Free theorems and runtime type representations

Dimitrios Vytiniotis and Stephanie Weirich

University of Pennsylvania
{dimitriv,sweirich}@cis.upenn.edu

Abstract. Reynolds' abstraction theorem [21], often referred to as the parametricity theorem, can be used to derive properties about functional programs solely from their types. Unfortunately, in the presence of runtime type analysis, the abstraction properties of polymorphic programs are no longer valid. However, runtime type analysis can be implemented with term-level representations of types, as in the λ_R language of Crary *et al.* [10], where case analysis on these runtime representations introduces type refinement. In this paper, we show that representation-based analysis is consistent with type abstraction by extending the abstraction theorem to such a language. We also discuss the "free theorems" that result. This work provides a foundation for the more general problem of extending the abstraction theorem to languages with generalized algebraic datatypes (GADTs).

1 Introduction

Reynolds' abstraction theorem [21] serves as a characterization of *parametric polymorphism*. It asserts that parametrically polymorphic functions behave in a uniform way, independently of the types at which they are used. Importantly, the abstraction theorem can be used to derive equivalences involving functional programs, just by observing the types of these programs. Wadler [26] refers to these equivalences as the "free theorems" associated with particular types.

For example, one free theorem about the polymorphic λ-calculus (also known as System F [13]) is that for any function f of type

$$\forall a \, . \, a \to a$$

we know that for any type τ and function $h : \tau \to \tau$ we have the following equivalence

$$f[\tau] \circ h \cong h \circ f[\tau]$$

where $\circ$ indicates function composition and $\cong$ indicates *program equivalence*, a relation that we will make more precise later. From this free theorem we can conclude that f must behave like the identity function, as h could be any arbitrary function.

However, Reynolds' abstraction theorem does not hold for all extensions of the polymorphic λ-calculus. In particular, it does not hold in the presence of an operator for runtime type analysis, such as the *typecase* operator from Harper and Morrisett's language λ_i^{ML} [14]. In this language, polymorphic functions do not always behave parametrically. For example, the following function increments integers, but is the identity function for any other type.

$$f = \Lambda a \,.\, \mathit{typecase}\ a\ \mathit{of}\ \{\mathit{Int} \Rightarrow \lambda x{:}\mathit{Int} \,.\, x + 1 \ \mid\ \_ \Rightarrow \lambda x{:}a \,.\, x\}$$

Consequently, even though f is of type $\forall a \,.\, a \to a$, we can contradict its free theorem by picking $h = (\lambda x{:}\mathit{Int} \,.\, 8)$.

$$f[\mathit{Int}] \circ (\lambda x{:}\mathit{Int} \,.\, 8) \not\cong (\lambda x{:}\mathit{Int} \,.\, 8) \circ f[\mathit{Int}]$$

Runtime type analysis is a useful language feature. It can be used to define type-indexed operations such as generic parsers, pretty printers, iterators and other operations that automate the boilerplate of working with algebraic datatypes [7, 28]. However, partly because of the negative interactions with type abstraction, few typed functional languages support it.

One promising approach is to use *term representations of types* to simulate runtime type analysis, such as with Crary, Weirich and Morrisett's language λ_R [10]. In this language, *typecase* analyzes terms that represent types, instead of types. The type of a term representation reveals what type it represents—if the term e represents type τ, then term e has type $R\ \tau$. Determining the identity of e simultaneously determines the identity of τ. Because polymorphic functions in λ_R treat their type arguments parametrically, Crary et al. conjectured that the abstraction theorem could be extended to that language, but no one has yet done so.

The question about representation types and parametricity has recently become more relevant to modern languages with the introduction of *generalized algebraic datatypes* (GADTs) [3, 8, 23, 24, 16, 25], a variant of *inductive families of types* [12] originally developed in dependent type theory. With GADTs, we may implement representation types, so that, as we discuss below, extending the abstraction theorem to a language with representation types tells us how to extend it to a language with GADTs.

Using the GADT syntax of the Glasgow Haskell Compiler (GHC), we can define the R representation type using the following datatype declaration.

$$\begin{array}{l} \mathit{data}\ R\ a\ \mathit{where} \\ \quad R_{\mathit{Int}} \ :: R\ \mathit{Int} \\ \quad R_{\to} \ :: \forall ab \,.\, R\ a \to R\ b \to R\ (a \to b) \\ \quad R_{\mathit{any}} :: \forall a \,.\, R\ a \end{array}$$

The R datatype has several constructors, each corresponding to the representation of a particular type. For example, R_{Int} serves as a runtime representation of the *Int* datatype. The $R_{\rightarrow}$ constructor takes the representations for the argument and the result type of a function type, and returns a representation of that function type. The R_{any} constructor is an "un-representation"—it represents *any* type, so does not actually provide any run-time information.

Functions that take arguments of type $R\ \tau$ may perform case analysis on these arguments. However, unlike ordinary pattern matching, in the types of the branches the type τ is *refined* according to the constructor matched each time. Consider the function g below of type $\forall a\,.\, R\ a \rightarrow a \rightarrow a$.

$$g = \Lambda a\,.\,\lambda y{:}R\ a\,.\,case\ y\ of\ \{R_{Int} \Rightarrow \lambda x : Int\,.\,x + 1 \mid \_ \Rightarrow \lambda x : a\,.\,x\}$$

In the case for R_{Int}, the type variable a is refined to be equal to *Int*, so the particular branch is acceptable even though the type of the case expression is $a \rightarrow a$.

The free theorems about functions that take type representation arguments are weaker than those for functions that do not. For example for any function of type

$$\forall a\,.\,R\ a \rightarrow a \rightarrow a$$

we should *not* expect that

$$(g[\tau]\ r) \circ h \cong h \circ (g[\tau]\ r) \tag{1}$$

for any appropriately typed r and h. To see why consider the function g above. Equivalence (1) does not hold when $h = (\lambda x : Int\,.\,8)$ and $r = R_{Int}$, since:

$$(g[Int]\ R_{Int}) \circ (\lambda x : Int\,.\,8) \ncong (\lambda x : Int\,.\,8) \circ (g[Int]\ R_{Int})$$

Nevertheless, we can still derive a free theorem for g when it is applied to R_{any}, since R_{any} does not introduce any type refinement:

$$(g[\tau]\ (R_{any}[\tau])) \circ h \cong h \circ (g[\tau]\ (R_{any}[\tau]))$$

In this paper, we explore parametricity in the context of an explicitly typed polymorphic λ-calculus which includes runtime type representations. In particular:

– We present a parametricity result for our language by giving a *sound relational interpretation* of types as sets of pairs of closed values and showing that every well-typed expression is related to itself in the interpretation of its type. We derive free theorems from this soundness property.
– We show that for programs that have pure System F types, the *same free theorems* as in System F are derivable.
– We show that for programs with types that involve the R datatype, free theorems *can still be derived*, but may be, in general, less informative than theorems for R-free types.

