Adequacy using a Binary Logical Relation

August 16, 2016

We define a binary logical relation R, which contains relations $R_A \subseteq [\![A]\!] \times \{e \mid \vdash e : A\}$, defined by induction on types for each type as follows:

$$dR_{\mathrm{Nat}}e \Leftrightarrow \forall n \in \mathbb{N}.\ d = n \Rightarrow e \mapsto^* n$$

$$fR_{A \to B}e \Leftrightarrow \forall d \in [\![A]\!].\ \forall e' \in \{e \mid\ \vdash e : A\}.\ dR_Ae' \Rightarrow f(d)R_Be\ e'$$

1 Lemmas for Main Lemma

1.1 Bottom Element Lemma

Lemma 1. *For any type A and $\Gamma \vdash e : A$, $\perp R_A\ e$*

Proof. By induction on types. For Nat, we want to show $\forall n \in \mathbb{N}.\ \perp = n \Rightarrow e \mapsto^* n$. Because $\perp \notin \mathbb{N}$, this statement is vacuously true.

For $R_{A \to B}$, we have that $\perp$ is the function $\lambda x : A.\perp$, so we want to show $\forall d \in [\![A]\!].\ \forall e' \in \{e \mid\ \vdash e : A\}.\ dR_Ae' \Rightarrow (\lambda x : A.\perp)(d)R_Be\ e'$. Assume d is an element of the domain representing type A and e' is an expression of type A such that $d\ R_Ae'$. We want to show that $\perp\ R_B\ e\ e'$ and by the inductive hypothesis, we know for any $e : B$ that $\perp\ R_Be$, so we can just use this with $e\ e'$ to get our conclusion. ∎

1.2 Expansion Lemma

Lemma 2. *If $\Gamma \vdash e : A$ and $e \mapsto e'$ and dR_Ae' then dR_Ae*

Proof. By induction on types. For base case we assume $dR_{\text{Nat}}e'$, so we have $\forall n \in \mathbb{N}.\ d = n \Rightarrow e' \mapsto^* n$. Let $n = d$. Then, as $e \mapsto e'$ and $e' \mapsto^* n$, we know that $e \mapsto^* n$. Therefore, $dR_{\text{Nat}}e$.

For the inductive case, assume $e_0 \mapsto e'_0$ and $f\ R_{A \to B}\ e_0$, so we have $\forall a \in [\![A]\!].\ \forall e' \in \{e \mid\ \vdash e : A\}.\ a\ R_A\ e' \Rightarrow f(a)\ R_B\ e_0\ e'$. Let a be an element in the domain representing A and e_1 be an expression of type A such that aR_Ae_1. Then $f(a)\ R_B\ e_0\ e_1$.

By the inductive hypothesis we know that for any $e \mapsto e'$ for expressions of type B, that they are both related to the same denotation. Therefore we have $f(a)\ R_B\ e'_0\ e_1$, so we know $\forall a \in [\![A]\!].\ \forall e' \in \{e \mid\ \vdash e : A\}.\ a\ R_A\ e' \Rightarrow f(a)\ R_B\ e'_0\ e'$, so $f\ R_{A \to B}\ e'_0$. $\square$

1.3 Chains Lemma

Lemma 3. *For an expression $e : A$ and a chain $x_0 \sqsubseteq x_1 \sqsubseteq \dots$, if $x_n R_A e$, then $\bigsqcup x_n\ R_A\ e$*

Proof. By induction on types. For base type, Nat, then we assume we have a chain of elements in $\mathbb{N}_\perp$ such that $x_n\ R_{\text{Nat}}e$. Therefore for any element in the chain we know $\forall n \in \mathbb{N}.\ x_n = n \Rightarrow e \mapsto^* n$. We have two cases depending on the values of $\bigsqcup x_n$:

1. $\bigsqcup x_n = n$. Then we know that $e \mapsto^* \sqcup x_n$, as any $x_n R_{\text{Nat}} e$
2. $\bigsqcup x_n = \perp$. By Lemma 2 we know that $\perp R_{\text{Nat}} e$ for any e

