Logical Relations for PCF

Peter Gammie

August 28, 2014

Abstract

We apply Andy Pitts’s methods of defining relations over domains to several classical results in the literature. We show that the Y combinator coincides with the domain-theoretic fixpoint operator, that parallel-or and the Plotkin existential are not definable in PCF, that the continuation semantics for PCF coincides with the direct semantics, and that our domain-theoretic semantics for PCF is adequate for reasoning about contextual equivalence in an operational semantics. Our version of PCF is untyped and has both strict and non-strict function abstractions. The development is carried out in HOLCF.
1 Introduction

Showing the existence of relations on domains has historically been an involved process. This is due to the presence of the contravariant function space domain constructor that defeats familiar inductive constructions; in particular we wish to define "logical" relations, where related functions take related arguments to related results, and the corresponding relation transformers are not monotonic. Before Pitts (1996) such demonstrations involved laborious appeals to the details of the domain constructions themselves. (See Mulmuley (1987); Stoy (1977) for historical perspective.)

Here we develop some standard results about PCF using Pitts’s technique for showing the existence of particular recursively-defined relations on domains. By doing so we demonstrate that HOLCF (Müller et al. 1999; Huffman 2012b) is useful for reasoning about programming language semantics and not just particular programs.

We treat a variant of the PCF language due to Plotkin (1977). It contains both call-by-name and call-by-value abstractions and is untyped. We show the breadth of Pitts’s technique by compiling several results, some of which have only been shown in simply-typed settings where the existence of the logical relations is straightforward to demonstrate.

2 Pitts’s method for solving recursive domain predicates

We adopt the general theory of Pitts (1996) for solving recursive domain predicates. This is based on the idea of minimal invariants that Pitts (1993, Def 2) ascribes “essentially to D. Scott”.

Ideally we would like to do the proofs once and use Pitts’s relational structures. Unfortunately it seems we need higher-order polymorphism (type functions) to make this work (but see Huffman (2012a)). Here we develop three versions, one for each of our applications. The proofs are similar (but not quite identical) in all cases.

We begin by defining an admissible set (aka an inclusive predicate) to be one that contains ⊥ and is closed under countable chains:

definition admS :: ‘a::pcpo set set where
admS ≡ { R :: ‘a set. ⊥ ∈ R ∧ adm (λx. x ∈ R) }

typedef (‘a::pcpo) admS = { x::’a::pcpo set . x ∈ admS }

morphism unlr mklr unfolding admS-def by fastforce

These sets form a complete lattice.

2.1 Sets of vectors

The simplest case involves the recursive definition of a set of vectors over a single domain. This involves taking the fixed point of a functor where the positive (covariant) occurrences of the recursion variable are separated from the negative (contravariant) ones. (See §3.4 etc. for examples.)

By dually ordering the negative uses of the recursion variable the functor is made monotonic with respect to the order on the domain ‘d. Here the type constructor ‘a dual yields a type
with the same elements as `'a` but with the reverse order. The functions dual and undual mediate the isomorphism.

```plaintext
type-synonym 'd lf-rep = 'd admS dual × 'd admS ⇒ 'd set
type-synonym 'd lf = 'd admS dual × 'd admS ⇒ 'd admS
```

The predicate $eRSV$ encodes our notion of relation. (This is Pitts’s $e : R ⊂ S$.) We model a vector as a function from some index type `'i` to the domain `'d`. Note that the minimal invariant is for the domain `'d` only.

```plaintext
abbreviation $eRSV :: ('d::pcpo ⇒ 'd) ⇒ ('i::type ⇒ 'd) admS dual ⇒ ('i ⇒ 'd) admS ⇒ bool$
where $eRSV e R S ≡ ∀ d ∈ unlr (undual R). (λx. e·(d x)) ∈ unlr S$
```

In general we can also assume that $e$ here is strict, but we do not need to do so for our examples.

Our locale captures the key ingredients in Pitts’s scheme:

- that the function $δ$ is a minimal invariant;
- that the functor defining the relation is suitably monotonic; and
- that the functor is closed with respect to the minimal invariant.

```plaintext
locale DomSolV = 
  fixes $δ :: ('d::pcpo ⇒ 'd) ⇒ 'd ⇒ 'd$
  fixes $F :: ('i::type ⇒ 'd::pcpo) lf$
  assumes min-inv-ID: $fix · δ = ID$
  assumes monoF: mono $F$
  assumes eRSV-deltaF:
      $⋀ (e :: 'd ⇒ 'd) (R :: ('i ⇒ 'd) admS dual) (S :: ('i ⇒ 'd) admS).$
      $eRSV e R S ⇒ eRSV (δ·e) (dual (F (dual S, undual R))) (F (R, S))$
```

From these assumptions we can show that there is a unique object that is a solution to the recursive equation specified by $F$.

```plaintext
definition $delta ≡ delta-pos$
lemma delta-sol: $delta = F (dual delta, delta)$
lemma delta-unique:
    assumes $r : F (dual r, r) = r$
    shows $r = delta$
end
```

We use this to show certain functions are not PCF-definable in §3.3.

### 2.2 Relations between domains and syntax

To show computational adequacy (§4.3) we need to relate elements of a domain to their syntactic counterparts. An advantage of Pitts’s technique is that this is straightforward to do.

```plaintext
definition synlr :: ('d::pcpo × 'a::type) set set where
```
The inclusions need to be strict to get our example through.

\[
\text{type-synonym} \set\ (\text{type-synonym} \set) \text{ recursive domains. Each of the pairs represents a (monadic) computation and value space.}
\]

Following Reynolds (1974) and Filinski (2007), we want to relate two pairs of mutually-

\[2.3 \text{ Relations between pairs of domains}\]

Following Reynolds (1974) and Filinski (2007), we want to relate two pairs of mutually-

\[
typedef ('d::pcpo, 'a::type) \text{ synlr} = \{ x::('d \times 'a) \text{ set. } x \in \text{synlr} \}
\]

\[
\text{morphisms unsynlr mksynlr unfolding synlr-def by fastforce}
\]

An alternative representation (suggested by Brian Huffman) is to directly use the type \('a \Rightarrow \text{ admS}'\ as this is automatically a complete lattice. However we end up fighting the automatic methods a lot.

Again we define functors on \('(d, 'a) \text{ synlr}'\).

\[
\text{type-synonym} \ (d, 'a) \text{ synlf-rep} = (d, 'a) \text{ synlr dual \times (d, 'a) synlr} \Rightarrow (d \times 'a) \text{ set}
\]

\[
\text{where} \ e \text{RSS} \ e R S \equiv \forall (d, a) \in \text{unsynlr (undual R)}. (e \cdot d, a) \in \text{unsynlr S}
\]

\[
\text{locale DomSolSyn =}
\]

\[
\text{fixes \(e \text{RSS} \ e R S \equiv \forall (d, a) \in \text{unsynlr (undual R)}. (e \cdot d, a) \in \text{unsynlr S}\)
\]

\[
\text{locale DomSolSyn =}
\]

\[
\text{fixes \(e \text{RSS} \ e R S \equiv \forall (d, a) \in \text{unsynlr (undual R)}. (e \cdot d, a) \in \text{unsynlr S}\)
\]

Again, from these assumptions we can construct the unique solution to the recursive equation

specified by \(F\).

\[
\text{2.3 Relations between pairs of domains}
\]

Following Reynolds (1974) and Filinski (2007), we want to relate two pairs of mutually-

\[
\text{type-synonym} \ (\text{am}, \text{bm}, \text{av}, \text{bv}) \text{ lr-pair} = (\text{am} \times \text{bm}) \text{ admS} \times (\text{av} \times \text{bv}) \text{ admS}
\]

\[
\text{type-synonym} \ (\text{am}, \text{bm}, \text{av}, \text{bv}) \text{ lf-pair-rep} =
\]

\[
(\text{am}, \text{bm}, \text{av}, \text{bv}) \text{ lr-pair dual} \times (\text{am}, \text{bm}, \text{av}, \text{bv}) \text{ lr-pair} \Rightarrow ((\text{am} \times \text{bm}) \text{ set} \times (\text{av} \times \text{bv}) \text{ set})
\]

\[
\text{type-synonym} \ (\text{am}, \text{bm}, \text{av}, \text{bv}) \text{ lf-pair} =
\]

\[
(\text{am}, \text{bm}, \text{av}, \text{bv}) \text{ lr-pair dual} \times (\text{am}, \text{bm}, \text{av}, \text{bv}) \text{ lr-pair} \Rightarrow ((\text{am} \times \text{bm}) \text{ admS} \times (\text{av} \times \text{bv}) \text{ admS})
\]

The inclusions need to be strict to get our example through.

\[
\text{abbreviation}
\]

\[
\text{eRSP} :: ((\text{am::pcpo} \rightarrow \text{am}) \times (\text{av::pcpo} \rightarrow \text{av}))
\]

\[
\Rightarrow ((\text{bm::pcpo} \rightarrow \text{bm}) \times (\text{bv::pcpo} \rightarrow \text{bv}))
\]

\[
\Rightarrow ((\text{am} \times \text{bm}) \text{ admS} \times (\text{av} \times \text{bv}) \text{ admS}) \text{ dual}
\]
⇒ ('am × 'bm) admS × ('av × 'bv) admS
⇒ bool

where

eRSP \alpha \beta R S \equiv
\forall (am, bm) \in unlr (fst (undual R)). (fst ea-am, fst eb-bm) \in unlr (fst S)
\land (\forall (av, bv) \in unlr (snd (undual R)). (snd ea-av, snd eb-bv) \in unlr (snd S))

locale DomSolP =
fixes ad :: (('am::pcpo \to 'am) \times ('av::pcpo \to 'av)) \to (('am \to 'am) \times ('av \to 'av))
fixes bd :: (('bm::pcpo \to 'bm) \times ('bv::pcpo \to 'bv)) \to (('bm \to 'bm) \times ('bv \to 'bv))
fixes F :: ('am, 'bm, 'av, 'bv) lf-pair
assumes monoF:
assumes ad-ID:
assumes bd-ID:
assumes ad-strict:
assumes bd-strict:
assumes eRSP-deltaF:

We use this solution to relate the direct and continuation semantics for PCF in §5.

