Logical Relations for PCF

Peter Gammie

June 11, 2019

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 \( \perp \) and is closed under countable chains:

\[
\text{definition adms :: 'a::pcpo set where}
\]
\[
\text{adm} S \equiv \{ \ R :: 'a set. \ \perp \in R \land \text{adm} \ (\lambda x. x \in R) \}
\]

\[
\text{typedef ('a::pcpo)} \text{ adms} = \{ x::'a::pcpo set . x \in \text{adms} \}
\]

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 \(a\,{}^{\text{dual}}\) yields a type with the same elements as \(a\) but with the reverse order. The functions \(\text{dual}\) and \(\text{undual}\) mediate the isomorphism.

**type-synonym** \(d\,{}^{\text{lf-rep}} = a\,{}^{\text{dual}} \times a\,{}^{\text{admS}} \Rightarrow d\,{}^{\text{admS}}\)

**type-synonym** \(d\,{}^{\text{lf}} = a\,{}^{\text{dual}} \times a\,{}^{\text{admS}} \Rightarrow d\,{}^{\text{admS}}\)

The predicate \(eRSV\) encodes our notion of relation. (This is Pitts’s \(e : R \subset S\).) 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.

**abbreviation**
\[
eRSV :: (d::pcpo \rightarrow d) \Rightarrow (i::type \Rightarrow d) \,{}^{\text{admS}} \,{}^{\text{dual}} \Rightarrow (i \Rightarrow d) \,{}^{\text{admS}} \Rightarrow \text{bool}
\]

where
\[
eRSV e R S \equiv \forall d \in \text{unlr} (\text{undual R}). (\lambda x. e \cdot (d x)) \in \text{unlr} S
\]

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 \(\delta\) 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.

**locale** DomSol =
- fixes \(F :: a::order \,{}^{\text{dual}} \times a::order \Rightarrow a\)
- assumes monoF: mono \(F\)

**definition** sym-lr :: \(a\,{}^{\text{dual}} \times a \Rightarrow a\,{}^{\text{dual}} \times a\)

where
\[
sym-lr = (\lambda (rm, rp). (\text{dual} (F (\text{dual} rp, \text{undual} rm)), F (rm, rp)))
\]

**lemma** sym-lr-mono:
\[
\text{mono sym-lr}
\]

**locale** DomSolV = DomSol \(F\) ::
- fixes \(\delta :: (d::pcpo \rightarrow d) \rightarrow d \rightarrow d\)
- assumes min-inv-ID: fix-\(\delta\) = ID
- assumes eRSV-deltaF:
\[
\forall (e :: d \rightarrow d) (R :: (i \Rightarrow d) \,{}^{\text{admS}} \,{}^{\text{dual}}) (S :: (i \Rightarrow d) \,{}^{\text{admS}}). eRSV e R S \Rightarrow eRSV (\delta \cdot e) (\text{dual} (F (\text{dual} S, \text{undual} R))), (F (R, S))\}
\]

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

**definition** delta \equiv 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.

definition synlr :: (′d::pcpo × ′a::type) set set where
  synlr ≡ { R :: (′d × ′a) set. ∀ a. { d. (d, a) ∈ R } ∈ admS }

typedef (′d::pcpo, ′a::type) synlr = { x::(′d × ′a) set. x ∈ synlr }

morphism unsynlr mksynlr (proof)

An alternative representation (suggested by Brian Huffman) is to directly use the type ′a ⇒ ′b 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) synlr.

type-synonym (′d, ′a) synlf-rep = (′d, ′a) synlr dual × (′d, ′a) synlr ⇒ (′d × ′a) set
type-synonym (′d, ′a) synlf = (′d, ′a) synlr dual × (′d, ′a) synlr ⇒ (′d, ′a) synlr

We capture our relations as before. Note we need the inclusion e to be strict for our example.

abbreviation
eRSS :: (′d::pcpo ⇒ ′d) ⇒ (′d, ′a::type) synlr dual ⇒ (′d, ′a) synlr ⇒ bool

where
eRSS e R S ≡ ∀ (d, a) ∈ unsynlr (undual R). (e·d, a) ∈ unsynlr S

locale DomSolSym = DomSol F :: (′d::pcpo, ′a::type) synlf for F +

fixes δ :: (′d::pcpo ⇒ ′d) ⇒ ′d ⇒ ′d

assumes min-inv-ID: fix δ = ID

assumes min-inv-strict: ∀ r. δ·r·⊥ = ⊥

assumes eRS-deltaF:
  ⟨(e :: ′d ⇒ ′d) (R :: ′d, ′a) synlr dual) (S :: ′d, ′a) synlr⟩.
  ⟨e·⊥ = ⊥; eRSS e R S ⟹ eRSS (δ·e) (dual (F (dual S, undual R))) (F (R, S))(proof)(proof)(proof)(proof)(proof)(proof)(proof)(proof)

Again, from these assumptions we can construct the unique solution to the recursive equation specified by F.

2.3 Relations between pairs of domains

Following Reynolds (1974) and Filinski (2007), we want to relate two pairs of mutually-recursive domains. Each of the pairs represents a (monadic) computation and value space.
where DomSolP abbreviation The inclusions need to be strict to get our example through.

We use this solution to relate the direct and continuation semantics for PCF in type-synonym set (1974). We also adopt some of the presentation of Winskel (1993, Chapter 11), in particular including both call-by-name (CBN) and call-by-value (CBV) abstractions following Reynolds. We diverge from the traditional treatment by considering PCF as an untyped language and type-synonym set Using this machinery we can demonstrate some classical results about PCF (Plotkin 1977).

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:

datatype expr = Var var | App expr expr | AbsN var expr

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

We use this solution to relate the direct and continuation semantics for PCF in §5.
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 (lazy appF :: ValD → ValD)
  | ValTT | ValFF
  | ValN (lazy nat)

The lazy keyword means that the ValF constructor is lifted, i.e. ValF·⊥̸ ≠ ⊥, which further means that ValF·(Λ x. ⊥) ≠ ⊥.

The naturals are discretely ordered.

