Trace Semantics for Polymorphic References
Jaber, G; TZEVELEKOS, NP; Logic in Computer Science (LICS)

Copyright 2016 held by Owner/Author. Publication Rights Licensed to ACM. Copyright © 2016 ACM
This is a pre-copyedited, author-produced version of an article accepted for publication in
LICS ’16 Proceedings of the 31st Annual ACM/IEEE Symposium on Logic in Computer
Science following peer review. The version of record is available
http://dl.acm.org/citation.cfm?id=2934509

For additional information about this publication click this link.
http://qmro.qmul.ac.uk/xmlui/handle/123456789/13081

Information about this research object was correct at the time of download; we occasionally
make corrections to records, please therefore check the published record when citing. For
more information contact scholarlycommunications@qmul.ac.uk
Trace semantics for polymorphic references

Guilhem Jaber
Université Paris Diderot

Nikos Tzevelekos
Queen Mary University of London

Abstract

We introduce a trace semantics for a call-by-value language with full polymorphism and higher-order references. This is an operational game semantics model based on a nominal interpretation of parametricity whereby polymorphic values are abstracted with special kinds of names. The use of polymorphic references leads to violations of parametricity which we counter by closely recording the disclosure of typing information in the semantics. We prove the model sound for the full language and strengthen our result to full abstraction for a large fragment where polymorphic references obey specific inhabitation conditions.

1. Introduction

Polymorphism is a prevalent feature of modern programming languages, allowing one to use generic data structures and powerful code abstractions. Reasoning with polymorphism is both challenging and rewarding: polymorphic code is bound to have uniform behaviour under different instantiations, a property known as parametricity [27] and formalized by Reynolds as relational parametricity [25], which in turn provides “theorems for free” [29]. Understanding the formal semantics of polymorphism amounts to capturing the parametric behaviour of code under different instantiations. This has traditionally been hard, effectively due to the requirement for a model where instantiations from within the same model are possible. As far as the full abstraction problem is concerned, the construction of fully abstract models has so far had successes in the game semantics framework. The problem has so far been addressed by use of hypergames by Hughes [9], whereby game arenas can be seen as moves which can be opened inside enclosing arenas during a play. The model of Abramsky and Jagadeesan [1] followed a different approach, namely that of fixing a universe of moves with holes, the latter representing type variables awaiting instantiation, and constructing arenas from that given pool of moves, which is effectively closed under instantiation. While these models addressed purely functional languages, in recent years a remarkable research programme by Laird [18] has extended the reach of polymorphic games to languages with higher-order state.

An important aspect of previous models [9] [19] [18], and of the modelled languages, is the uniformity of polymorphic behaviour. However, when we move to languages with mutable references that can extrude their scope, this property can be easily broken as we see below. Thus, the modelling of languages with ML- or Java-like references presents additional complications and, as far as we are aware, is still open. Our paper addresses precisely this problem.

The language we analyse, System ReF, includes a typed lambda calculus with products, references and polymorphism. For instance, we can examine the following type:

$$\forall \alpha. (\text{ref}\ \alpha \times \text{ref}\ \text{Int}) \rightarrow \alpha$$

One may be tempted to think that any term inhabiting this type is bound to return, given input $$(x, y)$$, the value stored in $$x$$. Of course, this is not necessarily the case if, for example, $$\alpha$$ is instantiated with Int and $$x$$ and $$y$$ happen to represent the same location. The following term would take advantage of such a coincidence,

$$\Lambda \alpha. \lambda (x, y)^{\text{ref}\ \alpha \times \text{ref}\ \text{Int}}. y := 42; !x$$

and in that case return 42 regardless of what the initial value stored in $$x$$ was. Thus, in this example, the given coincidence leads to an accidental interference with the returned result. More interestingly, we can instrument our example in a way that it can discover such coincidences and effectively deduce that $$\alpha = \text{Int}$$. Let us write $$y++$$ below for $$y := y + 1$$.

$$\Lambda \alpha. \lambda (x, y)^{\text{ref}\ \alpha \times \text{ref}\ \text{Int}}. \text{let } x' = \text{ref } x, y' = \text{ref } y \text{ in }$$

$$y++; x := x';$$

$$\text{if } y' = y \text{ then } (y := 42; !x) \text{ else } !x$$

The term above increases the value of $$y$$ and then restores $$x$$ to its initial value $$x'$$. It then compares the value of $$y$$ with its initial one $$y'$$. If these are not the same, then $$x$$ and $$y$$ are different locations, so the value of $$x$$ is returned. If, however, the value of $$y$$ has not changed then the term has successfully discovered that $$x$$ and $$y$$ refer to the same location, whence 42 is returned.

The above example demonstrates that uniform polymorphic behaviour can be violated through references, as differently typed variables can be instantiated with a common reference. More than that, references can disclose type instantiation information which can then be taken advantage of by a polymorphic function. In our example above the result of this disclosure was a non-parametric return value of 42, but we can imagine scenarios where a term records the references $$x$$ and $$y$$ that allowed it to escape uniform behaviour, and uses them as a general-use “bridge” between values of type $$\alpha$$ and Int. In fact, such devices, called casting functions, shall play a central role in our semantics. More generally, our modelling approach is crafted around carefully keeping track of the type information that has been leaked from the program to its environment, and viceversa, and allowing moves to be played in accordance with that information assuming that the context (the Opponent) has the epistemic power to exploit all such leaked information.
Related work  Operational techniques have been designed to study languages with both polymorphism and references. Realizability models [24][25], later refined into Kripke logical relations [2][6], use a notion of “world as heap-invariant” to model references. Environmental bisimulations have also been designed to deal with equivalence of programs in such languages [23]. While complete, these approaches partially rely on context quantifications and in particular do not directly account for the interaction between polymorphism and references, and the kind of type disclosure that the latter brings in.

Our approach follows the line of research on trace semantics for higher-order languages [13][15][17][8], which in turn can be seen as an operational reformulation of game semantics [23][11], on one hand; and of open bisimulation techniques [20][13][21], on the other. In this area, Jeffrey and Rathke proposed a fully abstract trace semantics for a polymorphic variant of the pi-calculus [16], which refined a previous sound model of Pierce and Sangiorgi [25]. That work is related to ours in spirit, and it already raises the intricacies involved in combining polymorphism with name equality testing.

Our approach follows the line of research on trace semantics for higher-order languages [13][15][17][8], which in turn can be seen as an operational reformulation of game semantics [23][11], on one hand; and of open bisimulation techniques [20][13][21], on the other. In this area, Jeffrey and Rathke proposed a fully abstract trace semantics for a polymorphic variant of the pi-calculus [16], which refined a previous sound model of Pierce and Sangiorgi [25]. That work is related to ours in spirit, and it already raises the intricacies involved in combining polymorphism with name equality testing.

We introduce System ReF, a polymorphic call-by-value λ-calculus with higher-order references. The typing rules for System ReF include standard rules for functions and projections, rules for integers, and rules for polymorphism and references given in Figure 1. Typing judgments are of the form \( \frac{\text{type}}{\Delta; \Sigma, \Gamma \vdash M : \theta} \), where \( \Sigma \) is a location context, i.e., a finite partial function from locations to \( \text{closed} \) types; \( \Gamma \) a variable context; and \( \Delta \) a set of type variables containing all free type variables of \( \Gamma \).

A finitely partial map \( S : \text{Loc} \rightarrow \text{Val} \) from locations to values. We define the following notion for stores, which we shall also be using for general partial maps:

- The empty store is written \( s \). Adding a new element \( (l, v) \) to a store \( S \) is written \( S \cdot [ l \mapsto v] \), and is defined only if \( l \notin \text{dom}(S) \).
- We also define \( S[l \mapsto v] \), for \( l \in \text{dom}(S) \), as the partial function \( S' \) which satisfies \( S' \theta \Sigma = S \theta \Sigma \) when \( l \notin \theta \), and \( S'(l) = v \).
- The restriction of a store \( S \) to a set of locations \( L \) is written \( S\upharpoonright L \).

We write \( \Sigma : \Delta \) just if \( \forall z \in \Sigma : ( l \in \Delta) \Rightarrow (l, z) \in S \cdot \theta \).

Given a set \( L \) of locations and a store \( S \), we define the image of \( L \) by \( S \), written \( S \upharpoonright L \), as \( S \upharpoonright L = \cup_{l \in L} S(l) \) with \( \Sigma \upharpoonright L = S \theta \Sigma \upharpoonright L \) and \( \{ l \in \text{Loc} \mid l \text{ contained in } S(l) \} \) and \( S(0) \upharpoonright L = L \), which is called closed just if \( \text{dom}(S) = S \theta \text{dom}(S) \).

Definition 1. The operational semantics of System ReF involves pairs \( (\Delta, \Sigma) \) consisting of a closed term \( \Delta; \Sigma, \Gamma \vdash M : \theta \) and a closed store \( \Sigma : \Delta \). Its small-step rules are given in Figure 2. We write \( (\Delta, \Sigma) \Downarrow (\theta, \Sigma') \) if \( S \in \Sigma \) and \( \Sigma' = \Sigma \upharpoonright \theta \).