3 Logical relations for definability in PCF

Using this machinery we can demonstrate some classical results about PCF (Plotkin 1977). We diverge from the traditional treatment by considering PCF as an untyped language and including both call-by-name (CBN) and call-by-value (CBV) abstractions following Reynolds (1974). We also adopt some of the presentation of Winskel (1993, Chapter 11), in particular by making the fixed point operator a binding construct.

We model the syntax of PCF as a HOL datatype, where variables have names drawn from the naturals:

type-synonym var = nat
datatype expr =
  Var var
| App expr expr
| AbsN var expr
| AbsV var expr
| Diverge (Ω)
| Fix var expr
| tt
| ff
| Cond expr expr expr
| Num nat
| Succ expr
| Pred expr
| IsZero expr
3.1 Direct denotational semantics

We give this language a direct denotational semantics by interpreting it into a domain of values.

domain \( ValD = \)

\[ ValF \text{ (lazy } appF :: ValD \rightarrow ValD) \]  
\mid ValTT \mid ValFF  
\mid ValN \text{ (lazy } nat) \]

The \textit{lazy} keyword means that the \( ValF \) constructor is lifted, i.e. \( ValF \cdot \perp \neq \perp \), which further means that \( ValF \cdot (\Lambda x. \perp) \neq \perp \).

The naturals are discretely ordered.

The minimal invariant for \( ValD \) is straightforward; the function \( cfun-map \cdot f \cdot g \cdot h \) denotes \( g oo h oo f \).

\[ \text{fixrec } ValD-copy-rec :: (ValD \rightarrow ValD) \rightarrow (ValD \rightarrow ValD) \]  
\[ \text{where} \]

\[ ValD-copy-rec \cdot r \cdot (ValF \cdot f) = ValF \cdot (cfun-map \cdot r \cdot r \cdot f) \]  
\mid ValD-copy-rec \cdot r \cdot (ValTT) = ValTT  
\mid ValD-copy-rec \cdot r \cdot (ValFF) = ValFF  
\mid ValD-copy-rec \cdot r \cdot (ValN \cdot n) = ValN \cdot n \]

We interpret the PCF constants in the obvious ways. “Ill-typed” uses of these combinators are mapped to \( \perp \).

\[ \text{definition } cond :: ValD \rightarrow ValD \rightarrow ValD \rightarrow ValD \text{ where} \]

\[ cond \equiv \Lambda i t e. \text{ case } i \text{ of } ValF \cdot f \Rightarrow \perp | ValTT \Rightarrow t | ValFF \Rightarrow e | ValN \cdot n \Rightarrow \perp \]

\[ \text{definition } succ :: ValD \rightarrow ValD \text{ where} \]

\[ succ \equiv \Lambda (ValN \cdot n). ValN \cdot (n + 1) \]

\[ \text{definition } pred :: ValD \rightarrow ValD \text{ where} \]

\[ pred \equiv \Lambda (ValN \cdot n). \text{ case } n \text{ of } 0 \Rightarrow \perp | \text{Suc } n \Rightarrow ValN \cdot n \]

\[ \text{definition } isZero :: ValD \rightarrow ValD \text{ where} \]

\[ isZero \equiv \Lambda (ValN \cdot n). \text{ if } n = 0 \text{ then } ValTT \text{ else } ValFF \]

We model environments simply as continuous functions from variable names to values.

\[ \text{type-synonym } Var = \var \]
\[ \text{type-synonym } 'a Env = Var \rightarrow 'a \]

\[ \text{definition } env-empty :: 'a Env \text{ where} \]

\[ env-empty \equiv \perp \]

\[ \text{definition } env-ext :: Var \rightarrow 'a \rightarrow 'a Env \rightarrow 'a Env \text{ where} \]

\[ env-ext \equiv \Lambda v x \var v'. \text{ if } v = v' \text{ then } x \text{ else } \var v' \]

The semantics is given by a function defined by primitive recursion over the syntax.

\[ \text{type-synonym } EnvD = ValD Env \]

\[ \text{primrec} \]
\[
evalD :: \text{expr} \Rightarrow \text{EnvD} \rightarrow \text{ValD}
\]

where
\[
\begin{align*}
\evalD (\text{Var } v) &= (\Lambda \varrho. \varrho \cdot v) \\
\evalD (\text{App } f \ x) &= (\Lambda \varrho. \text{appF} \cdot (\evalD f \cdot \varrho) \cdot (\evalD x \cdot \varrho)) \\
\evalD (\text{AbsN } v \ e) &= (\Lambda \varrho. \text{ValF} \cdot (\Lambda \varrho. \evalD e \cdot (\text{env-ext} \cdot v \cdot x \cdot \varrho))) \\
\evalD (\text{AbsV } v \ e) &= (\Lambda \varrho. \text{ValF} \cdot (\Lambda \varrho. \evalD e \cdot (\text{env-ext} \cdot v \cdot x \cdot \varrho))) \\
\evalD (\text{Fix } v \ e) &= (\Lambda \varrho. \mu x. \evalD e \cdot (\text{env-ext} \cdot v \cdot x \cdot \varrho)) \\
\evalD (\text{tt}) &= (\Lambda \varrho. \text{ValTT}) \\
\evalD (\text{ff}) &= (\Lambda \varrho. \text{ValFF}) \\
\evalD (\text{Cond } i \ t \ e) &= (\Lambda \varrho. (\text{cond} \cdot (\evalD i \cdot \varrho) \cdot (\evalD t \cdot \varrho) \cdot (\evalD e \cdot \varrho))) \\
\evalD (\text{Num } n) &= (\Lambda \varrho. \text{ValN} \cdot n) \\
\evalD (\text{Succ } e) &= (\Lambda \varrho. \text{succ} \cdot (\evalD e \cdot \varrho)) \\
\evalD (\text{Pred } e) &= (\Lambda \varrho. \text{pred} \cdot (\evalD e \cdot \varrho)) \\
\evalD (\text{IsZero } e) &= (\Lambda \varrho. \text{isZero} \cdot (\evalD e \cdot \varrho))
\end{align*}
\]

abbreviation \(\evalD' :: \text{expr} \Rightarrow \text{ValD} \text{ Env} \Rightarrow \text{ValD} \) where
\[
\evalD' M \varrho \equiv \evalD M \cdot \varrho
\]

3.2 The Y Combinator

We can shown the Y combinator is the least fixed point operator Using just the minimal invariant. In other words, fix is definable in untyped PCF minus the Fix construct.

This is Example 3.6 from Pitts (1996). He attributes the proof to Plotkin.

These two functions are \(\Delta \equiv \lambda f x. f (x x)\) and \(Y \equiv \lambda f. (\Delta f) (\Delta f)\).

Note the numbers here are names, not de Bruijn indices.

definition \(Y\delta :: \text{expr}\) where
\[
Y\delta \equiv \text{AbsN } 0 \ (\text{AbsN } 1 \ (\text{App } (\text{Var } 0) \ (\text{App } (\text{Var } 1) \ (\text{Var } 1))))
\]

definition \(Y\text{comb} :: \text{expr}\) where
\[
Y\text{comb} \equiv \text{AbsN } 0 \ (\text{App } (\text{App } Y\delta \ (\text{Var } 0)) \ (\text{App } Y\delta \ (\text{Var } 0)))
\]

definition \(\text{fixD} :: \text{ValD} \Rightarrow \text{ValD}\) where
\[
\text{fixD} \equiv \Lambda (\text{ValF} \cdot f). \text{fix } f
\]

lemma \(Y; [Y\text{comb}] \varrho = \text{ValF} \cdot \text{fixD}\)

3.3 Logical relations for definability

An element of \(\text{ValD}\) is definable if there is an expression that denotes it.

definition \(\text{definable} :: \text{ValD} \Rightarrow \text{bool}\) where
\[
\text{definable } d \equiv \exists M. [M] \text{ env-empty } = d
\]

A classical result about PCF is that while the denotational semantics is \textit{adequate}, as we show in §4, it is not \textit{fully abstract}, i.e. it contains undefinable values (junk).

One way of showing this is to reason operationally; see, for instance, Plotkin (1977, §4) and Gunter (1992, §6.1).