Importantly, we are confident that the ideas presented in this paper will extend to a language that supports arbitrary GADTs, by combining known techniques for relational interpretations of recursive types in an operational setting [4, 9, 2, 1]. We sketch how this might be done, but we leave the full details of this experiment as future work.

We have a complete formalization of the parametricity result in this paper in the Isabelle/HOL [18] proof assistant, available from:

`www.cis.upenn.edu/~dimitriv/parametricity/`

This formalization should not only be viewed as supporting material, but also as an extensive real-world study of representation techniques and proof methods for polymorphic languages in proof assistants. Our proofs are thoroughly commented and available to other researchers who would like to explore extensions of the abstraction theorem.

The rest of the paper is structured as follows: As a warm-up we review parametricity for System F in Section 2. In Section 3 we introduce representation types and extend the relational interpretation of System F. We sketch how our technique extends to arbitrary GADTs in Section 4. We present related and future work in Section 5.

2 Parametricity for System F

As a starting point, we review a standard parametricity result for System F extended with an integer base type. In Section 3 we will extend this foundation to a language with representation types.

$$\begin{array}{lll}
\text{Types} & \sigma, \tau & ::= a \mid \mathit{Int} \mid \tau \to \tau \mid \forall a \,.\, \tau \\
\text{Terms} & e & ::= i \mid x \mid \lambda x{:}\tau \,.\, e \mid e\ e \mid \Lambda a \,.\, e \mid e[\tau] \\
\text{Environments} & \Gamma, \Delta & ::= \epsilon \mid \Gamma, a \mid \Gamma, (x{:}\tau) \\
\text{Values} & u, v, w & ::= i \mid \lambda x{:}\tau \,.\, e \mid \Lambda a \,.\, e
\end{array}$$

Types include type variables, the base type *Int*, arrow types, and universal types; terms include integer literals i, variables, abstractions, applications, type abstractions, and type applications. Environments record type variables introduced by type abstractions, and term variables introduced by term abstractions. We write ϵ for the empty environment. We write $\sigma\{\tau/a\}$ for the capture-avoiding substitution of τ for a in σ. The judgement $\Gamma \vdash \tau$ ensures that the free variables of the type τ are bound in Γ. The typing relation is given with judgements of the form $\Gamma \vdash e : \tau$. The operational semantics that we use is a standard, small-step, call-by-name. We write $e_1 \to e_2$ for the transition relation and $e_1 \to^* e_2$ for the reflexive and transitive closure of the transition relation. We write $e_1 \Downarrow e_2$ to mean that $e_1 \to^* e_2$ and $\nexists e_3 \,.\, e_2 \to e_3$.

2.1 Relational interpretation of System F types

Every type of System F can be interpreted as a relation between closed values. For a closed type τ, we define the set of all closed values of that type as $\mathit{Value}(\tau) = \{v \mid \epsilon \vdash v : \tau\}$ and the set of binary relations between values of two different (closed) types as $\mathit{VRel}(\tau_1, \tau_2) = \{r \mid r \subseteq \mathit{Value}(\tau_1) \times \mathit{Value}(\tau_2)\}$. We write id_τ for the set $\{(v, v) \mid v \in \mathit{Value}(\tau)\}$.

Definition 1 (Computation relation lifting). *Let $r \in \mathit{VRel}(\tau_1, \tau_2)$. The lifting of r to a computation relation r^* is given by:*

$$r^* = \{(e_1, e_2) \mid \epsilon \vdash e_i : \tau_i \wedge e_i \Downarrow v_i \wedge (v_1, v_2) \in r\}$$

Definition 2 (Semantic substitutions δ). *Assume that r ranges over arbitrary value relations. Semantic substitutions are given by:*

$$\gamma, \delta ::= \epsilon \mid \delta, a \mapsto (\tau_1, \tau_2, r) \mid \delta, x \mapsto (e_1, e_2)$$

We view semantic substitutions as partial maps. Whenever $\delta(a) = (\tau_1, \tau_2, r)$ we write $\delta^1 a$ for τ_1, $\delta^2 a$ for τ_2 and $\delta[a]$ for r. Similarly when $\delta(x) = (e_1, e_2)$ we write $\delta^1 x$ for e_1 and $\delta^2 x$ for e_2. We extend the definition to $\delta^i \tau$ and $\delta^i e$ homomorphically (modulo capture-avoidance).

Definition 3 (Function space relation constructor). *Let $r_a \in \mathit{VRel}(\tau_a^1, \tau_a^2)$ and $r_b \in \mathit{VRel}(\tau_b^1, \tau_b^2)$. Then let $r_a \Rightarrow r_b \in \mathit{VRel}(\tau_a^1 \to \tau_b^1, \tau_a^2 \to \tau_b^2)$ be*

$$\begin{aligned} r_a \Rightarrow r_b = \{(v_1, v_2) \mid \epsilon \vdash v_i : \tau_a^i \to \tau_b^i \wedge \\ \forall e_1 e_2 \,.\, (e_1, e_2) \in {r_a}^* \Longrightarrow (v_1\ e_1, v_2\ e_2) \in {r_b}^*\} \end{aligned}$$

We now give the relational interpretation of System F types.

