

# Step-Indexed Syntactic Logical Relations for Recursive and Quantified Types

Amal Ahmed

Harvard University, Cambridge, MA  
amal@eecs.harvard.edu

**Abstract.** We present a sound and complete proof technique, based on syntactic logical relations, for showing contextual equivalence of expressions in a  $\lambda$ -calculus with recursive types and impredicative universal and existential types. Our development builds on the step-indexed PER model of recursive types presented by Appel and McAllester. We have discovered that a direct proof of transitivity of that model does not go through, leaving the “PER” status of the model in question. We show how to extend the Appel-McAllester model to obtain a logical relation that we can prove is transitive, as well as sound and complete with respect to contextual equivalence. We then augment this model to support relational reasoning in the presence of quantified types.

Step-indexed relations are indexed not just by types, but also by the number of steps available for future evaluation. This stratification is essential for handling various circularities, from recursive functions, to recursive types, to impredicative polymorphism. The resulting construction is more elementary than existing logical relations which require complex machinery such as domain theory, admissibility, syntactic minimal invariance, and  $\top\top$ -closure.

## 1 Introduction

Proving equivalence of programs is important for verifying the correctness of compiler optimizations and other program transformations, as well as for establishing that program behavior is independent of the representation of an abstract type. This representation independence principle guarantees that if one implementation of an abstraction is exchanged for another, client modules will not be able to detect a difference.

Program equivalence is generally defined in terms of *contextual equivalence*. We say that two programs are contextually equivalent if they have the same observable behavior when placed in any program context  $C$ . Unfortunately, proving contextual equivalence is difficult in general, since it involves quantification over *all* possible contexts. As a result, there’s been much work on finding tractable techniques for proving contextual equivalence. Many of these are based on the method of *logical relations*.

Logical relations specify relations on well-typed terms via structural induction on the syntax of types. Thus, for instance, logically related functions take

logically related arguments to related results, while logically related pairs consist of components that are related pairwise. Logical relations may be based on denotational models (e.g. [1, 2, 3]) or on the operational semantics of a language [4, 5, 6, 7]. The latter are also known as syntactic logical relations [8] and it is this flavor that is the focus of this paper.

To prove the soundness of a logical relation, one must prove the Fundamental Property (also called the Basic Lemma) which says that any well-typed term is related to itself. For simple type systems, it is fairly straightforward to prove the Fundamental Property in the absence of nontermination. The addition of recursive functions, however, complicates matters: establishing the Fundamental Property now requires proving additional “unwinding” lemmas [9, 6, 7, 10] which show that in any terminating computation a recursively defined function is approximated by its finite unrollings. More challenging still is the addition of recursive types and impredicative quantified types<sup>1</sup> since the logical relation can no longer be defined by induction on types. Thus, showing the existence of a relational interpretation of recursive types requires proving a nontrivial *minimal invariance* property [3, 10, 8, 11, 12].

Appel and McAllester [13] proposed a radically different solution to the problem of recursive types. They defined *intensional* types, based on the operational semantics of the language, that are indexed by the number of available (future) execution steps. This extra information is sufficient to solve recursive equations on types. Appel and McAllester also presented a PER (relational) model of recursive types, which we build on in this paper. The advantage of step-indexed logical relations is that they avoid complex machinery like domain theory, admissibility, syntactic minimal invariance, and  $\top\top$ -closure (biorthogonality). The approach is promising since unary step-indexed models have scaled well to advanced features like impredicative quantified types and general references (i.e., mutable references that can store functions, recursive types, other references, and even impredicative quantified types) [14, 15].

Appel and McAllester proved the Fundamental Property for their PER model of equi-recursive types, and conjectured that their model was sound with respect to contextual equivalence. We show that their claim is correct — to be precise, we show soundness for a calculus with iso-recursive types, but the essence of the model is the same.

We discovered, however, that the expected proof of transitivity for the Appel-McAllester model does not go through. To definitively show that their model is not transitive we tried to find a counterexample, but could not. Thus, we note that the transitivity of the Appel-McAllester model remains an open problem.

In Section 2 we consider a  $\lambda$ -calculus with iso-recursive types and present a sound and complete logical relation for the language. We also show how a direct proof of transitivity of the Appel-McAllester model fails, and discuss some of the peculiarities of the step-indexed approach. In Section 3 we extend the logical relation to support quantified types. Proofs of all lemmas in the paper and

---

<sup>1</sup> A quantified type such as  $\forall\alpha. \tau$  is impredicative if  $\alpha$  may be instantiated with *any* type, including  $\forall\alpha. \tau$  itself.

several examples to illustrate the use of our logical relation are given in the accompanying technical report [16].

## 2 Recursive Types

We consider a call-by-value  $\lambda$ -calculus with iso-recursive types (dubbed the  $\lambda^{\text{rec}}$ -calculus). Figure 1 presents the syntax and small-step operational semantics for the language, which supports booleans and pairs in addition to recursive types. We define the operational semantics for  $\lambda^{\text{rec}}$  as a relation between closed terms  $e$ . We use evaluation contexts to lift the primitive rewriting rules to a standard, left-to-right, innermost-to-outermost, call-by-value interpretation of the language. We say that a term  $e$  is irreducible ( $\text{irred}(e)$ ) if  $e$  is a value ( $\text{val}(e)$ ) or if  $e$  is a “stuck” expression to which no operational rule applies. We also use  $e \Downarrow$  as an abbreviation for  $\exists e'. e \mapsto^* e' \wedge \text{val}(e')$ .

$$\begin{array}{l} \text{Types} \quad \tau ::= \text{bool} \mid \tau_1 \times \tau_2 \mid \tau_1 \rightarrow \tau_2 \mid \alpha \mid \mu\alpha. \tau \\ \text{Expressions } e ::= x \mid \text{tt} \mid \text{ff} \mid \text{if } e_0, e_1, e_2 \mid \langle e_1, e_2 \rangle \mid \text{let } \langle x_1, x_2 \rangle = e_1 \text{ in } e_2 \mid \\ \quad \lambda x. e \mid e_1 e_2 \mid \text{fold } e \mid \text{unfold } e \\ \text{Values} \quad v ::= \text{tt} \mid \text{ff} \mid \langle v_1, v_2 \rangle \mid \lambda x. e \mid \text{fold } v \end{array}$$

$$\text{Eval Ctxts } E ::= [\cdot] \mid \text{if } E, e_1, e_2 \mid \text{let } \langle x_1, x_2 \rangle = E \text{ in } e \mid E e \mid v E \mid \text{fold } E \mid \text{unfold } E$$

$$\begin{array}{ll} (\text{iftrue}) & \text{if tt}, e_1, e_2 \mapsto e_1 \\ (\text{iffalse}) & \text{if ff}, e_1, e_2 \mapsto e_2 \\ (\text{letpair}) & \text{let } \langle x_1, x_2 \rangle = \langle v_1, v_2 \rangle \text{ in } e \mapsto e[v_1/x_1][v_2/x_2] \\ (\text{app}) & (\lambda x. e) v \mapsto e[v/x] \\ (\text{unfold}) & \text{unfold}(\text{fold } v) \mapsto v \\ (\text{ctxt}) & \frac{e \mapsto e'}{E[e] \mapsto E[e']} \end{array}$$

**Fig. 1.**  $\lambda^{\text{rec}}$  Syntax and Operational Semantics

Typing judgments in  $\lambda^{\text{rec}}$  have the form  $\Gamma \vdash e : \tau$  where the context  $\Gamma$  is defined as follows:

$$\text{Value Context } \Gamma ::= \bullet \mid \Gamma, x:\tau .$$

Thus,  $\Gamma$  is used to track the set of variables in scope, along with their (closed) types. There may be at most one occurrence of a variable  $x$  in  $\Gamma$ . The  $\lambda^{\text{rec}}$  static semantics is entirely conventional (see, e.g., [17]) so we only show selected rules in Figure 2. We use the abbreviated judgment  $\vdash e : \tau$  when the value context is empty.

