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.

Contents

1 Introduction 2

2 Pitts’s method for solving recursive domain predicates 2
  2.1 Sets of vectors .................................................. 2
  2.2 Relations between domains and syntax .......................... 4
  2.3 Relations between pairs of domains ............................ 5

3 Logical relations for definability in PCF 5
  3.1 Direct denotational semantics ................................... 6
  3.2 The Y Combinator ................................................ 7
  3.3 Logical relations for definability ............................... 8
  3.4 Parallel OR is not definable .................................... 9
  3.5 Plotkin’s existential quantifier .................................. 11
  3.6 Concluding remarks ............................................. 12

4 Logical relations for computational adequacy 12
  4.1 Direct semantics using de Bruijn notation ....................... 13
  4.2 Operational Semantics ......................................... 15
  4.3 Computational Adequacy ........................................ 16
    4.3.1 Contextual Equivalence .................................... 18

5 Relating direct and continuation semantics 20
  5.1 Logical relation ................................................ 21
  5.2 A retraction between the two definitions ....................... 22

6 A small-step (reduction) operational semantics for PCF 24
  6.0.1 Reduction is consistent with evaluation ..................... 25
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 \( \bot \) and is closed under countable chains:

\[
\text{definition admS} ::= \text{`a::pcpo set set where} \\
\text{admS} \equiv \{ R :: `a set. \bot \in R \wedge \text{adm} (\lambda x. x \in R) \}
\]

\[
\text{typedef (`a::pcpo) admS = } \{ x:`a::pcpo set , x \in admS \}
\]

\[
\text{morphisms unlr mklr unfolding admS-def by fastforce}
\]

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.

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.

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.

locale DomSol =
fixes F :: ’a::order × ’a::order ⇒ ’a
assumes monoF : mono F
begin

definition sym-lr :: ’a dual × ’a ⇒ ’a dual × ’a
where

sym-lr = (λ(rm, rp). (dual (F (dual rp, undual rm)), F (rm, rp))

lemma sym-lr-mono:
mono sym-lr

proof

fix x y :: ’a dual × ’a

obtain x1 x2 y1 y2 where [simp]; x = (x1, x2) y = (y1, y2)

by (cases x, cases y)

assume x ≤ y

with monoF have F x ≤ F y ..

from x ≤ y have (dual y2, undual y1) ≤ (dual x2, undual x1)

by (simp-all add: dual-less-eq-iff)

with monoF have F (dual y2, undual y1) ≤ F (dual x2, undual x1) ..

with F x ≤ F y show sym-lr x ≤ sym-lr y

by (simp add: sym-lr-def)

ged

end
locale DomSolV = DomSol F :: (′i::type ⇒ ′d::pcpo) if for F +
  fixes δ :: (′d::pcpo ⇒ ′d) ⇒ ′d ⇒ ′d
  assumes min-inv-ID: fix-δ = ID
  assumes eRSV-deltaF:
  \( \bigwedge (e :: ′d ⇒ ′d) (R :: (′i ⇒ ′d) admS dual) (S :: (′i ⇒ ′d) admS).
  eRSV e R S \implies eRSV (δ ∗ e) (dual (F (dual S, undual R))) (F (R, S)) \) From these assumptions we can show that there is a unique object that is a solution to the recursive equation specified by F.
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.
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 \}
 morphisms unsynlr mksynlr unfolding synlr-def by fastforce
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 = \forall (d, a) ∈ unsynlr (undual R). (e, d, a) ∈ unsynlr S
locale DomSolSyn = 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: \( \bigwedge r. δ ∗ r ∗ ⊥ = ⊥ \)
  assumes eRS-deltaF:
  \( \bigwedge (e :: ′d ⇒ ′d) (R :: (′d, ′a) synlr dual) (S :: (′d, ′a) synlr).
  [ e ∗ ⊥ = ⊥; eRS e R S ] \implies eRS (δ ∗ e) (dual (F (dual S, undual R))) (F (R, S)) \)
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.

**abbreviation**

$$eRSP : \left((\text{'am} : \text{pcpo} \rightarrow \text{'am}) \times (\text{'av} : \text{pcpo} \rightarrow \text{'av})\right)$$

$$\Rightarrow (\text{'bm} : \text{pcpo} \rightarrow \text{'bm}) \times (\text{'bv} : \text{pcpo} \rightarrow \text{'bv})$$

$$\Rightarrow (\text{'am} \times \text{'bm}) \text{admS} \times (\text{'av} \times \text{'bv}) \text{admS} \text{ dual}$$

$$\Rightarrow (\text{'am} \times \text{'bm}) \text{admS} \times (\text{'av} \times \text{'bv}) \text{admS}$$

$$\Rightarrow \text{bool}$$

**where**

$$eRSP \text{ ea eb R S} \equiv$$

$$\forall (\text{am, bm}) \in \text{unlr (fst (undual R))}. (\text{fst ea-am, fst eb-bm}) \in \text{unlr (fst S)}$$

$$\land (\text{av, bv}) \in \text{unlr (snd (undual R))}. (\text{snd ea-av, snd eb-bv}) \in \text{unlr (snd S)}$$

**locale** $\text{DomSolP} = \text{DomSol F} : (\text{'am} : \text{pcpo, \text{'bm} : \text{pcpo, \text{'av} : \text{pcpo, \text{'bv} : \text{pcpo}}})$ $\text{if-pair for F +}$

**fixes**

$$\text{ad} : ((\text{'am} \rightarrow \text{'am}) \times (\text{'av} \rightarrow \text{'av})) \rightarrow ((\text{'am} \rightarrow \text{'am}) \times (\text{'av} \rightarrow \text{'av}))$$

$$\text{bd} : ((\text{'bm} \rightarrow \text{'bm}) \times (\text{'bv} \rightarrow \text{'bv})) \rightarrow ((\text{'bm} \rightarrow \text{'bm}) \times (\text{'bv} \rightarrow \text{'bv}))$$