The minimal invariant for ValD is straightforward; the function cfun-map·f·g·h denotes g oo h oo f.

fixrec
  ValD-copy-rec :: (ValD → ValD) → (ValD → ValD)
where
  ValD-copy-rec·r·(ValF·f) = ValF·(cfun-map·r·r·f)
  ValD-copy-rec·r·(ValTT) = ValTT
  ValD-copy-rec·r·(ValFF) = ValFF
  ValD-copy-rec·r·(ValN·n) = ValN·n⟨proof⟩⟨proof⟩⟨proof⟩

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

definition cond :: ValD → ValD → ValD → ValD where
  cond ≡ Λ i t e. case i of ValF·f ⇒ ⊥ | ValTT ⇒ t | ValFF ⇒ e | ValN·n ⇒ ⊥

definition succ :: ValD → ValD where
  succ ≡ Λ (ValN·n). ValN·(n + 1)

definition pred :: ValD → ValD where
  pred ≡ Λ (ValN·n). case n of 0 ⇒ ⊥ | Suc n ⇒ ValN·n

definition isZero :: ValD → ValD where
  isZero ≡ Λ (ValN·n). if n = 0 then ValTT else ValFF

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

type-synonym Var = var
type-synonym 'a Env = Var → 'a

definition env-empty :: 'a Env where
  env-empty ≡ ⊥

definition env-ext :: Var → 'a → 'a Env → 'a Env where
  env-ext ≡ Λ v x ϱ v'. if v = v' then x else ϱ·v'(proof)(proof)

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

type-synonym EnvD = ValD Env

primrec
  evalD :: expr ⇒ EnvD → ValD
where
  evalD (Var v) = (Λ ϱ. ϱ·v)
| evalD (App f x) = (Λ ϱ. appF·(evalD f·ϱ)·(evalD x·ϱ))
| evalD (AbsN v e) = (Λ ϱ. ValF·(Λ x. evalD e·(env-ext·v·x·ϱ)))
| evalD (AbsV v e) = (Λ ϱ. ValF·(strictify·(Λ x. evalD e·(env-ext·v·x·ϱ))))
| evalD (Diverge) = (Λ ϱ. ⊥)
| evalD (Fix v e) = (Λ ϱ. μ x·evalD e·(env-ext·v·x·ϱ))
| evalD (tt) = (Λ ϱ. ValTT)
| evalD (ff) = (Λ ϱ. ValFF)
| evalD (Cond i t e) = (Λ ϱ. cond·(evalD i·ϱ)·(evalD t·ϱ)·(evalD e·ϱ))
| evalD (Num n) = (Λ ϱ. ValN·n)
| evalD (Suc e) = (Λ ϱ. succ·(evalD e·ϱ))
| evalD (Pred e) = (Λ ϱ. pred·(evalD e·ϱ))
| evalD (IsZero e) = (Λ ϱ. isZero·(evalD e·ϱ))

abbreviation eval' :: expr ⇒ ValD Env ⇒ ValD ([-.] [0,1000] 60) where
  eval' M ϱ ≡ evalD M·ϱ

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 Δ ≡ λf x. f (x x) and Y ≡ λf. (Δ f) (Δ f).

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

definition Y-delta :: expr where
  Y-delta ≡ AbsN 0 (AbsN 1 (App (Var 0) (App (Var 1) (Var 1))))

definition Ycomb :: expr where
  Ycomb ≡ AbsN 0 (App (App Y-delta (Var 0)) (App Y-delta (Var 0))

definition fixD :: ValD → ValD where
  fixD ≡ Λ (ValF·fixD)(proof)

lemma Y: [Ycomb]g = ValF·fixD(proof)
### 3.3 Logical relations for definability

An element of $ValD$ is definable if there is an expression that denotes it.

**Definition**

$\text{definable :: } ValD \Rightarrow \text{bool}$

where

$\text{definable } d \equiv \exists M. \ [M]_{\text{env-empty}} = d$

A classical result about PCF is that while the denotational semantics is adequate, as we show in §4, it is not 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 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 $ValD$ that is closed under continuous functions of type $ValD \rightarrow ValD$. This is complicated by the $ValF$ tag and having strict function abstraction.

**Definition**

$\text{logical-relation :: } (\forall i::\text{type }\Rightarrow ValD) \text{ set } \Rightarrow \text{bool}$

where

$\text{logical-relation } R \equiv$

$(\forall fs \in R. \forall xs \in R. (\lambda j. \text{appF}\cdot(fs j)\cdot(xs j)) \in R)$

$\land (\forall fs. (\forall xs \in R. (\lambda j. \text{strictify}(\text{appF}\cdot(fs j))\cdot(xs j)) ) \in R)$

$\land (\forall fs. (\forall xs \in R. (\lambda j. \text{ValF}\cdot(fs j)) \in R)$

$\land (\forall cs \in R. (\lambda j. \text{cond}\cdot(cs j)\cdot(ts j)\cdot(es j)) \in R)$

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

**Definition**

$\text{PCF-consts-rel :: } (\forall i::\text{type }\Rightarrow ValD) \text{ set } \Rightarrow \text{bool}$

where

$\text{PCF-consts-rel } R \equiv$

$
\bot \in R \\
\land (\lambda i. \text{ValTT} ) \in R \\
\land (\lambda i. \text{ValFF} ) \in R \\
\land (\forall n. (\lambda i. \text{ValN-n} ) \in R)\langle\text{proof}\rangle\langle\text{proof}\rangle
$

**Abbreviation**

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

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** $lr :: \text{PCF-lr } R$
- **Assumes** $v \forall v. (\lambda i. g i \cdot v ) \in R$
- **Shows** $(\lambda i. [M](g i)) \in R\langle\text{proof}\rangle$
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 \( f \text{args} = \text{result} \) then we can conclude that \( f \) is not definable.

**abbreviation**

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

**where**

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

**lemma** \text{lr-appFLv}:

assumes \( \text{lr} \): logical-relation \( R \)
assumes \( f \): \( (\forall i::\text{type} \Rightarrow f) \in R \)
assumes \( \text{args} \): set \( \text{args} \subseteq R \)
shows \( \text{appFLv} f \text{args} \in R \)

**corollary** \text{not-definable}:

fixes \( R \):: \( (\forall i::\text{type} \Rightarrow \text{ValD}) \set \)
fixes \( \text{args} \):: \( (\forall i \Rightarrow \text{ValD}) \) set
fixes \( \text{result} \):: \( (\forall i \Rightarrow \text{ValD}) \)
assumes \( \text{lr} \): PCF-lr \( R \)
assumes \( \text{args} \): set \( \text{args} \subseteq R \)
assumes \( \text{result} \): 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 the familiar short-circuiting or except that if the first argument is \( \bot \) and the second one is \( \text{ValTT} \), we get \( \text{ValTT} \) (and not \( \bot \)). It is continuous and then have included in the \( \text{ValD} \) domain.

**definition** \( \text{por} :: \text{ValD} \Rightarrow \text{ValD} \Rightarrow \text{ValD} \) (\( \bot \) \- \( \text{por} \) \- \( [31,30] \) \( 30 \) ) where

\[
x \text{por} y \equiv 
\begin{align*}
\text{if} \ x = \text{ValTT} \ \text{then} \ \text{ValTT} \\
\text{else if} \ y = \text{ValTT} \ \text{then} \ \text{ValTT} \\
\text{else if} \ (x = \text{ValFF} \land y = \text{ValFF}) \ \text{then} \ \text{ValFF} \ \text{else} \ \bot
\end{align*}
\]

The defining properties of parallel-or.