**Theorem 1 ( $\lambda^{\text{rec}}$  Safety).** *If  $\bullet \vdash e : \tau$  and  $e \mapsto^* e'$ , then either  $e'$  is a value, or there exists an  $e''$  such that  $e' \mapsto e''$ .*

$$\boxed{\Gamma \vdash e : \tau}$$

$$\begin{array}{c}
(\text{Var}) \frac{}{\Gamma \vdash x : \Gamma(x)} \quad (\text{Fn}) \frac{\Gamma, x:\tau_1 \vdash e : \tau_2}{\Gamma \vdash \lambda x. e : \tau_1 \rightarrow \tau_2} \quad (\text{App}) \frac{\Gamma \vdash e_1 : \tau_1 \rightarrow \tau_2 \quad \Gamma \vdash e_2 : \tau_1}{\Gamma \vdash e_1 e_2 : \tau_2} \\
(\text{Fold}) \frac{\Gamma \vdash e : \tau[\mu\alpha. \tau/\alpha]}{\Gamma \vdash \mathbf{fold} e : \mu\alpha. \tau} \quad (\text{Unfold}) \frac{\Gamma \vdash e : \mu\alpha. \tau}{\Gamma \vdash \mathbf{unfold} e : \tau[\mu\alpha. \tau/\alpha]}
\end{array}$$

**Fig. 2.**  $\lambda^{\text{rec}}$  Static Semantics (Selected Rules)

## 2.1 $\lambda^{\text{rec}}$ : Contextual Equivalence

A context  $C$  is an expression with a single hole  $[\cdot]$  in it. Typing judgments for contexts have the form  $\Gamma_1 \vdash C : (\Gamma \triangleright \tau) \rightsquigarrow \tau_1$ , where  $(\Gamma \triangleright \tau)$  indicates the type of the hole — that is, if  $\Gamma \vdash e : \tau$ , then  $\Gamma_1 \vdash C[e] : \tau_1$ .

**Definition 2** ( $\lambda^{\text{rec}}$  Contextual Approximation  $\preceq^{\text{ctx}}$  & Equivalence  $\simeq^{\text{ctx}}$ ). *If  $\Gamma \vdash e : \tau$  and  $\Gamma \vdash e' : \tau$ , we write  $\Gamma \vdash e \preceq^{\text{ctx}} e' : \tau$  to mean*

$$\forall C, \tau_1. \bullet \vdash C : (\Gamma \triangleright \tau) \rightsquigarrow \tau_1 \wedge C[e] \Downarrow \implies C[e'] \Downarrow .$$

*Two terms are contextually equivalent if they contextually approximate one another:*

$$\Gamma \vdash e \simeq^{\text{ctx}} e' : \tau \stackrel{\text{def}}{=} \Gamma \vdash e \preceq^{\text{ctx}} e' : \tau \wedge \Gamma \vdash e' \preceq^{\text{ctx}} e : \tau .$$

## 2.2 $\lambda^{\text{rec}}$ : Logical Relation

Our step-indexed logical relation for  $\lambda^{\text{rec}}$  is based on the PER model for equi-recursive types presented by Appel and McAllester [13] (henceforth AM). The latter claimed, but did not prove, that their PER model was sound with respect to contextual equivalence. We have proved that this is indeed the case. However, “PER” may be somewhat of misnomer for the AM model since the status of transitivity is unclear, as we shall show.

In both models, the relational interpretation  $\mathcal{RV}[\tau]$  of a type  $\tau$  is a set of triples of the form  $(k, v, v')$  where  $k$  is a natural number (called the *approximation index* or *step index*), and  $v$  and  $v'$  are (closed) values. Intuitively,  $(k, v, v') \in \mathcal{RV}[\tau]$  says that in any computation running for no more than  $k$  steps,  $v$  approximates  $v'$  at the type  $\tau$ . Our model differs from the AM model in that whenever  $(k, v, v') \in \mathcal{RV}[\tau]$ , we additionally require that  $\bullet \vdash v' : \tau$ . This additional constraint enables us to prove the transitivity of our logical relation. Moreover, restricting the model to terms that are well-typed seems essential for completeness with respect to contextual equivalence, as others have also noted [12]. We defer an explanation of why we don’t also require  $\bullet \vdash v : \tau$  till Section 2.3.

Figure 3 gives the definition of our logical relation; shaded parts of the definitions have no analog in the AM model. We use the meta-variable  $\chi$  to denote sets of tuples of the form  $(k, v, v')$ , where  $v$  and  $v'$  are closed values ( $v, v' \in C\text{Values}$ ).

$$\begin{aligned}
Rel_\tau &\stackrel{\text{def}}{=} \{\chi \in 2^{\text{Nat} \times C\text{Values} \times C\text{Values}} \mid \forall (j, v, v') \in \chi. \bullet \vdash v' : \tau \wedge \\
&\quad \forall i \leq j. (i, v, v') \in \chi\} \\
|\chi|_k &\stackrel{\text{def}}{=} \{(j, v, v') \mid j < k \wedge (j, v, v') \in \chi\} \\
\mathcal{RV} \llbracket \alpha \rrbracket \rho &= \rho^{\text{sem}}(\alpha) \\
\mathcal{RV} \llbracket \text{bool} \rrbracket \rho &= \{(k, v, v') \mid \vdash v' : \text{bool} \wedge \\
&\quad (v = v' = \mathbf{tt} \vee v = v' = \mathbf{ff})\} \\
\mathcal{RV} \llbracket \tau_1 \times \tau_2 \rrbracket \rho &= \{(k, \langle v_1, v_2 \rangle, \langle v'_1, v'_2 \rangle) \mid \vdash \langle v'_1, v'_2 \rangle : (\tau_1 \times \tau_2)^{[\rho]} \wedge \\
&\quad (k, v_1, v'_1) \in \mathcal{RV} \llbracket \tau_1 \rrbracket \rho \wedge (k, v_2, v'_2) \in \mathcal{RV} \llbracket \tau_2 \rrbracket \rho\} \\
\mathcal{RV} \llbracket \tau_1 \rightarrow \tau_2 \rrbracket \rho &= \{(k, \lambda x. e, \lambda x. e') \mid \vdash \lambda x. e' : (\tau_1 \rightarrow \tau_2)^{[\rho]} \wedge \\
&\quad \forall j < k, v, v'. \\
&\quad (j, v, v') \in \mathcal{RV} \llbracket \tau_1 \rrbracket \rho \implies \\
&\quad (j, e[v/x], e'[v'/x]) \in \mathcal{RC} \llbracket \tau_2 \rrbracket \rho\} \\
\mathcal{RV} \llbracket \mu\alpha. \tau \rrbracket \rho &= \{(k, \text{fold } v, \text{fold } v') \mid \vdash \text{fold } v' : (\mu\alpha. \tau)^{[\rho]} \wedge \\
&\quad \forall j < k. \\
&\quad \text{let } \chi = \llbracket \mathcal{RV} \llbracket \mu\alpha. \tau \rrbracket \rho \rrbracket_{j+1} \text{ in} \\
&\quad (j, v, v') \in \mathcal{RV} \llbracket \tau \rrbracket \rho[\alpha \mapsto (\chi, (\mu\alpha. \tau)^{[\rho]})]\} \\
\mathcal{RC} \llbracket \tau \rrbracket \rho &= \{(k, e, e') \mid \forall j < k, e_f. \\
&\quad e \mapsto^j e_f \wedge \text{irred}(e_f) \implies \\
&\quad \exists e'_f. e' \mapsto^* e'_f \wedge (k - j, e_f, e'_f) \in \mathcal{RV} \llbracket \tau \rrbracket \rho\} \\
\mathcal{RG} \llbracket \bullet \rrbracket &= \{(k, \emptyset, \emptyset)\} \\
\mathcal{RG} \llbracket \Gamma, x:\tau \rrbracket &= \{(k, \gamma[x \mapsto v], \gamma'[x \mapsto v']) \mid (k, \gamma, \gamma') \in \mathcal{RG} \llbracket \Gamma \rrbracket \wedge (k, v, v') \in \mathcal{RV} \llbracket \tau \rrbracket \emptyset\} \\
\Gamma \vdash e \leq e' : \tau &\stackrel{\text{def}}{=} \Gamma \vdash e : \tau \wedge \Gamma \vdash e' : \tau \wedge \\
&\quad \forall k \geq 0. \forall \gamma, \gamma'. \\
&\quad (k, \gamma, \gamma') \in \mathcal{RG} \llbracket \Gamma \rrbracket \implies (k, \gamma(e), \gamma'(e')) \in \mathcal{RC} \llbracket \tau \rrbracket \emptyset \\
\Gamma \vdash e \sim e' : \tau &\stackrel{\text{def}}{=} \Gamma \vdash e \leq e' : \tau \wedge \Gamma \vdash e' \leq e : \tau
\end{aligned}$$

**Fig. 3.**  $\lambda^{\text{rec}}$  Relational Model (Shaded  $\not\in$  Appel-McAllester)

For any set  $\chi$ , we define the  $k$ -approximation of the set (written  $|\chi|_k$ ) as the subset of its elements whose indices are less than  $k$ .