**assumes**

$$\text{ad-ID: fix-ad = (ID, ID)}$$

$$\text{bd-ID: fix-bd = (ID, ID)}$$

$$\text{ad-strict:} \land r. \text{fst (ad-r)} \downarrow = \bot \land r. \text{snd (ad-r)} \downarrow = \bot$$

$$\text{bd-strict:} \land r. \text{fst (bd-r)} \downarrow = \bot \land r. \text{snd (bd-r)} \downarrow = \bot$$

**assumes**

$$eRSP-\text{deltaF} :$$

$$\left( eRSP \text{ ea eb R S; fst ea-\downarrow = \bot; snd ea-\downarrow = \bot; fst eb-\downarrow = \bot; snd eb-\downarrow = \bot \right)$$

$$\Rightarrow eRSP (\text{ad-\text{ea}}) (\text{bd-\text{eb}}) (\text{\text{\text{true}} (F \text{ (\text{\text{true}} S, \text{undual R}))}) (F \text{ (R, S))})$$

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 (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
```

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'

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

type-synonym EnvD = ValD Env

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

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

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, \textit{fix} is definable in untyped PCF minus the \textit{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** $\text{fixD} :: \text{ValD} \to \text{ValD}$ where
\[
\text{fixD} \equiv \Lambda (\text{ValF}. f). \text{fix}.f
\]

**lemma** $Y$: $[\text{Ycomb}]_\rho = \text{ValF} \cdot \text{fixD}$

### 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 *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 $\text{ValD}$ 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** $\text{logical-relation} :: (\forall i :: \text{type} \Rightarrow \text{ValD}) \text{ set} \Rightarrow \text{bool}$ where
\[
\text{logical-relation } R \equiv \\
(\forall fs \in R. \forall xs \in R. (\lambda j. \text{appF} \cdot (fs j) \cdot (xs j)) \in R) \\
\land (\forall fs. (\forall xs \in R. (\lambda j. \text{strictify} \cdot (\text{appF} \cdot (fs j)) \cdot (xs j)) \in R) \\
\land (\forall fs. (\forall xs \in R. (\lambda j. \text{strictify} \cdot (\text{appF} \cdot (fs j)) \cdot (xs j)) \in R) \\
\land (\forall xs \in R. (\lambda j. \text{fixD} \cdot (xs j)) \in R) \\
\land (\forall cs \in R. \forall ts \in R. \forall es \in R. (\lambda j. \text{cond} \cdot (cs j) \cdot (ts j) \cdot (es j)) \in R) \\
\land (\forall xs \in R. (\lambda j. \text{pred} \cdot (xs j)) \in R) \\
\land (\forall xs \in R. (\lambda j. \text{isZero} \cdot (xs j)) \in R)
\]

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

**definition** $\text{PCF-consts-rel} :: (\forall i :: \text{type} \Rightarrow \text{ValD}) \text{ set} \Rightarrow \text{bool}$ where
\[
\text{PCF-consts-rel } R \equiv \\
(\bot \in R) \\
\land (\lambda i. \text{ValTT}) \in R \\
\land (\lambda i. \text{ValFF}) \in R \\
\land (\forall n. (\lambda i. \text{ValN} \cdot n) \in R)
\]

**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 $M$. 

8
lemma lr-fundamental:
assumes lr: PCF-lr R
assumes ϱ: ∀v. (λi. ϱ i ⋅ v) ∈ R
shows (λi. [M] (ϱ i)) ∈ R

We can use this result to show that there is no PCF term that maps the vector args ∈ R to result / ∈ R for some logical relation R. If we further show that there is a function f in ValD such that f args = result then we can conclude that f is not definable.

abbreviation appFLv :: ValD ⇒ (′i::type ⇒ ValD) list ⇒ (′i ⇒ ValD)
where
appFLv f args ≡ (λi. foldl (λf x. appF · f · (x i)) f args)

lemma lr-appFLv:
assumes lr: logical-relation R
assumes f: (λi::′i::type. f) ∈ R
assumes args: set args ⊆ R
shows appFLv f args ∈ R

corollary not-definable:
fixes R :: (′i::type ⇒ ValD) set
fixes args :: (′i ⇒ ValD) list
fixes result :: (′i ⇒ ValD)
assumes lr: PCF-lr R
assumes args: set args ⊆ R
assumes result: result / ∈ R
shows ¬(∃(f::ValD). definable f ∧ appFLv f args = result)

3.4 Parallel OR is not definable

We show that parallel-or is not λ-definable following Sieber (1992) and Stoughton (1993).
Parallel-or is similar to the familiar short-circuiting or except that if the first argument is ⊥ and the second one is ValTT, we get ValTT (and not ⊥). It is continuous and then have included in the ValD domain.

definition por :: ValD ⇒ ValD ⇒ ValD (- por - [31,30] 30) where
x por y ≡
  if x = ValTT then ValTT
  else if y = ValTT then ValTT
  else if (x = ValFF ∧ y = ValFF) then ValFF else ⊥

The defining properties of parallel-or.

lemma POR-simps [simp]:
(ValTT por y) = ValTT
(x por ValTT) = ValTT
(ValFF por ValFF) = ValFF
(ValFF por ⊥) = ⊥
(ValFF por ValN·n) = ⊥
(ValFF por ValF·f) = ⊥
(⊥ por ValFF) = ⊥
(ValN·n por ValFF) = ⊥
(ValF·f por ValFF) = ⊥
We need three-element vectors.

datatype Three = One | Two | Three

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

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