Remark 2. We have equipped our language with a construct performing reference equality tests. This is in accordance with, and has the same operational semantics as, reference equality tests in ML, although extended to arbitrary reference types. Depending on type and type inhabitation, such tests can be encoded in ML via appropriately crafted sequences of writes and reads in examined references.

We finally introduce the notion of term equivalence we examine.

Definition 3. Let \( \Sigma \) be closed. Two terms \( \Delta; \Sigma, \Gamma \vdash M_1, M_2 : \theta \) are contextually equivalent, written \( \Delta; \Sigma, \Gamma \vdash M_1 \equiv M_2 : \theta \), if for all contexts \( C \), all \( \Sigma', \Sigma \upharpoonright \Sigma' \uplus \Sigma \) and all closed \( S : \Sigma' \) such that \( \Sigma' \vdash C[M_1] : \text{Unit} \), we have \( (C[M_1], S) \Downarrow (C[M_2], S) \).

2. System ReF

We introduce System ReF, a polymorphic call-by-value λ-calculus with higher-order references. The types of System ReF are:

\[ \theta, \theta' ::= \alpha \mid \text{Unit} \mid \text{Int} \mid \text{ref } \theta \mid \theta \times \theta' \mid \theta \rightarrow \theta' \mid \forall \alpha. \theta \mid \exists \alpha. \theta \]

where \( \alpha \in \text{TVar} \), and \( \text{TVar} \) a countably infinite set of type variables. As usual, a type is closed if all its type variables are bound.

We shall call arrow and universal types \( \text{function types} \). The syntax of values \( v \), terms \( M \) and evaluation contexts \( E \) is given in Figure 1. We assume a countably infinite set \( \text{Loc of locations} \) and some standard collection of binary integer operators, which we generally denote by \( \oplus \). We use the following macros: let \( x = N \in \text{M} \) stand for \((\lambda x.M)\ N\); and \( N; M \) means \((\lambda x.M)\ N\) with \( x \) fresh in \( M \).

The typing rules for System ReF include standard rules for functions and projections, rules for integers, and rules for polymorphism and references given in Figure 1. Typing judgments are of the form \( \Delta; \Sigma; \Gamma \vdash M : \theta \), where \( \Sigma \) is a location context, i.e., a finite partial function from locations to \( \text{closed} \) types; \( \Gamma \) a variable context; and \( \Delta \) a set of type variables containing all free type variables of \( \Gamma \). Given a closed evaluation context \( E \), we write \( \Delta; \Sigma; \Gamma \vdash E : \theta \rightarrow \theta' \) when \( \Delta; \Sigma; \Gamma \vdash x : \theta \rightarrow E[x] : \theta' \). Compared to the ML type-system, we work with Church-style polymorphism, where type abstractions and applications are explicit. This explains why we do not need the so-called \( \text{value restriction} \) to accommodate references.

We next proceed with the operational semantics. Closed terms are reduced using stores containing their locations. More precisely, a \( \text{store} \) is a finite partial map \( S : \text{Loc} \rightarrow \text{Val} \) from locations to

\[ v, u \coloneqq (\cdot) \mid n \mid x \mid l \mid \lambda x.\theta.M \mid \lambda \alpha. M \mid \text{pack}(\theta, v) \mid \langle v, u \rangle \]

\[ M, N \coloneqq v \mid MN \mid M \theta \mid M \uplus N \mid \text{if } M_1, M_2, M_3 \mid (M, N) \]

\[ \pi_1(M) \mid \pi_2(M) \mid \text{ref } M \mid \text{if } M \mid M \equiv N \]

\[ M = N \mid \text{pack}(\theta, M) \mid \text{unpack } M \text{ as } (\alpha, x) \text{ in } N \]

\[ E \coloneqq \cdot \mid EM \mid E \theta \mid E.v \mid E \circ p \mid M \mid v \circ p \mid E \text{ if } E \mid M \]

\[ \text{ref } E \mid E \theta \mid (E, M) \mid (v, E) \]

\[ \pi_1(E) \mid \pi_2(E) \]

\[ \text{pack}(\theta, E) \mid \text{unpack } E \text{ as } (\alpha, x) \text{ in } M \]

Figure 1. System ReF \((n \in \mathbb{Z}, l \in \text{Loc} \text{ and } op \in \{\oplus, \equiv, \downarrow\})\).

3. The Semantic Model

Our trace model is constructed within nominal sets, that is, a universe embedded with atomic objects for representing locations, type variables, functions and polymorphic values. We introduce the semantic universe next and then proceed to the operational rules defining the semantics.

3.1 Semantic Universe

We define the set of \textit{names} to be:

\[ \Lambda = \text{Loc} \uplus \text{TVar} \uplus \biguplus_{\theta \in \text{TFT}} \text{Fun}_{\theta} \uplus \bigcup_{\alpha \in \text{TVar}} \text{Pol}_{\alpha} \]

where \( \theta \) ranges over function types and each of the components in this countable union is itself a countable set. We let \( \text{Fun} = \bigcup_{\theta \in \text{TFT}} \text{Fun}_{\theta} \) and \( \text{Pol} = \bigcup_{\alpha \in \text{TVar}} \text{Pol}_{\alpha} \). We range over elements of \text{Loc} by \( l \) and \text{variants}; over \text{TVar} by \( \alpha \), \text{etc}; \text{over Fun} by \( f, g, \text{etc} \); and over \text{Pol} by \( p, \text{etc} \).

Semantic objects feature elements of \( \Lambda \) as atomic entities which, moreover, can be acted upon by finite permutations of \( \Lambda \). A \textit{nominal set} \( \{X, \ast\} \) is a pair \((X, \ast)\) of a set \( X \) along with an action \( \ast \) from the set of finite component-preserving computations of \( \Lambda \) on the set \( X \). Given some \( x \in X \), the set of names featuring in \( x \) form

\[ \text{A finite permutation } \pi : \Lambda \rightarrow \Lambda \text{ is component-preserving simply if it preserves the partition of } \Lambda, \text{e.g. if } d \in \text{Loc} \text{ then } \pi(d) \in \text{Loc}. \]
its support, written \( \nu(x) \), which we stipulate to be finite. Formally, \( \nu(x) \) is the smallest subset of \( \mathbb{A} \) such that all elements which elementwise fix \( \nu(x) \) also fix \( x \). We shall sometimes write \( \nu_{\cdot}(x) \), for \( C \in \{ \mathbb{L}, \mathbb{T}, \mathbb{F}, \mathbb{P} \} \) in order to select a specific kind of names from the support of \( x \). For instance, \( \nu(x) = \nu(x) \cap \text{Loc} \). Using the same notation, we also write \( \nu_\theta(x) \) for the free type variables of \( \theta \). We usually write \( (X, +) \) simply as \( X \), for economy.

We next introduce our basic semantic objects, which constitute the semantic representations of syntactic values.

**Definition 4.** We define abstract values as:

\[
\text{AValues} \ni \nu, u := (\nu \mathbin| \mathbin| \nu \cdot \mathbin| \nu \cdot \mathbin| (u, v))
\]

where \( i \in \mathbb{Z}, l \in \text{Loc}, f \in \text{Fun}, p \in \text{Pol} \) and \( \alpha \in \text{TVar} \). Note we still range over abstract values by \( u, v \) (and hope no confusion arises). We similarly set abstract stores to be finite partial maps \( \text{Loc} \rightarrow \text{AValues} \).

Thus, ground values (integers, \( , \) and locations) are represented by their concrete values, and for all other types but products we employ name abstractions. This abstraction is in order either because of polymorphism in the values, or simply because function code can only be examined by querying the given function. Functions are represented by functional names, and polymorphic values by polymorphic names.

The semantics of a type \( \theta \), written \( [\theta] \), consists of pairs \( (\nu, \phi) \) of an abstract value \( \nu \) along with a function \( \phi : \nu_1(\nu) \rightarrow \text{P(Types)} \), and is given as:

\[
\begin{align*}
\text{Unit} & = \{(()\} \\
\text{Int} & = \{(n, \cdot) \mid n \in \mathbb{Z}\} \\
\text{ref} \theta & = \{(l, (\cdot, \cdot)) \mid l \in \text{Loc}\} \\
\alpha & = \{(p, \cdot) \mid p \in \text{Pol}_\alpha\} \\
\theta \rightarrow \theta' & = \{(f, \cdot) \mid f \in \text{Fun}_\alpha\} \\
\text{Var} \cdot \theta & = \{(f, \cdot) \mid f \in \text{Fun}_\alpha \} \\
\text{Ω} \cdot \theta & = \{(\phi, \phi') \mid \phi, \phi' \in [\theta_{\alpha'}] \} \\
\text{ω}_1 \times \text{ω}_2 & = \{(\nu_1, \nu_2), \phi_1, \phi_2 \mid (\nu_1, \phi_1) \in [\theta], (\nu_2, \phi_2) \in [\theta']\}
\end{align*}
\]

The role of \( \phi \) is to assign types to all the locations of an abstract value. As discussed in the Introduction, though, the same location can appear with several types in the execution of a given term phrase. Hence, \( \phi \) assigns sets of types to each location instead of a unique type. More generally, a **typing function** is a finite map \( \phi : \text{Loc} \rightarrow \text{P(Types)} \). The type translation is extended to typing environments by mapping each \( \Delta = \{\alpha_1, \ldots, \alpha_k\}, \Sigma = \{l_1 : \theta_1, \ldots, l_n : \theta_n\} \) and \( \Gamma = \{x_1 : \theta_1', \ldots, x_k : \theta_k'\} \) to:

\[
[\Delta, \Sigma, \Gamma] = \{\{(\tilde{a}, \tilde{b}), \cup_{i=1}^n [l_i \mapsto \theta_i] \cup \cup_{j=1}^k \phi_j | (v_j, \phi_j) \in [\theta'_j]\}\}
\]

**Extending the syntax for Fun \cup Pol** While functional and polymorphic names are not part of the syntax of System ReF, their involvement in its semantics makes it useful to introduce them as syntax as well. We hence extend the set of values of System ReF to include \( \text{Fun} \cup \text{Pol} \), dealing with them as typed constants.