We define  $Rel_\tau$  (where  $\tau$  is a closed syntactic type) as the set of those sets  $\chi \in 2^{\text{Nat} \times C\text{Values} \times C\text{Values}}$  that have the following two properties: if  $(k, v, v') \in \chi$ , then  $v'$  must be well-typed with type  $\tau$ , and  $\chi$  must be closed with respect to a decreasing step-index.

We use the meta-variable  $\rho$  to denote type substitutions. These are partial maps from type variables  $\alpha$  to pairs  $(\chi, \tau)$  where  $\chi$  is the semantic substitution for  $\alpha$  and  $\tau$  (a closed syntactic type) is the syntactic substitution for  $\alpha$ . We note that our definitions ensure that if  $\rho(\alpha) = (\chi, \tau)$  then  $\chi \in Rel_\tau$ . Since types in  $\lambda^{\text{rec}}$  may contain free type variables, the interpretation of a type  $\tau$  is parametrized by a type substitution  $\rho$  such that  $FTV(\tau) \subseteq \text{dom}(\rho)$ . We use the following abbreviations:

- Let  $\rho(\alpha) = (\chi, \tau)$ . Then  $\rho^{\text{sem}}(\alpha) = \chi$  and  $\rho^{\text{syn}}(\alpha) = \tau$ .
- Let  $\rho = \{\alpha_1 \mapsto (\chi_1, \tau_1), \dots, \alpha_n \mapsto (\chi_n, \tau_n)\}$ .  
Then  $\tau^{[\rho]}$  is an abbreviation for  $\tau[\tau_1/\alpha_1, \tau_2/\alpha_2, \dots, \tau_n/\alpha_n]$ .

Next, we consider the relational interpretation  $\mathcal{RV} \llbracket \tau \rrbracket \rho$  of each type  $\tau$ . In each case, note that if  $(k, v, v') \in \mathcal{RV} \llbracket \tau \rrbracket \rho$  then  $\vdash v' : (\tau)^{[\rho]}$ .

*Booleans.* Two values are related at the type `bool` for any number of steps  $k \geq 0$ , if they are both `tt` or both `ff`.

*Pairs.* The pairs  $\langle v_1, v_2 \rangle$  and  $\langle v'_1, v'_2 \rangle$  are related at type  $\tau_1 \times \tau_2$  for  $k$  steps if  $v_i$  and  $v'_i$  are related for  $k$  steps at the type  $\tau_i$  (for  $i \in \{1, 2\}$ ).

*Functions.* Since functions are suspended computations, their interpretation is given in terms of the interpretation of types as computations (see below). Two functions are related if they map related arguments to related results. Specifically,  $\lambda x. e$  and  $\lambda x. e'$  are related at the type  $\tau_1 \rightarrow \tau_2$  for  $k$  steps if, at some point in the future, when there are  $j < k$  steps left to execute, and there are arguments  $v_a$  and  $v'_a$  that are related at the type  $\tau_1$  for  $j$  steps, then  $e[v_a/x]$  and  $e'[v'_a/x]$  are related as computations of type  $\tau_2$  for  $j$  steps.

*Recursive Types.* One would expect the values `fold`  $v$  and `fold`  $v'$  to be related at the type  $\mu\alpha. \tau$  for  $k$  steps if  $v$  and  $v'$  are related at the type  $\tau[\mu\alpha. \tau/\alpha]$  for  $j < k$  steps. We show that the latter is equivalent to what is required by the definition in Figure 3. Note that by the definition of  $\llbracket \cdot \rrbracket_k$

$$(j, v, v') \in \mathcal{RV} \llbracket \tau[\mu\alpha. \tau/\alpha] \rrbracket \rho \Leftrightarrow (j, v, v') \in \llbracket \mathcal{RV} \llbracket \tau[\mu\alpha. \tau/\alpha] \rrbracket \rho \rrbracket_{j+1} .$$

We prove a type substitution lemma (see [16]) that allows us to conclude that if  $\chi = \llbracket \mathcal{RV} \llbracket \mu\alpha. \tau \rrbracket \rho \rrbracket_{j+1}$  then:

$$\llbracket \mathcal{RV} \llbracket \tau[\mu\alpha. \tau/\alpha] \rrbracket \rho \rrbracket_{j+1} = \llbracket \mathcal{RV} \llbracket \tau \rrbracket \rho[\alpha \mapsto (\chi, (\mu\alpha. \tau)^{[\rho]})] \rrbracket_{j+1} .$$

Hence,

$$\begin{aligned} (j, v, v') \in \mathcal{RV} \llbracket \tau[\mu\alpha. \tau/\alpha] \rrbracket \rho & \\ \Leftrightarrow (j, v, v') \in \llbracket \mathcal{RV} \llbracket \tau[\mu\alpha. \tau/\alpha] \rrbracket \rho \rrbracket_{j+1} & \quad \text{by } \llbracket \cdot \rrbracket_k \\ \Leftrightarrow (j, v, v') \in \llbracket \mathcal{RV} \llbracket \tau \rrbracket \rho[\alpha \mapsto (\chi, (\mu\alpha. \tau)^{[\rho]})] \rrbracket_{j+1} & \quad \text{by type subst} \\ \Leftrightarrow (j, v, v') \in \mathcal{RV} \llbracket \tau \rrbracket \rho[\alpha \mapsto (\chi, (\mu\alpha. \tau)^{[\rho]})] & \quad \text{by } \llbracket \cdot \rrbracket_k \end{aligned}$$

which is exactly what is required by the definition of  $\mathcal{RV} \llbracket \mu\alpha. \tau \rrbracket \rho$ .

*Computations.* Two closed expressions  $e$  and  $e'$  are related as computations of type  $\tau$  for  $k$  steps as follows. If  $e$  steps to an irreducible term  $e_f$  in  $j < k$  steps, then  $e'$  must also step to some irreducible  $e'_f$ . Furthermore, both  $e_f$  and  $e'_f$  must be values that are related for the remaining  $k - j$  steps.

What is surprising about this definition is that  $e$  must terminate in  $j < k$  steps, while  $e'$  may terminate in *any* number of steps, say  $i$ . Hence,  $i$  may be greater than  $k$ . This has ramifications for transitivity in the AM model and we shall return to this point shortly.

*Logical Relation.* If  $\Gamma \vdash e : \tau$  and  $\Gamma \vdash e' : \tau$ , then we write  $\Gamma \vdash e \leq e' : \tau$  to mean that for all  $k \geq 0$ , if  $\gamma$  and  $\gamma'$  are mappings from variables  $x$  to closed values that are related for  $k$  steps at  $\Gamma$ , then  $\gamma(e)$  and  $\gamma'(e')$  are related for  $k$  steps as computations of type  $\tau$ . We say  $e$  and  $e'$  are logically equivalent, written  $\Gamma \vdash e \sim e' : \tau$ , if they logically approximate one another.

We now have to prove that each type  $\tau$  is a valid type — that is, that the relational interpretation of  $\tau$  belongs to  $Rel_\tau$  (i.e.,  $\mathcal{RV} \llbracket \tau \rrbracket \rho \in Rel_{\tau[\rho]}$ ). This involves showing well-typedness and closure under decreasing step-index.

Next, we prove a number of nontrivial lemmas (see the technical report [16]). Specifically, we prove that the logical relation defined in Figure 3 has the compatibility and substitutivity properties (see e.g., [9]). These allow us to show that the  $\lambda^{\text{rec}}$  typing rules preserve the logical relation, and hence prove the following lemma.

