Now, if $[\![M]\!]^*_S \not\leq [\![N]\!]^*_S$, either:

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

Full Abstraction in the Erratic Cases

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

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

We therefore obtain:

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

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

$$M \lesssim N \text{ iff } M \precsim N \text{ iff } [\![M]\!]_{\{\mathtt{A},\mathtt{D}\}} \leq [\![N]\!]_{\{\mathtt{A},\mathtt{D}\}}$$

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

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

$$M \lesssim N \text{ iff } [\![M]\!]_{\{\mathtt{A},\mathtt{D},\mathtt{P}\}} \leq [\![N]\!]_{\{\mathtt{A},\mathtt{D},\mathtt{P}\}}$$