Another is to use \textit{logical relations}, following Plotkin (1973), and also Mitchell (1996); Sieber (1992); Stoughton (1993).
For this purpose we define a logical relation to be a set of vectors over \( \text{ValD} \) that is closed under continuous functions of type \( \text{ValD} \to \text{ValD} \). This is complicated by the \( \text{ValF} \) tag and having strict function abstraction.

**definition**

\[ \text{logical-relation} :: (\forall \cdot \text{type} \Rightarrow \text{ValD}) \text{ set} \Rightarrow \text{bool} \]

**where**

\[
\text{logical-relation } R \equiv \\
(\forall fs \in R. \forall xs \in R. (\lambda j. \text{appF}(fs \cdot j)(xs j)) \in R) \\
\land (\forall fs \in R. \forall xs \in R. (\lambda j. \text{strictify}(\text{appF}(fs \cdot j))(xs j)) \in R) \\
\land (\forall fs. (\forall xs \in R. (\lambda j. (fs \cdot j)(xs j)) \in R) \implies (\lambda j. \text{ValF}(fs \cdot j)) \in R) \\
\land (\forall fs. (\forall xs \in R. (\lambda j. \text{strictify}(fs \cdot j)(xs j)) \in R) \implies (\lambda j. \text{ValF}(\text{strictify}(fs \cdot j))) \in R) \\
\land (\forall xs \in R. (\lambda j. \text{fixD}(xs j)) \in R) \\
\land (\forall cs \in R. \forall ts \in R. \forall es \in R. (\lambda j. \text{cond}(cs j)(ts j)(es j)) \in R) \\
\land (\forall xs \in R. (\lambda j. \text{succ}(xs j)) \in R) \\
\land (\forall xs \in R. (\lambda j. \text{pred}(xs j)) \in R) \\
\land (\forall xs \in R. (\lambda j. \text{isZero}(xs j)) \in R)
\]

In the context of PCF these relations also need to respect the constants.

**definition**

\[ \text{PCF-consts-rel} :: (\forall \cdot \text{type} \Rightarrow \text{ValD}) \text{ set} \Rightarrow \text{bool} \]

**where**

\[
\text{PCF-consts-rel } R \equiv \\
(\forall i. \text{ValTT}) \in R \\
(\forall i. \text{ValFF}) \in R \\
(\forall n. (\lambda i. \text{ValN} \cdot n) \in R)
\]

**abbreviation**

\[ \text{PCF-ir} R \equiv \text{adm} (\lambda x. x \in R) \land \text{logical-relation } R \land \text{PCF-consts-rel } R \]

The fundamental property of logical relations states that all PCF expressions satisfy all PCF logical relations. This result is essentially due to Plotkin (1973). The proof is by a straightforward induction on the expression \( M \).

**lemma** lr-fundamental:

**assumes** lr: PCF-ir R

**assumes** \( g \): \( \forall v. (\lambda i. g \cdot i v) \in R \)

**shows** (\( \lambda i. \llbracket M \rrbracket(\llbracket g \cdot i \rrbracket) \in R \)

We can use this result to show that there is no PCF term that maps the vector \( \text{args} \in R \) to \( \text{result} \notin R \) for some logical relation \( R \). If we further show that there is a function \( f \) in \( \text{ValD} \) such that \( f \cdot \text{args} = \text{result} \) then we can conclude that \( f \) is not definable.

**abbreviation**

\[ \text{appFLv} :: \text{ValD} \Rightarrow (\forall \cdot \text{type} \Rightarrow \text{ValD}) \text{ list} \Rightarrow (\forall \cdot \text{ValD}) \]

**where**

\[
\text{appFLv } f \cdot \text{args} \equiv (\lambda i. \text{foldl} (\lambda x. \text{appF}(f \cdot (x i)) \cdot \text{args})
\]

**lemma** lr-appFLv:

**assumes** lr: logical-relation R

**assumes** \( f \): (\( \lambda i: \forall \cdot \text{type} \cdot f \)) \in R

**assumes** \( \text{args} \): \text{set} \ \text{args} \subseteq R

**shows** \( \text{appFLv } f \cdot \text{args} \in R \)
corollary not-definable:

fixes $R :: ('i::{type} \Rightarrow \text{ValD}) \text{ set}$
fixes $\text{args} :: ('i \Rightarrow \text{ValD}) \text{ list}$
fixes $\text{result} :: 'i \Rightarrow \text{ValD}$
assumes $lr: \text{PCF-lr } R$
assumes $\text{args}: \text{set } \text{args} \subseteq R$
assumes $\text{result}: \text{result} \notin R$
shows $\neg (\exists (f::\text{ValD}). \text{ definable } f \land \text{appFLv } f \text{ args } = \text{result})$

3.4 Parallel OR is not definable

We show that parallel-or is not $\lambda$-definable following Sieber (1992) and Stoughton (1993).
Parallel-or is similar to lazy-or except that if the first argument is $\perp$ and the second one is $\text{ValTT}$, we get $\text{ValTT}$ (and not $\perp$). It is continuous and hence included in the $\text{ValD}$ domain.

definition $\text{por} :: \text{ValD} \Rightarrow \text{ValD} \Rightarrow \text{ValD}$ (- $\text{por}$ - [31,30] 30) where
$x \text{ por } y \equiv$
if $x = \text{ValTT}$ then $\text{ValTT}$
else if $y = \text{ValTT}$ then $\text{ValTT}$
else if $(x = \text{ValFF} \land y = \text{ValFF})$ then $\text{ValFF}$ else $\perp$

The defining properties of parallel-or.

lemma $\text{POR-simps}$ [simp]:
$(\text{ValTT por } y) = \text{ValTT}$
$(x \text{ por } \text{ValTT}) = \text{ValTT}$
$(\text{ValFF por } \text{ValFF}) = \text{ValFF}$
$(\text{ValFF por } \perp) = \perp$
$(\text{ValFF por } \text{ValN} \cdot n) = \perp$
$(\text{ValFF por } \text{ValF} \cdot f) = \perp$
$(\perp \text{ por } \text{ValFF}) = \perp$
$(\text{ValN} \cdot n \text{ por } \text{ValFF}) = \perp$
$(\text{ValF} \cdot f \text{ por } \text{ValFF}) = \perp$
$(\perp \text{ por } \perp) = \perp$
$(\perp \text{ por } \text{ValN} \cdot n) = \perp$
$(\perp \text{ por } \text{ValF} \cdot f) = \perp$
$(\text{ValN} \cdot n \text{ por } \perp) = \perp$
$(\text{ValF} \cdot f \text{ por } \perp) = \perp$
$(\text{ValN} \cdot m \text{ por } \text{ValN} \cdot n) = \perp$
$(\text{ValN} \cdot n \text{ por } \text{ValF} \cdot f) = \perp$
$(\text{ValF} \cdot f \text{ por } \text{ValN} \cdot n) = \perp$
$(\text{ValF} \cdot f \text{ por } \text{ValF} \cdot g) = \perp$

unfolding $\text{por-def}$ by $\text{simp-all}$

We need three-element vectors.

datatype $\text{Three} = \text{One} \mid \text{Two} \mid \text{Three}$

The standard logical relation $R$ that demonstrates POR is not definable is:

$$(x, y, z) \in R \text{ iff } x = y = z \lor (x = \perp \lor y = \perp)$$

That POR satisfies this relation can be seen from its truth table (see below).
Note we restrict the $x = y = z$ clause to non-function values. Adding functions breaks the “logical relations” property.
definition
POR-base-lf-rep :: (Three ⇒ ValD) lf-rep
where
POR-base-lf-rep ≡ λ(mR, pR).
{ (λi. ValTT) } ∪ { (λi. ValFF) } (* x = y = z for bools *) ∪ (∪ n. { (λi. ValN·n) }) (* x = y = z for numerals *) ∪ { f . f One = ⊥ } (* x = ⊥ *) ∪ { f . f Two = ⊥ } (* y = ⊥ *)

We close this relation with respect to continuous functions. This functor yields an admissible relation for all r and is monotonic.

definition fn-lf-rep :: (i::type ⇒ ValD) lf-rep
where
fn-lf-rep ≡ λ(mR, pR).
{ λi. ValF·(fs i) | fs. ∀ xs ∈ unlr (undual mR). (λj. (fs j)·(xs j)) ∈ unlr pR }

definition POR-lf-rep :: (Three ⇒ ValD) lf-rep where
POR-lf-rep R ≡ POR-base-lf-rep R ∪ fn-lf-rep R

abbreviation POR-lf ≡ λ r. mklr (POR-lf-rep r)

Again it yields an admissible relation and is monotonic. We need to show the functor respects the minimal invariant.

lemma min-inv-POR-lf:
assumes eRSV e R
shows eRSV (ValD-copy-rec·e) (dual (POR-lf (dual S, undual R))) (POR-lf (R', S'))

We can show that the solution satisfies the expectations of the fundamental theorem lr-fundamental.

lemma PCF-lr-POR-delta: PCF-lr (unlr POR·delta)

This is the truth-table for POR rendered as a vector: we seek a function that simultaneously maps the two argument vectors to the result.