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 \( \Rightarrow \) ValD) lf-rep
where
POR-base-lf-rep \( \equiv \lambda (mR, pR). \{ (\lambda i. \text{ValTT}) \} \cup \{ (\lambda i. \text{ValFF}) \} \) — \( x = y = z \) for bools
\( \cup (\bigcup n. \{ (\lambda i. \text{ValN} \cdot n) \}) \) — \( x = y = z \) for numerals
\( \cup \{ f . f \text{ One} = \bot \} \) — \( x = \bot \)
\( \cup \{ f . f \text{ Two} = \bot \} \) — \( y = \bot \)

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 \( \Rightarrow \) ValD) lf-rep
where
fn-lf-rep \( \equiv \lambda (mR, pR). \{ \lambda i. \text{ValF} \cdot (fs i) \} \mid \forall xs \in \text{unlr} (\text{undual mR}). (\lambda j. (fs j) \cdot (xs j)) \in \text{unlr} pR \}

definition POR-lf-rep :: (Three \( \Rightarrow \) ValD) lf-rep where
POR-lf-rep \( R \equiv \text{POR-base-lf-rep } R \cup \text{fn-lf-rep } R \)

abbreviation POR-lf \( \equiv \lambda r. \text{mklr } (\text{POR-lf-rep } r) \)

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 S'
shows eRSV (ValD-copy-rec-e) (\text{dual } (\text{POR-lf } (\text{dual } S', \text{undual } R'))) (\text{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 (\text{unlr } \text{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 ≡ \( \lambda i. \text{case } i \text{ of One } \Rightarrow \text{ValTT } \mid \text{Two } \Rightarrow \bot \mid \text{Three } \Rightarrow \text{ValFF} \)

**definition** POR-arg2-rel where
POR-arg2-rel ≡ \( \lambda i. \text{case } i \text{ of One } \Rightarrow \bot \mid \text{Two } \Rightarrow \text{ValTT } \mid \text{Three } \Rightarrow \text{ValFF} \)

**definition** POR-result-rel where
POR-result-rel ≡ \( \lambda i. \text{case } i \text{ of One } \Rightarrow \text{ValTT } \mid \text{Two } \Rightarrow \text{ValTT } \mid \text{Three } \Rightarrow \text{ValFF} \)

**lemma** lr-POR-arg1-rel: POR-arg1-rel ∈ unlr POR

**unfolding** POR-arg1-rel-def by auto

**lemma** lr-POR-arg2-rel: POR-arg2-rel ∈ unlr POR

**unfolding** POR-arg2-rel-def by auto

**lemma** lr-POR-result-rel: POR-result-rel /∈ unlr POR

Parallel-or satisfies these tests:

**theorem** POR-sat:
appFLv (ValF·(\( \lambda x. \text{ValF}·(\lambda y. x \text{ por } y) \))) [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 \( \neg(\exists f. \text{definable } f \land \text{appFLv } f [\text{POR-arg1-rel, POR-arg2-rel} ] = \text{POR-result-rel}) \)

apply (rule not-definable[where \( R=\text{unlr } POR.\text{delta} \)])

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

**definition** plotkin-exists :: ValD ⇒ ValD where
plotkin-exists \( f \equiv \)
if (appF·f·\bot = ValFF)
then ValFF
else if (\( \exists n. \text{appF}·f·n = \text{ValTT} \)) then ValTT else \( \bot \)

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 \textit{PE-arg-rel} where
\begin{align*}
\text{PE-arg-rel} & \equiv \lambda i. \text{ValF} \cdot (\text{case } i \text{ of } 0 \Rightarrow (\Lambda - \text{ValFF}) \\
& \quad | \ Suc n \Rightarrow (\Lambda (\text{ValN} \cdot x). \text{if } x = \text{Suc } n \text{ then ValTT else } \bot))
\end{align*}

definition \textit{PE-result-rel} where
\begin{align*}
\text{PE-result-rel} & \equiv \lambda i. \text{case } i \text{ of } 0 \Rightarrow \text{ValFF} \\
& \quad | \ Suc n \Rightarrow \text{ValTT}
\end{align*}

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:

\textbf{Theorem} pe-sat:
\begin{align*}
\text{appFLv } (\text{ValF} \cdot (\Lambda x. \text{plotkin-exists } x)) [\text{PE-arg-rel}] & = \text{PE-result-rel} \\
\text{unfolding } \text{PE-arg-rel-def} & \text{ PE-result-rel-def} \\
\text{by } (\text{clarsimp simp: fun-eq-iff split: nat.splits})
\end{align*}

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

\textbf{Definition} \textit{PE-base-lf-rep :: (nat } \Rightarrow \text{ ValD) lf-rep where}
\begin{align*}
\text{PE-base-lf-rep} & \equiv \lambda (m_R, p_R).
\{ \bot \} \\
& \quad \cup \{ \lambda i. \text{ValTT} \} \cup \{ \lambda i. \text{ValFF} \} \quad \text{— for bools}
\cup (\bigcup n. \{ (\lambda i. \text{ValN} \cdot n) \}) \quad x = y = z \text{ for numerals}
\cup \{ f . f \, 1 = \bot \lor f \, 2 = \bot \} \quad \text{— Vectors that diverge on one or two.}
\end{align*}

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

\textbf{Definition} \textit{PE-lf-rep :: (nat } \Rightarrow \text{ ValD) lf-rep where}
\begin{align*}
\text{PE-lf-rep } R & \equiv \text{PE-base-lf-rep } R \cup \text{fn-lf-rep } R
\end{align*}

\textbf{Abbreviation} \textit{PE-lf } \equiv \lambda r. \text{mklr } (\text{PE-lf-rep } r)

The solution satisfies the expectations of the fundamental theorem:

\textbf{Lemma} PCF-lr-PE-delta: PCF-lr (unlr \text{ PE.delta})
\textbf{Lemma} lr-PE-arg-rel: PE-arg-rel \in unlr \text{ PE.delta}
