A Two-Level Logic Approach to Reasoning about Typed Specification Languages

Mary Southern¹ and Kaustuv Chaudhuri²

¹ University of Minnesota, USA
marys@cs.umn.edu

² INRIA, France
kaustuv.chaudhuri@inria.fr

Abstract

The two-level logic approach (2LL) to reasoning about computational specifications, as implemented by the Abella theorem prover, represents derivations of a specification language as an inductive definition in a reasoning logic. This approach has traditionally been formulated with the specification and reasoning logics having the same type system, and only the formulas being translated. However, requiring identical type systems limits the approach in two important ways: (1) every change in the specification language’s type system requires a corresponding change in that of the reasoning logic, and (2) the same reasoning logic cannot be used with two specification languages at once if they have incompatible type systems. We propose a technique based on adequate encodings of the types and judgements of a typed specification language in terms of a simply typed higher-order logic program, which is then used for reasoning about the specification language in the usual 2LL. Moreover, a single specification logic implementation can be used as a basis for a number of other specification languages just by varying the encoding. We illustrate our technique with an implementation of the LF dependent type theory as a new specification language for Abella, co-existing with its current simply typed higher-order hereditary Harrop specification logic, without modifying the type system of its reasoning logic.

1 Introduction

Higher-order abstract syntax (HOAS) [14], also known as λ-tree syntax (λTS) [9], has become a standard representational style for data structures with variable binding. Such data are pervasive in the syntax of programming languages, proof systems, process calculi, formalized mathematics, etc. Variable binding issues are a particularly tricky aspect of the meta-theory of computational systems given in the form of structural operational semantics (SOS). Such specifications are nearly always formulated as relations presented in the form of a natural deduction proof system.

In this paper, we are concerned with proving properties about such higher-order relational specifications. For example, if the specification is of the typing relation for simply typed λ-calculus, then we may want to prove that a given λ-term has exactly one type (type-uniqueness), or that the type of a λ-term remains stable during evaluation (type-preservation). This kind of reasoning proceeds by induction on the derivations of the specified relations, so we need a formalism that supports both inductive definitions and reasoning by induction. The two-level logic approach (2LL) is a general scheme for such reasoning systems, where the specification language derivations are viewed as an inductively defined object in a reasoning logic. In this reasoning logic, the specification language derivations are given a closed world reading,
which is to say that that derivability in the specification language is completely specified: it can not only establish that certain specification formulas or judgements are derivable, but also that others are not derivable, or that two specification derivations are (bi)similar. We focus on the Abella implementation of the 2LL, which is an interactive tactics-based theorem prover designed to reason about a subset of higher-order λProlog programs seen as the logic of higher-order hereditary Harrop (HOHH) formulas [21, 20].

We consider an extension of the 2LL that can use a single reasoning logic to reason about a number of different specification languages in the same development. The HOHH language has only simple types, which makes both the specifications and the reasoning somewhat verbose because structural invariants must be separately specified and explicitly invoked in theorems. Richer type systems can often encode such invariants intrinsically in the types; to illustrate, dependent types can be used to define a type of (representations of) well-typed λ-terms, which is not possible with just simple types. Moreover, with such richer type systems one can often use the inductive structure of the terms themselves to drive the inductive argument rather than using auxiliary relations.

Unfortunately, the 2LL as currently defined [6] does not sufficiently address these desiderata. In particular, the specification and reasoning languages are required to have the same type system because the specification-level constants and their types are directly lifted to reasoning-level constants with the same type. Thus, if we required a version of Abella based on a dependent type theory as a specification language, we would need to also change its reasoning logic G to be dependently typed. This goes against the 2LL philosophy where the reasoning logic is seen as common, static, and eternal. More importantly, it both breaks portability of developments and causes duplication of effort.

Our position is that we should extend the 2LL in such a way that the reasoning-level and specification-level type systems are separated. Indeed, the specification types and judgements must themselves be encoded as terms and formulas of the reasoning logic. This encoding must be coherent with that of specification-level terms and formulas, both of which are encoded as reasoning-level atomic formulas. This is achieved by guaranteeing that our encoding of the type systems is adequate; that is, the encoding of the specification-level type system must be able to represent all specification-level typing derivations, and that reasoning about the specification-level type system should be reducible to reasoning, by induction, on the encoding. An essential ingredient of adequacy is a right-inverse of the encoding that extracts a specification-level typing judgement from a reasoning-level formula when the formula is in the image of the encoding.

To be concrete, we illustrate the extended 2LL in this paper by giving an encoding of the LF dependent type theory, which is then implemented as a translation layer in Abella. The reasoning logic of Abella is left untouched, as is the existing HOHH specification language for reasoning about λProlog programs. Our encoding of LF is based on that of [18, 19], suitably modified to the context of interactive theorem proving rather than logic programming. Since both LF and HOHH are based on intuitionistic logic, our extension of Abella uses a core implementation of an intuitionistic specification language that is shared by both the HOHH and the LF languages. Interestingly, the details of the encoding into this core language can almost entirely be obscured for the user; in particular, to use the system the user does not need to know how the specification language is encoded, since the system uses the right inverse mentioned above to present the types, terms, and judgements of the specification language in their native forms.

The rest of the paper is organized as follows. Section 2 presents the two-level logic approach (2LL) and its implementation in the Abella theorem prover. Section 3 presents LF
and its adequate translation into a simply typed higher-order logic programming language. This is then used in section 4 to explain our extension of the 2LL by means of adequate translations. Related work is surveyed in section 5.