**Lemma 3 ( $\lambda^{\text{rec}}$  Fundamental Property / Reflexivity).**

If  $\Gamma \vdash e : \tau$ , then  $\Gamma \vdash e \leq e : \tau$ .

### 2.3 Transitivity and the Appel-McAllester Model

Let us ignore the shaded parts of Figure 3 and try to prove the following lemma with the resulting definitions.

**Proposed Lemma (Transitivity: Appel-McAllester)**

If  $\Gamma \vdash e_1 \leq e_2 : \tau$  and  $\Gamma \vdash e_2 \leq e_3 : \tau$ , then  $\Gamma \vdash e_1 \leq e_3 : \tau$ .

**Proof Attempt:** Suppose  $k \geq 0$  and  $(k, \gamma, \gamma') \in \mathcal{RG} \llbracket \Gamma \rrbracket$ .

Show  $(k, \gamma(e_1), \gamma'(e_3)) \in \mathcal{RC} \llbracket \tau \rrbracket \emptyset$ . Suppose  $j < k$ ,  $\gamma(e_1) \mapsto^j e_{f_1}$ , and  $\text{irred}(e_{f_1})$ .

Show  $\exists e_{f_3}. \gamma'(e_3) \mapsto^* e_{f_3} \wedge (k - j, e_{f_1}, e_{f_3}) \in \mathcal{RV} \llbracket \tau \rrbracket \emptyset$ .

Instantiate  $\Gamma \vdash e_1 \leq e_2 : \tau$  with  $k \geq 0$  and  $(k, \gamma, \gamma') \in \mathcal{RG} \llbracket \Gamma \rrbracket$ .

Hence,  $(k, \gamma(e_1), \gamma'(e_2)) \in \mathcal{RC} \llbracket \tau \rrbracket \emptyset$ .

Instantiate this with  $j < k$ ,  $\gamma(e_1) \mapsto^j e_{f_1}$ , and  $\text{irred}(e_{f_1})$ .

Hence,  $\exists e_{f_2}, i$  such that  $i \geq 0$ ,  $\gamma'(e_2) \mapsto^i e_{f_2}$ , and  $(k - j, e_{f_1}, e_{f_2}) \in \mathcal{RV} \llbracket \tau \rrbracket \emptyset$ .

Now we need to use the premise  $\Gamma \vdash e_2 \leq e_3 : \tau$ . But what should we instantiate this with? We consider two ways we could proceed.

- (i) Instantiate  $\Gamma \vdash e_2 \leq e_3 : \tau$  with  $k, \gamma, \gamma'$ . Note that  $k \geq 0$  and  $(k, \gamma, \gamma') \in \mathcal{RG} \llbracket \Gamma \rrbracket$ . Hence,  $(k, \gamma(e_2), \gamma'(e_3)) \in \mathcal{RC} \llbracket \tau \rrbracket \emptyset$ .

**Problem:** We could instantiate this with  $i$  and  $e_{f_2}$ , but at that point we are stuck since we cannot show  $i < k$  (since  $i$  may be greater than  $k$ ), and we cannot show  $\gamma(e_2) \mapsto^i e_{f_2}$  (we only have  $\gamma'(e_2) \mapsto^i e_{f_2}$ ).

- (ii) Instantiate  $\Gamma \vdash e_2 \leq e_3 : \tau$  with  $i + 1, \gamma', \gamma'$ .

**Problem:** We cannot show  $(i + 1, \gamma', \gamma') \in \mathcal{RG} \llbracket \Gamma \rrbracket$ . All we know is that  $(k, \gamma, \gamma') \in \Gamma$ , where  $i$  may be greater than  $k$ .

We note that if we restrict our attention to closed terms  $e_1, e_2, e_3$ , then the above lemma can be proved. In the case of open terms, however, the status of transitivity of the AM model is unclear as we have been unable to find a counterexample.

There are several things one could attempt in order to rectify the above problem with the AM model (unshaded parts of Figure 3). One problem we encountered was that  $i$  may be greater than  $k$ . To get around this, we could change the definition of  $(k, e, e') \in \mathcal{RC} \llbracket \tau \rrbracket$  to require that  $e'$  must terminate in less than  $k$  steps. Unfortunately, if we step back and examine the resulting meaning of  $\Gamma \vdash e_1 \sim e_2 : \tau$ , we see that the latter now requires that both  $e_1$  and  $e_2$  must terminate in *exactly the same number of steps*. Clearly such a logical relation would not be very useful (unless we are concerned with reasoning about timing leaks in an information-flow setting). Other formulations involving the use of not one, but two step-indices (where the second bounds the number of steps in which  $e'$  must terminate) also lead to models where both terms are required to terminate in exactly the same number of steps.

Since we want a logical relation that considers programs equivalent modulo the number of steps they take, we will not change the definition of  $\mathcal{RC} \llbracket \tau \rrbracket$ . Instead we fix the problem with transitivity by moving to a typed setting where  $(k, v, v') \in \mathcal{RV} \llbracket \tau \rrbracket \emptyset$  implies  $\vdash v' : \tau$ . Assuming the definitions in Figure 3, including the shaded parts, let us again try to prove transitivity.

**Lemma 4 ( $\lambda^{\text{rec}}$  : Transitivity).** *(Our model: Figure 3, including shaded parts)*  
*If  $\Gamma \vdash e_1 \leq e_2 : \tau$  and  $\Gamma \vdash e_2 \leq e_3 : \tau$ , then  $\Gamma \vdash e_1 \leq e_3 : \tau$ .*

*Proof.* We start at the point where we got stuck before. Now from  $(k, \gamma, \gamma') \in \mathcal{RG} \llbracket \Gamma \rrbracket$  we can conclude that  $\vdash \gamma' : \Gamma$ . By reflexivity (Fundamental Property, Lemma 3) it follows that  $\vdash \gamma' \leq \gamma' : \Gamma$ . Hence, we can show that for all  $z \geq 0$ ,  $(z, \gamma', \gamma') \in \mathcal{RG} \llbracket \Gamma \rrbracket$  holds. Now we may instantiate  $\Gamma \vdash e_2 \leq e_3 : \tau$  above with  $i+1$  since we know that  $(i+1, \gamma', \gamma') \in \mathcal{RG} \llbracket \Gamma \rrbracket$ . The rest of the proof is relatively straightforward and is given in the accompanying technical report [16].

*Seemingly Asymmetric Well-Typedness Requirement.* The definitions in Figure 3 may have left the reader with the impression that we only require terms on one side of our logical relation to be well-typed. This, however, is not the case. In particular, notice that in the definition of  $\Gamma \vdash e \leq e' : \tau$ , we require that *both*  $e$  and  $e'$  be well-typed. However, once we have picked a step-index  $k$  (i.e., once we have moved under the  $\forall k$  quantifier), there is an asymmetry in the model in that when  $(k, e, e') \in \mathcal{RC} \llbracket \tau \rrbracket$ ,  $k$  pertains (as a bound) only to  $e$  and not to  $e'$ . As a result of this asymmetry, when working with a specific  $k$  (in the definition of  $\mathcal{RV} \llbracket \tau \rrbracket$ ) we do not need to know that  $v$  has type  $\tau$  in the limit, while the converse is true of  $v'$ . Hence, at the value interpretation level  $\mathcal{RV} \llbracket \tau \rrbracket$ , we chose only to require  $\vdash v' : \tau$ . One could add the requirement  $\vdash v : \tau$  in the interest of symmetry, but it would simply lead to additional proof obligations being shuffled around. It would also complicate definitions when we get to quantified types as  $Rel_\tau$  would have to be replaced by  $Rel_{\tau_1, \tau_2}$  (since in the presence of quantified types we wish to relate values of different types).

## 2.4 $\lambda^{\text{rec}}$ : Soundness

To prove that our logical relation is sound with respect to contextual equivalence, we first define what it means for two contexts to be logically related.



**Definition 5** ( $\lambda^{\text{rec}}$  Logical Relation: Contexts).
$$\Gamma_1 \vdash C \leq C' : (\Gamma \triangleright \tau) \rightsquigarrow \tau_1 \stackrel{\text{def}}{=} \forall e, e'. \Gamma \vdash e \leq e' : \tau \implies \Gamma_1 \vdash C[e] \leq C'[e'] : \tau_1$$

Next, we prove the compatibility lemmas for contexts, which allows us to prove the following.