Definition 4 (Relational interpretation of System F types). *The interpretation of types is given as a function defined recursively on the size of types:*

$$\begin{aligned} [\![\mathit{Int}]\!]_\delta &= id_{\mathit{Int}} \\ [\![a]\!]_\delta &= \delta[a] \\ [\![\sigma_1 \to \sigma_2]\!]_\delta &= [\![\sigma_1]\!]_\delta \Rightarrow [\![\sigma_2]\!]_\delta \\ [\![\forall a \,.\, \sigma]\!]_\delta &= \{(v_1, v_2) \mid \epsilon \vdash v_i : \delta^i(\forall a \,.\, \sigma) \wedge \\ &\qquad \forall \tau_1\ \tau_2\ r \,.\, r \in \mathit{VRel}(\tau_1, \tau_2) \Longrightarrow \\ &\qquad\qquad (v_1\ [\tau_1], v_2\ [\tau_2]) \in ([\![\sigma]\!]_{\delta, a \mapsto (\tau_1, \tau_2, r)})^*\} \end{aligned}$$

Note that the interpretation of quantified types extends the given semantic substitution δ, which is used for the interpretation of type variables. Strictly speaking, for the interpretation of open types we only need the bindings of type variables in semantic substitutions (and not bindings of term variables). However, the fact that semantic substitutions can be put in one-to-one correspondence with typing environments simplifies the formal treatment, which is important for our encoding in Isabelle/HOL. In particular, we define when a substitution δ is well-formed in an environment Γ, written as $\Gamma \vdash \delta$.

Definition 5 (Well-formed semantic substitutions).

$$\frac{}{\epsilon \vdash \epsilon}\ \text{WFSE} \qquad \frac{\Delta \vdash \delta \quad r \in \mathit{VRel}(\tau_1, \tau_2)}{\Delta, a \vdash \delta, a \mapsto (\tau_1, \tau_2, r)}\ \text{WFSTY} \qquad \frac{\Delta \vdash \delta \quad (e_1, e_2) \in [\![\tau]\!]_\delta^{\,*}}{\Delta, (x{:}\tau) \vdash \delta, x \mapsto (e_1, e_2)}\ \text{WFSTM}$$

The parametricity theorem can be proved with the following sequence of lemmas.

Lemma 1 (Interpretation of types is a value relation). *If $\Gamma \vdash \tau$ and $\Gamma \vdash \delta$ then $[\![\tau]\!]_\delta \in \mathit{VRel}(\delta^1\tau, \delta^2\tau)$.*

Compositionality asserts that the interpretation of types depends only on the interpretation of structurally smaller types.

Lemma 2 (Compositionality). *If $\Gamma, a \vdash \tau$ and $\Gamma \vdash \sigma$ and $\Gamma \vdash \delta$ then $[\![\tau]\!]_{\delta, a \mapsto (\delta^1\sigma, \delta^2\sigma, [\![\sigma]\!]_\delta)} = [\![\tau\{\sigma/a\}]\!]_\delta$*

The following theorem is referred as the "soundness lemma", or the "fundamental property of the logical relation" or the "abstraction theorem", or the "parametricity theorem". This theorem shows that well-typed terms are related in the relation which is given by the interpretation of their types, and can be proven by induction on the typing derivations appealing to the previous lemmas.

Theorem 1 (Fundamental property of logical relation). *If $\Gamma \vdash e : \tau$ and $\Gamma \vdash \delta$ then $(\delta^1 e, \delta^2 e) \in [\![\tau]\!]_\delta^{\,*}$.*

Free theorems can be derived by expanding definitions in the following corollary.

Corollary 1. *If $\epsilon \vdash e : \tau$ then $(e, e) \in [\![\tau]\!]_\epsilon^{\,*}$.*

Example 1 (Free theorem for $\forall a \,.\, a \rightarrow a$). Let $\epsilon \vdash f : \forall a \,.\, a \rightarrow a$. The fundamental property then gives:

$$\begin{aligned} &\forall \tau_1\ \tau_2\ r \,.\, r \in \mathit{VRel}(\tau_1, \tau_2) \Longrightarrow \\ &\quad \forall e_1\ e_2 \,.\, (e_1, e_2) \in r^* \Longrightarrow (f[\tau_1]\ e_1, f[\tau_2]\ e_2) \in r^* \end{aligned}$$

Let us consider any τ_1, τ_2, and $\epsilon \vdash h : \tau_1 \rightarrow \tau_2$. Let $\cong$ be an equivalence relation for typed terms that is evaluation-respecting and congruent.[1] Let r be the graph of h, defined as $r = \{(v_1, v_2) \mid \epsilon \vdash v_1 : \tau_1 \wedge \epsilon \vdash v_2 : \tau_2 \wedge h\ v_1 \Downarrow v_2\}$. Then pick a value x such that $\epsilon \vdash x : \tau_1$ and $(x, h\ x) \in r^*$. By the free theorem, it has

[1] Precisely, for this example we need the properties that, for appropriately typed expressions e and e_1 and e_2, if $e_1 \rightarrow e_2$ then $e_1 \cong e_2$, and $e_1 \cong e_2$ implies $e\ e_1 \cong e\ e_2$. These properties are true of any reasonable notion of program equivalence, such as contextual equivalence.

to be that $f[\tau_1]\ x \Downarrow w_1$ and $f[\tau_2]\ (h\ x) \Downarrow w_2$, such that $(w_1, w_2) \in r$, that is, $h\ w_1 \Downarrow w_2$. Because equivalence is evaluation-respecting we have $f[\tau_1]\ x \cong w_1$ and by congruence $h\ (f[\tau_1]\ x) \cong h\ w_1$. For the same reason $h\ w_1 \cong w_2$, therefore $h\ (f[\tau_1]\ x) \cong w_2$, and consequently

$$h\ (f[\tau_1]\ x) \cong f[\tau_2]\ (h\ x)$$

Moreover, because h is arbitrary, f must behave as the identity function.

We describe program equivalence abstractly, since for the various examples in this paper we need only certain congruence properties and the fact that equivalence is evaluation-respecting. The question of whether the logical relation that we have presented coincides with a specific standard notion of program equivalence (such as *ciu*-equivalence) is, to our knowledge, open. However, we have shown that if we restrict the interpretation of polymorphic types to only quantify over relations that respect a particular definition of program equivalence, that equivalence is a sound and complete characterization of the logical relation (both for System F and the extensions presented in the next section). We do not present the details here, as the focus of this paper is not about reasoning for program equivalences, but rather deriving free theorems from types.

Additionally, observe that it is an easy corollary of the fundamental property that all closed expressions of the language terminate. In essence, the relational interpretation of types assigns relations to type variables, just as in Girard's reducibility candidates method [13] a type variable is assigned a candidate set. Adding a recursion primitive in the language has no further complication for the soundness of the relational semantics, provided that we quantify over $\top\top$-closed relations [19], or (alternatively) admissible relations, that is, strict and limit-preserving ones. How to express admissibility syntactically has been studied elsewhere [4].

