Full Abstraction for Non-Deterministic and Probabilistic Extensions of PCF

Jean Goubault-Larrecq

ANR Blanc CPP

PLC Festschrift – Sep. 2013
Outline

1. Introduction

2. PCF(S)
   - Syntax
   - Operational Semantics
   - Denotational Semantics

3. The Full Abstraction Problem
   - Full Abstraction
   - Definability
   - Full Abstraction in Angelic Cases

4. Conclusion
Outline

1. Introduction

2. PCF($S$)
   - Syntax
   - Operational Semantics
   - Denotational Semantics

3. The Full Abstraction Problem
   - Full Abstraction
   - Definability
   - Full Abstraction in Angelic Cases

4. 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 [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:
- Will concentrate on angelic non-deterministic choice
- also probabilistic choice, + mixed
Outline

1. Introduction

2. PCF(S)
   - Syntax
   - Operational Semantics
   - Denotational Semantics

3. The Full Abstraction Problem
   - Full Abstraction
   - Definability
   - Full Abstraction in Angelic Cases

4. Conclusion
Types

\[ \gamma ::= \text{Nat} \mid S \quad \text{Ground types} \]
\[ \sigma, \tau ::= \gamma \mid \sigma \rightarrow \tau \mid T\tau \quad \text{Types} \]

Notes:
- \( S \) has only one (non-bottom) value
  \( = \text{unit type, termination type} \)
  Not required in principle, but practical
- \( T\tau \) type of \text{processes} computing value of type \( \tau \)
  \( \text{à la } [\text{Moggi91}] \)
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 $M : \tau$, val $M : T \tau$
  - for all $M : \sigma$, $N : T \tau$, let $x \leftarrow M$ in $N : T \tau$
  - Non-det. choice $\nabla : T \tau \rightarrow T \tau \rightarrow T \tau$
  - Prob. choice $\oplus : T \tau \rightarrow T \tau \rightarrow T \tau$
Operational Semantics

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

“The probability that $E \cdot M$ may terminate is $> a$”

- Redex discovery/computation rule $C \rightarrow C'$:
  
  $\begin{array}{c}
  C' \downarrow^{m} a \\
  \hline
  C \downarrow^{m} a
  \end{array}$

  for each rule $C \rightarrow C'$:

  $E \cdot MN \rightarrow E[\_N] \cdot M$

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

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

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

- Choice:

  $\begin{array}{ccc}
  E \cdot M \downarrow^{\text{may}} a & E \cdot N \downarrow^{\text{may}} a & E \cdot M \downarrow^{\text{may}} a \quad E \cdot N \downarrow^{\text{may}} b \\
  E[\_MN] \cdot \bigotimes \downarrow^{\text{may}} a & E[\_MN] \cdot \bigotimes \downarrow^{\text{may}} a & E[\_MN] \cdot \bigoplus \downarrow^{\text{may}} \frac{1}{2} (a + b)
  \end{array}$
Full Abstraction for PCF with Choice

PCF(S)

Operational Semantics

Termination Semantics

Definition

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

- \( \Pr(\text{val } \cdot \top \downarrow^\text{may}) = 1 \)
- \( \Pr(E[MN] \cdot \oplus \downarrow^\text{may}) = \frac{1}{2} (\Pr(E \cdot M \downarrow^\text{may}) + \Pr(E \cdot N \downarrow^\text{may})) \)
- \( \Pr(E[MN] \cdot \bigvee \downarrow^\text{may}) = \max(\Pr(E \cdot M \downarrow^\text{may}), \Pr(E \cdot N \downarrow^\text{may})) \)
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)
- $F\left(\frac{h+h'}{2}\right) \leq \frac{1}{2}(F(h) + F(h'))$
- $F(h) \in \{0, 1\}$ for every $h : X \to \{0, 1\}$ (if $P \not\in S$)

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

\[
\begin{align*}
\llbracket \lambda x \cdot M \rrbracket_S &= (x \mapsto \llbracket M \rrbracket_S) \\
\llbracket Y \rrbracket_S &= (f \mapsto \bigcup_{n \in \mathbb{N}} f^n(\bot)) \\
\llbracket \text{val } M : T \sigma \rrbracket_S &= (h \mapsto h(\llbracket M \rrbracket_S)) \\
\llbracket \text{let } x \leftarrow M \text{ in } N \rrbracket_S &= (h \mapsto \llbracket M \rrbracket_S (x \mapsto \llbracket N \rrbracket_S (h))) \\
\llbracket \bigvee \rrbracket_S &= (F_1, F_2, h \mapsto \max(F_1(h), F_2(h))) \\
\llbracket \bigoplus \rrbracket_S &= (F_1, F_2, h \mapsto \frac{1}{2}(F_1(h) + F_2(h)) (\text{if } \mathcal{P} \in S))
\end{align*}
\]
In usual PCF, **soundness** states that if $M \rightarrow^* V$ then $\llbracket M \rrbracket = \llbracket V \rrbracket$.