**lemma** \( \text{POR-simps} \) [simp]:

\[
\begin{align*}
(\text{ValTT por} y) &= \text{ValTT} \\
(\text{ValFF por} \text{ValTT}) &= \text{ValTT} \\
(\text{ValFF por} \text{ValFF}) &= \text{ValFF} \\
(\text{ValFF por} \bot) &= \bot \\
(\text{ValFF por} \text{ValN} \cdot n) &= \bot \\
(\text{ValFF por} \text{ValF} \cdot f) &= \bot \\
(\bot \text{por} \text{ValFF}) &= \bot \\
(\text{ValN} \cdot n \text{por} \text{ValFF}) &= \bot \\
(\text{ValF} \cdot f \text{por} \text{ValFF}) &= \bot \\
(\bot \text{por} \bot) &= \bot \\
(\bot \text{por} \text{ValN} \cdot n) &= \bot \\
(\bot \text{por} \text{ValF} \cdot f) &= \bot \\
(\text{ValN} \cdot n \text{por} \bot) &= \bot \\
(\text{ValF} \cdot f \text{por} \bot) &= \bot
\end{align*}
\]
\[(\text{ValN}\cdot m \text{ por ValN}\cdot n) = \bot\]
\[(\text{ValN}\cdot n \text{ por ValF}\cdot f) = \bot\]
\[(\text{ValF}\cdot f \text{ por ValN}\cdot n) = \bot\]
\[(\text{ValF}\cdot f \text{ por ValF}\cdot g) = \bot\]
\[
\langle \text{proof} \rangle \langle \text{proof} \rangle \langle \text{proof} \rangle \langle \text{proof} \rangle \langle \text{proof} \rangle \langle \text{proof} \rangle \langle \text{proof} \rangle \langle \text{proof} \rangle \langle \text{proof} \rangle
\]

We need three-element vectors.

datatype Three = One | Two | Three

The standard logical relation \( R \) that demonstrates POR is not definable is:

\[(x, y, z) \in R \iff x = y = z \lor (x = \bot \lor y = \bot)\]

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 = ⊥ } — \( x = \bot \)
∪ { f . f Two = ⊥ } — \( y = \bot \)

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 }
⟨ \text{proof} \rangle ⟨ \text{proof} \rangle ⟨ \text{proof} \rangle ⟨ \text{proof} \rangle

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 ≡ λr. mklr (POR-lf-rep \( r \))\langle \text{proof} \rangle

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' S'
shows eRSV (ValD-copy-rec-e) (Dual (POR-lf (Dual S', Undual R'))) (POR-lf (R', S'))\langle \text{proof} \rangle

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

lemma PCF-lf-POR-delta: PCF-lf (Undual POR.delta)\langle \text{proof} \rangle

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
**Definition** \text{POR-arg2-rel} where
\[
\text{POR-arg2-rel} \equiv \lambda \cdot \text{case } i \text{ of } \text{One } \Rightarrow \bot | \text{Two } \Rightarrow \text{ValTT} | \text{Three } \Rightarrow \text{ValFF}
\]

**Definition** \text{POR-result-rel} where
\[
\text{POR-result-rel} \equiv \lambda \cdot \text{case } i \text{ of } \text{One } \Rightarrow \text{ValTT} | \text{Two } \Rightarrow \text{ValTT} | \text{Three } \Rightarrow \text{ValFF}
\]

**Lemma** \text{lr-POR-arg1-rel}: \text{POR-arg1-rel} \in \text{unlr POR.delta}

**Lemma** \text{lr-POR-arg2-rel}: \text{POR-arg2-rel} \in \text{unlr POR.delta}

**Lemma** \text{lr-POR-result-rel}: \text{POR-result-rel} \notin \text{unlr POR.delta}

Parallel-or satisfies these tests:

**Theorem** \text{POR-sat}:
\[
\text{appFLv} \bigl( \text{ValF} \cdot (\Lambda x . \text{ValF} \cdot (\Lambda y . x \text{ por } y)) \bigr) [\text{POR-arg1-rel}, \text{POR-arg2-rel}] = \text{POR-result-rel}
\]

... but is not PCF-definable:

**Theorem** \text{POR-is-not-definable}:
\[
\text{shows} \ \neg (\exists f . \text{definable } f \land \text{appFLv } f [\text{POR-arg1-rel}, \text{POR-arg2-rel}] = \text{POR-result-rel})
\]

### 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 \text{ValTT} then \text{plotkin-exists} yields \text{ValTT}. It may be more plausible to test \(f\) on numerals only.

**Definition** \text{plotkin-exists} :: \text{ValD} \Rightarrow \text{ValD} where
\[
\text{plotkin-exists } f \equiv
\begin{cases}
\text{ValFF} & \text{if } (\text{appF} \cdot f \cdot \bot = \text{ValFF}) \\
\text{ValFF} & \text{if } (\exists n . \text{appF} \cdot f \cdot n = \text{ValTT}) \text{ then } \text{ValTT} \text{ else } \bot
\end{cases}
\]

We can show this function is continuous.

**Lemma** \text{cont-pe [cont2cont, simp]: cont plotkin-exists}(proof)

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

**Definition** \text{PE-arg-rel} where
\[
\text{PE-arg-rel} \equiv \lambda i . \text{ValF} \cdot (\text{case } i \text{ of } 0 \Rightarrow (\Lambda - . \text{ValFF}) \\
| \text{Suc } n \Rightarrow (\Lambda \ (\text{ValN} \cdot x) . \text{if } x = \text{Suc } n \text{ then } \text{ValTT} \text{ else } \bot))
\]

**Definition** \text{PE-result-rel} where
\[
\text{PE-result-rel} \equiv \lambda i . \text{case } i \text{ of } 0 \Rightarrow \text{ValFF} | \text{Suc } n \Rightarrow \text{ValTT}
\]
Note that unlike the POR case the argument relation does not characterise PE: we don’t treat functions that return \( \text{ValTT} \)s and \( \text{ValFF} \)s.