3 Type representations

We now extend System F to include type representations and show how to extend the relational interpretation of types.

$$\begin{array}{lll}
\text{Types } \tau & ::= & \ldots \mid R\ \tau \\
\text{Terms } e & ::= & \ldots \mid R_{\mathit{Int}} \mid R_{\rightarrow}[\tau_a][\tau_b] e_a\, e_b \mid R_{\mathit{any}}[\tau] \mid \mathit{rcase}\ e\ \mathit{of}\{ e_{\mathit{Int}}\ ;\ e_{\rightarrow}\ ;\ e_{\mathit{any}} \} \\
\text{Values } u, v & ::= & \ldots \mid R_{\mathit{Int}} \mid R_{\rightarrow}[\tau_a][\tau_b] e_a\, e_b \mid R_{\mathit{any}}[\tau]
\end{array}$$

We add the R type form, constructors for representing integer types (R_{Int}), function types ($R_{\rightarrow}$), and the "any" constructor (R_{any}), *rcase*. The *rcase* expression is an elimination form that performs pattern matching on values of type $R\ \tau$, selecting one of the branches (e_{Int}, $e_{\rightarrow}$, or e_{any}). Operationally, when the scrutinee reduces to R_{Int} the e_{Int} branch is taken, and analogously for $R_{\rightarrow}$ and R_{any}. For space reasons, we elide the necessary extensions to the operational semantics.

The typing relation is extended with the following new rules.

$$\frac{}{\Gamma \vdash R_{\mathit{Int}} : R\ \mathit{Int}}\ \textsc{rint} \qquad \frac{\Gamma \vdash \tau}{\Gamma \vdash R_{\mathit{any}}[\tau] : R\ \tau}\ \textsc{rany}$$

$$\frac{\Gamma \vdash e_a : R\ \tau_a \quad \Gamma \vdash e_b : R\ \tau_b}{\Gamma \vdash R_{\rightarrow}[\tau_a][\tau_b]\ e_a\ e_b : R\ (\tau_a \rightarrow \tau_b)}\ \textsc{rfun}$$

$$\frac{\begin{array}{c}\Gamma \vdash \forall c\,.\,\tau \qquad \Gamma \vdash e : R\ \sigma \qquad \Gamma \vdash e_{\mathit{Int}} : \tau\{\mathit{Int}/c\} \\ \Gamma \vdash e_{\rightarrow} : \forall ab\,.\,R\ a \rightarrow R\ b \rightarrow \tau\{(a \rightarrow b)/c\} \qquad \Gamma \vdash e_{\mathit{any}} : \forall c\,.\,\tau\end{array}}{\Gamma \vdash \mathit{rcase}\ e\ \mathit{of}\ \{e_{\mathit{Int}}\ ;\ e_{\rightarrow}\ ;\ e_{\mathit{any}}\} : \tau\{\sigma/c\}}\ \textsc{rcase}$$

The rules for the new constructors, RINT, RFUN, and RANY are standard. The rule RCASE is like a standard case expression, except that the type of each branch is specialized to the represented type. Rule RCASE first asserts that the type τ has one distinguished free variable c with $\Gamma \vdash \forall c\,.\,\tau$. The result type of the case expression is formed by replacing c with σ, when the scrutinee e has a $R\ \sigma$ type. In the case of e_{Int}, we know that σ is equal to Int, so c is replaced by Int in that type. Likewise, the $e_{\rightarrow}$ branch requires first two types a, and b, and two representations, $R\ a$ and $R\ b$, acting as a pattern to match against e. It then returns an expression of type τ, where c has been refined to $a \rightarrow b$. Finally, the type of e_{any} does not do any refinement. These typing rules allow us, for example, to typecheck the example from the introduction:

$$\begin{array}{l} g = \Lambda a\,.\,\lambda x{:}R\ a\,.\,\mathit{rcase}\ x\ \mathit{of}\ \{\ \lambda w{:}\mathit{Int}\,.\,w + 1; \\ \qquad\qquad\qquad\qquad\qquad\quad \Lambda bc\,.\,\lambda z{:}R\ b\,.\,\lambda y{:}R\ c\,.\,(\lambda w{:}b \rightarrow c\,.\,w); \\ \qquad\qquad\qquad\qquad\qquad\quad \Lambda c\,.\,\lambda w{:}c\,.\,w\} \end{array}$$

3.1 Extension of relational interpretation

We next extend Definition 4 with the interpretation of $R\ \tau$ types. A naïve attempt at this definition merely checks the mapping of the type τ in δ to determine the related pairs. For example, part of this definition might read

$$\mathit{If} \quad \delta^1\tau = \delta^2\tau = \mathit{Int} \quad \mathit{then} \quad [\![R\ \tau]\!]_\delta = \{(R_{\mathit{Int}}, R_{\mathit{Int}})\} \cup \{(R_{\mathit{any}}[\mathit{Int}], R_{\mathit{any}}[\mathit{Int}])\}$$

since if $\delta^i\tau = \mathit{Int}$ then the only closed values of type $R\ \mathit{Int}$ are R_{Int}, and $R_{\mathit{any}}[\mathit{Int}]$. This naïve interpretation would have a similar case for the other constructors as well: If $\delta^1\tau = \tau_a^1 \rightarrow \tau_b^1$ and $\delta^2\tau = \tau_a^2 \rightarrow \tau_b^2$ then we would relate pairs $(R_{\rightarrow}[\tau_a^1][\tau_b^1]\ e_a^1\ e_b^1, R_{\rightarrow}[\tau_a^2][\tau_b^2]\ e_a^2\ e_b^2)$ where $(e_a^1, e_a^2) \in ([\![R\ a]\!]_{a \mapsto (\tau_a^1, \tau_a^2, r_a)})^*$, for some arbitrary relation r_a, $(e_b^1, e_b^2) \in ([\![R\ b]\!]_{b \mapsto (\tau_b^1, \tau_b^2, r_b)})^*$, for some arbitrary relation r_b. Finally, no matter what the definition of $\delta^1\tau$ and $\delta^2\tau$ is, we would always include the pair $(R_{\mathit{any}}[\delta^1\tau], R_{\mathit{any}}[\delta^2\tau])$.