**Lemma 6** ( $\lambda^{\text{rec}}$  Reflexivity: Contexts).

If  $\Gamma_1 \vdash C : (\Gamma \triangleright \tau) \rightsquigarrow \tau_1$ , then  $\Gamma_1 \vdash C \leq C : (\Gamma \triangleright \tau) \rightsquigarrow \tau_1$ .

**Theorem 7** ( $\lambda^{\text{rec}}$  Soundness:  $\leq \subseteq \preceq^{\text{ctx}}$ ).

If  $\Gamma \vdash e \leq e' : \tau$  then  $\Gamma \vdash e \preceq^{\text{ctx}} e' : \tau$ .

*Proof.* Suppose  $\bullet \vdash C : (\Gamma \triangleright \tau) \rightsquigarrow \tau_1$  and  $C[e] \Downarrow$ . Hence, there exist  $v_f, k$  such that  $C[e] \mapsto^k v_f$ . We must show  $C[e'] \Downarrow$ .

Applying Lemma 6 to  $\bullet \vdash C : (\Gamma \triangleright \tau) \rightsquigarrow \tau_1$ , we have  $\bullet \vdash C \leq C : (\Gamma \triangleright \tau) \rightsquigarrow \tau_1$ .

Instantiate this with  $\Gamma \vdash e \leq e' : \tau$ . Hence,  $\bullet \vdash C[e] \leq C[e'] : \tau_1$ .

Instantiate this with  $k+1 \geq 0$  and  $(k+1, \emptyset, \emptyset) \in \mathcal{RG} \llbracket \bullet \rrbracket$ .

Hence,  $(k+1, C[e], C[e']) \in \mathcal{RC} \llbracket \tau_1 \rrbracket \emptyset$ .

Instantiate this with  $k < k+1$ ,  $C[e] \mapsto^k v_f$ , and  $\text{irred}(v_f)$ .

Hence, exists  $v'_f$  such that  $C[e'] \mapsto^* v'_f$ . Hence,  $C[e'] \Downarrow$ .

**2.5  $\lambda^{\text{rec}}$ : Completeness**

To show that our logical relation is complete with respect to contextual equivalence, we make use of the notion of *ciu-equivalence* introduced by Mason and Talcott [18]. Two closed terms of the same closed type are said to be *ciu-equivalent* if they have the same termination behavior in any evaluation context  $E$  (a use of the term). The relation is extended to open terms via closing substitutions (i.e., closed instantiations). We note that evaluation contexts  $E$  are a simply a subset of general contexts  $C$  and that only closed terms can be placed in an evaluation context.

**Definition 8** ( $\lambda^{\text{rec}}$  Ciu Approximation  $\preceq^{\text{ciu}}$  & Equivalence  $\simeq^{\text{ciu}}$ ). Let  $\Gamma \vdash e : \tau$  and  $\Gamma \vdash e' : \tau$ .

$$\Gamma \vdash e \preceq^{\text{ciu}} e' : \tau \stackrel{\text{def}}{=} \forall \gamma, E, \tau_1. \bullet \vdash \gamma : \Gamma \wedge \bullet \vdash E : (\bullet \triangleright \tau) \rightsquigarrow \tau_1 \wedge E[\gamma(e)] \Downarrow \implies E[\gamma(e')] \Downarrow$$

$$\Gamma \vdash e \simeq^{\text{ciu}} e' : \tau \stackrel{\text{def}}{=} \Gamma \vdash e \preceq^{\text{ciu}} e' : \tau \wedge \Gamma \vdash e' \preceq^{\text{ciu}} e : \tau$$

**Theorem 9** ( $\lambda^{\text{rec}} : \preceq^{\text{ctx}} \subseteq \preceq^{\text{ciu}}$ ). If  $\Gamma \vdash e \preceq^{\text{ctx}} e' : \tau$  then  $\Gamma \vdash e \preceq^{\text{ciu}} e' : \tau$ .

To prove that two *ciu-equivalent* terms are logically related, we will need the following lemma which shows that our logical relation respects *ciu equivalence*. Pitts [9] proves a similar property which he calls “equivalence-respecting”.

**Lemma 10** ( $\lambda^{\text{rec}}$  Equivalence-Respecting: Closed Values). If  $(k, v_1, v_2) \in \mathcal{RV} \llbracket \tau \rrbracket \emptyset$  and  $\bullet \vdash v_2 \preceq^{\text{ciu}} v_3 : \tau$ , then  $(k, v_1, v_3) \in \mathcal{RV} \llbracket \tau \rrbracket \emptyset$ .

*Proof.* By induction on  $k$  and nested induction on the structure of the (closed) type  $\tau$ .

**Theorem 11** ( $\lambda^{\text{rec}} : \preceq^{\text{ciu}} \subseteq \leq$ ). *If  $\Gamma \vdash e \preceq^{\text{ciu}} e' : \tau$  then  $\Gamma \vdash e \leq e' : \tau$ .*

*Proof.* Suppose  $k \geq 0$  and  $(k, \gamma, \gamma') \in \mathcal{RG}[\Gamma]$ . Show  $(k, \gamma(e), \gamma'(e')) \in \mathcal{RC}[\tau] \emptyset$ . Suppose  $j < k$ ,  $\gamma(e) \mapsto^j e_f$ , and  $\text{irred}(e_f)$ .

Show  $\exists e'_f. \gamma'(e') \mapsto^* e'_f \wedge (k - j, e_f, e'_f) \in \mathcal{RV}[\tau] \emptyset$ .

From  $\Gamma \vdash e \preceq^{\text{ciu}} e' : \tau$ , we have  $\Gamma \vdash e : \tau$ . Applying Lemma 3 to  $\Gamma \vdash e : \tau$ , we have  $\Gamma \vdash e \leq e : \tau$ . Instantiate this with  $k \geq 0$  and  $(k, \gamma, \gamma') \in \mathcal{RG}[\Gamma]$ . Hence,  $(k, \gamma(e), \gamma'(e)) \in \mathcal{RC}[\tau] \emptyset$ . Instantiate this with  $j < k$ ,  $\gamma(e) \mapsto^j e_f$ , and  $\text{irred}(e_f)$ . Hence,  $\exists e'_f$  such that  $\gamma'(e) \mapsto^* e'_f$  and  $(k - j, e_f, e'_f) \in \mathcal{RV}[\tau] \emptyset$ . Hence,  $e_f \equiv v_f$  and  $e'_f \equiv v'_f$ . Hence,  $\gamma'(e) \Downarrow v'_f$ .

Instantiate  $\Gamma \vdash e \preceq^{\text{ciu}} e' : \tau$  with  $\vdash \gamma' : \Gamma$  (follows from  $(k, \gamma, \gamma') \in \mathcal{RG}[\Gamma]$ ), and  $\bullet \vdash [\cdot] : (\bullet \triangleright \tau) \rightsquigarrow \tau$ , and  $\gamma'(e) \Downarrow$ . Hence,  $\exists v''_f$  such that  $\gamma'(e') \mapsto^* v''_f$ .

Remains to show:  $(k - j, v_f, v''_f) \in \mathcal{RV}[\tau] \emptyset$ .

This follows from Lemma 10 applied to  $(k - j, v_f, v''_f) \in \mathcal{RV}[\tau] \emptyset$  and  $v'_f \preceq^{\text{ciu}} v''_f : \tau$  (which follows from  $\Gamma \vdash e \preceq^{\text{ciu}} e' : \tau$  and  $\gamma'(e) \Downarrow v'_f$  and  $\gamma'(e') \Downarrow v''_f$ ).