The inductive case is for $R_{A \to B}$. Assume we have a chain $f_1 \sqsubseteq f_2 \sqsubseteq \dots$ of elements in $[\![A]\!] \to [\![B]\!]$ and $d\ R_A\ e'$ for some $d \in [\![A]\!]$ and $e : A$. Then we need to show $\bigsqcup f_n(d)\ R_B\ e\ e'$. By induction we know for any expression of type B and a chain $f_1(d) \sqsubseteq f_2(d) \sqsubseteq \dots$ of elements of $[\![B]\!]$, $\bigsqcup f_n(d)$ is related to that expression. Therefore we have $\bigsqcup f_n(d)\ R_B e\ e'$. $\square$

2 Fixpoint Constant

We can define a constant Fix, for any type A, as the term $\text{Fix}_A : (A \to A) \to A$ that takes a function of type $A \to A$ to its fixpoint.

The interpretation of Fix applied to a function f is the following:

$$[\![\text{Fix}]\!]f = \bigsqcup_n f^n(\perp)$$

which is the limit of chain obtained by repeatedly applying f to $\perp$.

We can use this to prove the following lemma:

Lemma 4. *For any* $f \in D_{A \to A}$ *and* $e : A \to A$*,* $f R_{A \to A} e \Rightarrow [\![\mathrm{Fix}]\!] \; f \; R_A \; \mathrm{Fix} \; e$

Proof. Assume there is f and e such that $f \; R_{A \to A} \; e$. Then we want to prove $[\![\mathrm{Fix}]\!] \; f \; R_A \; \mathrm{Fix} \; e$, which is the same as $\bigsqcup_n f^n(\bot) \; R_A \; \mathrm{Fix} \; e$.

Next we must prove $\forall n \in \mathbb{N}. \; f^n(\bot) \; R_A \; \mathrm{Fix} \; e$, which we prove by induction:

The base case is $\bot \; R_A \; \mathrm{Fix} \; e$, which we know by Lemma 2. For the inductive case, assume $f^n(\bot) \; R_A \; \mathrm{Fix} \; e$. As we know $f \; R_A \; e$, we have $f(f^n(\bot)) \; R_A \; e(\mathrm{Fix} \; e)$. by its definition. As $\mathrm{Fix} \; e \mapsto e(\mathrm{Fix} \; e)$, we can use Lemma 3 to get $f^{n+1} \; R_A \; \mathrm{Fix} \; e$.

Then by Lemma 4, as we have the chain $f^0(\bot) \sqsubseteq f^1(\bot) \sqsubseteq \dots$ and we know $\forall n \in \mathbb{N}. \; f^n(\bot) \; R_A \; \mathrm{Fix} \; e$, we know $\bigsqcup_n f^n(\bot) \; R_A \; \mathrm{Fix} \; e$. □

2.1 Converting between terms

Converting from our PCF term to the constant:

$$\mathrm{fix}\, x : A.e : A = \mathrm{Fix}(\lambda x : A. \; e)$$

Converting from the constant to our PCF term:

$$\mathrm{Fix}\, e = \mathrm{fix}\, x : A. \; (e \; x) : A$$

3 Main Lemma

For this relation, the **Main Lemma** will be the following:

Lemma 5. *If* $\Gamma = x_1 : A_1, \dots, x_n : A_n$*,* $\Gamma \vdash e : A$ *and* $d_1 R_{A_1} t_1, d_2 R_{A_2} t_2, \dots, d_n R_{A_n} t_n$*, then*

$$[\![\Gamma \vdash e : A]\!](d_1, \dots, d_n) \; R_A \; e[x_1/t_1, \dots, x_n/t_n]$$

Proof. By induction on the possible values of e.