### 3.2 Interaction Reduction

Traces will consist of sequences of **moves** enriched with abstract stores and value disclosures. Moves represent the interaction between the modelled program and its enclosing context and consist of function calls and returns. Each move comes with a polarity: \( P \) for Player (i.e. the program produces the move), and \( O \) for Opponent (the context/environment). There are four kinds of moves:

**PQ. Player Questions** are moves of the form \( \mathcal{J}(u) \), representing a call to a functional name \( f \in \text{Fun} \) with argument \( u \in \text{AValues} \).

**OQ. Opponent Questions** are of the form \( \mathcal{J}(u) \), with \( f \in \text{Fun} \) and \( u \in \text{AValues} \); moreover, there are **initial opponent questions** of the form \( \mathcal{J}(u) \) \( (u \in \text{AValues}) \).

**PA. Player Answers** are moves of the form \( \mathcal{J}(u) \), with \( u \in \text{AValues} \).

**OA. Opponent Answers** which are of the form \( \mathcal{J}(u) \) \( (u \in \text{AValues}) \).

On the other hand, value disclosures are partial functions \( \rho \) representing the values of polymorphic names revealed in a move. Their role will be explained in the next section.

**Definition 5.** A full move is a triple \((m, \rho, \delta)\) of a move \( m \), a closed abstract store \( S \) and a finite map \( \rho : \text{Pol} \rightarrow \text{AValues} \). A sequence of full moves is called a **trace**.

The trace semantics is produced via a reduction relation for open terms which only reveals the steps in the computation where there is interaction: a call or return between the term and its context. More precisely, this relation is a bipartite labelled transition system between Player and Opponent configurations, where labels are full moves, and whose main components are evaluation stacks \( \mathcal{E} \), defined as either:

- passive, which are related to Opponent configurations and are of the form \( \mathcal{E}^\rho, \theta_n : \theta'_n : \cdots : (\mathcal{E}^{\rho_1, \theta_1} : \theta_1) \), where each \( \mathcal{E}^{c} \) is an evaluation context of type \( \theta_c \rightarrow \theta'_c \);
- or active, which are related to Player configurations and are of the form \( (M, \theta) : \mathcal{E}' \), i.e. they consist of a term \( M \) of type \( \theta \) and a passive stack \( \mathcal{E}' \).

The empty stack is written \( \emptyset \).

**Definition 6.** A **configuration** is a tuple \((\mathcal{E}, \gamma, \phi, \delta, \lambda)\) with:

- an evaluation stack \( \mathcal{E} \), a typing function \( \phi \) for locations, and a closed store \( S \);
- an environment \( \gamma \) mapping names to values;
- an ownership function \( \lambda \in (\lambda \times (\mathbb{O}, \mathbb{P})) \) mapping played names and mapping them to the party who has introduced them; and which satisfies the following conditions:
  - the relation \( ((\alpha, X) \mid \lambda = \lambda_1 : (a, X) \cdot \lambda_2) \) is a partial function and \( \lambda \) has no repetition of names
  - \( \text{dom}(\gamma) = \{a \in \text{Pol} \cup \text{Fun} \cup \text{TVar} \mid \text{Proj}(\lambda) = \mathbb{P}\} \)
  - \( \text{dom}(\phi) = \{l \in \text{Loc} \cap \text{dom}(\lambda) \} \subseteq \text{dom}(\mathcal{S}) \)
  - for all \( a \in \nu(\mathcal{E}, \text{cod}(\mathcal{S}), \text{cod}(\gamma)) \) \( \text{Loc}, \lambda(a) = O \) where, because of the first condition above, we write \( \lambda(a) = X \) if \( \lambda = \lambda_1 \cdot (a, X) \cdot \lambda_2 \) for some \( \lambda_1, \lambda_2 \).
In addition, we include special configurations of the form \((\Delta; \Sigma; \Gamma \vdash M : \theta)\), one for each typed term \(\Delta; \Sigma; \Gamma \vdash M : \theta\).

Thus, a configuration registers syntactic and semantic information on the execution of a term necessary to produce its traces. \(\mathcal{E}\) and \(S\) are syntactic objects directly connected to the operational semantics. The other components either are of semantic nature (\(\phi, \lambda\)) or bridge the semantics and the syntax (\(\gamma\)). In \(\gamma\) we record the actual values that correspond to the functional and polymorphic names and type variables that the term (i.e. \(P\)) has produced. On the other hand, \(\lambda\) is a name-polarity function which also keeps track of the order in which names were introduced. The last condition on \(\lambda\) in the above definition is especially important: it stipulates that, except for location names, all the free names that appear in the term, either directly or indirectly via \(\gamma\) or \(S\), must belong to \(O\). In other words, \(P\) cannot see the abstract values that he has provided to \(O\) during the interaction.

When the evaluation of a term \(E[M]\) reaches, for example, some \(E[f \nu]\) where \(f\) is a function name provided by the context, a move asking the context to evaluate \(f(\nu)\) will be produced. However, since \(\nu\) is a syntactic value and in moves we only allow semantic entities, we need a way to pass from syntactic values to abstract ones. This is achieved as follows. To each value \(u\) of type \(\theta\) we associate the set \(AVal(u, \theta)\) of triples \((\nu, \gamma, \phi)\), where each of them represents: • a corresponding abstract value \(v\); • an environment \(\gamma\) instructing the related mapping of names to values; • a typing function \(\phi\) recording the types used for each location in the translation. It is defined as:

\[
AVal(u, i) = \{(u, \epsilon, \phi)\} \quad \text{for } i = \text{Unit or Int and } u \in \mathbb{I}
\]

\[
AVal(l, \text{ref } \theta) = \{(l, \epsilon, \{(l, \text{ref } \theta)\}) \mid l \in \text{Loc}\}
\]

\[
AVal(u, \alpha) = \{(p, p \rightarrow u, \phi) \mid p \in \text{Pol}\} \cup \{(u, \epsilon, \phi) \mid u \in \text{Pol}\}
\]

\[
AVal(u, \theta) = \{(f, f \rightarrow u, \phi) \mid f \in \text{Fun}_{\theta}\} \quad \text{for } \theta \text{ functional}
\]

\[
AVal((u_1, u_2), \theta_1 \times \theta_2) = \{(u_1, u_2), \gamma_1 \cdot \gamma_2, \phi_1 \cup \phi_2 \mid (u_1, \gamma_1, \phi_1) \in AVal(u_1, \theta_1)\}
\]

\[
AVal((\theta', u), \exists \alpha.\theta) = \{(\{(u', v), \gamma \cdot [\alpha' \mapsto \theta']_\phi\}, (u, \gamma, \phi) \in AVal(u, \theta(\alpha'/\alpha))\}
\]

For uniformity, it makes sense to view types as values of special "universe" type \(\mathcal{U}\) and set \(AVal(\theta, \mathcal{U}) = \{(\alpha, \alpha \mapsto \theta, \phi) \mid \alpha \in \text{TVar}\}\). By abuse of notation, we shall use \(u\) and \(v\) to range over values, abstract values and types when utilising the notation presented next. Given a functional type \(\theta\) and some \(u\), we let the argument and return type of \(\theta\) be:

\[
\begin{align*}
\text{arg}(\theta' \rightarrow \theta) &= \theta' \\
\text{arg}(\forall \alpha.\theta) &= \mathcal{U} \\
\text{return}_{\theta} = \theta' \rightarrow \theta &= \theta \\
\text{return}_{\forall \alpha.\theta} &= \theta[\alpha/\alpha]
\end{align*}
\]

with the last expression above being well-defined only if \(u\) is a type.