\textbf{Lemma} lr-PE-result-rel: PE-result-rel \notin unlr \text{ PE.delta}
\textbf{Theorem} PE-is-not-definable: \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 \textit{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 \textit{seq} on these objects (given \textit{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 α-equivalent terms, as we would like our operational semantics to identify 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 \texttt{db} =
\begin{align*}
\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
\end{align*}

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.

\begin{verbatim}
fun lift :: \texttt{db} \Rightarrow \texttt{nat} \Rightarrow \texttt{db}
where
lift (DBVar i) k = DBVar (\text{if } i < k \text{ then } i \text{ else } (i + 1))
\end{verbatim}

\begin{verbatim}
where
\text{DBVar} \ i \ \text{<s/k>} =
\begin{align*}
(i < k \text{ then } \text{DBVar} (i - 1) \text{ else } i = k \text{ then } s \text{ else } \text{DBVar} i)
\end{align*}
\end{verbatim}

\begin{verbatim}
\text{DBAbsN} \ t \ \text{<s/k>} = \text{DBAbsN} \ (\text{lift } s / k + 1)
\end{verbatim}

\begin{verbatim}
\text{DBAbsV} \ t \ \text{<s/k>} = \text{DBAbsV} \ (\text{lift } s / k + 1)
\end{verbatim}

\begin{verbatim}
\text{DBApp} \ s \ t \ \text{<s/k>} = \text{DBApp} \ (\text{lift } s k) \ (\text{lift } t k)
\end{verbatim}

\begin{verbatim}
\text{DBFix} \ e \ \text{<s/k>} = \text{DBFix} \ (\text{lift } e (k + 1))
\end{verbatim}

\begin{verbatim}
\text{DBCond} c \ t \ e \ \text{<s/k>} = \text{DBCond} \ (\text{lift } c k) \ (\text{lift } t k) \ (\text{lift } e k)
\end{verbatim}

\begin{verbatim}
\text{DBSucc} \ e \ \text{<s/k>} = \text{DBSucc} \ (\text{lift } e k)
\end{verbatim}

\begin{verbatim}
\text{DBPred} \ e \ \text{<s/k>} = \text{DBPred} \ (\text{lift } e k)
\end{verbatim}

\begin{verbatim}
\text{DBIsZero} \ e \ \text{<s/k>} = \text{DBIsZero} \ (\text{lift } e k)
\end{verbatim}

\begin{verbatim}
lift x \ k = x
\end{verbatim}

\begin{verbatim}
fun subst :: \texttt{db} \Rightarrow \texttt{db} \Rightarrow \texttt{var} \Rightarrow \texttt{db} \ (\text{<s/k>} [300, 0, 0] 300)
where
\text{DBVar} \ i \ <s/k> =
\begin{align*}
\text{DBAbsN} \ t \ <s/k> = \text{DBAbsN} \ (\text{lift } s / k + 1)
\end{align*}
\end{verbatim}

\begin{verbatim}
\text{DBAbsV} \ t \ <s/k> = \text{DBAbsV} \ (\text{lift } s / k + 1)
\end{verbatim}

\begin{verbatim}
\text{DBApp} \ s \ t \ <s/k> = \text{DBApp} \ (\text{lift } s k) \ (\text{lift } t k)
\end{verbatim}

\begin{verbatim}
\text{DBFix} \ e \ <s/k> = \text{DBFix} \ (\text{lift } e (k + 1))
\end{verbatim}

\begin{verbatim}
\text{DBCond} c \ t \ e \ <s/k> = \text{DBCond} \ (\text{lift } c k) \ (\text{lift } t k) \ (\text{lift } e k)
\end{verbatim}

\begin{verbatim}
\text{DBSucc} \ e \ <s/k> = \text{DBSucc} \ (\text{lift } e k)
\end{verbatim}

\begin{verbatim}
\text{DBPred} \ e \ <s/k> = \text{DBPred} \ (\text{lift } e k)
\end{verbatim}

\begin{verbatim}
\text{DBIsZero} \ e \ <s/k> = \text{DBIsZero} \ (\text{lift } e k)
\end{verbatim}

\begin{verbatim}
lift x \ k = x
\end{verbatim}
We elide the standard lemmas about these operations.

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

fun
freedb :: db ⇒ var ⇒ bool

where
freedb (DBVar j) k = (j = k)
freedb (DBAbsN s) k = freedb s (k + 1)
freedb (DBAbsV s) k = freedb s (k + 1)
freedb (DBApp s t) k = (freedb s k ∨ freedb t k)
freedb (DBFix e) k = freedb e (Suc k)
freedb (DBCond c t e) k = (freedb c k ∨ freedb t k ∨ freedb e k)
freedb (DBSucc e) k = freedb e k
freedb (DBPred e) k = freedb e k
freedb (DBIsZero e) k = freedb e k
freedb - - = False

Programs are closed expressions.

definition closed :: db ⇒ bool where
closed e ≡ ∀ i. ¬ 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
eenv-empty-db ≡ ⊥

definition env-ext-db :: 'a → 'a Env → 'a Env where
eenv-ext-db ≡ Λ x g v. (case v of 0 ⇒ x | Suc v' ⇒ g·v')

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·(strictify·(Λ x. evalDdb e·(env-ext-db·x·g))))
evalDdb (DBFix e) = (Λ g. ⊥)
evalDdb (DBCond c t e) = (Λ g. cond·(evalDdb c·g)·(evalDdb t·g)·(evalDdb e·g))
evalDdb (DBNum n) = (Λ g. ValN·n)
evalDdb (DBSucc e) = (Λ g. succ·(evalDdb e·g))
evalDdb (DBPred e) = (Λ g. pred·(evalDdb e·g))
evalDdb (DBIsZero e) = (Λ g. isZero·(evalDdb e·g))
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.

\textit{primrec} \texttt{index :: var list ⇒ var ⇒ nat ⇒ nat} \texttt{where}

\begin{itemize}
  \item \texttt{index [] v n = n}
  \item \texttt{index (h # t) v n = (if v = h then n else index t v (Suc n))}
\end{itemize}

\textit{primrec} \texttt{transdb :: expr ⇒ var list ⇒ db}

\texttt{where}

\begin{itemize}
  \item \texttt{transdb (Var i) Γ = DBVar (index Γ i 0)}
