Adequacy of PCF

Natalie Ravenhill

24th August 2016

Aim of the Project

- Study the operational and denotational semantics of the programming language PCF
- Prove that these semantics are equivalent at base type, by proving a theorem called Adequacy

PCF

Syntax of PCF:

$$A ::= \text{Nat} \mid A \to B$$

$$e ::= \lambda x : A.e \mid e\ e \mid x$$
$$\mid\ z\ \mid s(e)\ \mid\ case\ \ (e,\ \ z\ \ \to\ \ e_0\ \ ,$$
$$s(n) \to e_s)$$
$$\mid \text{fix } x : A\ .\ e$$

PCF

Operational Semantics:

- How to run programs
- Relation $\mapsto$

Denotational Semantics:

- Mathematical meaning of programs - Types are Sets, Programs are functions
- Recursion is given by fixed points

Domain Theory

Domains:

- $(D, \sqsubseteq)$
- $\bot$
- For $x_0 \sqsubseteq x_1 \sqsubseteq \ldots$, exists $\bigsqcup_n x_n$

Continuity : $f(\bigsqcup_n x_n) = \bigsqcup_n fx_n$

Domains including Natural Numbers, Single Element Domain, Product of Domains, **Continuous Functions**

Fixpoint Theorem

Continuous Functions are used to model fixpoint recursion.

Theorem

Every continuous function $f : X \to X$ has a least fixpoint, which is the limit of the chain $\perp \sqsubseteq f(\perp) \sqsubseteq f^2(\perp) \sqsubseteq \ldots$

Proof.

in 2 steps:

1. Prove limit of chain is a fixpoint
2. Limit $\sqsubseteq$ any other fixpoint

$\square$

Adequacy

Theorem

If $\vdash e : Nat$ *(ie. e is a closed term of type Nat) then* $[\![e]\!] = n \Leftrightarrow e \mapsto^* \underline{n}$

Relates operational semantics to denotational semantics.

Correctness

Now we can relate the Operational Semantics to the Denotational semantics with the following theorem:

Theorem

If $\Gamma \vdash e : A$ *and* $e \mapsto e'$ *and* $\gamma \in [\![\Gamma]\!]$, *then* $[\![\Gamma \vdash e : A]\!]\gamma = [\![\Gamma \vdash e' : A]\!]\gamma$

Proof.

by induction on $e \mapsto e'$, so the cases are on the evaluation rules. We can use the fact that $f(\mathit{fix}(f)) = \mathit{fix}(f)$ and a substitution lemma $\square$

Substitution Lemma

Lemma

If $\Gamma \vdash e : A$ *and* $\Gamma, x : A \vdash e' : C$ *and* $\gamma \in [\![\Gamma]\!]$, *then* $[\![\Gamma \vdash [e/x]e' : C]\!]\gamma = [\![\Gamma, x : A \vdash e' : C]\!](\gamma, [\![\Gamma \vdash e : A]\!]\gamma/x)$

Proof.

By induction on e' $\square$

Adequacy

Adequacy is the following theorem:

Theorem

If $\vdash e : Nat$ *(ie. e is a closed term of type Nat) and* $[\![e]\!] = n$ *then* $[\![e]\!] = n \Leftrightarrow e \mapsto^* \underline{n}$

Backwards direction = Correctness
Forwards direction = Logical Relations

Logical Predicate

We defined the following logical predicate (i.e. a unary logical relation:

$$\mathrm{Adeq}_{\mathrm{Nat}} = \{e \mid \; \vdash e : \mathrm{Nat} \;\wedge\; ([\![e]\!] = n \Rightarrow e \mapsto^{*} \underline{n})\}$$

$$\mathrm{Adeq}_{A \to B} = \{e \mid \; \vdash e : A \to B \wedge \forall e' \in \mathrm{Adeq}_{A} \,.\, (e\ e') \in \mathrm{Adeq}_{B}\}$$