Finally, in a similar fashion that \(AVal\) allows us to move from concrete values to abstract ones, the operator \(AStore\) takes us from stores to abstractions thereof. That is, for each store \(S\) and typing function \(\phi\), the set \(AStore(S, \phi)\) consists of triples of the form \((S', \gamma', \phi')\) where: • \(S'\) is an abstraction of \(S\) according to the type information in \(\phi\); • \(\gamma'\) is the mapping of the fresh abstract names of \(S'\) to their concrete values; • \(\phi'\) is the type information for any locations in the codomain of \(S'\). The formal definition in the case where \(\gamma\) is single-valued is given as follows. We postpone the definition for general \(\phi\) to Section\[\text{\ref{section:interaction_reduction}}\).

\[
AStore(S, \phi) = \bigcup_{\ell \in \text{dom}(\phi)} \{((l \mapsto v, \gamma', \phi'), (v, \gamma', \phi') \in AVal(S(l), \phi(l))\}
\]

Here \(\phi\) is the pointwise concatenation of sets of triples \((S, \gamma, \phi)\), defined as \(X_1 \oplus X_2 = \{(S_1, \gamma_1, \phi_1) \cup (S_2, \gamma_2, \phi_2) \mid (S_i, \gamma_i, \phi_i) \in X_i, i \in \{1, 2\}\}\), and \(\bigcup_{\ell \in \text{dom}(\phi)} X_\ell = \{(\epsilon, \epsilon, \phi)\}\). A similar notion is used for producing abstract stores where only typing information (and no concrete store) is defined as follows.

\[
S[\phi] = \bigcup_{\ell \in \text{dom}(\phi)} \{((l \mapsto v, \phi'), (v, \phi') \in \phi(l))\}
\]

This is used for determining what stores \(O\) can play.

We now give the definition of our trace semantics. Note that, for syntactic objects \(Z\) and (e.g. type) environments \(\delta\), we write \(Z[\delta]\) for the result of recursively applying \(\delta\) in \(Z\) as a substitution.

**Definition 7** (Trace Semantics). We call Interaction Reduction the system generated by the rules in Figure\[\text{\ref{section:interaction_reduction}}\]. Given a configuration \(C\), we let \(\text{Tr}(C)\) be the set of all traces produced from \(C\). Terms are translated by setting

\[
[\Delta; \Sigma; \Gamma \vdash M : \theta] = \text{comp}(\text{Tr}(\Delta; \Sigma; \Gamma \vdash M : \theta))
\]

for each typed term \(\Delta; \Sigma; \Gamma \vdash M : \theta\), where \(\text{comp}\) selects the complete traces, that is those traces where the number of answers is greater or equal to the number of questions.

In the rest of this section we explain the reduction rules and their conditions, apart from conditions \(P^*\) and \(O^*\) which concern type disclosure and are relegated to the next section. For the same reason, we also assume that typing functions \(\phi\) are always single-valued and disregard any indexing with \(\kappa\) used in the rules (\(\kappa\)'s are cast functions).

**Internal** (INT) This rule dictates that the interaction reduction includes the operational semantics of System Ref\(\#\) as long as internal computation steps are concerned, i.e. ones that do not involve external functions.

**P-Question** (PQ) This rule describes the move occurring when an external function call is reached. Thus, in order for \(P\) to provide the value (say) \(u\) and store \(S\), he first needs to abstract it to \(v\) by hiding away all private code under fresh names. These will be the names put in \(X\), along with any new location names revealed in the store \(S'\) to be played. Since this is a \(P\)-move then, all names in \(X\) are owned by \(P\) (P1). In turn, \(S'\) is the restriction of \(S\) to public locations, again elevated to its abstraction. These abstractions result in new \(\gamma = \gamma \cdot [\gamma u \cdot \gamma S] \quad \text{and} \quad \phi' = \phi \cup \phi_2 \cup \phi_3 (P1)\). Note that the \(\lambda\) component of a configuration enlists the public names of a trace, i.e. those explicitly played in moves. Hence, P3 stipulates that the locations included in the store \(S'\) are precisely the ones reachable in \(S\) from the names in \(\lambda\) and any names in \(v\) (put otherwise, name privacy is imposed). Finally, P2 dictates that any functional or type variable names played in the move must be fresh (as they represent abstractions of concrete values). Similarly, every polymorphic name played of type \(\alpha\), with \(\alpha\) of own polarity, must be fresh. If, on the other hand, \(\alpha\) belongs to \(O\), then \(P\) can only play old polymorphic names of that type (P4).

**P-Answer** (PA) In this case, a final value is reached and returns, with similar conditions applied.

**O-Question** (OQ) When it is the context’s turn to play, one option is for \(O\) to call one of the functions provided by \(P\). The rule looks very similar to the P-Question, yet it differs in one important point: while \(O\) plays \(v\) and \(S'\), what is fed instead to the configuration is \(v\) where all its \(P\) polymorphic and functional names have been replaced by their actual values (i.e. \(v(\gamma)\)) and the same goes for the abstract store \(S'\). This is enforced by the use of \(\bar{\gamma}\) instead of \(\gamma\) and is due to the fact that \(P\) knows the actual values of these names, and therefore they should not remain abstract to him. Another difference is the freedom to build \(S'\), which nonetheless stipulates that \(O\) cannot guess any locations from \(S\) unless the latter were already public. Finally, observe in O1 the single-played restriction on fresh polymorphic, type or function names: as each

\[\text{\footnote{\text{we also substitute via } \rho, \text{ but this we discuss in the next section.}}}\]
such introduced name has the purpose of abstracting some concrete value or type played, every such name should be distinct (and fresh)\(^3\). This condition is implicitly imposed in P1 as well, via the domain disjointness requirements in the definition of \(\gamma\).

O-Answer (OA) On the other hand, a context can also return with a value, with similar conditions applied.

Initial move (Init) Initial moves are special O-Questions. In order for the interaction to commence, \(O\) needs to provide the context, that is, the values corresponding to the typing environment \(\Delta, \Sigma, \Gamma\).

Let us look at a couple of examples.

**Example 8.** Consider the term \(v \equiv \Lambda x.\lambda x.\alpha \times \alpha. \pi_1(x)\) of type \(\Theta = \forall \alpha. \alpha \times \alpha \to \alpha\). A characteristic trace of \(v\) is \(\theta_1 = \lambda x. \forall \alpha. \alpha \times \alpha \to \alpha\).

\[\begin{align*}
(\forall \alpha. \forall \alpha) & \Rightarrow (\forall \alpha. \alpha \times \alpha \to \alpha) \\
(\forall \alpha. \alpha \times \alpha \to \alpha) & \Rightarrow (\forall \alpha. \forall \alpha) \\
\end{align*}\]

Each \(\forall \alpha. \forall \alpha\) is of the form \(\forall \alpha. \alpha \times \alpha \to \alpha\). The next \(O\) decides to also interrogate \(f\), say on input \(4.2\). This translates to the move \(f(p_1, p_2)\), where now \(p_1 \mapsto 4\) and \(p_2 \mapsto 2\) for \(O\). The trace concludes with \(P\) replying \((\bar{p}_1)\), which is the return value of the first projection on \((p_1, p_2)\).

**Example 9.** Let us take \(v \equiv \lambda x. \forall \alpha. \alpha \to \alpha\). Int 3 and Int 5 of type \(\theta = \forall \alpha. \alpha \to \alpha \to \alpha\) to \(\Lambda x. \forall \alpha. \alpha \to \alpha\). A characteristic trace of \(v\) is \(\gamma_1 = \gamma_2 = \forall \alpha. \forall \alpha \times \alpha \to \alpha\).

\[\begin{align*}
(\forall \alpha. \forall \alpha) & \Rightarrow (\forall \alpha. \forall \alpha) \\
(\forall \alpha. \forall \alpha) & \Rightarrow (\forall \alpha. \forall \alpha) \\
\end{align*}\]

Each \(\forall \alpha. \forall \alpha\) is of the form \(\forall \alpha. \forall \alpha\) or \(\forall \alpha. \forall \alpha\). The next \(O\) decides to also interrogate \(f\), say on input \(4.2\). This translates to the move \(f(p_1, p_2)\), where now \(p_1 \mapsto 4\) and \(p_2 \mapsto 2\) for \(O\). The trace concludes with \(P\) replying \((\bar{p}_1)\), which is the return value of the first projection on \((p_1, p_2)\).

\[\begin{align*}
(\forall \alpha. \forall \alpha) & \Rightarrow (\forall \alpha. \forall \alpha) \\
\end{align*}\]

Each \(\forall \alpha. \forall \alpha\) is of the form \(\forall \alpha. \forall \alpha\) or \(\forall \alpha. \forall \alpha\). The next \(O\) decides to also interrogate \(f\), say on input \(4.2\). This translates to the move \(f(p_1, p_2)\), where now \(p_1 \mapsto 4\) and \(p_2 \mapsto 2\) for \(O\). The trace concludes with \(P\) replying \((\bar{p}_1)\), which is the return value of the first projection on \((p_1, p_2)\).