  \item \texttt{transdb (App t1 t2) Γ = DBAp p (transdb t1 Γ) (transdb t2 Γ)}
  \item \texttt{transdb (AbsN v t) Γ = DBAbsN (transdb t (v # Γ))}
  \item \texttt{transdb (AbsV v t) Γ = DBAbsV (transdb t (v # Γ))}
  \item \texttt{transdb (Diverge) Γ = DBDiverge}
  \item \texttt{transdb (Fix v e) Γ = DBFix (transdb e (v # Γ))}
  \item \texttt{transdb (tt) Γ = DBtt}
  \item \texttt{transdb (ff) Γ = DBff}
  \item \texttt{transdb (Cond c t e) Γ = DBCond (transdb c Γ) (transdb t Γ) (transdb e Γ)}
  \item \texttt{transdb (Num n) Γ = (DBNum n)}
  \item \texttt{transdb (Suc c) Γ = DBSuc c (transdb e Γ)}
  \item \texttt{transdb (Pred c) Γ = DBPred (transdb e Γ)}
  \item \texttt{transdb (IsZero e) Γ = DBIsZero (transdb e Γ)}
\end{itemize}

This semantics corresponds with the direct semantics for named expressions.

\textit{lemma} \texttt{evalD-evalDb:}

\texttt{assumes free e []}

\texttt{shows [e]ϱ = evalDb (transdb e []) ϱ}

\texttt{using assms by (simp add: evalD-evalDb-open)}

Conversely, all de Bruijn expressions have named equivalents.

\textit{primrec} \texttt{transdb-inv :: db ⇒ (var ⇒ var) ⇒ var ⇒ var ⇒ expr}

\texttt{where}

\begin{itemize}
  \item \texttt{transdb-inv (DBVar i) Γ c k = Var (Γ i)}
  \item \texttt{transdb-inv (DBApp t1 t2) Γ c k = App (transdb-inv t1 Γ c k) (transdb-inv t2 Γ c k)}
  \item \texttt{transdb-inv (DBAbsN e) Γ c k = AbsN (c + k) (transdb-inv e (case-nat (c + k) Γ) c (k + 1))}
  \item \texttt{transdb-inv (DBAbsV e) Γ c k = AbsV (c + k) (transdb-inv e (case-nat (c + k) Γ) c (k + 1))}
  \item \texttt{transdb-inv (DBDiverge) Γ c k = Diverge}
  \item \texttt{transdb-inv (DBFix e) Γ c k = Fix (c + k) (transdb-inv e (case-nat (c + k) Γ) c (k + 1))}
  \item \texttt{transdb-inv (DBtt) Γ c k = tt}
  \item \texttt{transdb-inv (DBff) Γ c k = ff}
  \item \texttt{transdb-inv (DBCond i t e) Γ c k =}
    \begin{itemize}
      \item \texttt{Cond (transdb-inv i Γ c k) (transdb-inv t Γ c k) (transdb-inv e Γ c k)}
    \end{itemize}
  \item \texttt{transdb-inv (DBNum n) Γ c k = (Num n)}
  \item \texttt{transdb-inv (DBSuc c) Γ c k = Succ (transdb-inv e Γ c k)}
  \item \texttt{transdb-inv (DBPred c) Γ c k = Pred (transdb-inv e Γ c k)}
  \item \texttt{transdb-inv (DBIsZero e) Γ c k = IsZero (transdb-inv e Γ c k)}
\end{itemize}

\textit{lemma} \texttt{transdb-inv:}
assumes closed e
shows transdb (transdb-inv e Γ c k) Γ′ = 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<DBFixx P/0>⇓V ⇒ DBFixx P⇓V
  evalOP-tt[intro]: DBtt⇓DBtt
  evalOP-ff[intro]: DBff⇓DBff
  evalOP-CondTT[intro]: [ [C⇓DBtt; T⇓V] ] ⇒ DBCond C T E⇓V
  evalOP-CondFF[intro]: [ [C⇓DBff; E⇓V] ] ⇒ DBCond C T E⇓V
  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 Pˌϱ = evalDdb Vˌϱ

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 isPORdb e ≡ closed e
  ∧ DBApp (DBApp e DBtt) DBDiverge⇓DBtt
  ∧ DBApp (DBApp e DBDiverge) DBtt⇓DBtt
  ∧ DBApp (DBApp e DBff) DBff⇓DBff
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 \( \text{ValD} \) 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** \( \text{Prog} = \{ \text{P. closed } P \} \)

** morphisms** \( \text{unProg mkProg} \) by fastforce

**definition**
\[
\text{ca-lf-rep :: (ValD, Prog) synlf-rep}
\]
\[
\text{where}
\]
\[
\text{ca-lf-rep} \equiv \lambda (rm, rp). \bigcup \{ (d, P) \mid d P.
\begin{align*}
& (\exists n. d = \text{ValN} \cdot n \land \text{unProg } P \downarrow \text{DBNum } n) \\
& \lor (d = \text{ValTT} \land \text{unProg } P \downarrow \text{DBtt}) \\
& \lor (d = \text{ValFF} \land \text{unProg } P \downarrow \text{DBff}) \\
& \lor (\exists f M. d = \text{ValF} \cdot f \land \text{unProg } P \downarrow \text{DBAbsN } M)
\begin{align*}
& \land (\forall (x, X) \in \text{unsynlr } (\text{undual } rm). (f \cdot x, \text{mkProg } (M < \text{unProg } X / \theta >)) \in \text{unsynlr } rp))
\end{align*}
\]
\[
\lor (\exists f M. d = \text{ValF} \cdot f \land \text{unProg } P \downarrow \text{DBAbsV } M \land f \cdot \bot = \bot \\
\begin{align*}
& \land (\forall (x, X) \in \text{unsynlr } (\text{undual } rm). \forall V. \text{unProg } X \downarrow V 
\end{align*}
\begin{align*}
& \rightarrow (f \cdot x, \text{mkProg } (M < V / \theta >)) \in \text{unsynlr } rp)) \}
\end{align*}
\]
**abbreviation** \( \text{ca-lr :: (ValD, Prog) synlf where} \)
\[
\text{ca-lr} \equiv \lambda r. \text{mksynlr } (\text{ca-lf-rep } r)
\]

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

**interpretation** \( \text{ca} : \text{DomSolSyn } \text{ca-lr } \text{ValD-copy-rec} \)

**apply** standard

**apply** (rule mono-ca-lr)

**apply** (rule ValD-copy-ID)

**apply** simp

**apply** (erule (1) min-inv-ca-lr)

**done**

**definition** \( \text{ca-lr-syn :: ValD } \Rightarrow \text{db } \Rightarrow \text{bool} \ (\neg \circ [80,80] \ 80) \) where
\[