The Plotkin existential satisfies these tests:

\[ \text{theorem pe-sat:} \quad \text{appFLv} \left( \text{ValF} \cdot (\Lambda x. \text{plotkin-exists } x) \right) [\text{PE-arg-rel}] = \text{PE-result-rel} \]

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

\[ \text{definition PE-base-lf-rep :: (nat } \Rightarrow \text{ ValD) lf-rep where} \]
\[ \text{PE-base-lf-rep } \equiv \lambda (mR, pR).
\]
\[ \quad \{ \bot \}
\]
\[ \quad \cup \{ (\lambda i. \text{ValTT}) \} \cup \{ (\lambda i. \text{ValFF}) \} \quad \text{— } x = y = z \text{ for bools}
\]
\[ \quad \cup \{ (\bigcup n. \{ (\lambda i. \text{ValN-n}) \}) \quad \text{— } x = y = z \text{ for numerals}
\]
\[ \quad \cup \{ f \cdot f 1 = \bot \lor f 2 = \bot \} \quad \text{— Vectors that diverge on one or two.} \]

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

\[ \text{definition PE-lf-rep :: (nat } \Rightarrow \text{ ValD) lf-rep where} \]
\[ \text{PE-lf-rep } R \equiv \text{PE-base-lf-rep } R \cup \text{fn-lf-rep } R \]

\[ \text{abbreviation PE-lf } \equiv \lambda r. \text{mklr (PE-lf-rep } r) \]

The solution satisfies the expectations of the fundamental theorem:

\[ \text{lemma PCF-lr-PE-delta:} \quad \text{PCF-lr (unlr PE.delta)} \]
\[ \text{lemma lr-PE-arg-rel:} \quad \text{PE-arg-rel } \in \text{unlr PE.delta} \]
\[ \text{lemma lr-PE-result-rel:} \quad \text{PE-result-rel } \notin \text{unlr PE.delta} \]
\[ \text{theorem PE-is-not-definable:} \quad \neg (\exists f. \text{definable } f \land \text{appFLv } f [\text{PE-arg-rel}] = \text{PE-result-rel}) \]

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** 

\[ db = \]

\[ \text{DBVar var} \]
\[ \text{DBApp db db} \]
\[ \text{DBAbsN db} \]
\[ \text{DBAbsV db} \]
\[ \text{DBDiverge} \]
\[ \text{DBFix db} \]
\[ \text{DBtt} \]
\[ \text{DBff} \]
\[ \text{DBCond db db db} \]
\[ \text{DBNum nat} \]
\[ \text{DBSucc db} \]
\[ \text{DBPred db} \]
\[ \text{DBIsZero db} \]

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 0::’a may be free, and while we could develop a simpler account, we retain the traditional one.

```
fun lift :: db ⇒ nat ⇒ db
where
  lift (DBVar i) k = DBVar (if i < k then i else (i + 1))
  lift (DBAbsN s) k = DBAbsN (lift s (k + 1))
  lift (DBAbsV s) k = DBAbsV (lift s (k + 1))
  lift (DBApp s t) k = DBApp (lift s k) (lift t k)
  lift (DBFix e) k = DBFix (lift e (k + 1))
  lift (DBCond c t e) k = DBCond (lift c k) (lift t k) (lift e k)
  lift (DBSucc e) k = DBSucc (lift e k)
  lift (DBPred e) k = DBPred (lift e k)
  lift (DBIsZero e) k = DBIsZero (lift e k)
  lift x k = x
```

We elide the standard lemmas about these operations.

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

```
fun subst :: db ⇒ db ⇒ var ⇒ db
where
  subst-Var: (DBVar i)<s/k> =
    (if k < i then DBVar (i - 1) else if i = k then s else DBVar i)
  subst-AbsN: (DBAbsN t)<s/k> = DBAbsN (t<lift s 0 / k+1>)
  subst-AbsV: (DBAbsV t)<s/k> = DBAbsV (t<lift s 0 / k+1>)
  subst-App: (DBApp t u)<s/k> = DBApp (t<s/k>) (u<s/k>)
  (DBFix e)<s/k> = DBFix (e<lift s 0 / k+1>)
  (DBCond c t e)<s/k> = DBCond (c<s/k>) (t<s/k>) (e<s/k>)
  (DBSucc e)<s/k> = DBSucc (e<s/k>)
  (DBPred e)<s/k> = DBPred (e<s/k>)
  (DBIsZero e)<s/k> = DBIsZero (e<s/k>)
  subst-Consts: x<s/k> = x<proof><proof><proof><proof><proof><proof><proof><proof><proof>
```

We elide the standard lemmas about these operations.
The direct denotational semantics is almost identical to that given in §3.1, apart from this change in the representation of environments.

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

closed e ≡ ∀ i. ¬ freedb e i(\langle proof⟩) (\langle proof⟩)

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

env-empty-db ≡ ⊥

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

env-ext-db ≡ Λ x. g. v. (case v of 0 ⇒ x | Suc v' ⇒ g.v')(\langle proof⟩) (\langle proof⟩)

**primrec**

evalDdb :: db ⇒ ValD Env → ValD

where

evalDdb (DBVar i) = (Λ g. g.i)
| evalDdb (DBApp f x) = (Λ g. appF.(evalDdb f.g).(evalDdb x.g))
| evalDdb (DBAbsN e) = (Λ g. ValF.(Λ x. evalDdb e.(env-ext-db x.g)))
| evalDdb (DBAbsV e) = (Λ g. ValF.(\langle proof⟩) (\langle proof⟩))
| evalDdb (DBSucc e) = (Λ g. ValF.(\langle proof⟩) (\langle proof⟩)
| evalDdb (DBFix e) = (Λ g. ValF.(\langle proof⟩) (\langle proof⟩)
| evalDdb (DBPred e) = (Λ g. ValF.(\langle proof⟩) (\langle proof⟩)
| evalDdb (DBIsZero e) = (Λ g. ValF.(\langle proof⟩) (\langle proof⟩)

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

index [] v n = n
| index (h # t) v n = (if v = h then n else index t v (Suc n))
transdb :: expr ⇒ var list ⇒ db

where
transdb (Var i) Γ = DBVar (index Γ i 0)
| transdb (App t1 t2) Γ = DBApp (transdb t1 Γ) (transdb t2 Γ)
| transdb (AbsN v t) Γ = DBAbsN (transdb t (v # Γ))
| transdb (AbsV v t) Γ = DBAbsV (transdb t (v # Γ))
| transdb (Diverge) Γ = DBDiverge
| transdb (Fix v e) Γ = DBFix (transdb e (v # Γ))
| transdb (tt) Γ = DBtt
| transdb (ff) Γ = DBff
| transdb (Cond c t e) Γ = DBCond (transdb c Γ) (transdb t Γ) (transdb e Γ)
| transdb (Num n) Γ = (DBNum n)
| transdb (Succ e) Γ = DBSucc (transdb e Γ)
| transdb (Pred e) Γ = DBPred (transdb e Γ)
| transdb (IsZero e) Γ = DBIsZero (transdb e Γ)