Notice that \(p_1, p_2\) are of different type, respectively \(\alpha_1\) and \(\alpha_2\). As an exercise, we invite the reader to verify that the term \(v' = \lambda x. \forall \alpha. \alpha \to \alpha\) at \(\forall \alpha. \alpha \to \alpha\) at \(\forall \alpha. \alpha \times \alpha \to \alpha\) and \(\forall \alpha. \alpha \to \alpha\) at \(\forall \alpha. \alpha \times \alpha \to \alpha\). At that point, the environment \(O\) may wish to interrogate \(g\), supplying a type variable \(\alpha\) which is an abstraction of any type instantiation the environment may have chosen. Such a question would be of the form \(g(\alpha')\). To the latter, \(P\) replies with a functional name \(f\), via the move \((\bar{f})\), of type \(\alpha' \to \alpha')\). Next, \(O\) decides to also interrogate \(f\), say on input \(4.2\). This translates to the move \(f(p_1, p_2)\), where now \(p_1 \mapsto 4\) and \(p_2 \mapsto 2\) for \(O\). The trace concludes with \(P\) replying \((\bar{p}_1)\), which is the return value of the first projection on \((p_1, p_2)\).
4. Type Disclosure, Casts and \textbf{-Conditions}

As already discussed in the Introduction, the existence of references can be used to the advantage of a program in order to break parametricity. This is done by discovering variables of different reference types which, upon execution, end up with the same concrete type. Consider types which, upon execution, end up with the same concrete metricity. This is done by discovering variables of different referential types and binding them to each location, employing the non-unicity of typing functions. Type disclosure is the result of the same location appearing in for all cast relations. We can start forming cast functions to move between types. We can now define the cast relation \( \text{Cast}(\phi) \) related to a typing function \( \phi \). We can show that, for any valid typing function \( \phi \), \( \text{Cast}(\phi) \) is a valid cast relation.

\begin{definition}
Given a typing function \( \phi \), its associated cast relation \( \text{Cast}(\phi) \) is the closure of \( \{(\theta, \theta') | \exists \phi \in \phi(I)\} \).
\end{definition}

Given a cast relation \( \kappa \) and a type \( \theta \), we let
\[
\min(\kappa(\theta)) = \{ \theta' \in \kappa(\theta) \mid \forall \theta'' \in \kappa(\theta), \theta'' \leq \theta' \implies \theta'' = \theta' \}
\]
be the set of minimal types of \( \kappa(\theta) \). Because the closure rules above are not reversible on ref types, this set is not in general a singleton (e.g. \( \min(X) = X \) for \( X = \text{ref} \{\text{Int} \times \text{Int} \} \)). This means that a type \( \theta \) can have several minimal types in its cast class, and each of them needs to be taken into account when computing abstract values to be played in a move. Hence, minimal types are central to the (full) definitions of AVal, AStore, etc.

4.2 The starred conditions

We next look at the use of environments \( \rho \) and the conditions \( \text{O}^\ast \) and \( \text{P}^\ast \) which govern type disclosure in the interaction reduction.

Each move \( (m, S, \rho) \) played in an interaction has the potential to reveal type information. Looking at the reduction rules, in particular, we see that such a move can enlarge the current typing function \( \phi \) to a (valid) superset \( \phi \cup \phi' \): this is due to the fact that locations \( l \) which up until now had types \( \phi(l) \) are put in positions which expect types \( \theta \in \phi(\ell) \) (e.g. in return position of some \( f \in \text{funs}^\ast \)). This leads to a corresponding increase in the cast capabilities to \( \kappa' = \text{Cast}(\phi \cup \phi') \). Cast capabilities, though, may reveal the values behind polymorphic names: for instance, if we are able to form a cast from \( \alpha \) to \( \text{Int} \), we can go back to an old \( p \in A_{\alpha} \), cast it as an integer and read its value. This decoding capability is the reason behind the presence of \( \rho \) in the move: \( \rho \) contains all those polymorphic names \( p \) whose value is being revealed (indirectly, via casts) through the current move, along with the revealed values.

The way polymorphic values are revealed is governed by conditions \( \text{P}^\ast \) and \( \text{O}^\ast \). The former stipulates that, given the old cast relation \( \kappa \), the new castings \( \kappa' \) is the one we obtain via the updated typing function \( \phi \cup \phi' \). Moreover, as explained above, each concrete value \( \gamma(p) \) of a polymorphic name \( p \) needs to be partially revealed. The degree to which the codomain of \( \gamma(p) \) will be revealed is determined by the function \( \text{AEnv} \). That is, \( \text{AEnv}(\gamma(p), \phi, \phi') \) for these newly revealed values, that is moreover unique up to permutation of fresh names. The

---

\footnote{Assuming \( \theta_1 \) and \( \theta_2 \) are inhabited types.}
first component (ρ) is the map from polymorphic names to their revealed values. The other two components record the location types (φα) and value abstraction (γρ) occurring via this disclosure. In the case of Oρ, a similar disclosure occurs, only that this time there is no γ to guide the revealed values, R supplies the disclosure in a non-deterministic fashion.

The definition of AEnv and its O-counterpart are given below.

$$E [\theta \leftarrow \theta', \varphi], \{ \varphi \theta \} = \bigcup_{\theta \in \Int} \varphi \theta$$

$$\text{AEnv}(\gamma, \kappa) = \bigcup_{\theta \in \Int} \{ (\varphi \theta) \}$$

$$\text{AVal}(\gamma, \theta) = \bigcup_{\theta \in \Int} \varphi \theta$$

with dom(γ) ≤ Pol and Xp = minκ(α) minκ(α) for p ∈ Polα. Thus, for each p ∈ Polα in the domain of γ such that, going from κ to κ′, there is a new type disclosure on the type of p (i.e. such that Xp ̸= φp), to compute the disclosure happening on γ(p) we look at all the newly disclosed types in Xp and for each of them select an abstract environment from AVal(γ(p), θ).

If we pick the environments so that all agree in their value component v, we can reveal that maps to v. Note that Xp determines how much of γ(p) is revealed: for instance, Xp = {α′} with α′ another type variable, then v will simply be another polymorphic name p′. On the other hand, E[θ \leftarrow \theta′] is a more liberal in choosing the common revealed value v, as it scans through each [θ] instead of AVal(γ(p), θ). In a similar vein, we get:

$$\text{AVal}(u, \theta) = \{ (v, \gamma, \phi) | \phi \in \bigcup_{\theta \in \Int} \varphi \theta \}$$

$$\text{AStore}(S, \phi) = \bigcup_{\theta \in \Int} \{ (\varphi \theta) \}$$

$$\text{AVal}(S, \phi) = \bigcup_{\theta \in \Int} \varphi \theta$$

5. Soundness

We show that our model is sound, i.e. equality of term denotations implies contextual equivalence. In fact, we prove a stronger result (Theorem 24), whereby equality is replaced by a larger equivalence relation which rules out some over-distinguishing O behaviours.

5.1 Valid configurations

To reason on the interaction reduction, we prove it preserves some invariants which we collect in the notion of valid configuration.

An obvious invariant we want to preserve is that elements of the evaluation stack are well-typed. However, due to the fact that locations do not always have a unique type, and the ensuing casting capabilities that arise, we cannot use the standard typing system defined in Section 3. We thus need to generalise it by allowing context boxes to be multi-valued, i.e. use valid typing functions φ (instead of Σ), together with the new typing rule:

$$\Delta; \phi; \Gamma \vdash_{e} M : \theta \rightarrow_{\theta} \phi \in \text{Cast}(\phi)$$

We write S ⊢ φ if ∀v ∈ dom(S), 30 ∈ φ(l), 37 ∈ φ(\theta0). The extended type system still satisfies a safety property, on which rely in order to show our model sound.

5.1 Valid configurations

To reason on the interaction reduction, we prove it preserves some invariants which we collect in the notion of valid configuration.

An obvious invariant we want to preserve is that elements of the evaluation stack are well-typed. However, due to the fact that locations do not always have a unique type, and the ensuing casting capabilities that arise, we cannot use the standard typing system defined in Section 3. We thus need to generalise it by allowing context boxes to be multi-valued, i.e. use valid typing functions φ (instead of Σ), together with the new typing rule:

$$\Delta; \phi; \Gamma \vdash_{e} M : \theta \rightarrow_{\theta} \phi \in \text{Cast}(\phi)$$

We write S ⊢ φ if ∀v ∈ dom(S), 30 ∈ φ(l), 37 ∈ φ(\theta0). The extended type system still satisfies a safety property, on which rely in order to show our model sound.

**Lemma 13.** Given Δ; φ; e : M : \theta and S ⊢ φ such that for all p ∈ v(M; S) \cap Polα, min(Cast(\phi)(\alpha)) ≥ 1 either (M, S) diverges or there exists (M′, S′) irreducible such that:

- (M, S) →∗ (M′, S′).
- M′ is either equal to a value v or to a callback E[v].
- there exists v′ disjoint from φ such that Δ; φ ∪ φ′; e : M′ : \theta and S′ ⊢ φ ∪ φ′.