d \circ P \equiv (d, P) \in \{ (x, \text{unProg } Y) \mid x Y. (x, Y) \in \text{unsynlr } \text{ca.delta} \}
\]

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 ≤ i then Γ (i – k) else DBVar i)  
closing-subst (DBApp t a) Γ k = DBApp (closing-subst t Γ k) (closing-subst u Γ k)  
closing-subst (DBAbsN 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)  
closing-subst (DBSucc e) Γ k = DBSucc (closing-subst e Γ k)  
closing-subst (DBPred e) Γ k = DBPred (closing-subst e Γ k)  
closing-subst (DBIsZero e) Γ k = DBIsZero (closing-subst e Γ k)  
closing-subst x Γ k = x  

We can show it has the expected properties when all terms in Γ are closed.

The key lemma is shown by induction over e for arbitrary environments (Γ and ϱ):

lemma ca-open:  
assumes ∀ v. freedb e v −→ ϱ·v ≫ Γ v ∧ closed (Γ v)  
shows evalDdb e·ϱ ≪ closing-subst e Γ 0

lemma ca-closed:  
assumes closed e  
shows evalDdb e·ϱ ≪ closing-subst e Γ 0

using ca-open[where e=e and ϱ=env-empty-db] assms  
by (simp add: closed-def)

theorem ca:  
assumes nb: evalDdb e·env-empty-db ≠ ⊥  
assumes closed e  
shows ∃ V. e ⊣− 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 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 ⇒ db ⇒ db ((<->) [300, 0] 300) where  
C<e> ≡ closing-subst C (λ 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

\textit{have-the-same-form} :: \(db \Rightarrow db \Rightarrow bool (\sim - [50,50] 50)\)

\textbf{where}

\begin{align*}
DBAbsN e & \sim DBAbsN e' \\
DBAbsN e & \sim DBAbsV e' \\
DBAbsV e & \sim DBAbsN e' \\
DBAbsV e & \sim DBAbsV e' \\
DBFix e & \sim DBFix e' \\
DBtt & \sim DBtt \\
DBff & \sim DBff \\
DBNum n & \sim DBNum n
\end{align*}

A program \(e_2\) \textit{refines} the program \(e_1\) if it converges in context at least as often. This is a preorder on programs.

\textbf{definition}

\textit{refines} :: \(db \Rightarrow db \Rightarrow bool (\sim - [50,50] 50)\)

\textbf{where}

\begin{align*}
e_1 \triangleq e_2 & \equiv \forall C. \exists V1. C < e_1 > \Downarrow V1 \longrightarrow (\exists V2. C < e_2 > \Downarrow V2 \wedge V1 \sim V2)
\end{align*}

Contextually-equivalent programs refine each other.

\textbf{definition}

\textit{contextually-equivalent} :: \(db \Rightarrow db \Rightarrow bool (\sim \sim)\)

\textbf{where}

\begin{align*}
e_1 \approx e_2 & \equiv e_1 \triangleq e_2 \wedge e_2 \triangleq e_1
\end{align*}

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

\textbf{theorem} computational-adequacy:

\begin{align*}
\text{assumes 1: } & \text{closed } e_1 \\
\text{assumes 2: } & \text{closed } e_2 \\
\text{assumes D: } & \text{evalDdb } e_1 \cdot \text{env-empty-db} = \text{evalDdb } e_2 \cdot \text{env-empty-db} \\
\text{shows } & e_1 \approx e_2
\end{align*}

This gives us a sound but incomplete method for demonstrating contextual equivalence. We expect this result is useful for showing contextual equivalence for \textit{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 \((\text{ValK} K, \text{ValK} K) \to \text{ValK} K\) as our language includes call-by-name.

type-synonym \((\text{ValK} K, \text{ValK} K) \to \text{ValK} K\)

domain \((\text{ValK} K)\)

\begin{align*}
\text{ValK} K &= (\text{lzy appK} : (\text{ValK} K, \text{ValK} K) \to (\text{ValK} K, \text{ValK} K)) \\
&| \text{ValKTT} | \text{ValKFF}
\end{align*}

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

definition unitK :: \((\text{ValK} K)\)

\begin{align*}
\text{unitK} &\equiv \Lambda a. \Lambda c. \Lambda a. \Lambda c. c \cdot a
\end{align*}

definition bindK :: \((\text{ValKM} K) \to (\text{ValK} K \to \text{ValKM} K) \to \text{ValKM} K\)

\begin{align*}
\text{bindK} &\equiv \Lambda m k. \Lambda c. m \cdot \Lambda a. k \cdot a \cdot c
\end{align*}

definition appKM :: \((\text{ValKM} K) \to \text{ValKM} K\)

\begin{align*}
\text{appKM} &\equiv \Lambda fK xK. \text{bindK} \cdot fK \cdot (\Lambda f. f \cdot xK)
\end{align*}

The interpretations of the constants.

definition condK :: \((\text{ValKM} K) \to \text{ValKM} K \to \text{ValKM} K \to \text{ValKM} K\)

\begin{align*}
\text{condK} &\equiv \Lambda iK tK eK. \text{bindK} \cdot iK \cdot \Lambda i. \text{case i of ValKf} \Rightarrow \bot | \text{ValKTT} \Rightarrow tK | \text{ValKFF} \Rightarrow eK | \text{ValKN} \Rightarrow \bot
\end{align*}

definition succK :: \((\text{ValKM} K)\)

\begin{align*}
\text{succK} &\equiv \Lambda nK. \text{bindK} \cdot nK \cdot (\Lambda (\text{ValKN} n). \text{unitK} \cdot (\text{ValKN} (n + 1)))
\end{align*}

definition predK :: \((\text{ValKM} K)\)

\begin{align*}
\text{predK} &\equiv \Lambda nK. \text{bindK} \cdot nK \cdot (\Lambda (\text{ValKN} n). \text{case} n \text{ of 0} \Rightarrow \bot | \text{Suc} n \Rightarrow \text{unitK} \cdot (\text{ValKN} n))