definition POR-arg1-rel where
POR-arg1-rel ≡ λ i. case i of One ⇒ ValTT | Two ⇒ ⊥ | Three ⇒ ValFF

definition POR-arg2-rel where
POR-arg2-rel ≡ λ i. case i of One ⇒ ⊥ | Two ⇒ ValTT | Three ⇒ ValFF

definition POR-result-rel where
POR-result-rel ≡ λ i. case i of One ⇒ ValTT | Two ⇒ ValTT | Three ⇒ ValFF

lemma lr-POR-arg1-rel: POR-arg1-rel ∈ unlr POR·delta
unfolding POR-arg1-rel-def by auto

lemma lr-POR-arg2-rel: POR-arg2-rel ∈ unlr POR·delta
unfolding POR-arg2-rel-def by auto

lemma lr-POR-result-rel: POR-result-rel ∉ unlr POR·delta

Parallel-or satisfies these tests:
theorem POR-sat:
  appFLv (ValF · (λ x. ValF · (λ y. x por y))) [POR-arg1-rel, POR-arg2-rel] = POR-result-rel
unfolding POR-arg1-rel-def POR-arg2-rel-def POR-result-rel-def
by (simp add: fun-eq-iff split: Three.splits)

... but is not PCF-definable:

theorem POR-is-not-definable:
  shows ¬(∃ f. definable f ∧ appFLv f [POR-arg1-rel, POR-arg2-rel] = POR-result-rel)
apply (rule not-definable[where R=unlr POR.delta])
  using lr-POR-arg1-rel lr-POR-arg2-rel lr-POR-result-rel PCF-lr-POR-delta
apply simp-all
done

3.5 Plotkin’s existential quantifier

We can also show that the existential quantifier of Plotkin (1977, §5) is not PCF-definable
using logical relations.

Our definition is quite loose; if the argument function f maps any value to ValTT then
plotkin-exists yields ValTT. It may be more plausible to test f on numerals only.

definition plotkin-exists :: ValD ⇒ ValD where
  plotkin-exists f ≡
  if (appF · f · ⊥ = ValFF)
    then ValFF
  else if (∃ n. appF · f · n = ValTT) then ValTT else ⊥

We can show this function is continuous.

lemma cont-pe [cont2cont, simp]: cont plotkin-exists

Again we construct argument and result test vectors such that plotkin-exists satisfies these
tests but no PCF-definable term does.

definition PE-arg-rel where
  PE-arg-rel ≡ λ i. ValF · (case i of
    0 ⇒ (Λ _. ValFF)
    Suc n ⇒ (Λ (ValN · x). if x = Suc n then ValTT else ⊥))

definition PE-result-rel where
  PE-result-rel ≡ λ i. case i of 0 ⇒ ValFF | Suc n ⇒ ValTT

Note that unlike the POR case the argument relation does not characterise PE: we don’t treat
functions that return ValTTs and ValFFs.

The Plotkin existential satisfies these tests:

theorem pe-sat:
  appFLv (ValF · (λ x. plotkin-exists x)) [PE-arg-rel] = PE-result-rel
unfolding PE-arg-rel-def PE-result-rel-def
by (clarsimp simp: fun-eq-iff split: nat.splits)

As for POR, the difference between the two vectors is that the argument can diverge but not
the result.

definition PE-base-lf-rep :: (nat ⇒ ValD) lf-rep where

11
$PE$-base-lf-rep $\equiv \lambda (mR, pR)$.
\[
\{ \bot \} \cup \{ (\lambda i. \ValTT) \} \cup \{ (\lambda i. \ValFF) \} (\ast x = y = z \text{ for boods } \ast)
\cup (\bigcup n. \{ (\lambda i. \ValN \cdot n) \}) (\ast x = y = z \text{ for numerals } \ast)
\cup \{ f . f 1 = \bot \lor f 2 = \bot \} (\ast \text{ Vectors that diverge on one or two. } \ast)
\]

Again we close this under the function space, and show that it is admissible, monotonic and respects the minimal invariant.

definition $PE$-lf-rep :: (nat $\Rightarrow$ ValD) if-rep where
$PE$-lf-rep $R$ $\equiv$ $PE$-base-lf-rep $R$ $\cup$ fn-lf-rep $R$

abbreviation $PE$-lf $\equiv \lambda r. mklr (PE$-lf-rep $r)$

The solution satisfies the expectations of the fundamental theorem:

lemma $PCF$-lr-$PE$-delta: $PCF$-lr (unlr $PE$-delta)

lemma lr-$PE$-arg-rel: $PE$-arg-rel $\in$ unlr $PE$-delta

lemma lr-$PE$-result-rel: $PE$-result-rel $\notin$ unlr $PE$-delta

theorem $PE$-is-not-definable: $\neg (\exists f. \text{ definable } f \land \text{appFLv } f [PE$-arg-rel] = PE$-result-rel)

3.6 Concluding remarks

These techniques could be used to show that Haskell’s $\text{seq}$ operation is not $PCF$-definable. (It is definable for each base “type” separately, and requires some care on function values.) If we added an (unlifted) product type then it should be provable that parallel evaluation is required to support $\text{seq}$ on these objects (given $\text{seq}$ on all other objects). (See Hudak et al. (2007, §5.4) and sundry posts to the internet by Lennart Augustsson.) This may be difficult to do plausibly without adding a type system.

4 Logical relations for computational adequacy

We relate the denotational semantics for $PCF$ of §3.1 to a big-step (or natural) operational semantics. This follows Pitts (1993).

4.1 Direct semantics using de Bruijn notation

In contrast to §3 we must be more careful in our treatment of $\alpha$-equivalent terms, as we would like our operational semantics to identify of all these. To that end we adopt de Bruijn notation, adapting the work of Nipkow (2001), and show that it is suitably equivalent to our original syntactic story.

datatype $db =$

| $DBVar$ var |
| $DBApp$ db db |
| $DBAbsN$ db |
| $DBAbsV$ db |
| $DBDiverge$ |
| $DBFix$ db |
| $DBtt$ |
| $DBff$ |
Nipkow et al.'s substitution operation is defined for arbitrary open terms. In our case we only substitute closed terms into terms where only the variable $\theta::'a$ may be free, and while we could develop a simpler account, we retain the traditional one.

**fun**

\[
\text{lif} :: \db \Rightarrow \nat \Rightarrow \db
\]
**where**

\[
\begin{align*}
\text{lif} \ (\text{DBVar} \ i) \ k & = \text{DBVar} \ (\text{if} \ i < k \ \text{then} \ i \ \text{else} \ (i + 1)) \\
\text{lif} \ (\text{DBAbsN} \ s) \ k & = \text{DBAbsN} \ (\text{lif} \ s \ (k + 1)) \\
\text{lif} \ (\text{DBAbsV} \ s) \ k & = \text{DBAbsV} \ (\text{lif} \ s \ (k + 1)) \\
\text{lif} \ (\text{DBApp} \ s \ t) \ k & = \text{DBApp} \ (\text{lif} \ s \ k) \ (\text{lif} \ t \ k) \\
\text{lif} \ (\text{DBFix} \ e) \ k & = \text{DBFix} \ (\text{lif} \ e \ (k + 1)) \\
\text{lif} \ (\text{DBCond} \ c \ t \ e) \ k & = \text{DBCond} \ (\text{lif} \ c \ k) \ (\text{lif} \ t \ k) \ (\text{lif} \ e \ k) \\
\text{lif} \ (\text{DBSucc} \ e) \ k & = \text{DBSucc} \ (\text{lif} \ e \ k) \\
\text{lif} \ (\text{DBPred} \ e) \ k & = \text{DBPred} \ (\text{lif} \ e \ k) \\
\text{lif} \ (\text{DBIsZero} \ e) \ k & = \text{DBIsZero} \ (\text{lif} \ e \ k) \\
\text{lif} \ x \ k & = x
\end{align*}
\]

**fun**

\[
\text{subst} :: \db \Rightarrow \db \Rightarrow \text{var} \Rightarrow \db \ (\Rightarrow \Rightarrow \ [300, \ 0, \ 0] \ 300)
\]
**where**

\[
\begin{align*}
\text{subst-Var} \ (\text{DBVar} \ i)<s/k> & = \\
& \ (\text{if} \ k < i \ \text{then} \ \text{DBVar} \ (i - 1) \ \text{else} \ if \ i = k \ \text{then} \ s \ \text{else} \ \text{DBVar} \ i) \\
\text{subst-AbsN} \ (\text{DBAbsN} \ t)<s/k> & = \text{DBAbsN} \ (t<\text{lif} \ s \ 0 / k + 1>) \\
\text{subst-AbsV} \ (\text{DBAbsV} \ t)<s/k> & = \text{DBAbsV} \ (t<\text{lif} \ s \ 0 / k + 1>) \\
\text{subst-App} \ (\text{DBApp} \ t \ u)<s/k> & = \text{DBApp} \ (t<s/k>) \ (u<s/k>) \\
\text{DBFix} \ e<s/k> & = \text{DBFix} \ (e<\text{lif} \ s \ 0 / k + 1>) \\
\text{DBCond} \ c \ t \ e<s/k> & = \text{DBCond} \ (c<s/k>) \ (t<s/k>) \ (e<s/k>) \\
\text{DBSucc} \ e<s/k> & = \text{DBSucc} \ (e<s/k>) \\
\text{DBPred} \ e<s/k> & = \text{DBPred} \ (e<s/k>) \\
\text{DBIsZero} \ e<s/k> & = \text{DBIsZero} \ (e<s/k>) \\
\text{subst-Consts} \ x<s/k> & = x
\end{align*}
\]

We elide the standard lemmas about these operations.