Using this extended system, we can evaluate stacks of configurations. A passive evaluation stack \(E_{\alpha}, \theta_{\alpha} \rightarrow \theta'_{\alpha} : \cdots \rightarrow (E_{l_{1}}, \theta_{l_{1}} \rightarrow \theta'_{l_{1}})\) is said to be well-typed with respect to a type environment \(\delta : T \vdash_{e} \text{types}\) if, for all \(1 \leq i \leq n, \delta_{i} \vdash_{e} \theta_{i} : \theta'_{i}\). An active evaluation stack \((M, \theta, \Phi) : E\) is well-typed for \(\phi, \delta\) if \(\Delta: \phi \cup \Phi; e : M : \theta \rightarrow_{\theta} \delta\). We can now specify which configurations are valid.

**Definition.** We call \(E, \gamma, \phi, \lambda, \alpha)\) a valid configuration if:

- \(\text{dom}(\gamma) = \{ \alpha \in \text{Pol} \cup \text{Un} \cup \text{TVar} \mid \lambda(\alpha) = P \},\)
- \(\text{dom}(\phi) = \text{dom}(\lambda) \cap \text{Loc} \subseteq \text{dom}(\alpha)\),
- for all \(a \in v(E, \text{cos}(\lambda), \text{cond}(\gamma))\) \text{Loc}, \(\lambda(\alpha) = O,\)
- there exists \(\phi'\) disjoint from \(\phi\) s.t. \(S' \vdash \phi \cup \phi'\),
- \(E\) is well-typed for \(\phi \cup \phi', \text{TVar}\)
- for all \(p \in v(E, \text{cos}(\lambda), \text{cond}(\gamma)) \cup \text{Pol}_{\text{a}}, \min(Cast(\phi)(\alpha)) = (\alpha)\).

We write \(C \vdash M \in S\) when \(C \vdash M \in S\) for some configuration \(C\). Validity of configurations is preserved as follows.

**Definition.** If \(C \vdash M \in S\) and \(C\) is valid, then \(C\) is valid.
5.2 Composite reduction

The main ingredient in the soundness argument is a refinement of the LTS introduced previously which will eventually allow us to compose term denotations, in a way akin to composition in game semantics: each term in the composition becomes the Opponent for the other term. More concretely, in the composite LTS the behaviour of Opponent is fully specified by expanding the configurations with an extra extraction stack, environment and store.

The new LTS is called composite interaction reduction. It works on composite configurations $\langle E, E_0, \gamma, \phi_0, S, P, S_0 \rangle$, where:

- $E, E_0$ are evaluation stacks (one passive and one active);
- $\gamma, \gamma_0$ are environments; and $S_0, S_0$ are stores;
- $\phi$ is a common typing function for locations.

The rules of the composite reduction are in effect the P-rules of the ordinary interaction reduction, plus dual forms thereof freeing out the O-rules.

A trace $t$ is said to be generated by a composite configuration $C$ if it can be written as a sequence $(m_1, S_1, \rho_1) \cdots (m_n, S_n, \rho_n)$ of full moves such that $C = (m_1, S_1, \rho_1) \rightarrow C_1 = (m_2, S_2, \rho_2) \cdots \rightarrow C_n$, in which case we write $C \Rightarrow C_n$. We say that a composite configuration $C$ terminates with the trace $t$, written $\downarrow t$, if there exists a store $S$ such that $C \Downarrow (t, (S_0, \rho))$.

We now define how to merge configurations $C_1, C_0$ into a composite one. For each $X \in \{O, P\}$, we write $X^*$ for its dual $\{X, X\} = \{O, P\}$, and extend this to $\lambda^{X^*} = (\_^X)$.

**Definition 16.** Given a pair of environments $(\gamma, \gamma_0)$ from $A \cup \Loc$ to values, we say these are compatible when:

- $\dom(\gamma) \cap \dom(\gamma_0) = \emptyset$.
- For all $a \in \dom(\gamma_X)$, $X \in \{P, O\}$, $\nu(\gamma_X(a)) \cup \dom(\gamma_X)$.
- Setting $\gamma'[X] = \gamma \cdot \gamma_0 \cdot \gamma'[X_0]$, and $\gamma'[X] = \{ (a, v') \in \gamma'[X'] | (a, v) \in \gamma'. \}$ ($X > 0$), there is an integer $n$ such that $\nu(\dom(\gamma'[X])) = \nu(\emptyset)$.

Write $(\gamma, \gamma_0)^* X$ for the environment from $A \cup \Loc$ to $Val$ defined as $\gamma[n]$, for the least $n$ satisfying the latter condition above.

A pair of valid configurations $(C_1, C_0)$ are called compatible if, given $X \in \{E, P, O\}$, $\gamma_X$ and $\gamma_0$ are compatible (for $X \in \{P, O\}$);

- $\phi_P = \phi_0$ and $\lambda_P = \lambda_0$.
- $(\gamma, \gamma_0)$ are compatible and $\dom(\gamma) \cap \dom(\gamma_0) = \dom(\lambda_P) \cup \dom(\gamma_0) \cup \Loc$.

We write $C = C_1 \circ C_0$ for $(\gamma, \gamma_0)^* E_0 = \gamma$ and $C_0 \circ C_1$ is valid.

We can merge the (well-typed) evaluation stacks $(\nu, E_0, E_0)$ of compatible configurations by the following operation:

$\nu(\langle E, \theta \rightarrow \theta' \rangle) = E \cdot (E_0, \theta \rightarrow \theta') \cdot (E_0, \theta' \rightarrow \theta E_0) = (E_0, \theta \rightarrow \theta')$.

Theorem 19. For all pairs of compatible configurations $C_P$ and $C_0$, $C_P \circ C_0 \Downarrow t$ iff $C_P \Downarrow C_0 \Downarrow \Downarrow t$.

5.3 Soundness result

We need two final pieces of machinery for soundness. The first is so-called $\textit{ciu-equivalence}$, which allows one to characterise contextual equivalence by restricting focus to evaluation contexts.

**Definition 20.** Let $\Sigma$ be a location context. Two terms $\Delta, \Sigma; \Gamma \vdash M_1, M_2 : \theta$ are $\textit{ciu-equivalent}$, written $\Delta, \Sigma; \Gamma \vdash M_1 =_{\textit{ciu}} M_2 : \theta$, when for all typing substitutions $\gamma_1, \ldots, \gamma_n : \Delta, \Sigma$; location contexts $\Sigma' \equiv \Sigma$, closed stores $S \equiv \Sigma'$, value substitutions $\nu : \Sigma' \rightarrow \nu : \Gamma$ and evaluation contexts $\nu : \Gamma(\Sigma[\delta])$, we have $\nu(E[M_2(\gamma_1) \ldots (\gamma_n)](S)) \Downarrow \nu(E[M_2(\gamma_1) \ldots (\gamma_n)](S))$.

**Theorem 21.** $\Delta; \Sigma; \Gamma \vdash M_1 =_{\textit{ciu}} M_2 : \theta$ iff $\Delta; \Sigma; \Gamma \vdash M_1 = M_2 : \theta$.

As mentioned at the beginning of this section, we introduce an equivalence on term denotations which includes equality. The motivation for this is so as to prune out some distinctions that the model makes between behaviours that are in fact indistinguishable. More precisely, our model abstracts away any actual values provided by Opponent for polymorphic inputs by names in Pol. Moreover, when $P$ plays back one of those names, $O$ is in position to determine precisely which actual value is $P$ returning in reality (as all polymorphic names introduced by $O$ must be distinct). This discipline is based on the assumption that $O$ can always instrument the values he provides to $P$ so that he can later distinguish between them. It is a valid assumption, apart from the case when later in the trace there is some value disclosure for those polymorphic names which forbids $O$ to implement such instrumentations.

To remove this extra intensity from the model, we introduce an equivalence of traces which blurs out such distinctions:

- we first substitute in every $P$-move all the $O$ polymorphic names whose value have been disclosed by their disclosed value;
- we then enforce the freshness of $P$ polymorphic names played in $P$ moves, which may be broken because of these substitutions.

The latter step is implemented via a name-refreshing procedure, defined as follows. Given traces $t, t'$, we say that $t'$ is a $P$-refreshing of $t$, written $t \rightarrow t'$, if $t = t'_1 \cdot (m, S, \rho) \cdot t_2$, $t' = t'_1 \cdot t_2$, with $m$ a $P$-move, and there are polymorphic names $p, p'$ such that:

$\rho \notin (t_1 \cdot p) \cap (m, S, \rho)$ is introduced in a $P$-move of $t_1$, $p \notin (t_2 \cdot p)$ and $t_2$ is $(m, S, \rho) \cdot t_2$ where we first replace a single occurrence of $p$ in $(m, S, \rho)$ by $p'$, and then replace any $[p \mapsto v]$ in the resulting subtrace by $[p' \mapsto v] \cdot [p' \mapsto v]$, $P$-refreshing is bound to terminate in the traces we examine. We write $\mathcal{F}(t)$ for the set of all such $t'$ that $t \rightarrow t'$ and $t' \neq t$.