**Theorem (Soundness)**

Let $\blacklozenge = \chi_{\{\top\}} : \llbracket S \rrbracket \to I$ map $\perp$ to 0, $\top$ to 1 (termination-observing continuation).

- If $E \cdot M \downarrow^{\text{may}} a$ then $\llbracket E[M] \rrbracket_S (\blacklozenge) > a$

**Proof:** induction.

**Corollary**

- $\llbracket E[M] \rrbracket_S (\blacklozenge) \geq \Pr(E \cdot M \downarrow^{\text{may}})$
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)**

\[ \llbracket M \rrbracket_S (\Diamond) = Pr(\_ \cdot M \downarrow^{\text{may}}) \]

**Proof:** The key point is the definition of a suitable logical relation... and precisely there is a general definition of...
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)**

$\square \llbracket M \rrbracket_S (♦) = Pr(_- \cdot M \downarrow^{\text{may}})$

**Proof:** The key point is the definition of a suitable logical relation... and precisely there is a general definition of...
In usual PCF, $M \rightarrow^* V$ iff $\llbracket M \rrbracket = \llbracket V \rrbracket$, at ground types. Here, use $E = \bot$ (empty context, of type $TS \vdash TS$).

**Theorem (Computational Adequacy)**

$\llbracket M \rrbracket_S (\diamond) = Pr(\bot \cdot M \downarrow^{may})$

**Proof:** Define a logical relation $R_\sigma$ by (something like) double orthogonality:

$M R_{T_\sigma} F$ 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 $Q R_\sigma \nu$, $Pr(E \cdot \text{val} Q \downarrow^m) \geq h(\nu)$

Then do some stuff and conclude. \qed
Outline

1. Introduction

2. PCF(S)
   - Syntax
   - Operational Semantics
   - Denotational Semantics

3. The Full Abstraction Problem
   - Full Abstraction
   - Definability
   - Full Abstraction in Angelic Cases

4. Conclusion
Full Abstraction

Let $M \simeq_{\text{may}} N$ iff $\Pr(E \cdot M \downarrow_{\text{may}}) \leq \Pr(E \cdot N \downarrow_{\text{may}})$ for every $E : \tau \vdash TS$.

Conjecture (Full Abstraction)

$M \simeq_{\text{may}} N$ 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 $E : \tau \vdash TS$
  So $\Pr(E \cdot M \downarrow_{\text{may}}) \leq \Pr(E \cdot N \downarrow_{\text{may}})$ by computational adequacy.

- Hard direction: assume $\llbracket M \rrbracket_S \nleq \llbracket N \rrbracket_S$, find $E$ such that $\Pr(E \cdot M \downarrow_{\text{may}}) > \Pr(E \cdot N \downarrow_{\text{may}})$
  So hard that it is wrong for PCF... but true for PCF($A$)!
Pierre-Louis has always told us that \textit{definability} was the key to full abstraction.

---

**Definability and full abstraction**

Pierre-Louis Curien

\textit{PPS, CNRS and University Paris 7}

---

**Abstract**

Game semantics has renewed denotational semantics. It offers among other things an attractive classification of programming features, and has brought a bunch of new definability results. In parallel, in the denotational semantics of proof theory, several full completeness results have been shown since the early nineties. In this note, we review the relation between definability and full abstraction, and we put a few old and recent results of this kind in perspective.

\textit{Keywords:} operational semantics, denotational semantics, sequentiality.
Definability... of Opens

So assume $[[M]]_S \not\leq [[N]]_S$, of type $\tau$.

- Since $\leq$ is specialization ordering of (Scott) topology, there is a separating open set $U$:

  $[[M]]_S \in U \quad [[N]]_S \not\in U$

- If we can define $U$ by a context $E$, then:

  $[[E[M]]]_S = \top \quad [[E[N]]]_S = \bot$

  so by computational adequacy

  $\Pr(\text{val } E \cdot M \downarrow^\text{may}) = 1 > 0 = \Pr(\text{val } E \cdot N \downarrow^\text{may})$

  So $M \not\preceq^\text{may} N$.