A variable is free in a de Bruijn term in the standard way.

**fun**

\[
\text{freedb} :: \db \Rightarrow \text{var} \Rightarrow \text{bool}
\]
**where**

\[
\begin{align*}
\text{freedb} \ (\text{DBVar} \ j) \ k & = (j = k) \\
\text{freedb} \ (\text{DBAbsN} \ s) \ k & = \text{freedb} \ s \ (k + 1) \\
\text{freedb} \ (\text{DBAbsV} \ s) \ k & = \text{freedb} \ s \ (k + 1) \\
\text{freedb} \ (\text{DBApp} \ s \ t) \ k & = (\text{freedb} \ s \ k \ \text{\vee} \ \text{freedb} \ t \ k) \\
\text{freedb} \ (\text{DBFix} \ e) \ k & = \text{freedb} \ e \ (\text{Suc} \ k) \\
\text{freedb} \ (\text{DBCond} \ c \ t \ e) \ k & = (\text{freedb} \ c \ k \ \text{\vee} \ \text{freedb} \ t \ k \ \text{\vee} \ \text{freedb} \ e \ k) \\
\text{freedb} \ (\text{DBSucc} \ e) \ k & = \text{freedb} \ e \ k \\
\text{freedb} \ (\text{DBPred} \ e) \ k & = \text{freedb} \ e \ k \\
\text{freedb} \ (\text{DBIsZero} \ e) \ k & = \text{freedb} \ e \ k
\end{align*}
\]
Programs are closed expressions.

**definition closed :: db ⇒ bool where**

\[ \text{closed } e \equiv \forall i. \neg \text{freedb } e \, i \]

The direct denotational semantics is almost identical to that given in §3.1, apart from this change in the representation of environments.

**definition env-empty-db :: 'a Env where**

\[ \text{env-empty-db } \equiv \perp \]

**definition env-ext-db :: 'a → 'a Env → 'a Env where**

\[ \text{env-ext-db } \equiv \Lambda x \, \rho \, v. (\text{case } v \text{ of } 0 \Rightarrow x \mid \text{Suc } v' \Rightarrow \rho \cdot v') \]

**primrec evalDdb :: db ⇒ ValD Env → ValD where**

\[
\begin{align*}
\text{evalDdb } (DBVar i) & = (\Lambda \rho. \rho \cdot i) \\
\text{evalDdb } (DBApp f x) & = (\Lambda \rho. \text{appF} \cdot (\text{evalDdb } f \cdot \rho) \cdot (\text{evalDdb } x \cdot \rho)) \\
\text{evalDdb } (DBAbsN e) & = (\Lambda \rho. \text{ValF} \cdot (\Lambda x. \text{evalDdb } e \cdot (\text{env-ext-db } x \cdot \rho))) \\
\text{evalDdb } (DBAbsV e) & = (\Lambda \rho. \text{ValF} \cdot (\Lambda x. \text{evalDdb } e \cdot (\text{env-ext-db } x \cdot \rho))) \\
\text{evalDdb } (DBDiverge) & = (\Lambda \rho. \perp) \\
\text{evalDdb } (DBFix e) & = (\Lambda \rho. \mu x. \text{evalDdb } e \cdot (\text{env-ext-db } x \cdot \rho)) \\
\text{evalDdb } (DBtt) & = (\Lambda \rho. \text{ValTT}) \\
\text{evalDdb } (DBff) & = (\Lambda \rho. \text{ValFF}) \\
\text{evalDdb } (DBCond c t e) & = (\Lambda \rho. \text{cond} \cdot (\text{evalDdb } c \cdot \rho) \cdot (\text{evalDdb } t \cdot \rho) \cdot (\text{evalDdb } e \cdot \rho)) \\
\text{evalDdb } (DBNum n) & = (\Lambda \rho. \text{ValN} \cdot n) \\
\text{evalDdb } (DBSucc e) & = (\Lambda \rho. \text{succ} \cdot (\text{evalDdb } e \cdot \rho)) \\
\text{evalDdb } (DBPred e) & = (\Lambda \rho. \text{pred} \cdot (\text{evalDdb } e \cdot \rho)) \\
\text{evalDdb } (DBIsZero e) & = (\Lambda \rho. \text{isZero} \cdot (\text{evalDdb } e \cdot \rho)) \\
\end{align*}
\]

We show that our direct semantics using de Bruijn notation coincides with the evaluator of §3 by translating between the syntaxes and showing that the evaluators yield identical results.

Firstly we show how to translate an expression using names into a nameless term. The following function finds the first mention of a variable in a list of variables.

**primrec index :: var list ⇒ var ⇒ nat ⇒ nat where**

\[
\begin{align*}
\text{index } [] \, v \, n & = n \\
\text{index } (h \# t) \, v \, n & = (i f v = h \text{ then } n \text{ else } \text{index } t \, v \, (\text{Suc } n))
\end{align*}
\]

**primrec transdb :: expr ⇒ var list ⇒ db where**

\[
\begin{align*}
\text{transdb } (Var i) \, \Gamma & = DBVar \, (\text{index } \Gamma \, i \, 0) \\
\text{transdb } (App \, t1 \, t2) \, \Gamma & = DBApp \, (\text{transdb } t1 \, \Gamma) \cdot (\text{transdb } t2 \, \Gamma) \\
\text{transdb } (AbsN \, v \, t) \, \Gamma & = DBAbsN \, (\text{transdb } t \, (v \# \Gamma)) \\
\text{transdb } (AbsV \, v \, t) \, \Gamma & = DBAbsV \, (\text{transdb } t \, (v \# \Gamma)) \\
\text{transdb } (Diverge) \, \Gamma & = DBDiverge \\
\text{transdb } (Fix \, v \, e) \, \Gamma & = DBFix \, (\text{transdb } e \, (v \# \Gamma)) \\
\text{transdb } (tt) \, \Gamma & = DBtt \\
\text{transdb } (ff) \, \Gamma & = DBff \\
\text{transdb } (Cond \, c \, t \, e) \, \Gamma & = DBCond \, (\text{transdb } t \, \Gamma) \cdot (\text{transdb } e \, \Gamma)
\end{align*}
\]
This semantics corresponds with the direct semantics for named expressions.

**Lemma evalD-evalDdb:**

- **Assumes** free \(e\) = []
- **Shows** \(\llbracket e \rrbracket \varrho = \text{evalDdb}(\text{transdb e} [] \varrho)\)
- **Using assms by** (simp add: evalD-evalDdb-open)

Conversely, all de Bruijn expressions have named equivalents.

**Primrec**

\[
\begin{align*}
\text{transdb-inv} :: \text{db} & \Rightarrow (\text{var} \Rightarrow \text{var}) \Rightarrow \text{var} \Rightarrow \text{var} \Rightarrow \text{expr} \\
\text{where} & \\
\text{transdb-inv} (\text{DBVar i}) \Gamma c k & = \text{Var} (\Gamma i) \\
\text{transdb-inv} (\text{DBApp t1 t2}) \Gamma c k & = \text{App} (\text{transdb-inv} t1 \Gamma c k) (\text{transdb-inv} t2 \Gamma c k) \\
\text{transdb-inv} (\text{DBAbsN e}) \Gamma c k & = \text{AbsN} (c + k) (\text{transdb-inv} e (\text{case-nat} (c + k) \Gamma) c (k + 1)) \\
\text{transdb-inv} (\text{DBAbsV e}) \Gamma c k & = \text{AbsV} (c + k) (\text{transdb-inv} e (\text{case-nat} (c + k) \Gamma) c (k + 1)) \\
\text{transdb-inv} (\text{DBDiverge}) \Gamma c k & = \text{Diverge} \\
\text{transdb-inv} (\text{DBFix e}) \Gamma c k & = \text{Fix} (c + k) (\text{transdb-inv} e (\text{case-nat} (c + k) \Gamma) c (k + 1)) \\
\text{transdb-inv} (\text{DBtt}) \Gamma c k & = \text{tt} \\
\text{transdb-inv} (\text{DBff}) \Gamma c k & = \text{ff} \\
\text{transdb-inv} (\text{DBCond i t e}) \Gamma c k & = \\
\text{Cond} (\text{transdb-inv} i \Gamma c k) (\text{transdb-inv} t \Gamma c k) (\text{transdb-inv} e \Gamma c k) \\
\text{transdb-inv} (\text{DBNum n}) \Gamma c k & = (\text{Num n}) \\
\text{transdb-inv} (\text{DBSucc e}) \Gamma c k & = \text{Succ} (\text{transdb-inv} e \Gamma c k) \\
\text{transdb-inv} (\text{DBPred e}) \Gamma c k & = \text{Pred} (\text{transdb-inv} e \Gamma c k) \\
\text{transdb-inv} (\text{DBIsZero e}) \Gamma c k & = \text{IsZero} (\text{transdb-inv} e \Gamma c k)
\end{align*}
\]

**Lemma transdb-inv:**

- **Assumes** closed \(e\)
- **Shows** \(\text{transdb} (\text{transdb-inv} e \Gamma c k) \Gamma' = e\)

### 4.2 Operational Semantics

The evaluation relation (big-step, or natural operational semantics). This is similar to Gunter (1992, §6.2), Pitts (1993) and Winskel (1993, Chapter 11).