**Definition 22.** Two traces $t_1, t_2$ are said to be equivalent, written $t_1 \sim t_2$, if $\mathcal{F}(t_1) = \mathcal{F}(t_2)$, where $\mathcal{P} \cdot \mathcal{P}_\rho$ is defined as:

$\mathcal{P} \cdot \mathcal{P}_\rho = (\mathcal{P} \cdot \mathcal{P}_\rho)(m, S, \rho(p)) \cdot (\mathcal{P} \cdot \mathcal{P}_\rho)(m, S, \rho(p))$.

We extend equivalence to sets of traces in an elementwise fashion.

**Lemma 23.** Let $t_1$ be a trace such that $t_1 \in \mathcal{T}(C)$ with $C$ a valid configuration. Then for all $t_2 \sim t_1$ we have $t_2 \in \mathcal{T}(C)$.

We can now prove the main theorem of this section.

**Theorem 24 (Soundness).** For all terms $\Delta; \Sigma; \Gamma \vdash M_1, M_2 : \theta$, $\Delta; \Sigma; \Gamma \vdash M_1 \sim M_2$ implies $M_1 \equiv M_2$.

Proof. Suppose $M_1 \sim M_2$. Using Theorem 21 we prove that $M_1 \equiv M_2$. Let us take $\delta, \Sigma \vdash \Sigma$, and $E$ as in Definition 20 and suppose that $(E[M_1(\gamma_1) \ldots (\gamma_n)](S)) \Downarrow$.

Take $(\alpha, \delta, \theta) \in (\Delta; \Sigma; \Gamma)$ and write $C_{P_1}$ for the $P$-configuration $(\langle M_1, \alpha; \delta(x, \theta), \epsilon, \phi, S, \Lambda \rangle, \Lambda \equiv (\Delta; \Sigma; \Gamma \vdash M_1 : \theta)^{\gamma[\alpha, \delta, \theta]} S, \rho \ast C_{P_1}$.
Let $C_0 = ((E, \theta \leadsto \theta'), \gamma, \delta, \phi, S, \lambda')$ where $\gamma' = \{(u_i, v_i) \mid |\gamma(x_i)| = v_i\}$. From Lemma 17 there exists a complete trace $t$ such that $C_{P, t} \equiv C_0$. Then, from Theorem 19, $C_{P, t} \equiv C_0$, so that $t \in \text{Tr}(C_{P, t})$ and $t' \in \text{Tr}(C_0)$. Writing $C_{P, t}$ for the Player configuration $((M_2 \{x/z\}, \theta), e, \phi, S, \lambda)$, from the hypothesis of the theorem, there exists a complete trace $t'$ such that $t' \in \text{Tr}(C_{P, t})$. From Proposition 4 $t' \in \text{Tr}(C_0)$, so that $C_{P, t} \equiv C_0$, and using Theorem 19 (in the other direction), we get that $C_{P, t} \equiv C_0$.

Finally, using Lemma 17 we get that $(E[M_2(\gamma) \{z\}], S) \equiv \frac{\top}{\bot}$.

6. Completeness

While sound, our model fails to be fully abstract as it overestimates the power of O: the way cast relations (Cast) are computed over-approximates the casts that can be implemented by the context in practice, as inhabitation constraints are not taken into account. For instance, a cast from $\theta \rightarrow \theta_1$ to $\theta \rightarrow \theta_2$ does not yield one from $\theta_1$ to $\theta_2$ unless a value of type $\theta$ is available in this section. In all cases we restrict our attention to a fragment of System ReF, called System ReF*, carved in such a way that the above problem cannot be manifested. We then prove our model fully abstract for terms in System ReF*.

System ReF* is defined by means of restricting the types allowed at the type interface of a term. In particular, we pose the following restrictions affecting the types which can appear under a ref constructor. First, we do not allow any binders $\forall \exists$ to appear in the scope of a ref and, moreover, any type variable $\alpha$ inside a ref $\theta$ must be reachably inhabited: in order for a value of type ref $\theta$ to be played in a trace, a value of type $\alpha$ must have been played before.

Both these restrictions are captured by the following type predicate $\text{good}_\alpha(\theta)$, which determines whether a type $\theta$ is in the defined fragment, assuming that the type variables in $\Theta$ are inhabited:

$$\text{good}_\alpha(\theta) = \begin{cases} \text{true} & \text{for } \alpha = \theta_0 \land \forall_\theta(\alpha) \subseteq \Gamma \land \text{quantifier-free} \\ \text{good}_\alpha(\theta') \land \text{good}_\alpha(\gamma(\theta')) & \text{for } \theta \rightarrow \theta' \\ \text{good}_\alpha(\forall_\theta(\gamma(\theta))) & \text{for } \forall_\theta(\gamma(\theta)) \rightarrow \theta \\ \text{false} & \text{otherwise} \end{cases}$$

Above, $\gamma(\theta)$ returns the type variables at the ground level of $\theta$:

$$\gamma(\alpha) = \{\alpha\}$$

$$\gamma(\theta \rightarrow \theta') = \gamma(\theta) \cup \gamma(\theta')$$

$$\gamma(\forall_\theta(\gamma(\theta))) = \gamma(\forall_\theta(\gamma(\theta)))$$

and $\gamma(\theta)$ is reachably inhabited. We extend goodness to type interfaces by setting, given $\Sigma = \{t_1 : \Theta_1, \ldots, t_n : \Theta_n\}$, $\Gamma = (\theta_1, \ldots, \theta_n)$, $\lambda''$:

$$\text{good}(\Delta ; \Sigma ; \Gamma \vdash \Theta) = \text{good}_\delta(\text{ref}_1 \times \cdots \times \text{ref}_n \theta_1 \times \cdots \times \theta_n) \rightarrow \Theta$$

Definition 25. We let System ReF* contain all terms $\Delta ; \Sigma ; \Gamma \vdash M : \Theta$ such that $\text{good}(\Delta ; \Sigma ; \Gamma)$ holds.

Example 26. The terms form Example 10(2) are not in System ReF*, as $\alpha'$ is not inhabited. The two terms are therefore equivalent, because Opponent cannot cast $\alpha$ to Int, lacking a value of type $\alpha'$ to do so. Our model, however, does not capture this equivalence.

Moreover, we call an initial configuration $(\Delta ; \Sigma ; \Gamma \vdash M : \Theta)$ $\text{good}$ just if its interface is, while a valid configuration $(\Delta' ; \Sigma' ; \Gamma' \vdash M : \Theta')$ is good just if, taking $X_\Delta = \{ \alpha \mid \nu(\lambda) \cap \text{Pol}_\alpha \neq \emptyset \}$, $\nu(\phi) \subseteq X_\Delta$ and good$_\Delta$($\phi$) hold, for all $\theta \in \text{cod}(\alpha) \cup \{ \theta \mid \nu(\lambda) \cap \text{Fun}_\alpha \neq \emptyset \}$.

We can then check that goodness is preserved under reduction.

In this restricted fragment, we can always implement all possible casts anticipated from the cast closure construction of Section 3. Moreover specifically, a cast-term from $\theta$ to $\theta'$ based on aliased pairs $(\theta_1, \theta_0), \ldots, (\theta_n, \theta_n')$ and inhabited variables $\alpha_1, \ldots, \alpha_n$ is a term cast$_{\theta_0 \rightarrow \theta'}$ such that:

- For any $\Sigma = \{t_i : \Theta_i\}$, $p_j \in \text{Pol}_{\theta_j}$, $S : \Sigma$ and $\Delta ; \Sigma' \vdash \Theta : \Theta'$,
- $(\text{cast}_{\theta_0 \rightarrow \theta'}(t_i, z_j, y_j)) v, S \rightarrow (v', S', S')$ with $v \equiv v'$.

The $\Theta$ rule, though useful for soundness, has no clear way to be implemented with cast-terms, hence the reason for aiming at its exclusion. The restriction we pose on System ReF* in that quantifiers cannot appear under a ref constructor renders the rule indeed redundant. Each $\phi$ produced in the model contains no types with quantifiers, so that the $\Theta$ rule can be eliminated.

The proof of full abstraction is based on a definability result: we show that every complete trace produced by a good P-configuration $C_P$ can be accepted by an appropriately designed O-configuration $C_O$. In addition, the given trace is all $C_O$ can accept up to nominal and trace equivalence. The technique follows e.g. [17], albeit expanded to the polymorphic setting. Note that the absence of generic types in our language, because of type disclosure, rules out the option of reducing the problem to that for the monomorphic setting.

Theorem 27 (Definability). Let $C_P$ be a good configuration and $t$ a complete trace in $\text{Tr}(C_P)$ with final store $S$. There exists a valid configuration $C_O$ compatible with $C_P$ such that $\text{Tr}(C_O) = \{ t \mapsto t' \mid (\forall x \in \text{Var}(\nu(\phi))) \gamma(\phi(\nu(\theta'))) = \gamma(\phi(\nu(\theta'))) \}$.