### 3 Type Abstraction

We now extend  $\lambda^{\text{rec}}$  with impredicative universal and existential types; we call the extended language the  $\lambda^{\forall\exists}$ -calculus. The syntactic extensions to support quantified types are as follows:

$$\begin{array}{ll} \text{Types} & \tau ::= \dots \mid \forall \alpha. \tau \mid \exists \alpha. \tau \\ \text{Values} & v ::= \dots \mid \Lambda. e \mid \text{pack } v \\ \text{Expressions } e & ::= \dots \mid e [] \mid \text{unpack } e_1 \text{ as } x \text{ in } e_2 \end{array}$$

Note that terms are not decorated with types (which was also the case for  $\lambda^{\text{rec}}$ ). Here we let the vestigial operators remain in the untyped syntax in order to preserve the operational semantics. For instance, the term  $\Lambda. e$  is a suspended computation (normally written  $\Lambda \alpha. e$ );  $e []$  runs the suspended computation. We extend the  $\lambda^{\text{rec}}$  operational semantics as follows:

$$\text{Evaluation Contexts } E ::= \dots \mid E [] \mid \text{unpack } E \text{ as } x \text{ in } e$$

$$\text{(inst)} \quad (\Lambda. e) [] \mapsto e$$

$$\text{(unpack)} \quad \text{unpack } (\text{pack } v) \text{ as } x \text{ in } e \mapsto e[v/x]$$

$\lambda^{\forall\exists}$  typing judgments have the form  $\Delta; \Gamma \vdash e : \tau$ , where the context  $\Gamma$  is as before, and the context  $\Delta$  is defined as follows:

$$\text{Type Context } \Delta ::= \bullet \mid \Delta, \alpha .$$

The type context  $\Delta$  is used to track the set of type variables in scope. We modify the typing rules in Figure 2 by adding  $\Delta$  to each typing judgment. Figure 4 gives the typing rules for the additional terms in  $\lambda^{\forall\exists}$ . We prove soundness of the  $\lambda^{\forall\exists}$  typing rules, show that value and type substitution hold, and prove type safety.

$$\boxed{\Delta; \Gamma \vdash e : \tau}$$

$$\begin{array}{c}
\text{(All)} \frac{\Delta, \alpha; \Gamma \vdash e : \tau}{\Delta; \Gamma \vdash \lambda. e : \forall \alpha. \tau} \qquad \text{(Inst)} \frac{\Delta; \Gamma \vdash e : \forall \alpha. \tau \quad \Delta \vdash \tau_1}{\Delta; \Gamma \vdash e[] : \tau[\tau_1/\alpha]} \\
\text{(Pack)} \frac{\Delta \vdash \tau_1 \quad \Delta; \Gamma \vdash e : \tau[\tau_1/\alpha]}{\Delta; \Gamma \vdash \text{pack } e : \exists \alpha. \tau} \qquad \text{(Unpack)} \frac{\Delta; \Gamma \vdash e_1 : \exists \alpha. \tau_1 \quad \Delta \vdash \tau_2}{\Delta, \alpha; \Gamma, x : \tau_1 \vdash e_2 : \tau_2} \\
\Delta; \Gamma \vdash \text{unpack } e_1 \text{ as } x \text{ in } e_2 : \tau_2
\end{array}$$

Fig. 4.  $\lambda^{\forall\exists}$  Static Semantics

**Theorem 12** ( $\lambda^{\forall\exists}$  Safety). *If  $\bullet; \bullet \vdash e : \tau$  and  $e \mapsto^* e'$ , then either  $e'$  is a value, or there exists an  $e''$  such that  $e' \mapsto e''$ .*

### 3.1 $\lambda^{\forall\exists}$ : Contextual Equivalence

Typing judgments for contexts  $C$  now have the form  $\Delta_1; \Gamma_1 \vdash C : (\Delta; \Gamma \triangleright \tau) \rightsquigarrow \tau_1$  (where  $(\Delta; \Gamma \triangleright \tau)$  represents the type of the hole) indicating that whenever  $\Delta; \Gamma \vdash e : \tau$ , then  $\Delta_1; \Gamma_1 \vdash C[e] : \tau_1$ .

**Definition 13** ( $\lambda^{\forall\exists}$  Contextual Approximation  $\preceq^{ctx}$ ).

*If  $\Delta; \Gamma \vdash e : \tau$  and  $\Delta; \Gamma \vdash e' : \tau$ , then we write  $\Delta; \Gamma \vdash e \preceq^{ctx} e' : \tau$  to mean*

$$\forall C, \tau_1. \bullet; \bullet \vdash C : (\Delta; \Gamma \triangleright \tau) \rightsquigarrow \tau_1 \wedge C[e] \Downarrow \implies C[e'] \Downarrow .$$

### 3.2 $\lambda^{\forall\exists}$ : Logical Relation

As in the case of  $\lambda^{\text{rec}}$ , the relational interpretation of a type  $\mathcal{RV}[\tau] \rho$  in  $\lambda^{\forall\exists}$  is a set of triples of the form  $(k, v, v')$ . However, there is now one additional property (in addition to well-typedness of the second value of each tuple and closure under decreasing step-index) that every set  $\chi$  in  $Rel_\tau$  must satisfy. To motivate this property, we take the reader back to the proof of completeness of  $\lambda^{\text{rec}}$ , specifically to Lemma 10 which establishes that the relational value interpretation  $\mathcal{RV}[\tau]$  is equivalence-respecting. The proof of that lemma requires induction on  $k$  and nested induction on the structure of the closed type  $\tau$ . In the case of  $\lambda^{\forall\exists}$ , when we get to the proof of the corresponding lemma,  $\tau$  may have free type variables. Thus, one of the cases we must consider for the inner induction is  $\tau = \alpha$ . Assuming that  $\rho(\alpha) = (\chi, \tau_\alpha)$ , we will be required to show that if  $(k, v_1, v_2) \in \mathcal{RV}[\alpha] \rho \equiv \rho^{\text{sem}}(\alpha) \equiv \chi$  and  $\vdash v_2 \preceq^{ciu} v_3 : \alpha^{[\rho]}$  (where  $\alpha^{[\rho]} \equiv \tau_\alpha$ ), then  $(k, v_1, v_3) \in \chi$ . Note that  $\chi \in Rel_{\tau_\alpha}$ . Thus, we must add this requirement directly to the definition of  $Rel_\tau$ .

A more informal justification is that in the presence of quantified types, we can instantiate a type variable with a relational interpretation of our own choosing. Thus, we have to show that the relation we pick satisfies certain properties, one of which is that it must be equivalence-respecting.

The modified definition of  $Rel_\tau$  is given below. It makes use of a notion of  $ciu$ -equivalence restricted to closed values.

$$v \prec^{ciu} v' : \tau \stackrel{\text{def}}{=} \forall E, \tau_1. \bullet; \bullet \vdash E : (\bullet; \bullet \triangleright \tau) \rightsquigarrow \tau_1 \wedge E[v] \Downarrow \implies E[v'] \Downarrow$$

$$\begin{aligned} Rel_{\tau} \stackrel{\text{def}}{=} \{ \chi \in 2^{Nat \times CValues \times CValues} \mid \\ \forall (j, v, v') \in \chi. \vdash v' : \tau \wedge \\ \forall i \leq j. (i, v, v') \in \chi \wedge \\ (\forall v''. v' \prec^{ciu} v'' : \tau \implies (j, v, v'') \in \chi) \} \end{aligned}$$

The relational interpretation of universal and existential types is given in Figure 5. Two values  $\text{pack } v$  and  $\text{pack } v'$  are related at the type  $\exists \alpha. \tau$  for  $k$  steps if there exists a syntactic type  $\tau_2$  and a semantic interpretation  $\chi \in Rel_{\tau_2}$  such that for all  $j < k$ ,  $(j, v, v') \in \mathcal{RV}[\tau] \rho[\alpha \mapsto (\chi, \tau_2)]$ . Here we only pick a type  $\tau_2$  for the second value  $v'$  while the type of  $v$  is left unrestricted. Intuitively, this suffices because when showing logical equivalence of two terms  $(\Delta; \Gamma \vdash e \sim e' : \tau)$ , we pick a type for  $v'$  while proving  $\Delta; \Gamma \vdash e \leq e' : \tau$  and we pick a type for  $v$  while proving  $\Delta; \Gamma \vdash e' \leq e : \tau$ . The relational interpretation of universal types is the dual of existential types.