We firstly define the **values** that expressions can evaluate to: these are either constants or closed abstractions.

**Inductive**

\[
\begin{align*}
\text{val} :: \text{db} & \Rightarrow \text{bool} \\
\text{where} & \\
\text{v-Num}[\text{intro}]: & \text{val} (\text{DBNum n}) \\
\text{v-FF}[\text{intro}]: & \text{val} \text{DBff} \\
\text{v-TT}[\text{intro}]: & \text{val} \text{DBtt} \\
\text{v-AbsN}[\text{intro}]: & \text{closed} (\text{DBAbsN e}) \Rightarrow \text{val} (\text{DBAbsN e}) \\
\text{v-AbsV}[\text{intro}]: & \text{closed} (\text{DBAbsV e}) \Rightarrow \text{val} (\text{DBAbsV e})
\end{align*}
\]

**Inductive**

\[
\begin{align*}
\text{evalOP} :: \text{db} & \Rightarrow \text{db} \Rightarrow \text{bool} (- \updownarrow - [50,50] 50)
\end{align*}
\]
where

\begin{align*}
\text{evalOP-AppN}[\text{intro}]: & \quad [ P \Downarrow DBAbsN M; M < Q/0 > \Downarrow V ] \implies DBApp P Q \Downarrow V \\
\text{evalOP-AppV}[\text{intro}]: & \quad [ P \Downarrow DBAbsV M; Q \Downarrow q; M < q/0 > \Downarrow V ] \implies DBApp P Q \Downarrow V \\
\text{evalOP-AbsN}[\text{intro}]: & \quad \text{val} (DBAbsN e) \implies DBAbsN e \Downarrow DBAbsN e \\
\text{evalOP-AbsV}[\text{intro}]: & \quad \text{val} (DBAbsV e) \implies DBAbsV e \Downarrow DBAbsV e \\
\text{evalOP-Fix}[\text{intro}]: & \quad P < DBFix P/0 > \Downarrow V \implies DBFix P \Downarrow V \\
\text{evalOP-tt}[\text{intro}]: & \quad DBtt \Downarrow DBtt \\
\text{evalOP-ff}[\text{intro}]: & \quad DBff \Downarrow DBff \\
\text{evalOP-CondTT}[\text{intro}]: & \quad [ C \Downarrow DBtt; T \Downarrow V ] \implies DBCond C T E \Downarrow V \\
\text{evalOP-CondFF}[\text{intro}]: & \quad [ C \Downarrow DBff; E \Downarrow V ] \implies DBCond C T E \Downarrow V \\
\text{evalOP-Num}[\text{intro}]: & \quad DBNum n \Downarrow DBNum n \\
\text{evalOP-Succ}[\text{intro}]: & \quad P \Downarrow DBNum n \implies DBSucc P \Downarrow DBNum (Suc n) \\
\text{evalOP-Pred}[\text{intro}]: & \quad P \Downarrow DBNum (Suc n) \implies DBPred P \Downarrow DBNum n \\
\text{evalOP-IsZeroTT}[\text{intro}]: & \quad [ E \Downarrow DBNum 0 ] \implies DBIsZero E \Downarrow DBtt \\
\text{evalOP-IsZeroFF}[\text{intro}]: & \quad [ E \Downarrow DBNum n; 0 < n ] \implies DBIsZero E \Downarrow DBff
\end{align*}

It is straightforward to show that this relation is deterministic and sound with respect to the denotational semantics.

**Lemma evalOP-sound:**

\begin{align*}
\text{assumes} & \quad P \Downarrow V \\
\text{shows} & \quad evalDdb P \varrho = evalDdb V \varrho
\end{align*}

We can use soundness to conclude that POR is not definable operationally either. We rely on transdb-inv to map our de Bruijn term into the syntactic universe of §3 and appeal to the results of §3.4. This takes some effort as ValD contains irrelevant junk that makes it hard to draw obvious conclusions; we use DBCond to restrict the arguments to the putative witness.

**Definition**

\begin{align*}
\text{isPORdb e} & \equiv \text{closed e} \\
& \land DBApp (DBApp e DBtt) DBDiverge \Downarrow DBtt \\
& \land DBApp (DBApp e DBDiverge) DBtt \Downarrow DBtt \\
& \land DBApp (DBApp e DBff) DBff \Downarrow DBff
\end{align*}

**Lemma** POR-is-not-operationally-definable: $\neg \text{isPORdb e}$

### 4.3 Computational Adequacy

The lemma evalOP-sound tells us that the operational semantics preserves the denotational semantics. We might also hope that the two are somehow equivalent, but due to the junk in the domain-theoretic model (see §3.3) we cannot expect this to be entirely straightforward. Here we show that the denotational semantics is computationally adequate, which means that it can be used to soundly reason about contextual equivalence.

We follow Pitts (1993, 1996) by defining a suitable logical relation between our ValD domain and the set of programs (closed terms). These are termed "formal approximation relations" by Plotkin. The machinery of §2.2 requires us to define a unique bottom element, which in this case is $\{ \bot \} \times \{ P. \text{closed P} \}$. To that end we define the type of programs.

**typedef**

\begin{align*}
\text{Prog} & = \{ P. \text{closed P} \} \\
\text{morphisms} & \text{unProg mkProg by fastforce}
\end{align*}

**Definition**

\begin{align*}
\text{ca-lf-rep} & :: (\text{ValD, Prog}) \rightarrow \text{synlf-rep}
\end{align*}
The key lemma is shown by induction over \( \Gamma \).

We can show it has the expected properties when all terms in \( \Gamma \) are closed.

\[ \text{definition ca-lr-syn} \equiv \lambda (\text{rm}, \text{rp}). \]

\[ \text{interpretation ca-lr} \equiv \lambda r. \text{mksynlr} (\text{ca-lf-rep} r) \]

Intuitively we relate domain-theoretic values to all programs that converge to the corresponding syntactic values. If a program has a non-\( \perp \) denotation then we can use this relation to conclude something about the value it (operationally) converges to.

\[ \text{fun closing-subst} :: \text{db} \Rightarrow (\text{var} \Rightarrow \text{db}) \Rightarrow \text{var} \Rightarrow \text{db} \]

We can show it has the expected properties when all terms in \( \Gamma \) are closed.
lemma **ca-open:**
assumes $\forall v. \text{freedb } v \rightarrow g \cdot v \bowtie \Gamma v \land \text{closed } (\Gamma v)$
shows $\text{evalDdb } e \cdot g \bowtie \text{closing-subst } e \cdot \Gamma 0$

lemma **ca-closed:**
assumes $\text{closed } e$
shows $\text{evalDdb } e \cdot \text{env-empty-db} \bowtie e$
using **ca-open**[where $e = e$ and $g = \text{env-empty-db}$] assms
by (simp add: closed-def)

theorem **ca:**
assumes $\text{nb}: \text{evalDdb } e \cdot \text{env-empty-db} \neq \bot$
assumes $\text{closed } e$
shows $\exists V. e \downarrow V$
using **ca-closed**[OF (closed $e$)] nb
by (auto elim!: ca-lrE)

This last result justifies reasoning about contextual equivalence using the denotational semantics, as we now show.

### 4.3.1 Contextual Equivalence

As we are using an un(i)typed language, we take a context $C$ to be an arbitrary term, where the free variables are the “holes”. We substitute a closed expression $e$ uniformly for all of the free variables in $C$. If open, the term $e$ can be closed using enough $\text{AbsNs}$. This seems to be a standard trick now, see e.g. Koutavas and Wand (2006). If we didn’t have CBN (only CBV) then it might be worth showing that this is an adequate treatment.

**definition** **ctxt-sub** :: $db \Rightarrow db \Rightarrow db$ ((-<->) [300, 0] 300) where
$C < e > \equiv \text{closing-subst } C (\lambda - e) 0$

Following Pitts (1996) we define a relation between values that “have the same form”. This is weak at functional values. We don’t distinguish between strict and non-strict abstractions.

**inductive**

**have-the-same-form** :: $db \Rightarrow db \Rightarrow bool$ ($\sim$ - [50,50] 50)
where
$\text{DBAbsN } e \sim \text{DBAbsN } e'$
$\text{DBAbsN } e \sim \text{DBAbsV } e'$
$\text{DBAbsV } e \sim \text{DBAbsN } e'$
$\text{DBAbsV } e \sim \text{DBAbsV } e'$
$\text{DBFix } e \sim \text{DBFix } e'$
$\text{DBtt} \sim \text{DBtt}$
$\text{DBff} \sim \text{DBff}$
$\text{DBNum } n \sim \text{DBNum } n$

A program $e2$ refines the program $e1$ if it converges in context at least as often. This is a preorder on programs.

**definition**

**refines** :: $db \Rightarrow db \Rightarrow bool$ ($\leq$ - [50,50] 50)
where $e1 \leq e2 \equiv \forall C. \exists V1. C < e1 > \downarrow V1 \rightarrow (\exists V2. C < e2 > \downarrow V2 \land V1 \sim V2)$
Contextually-equivalent programs refine each other.