\end{align*}

definition isZeroK :: \((\text{ValKM} K)\)

\begin{align*}
\text{isZeroK} &\equiv \Lambda nK. \text{bindK} \cdot nK \cdot (\Lambda (\text{ValKN} n). \text{unitK} \cdot (\text{if} \ n = 0 \ \text{then} \ \text{ValKTT} \ \text{else} \ \text{ValKFF}))
\end{align*}

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 \((\text{ValKM Env})\)

20
Theorem 1.1

\[
\text{valK} \mapsto \text{expr} \Rightarrow 'o \text{EnvK} \rightarrow 'o \text{ValKM}
\]

where

\[
\begin{align*}
\text{valK} (\text{Var} v) &= (\Lambda \, g. \, g \cdot v) \\
\text{valK} (\text{App} f \, x) &= (\Lambda \, g. \, \text{appKM}(\text{valK} \, f \cdot g) \cdot (\text{valK} \, x \cdot g)) \\
\text{valK} (\text{Abs} \, \Gamma \, v \, e) &= (\Lambda \, g. \, \text{unitK} \cdot (\text{ValKF} \cdot (\Lambda \, x. \, \text{valK} \, e \cdot (\text{env-ext} \cdot v \cdot x \cdot g)))) \\
\text{valK} (\text{Abs} \, \Gamma \, v \, e) &= (\Lambda \, g. \, \text{unitK} \cdot (\text{ValKF} \cdot (\Lambda \, x. \, \text{valK} \, e \cdot (\text{env-ext} \cdot v \cdot (\text{unitK} \cdot x \cdot \_ \cdot g) \cdot g)))) \\
\text{valK} (\text{Diverge}) &= (\Lambda \, g. \, \bot) \\
\text{valK} (\text{Fix} \, v \, e) &= (\Lambda \, g. \, \mu \cdot x. \, \text{valK} \, e \cdot (\text{env-ext} \cdot v \cdot x \cdot g)) \\
\text{valK} (tt) &= (\Lambda \, g. \, \text{unitK} \cdot \text{ValKTT}) \\
\text{valK} (ff) &= (\Lambda \, g. \, \text{unitK} \cdot \text{ValKK}) \\
\text{valK} (\text{Cond} \, i \, t \, e) &= (\Lambda \, g. \, \text{condK} \cdot (\text{valK} \cdot \_ \cdot \text{g}) \cdot (\text{valK} \cdot t \cdot \text{g}) \cdot (\text{valK} \cdot e \cdot \text{g})) \\
\text{valK} (\text{Succ} \, e) &= (\Lambda \, g. \, \text{succK} \cdot (\text{valK} \cdot e \cdot \text{g})) \\
\text{valK} (\text{Pred} \, e) &= (\Lambda \, g. \, \text{predK} \cdot (\text{valK} \cdot e \cdot \text{g})) \\
\text{valK} (\text{IsZero} \, e) &= (\Lambda \, g. \, \text{isZeroK} \cdot (\text{valK} \cdot e \cdot \text{g}))
\end{align*}
\]

To establish the chain completeness (admissibility) of our logical relation, we need to show that \(\text{unitK}\) is an order monic, i.e., if \(\text{unitK} \cdot x \subseteq \text{unitK} \cdot y\) then \(x \subseteq y\). 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:

\[
\begin{align*}
\text{locale} \atleasttwoelements &= \\
\text{fixes} \text{some-non-bottom-element} &= \text{'o:domain} \\
\text{assumes} \text{some-non-bottom-element} &= \text{some-non-bottom-element} \neq \bot
\end{align*}
\]

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

\[
\begin{align*}
\text{lemma} \ contbelow &\ [\text{simp}, \text{cont2cont}] \\
\text{cont} &\ (\lambda x::'a::pcpo. \text{if} \ x \subseteq d \ \text{then} \ \bot \ \text{else} \ c)
\end{align*}
\]

\[
\begin{align*}
\text{lemma} \ \text{in} \atleasttwoelements \ &\ \text{belowmonicunitK} \ [\text{intro}, \text{simp}] \\
\text{belowmoniccfun} &\ \text{(unitK} :: \text{'}o \text{ValK} \rightarrow 'o \text{ValKM})
\end{align*}
\]

\[
\begin{align*}
\text{proof} \ (\text{rule belowmonicI}) \\
\text{fix} \ v \ v' &= \text{'}o \text{ValK} \\
\text{assume} \ vv' &= \text{unitK} \cdot v \subseteq \text{unitK} \cdot v' \\
\text{let} \ \_k &= \Lambda \, x. \, \text{if} \ x \subseteq v' \ \text{then} \ \bot \ \text{else} \ \text{some-non-bottom-element} \\
\text{from} \ vv' &\ \text{have} \ \text{unitK} \cdot v \cdot \_k \subseteq \text{unitK} \cdot v' \cdot \_k \ \text{by} \ (\text{rule monofun-cfun-fun}) \\
\text{hence} \ \_k \cdot v \subseteq \_k \cdot v' \ \text{by} \ (\text{simp add: unitK-def}) \\
\text{with} \ \text{some-non-bottom-element} &\ \text{show} \ v \subseteq v' \ \text{by} \ (\text{auto split: if-split-asm})
\end{align*}
\]

\[
\text{qed}
\]

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.

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

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-theta-rep where
lr-theta-rep ≡ λr. lr-eta-rep-N ⊔ lr-eta-rep-F r

definition lr-rep :: ‘o lfr where
lr-rep ≡ λr. (lr-eta-rep r, lr-theta-rep r)

abbreviation lr :: ‘o lff where
lr ≡ λr. (mklr (fst (lr-rep r)), mklr (snd (lr-rep r))) end

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.


apply standard
  apply (rule mono-lr)
  apply (rule fix-ValD-copy-rec-ID)
  apply (rule fix-ValK-copy-rec-ID)
  apply (simp-all add: cfun-map-def)[4]
  apply (erule (2) min-inv-lr)
  done

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.
\( \eta : x \mapsto x' \equiv (x, x') \in \text{unlr } (\text{fst } F . \delta) \)

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

Theorem 1 from Reynolds (1974).

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

theorem Theorem1:
  assumes \( \forall v, \eta : \vartheta \cdot v \mapsto \vartheta' \cdot v \)
  shows \( \eta : \text{evalD } e \cdot \vartheta \mapsto \text{evalK } e \cdot \vartheta' \)
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. \( 'o \text{ ValK} \).

locale value-retraction =
  fixes \( VtoO : 'o \text{ ValK } \mapsto 'o \)
  fixes \( OtoV : 'o \mapsto 'o \text{ ValK} \)
  assumes \( OV : OtoV \circ VtoO = \text{ID} \)

sublocale value-retraction < at-least-two-elements \( VtoO \cdot (\text{ValKN } \cdot 0) \)
using \( OV \) by \( \text{(standard, simp add: injection-defined cfcomp1 cfun-eq-iff)} \)

collection value-retraction
begin
  fun \( \text{DtoKM-i } : \text{nat } \Rightarrow \text{ValD } \mapsto 'o \text{ ValKM} \)
  and \( \text{KMtoD-i } : \text{nat } \Rightarrow 'o \text{ ValKM } \mapsto \text{ValD} \)
where
  \( \text{DtoKM-i } 0 = \perp \)
  \( \text{DtoKM-i } (\text{Suc } n) = (\Lambda v \cdot \text{case } v \text{ of } \text{ValF } f \mapsto \text{unitK } (\text{ValKF } (\text{cfun-map } (\text{KMtoD-i } n) \cdot (\text{DtoKM-i } n) ) \cdot f)) \)
  \( \text{ValTT } \Rightarrow \text{unitK } \cdot \text{ValKTT} \)
  \( \text{ValFF } \Rightarrow \text{unitK } \cdot \text{ValKFF} \)
  \( \text{ValN } \cdot m \Rightarrow \text{unitK } (\text{ValKN } \cdot m) \)

  \( \text{KMtoD-i } 0 = \perp \)
  \( \text{KMtoD-i } (\text{Suc } n) = (\Lambda y \cdot \text{case } OtoV \cdot (v \cdot VtoO) \text{ of } \text{ValKF } f \Rightarrow \text{ValF } (\text{cfun-map } (\text{DtoKM-i } n) \cdot (\text{KMtoD-i } n) \cdot f)) \)
  \( \text{ValTT } \Rightarrow \text{ValTT} \)
  \( \text{ValFF } \Rightarrow \text{ValFF} \)
  \( \text{ValKN } \cdot m \Rightarrow \text{ValN } \cdot m) \)

abbreviation \( \text{DtoKM } \equiv (\bigsqcup i \cdot \text{DtoKM-i } i) \)
abbreviation \( \text{KMtoD } \equiv (\bigsqcup i \cdot \text{KMtoD-i } i) \)

Lemma 1 from Reynolds (1974).
lemma Lemma1:
\[ \eta : x \mapsto \text{DtoKM} \cdot x \]
\[ \eta : x \mapsto x' \implies x = \text{KMtoD} \cdot x' \]

Theorem 2 from Reynolds (1974).

theorem Theorem2: \( \text{evalD} \cdot \varrho = \text{KMtoD} \cdot (\text{evalK} \cdot \varrho) \)
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 of Wand and Vaillancourt (2004).
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 \(\beta\)-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 :: \( \text{db} \Rightarrow \text{db} \Rightarrow \text{bool} (\rightarrow_v [-50, 50]) \)

where
 betaN: \( \text{DBApp} (\text{DBAbsN} u) v \rightarrow_v u <\text{v} / 0 > \)
| betaV: \( \text{val} v \Longrightarrow \text{DBApp} (\text{DBAbsV} u) v \rightarrow_v u <\text{v} / 0 > \)
| \( f \rightarrow_v f' \Longrightarrow \text{DBApp} f x \rightarrow_v \text{DBApp} f' x \)
| \( [f = \text{DBAbsV} u; x \rightarrow_v x'] \Longrightarrow \text{DBApp} f x \rightarrow_v \text{DBApp} f x' \)
| \( \text{DBFix} f \rightarrow_v f <\text{DBFix} f / 0 > \)
| \( \text{DBCond} DBtt t e \rightarrow_v t \)
| \( \text{DBCond} DBff t e \rightarrow_v e \)
| \( \text{DBSucc} (\text{DBNum} n) \rightarrow_v \text{DBNum} (\text{Succ} n) \)
| \( \text{DBPred} (\text{DBNum} (\text{Succ} n)) \rightarrow_v \text{DBNum} n \)
| \( \text{DBIsZero} (\text{DBNum} 0) \rightarrow_v \text{DBtt} \)
| \( 0 < n \Longrightarrow \text{DBIsZero} (\text{DBNum} n) \rightarrow_v \text{DBff} \)

abbreviation — The transitive, reflexive closure of the reduction relation.
 reduction-trc :: \( \text{db} \Rightarrow \text{db} \Rightarrow \text{bool} (\rightarrow_v^* [-100, 100]) \)

where
 reduction-trc \( \equiv \text{rtranclp} \text{ reduction} \)
declare reduction.intros[intro]

inductive-cases reduction-inv:
  DBVar v ↦_v t'
  DBApp f x ↦_v t'
  DBAbsN u ↦_v t'
  DBAbsV u ↦_v t'
  DBFix f ↦_v t'
  DBCond i t e ↦_v t'
  DBff ↦_v t'
  DBtt ↦_v t'
  DBNum n ↦_v t'
  DBSucc n ↦_v t'
  DBPred n ↦_v t'
  DBIsZero n ↦_v t'

lemma reduction-val:
  assumes val v
  assumes v ↦_v v'
  shows False
  using assms by (auto elim: val.cases reduction-inv)

lemma reduction-deterministic:
  assumes t ↦_v v
  assumes t ↦_v v''
  shows t'' = t'
  using assms by (induct arbitrary: t'') (blast dest: reduction-val elim: reduction-inv)+

6.0.1 Reduction is consistent with evaluation

lemma reduction-eval:
  assumes t ↦_v t'
  assumes t' ↓ v
  shows t ↓ v
  using assms by (induct arbitrary: v) (auto elim!: evalOP-inv val.cases intro: eval-val)

lemma reduction-trc-eval:
  assumes t ↦_v t'
  assumes t' ↓ v
  shows t ↓ v
  using assms by induct (auto simp: reduction-eval)

theorem reduction-trc-eval-eval:
  assumes t ↦_v t'
  assumes val v
  shows t ↓ v
  using assms by (induct rule: converse-rtranclp-induct) (auto intro: eval-val reduction-trc-eval)

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