This semantics corresponds with the direct semantics for named expressions.

lemma evalD-evalDdb:
assumes free e = []
shows [[e]_{\rho} = evalDdb (transdb e [])_{\rho}

Conversely, all de Bruijn expressions have named equivalents.

primrec
transdb-inv :: db ⇒ (var ⇒ var) ⇒ var ⇒ var ⇒ expr

where
transdb-inv (DBVar i) Γ c k = Var (Γ i)
| transdb-inv (DBApp t1 t2) Γ c k = App (transdb-inv t1 Γ) (transdb-inv t2 Γ) c k
| transdb-inv (DBAbsN e) Γ c k = AbsN (c + k) (transdb-inv e (case-nat (c + k) Γ) c (k + 1))
| transdb-inv (DBAbsV e) Γ c k = AbsV (c + k) (transdb-inv e (case-nat (c + k) Γ) c (k + 1))
| transdb-inv (DBDiverge) Γ c k = Diverge
| transdb-inv (DBFix e) Γ c k = Fix (c + k) (transdb-inv e (case-nat (c + k) Γ) c (k + 1))
| transdb-inv (DBtt) Γ c k = tt
| transdb-inv (DBff) Γ c k = ff
| transdb-inv (DBCond i t e) Γ c k = Cond (transdb-inv i Γ) (transdb-inv t Γ) (transdb-inv e Γ) c k
| transdb-inv (DBNum n) Γ c k = (Num n)
| transdb-inv (DBSucc e) Γ c k = Succ (transdb-inv e Γ) c k
| transdb-inv (DBPred e) Γ c k = Pred (transdb-inv e Γ) c k
| transdb-inv (DBIsZero e) Γ c k = IsZero (transdb-inv e Γ) c k

lemma transdb-inv:
assumes closed e
shows transdb (transdb-inv e Γ) c k = 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
val :: db ⇒ bool
where
v-Num[intro]: val (DBNum n)
v-FF[intro]: val DBff
v-TT[intro]: val DBtt
v-AbsN[intro]: val (DBAbsN e)
v-AbsV[intro]: val (DBAbsV e)

inductive
evalOP :: db ⇒ db ⇒ bool
where
evalOP-AppN[intro]: [ [ P ⇓ DBAbsN M ; M <Q/0> ⇓ V ] ] =⇒ DBApp P Q ⇓ V
| evalOP-AppV[intro]: [ [ P ⇓ DBAbsV M ; Q ⇓ q ; M <q/0> ⇓ V ] ] =⇒ DBApp P Q ⇓ V
| evalOP-AbsN[intro]: val (DBAbsN e) =⇒ DBAbsN e ⇓ DBAbsN e
| evalOP-AbsV[intro]: val (DBAbsV e) =⇒ DBAbsV e ⇓ DBAbsV e
| evalOP-Fix[intro]: P <DBFix P /0> ⇓ V =⇒ DBFix P ⇓ V
| evalOP-tt[intro]: DBtt ⇓ DBtt
| evalOP-ff[intro]: DBff ⇓ DBff
| evalOP-Num[intro]: DBNum n ⇓ DBNum n
| evalOP-Succ[intro]: P ⇓ DBNum n =⇒ DBSucc P ⇓ DBNum (Suc n)
| evalOP-Pred[intro]: P ⇓ DBNum (Suc n) =⇒ DBPred P ⇓ DBNum n
| evalOP-IsZeroTT[intro]: [ [ E ⇓ DBNum 0 ] ] =⇒ DBIsZero E ⇓ DBtt
| evalOP-IsZeroFF[intro]: [ [ E ⇓ DBNum n ; 0 < n ] ] =⇒ DBIsZero E ⇓ DBff

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

 theorem evalOP-sound:
 assumes P ⇓ V
 shows evalDdb P · ϱ = evalDdb V · ϱ

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 \( \{ \bot \} \times \{ \text{P. closed} \ P \} \). To that end we define the type of programs.

typedef Prog = \{ P. closed P \}

morphisms unProg mkProg ⟨proof⟩

definition ca-lf-rep :: (ValD, Prog) synlf-rep

where

cia-lf-rep \equiv \lambda (rm, rp).

\( \{ \bot \} \times \text{UNIV} \)

\( \cup \{ (d, P) \mid d P. \)

(∃ n. d = ValN.n ∧ unProg P ⊑ DBNum n)

\( \lor \{ (d = ValTT ∧ unProg P ⊑ DBtt) \}

\( \lor \{ (d = ValFF ∧ unProg P ⊑ DBff) \}

\( \lor \{ (∃ M. d = ValF.f ∧ unProg P ⊑ DBAbsN M \land (∀ (x, X) \in \text{unsynlr} \ (\text{undual} \ rm), (f-x, \ mkProg \ (M < \text{unProg} X / \theta >)) \in \text{unsynlr} \ rp)) \}

\( \lor \{ (∃ J M. d = ValF.f ∧ unProg P ⊑ DBAbsV M \land f-\bot = \bot \land (∀ (x, X) \in \text{unsynlr} \ (\text{undual} \ rm), ∀ V. \ unProg X \downarrow V \rightarrow (f-x, \ mkProg \ (M < \text{V/θ} >)) \in \text{unsynlr} \ rp)) \} \}

abbreviation ca-lr :: (ValD, Prog) synlf where

cia-lr \equiv \lambda r. \ mksynlr (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-\( \bot \) denotation then we can use this relation to conclude something about the value it (operationally) converges to.

⟨proof⟩ ⟨proof⟩ ⟨proof⟩ ⟨proof⟩ ⟨proof⟩ ⟨proof⟩

interpretation ca: DomSolSyn ca-lr ValD-copy-rec

⟨proof⟩

definition ca-lr-syn :: ValD ⇒ db ⇒ bool (- ∘ [-80,80] 80) where

d ◦ P \equiv \{ (d, P) \} (x, unProg Y) | x Y. (x, Y) ∈ unsynlr ca.delta \} ⟨proof⟩ ⟨proof⟩ ⟨proof⟩ ⟨proof⟩ ⟨proof⟩ ⟨proof⟩ ⟨proof⟩

To establish this result we need a “closing substitution” operation. It seems easier to define it directly in this simple-minded way than reusing the standard substitution operation.