$$\begin{aligned} \mathcal{RV}[\forall \alpha. \tau] \rho = \{ (k, \Lambda, e, \Lambda, e') \mid \vdash \Lambda, e' : (\forall \alpha. \tau)^{[\rho]} \wedge \\ \forall \tau_2, \chi. \chi \in Rel_{\tau_2} \implies \\ \forall j < k. (j, e, e') \in \mathcal{RC}[\tau] \rho[\alpha \mapsto (\chi, \tau_2)] \} \end{aligned}$$

$$\begin{aligned} \mathcal{RV}[\exists \alpha. \tau] \rho = \{ (k, \text{pack } v, \text{pack } v') \mid \vdash \text{pack } v' : (\exists \alpha. \tau)^{[\rho]} \wedge \\ \exists \tau_2, \chi. \chi \in Rel_{\tau_2} \wedge \\ \forall j < k. (j, v, v') \in \mathcal{RV}[\tau] \rho[\alpha \mapsto (\chi, \tau_2)] \} \end{aligned}$$

$$\begin{aligned} \mathcal{RD}[\bullet] &= \{\emptyset\} \\ \mathcal{RD}[\Delta, \alpha] &= \{ \rho[\alpha \mapsto (\chi, \tau_2)] \mid \rho \in \mathcal{RD}[\Delta] \wedge \chi \in Rel_{\tau_2} \} \end{aligned}$$

$$\begin{aligned} \mathcal{RG}[\bullet] \rho &= \{ (k, \emptyset, \emptyset) \} \\ \mathcal{RG}[\Gamma, x : \tau] \rho &= \{ (k, \gamma[x \mapsto v], \gamma'[x \mapsto v']) \mid (k, \gamma, \gamma') \in \mathcal{RG}[\Gamma] \rho \wedge (k, v, v') \in \mathcal{RV}[\tau] \rho \} \end{aligned}$$

$$\begin{aligned} \Delta; \Gamma \vdash e \leq e' : \tau \stackrel{\text{def}}{=} \Delta; \Gamma \vdash e : \tau \wedge \Delta; \Gamma \vdash e' : \tau \wedge \\ \forall k \geq 0. \forall \rho, \gamma, \gamma'. \rho \in \mathcal{RD}[\Delta] \wedge (k, \gamma, \gamma') \in \mathcal{RG}[\Gamma] \rho \implies \\ (k, \gamma(e), \gamma'(e')) \in \mathcal{RC}[\tau] \rho \end{aligned}$$

**Fig. 5.**  $\lambda^{\forall\exists}$  Relational Model

The relational interpretation of types as computations is defined exactly as before. The definition of the logical relation  $\Delta; \Gamma \vdash e \leq e' : \tau$  appears in Figure 5.

We prove that each type  $\tau$  is a valid type:  $\mathcal{RV}[\tau] \rho \in Rel_{\tau^{[\rho]}}$ . Specifically, we have to show well-typedness, closure under decreasing step-index, and the following lemma.

**Lemma 14** ( $\lambda^{\forall\exists}$  **Rel Equivalence-Respecting**). *Let  $\rho \in \mathcal{RD}[\Delta]$  and  $\Delta \vdash \tau$ . If  $(k, v_1, v_2) \in \mathcal{RV}[\tau] \rho$  and  $v_2 \prec^{ciu} v_3 : \tau^{[\rho]}$ , then  $(k, v_1, v_3) \in \mathcal{RV}[\tau] \rho$ .*

To show the Fundamental Property of the logical relation, we prove the new set of compatibility lemmas, as well as value and type substitutivity.

**Lemma 15** ( $\lambda^{\forall\exists}$  **Fundamental Property / Reflexivity**).

If  $\Delta; \Gamma \vdash e : \tau$  then  $\Delta; \Gamma \vdash e \leq e : \tau$ .

**3.3**  $\lambda^{\forall\exists}$  **Soundness and Completeness**

We prove that the logical relation in Figure 5 is sound with respect to contextual equivalence. The overall proof structure is the same as for  $\lambda^{\text{rec}}$ .

**Theorem 16** ( $\lambda^{\forall\exists} : \leq \subseteq \preceq^{\text{ctx}} \subseteq \preceq^{\text{ciu}}$ ). If  $\Delta; \Gamma \vdash e \leq e' : \tau$  then  $\Delta; \Gamma \vdash e \preceq^{\text{ctx}} e' : \tau$ .

To establish completeness, we again rely on the notion of ciu-equivalence, which we define for  $\lambda^{\forall\exists}$  as follows.

**Definition 17** ( $\lambda^{\forall\exists}$  **Ciu Approximation**  $\preceq^{\text{ciu}}$ ).

Let  $\Delta; \Gamma \vdash e : \tau$  and  $\Delta; \Gamma \vdash e' : \tau$ . If  $\delta$  is a mapping from type variables  $\alpha$  to closed syntactic types  $\tau$ , we write  $\delta \models \Delta$  whenever  $\text{dom}(\delta) = \Delta$ .

$$\Delta; \Gamma \vdash e \preceq^{\text{ciu}} e' : \tau \stackrel{\text{def}}{=} \forall \delta, \gamma, E, \tau_1. \delta \models \Delta \wedge \vdash \gamma : \delta(\Gamma) \wedge \\ \bullet; \bullet \vdash E : (\bullet; \bullet \triangleright \delta(\tau)) \rightsquigarrow \tau_1 \wedge \\ E[\gamma(e)] \Downarrow \implies E[\gamma(e')] \Downarrow$$

**Theorem 18** ( $\lambda^{\forall\exists} : \preceq^{\text{ctx}} \subseteq \preceq^{\text{ciu}} \subseteq \leq$ ).

If  $\Delta; \Gamma \vdash e \preceq^{\text{ctx}} e' : \tau$  then  $\Delta; \Gamma \vdash e \preceq^{\text{ciu}} e' : \tau$ .

If  $\Delta; \Gamma \vdash e \preceq^{\text{ciu}} e' : \tau$  then  $\Delta; \Gamma \vdash e \leq e' : \tau$ .

**3.4 Example: Simple Existential Packages**

For lack of space, we present only one simple example (from Sumii and Pierce[19]) to illustrate the use of our logical relation to prove contextual equivalence. Additional examples involving existential packages, recursive types, and higher-order functions are given in the technical report [16].

**Notation:** Let  $\chi$  be a set of tuples of the form  $(k, v, v')$  such that  $\vdash v' : \tau$ . We define the closure of  $\chi$  under ciu approximation at type  $\tau$  as follows:

$$\chi_\tau^* = \{(k, v_1, v_2) \mid (k, v_1, v_2) \in \chi \vee ((k, v_1, v) \in \chi \wedge v \preceq^{\text{ciu}} v_2 : \tau)\}$$

**Example:** Consider the following existential packages  $e$  and  $e'$  of type  $\tau$ :

$$e = \text{pack} \langle 1, \lambda x. x \stackrel{\text{int}}{=} 0 \rangle \quad e' = \text{pack} \langle \text{tt}, \lambda x. \neg x \rangle \quad \tau = \exists \alpha. \alpha \times (\alpha \rightarrow \text{bool})$$

Show  $\bullet; \bullet \vdash e \sim e' : \tau$ . We only show  $\bullet; \bullet \vdash e \leq e' : \tau$ .  $\bullet; \bullet \vdash e' \leq e : \tau$  is symmetric.

Suppose  $k \geq 0$ . Unwinding definitions, we must show  $(k, e, e') \in \mathcal{RV} \llbracket \tau \rrbracket \equiv$

$$(k, \text{pack} \langle 1, \lambda x. x \stackrel{\text{int}}{=} 0 \rangle, \text{pack} \langle \text{tt}, \lambda x. \neg x \rangle) \in \mathcal{RV} \llbracket \exists \alpha. \alpha \times (\alpha \rightarrow \text{bool}) \rrbracket \emptyset.$$

Let  $\chi_0 = \{(k', 1, \text{tt}) \mid k' \geq 0\}$ . Take  $\tau_2 = \text{bool}$  and  $\chi = (\chi_0)_{\text{bool}}^*$ .

Note that  $\chi \in \text{Rel}_{\text{bool}}$  (from defn of  $(\chi_0)_{\text{bool}}^*$ ). Suppose  $j < k$ .