- By contraposition, $M \not\preceq^\text{may} N$ implies $[[M]]_S \leq [[N]]_S$.

  So full abstraction will hold.
Definability... of Subbasic Opens

So assume \([M]_S \not\leq [N]_S\), of type \(\tau\).

- Since \(\leq\) is specialization ordering of (Scott) topology, there is a separating open set \(U\) in a given subbase \(B_\tau\):

\[
[M]_S \in U \quad [N]_S \not\in U
\]

- If we can define \(U\) by a context \(E\), then:

\[
[E[M]]_S = \top \quad [E[N]]_S = \bot
\]

so by computational adequacy

\[
\Pr(\text{val } E \cdot M \downarrow^{\text{may}}) = 1 > 0 = \Pr(\text{val } E \cdot N \downarrow^{\text{may}})
\]

So \(M \not\leadsto^{\text{may}} N\).

- By contraposition, \(M \not\leadsto^{\text{may}} N\) implies \([M]_S \not\leq [N]_S\).

So full abstraction will hold.
Choosing the Right Subbase

Fortunately:

**Lemma**

For every type $\tau$, $[\tau]_S$ is a bc-domain.

(One of the nice CCCs of continuous domains.)

**Proposition (Key result — coincidence of topologies)**

If $X$ and $Y$ are bc-domains, then:

- **Scott topology on $[X \rightarrow Y]$ = pointwise convergence**  
  *Subbasis:*$[a \in V] = \{ f \mid f(a) \in V \}$, $a \in X$, $V$ open in $Y$

- **Scott topology on previsions on $X$ = weak topology**  
  *Subbasis:*$[h > r] = \{ F \mid F(h) > r \}$, $h \in [X \rightarrow I]$, $r \in \mathbb{Q}$
Miracle

All these subbasic opens are \textit{definable}.

- E.g., on $[X \to Y]$, let $a$ be defined by term $t$
  - Let $V$ be defined by context $E$
  - Then $[a \in V]$ is defined by context $E[t]$.

Mission accomplished!

\ldots almost.

We actually need to define \textit{elements} $a$ as well.

Eventually, this requires some additional constructions.

E.g., sup of maps requires $\boxplus$ (non-det. choice).

Worse: prob. choice $\boxplus$ requires statistical termination testers.
The Purely Angelic Case

Without probabilities, $M \preceq_{\text{may}} N$ simplifies to:
for every context $E$, $E \cdot M \downarrow_{\text{may}}$ implies $E \cdot N \downarrow_{\text{may}}$.

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

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

\[ M \preceq_{\text{may}} N \text{ iff } \llbracket M \rrbracket_{\{A\}} \leq \llbracket N \rrbracket_{\{A\}} \]

**Note 1:** No need for parallel or
\[ M \parallel N = (M \parallel N) \ominus (N \parallel M) \]

**Note 2:** Proof much simpler than Plotkin’s for PCF+$\parallel$. . . but language is different.

**Note 3:** Implies full abstraction for (isomorphic) semantics using Hoare powerdomains instead of previsions.
The Angelic+Probabilistic Case

We now need termination testers $\Pr(M > b)$ to the language $(M : TS)$

$$
\frac{\_ \cdot M \downarrow \text{may } b \quad E \cdot \bot \downarrow \text{may } a}{E \cdot \Pr(M > b) \downarrow \text{may } a} \quad (\Pr) \quad \lbrack \Pr(M > b) \rbrack_s = \begin{cases} 
\bot & \text{if } \lbrack M \rbrack_s (\Diamond) > b \\
\bot & \text{otherwise}
\end{cases}
$$
The Angelic+Probabilistic Case

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

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

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

\[ M \leq^{\text{may}} N \iff \llbracket M \rrbracket_{\{A, P\}} \leq \llbracket N \rrbracket_{\{A, P\}} \]

**Proof.** As before, there is a subbasis of definable opens. \qed
Outline

1. Introduction

2. PCF(S)
   - Syntax
   - Operational Semantics
   - Denotational Semantics

3. The Full Abstraction Problem
   - Full Abstraction
   - Definability
   - Full Abstraction in Angelic Cases

4. Conclusion
Conclusion

The angelic cases ... are angelic:

- PCF(\{A\}) is fully abstract
- PCF(\{A, P\}) is fully abstract provided we add statistical termination testers
- I cheated a bit: we need a bit of call-by-value to define the probabilistic contexts
- Demonic/erratic cases slightly more difficult
- Purely probabilistic case hopeless unless we turn to random variables, maybe.