We present the main ingredients of the definability argument. We argue by induction on the length of $t$. Suppose $C_P = (\Theta_P, \gamma_P, \phi_P, S_P, \lambda)$, let $\lambda$ be the set of all the names that appear in $t$ and $C_P$. To determine the types behind the O-type-variables in $A_\Theta$, we define a mapping $\delta$ by collecting all type constraints we can derive from the trace $t$ about O-type-variables, mapping to Int when no such constraints exist. We number P-moves in $t$ in decreasing order, that is, the head move of $t$ has index $|t| = |t| + 1/2$, and let $\Theta[t]$ recursively include all function, reference and variable types that appear in $\phi_P(\delta)$ and $\delta(\lambda)$. At the i-th P-move of $t$, this set is updated to $\Theta[t, \delta(\lambda)](\delta(\lambda), \delta(\lambda))$ by including all the types disclosed in intermediate moves.

We use a counter $c$ to determine the position we are in and inductively construct $C_O = (\Theta_O, \gamma_O, \phi_O, S_O, \lambda)$ with the additional assumptions that:

- $\Theta_O = (\Theta_{P, \eta_1 \eta_2} \ni \eta_1, \eta_2, \phi_{\text{last}}) = \cdots = (\Theta, \eta_1, \eta_2, \phi_{\text{last}})$, $n$ is determined from $t$ and $E_i \equiv (\lambda z. \text{fr}(\text{cnt})z)$, for each $i$.

- $\gamma_O$ obeys $\delta$ (i.e. $\gamma_O(\text{Var}) \subseteq \delta$) and, moreover, assigns values to each function or pointer belonging to $O$ by referring to purpose-specific private references in $S_O$.

- For each $f$ of arrow type, a $\gamma_O(f) = \lambda z. \text{fr}(\text{cnt})z$.

- For each $g$ of universal type, $\gamma_O(g) = \lambda a. \text{fr}_g(\text{cnt})a$.

- For each pointer name $p$ of type $\beta$,
  - if $\gamma_O(\beta)$ an arrow type, $\gamma_O(p) = \lambda z. \text{fr}_p(\text{cnt})z$.
  - if $\gamma_O(\beta)$ a universal type, $\gamma_O(p) = \lambda a. \text{fr}_p(\text{cnt})\alpha$.
  - if $\gamma_O(\beta)$ an existential type, $\gamma_O(p) = (\alpha, v)$ and $v$ recursively follows the same discipline.
  - if $\gamma_O(\beta)$ a product type, $\gamma_O(p) = (v_1, v_2)$ and $v_1, v_2$ recursively follow the same discipline.
  - if $\gamma_O(\beta)$ is Int/ref $\theta$ and the value of $p$ gets disclosed in $t$, $\gamma_O(p)$ is the revealed value; otherwise, $\gamma_O(p)$ is a unique integer/location representing $p$.

- if $\gamma_O(\beta) = \alpha'$, $\gamma_O(p)$ is some polymorphic name respecting the type disclosures in $t$.

- $\text{dom}(S_O) \subseteq Q \times Q \cup Q \times \text{Pol}_Q \cup \{ (t_1, \ldots, t_n), (t_1, \ldots, t_n) \}$.

- $\text{con}(\text{cnt}) = \{ (t_1, \ldots, t_n), (t_1, \ldots, t_n) \} \iff (\text{getval} | i \in [1, |t|])$.
where $Q_F$ contains a unique location $q_F$ for each function name $f$ in \( \text{dom}(\gamma_0) \). $Q_F$ contains the $q_F'$s, $Q_P$ the $q_P$'s, and $Q_O$ the $q_O$'s.

The main engine behind the construction is the use of references to record values played, continuations, functions, and generally all history of $t$ so that O can refer to it in order to: decide to accept each expected move by $P$, and play the corresponding expected move.

To record values played, continuations, functions, and generally all $C$ that counts the remaining $P$-moves in $t$. We set $S_0(\text{cnt}) = \|t\|$. $L = \{e_1, \ldots, e_{\|t\|} \}$ is a set of private auxiliary locations which we shall use in order to cast between known types and types obtained by opening existential packages.

The role of the getvals's is to us to store all names that appear in the trace. For each $i$, getval, is a location of type:

$$3\exists!_i ( (\text{Int} \to \theta_1') \times \cdots \times (\text{Int} \to \theta_i') ) \times ((\text{Unit} \to \theta_1') \times \cdots \times (\text{Unit} \to \theta_i'))$$

where $\alpha$ is the sequence of all free type variables in $\Theta_t$. Thus, the value of getvals, is an existential package whose first component contains enumerations of all values of type $\theta_j'$, for each $i, j$. These are is enough to represent all the available values at each point in the trace. The second component inside the package stored in getvals, contains a single reference for each type and we shall assign it to a special role, namely of holding a private reference from the set $L$.

To see how the above work, let $t = (m_1, S_1, \rho_1) \cdot (m_2, S_2, \rho_2) \cdot t'$. Suppose $m_1$ is a question $f(t)$, introducing fresh type variables $\beta_1, \ldots, \beta_i$ (via values of existential type). We encode acceptance of these first two moves in $q$, by setting $S_0(q_i(\|t\|))$ to be:

$$\text{unpack}{\text{getval}_{i\|t\|}}\text{as } (\alpha', (z', h))\text{in}$$

$$\text{let } z = \text{castPk}(z', h)\text{in}$$

$$\lambda\gamma_0. \text{unpack } N_i \text{as } (\beta_0, x) \text{in} \quad \text{unpack } N_i \text{as } (\beta_0, x)$$

$$\text{let } \text{val} = \text{ref}(z, \lambda_0. \Omega, \ldots, \lambda. \Omega)\text{in}$$

$$\text{cnt} \leftarrow F_{\text{shvals}}; \text{Chkvals}; \text{Newvals}; \text{Setter}; \text{Play} \text{ (**)}$$

Since the type of $\text{getval}_{i\|t\|}$ is fully existentially quantified, when we (statically) unpack $\text{getval}_{i\|t\|}$ and get $\alpha', z'$, the $\alpha'$ are distinct from the type variables $\Theta_t$ and, consequently, each component $z': \text{Int} \to \theta_j'$ of $z'$ is not of the expected type $\text{Int} \to \theta_j$. However, when the unpack will actually happen this mismatch will be resolved. For visible types (in the game-theoretic view sense [10]), we need this mismatch to also be resolved statically, as we would like to be able to relate the values in $z'$ with $x_0$, any open variables, or the return value of $\lambda q$. Hence, we employ the castPk function which casts values of type $\theta_j'$ to $\theta_j$ in $z'$, using the locations in $L$ (each of type $\theta_j$) and their representations in $h$.

Each term $N_i$ is selected in such a way so that, using val and $x_0, x_1, \ldots, x_{i-1}$, it captures the precise position within $(m_1, S_1, \rho_1)$ which introduces the type variable $\beta_i$. Note that, here and below, in order to access the values of $\rho_1$ we make use of the cast terms of Lemma[27] We then create the location val to contain the old value stores (z), extended with an empty store for each $\beta_i (\lambda. \Omega)$.

$\text{Fshvals}$ detects the positions inside $(m_1, S_1, \rho_1)$ that introduce fresh names and updates val by adding them as new values in their corresponding types. This yields an updated store $S_{\|t\|}$.

$\text{Chkvals}$ checks that $x_0$, the public part of $S_0$ and the values revealed by type disclosure are the ones expected, that is, $v_i, S_1$ and $\rho_1$ respectively. For these comparisons to be implemented, it suffices to focus on variable types only: the rest are either integers/references (can always be checked), or units/functions (no need to check them). Variable types belonging to $P$ cannot be checked (P always plays fresh names for them), so we skip them. Values of variable types $\alpha$ belonging to $O$ will appear e.g. in $x_0$ with their instantiated types $\delta(\alpha)$. In this case, we are in position to distinguish between function names: these are functions provided by O as polymorphic values so O can pre-instrument so that when calling them they each produce a unique observable effect.

$\text{Newvals}$ creates all the fresh locations of $(m_2, S_2)$ and stores them in the corresponding index of val. Moreover, for each name $j'$ of arrow type in $(m_2, S_2)$, Newvals includes a code portion creating a reference $q_o$ to store a function which takes as an argument the value of the counter specifying the current move, and returns a function following the expected behaviour (and that stipulated by the store obtained for $t'$ by the inductive hypothesis). Similarly for names of universal types. Finally, for each polymorphic O-name $p$ in $(m_2, S_2)$ of type $\alpha$, Newvals includes code creating $q_p$ and adding a function in val according to the type $\gamma_0(\alpha)$ (e.g. if an arrow type then we add $\lambda z. \text{lambda}_{(\text{cnt})} z$, where $q_p$ encapsulates an effect which allows its recognition in the future).

$\text{Setter}$ updates the store in such a way that all the values of $S_2$ are set, while Play is defined by case analysis on $m_2$.

Using Definability, we can now prove the main theorem.

*Theorem 29* (Completeness). Given System Rep* terms $\Delta; \Sigma; \Gamma \vdash M_1, M_2 : \theta$ if $M_1 \equiv M_2$ then $[M_1] \equiv [M_2]$.

**References**