However this definition is problematic. Consider the free theorem that results from this definition when $\epsilon \vdash g : \forall a \,.\, R\ a \rightarrow a \rightarrow a$.

$$\begin{array}{l} \forall \tau_1\ \tau_2\ r \,.\, r \in \mathit{VRel}(\tau_1, \tau_2) \Longrightarrow \\ \quad \forall e_r^1\ e_r^2\ e_1\ e_2 \,.\, (e_r^1, e_r^2) \in (\llbracket R\ a \rrbracket_{a \mapsto (\tau_1, \tau_2, r)})^* \wedge (e_1, e_2) \in r^* \Longrightarrow \\ \qquad (g[\tau_1]\ e_r^1\ e_1, g[\tau_2]\ e_r^2\ e_2) \in r^* \end{array}$$

Specifically, the above implies that:

$$\begin{array}{l} \forall r \,.\, r \in \mathit{VRel}(\mathit{Int}, \mathit{Int}) \Longrightarrow \\ \quad \forall e_1\ e_2 \,.\, (e_1, e_2) \in r^* \Longrightarrow (g[\mathit{Int}]\ R_{\mathit{Int}}\ e_1, g[\mathit{Int}]\ R_{\mathit{Int}}\ e_2) \in r^* \end{array}$$

Let r be the graph of the constant function $\mathit{eight} = \lambda x{:}\mathit{Int} \,.\, 8$. Consequently:

$$g[\mathit{Int}]\ R_{\mathit{Int}}\ (\mathit{eight}\ x) \cong \mathit{eight}\ (g[\mathit{Int}]\ R_{\mathit{Int}}\ x) \tag{2}$$

But, as we saw in Section 1, this equation is not true for every g of type $\forall a \,.\, R\ a \rightarrow a \rightarrow a$!

Technically the problem lies in the proof of the fundamental property. Specifically the fundamental property states that $\Gamma \vdash e : \tau$ and $\Gamma \vdash \delta$ then $(\delta^1 e, \delta^2 e) \in \llbracket \tau \rrbracket_\delta{}^*$ and its proof proceeds by induction on the typing derivation. The interesting case follows:

– Case RCASE. We have that $\Gamma \vdash \mathit{rcase}\ e\ \mathit{of}\ \{e_{\mathit{Int}}\ ;\ e_{\rightarrow}\ ;\ e_{\mathit{any}}\} : \tau\{\sigma/c\}$ given that $\Gamma \vdash \forall c \,.\, \tau$, $\Gamma \vdash e : R\ \sigma$, and $\Gamma \vdash e_{\mathit{Int}} : \tau\{\mathit{Int}/c\}$ (and others). By induction $(\delta^1 e, \delta^2 e) \in \llbracket R\ \sigma \rrbracket_\delta{}^*$. We now proceed by case analysis on $\delta^1\sigma$ and $\delta^2\sigma$. Assume that $\delta^1\sigma = \delta^2\sigma = \mathit{Int}$ (the other cases would create similar problems). Then $\delta^1 e$ and $\delta^2 e$ either both evaluate to R_{Int} or the both evaluate to $R_{\mathit{any}}[\mathit{Int}]$. Suppose the former. By induction, $(\delta^1 e_{\mathit{Int}}, \delta^2 e_{\mathit{Int}}) \in \llbracket \tau\{\mathit{Int}/c\} \rrbracket_\delta{}^*$, hence $\delta^1 e_{\mathit{Int}} \Downarrow w_1$ and $\delta^2 e_{\mathit{Int}} \Downarrow w_2$ so that $(w_1, w_2) \in \llbracket \tau\{\mathit{Int}/c\} \rrbracket_\delta$. Hence $\delta^1(\mathit{rcase}\ e\ \mathit{of}\ \{e_{\mathit{Int}}\ ;\ e_{\rightarrow}\ ;\ e_{\mathit{any}}\})$ and $\delta^2(\mathit{rcase}\ e\ \mathit{of}\ \{e_{\mathit{Int}}\ ;\ e_{\rightarrow}\ ;\ e_{\mathit{any}}\})$ evaluate to w_1 and w_2 respectively. We need to establish finally that $\llbracket \tau\{\mathit{Int}/c\} \rrbracket_\delta = \llbracket \tau\{\sigma/c\} \rrbracket_\delta$. Appealing to the compositionality lemma, it suffices to show that:

$$\llbracket \tau \rrbracket_{\delta, (c \mapsto (\mathit{Int}, \mathit{Int}, \mathit{id}_{\mathit{Int}}))} = \llbracket \tau \rrbracket_{\delta, (c \mapsto (\delta^1\sigma, \delta^2\sigma, \llbracket \sigma \rrbracket_\delta))}$$

  At this point the proof is stuck! Although we have that $\delta^1\sigma = \delta^2\sigma = \mathit{Int}$ we have *no restriction on the interpretation of* σ.

From this failed proof we see that in the interpretation of $R\ \sigma$ we can return the pair $(R_{\mathit{Int}}, R_{\mathit{Int}})$ if $\delta^1\sigma = \delta^2\sigma = \mathit{Int}$ *and* $\llbracket \sigma \rrbracket_\delta = \mathit{id}_{\mathit{Int}}$. Generalizing this idea, we see that the interpretation of $R\ \sigma$ must restrict the interpretation of σ. We define the interpretation of $R\ \sigma$ types using the operator $\mathfrak{R}\ r$ below.

Definition 6 (Extension for $R\ \sigma$ types).

$$
\begin{aligned}
[\![R\ \sigma]\!]_\delta \quad &= \mathfrak{R}\ [\![\sigma]\!]_\delta \\
\mathfrak{R}\ (r^{\in VRel(\tau_1,\tau_2)}) &= \{\ (R_{Int}, R_{Int}) \mid \boxed{r = id_{Int} \wedge \tau_1 = \tau_2 = Int}\} \cup \\
&\quad \{\ (R_{\rightarrow}[\tau_a^1][\tau_b^1]\ e_a^1\ e_b^1, R_{\rightarrow}[\tau_a^2][\tau_b^2]\ e_a^2\ e_b^2)\ \mid \\
&\qquad \exists r_a \in VRel(\tau_a^1,\tau_a^2)\,.\,\exists r_b \in VRel(\tau_b^1,\tau_b^2)\,. \\
&\qquad\quad \boxed{r = r_a \Rightarrow r_b \wedge \tau_i = \tau_a^i \rightarrow \tau_b^i} \wedge \\
&\qquad\quad (e_a^1, e_a^2) \in (\mathfrak{R}\ r_a)^* \wedge (e_b^1, e_b^2) \in (\mathfrak{R}\ r_b)^*\ \} \cup \\
&\quad \{\ (R_{any}[\tau_1], R_{any}[\tau_2])\ \}
\end{aligned}
$$

The $\mathfrak{R}\ r$ function is well-defined since the size of the types becomes smaller in sub-calls.[2] The boxed parts of the definition indicate the restrictions imposed on the interpretation of σ when interpreting $R\ \sigma$ types. Note that the constructor R_{any} does not restrict the interpretation of σ. The constructor $R_{\rightarrow}$ only restricts the interpretation of σ to be "functional".