Show  $(j, \langle 1, \lambda x. x \stackrel{\text{int}}{=} 0 \rangle, \langle \text{tt}, \lambda x. \neg x \rangle) \in \mathcal{RV} \llbracket \alpha \times (\alpha \rightarrow \text{bool}) \rrbracket \emptyset[\alpha \mapsto (\chi, \text{bool})]$ , which follows from:

- $\vdash \langle \text{tt}, \lambda x. \neg x \rangle : (\alpha \times (\alpha \rightarrow \text{bool}))[\text{bool}/\alpha]$
- $(j, 1, \text{tt}) \in \mathcal{RV} \llbracket \alpha \rrbracket \emptyset[\alpha \mapsto (\chi, \text{bool})] \equiv (j, 1, \text{tt}) \in \chi$  (by defn of  $\mathcal{RV} \llbracket \alpha \rrbracket \rho$ )  
which follows from  $\chi \supseteq \chi_0 \supseteq \{(j, 1, \text{tt})\}$ , which follows from defn of  $\chi$ .

- $(j, (\lambda x. x \stackrel{\text{int}}{=} 0), (\lambda x. \neg x)) \in \mathcal{RV} \llbracket \alpha \rightarrow \text{bool} \rrbracket \emptyset[\alpha \mapsto (\chi, \text{bool})]$ , which follows from:
  - First, note that  $\vdash \lambda x. \neg x : (\alpha \rightarrow \text{bool})[\text{bool}/\alpha] \equiv \vdash \lambda x. \neg x : \text{bool} \rightarrow \text{bool}$ .
  - Next, suppose  $i < j$ , and  $(i, v_1, v'_1) \in \mathcal{RV} \llbracket \alpha \rrbracket \emptyset[\alpha \mapsto (\chi, \text{bool})]$ .
  - Note that  $\mathcal{RV} \llbracket \alpha \rrbracket \emptyset[\alpha \mapsto (\chi, \text{bool})] \equiv \chi$  by defn of  $\mathcal{RV} \llbracket \alpha \rrbracket \rho$ . Hence,  $(i, v_1, v'_1) \in \chi$ .
  - Then, from defn of  $\chi$ ,  $v_1 = 1$  and, using more subtle reasoning,  $v'_1 = \text{tt}$ .
  - Show:  $(i, (x \stackrel{\text{int}}{=} 0)[v_1/x], (\neg x)[v'_1/x]) \in \mathcal{RC} \llbracket \text{bool} \rrbracket \emptyset[\alpha \mapsto (\chi, \text{bool})]$ 
    - $\equiv (i, v_1 \stackrel{\text{int}}{=} 0, \neg v'_1) \in \mathcal{RC} \llbracket \text{bool} \rrbracket \emptyset[\alpha \mapsto (\chi, \text{bool})]$
    - $\equiv (i, 1 \stackrel{\text{int}}{=} 0, \neg \text{tt}) \in \mathcal{RC} \llbracket \text{bool} \rrbracket \emptyset[\alpha \mapsto (\chi, \text{bool})]$  .
  - Note that  $(1 \stackrel{\text{int}}{=} 0) \mapsto^1 \text{ff}$  and  $(\neg \text{tt}) \mapsto^* \text{ff}$ . Hence, remains to show:  $(i - 1, \text{ff}, \text{ff}) \in \mathcal{RV} \llbracket \text{bool} \rrbracket \emptyset[\alpha \mapsto (\chi, \text{bool})]$ , which is immediate.

## 4 Related Work and Conclusion

Logical relations were first developed for denotational semantics of typed  $\lambda$ -calculi (e.g., [1, 2]). Early examples of the use of logical relations based on operational semantics include Tait’s [4] proof of strong normalization of the simply typed  $\lambda$ -calculus, and Girard’s method of reducibility candidates [5] used to prove normalization for System F.

Pitts [7, 6, 9] developed syntactic logical relations for a  $\lambda$ -calculus with recursive functions and quantified types (but no recursive types). To support recursive functions without using denotational techniques, Pitts makes use of  $\top\top$ -closure (or biorthogonality [12]). Relations that are  $\top\top$ -closed can be immediately shown to be equivalence-respecting and admissible [9]. In comparison, we directly require that our relations be equivalence-respecting and closed under decreasing step-index — the latter, effectively, gives us admissibility.

Birkedal and Harper [10] and Crary and Harper [8] extended syntactic logical relations with recursive types (the latter also support polymorphic types) by adapting Pitts’ minimal invariance [3] technique for use in a purely syntactic setting. Mellès and Vouillon [12, 11] construct a realizability model of a language with recursive types and polymorphism based on intuitions from the ideal model of types [20]. They also present a relational model based on an orthogonality relation between quadruples of terms and contexts [12]. We note that to show completeness, they too must move to a typed setting. An issue that merits further investigation is the relationship between the different notions of approximation — i.e., syntactic projections [8], interval types [12], and step counts.

Contextual equivalence may also be proved using bisimulations. Sumii and Pierce [19] present a bisimulation for recursive and quantified types. Using their examples as a point of comparison (see [16]) we show that our logical relations are somewhat easier to use when proving contextual equivalence. Also, unlike logical relations, Sumii and Pierce note that their bisimulation cannot be used to derive free theorems [21] based only on types.

We have presented a step-indexed logical relation for recursive and impredicative quantified types. The construction is far more elementary than that of

existing logical relations for such types. In future work, we hope to scale this up to support dynamically allocated (ML-style) mutable references.

## References

1. Plotkin, G.D.: Lambda-definability and logical relations. Memorandum SAI-RM-4, University of Edinburgh, Edinburgh, Scotland (1973)
2. Statman, R.: Logical relations and the typed  $\lambda$ -calculus. *Information and Control* **65**(2-3) (1985) 85–97
3. Pitts, A.M.: Relational properties of domains. *Information and Computation* **127**(2) (1996) 66–90
4. Tait, W.W.: Intensional interpretations of functionals of finite type i. *Journal of Symbolic Logic* **32**(2) (1967) 198–212
5. Girard, J.Y.: *Interprétation Fonctionnelle et Élimination des Coupures de l'Arithmétique d'Ordre Supérieur*. Thèse de doctorat d'état, Université Paris VII, Paris, France (1972)
6. Pitts, A.M.: Parametric polymorphism and operational equivalence. *Mathematical Structures in Computer Science* **10** (2000) 321–359
7. Pitts, A.M.: Existential types: Logical relations and operational equivalence. *Lecture Notes in Computer Science* **1443** (1998) 309–326
8. Crary, K., Harper, R.: Syntactic logical relations over polymorphic and recursive types. Draft (2000)
9. Pitts, A.M.: Typed operational reasoning. In Pierce, B.C., ed.: *Advanced Topics in Types and Programming Languages*. MIT Press (2005)
10. Birkedal, L., Harper, R.: Relational interpretations of recursive types in an operational setting. In: *Theoretical Aspects of Computer Software (TACS)*. (1997)
11. Melliès, P.A., Vouillon, J.: Semantic types: A fresh look at the ideal model for types. In: *POPL*, Venice, Italy. (2004)
12. Melliès, P.A., Vouillon, J.: Recursive polymorphic types and parametricity in an operational framework. In: *LICS*, Chicago, Illinois. (2005)
13. Appel, A.W., McAllester, D.: An indexed model of recursive types for foundational proof-carrying code. *ACM TOPLAS* **23**(5) (2001) 657–683
14. Ahmed, A., Appel, A.W., Virga, R.: An indexed model of impredicative polymorphism and mutable references. Available at <http://www.cs.princeton.edu/~appel/papers/impred.pdf> (2003)
15. Ahmed, A.J.: *Semantics of Types for Mutable State*. PhD thesis, Princeton University (2004)
16. Ahmed, A.: Step-indexed syntactic logical relations for recursive and quantified types. Technical Report TR-01-06, Harvard University (2006)
17. Pierce, B.C.: *Types and Programming Languages*. MIT Press (2002)
18. Mason, I.A., Talcott, C.L.: Equivalence in functional languages with effects. *Journal of Functional Programming* **1**(3) (1991) 287–327
19. Sumii, E., Pierce, B.C.: A bisimulation for type abstraction and recursion. In: *POPL*, Long Beach, California. (2005) 63–74
20. MacQueen, D., Plotkin, G., Sethi, R.: An ideal model for recursive polymorphic types. *Information and Computation* **71**(1/2) (1986) 95–130
21. Wadler, P.: Theorems for free! In: *ACM Symposium on Functional Programming Languages and Computer Architecture (FPCA)*, London (1989)