Variables For a variable $x_1 : A_1, \dots, x_n : A_n \vdash x : A$, assume for any $i = 1, \dots, n$ that $d_i R_{A_i} t_i$. Then we want to show:

$$(\lambda(d_1, \dots, d_n) \in [\![\Gamma]\!]. \; \pi_i(d_1, \dots, d_n))(d_1, \dots, d_n) \; R_A \; [x_1/t_1, \dots, x_n/t_n]x$$

As we have $\Gamma \vdash x : A$, by the typing rule for variables we have $\Gamma(x) = A$, so $x \in dom(\Gamma)$ and $\exists i.\ d_i R_{A_i} t_i$. Then on the right hand side we have $[x/t_i]x$. Therefore we want to show

$$d_i R_{A_i} t_i$$

which we have as an assumption.

Zero For $z : \mathrm{Nat}$, we want to show:

$$[\![\Gamma \vdash z : \mathrm{Nat}]\!](d_1, \ldots, d_n)\ R_{\mathrm{Nat}}\ [x_1/t_1, \ldots, x_n/t_n]z$$

Expanding the definitions gives us $0\ R_{\mathrm{Nat}}\ z$, so we must show $\forall n \in \mathbb{N}.0 = n \Rightarrow z \mapsto^* n$, which is the case as z reduces to n in zero steps. Therefore $0\ R_{\mathrm{Nat}}\ z$.

Successor For $x_1 : A_1, \ldots, x_n : A_n \vdash s(e) : \mathrm{Nat}$, assume for any $i = 1, \ldots, n$ that $d_i R_{A_i} t_i$. Then we want to show:

$$[\![\Gamma \vdash s(e) : \mathrm{Nat}]\!](d_1, \ldots, d_n)\ R_{\mathrm{Nat}}\ [x_1/t_1, \ldots, x_n/t_n](s(e))$$

Which expands to $\forall n \in \mathbb{N}.\ [\![\Gamma \vdash s(e) : \mathrm{Nat}]\!](d_1, \ldots, d_n) = n \Rightarrow [x_1/t_1, \ldots, x_n/t_n]s(e) \mapsto^* n$. By the inductive hypothesis, we know:

$$[\![\Gamma \vdash e : \mathrm{Nat}]\!](d_1, \ldots, d_n)\ R_{\mathrm{Nat}}\ [x_1/t_1, \ldots, x_n/t_n]e$$

This expands to $\forall n \in \mathbb{N}.\ [\![\Gamma \vdash e : \mathrm{Nat}]\!](d_1, \ldots, d_n) = n \Rightarrow [x_1/t_1, \ldots, x_n/t_n]e \mapsto^* n$. (If the denotation of e is $\perp$ then this is vacuously true.)

Therefore there will be two cases:

1. If $[\![\Gamma \vdash e : \mathrm{Nat}]\!](d_1, \ldots, d_n) = \perp$, then we must show $\perp R_{\mathrm{Nat}}[x_1/t_1, \ldots, x_n/t_n]s(e)$, which we get from Lemma 2
2. If $[\![\Gamma \vdash e : \mathrm{Nat}]\!](d_1, \ldots, d_n) = v$, then we must show $v{+}1\ R_{\mathrm{Nat}}\ [x_1/t_1, \ldots, x_n/t_n]s(e)$. Let $n = v{+}1$. From the inductive hypothesis we know that $[x_1/t_1, \ldots, x_n/t_n]e \mapsto^* v$. Using the congruence evaluation rule for successor, we get $s([x_1/t_1, \ldots, x_n/t_n]e) \mapsto s(v)$ and $s(v)$ is the same as $v + 1$. Therefore we have $v + 1\ R_{Nat} s(v)$, so if we use this with the congruence rule in Lemma 3, we have $v + 1\ R_{Nat} s([x_1/t_1, \ldots, x_n/t_n]e)$

Case For $x_1 : A_1, \ldots, x_n : A_n \vdash \text{case}(e, z \mapsto e_0, s(x) \mapsto e_S)$, assume for any $i = 1, \ldots, n$ that $d_i R_{A_i} t_i$. Then we want to show:

$$[\![\Gamma \vdash \text{case}(e, z \mapsto e_0, s(x) \mapsto e_S) : A]\!](d_1, \ldots, d_n)\ R_A\ [x_1/t_1, \ldots, x_n/t_n]\,\text{case}(z \mapsto e_0, s(x) \mapsto e_S)$$