We have validated the fundamental property for this definition, and we now show how it can be used to derive free theorems. (Note that the fundamental property also gives us type soundness and termination.)

Example 2 (Free theorem for $\forall a\,.\,R\ a \rightarrow a \rightarrow a$). We show here that if $\epsilon \vdash f : \forall a\,.\,R\ a \rightarrow a \rightarrow a$, then $f[\tau]\ (R_{any}[\tau])$ must behave as the identity function. Note that it is not the case that f behaves as the identity on its second argument in general. The free theorem is:

$$
\begin{aligned}
&\forall \tau_1\ \tau_2\ r \in VRel(\tau_1,\tau_2)\,.\implies \\
&\quad (\forall e_1\ e_2\,.\,(e_1,e_2) \in r^* \implies (f[\tau_1]\ (R_{any}[\tau_1])\ e_1, f[\tau_2]\ (R_{any}[\tau_2])\ e_2) \in r^*) \wedge \\
&\quad (\forall e_1\ e_2\,.\,r = id_{Int} \wedge \tau_i = Int \wedge (e_1,e_2) \in r^* \implies \\
&\qquad (f[\tau_1]\ R_{Int}\ e_1, f[\tau_2]\ R_{Int}\ e_2) \in r^*) \wedge \\
&\quad (\forall \tau_a^{1,2} \tau_b^{1,2} e_a^{1,2} e_b^{1,2}\ r_a \in VRel(\tau_a^1,\tau_a^2)\ r_b \in VRel(\tau_b^1,\tau_b^2) e_1\ e_2\,. \\
&\qquad \tau_i = \tau_a^i \rightarrow \tau_b^i \wedge r = r_a \Rightarrow r_b \wedge (e_1,e_2) \in r^* \implies \\
&\qquad\quad (f[\tau_1]\ (R_{\rightarrow}[\tau_a^1][\tau_b^1] e_a^1\ e_b^1) e_1, f[\tau_2]\ (R_{\rightarrow}[\tau_a^2][\tau_b^2] e_a^2\ e_b^2) e_2) \in r^*
\end{aligned}
$$

Assuming that x is of type τ_1 and r is the graph of a function h with $\epsilon \vdash h : \tau_1 \rightarrow \tau_2$ we get that

$$h\ (f[\tau_1]\ (R_{any}[\tau_1])\ x) \cong f[\tau_2]\ (R_{any}[\tau_2])\ (h\ x)$$

Taking $\tau_1 = \tau_2$, since the equation above must be true for any h we conclude that $f[\tau]\ (R_{any}[\tau])$ must behave as the identity function on any type τ.

[2] In our Isabelle/HOL formalization we deviated slightly from this definition and used an inductively defined relation, with judgements of the form $(v_1, v_2) \in \mathfrak{R}\ r$. This allowed us to derive inversion principles automatically instead of having to prove them from the definition of the function $\mathfrak{R}$.

However, the free theorems for functions that include representation types have a "you get what you pay for" feeling. Observe, for example, that the case of the theorem above for $f\ [Int]\ R_{Int}$ is not particularly informative.

$$\begin{array}{l}\forall \tau_1\ \tau_2\ r \in VRel(\tau_1, \tau_2)\,.\\ \quad \forall e_1\ e_2\,.\, r = id_{Int} \wedge \tau_i = Int \wedge (e_1, e_2) \in r^* \Longrightarrow\\ \qquad (f[\tau_1]\ R_{Int}\ e_1, f[\tau_2]\ R_{Int}\ e_2) \in r^*\end{array}$$

This case derives the following:

$$\forall e_1\ e_2\ i\,.\, e_1 \Downarrow i \wedge e_2 \Downarrow i \Longrightarrow \exists j\,.\,(f[Int]\ R_{Int}\ e_1) \Downarrow j \wedge f[Int]\ R_{Int}\ e_2 \Downarrow j$$

The above simply asserts that if the function takes two arguments that can be reduced to the same integer value, then the results will always be reducible to the same integer value.

4 Arbitrary GADTs

The form of Definition 6 has a close connection to a constraint-based presentation of the constructors of the R datatype. In such presentations [29, 8, 24] the types of the various R-constructors would be written as:

$$\begin{array}{rl} R_{Int} & ::\ \forall a\ .\ (a = Int) \Rightarrow R\ a\\ R_{\rightarrow} & ::\ \forall abc\ .\ (a = b \rightarrow c) \Rightarrow R\ b \rightarrow R\ c \rightarrow R\ a\\ R_{any} & ::\ \forall a\ .\ true \Rightarrow R\ a\end{array}$$

Each of these constructors induces a certain refinement, indicated by an *equality constraint*. Our interpretation is motivated by the intuition that a constructor-induced equality constraint $\tau_1 = \tau_2$ must restrict the interpretations of τ_1 and τ_2 in the semantic substitution δ such that $[\![\tau_1]\!]_\delta = [\![\tau_2]\!]_\delta$ and $\delta^i(\tau_1) = \delta^i(\tau_2)$. Note additionally that the variables b and c on the type of the $R_{\rightarrow}$ constructor can be viewed as "existentially" quantified because they only appear only negatively in the type of $R_{\rightarrow}$. This existential quantification is reflected in the logical relation with the existential quantification over relations r_a and r_b.