This is quite similar to a context-plugging (non-capturing) substitution operation, where the “holes” are free variables, and indeed we use it as such below.

fun

closing-subst :: db ⇒ (var ⇒ db) ⇒ var ⇒ db

where

closing-subst (DBVar i) Γ k = (if k \leq i then Γ (i - k) else DBVar i)

closing-subst (DBApp t u) Γ k = DBApp (closing-subst t Γ k) (closing-subst u Γ k)

closing-subst (DBAbs t) Γ k = DBAbsN (closing-subst t Γ (k + 1))

closing-subst (DBAbsV t) Γ k = DBAbsV (closing-subst t Γ (k + 1))

closing-subst (DBFix e) Γ k = DBFix (closing-subst e Γ (k + 1))

closing-subst (DBCond c t e) Γ k =

DBCond (closing-subst c Γ k) (closing-subst t Γ k) (closing-subst e Γ k)
\[ \text{closing-subst} \ (\text{DBSucc} \ e) \ \Gamma \ k = \text{DBSucc} \ (\text{closing-subst} \ e \ \Gamma \ k) \]
\[ \text{closing-subst} \ (\text{DBPred} \ e) \ \Gamma \ k = \text{DBPred} \ (\text{closing-subst} \ e \ \Gamma \ k) \]
\[ \text{closing-subst} \ (\text{DBIsZero} \ e) \ \Gamma \ k = \text{DBIsZero} \ (\text{closing-subst} \ e \ \Gamma \ k) \]
\[ \text{closing-subst} \ x \ \Gamma \ k = x \]

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

\[ \langle \text{proof} \rangle \langle \text{proof} \rangle \langle \text{proof} \rangle \langle \text{proof} \rangle \langle \text{proof} \rangle \langle \text{proof} \rangle \]

The key lemma is shown by induction over \( e \) for arbitrary environments (\( \Gamma \) and \( \rho \)):

**Lemma ca-open:**
- **Assumes** \( \forall \ v. \ \text{free} db \ e \ v \rightarrow \varrho \cdot v \triangleleft \Gamma \ v \land \text{closed} \ (\Gamma \ v) \)
- **Shows** \( \text{eval} db \ e \cdot \varrho \triangleleft \text{closing-subst} \ e \ \Gamma \ 0 \)

**Lemma ca-closed:**
- **Assumes** \( \text{closed} \ e \)
- **Shows** \( \text{eval} db \ e \cdot \text{env-empty} \triangleleft \ e \)

**Theorem ca:**
- **Assumes** \( \text{nb} : \ \text{eval} db \ e \cdot \text{env-empty} \neq \bot \)
- **Assumes** \( \text{closed} \ e \)
- **Shows** \( \exists \ V. \ e \downarrow V \)

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 \( \text{AbsN} \)s. 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:** \( \text{db} \Rightarrow \text{db} \Rightarrow \text{db} \ (\ (\ < \ - \ < \ - \ > \ ) \ [300, \ 0] \ 300) \ ) \text{ where} \)
\[ C<e> \equiv \text{closing-subst} \ C \ (\lambda -. \ e \ ) \ 0 \langle \text{proof} \rangle \langle \text{proof} \rangle \]

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**
\[ \text{have-the-same-form} :: \ \text{db} \Rightarrow \text{db} \Rightarrow \text{bool} \ (\sim \ - \ [50, \ 50] \ 50) \]
\[ \text{where} \]
- \( \text{DBAbsN} \ e \sim \text{DBAbsN} \ e' \)
- \( \text{DBAbsN} \ e \sim \text{DBAbsV} \ e' \)
- \( \text{DBAbsV} \ e \sim \text{DBAbsN} \ e' \)
- \( \text{DBAbsV} \ e \sim \text{DBAbsV} \ e' \)
- \( \text{DBFix} \ e \sim \text{DBFix} \ e' \)
- \( \text{DBtt} \sim \text{DBtt} \)
- \( \text{DBff} \sim \text{DBff} \)
- \( \text{DBNum} \ n \sim \text{DBNum} \ n \langle \text{proof} \rangle \)
A program $e_2$ refines the program $e_1$ if it converges in context at least as often. This is a preorder on programs.

**definition**

\[ \text{refines} :: \text{db} \Rightarrow \text{db} \Rightarrow \text{bool} \] 

where \[ e_1 \sqsubseteq e_2 \equiv \forall C. \exists V_1. C < e_1 > \Downarrow V_1 \rightarrow (\exists V_2. C < e_2 > \Downarrow V_2 \land V_1 \sim V_2) \]

Contextually-equivalent programs refine each other.

**definition**

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

where \[ e_1 \approx e_2 \equiv e_1 \sqsubseteq e_2 \land e_2 \sqsubseteq e_1 \langle \text{proof} \rangle \langle \text{proof} \rangle \]

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 $D$: eval$D$\$db \ e_1$.\$env-empty-db = eval$D$\$db \ e_2$.\$env-empty-db$

shows $e_1 \approx e_2 \langle \text{proof} \rangle$

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 combinatory.

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 \((\ell o \ ValK, \ell o) \ K \to (\ell o \ ValK, \ell o) \ K\) as our language includes call-by-name.

**type-synonym** \((\ell o, \ell o) \ K = (\ell o \to \ell o) \to \ell o\)

**domain** \(\ell o \ ValK\)
- \(ValKF (\text{lazy} \ appKF : (\ell o \ ValK, \ell o) \ K \to (\ell o \ ValK, \ell o) \ K)\)
- \(ValKTT \mid ValKF\)
- \(ValKN \ (\text{lazy} \ \text{nat})\)

**type-synonym** \(\ell o \ ValKM = (\ell o \ ValK, \ell o) \ K\langle \text{proof}\rangle\langle \text{proof}\rangle\langle \text{proof}\rangle\langle \text{proof}\rangle\)

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

**definition** \(\text{unitK} :: \ell o \ ValK \to \ell o \ ValKM\) where
\[
\text{unitK} \equiv \Lambda a. \Lambda c. \ c \cdot a
\]

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

**definition** \(\text{appKM} :: \ell o \ ValK \to (\ell o \ ValK \to \ell o \ ValKM) \to \ell o \ ValKM\) where
\[
\text{appKM} \equiv \Lambda fK. \Lambda xK. \text{bindK} : fK \cdot (\Lambda (ValKF \ f). f \cdot xK)\langle \text{proof}\rangle\langle \text{proof}\rangle\langle \text{proof}\rangle\langle \text{proof}\rangle
\]

The interpretations of the constants.