The result of the denotation depends on the value of e, so we have three cases:

1. $[\![\Gamma \vdash e : \text{Nat}]\!](d_1, \ldots, d_n) = \bot$, then we must show $\bot\ R_A\ [x_1/t_1, \ldots, x_n/t_n]$ $\text{case}(z \mapsto e_0, s(x) \mapsto e_S)$, which we get by applying Lemma 2.
2. $[\![\Gamma \vdash e : \text{Nat}]\!](d_1, \ldots, d_n) = 0$, then we want to show $[\![\Gamma \vdash e_0 : A]\!](d_1, \ldots, d_n)$ $R_A[x_1/t_1, \ldots, x_n/t_n]\,\text{case}(z \mapsto e_0, s(x) \mapsto e_S)$. As we have $\Gamma \vdash e_0 : A$ from the typing rule of case, we can get $[\![\Gamma \vdash e_0 : A]\!](d_1, \ldots, d_n)\ R_A[x_1/t_1, \ldots, x_n/t_n]e_0$ by the induction hypothesis. We can now use this in Lemma 3, with the operational semantics rule for case when the expression is zero, to get $[\![\Gamma \vdash e_0 : A]\!](d_1, \ldots, d_n)\ R_A[x_1/t_1, \ldots, x_n/t_n]\,\text{case}(z \mapsto e_0, s(x) \mapsto e_S)$
3. $[\![\Gamma \vdash e : \text{Nat}]\!](d_1, \ldots, d_n) = n + 1$ we want to show

   $$[\![\Gamma, x : \text{Nat} \vdash e_S : \text{Nat}]\!](d_1, \ldots, d_n, d)\ \ R_A\ [x_1/t_1, \ldots, x_n/t_n, x/t]\,\text{case}(e, z \mapsto e_0, s(x) \mapsto e_S)$$

   From the induction hypothesis we have

   $$[\![\Gamma, x : \text{Nat} \vdash e_S : \text{Nat}]\!](d_1, \ldots, d_n, d)\ \ R_A\ [x_1/t_1, \ldots, x_n/t_n, x/t]e_S$$

   We can now use this in Lemma 3, with the operational semantics rule for case when the expression is not zero to get $[\![\Gamma, x : \text{Nat} \vdash e_S : \text{Nat}]\!](d_1, \ldots, d_n, d)$ $R_A\ [x_1/t_1, \ldots, x_n/t_n, x/t]\,\text{case}(e, z \mapsto e_0, s(x) \mapsto e_S)$.

Application For $x_1 : A_1, \ldots, x_n : A_n \vdash e\ e' : B$, assume for any $i = 1, \ldots, n$ that $d_i R_{A_i} t_i$. Then we want to show:

$$[\![\Gamma \vdash e\ e' : B]\!](d_1, \ldots, d_n)\ R_B\ [x_1/t_1, \ldots, x_n/t_n]e\ e'$$

Using the denotational semantics and substitution function we can rewrite this as:

$$[\![\Gamma \vdash e : A \to B]\!](d_1, \ldots, d_n)([\![\Gamma \vdash e' : B]\!](d_1, \ldots, d_n))\ R_B\ ([x_1/t_1, \ldots, x_n/t_n]e)([x_1/t_1, \ldots, x_n/t_n]e')$$

By the inductive hypothesis we have $[\![\Gamma \vdash e : A \to B]\!](d_1, \ldots, d_n)\ R_{A \to B}\ [x_1/t_1, \ldots, x_n/t_n]e$. Expanding this gives us $\forall d \in [\![A]\!].\ \forall e' \in \{e \mid\ \vdash e : A\}.\ dR_A e' \Rightarrow [\![\Gamma \vdash e : A \to B]\!](d_1, \ldots, d_n)(d)R_B[x_1/t_1, \ldots, x_n/t_n]e\ e'$. Let $d = ([\![\Gamma \vdash e' : B]\!](d_1, \ldots, d_n))$ and $e' = [x_1/t_1, \ldots, x_n/t_n]e'$. Then we have $[\![\Gamma \vdash e : A \to B]\!](d_1, \ldots, d_n)([\![\Gamma \vdash e' : B]\!](d_1, \ldots, d_n)\ R_B\ ([x_1/t_1, \ldots, x_n/t_n]e)([x_1/t_1, \ldots, x_n/t_n]e')$.