**definition**

\[ \text{contextually-equivalent :: } db \Rightarrow db \Rightarrow \text{bool} \ (\sim \sim) \]

**where**

\[ e_1 \approx e_2 \equiv e_1 \subseteq e_2 \land e_2 \subseteq e_1 \]

Our ultimate theorem states that if two programs have the same denotation then they are contextually equivalent.

**theorem computational-adequacy:**

**assumes** 1: closed \( e_1 \)

**assumes** 2: closed \( e_2 \)

**assumes** \( D: \text{evalDdb } e_1 \cdot \text{env-empty-db} = \text{evalDdb } e_2 \cdot \text{env-empty-db} \)

**shows** \( e_1 \approx e_2 \)

This gives us a sound but incomplete method for demonstrating contextual equivalence. We expect this result is useful for showing contextual equivalence for typed programs as well, but leave it to future work to demonstrate this.

See Gunter (1992, §6.2) for further discussion of computational adequacy at higher types.

The reader may wonder why we did not use Nominal syntax to define our operational semantics, following Urban and Narboux (2009). The reason is that Nominal2 does not support the definition of continuous functions over Nominal syntax, which is required by the evaluators of §3 and §4.1. As observed above, in the setting of traditional programming language semantics one can get by with a much simpler notion of substitution than is needed for investigations into \( \lambda \)-calculi. Clearly this does not hold of languages that reduce “under binders”.

The “fast and loose reasoning is morally correct” work of Danielsson et al. (2006) can be seen as a kind of adequacy result.

Benton et al. (2009b) demonstrate a similar computational adequacy result in Coq. However their system is only geared up for this kind of metatheory, and not reasoning about particular programs; its term language is combinatorial.

Benton et al. (2007, 2009a) have shown that it is difficult to scale this domain-theoretic approach up to richer languages, such as those with dynamic allocation of mutable references, especially if these references can contain (arbitrary) functional values.

5 Relating direct and continuation semantics

This is a fairly literal version of Reynolds (1974), adapted to untyped PCF. A more abstract account has been given by Filinski (2007) in terms of a monadic meta language, which is difficult to model in Isabelle (but see Huffman (2012a)).

We begin by giving PCF a continuation semantics following the modern account of Wadler (1992). We use the symmetric function space \((′a \text{ ValK}, ′o) K \rightarrow (′o \text{ ValK}, ′o) K\) as our language includes call-by-name.

**type-synonym** \((′a, ′o) K = (′a \rightarrow ′o) \rightarrow ′o\)

**domain** ′o ValK

\[ = \text{ValK}F \] (lazy appKF :: (′o ValK, ′o) K \rightarrow (′o ValK, ′o) K)

| ValKTT | ValKFF |
To establish the chain completeness (admissibility) of our logical relation, we need to show

where

\[ \text{type-synonym} \ 'o \ ValKM = (\ 'o \ ValK, \ 'o \ K) \]

We use the standard continuation monad to ease the semantic definition.

**definition** unitK :: 'o ValK → 'o ValKM where
\[ \text{unitK} \equiv \Lambda \ a. \ Lambda \ c. \ c \ a \]

**definition** bindK :: 'o ValKM → ('o ValK → 'o ValKM) → 'o ValKM where
\[ \text{bindK} \equiv \Lambda \ m \ k. \ Lambda \ c. \ m \ (\Lambda \ a. \ k \ a \ c) \]

**definition** appKM :: 'o ValKM → 'o ValKM → 'o ValKM where
\[ \text{appKM} \equiv \Lambda \ fK \ xK. \ \text{bindK}. fK \ (\Lambda \ (ValKF \cdot f) \cdot f \ xK) \]

The interpretations of the constants.

**definition** condK :: 'o ValKM → 'o ValKM → 'o ValKM → 'o ValKM
where
\[ \text{condK} \equiv \Lambda \ iK. \ \text{bindK}. iK \cdot (\Lambda \ i. \ \text{case} \ i \ \text{of} \ ValKF \cdot f \Rightarrow \bot \mid ValKTT \Rightarrow tK \mid ValKFF \Rightarrow eK \mid ValKN \cdot n \Rightarrow \bot) \]

**definition** succK :: 'o ValKM → 'o ValKM where
\[ \text{succK} \equiv \Lambda \ nK. \ \text{bindK}. nK \cdot (\Lambda \ (ValKN \cdot n). \ \text{unitK} \cdot (ValKN \cdot (n + 1))) \]

**definition** predK :: 'o ValKM → 'o ValKM where
\[ \text{predK} \equiv \Lambda \ nK. \ \text{bindK}. nK \cdot (\Lambda \ (ValKN \cdot n). \ \text{case} \ n \ \text{of} \ 0 \Rightarrow \bot \mid \text{Suc} \ n \Rightarrow \text{unitK} \cdot (ValKN \cdot n)) \]

**definition** isZeroK :: 'o ValKM → 'o ValKM where
\[ \text{isZeroK} \equiv \Lambda \ nK. \ \text{bindK}. nK \cdot (\Lambda \ (ValKN \cdot n). \ \text{case} \ n \ \text{of} \ 0 \ \text{then} \ ValKTT \ \text{else} \ ValKFF) \]

A continuation semantics for PCF. If we had defined our direct semantics using a monad then the correspondence would be more syntactically obvious.

**type-synonym** 'o EnvK = 'o ValKM Env

**primrec**
\[ \text{evalK} :: \text{expr} \Rightarrow 'o \ EnvK \rightarrow 'o \ ValKM \]
\[ \text{evalK} \ (\text{Var} \ v) = (\Lambda \ g. \ g \cdot v) \]
\[ \text{evalK} \ (\text{App} \ f \ x) = (\Lambda \ g. \ \text{appKM} \cdot (\text{evalK} \ f \cdot g) \cdot (\text{evalK} \ x \cdot g)) \]
\[ \text{evalK} \ (\text{Abs} \ v \ e) = (\Lambda \ g. \ \text{unitK} \cdot (\text{ValKF} \cdot (\Lambda \ x. \ \text{evalK} \ e \cdot (\text{env-ext} \cdot v \cdot x \cdot g)))) \]
\[ \text{evalK} \ (\text{AbsV} \ v \ e) = (\Lambda \ g. \ \text{unitK} \cdot (\text{ValKF} \cdot (\Lambda \ x. \ x' \cdot \lambda \ g. \ \text{evalK} \ e \cdot (\text{env-ext} \cdot v \cdot (\text{unitK} \cdot x') \cdot g) \cdot c))) \]
\[ \text{evalK} \ (\text{Diverge}) = (\Lambda \ g. \ \bot) \]
\[ \text{evalK} \ (\text{Fix} \ v \ e) = (\Lambda \ g. \ \mu \ x. \ \text{evalK} \ e \cdot (\text{env-ext} \cdot v \cdot x \cdot g)) \]
\[ \text{evalK} \ (\text{tt}) = (\Lambda \ g. \ \text{unitK} \cdot \text{ValKTT}) \]
\[ \text{evalK} \ (\text{ff}) = (\Lambda \ g. \ \text{unitK} \cdot \text{ValKFF}) \]
\[ \text{evalK} \ (\text{Cond} \ i \ t \ e) = (\Lambda \ g. \ \text{condK} \cdot (\text{evalK} \ i \cdot g) \cdot (\text{evalK} \ t \cdot g) \cdot (\text{evalK} \ e \cdot g)) \]
\[ \text{evalK} \ (\text{Num} \ n) = (\Lambda \ g. \ \text{unitK} \cdot (\text{ValKN} \cdot n)) \]
\[ \text{evalK} \ (\text{Suc} \ e) = (\Lambda \ g. \ \text{succK} \cdot (\text{evalK} \ e \cdot g)) \]
\[ \text{evalK} \ (\text{Pred} \ e) = (\Lambda \ g. \ \text{predK} \cdot (\text{evalK} \ e \cdot g)) \]
\[ \text{evalK} \ (\text{IsZero} \ e) = (\Lambda \ g. \ \text{isZeroK} \cdot (\text{evalK} \ e \cdot g)) \]

To establish the chain completeness (admissibility) of our logical relation, we need to show
that $\text{unit}_K$ is an order monic, i.e., if $\text{unit}_K \cdot x \sqsubseteq \text{unit}_K \cdot y$ then $x \sqsubseteq y$. This is an order-theoretic version of injectivity.