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

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

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

**definition** \(\text{isZeroK} :: \ell o \ ValK \to \ell o \ ValKM\) where
\[
\text{isZeroK} \equiv \Lambda nK. \text{bindK} : nK \cdot (\Lambda (ValKN \cdot n). \ \text{unitK} : (\text{if} \ n = 0 \ \text{then} \ \text{ValKTT} \ \text{else} \ \text{ValKF}))
\]

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** \(\ell o \ EnvK = \ell o \ ValK \ Env\)

**primrec**
\[
\text{evalK} :: \text{expr} \Rightarrow \ell o \ EnvK \to \ell o \ ValKM
\]

**where**
\[
\text{evalK} \ (\text{Var} \ v) = (\Lambda \ \ell o. \ \ell o \cdot v)
\]
\[
\text{evalK} \ (\text{App} \ f \ x) = (\Lambda \ \ell o. \ \text{appKM} : (\ell o \ ValK, \ell o) \ K \to (\ell o \ ValK, \ell o) \ K)\langle \text{proof}\rangle\langle \text{proof}\rangle\langle \text{proof}\rangle\langle \text{proof}\rangle
\]
\[
\text{evalK} \ (\text{AbsN} \ v \ e) = (\Lambda \ \ell o. \ \text{unitK} : (\Lambda x. \ \text{evalK} : (\text{env-ext} \cdot v \cdot \ell o \cdot x)\langle \text{proof}\rangle\langle \text{proof}\rangle\langle \text{proof}\rangle\langle \text{proof}\rangle))
\]
\[
\text{evalK} \ (\text{AbsV} \ v \ e) = (\Lambda \ \ell o. \ \text{unitK} : (\Lambda x. \ \text{evalK} : (\text{env-ext} \cdot v \cdot (\text{unitK} \cdot x)\langle \text{proof}\rangle\langle \text{proof}\rangle\langle \text{proof}\rangle\langle \text{proof}\rangle)\langle \text{proof}\rangle\langle \text{proof}\rangle\langle \text{proof}\rangle\langle \text{proof}\rangle))
\]
\[
\text{evalK} \ (\text{Diverge}) = (\Lambda \ \ell o. \ \bot)
\]
\[
\text{evalK} \ (\text{Fix} \ v \ e) = (\Lambda \ \ell o. \ \mu x. \ \text{evalK} : (\text{env-ext} \cdot v \cdot x \cdot \ell o)\langle \text{proof}\rangle\langle \text{proof}\rangle\langle \text{proof}\rangle\langle \text{proof}\rangle)
\]
\[
\text{evalK} \ (\text{tl}) = (\Lambda \ \ell o. \ \text{unitK} : \text{ValKTT})
\]
| evalK (ff) = (Λ ϱ. unitK · ValKFF) |
| evalK (Cond i t e) = (Λ ϱ. condK · (evalK i · ϱ) · (evalK t · ϱ) · (evalK e · ϱ)) |
| evalK (Num n) = (Λ ϱ. unitK · (ValKN · n)) |
| evalK (Succ e) = (Λ ϱ. succK · (evalK e · ϱ)) |
| evalK (Pred e) = (Λ ϱ. predK · (evalK e · ϱ)) |
| evalK (IsZero e) = (Λ ϱ. isZeroK · (evalK e · ϱ)) |

To establish the chain completeness (admissibility) of our logical relation, we need to show that unitK is an order monic, i.e., if unitK · x ⊑ unitK · y then x ⊑ 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 :: 'o:domain
  assumes some-non-bottom-element: some-non-bottom-element ≠ ⊥
```

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

```
lemma cont-below [simp, cont2cont]:
  cont (λx::'a::pcpo. if x ⊑ d then ⊥ else c)(proof)
```

```
lemma (in at-least-two-elements) below-monic-unitK [intro, simp]:
  below-monic-cfun (unitK :: 'o ValK → 'o ValKM)
(proof)
```

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 → ValD, 'o ValKM → 'o ValKM) lfr-pair-rep
```

```
type-synonym 'o lflf = (ValD, 'o ValKM, ValD → ValD, 'o ValKM → 'o ValKM) lflf-pair
```

```
context at-least-two-elements begin

abbreviation lr-eta-rep-N where
  lr-eta-rep-N ≡ { (e, e') .
       (e = ⊥ ∧ e' = ⊥)
   ∨ (e = ValTT ∧ e' = unitK · ValKTT)
   ∨ (e = ValFF ∧ e' = unitK · ValKFF)
   ∨ (∃ n. e = ValN · n ∧ e' = unitK · (ValKN · n)) }
```