λ-Abstraction For $x_1 : A_1, \ldots, x_n : A_n \vdash \lambda x : A.\ e : A \to B$, assume for any $i = 1, \ldots, n$ that $d_i R_{A_i} t_i$. Then we want to show:

$$[\![\Gamma \vdash \lambda x : A.\ e : A \to B]\!](d_1, \ldots, d_n)\ R_{A\to B}[x_1/t_1, \ldots, x_n/t_n](\lambda x : A.\ e)$$

Expanding the definition of the logical relation gives us

$$\forall d \in [\![A]\!].\ \forall e' \in \{e \mid\ \vdash e : A\}.\ dR_A e' \Rightarrow$$
$$[\![\Gamma, x : A \vdash e : B]\!](d_1, \ldots, d_n)(d)\ R_B\ [x_1/t_1, \ldots, x_n/t_n](\lambda x : A.\ e)\ t$$

Let d be an element of the domain of type A and t be an expression of type A such that $dR_A t$.

Then by the using the denotational semantics for λ abstraction, we want to show:

$$(\lambda d \in [\![A]\!].\ [\![\Gamma, x : A \vdash e : B]\!](d_1, \ldots, d_n))(d)\ R_B\ [x_1/t_1, \ldots, x_n/t_n](\lambda x : A.\ e)\ t$$

which is the same as:

$$[\![\Gamma, x : A \vdash e : B]\!](d_1, \ldots, d_n, d)\ R_B\ [x_1/t_1, \ldots, x_n/t_n, x/t]\ e$$

which we get by the inductive hypothesis.

Fixpoint For $x_1 : A_1, \ldots, x_n : A_n \vdash \lambda x : A.\ \mathrm{fix}\, x : A.\ e : A$, assume for any $i = 1, \ldots, n$ that $d_i R_{A_i} t_i$. Then we want to show:

$$[\![\Gamma \vdash \mathrm{fix}\, x : A.\ e : A]\!](d_1, \ldots, d_n)\ R_A\ [x_1/t_1, \ldots, x_n/t_n](\mathrm{fix}\, x : A.\ e : A)$$

Using the fixpoint constant (see 1.1) , we can rewrite this as:

$$[\![\Gamma \vdash \mathrm{Fix}\ (\lambda x : A.\ e) : A]\!](d_1, \ldots, d_n)\ R_A\ [x_1/t_1, \ldots, x_n/t_n](\mathrm{Fix}\ (\lambda x : A.\ e) : A)$$

As Fix $(\lambda x : A.\ e)$ is a function application, by its typing rule we have $\Gamma \vdash \lambda x : A.\ e : A \to A$, so we can use the inductive hypothesis to get:

$$[\![\Gamma \vdash \lambda x : A.\ e]\!](d_1, \ldots, d_n)\ R_{A\to A}\ [x_1/t_1, \ldots, x_n/t_n](\lambda x : A.\ e)$$

Then, we use Lemma 1 with $f = [\![\Gamma \vdash \lambda x : A.\ e]\!](d_1, \ldots, d_n)$ and $e = [x_1/t_1, \ldots, x_n/t_n](\lambda x : A.e)$. This gives us $[\![\mathrm{Fix}]\!][\![\Gamma \vdash \lambda x : A.\ e]\!](d_1, \ldots, d_n)\ R_A\ \mathrm{Fix}\ [x_1/t_1, \ldots, x_n/t_n](\lambda x : A.e)$.

Using the denotational semantics for function application, we have:

$$[\![\Gamma \vdash \mathrm{Fix}\ \ \lambda x : A.\ e]\!](d_1, \ldots, d_n)\ R_A\ [x_1/t_1, \ldots, x_n/t_n]\,\mathrm{Fix}(\lambda x : A.\ e)$$

.

□