This same intuition is applicable to the interpretation of arbitrary GADTs. As an example, let us consider a generalized algebraic datatype $Eq\ \tau_1\ \tau_2$ with one constructor, $Refl[\tau]$, that enforces *equality at the level of types.*

$$\frac{\Gamma \vdash \tau}{\Gamma \vdash Refl[\tau] : Eq\ \tau\ \tau}\ \text{REFL} \qquad \frac{\Gamma \vdash e : Eq\ \sigma_1\ \sigma_2 \quad \Gamma \vdash \forall a\,.\,\tau \qquad \Gamma \vdash e_{Refl} : \tau\{\sigma_2/a\}}{\Gamma \vdash rcase\ e\ of\ \{e_{Refl}\} : \tau\{\sigma_1/a\}}\ \text{REFL-CASE}$$

The rule REFL-CASE ensures that in the body of the expression, the type σ_1 is replaced with σ_2. Turning to the relational interpretation, we can view *Refl* as having type $\forall ab\,.\,(a = b) \Rightarrow Eq\ a\ b$, producing the following definition

$$[\![Eq\ \tau_1\ \tau_2]\!]_\delta = \{(Refl[\sigma_1], Refl[\sigma_2]) \mid \delta^i(\tau_1) = \delta^i(\tau_2) = \sigma_i \wedge [\![\tau_1]\!]_\delta = [\![\tau_2]\!]_\delta\}$$

Using this definition, and assuming the fundamental property, we have an interesting free theorem.

Example 3 (Free theorem for $\forall ab \,.\, Eq\ a\ b \to a \to b$). The free theorem that we get for this type is:

$$\begin{array}{l}\forall \tau_a^1\ \tau_a^2\ r_a\ \tau_b^1\ \tau_b^2\ r_b\ \tau_1\ \tau_2\ r\,.\\ \quad r_a \in \mathit{VRel}(\tau_a^1, \tau_a^2) \wedge r_b \in \mathit{VRel}(\tau_b^1, \tau_b^2) \Longrightarrow\\ \qquad \tau_a^i = \tau_b^i = \tau_i \wedge r_a = r_b = r \Longrightarrow (f\ (\mathit{Refl}[\tau_1]), f\ (\mathit{Refl}[\tau_2])) \in r \Rightarrow r^*\end{array}$$

We can now argue that for any $\epsilon \vdash x : \tau_1$ and $\epsilon \vdash h : \tau_1 \to \tau_2$, taking r to be the graph of h, we have:

$$h\ ((f[\tau_1]\ (\mathit{Refl}[\tau_1])\ x) \cong (f[\tau_2]\ (\mathit{Refl}[\tau_2]))\ (h\ x)$$

In other words, $f[\tau]\ (\mathit{Refl}[\tau])$ can only behave as the identity function on τ and hence f can safely be used as (a part of) a type-safe generic cast function. The theorem guarantees that it its implementation is correct.

All GADTs can be written as normal datatypes augmented with equality constraints. So the technique that we describe here may be generally applied. However, in the general case, interpreting arbitrary GADTs subsumes interpreting arbitrary recursive polymorphic datatypes, which itself is not an easy problem. This problem has been extensively studied, as we discuss in the next section.

5 Related and future work

Relational parametricity and typing constraints. The relational interpretation of representation types that we give in this paper could be used to give a general treatment of equality-constrained polymorphism, which we have never seen presented. We also are not aware of any extensions of the abstraction theorem to type systems that include arbitrary constraints, such as qualified types, although parametricity in the presence of subtyping constraints has been studied [5] (though not syntactically).

Parametricity and intensional type analysis. Washburn and Weirich [27] address the issue of parametricity and runtime type analysis by using an information-flow type and kind system to track which types are analyzed. In that setting, the non-interference theorem generalizes Reynolds' abstraction theorem. The free theorems in that language are more informative than here because the types are more informative. However, that work did not address free theorems for languages with GADTs.

Mechanizing logical relations arguments. There is some related work in the formalization of logical relations arguments about polymorphic λ-calculi in theorem provers. Donnelly and Xi prove termination for the simply typed λ-calculus and System F using ATS/LF [11]. Also, Sarnat and Schürmann [22] show that it is possible to define logical relations in Twelf, by first encoding an appropriate assertion logic. In that way, theorems about the logical relation reduce to theorems about the consistency of the assertion logic. However, some logical relations (such as this one) require higher-order logic as their assertion logic, and it is not known how to express the consistency of such a logic in Twelf.

For our particular formalization in Isabelle/HOL we used the locally nameless technique. Bound variables are represented as de Bruijn indices, and free variables as names. Our starting point was Leroy's solution to the POPLmark challenge in Coq[3], with slight modifications in the way that we distinguished between type and term variables, which eliminated a significant amount of extra reasoning. Additionally, we found Charguéraud's suggestions [6] for avoiding equivariance proofs helpful.

Recursive types and logical relations. There is much related work in the area of logical relations for recursive and polymorphic types. Logical relation proofs are notoriously difficult for recursive datatypes—without even considering GADTs. The reason is that recursive datatypes prevent us from defining the logical relation inductively on the structure or size of types. To circumvent this restriction we can define such logical relations as fixpoints of certain generating functions. To solve the problem with contravariance, Pitts (based on work of Freyd) [20, 19], pioneered the domain-theoretic technique of defining logical relations by a diagonization argument as fixpoints of bi-functors, that generate relations. Showing that the "positive" fixpoint and the "negative" fixpoint of such functors coincide relies crucially on the local continuity of these functors. Harper and Birkedal [4], and later Crary and Harper [9] translate this technique into a purely operational setting. A different approach involves step-indexed models [2, 1], where the logical relation relates triples consisting of an integer k and two values, to mean that the two values are actually equivalent inside any computation that runs at most for k steps, but may be distinguished later. Recently Vouillon and Mellies [17] have proposed an operationally-based relational model in which recursive types can be interpreted, the main characteristic being that the type language is augmented with interval types. Finally, for positive datatypes, Johann [15] shows that the logical relation can in general be defined by taking "local fixpoints" in the definition of the relation. For example, the lifting of a relation to the list datatype will be a fixpoint of an appropriate generating function. However, the particular work does not show how to extend this to arbitrary *type-parameterized* positive datatypes.

[3] `http://pauillac.inria.fr/~xleroy/POPLmark/locally-nameless/`

Future work. There are several avenues that we plan to explore in future work. Most importantly, we would like to extend this work to arbitrary GADTs in a nonterminating language, using a constraint-based presentation and a syntactic model for recursive polymorphic datatypes. That way our work would more directly relate to Haskell programs. We would also like to add higher-order types (as in F_ω) and a type-level type analysis operator so that we may show parametricity for full λ_R. To do so, we would start with ideas of Washburn and Weirich [27] who show how to extend a relational interpretation of a second-order language with a limited form of type-level type analysis.