abbreviation lr-eta-rep-F where
  lr-eta-rep-F ≡ λ(rm, rp). { (e, e') .
       (e = ⊥ ∧ e' = ⊥)
   ∨ (∃ f f'. e = ValF · f ∧ e' = unitK · (ValKF · f') ∧ (f, f') ∈ unlr (snd rp)) }
```

definition lr-eta-rep where
\[
\text{lreta-rep} \equiv \lambda r. \text{lreta-rep-N} \cup \text{lreta-rep-F} r
\]

definition \text{ltheta-rep} where
\[
\text{ltheta-rep} \equiv \lambda (rm, rp). \{ (f, f') . \forall (x, x') \in \text{unlr (fst (undual rm))}. (f \cdot x, f' \cdot x') \in \text{unlr (fst rp)} \}
\]

definition \text{lrep} :: 'o lfr where
\[
\text{lrep} \equiv \lambda r. (\text{lreta-rep r}, \text{ltheta-rep r})
\]

abbreviation \text{lr} :: 'o lflf where
\[
\text{lr} \equiv \lambda r. (\text{mklr (fst (lrep r))}, \text{mklr (snd (lrep r))})
\]

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.

\[
\text{context at-least-two-elements begin}
\]

abbreviation \text{mrel (}\eta:: [\text{50}, \text{51}] \text{50}) where
\[
\eta: x \mapsto \equiv (x, x') \in \text{unlr (fst F.delta)}
\]

abbreviation \text{vrel (}\vartheta:: [\text{50}, \text{51}] \text{50}) where
\[
\vartheta: y \mapsto \equiv (y, y') \in \text{unlr (snd F.delta)}
\]

Theorem 1 from Reynolds (1974).

lemma \text{AbsV-aux}:
\[
\text{assumes } \eta: \text{ValF} \cdot f \mapsto \text{unitK} \cdot (\text{ValKF} \cdot f')
\]
\[
\text{shows } \eta: \text{ValF} \cdot (\text{strictify} f) \mapsto \text{unitK} \cdot (\text{ValKF} \cdot (\Lambda x. x \cdot (\Lambda x'. f' \cdot (\text{unitK} \cdot x') \cdot c)))
\]

theorem \text{Theorem1}:
\[
\text{assumes } \forall v. \eta: \varrho \cdot v \mapsto \varrho' \cdot v
\]
\[
\text{shows } \eta: \text{evalD} \cdot e \cdot \varrho \mapsto \text{evalK} \cdot e \cdot \varrho'(\text{proof})
\]

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. \text{'}o ValK.

locale value-retraction =
\[
\text{fixes VtoO :: } 'o \text{ ValK} \rightarrow 'o
\]
\[
\text{fixes OtoV :: } 'o \rightarrow 'o \text{ ValK}
\]
\[
\text{assumes } OV: OtoV \circ VtoO = \text{ID}
\]

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.

\[
\text{context at-least-two-elements begin}
\]

abbreviation \text{mrel (}\eta:: [\text{50}, \text{51}] \text{50}) where
\[
\eta: x \mapsto \equiv (x, x') \in \text{unlr (fst F.delta)}
\]

abbreviation \text{vrel (}\vartheta:: [\text{50}, \text{51}] \text{50}) where
\[
\vartheta: y \mapsto \equiv (y, y') \in \text{unlr (snd F.delta)}
\]

Theorem 1 from Reynolds (1974).

lemma \text{AbsV-aux}:
\[
\text{assumes } \eta: \text{ValF} \cdot f \mapsto \text{unitK} \cdot (\text{ValKF} \cdot f')
\]
\[
\text{shows } \eta: \text{ValF} \cdot (\text{strictify} f) \mapsto \text{unitK} \cdot (\text{ValKF} \cdot (\Lambda x. x \cdot (\Lambda x'. f' \cdot (\text{unitK} \cdot x') \cdot c)))
\]

theorem \text{Theorem1}:
\[
\text{assumes } \forall v. \eta: \varrho \cdot v \mapsto \varrho' \cdot v
\]
\[
\text{shows } \eta: \text{evalD} \cdot e \cdot \varrho \mapsto \text{evalK} \cdot e \cdot \varrho'(\text{proof})
\]

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. \text{'}o ValK.

locale value-retraction =
\[
\text{fixes VtoO :: } 'o \text{ ValK} \rightarrow 'o
\]
\[
\text{fixes OtoV :: } 'o \rightarrow 'o \text{ ValK}
\]
\[
\text{assumes } OV: OtoV \circ VtoO = \text{ID}
\]
sublocale value-retraction < at-least-two-elements VtoO·(ValKN·0) (proof)

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))
| ValTT ⇒ unitK·ValKTT
| ValFF ⇒ unitK·ValKFF
| ValN·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 ⇒ ValTT
| ValKFF ⇒ ValFF
| ValKN·m ⇒ ValN·m)

abbreviation DtoKM ≡ (⨆ i. DtoKM-i i)
abbreviation KMtoD ≡ (⨆ i. KMtoD-i i) (proof)

Lemma 1 from Reynolds (1974).

lemma Lemma1:
η: x ↦ DtoKM·x
η: x ↦ x’ ⇒⇒ x = KMtoD·x’ (proof)

Theorem 2 from Reynolds (1974).

theorem Theorem2: evalD e·ϱ = KMtoD·(evalK e·(DtoKM oo ϱ)) (proof)

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 A small-step (reduction) operational semantics for PCF

A small-step semantics allows us to express more things, like the progress of well-typed programs.

FIXME adjust: This relation is non-deterministic, but only β-reduces terms where the argument is a value. Moreover if we start with a closed term then our values are also closed. So while in general (i.e., for open terms) our substitution operation is wrong and this relation is too big, we show that things work out if we start reducing from a closed term (i.e., a program).

FIXME following Tolmach https://www.cis.upenn.edu/~bcpierce/sf/current/Norm.html we make this relation deterministic. Eases the normalization proof.

inductive

reduction :: \( db \Rightarrow db \Rightarrow \text{bool} \) (- \( \rightarrow \) \([50, 50] \) 50)

where

\( \beta N \): \( \text{DBApp} (DBAbsN u) v \rightarrow u < v/0 > \)

\( \beta V \): \( \text{val} v \Rightarrow \text{DBApp} (DBAbsV u) v \rightarrow u < v/0 > \)

\( f \rightarrow v f' \Rightarrow \text{DBApp} f x \rightarrow v \text{DBApp} f' x \)

\( [] = \text{DBAbsV u} ; x \rightarrow v x' \) \( \Rightarrow \text{DBApp} f x \rightarrow v \text{DBApp} f x' \)

\( \text{DBFix} f \rightarrow v f < \text{DBFix} f / 0 > \)

\( \text{DBCond DBtt t e} \rightarrow v t \)

\( \text{DBCond DBff t e} \rightarrow v e \)

\( \text{DBSucc (DBNum n)} \rightarrow v \text{DBNum} (\text{Suc} n) \)

\( \text{DBPred (DBNum (Suc n))} \rightarrow v \text{DBNum} n \)

\( \text{DBIsZero (DBNum 0)} \rightarrow v \text{DBtt} \)

\( 0 < n \Rightarrow \text{DBIsZero (DBNum n)} \rightarrow v \text{DBff} \)

abbreviation — The transitive, reflexive closure of the reduction relation.

\( \text{reduction-trc :: } db \Rightarrow db \Rightarrow \text{bool} \) (- \( \rightarrow ^* \) \(- [100, 100] \) 100)

where

\( \text{reduction-trc} \equiv \text{rtranclp reduction} \)

declare reduction.intros[introl]

inductive-cases reduction-inv:

\( \text{DBVar v} \rightarrow v t' \)

\( \text{DBApp f} x \rightarrow v t' \)

\( \text{DBAbsN u} \rightarrow v t' \)

\( \text{DBAbsV u} \rightarrow v t' \)

\( \text{DBFix f} \rightarrow v t' \)

\( \text{DBCond i t e} \rightarrow v t' \)

\( \text{DBff} \rightarrow v t' \)

\( \text{DBtt} \rightarrow v t' \)

\( \text{DBNum n} \rightarrow v t' \)

\( \text{DBSucc n} \rightarrow v t' \)

\( \text{DBPred n} \rightarrow v t' \)

\( \text{DBIsZero n} \rightarrow v t' \)

lemma reduction-val:

assumes \( \text{val} v \)

assumes \( v \rightarrow v v' \)

shows \( \text{False} \)

(proof)
lemma reduction-deterministic:
  assumes $t \rightarrow_v t'$
  assumes $t \rightarrow_v t''$
  shows $t'' = t'$
(proof)

6.0.1 Reduction is consistent with evaluation

lemma reduction-eval:
  assumes $t \rightarrow_v t'$
  assumes $t' \downarrow v$
  shows $t \downarrow v$
(proof)

lemma reduction-trc-eval:
  assumes $t \rightarrow_v^* t'$
  assumes $t' \downarrow v$
  shows $t \downarrow v$
(proof)

theorem reduction-trc-val-eval:
  assumes $t \rightarrow_v^* v$
  assumes val $v$
  shows $t \downarrow v$
(proof)

We show the converse (of sorts) using the frame stack machinery of the next section.

7 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


N. Benton, A. Kennedy, L. Beringer, and M. Hofmann. Relational semantics for effect-based