In order to define a continuation that witnesses this, we need to be able to distinguish converging and diverging computations. We therefore require our observation domain to contain at least two elements:

**locale** at-least-two-elements =
  **fixes** some-non-bottom-element :: 'a::domain
  **assumes** some-non-bottom-element: some-non-bottom-element \neq \bot

Following Reynolds (1974) and Filinski (2007, Remark 47) we use the following continuation:

**lemma** cont-below [simp, cont2cont]:
  \(\text{cont}(\lambda x::'a::pcpo. \text{if } x \sqsubseteq d \text{ then } \bot \text{ else } c)\)

**lemma** (in at-least-two-elements) below-monic-unitK [intro, simp]:
  \(\text{below-monic-cfun}(\text{unit}_K :: 'a::\text{Val}_K \rightarrow 'a::\text{Val}_KM)\)

**proof** (rule below-monicI)
  \(\text{fix } v v' :: 'a::\text{Val}_K\)
  \(\text{assume } vv'::\text{unit}_K \cdot v \sqsubseteq \text{unit}_K \cdot v'\)
  \(\text{let } \ ?k = \Lambda x. \text{if } x \sqsubseteq v' \text{ then } \bot \text{ else } \text{some-non-bottom-element}\)
  \(\text{from } vv' \text{ have } \text{unit}_K \cdot v \cdot ?k \sqsubseteq \text{unit}_K \cdot v' \cdot ?k \text{ by (rule monofun-cfun-fun)}\)
  \(\text{hence } ?k \cdot v \sqsubseteq ?k \cdot v' \text{ by (simp add: unitK-def)}\)
  \(\text{with some-non-bottom-element show } v \sqsubseteq v' \text{ by (auto split: split-if-asm)}\)
  \(\text{qed}\)

5.1 Logical relation

We follow Reynolds (1974) by simultaneously defining a pair of relations over values and functions. Both are bottom-reflecting, in contrast to the situation for computational adequacy in §4.3. Filinski (2007) differs by assuming that values are always defined, and relates values and monadic computations.

**type-synonym** 'o lfr = (ValD, 'o ValKM, ValD \rightarrow ValD, 'o ValKM \rightarrow 'o ValKM) \(\text{lfr-pair-rep}\)

**type-synonym** 'o lflf = (ValD, 'o ValKM, ValD \rightarrow ValD, 'o ValKM \rightarrow 'o ValKM) \(\text{lfr-pair}\)

**context** at-least-two-elements

**begin**

**abbreviation** lr-eta-rep-N where
  \(\text{lr-eta-rep-N} \equiv \{ (e, e') .
  (e = \bot \land e' = \bot) \lor (e = \text{ValTT} \land e' = \text{unit}_K \cdot \text{ValTT})
  \lor (e = \text{ValFF} \land e' = \text{unit}_K \cdot \text{ValFF})
  \lor (\exists n. \ e = \text{ValN} \cdot n \land e' = \text{unit}_K \cdot (\text{ValKN} \cdot n)) \} \)

**abbreviation** lr-eta-rep-F where
  \(\text{lr-eta-rep-F} \equiv \lambda(rm, rp). \{ (e, e') .
  (e = \bot \land e' = \bot) \lor (\exists f f'. \ e = \text{ValF} \cdot f \land e' = \text{unit}_K \cdot (\text{ValKF} \cdot f') \land (f, f') \in \text{unlr} (\text{snd} rp)) \} \)

**definition** lr-eta-rep where
  \(\text{lr-eta-rep} \equiv \lambda r. \text{lr-eta-rep-N} \cup \text{lr-eta-rep-F} \ r\)
\textbf{definition} \textit{lr-theta-rep} where
\begin{align*}
\text{lr-theta-rep} \equiv \lambda (\text{rm}, \text{rp}). \{ (f, f') . \forall (x, x') \in \text{unlr} (\text{fst } (\text{undual } \text{rm})). (f \cdot x, f' \cdot x') \in \text{unlr} (\text{fst } \text{rp}) \}
\end{align*}

\textbf{definition} \textit{lr-rep :: 'o lfr} where
\begin{align*}
\text{lr-rep} \equiv \lambda r. (\text{lr-eta-rep } r, \text{lr-theta-rep } r)
\end{align*}

\textbf{abbreviation} \textit{lr :: 'o lflf} where
\begin{align*}
\text{lr} \equiv \lambda r. (\text{mklr } (\text{fst } (\text{lr-rep } r)), \text{mklr } (\text{snd } (\text{lr-rep } r)))
\end{align*}

It takes some effort to set up the minimal invariant relating the two pairs of domains. One might hope this would be easier using deflations (which might compose) rather than “copy” functions (which certainly don’t).

We elide these as they are tedious.

\textbf{sublocale} at-least-two-elements < F!:: DomSolP ValD-copy-rec ValK-copy-rec lr

\textbf{apply} default
\begin{align*}
\text{apply } (\text{rule mono-lr}) \\
\text{apply } (\text{rule fix-ValD-copy-rec-ID}) \\
\text{apply } (\text{rule fix-ValK-copy-rec-ID}) \\
\text{apply } (\text{simp-all add: cfun-map-def})[] \\
\text{apply } (\text{erule } (2) \text{ min-inv-lr}) \\
\text{done}
\end{align*}

5.2 A retraction between the two definitions

We can use the relation to establish a strong connection between the direct and continuation semantics. All results depend on the observation type being rich enough.

\textbf{context} at-least-two-elements

\textbf{begin}

\textbf{abbreviation} \textit{mrel} (\eta: - \mapsto \rightarrow [50, 51] 50) where
\begin{align*}
\eta: x \mapsto x' \equiv (x, x') \in \text{unlr} (\text{fst } F.\text{delta})
\end{align*}

\textbf{abbreviation} \textit{vrel} (\vartheta: - \mapsto \rightarrow [50, 51] 50) where
\begin{align*}
\vartheta: y \mapsto y' \equiv (y, y') \in \text{unlr} (\text{snd } F.\text{delta})
\end{align*}

Theorem 1 from Reynolds (1974).

\textbf{lemma} AbsV-aux:
\begin{align*}
\text{assumes } \eta: \text{ValF} \cdot f \mapsto \text{unitK} \cdot (\text{ValKF} \cdot f') \\
\text{shows } \eta: \text{ValF} \cdot (\text{strictify} \cdot f) \mapsto \text{unitK} \cdot (\text{ValKF} \cdot (\Lambda x \ c. x \cdot (\Lambda x'. f' \cdot (\text{unitK} \cdot x') \cdot c)))
\end{align*}

\textbf{theorem} Theorem1:
\begin{align*}
\text{assumes } \forall v. \eta: \varrho \cdot v \mapsto \varrho' \cdot v \\
\text{shows } \eta: \text{evalD } e \cdot \varrho \mapsto \text{evalK } e \cdot \varrho'
\end{align*}

\textbf{end}

The retraction between the two value and monadic value spaces.

Note we need to work with an observation type that can represent the “explicit values”, i.e. ‘o ValK.
locale value-retraction =
  fixes VtoO :: 'o ValK → 'o
  fixes OtoV :: 'o → 'o ValK
  assumes OV: OtoV oo VtoO = ID

sublocale value-retraction < at-least-two-elements VtoO·(ValKN·0)
using OV by - (default, simp add: injection-defined cfcomp1 cfun-eq-iff)

context value-retraction begin

fun DtoKM-i :: nat ⇒ ValD → 'o ValKM
and KMtoD-i :: nat ⇒ 'o ValKM → ValD
where
  DtoKM-i 0 = ⊥
  | DtoKM-i (Suc n) = (Λ v. case v of
       ValF·f ⇒ unitK·(ValKF·(cfun-map·(KMtoD-i n)·(DtoKM-i n)·f))
       | ValKTT ⇒ unitK·ValKTT
       | ValKFF ⇒ unitK·ValKFF
       | ValKN·m ⇒ unitK·(ValKN·m))
  | KMtoD-i 0 = ⊥
  | KMtoD-i (Suc n) = (Λ v. case OtoV·(v·VtoO) of
       ValKF·f ⇒ ValF·(cfun-map·(DtoKM-i n)·(KMtoD-i n)·f)
       | ValKTT ⇒ ValKTT
       | ValKFF ⇒ ValKFF
       | ValKN·m ⇒ ValKN·m)

abbreviation DtoKM ≡ (∐ i. DtoKM-i i)
abbreviation KMtoD ≡ (∐ i. KMtoD-i i)

Lemma 1 from Reynolds (1974).

lemma Lemma1:
  η: x ↦ DtoKM·x
  η: x ↦ x' ⇒⇒ x = KMtoD·x'

Theorem 2 from Reynolds (1974).

theorem Theorem2: evalD e·q = KMtoD·(evalK e·(DtoKM oo q))
using Lemma1(2)(OF Theorem1) Lemma1(1) by (simp add: cfcomp1)

end

Filinski (2007, Remark 48) observes that there will not be a retraction between direct and
continuation semantics for languages with richer notions of effects.
It should be routine to extend the above approach to the higher-order backtracking language
I wonder if it is possible to construct continuation semantics from direct semantics as proposed
by Sethi and Tang (1980). Roughly we might hope to lift a retraction between two value
domains to a retraction at higher types by synthesising a suitable logical relation.
6 Concluding remarks

We have seen that Pitts’s techniques for showing the existence of relations over domains is straightforward to mechanise and use in HOLCF.

One source of irritation in doing so is that Pitts’s technique is formulated in terms of minimal invariants, which presently must be written out by hand. (Earlier versions of HOLCF’s domain package provided these copy functions, though we would still need to provide our own in such cases as §5.) HOLCF ’11 provides us with take functions (approximations, deflations) on domains that compose, and so one might hope to adapt Pitts’s technique to use these instead. This has been investigated by Benton et al. (2009a, §6), but it is unclear that the deflations involved are those generated by HOLCF ’11.

References