References

1. Amal J. Ahmed. Step-indexed syntactic logical relations for recursive and quantified types. In Peter Sestoft, editor, *ESOP*, volume 3924 of *Lecture Notes in Computer Science*, pages 69–83. Springer, 2006.
2. Andrew W. Appel and David McAllester. An indexed model of recursive types for foundational proof-carrying code. *ACM Trans. Program. Lang. Syst.*, 23(5):657–683, 2001.
3. Lennart Augustsson and Kent Petersson. Silly type families. Available from http://www.cs.pdx.edu/ sheard/papers/silly.pdf, September 1994.
4. Lars Birkedal and Robert Harper. Relational interpretations of recursive types in an operational setting. In *Theoretical Aspects of Computer Software*, 1997.
5. Luca Cardelli, John C. Mitchell, Simone Martini, and Andre Scedrov. An extension of system F with subtyping. In Takayasu Ito and Albert R. Meyer, editors, *Proc. of 1st Int. Symp. on Theor. Aspects of Computer Software, TACS'91, Sendai, Japan, 24–27 Sept 1991*, volume 526, pages 750–770. Springer-Verlag, Berlin, 1991.
6. Arthur Charguéraud, Benjamin Pierce, and Stephanie Weirich. Proof engineering, practical techniques for mechanized metatheory. (Submitted for publication.), October 2006.
7. James Cheney and Ralf Hinze. Poor man's dynamics and generics. In *Proceedings of the ACM SIGPLAN 2002 Haskell Workshop*, September 2002.
8. James Cheney and Ralf Hinze. First-class phantom types. CUCIS TR2003-1901, Cornell University, 2003.
9. Karl Crary and Robert Harper. Syntactic logical relations for polymorphic and recursive types. (Submitted for publication.), August 2006.
10. Karl Crary, Stephanie Weirich, and Greg Morrisett. Intensional polymorphism in type erasure semantics. *Journal of Functional Programming*, 12(6):567–600, November 2002.
11. Kevin Donnelly and Hongwei Xi. A formalization of strong normalization for simply typed lambda-calculus and System F. In *International Workshop on Logical Frameworks and Meta-Languages: Theory and Practice (LFMTP'06), Seattle, WA*, Aug 2006.
12. Peter Dybjer. Inductive sets and families in Martin-Löf's type theory and their set-theoretic semnatics. In Gerard Huet and Gordon Plotkin, editors, *Logical Frameworks*, pages 280–306. Prentice Hall, 1991.
13. Jean-Yves Girard. Une extension de l'interprétation de Gödel à l'analyse, et son application à l'élimination de coupures dans l'analyse et la théorie des types. In J. E. Fenstad, editor, *Proceedings of the Second Scandinavian Logic Symposium*, pages 63–92. North-Holland Publishing Co., 1971.

14. Robert Harper and Greg Morrisett. Compiling polymorphism using intensional type analysis. In *Twenty-Second ACM SIGPLAN-SIGACT Symposium on Principles of Programming Languages*, pages 130–141, San Francisco, January 1995.
15. Patricia Johann and Janis Voigtlnder. Free theorems in the presence of seq. *SIGPLAN Not.*, 39(1):99–110, 2004.
16. Simon Peyton Jones, Dimitrios Vytiniotis, Stephanie Weirich, and Geoffrey Washburn. Simple unification-based type inference for gadts. In *ICFP '06: Proceedings of the eleventh ACM SIGPLAN international conference on Functional programming*, pages 50–61, New York, NY, USA, 2006. ACM Press.
17. Paul-Andre Mellies and Jerome Vouillon. Recursive polymorphic types and parametricity in an operational framework. In *LICS '05: Proceedings of the 20th Annual IEEE Symposium on Logic in Computer Science (LICS' 05)*, pages 82–91, Washington, DC, USA, 2005. IEEE Computer Society.
18. Tobias Nipkow, Lawrence C. Paulson, and Markus Wenzel. *Isabelle/HOL — A Proof Assistant for Higher-Order Logic*, volume 2283 of *LNCS*. Springer, 2002.
19. A. M. Pitts. Typed operational reasoning. In B. C. Pierce, editor, *Advanced Topics in Types and Programming Languages*, chapter 7, pages 245–289. The MIT Press, 2005.
20. Andrew M. Pitts. Parametric polymorphism and operational equivalence. *Mathematical Structures in Computer Science*, 10:321–359, 2000.
21. John C. Reynolds. Types, abstraction and parametric polymorphism. In *Information Processing '83*, pages 513–523. North-Holland, 1983. Proceedings of the IFIP 9th World Computer Congress.
22. Jeffrey Sarnat and Carsten Schurmann. On the representation of logical relations in twelf. Technical Report YaleU/DCS/TR-1362, Yale University, 2006.
23. Tim Sheard and Emir Pasalic. Meta-programming with built-in type equality. In *Proc 4th international workshop on logical frameworks and meta-languaegs (LFM'04), Cork*, July 2004.
24. Vincent Simonet and François Pottier. Constraint-based type inference with guarded algebraic data types. Technical report, INRIA, July 2003.
25. Martin Sulzmann, Jeremy Wazny, and Peter Stuckey. A framework for extended algebraic data types. Technical report, National University of Singapore, 2005.
26. Philip Wadler. Theorems for free! In *FPCA89: Conference on Functional Programming Languages and Computer Architecture*, London, September 1989.
27. Geoffrey Washburn and Stephanie Weirich. Generalizing parametricity using information flow. In *The Twentieth Annual IEEE Symposium on Logic in Computer Science (LICS 2005)*, pages 62–71, Chicago, IL, June 2005. IEEE Computer Society, IEEE Computer Society Press.
28. Stephanie Weirich. RepLib: A library for derivable type classes. In *Haskell Workshop*, Portland, OR, USA, September 2006.
29. Hongwei Xi, Chiyan Chen, and Gang Chen. Guarded recursive datatype constructors. In *Thirtieth ACM SIGPLAN-SIGACT Symposium on Principles of Programming Languages*, pages 224–235, New Orleans, LA, USA, January 2003.