Logical Predicate

Now to prove adequacy, we just prove that every well typed term is in Adeq, so we also defined Adeq on typing contexts:

$$\mathrm{Adeq}_{Ctx}(\cdot) = \{<>\}$$

where $<>$ is the empty substitution and $\cdot$ is the empty context.

$$\mathrm{Adeq}_{Ctx}(\Gamma, A) = \{(\gamma, e/x) \mid \gamma \in \mathrm{Adeq}_{Ctx}(\Gamma) \ \wedge \ e \in \mathrm{Adeq}_A\}$$

Main Lemma

Lemma

If $\Gamma \vdash e : A$ *and* $\gamma \in \mathrm{Adeq}_{Ctx}(\Gamma)$, *then* $[\gamma](e) \in \mathrm{Adeq}_A$

Proof.

By induction on derivations of $\Gamma \vdash e : A$ $\square$

The main difficulty of this is the fixpoint case (we shall prove this if time).

Lemmas

Expansion Lemma

If $\vdash e : A$ *and* $e \mapsto e'$ *and* $e' \in \mathrm{Adeq}_A$ *then* $e \in \mathrm{Adeq}_A$

Proof.

By induction on types. □

Non Termination Lemma

If $[\![e]\!] = \bot$ *and* $\vdash e : A$ *and* $e \mapsto^{\infty}$, *then* $e \in \mathrm{Adeq}_A$

Proof.

By induction on types. □

Lemmas

Substitution Lemma

If $\gamma \in \text{Adeq}_{Ctx}(\Gamma)$ *and* $\Gamma \vdash e : A$ *then* $\vdash [\gamma](e) : A$

Proof.

By induction on Γ. $\square$

Adequacy of Successor

$[\gamma]s(e) = s([\gamma]e) \in \text{Adeq}_{\text{Nat}}$

Need to show:

1. $\vdash s([\gamma]e) : \text{Nat}$

   Use typing rule with $\vdash [\gamma]e : \text{Nat}$

2. $[\![s([\gamma]e)]\!] = n \Rightarrow s([\gamma]e) \mapsto^* \underline{n}$

   Use $[\![[\gamma]e]\!] = n - 1 \Rightarrow [\gamma]e \mapsto^* \underline{n-1}$ *and congruence rule from operational semantics*

Adequacy of Fixpoint

Define fixpoint approximation:

Definition

Let $M = \mathrm{fix}\, x : A.\ e : A$ *be a well typed term and define:*

$$M^0 = \mathrm{fix}\, x : A.\ x$$

$$M^{k+1} = (\lambda x : A.\ e)(M^k)$$

So prove $[\gamma]M^k \in \mathrm{Adeq}_A$, by induction on k.

Adequacy of Fixpoint

Base case:
Use Non termination Lemma, as $[\![[\gamma]M^0]\!] = \perp$ and $[\gamma]M^0 \mapsto^\infty$.
(Use Fixpoint Theorem to show $[\![[\gamma]M^0]\!] = \perp$)

Inductive case:

$$[\gamma]M^{k+1} = [\gamma, [\gamma]M^k/x]e = [\gamma']e$$

- Use inductive hypothesis of Main Lemma with $\Gamma, x : \mathrm{Nat} \vdash e : A$ to get $[\gamma']e \in \mathrm{Adeq}_A$.
- Use Expansion Lemma to get $[\gamma]M^k \in \mathrm{Adeq}_A$.

Adequacy

Adequacy can be proved as a corollary of the Main Lemma:

Proof.

Use $\vdash e : A$ and $<>$ in Main Lemma to get
$<>\ e = e \in \mathrm{Adeq}_{\mathrm{Nat}}$.
This says $\vdash e : Nat \wedge [\![e]\!] = n \Rightarrow e \mapsto^{*} \underline{n}$.
RHS is forwards direction of Adequacy! □

Backwards direction was correctness!

Summary

- Learned about Domain Theory and Logical Relations
- Proved standard theorems in Semantics (Type Safety, Soundness, Adequacy, ...)
- Choosing a logical relation that would make Adequacy easy to prove using our semantics
- Proving the fixpoint case for our semantics using the domain theoretic fixpoint theorem