2 Background

This section sketches the two-level logic approach (2LL) as implemented in the Abella theorem prover \[21\]. More details, including the full proof systems and their meta-theory, can be found in the following sequence of papers: \[20\, 6\, 8\].

2.1 The Reasoning Logic $G$

The reasoning logic of Abella, $G$, is a predicative and intuitionistic version of Church’s Simple Theory of Types. Types are built freely from primitive types, which includes the type $\text{prop}$ of formulas, using the function type constructor $\to$. Intuitionistic logic is introduced into this type system by means of the constants $\text{true}, \text{false} : \text{prop}$, binary connectives $\land, \lor, \supset : (\tau \to \text{prop}) \to \text{prop}$ for types $\tau$ that do not contain $\text{prop}$. For every type $\tau$ not containing $\text{prop}$, we also add an atomic predicate symbol $= : \tau \to \tau \to \text{prop}$ to reason about intensional (i.e., up to $\alpha\beta\gamma$-conversion) equality. Following usual conventions, we write $\land, \lor, \supset$, and $= : \tau \to \tau \to \text{prop}$ infix, and write $\forall x : \tau. A$ for $\forall \tau (\lambda x. A)$ (and similarly for $\exists$). We also omit the type subscripts and type-ascription on variables when unambiguous.

To provide the ability to reason on open $\lambda$-terms, which is necessary when reasoning about HOAS representations, $G$ also supports generic reasoning. This is achieved by adding, for each type $\tau$ not containing $\text{prop}$, an infinite set of nominal constants and a generic quantifier $\forall : (\tau \to \text{prop}) \to \text{prop}$. We also add a weaker form of intensional equality called equivariance that equates two terms whose free nominal constants may be systematically permuted to each other. Note that equivariance is only used to match conclusions to hypotheses in the $G$ proof system; $=$ continues to have the standard $\lambda$-conversion semantics. The support of a term $t$, written $\text{supp}(t)$, is the multiset of nominal constants that occur in it; whenever we introduce a new eigenvariable, such as using the $\forall$-right or $\exists$-left rules, we raise the eigenvariables over the support of the formula. This raising is needed to express permitted dependencies on these nominal constants.

To accommodate fixed-point definitions, $G$ is parameterized by sets of definitional clauses. Each such clause has the form $\forall \vec{x}. (\forall \vec{z}. A) \equiv B$ where $A$ (the head) is an atomic formula whose free variables belong to $\vec{x}$ or $\vec{z}$, while $B$ (the body) is any arbitrary formula that can only mention the variables in $\vec{x}$, and can additionally have recursive occurrences of the predicate symbol in the head. Each clause partially defines a relation named by the predicate in the head. We additionally require that $\text{supp}(\forall \vec{z}. A)$ and $\text{supp}(B)$ be both empty, and that recursive predicate occurrences satisfy a stratification condition [5]. Finally, some of these definitions in $G$ can be marked as inductive or co-inductive, in which case the set of definitional clauses for that relation are given least or greatest fixed-point semantics. This is approximated in Abella by means of size annotations, which are formally defined and proved correct in [4].

1 Roughly, stratification prevents definitions such as $p \equiv \neg p$, which would lead to inconsistency.
A Two-Level Logic Approach to Reasoning about Typed Specification Languages

The need for the two kinds of specification sequents and the mechanism for proving properties is the case for the

The essence of the inference system such as:

\[ \text{seq} \ L \ (G_1 \land G_2) \trianglerighteq \text{seq} \ L \ G_1 \land \text{seq} \ L \ G_2 \]

\[ \text{seq} \ L \ (F \Rightarrow G) \trianglerighteq \text{seq} \ (F : : L) \ G \]

\[ \text{seq} \ L \ (\pi \ F) \trianglerighteq \forall x. \text{seq} \ L \ (F \ x) \]

\[ \text{seq} \ L \ A \trianglerighteq \text{mem} \ F \ L \land \text{bch} \ L \ F \ A \]

\[ \text{seq} \ L \ A \trianglerighteq \text{prog} \ F \land \text{bch} \ L \ F \ A \]

Figure 1 Encoding HOHH using definitional clauses in \( G \). \( F \) and \( G \) range over arbitrary specification formulas, while \( A \) ranges over atomic specification formulas. All clauses are implicitly universally closed over their capitalized variables.

2.2 The Specification Language: HOHH

The essence of the 2LL is to encode the deductive formalism of the specification language in terms of an inductive definition. However, before this can be done, the terms and formulas—and types!—of the specification language must be represented in the reasoning logic. This is trivial if the specification and reasoning logics have the same term and type language, which is the case for the HOHH language. To encode HOHH formulas, we use a new basic type \( o \), and formula constructors \( \Rightarrow, \& : o \rightarrow o \rightarrow o \) (written infix), and an infinite family of specification-level quantifiers \( \pi_i : (\tau \rightarrow o) \rightarrow o \) (written prenex) for types \( \tau \) that do not contain \( o \). To prevent circularity, we disallow the type \( \text{prop} \) and the reasoning level formula constructors from occurring inside specification level types and terms.

The proof system for HOHH is a standard focused sequent calculus for this fragment of the logic, assuming that all atoms have negative polarity; this is equivalent to saying that the proof system implements backchaining [20]. This proof system is implemented in \( G \) using two predicates, \( \text{seq} : \text{olist} \rightarrow o \rightarrow \text{prop} \) and \( \text{bch} : \text{olist} \rightarrow o \rightarrow o \rightarrow \text{prop} \), standing for goal reduction and backwrd chaining respectively, with the definitional clauses shown in figure 1. Here, \( \text{olist} \) is the type of lists of \( o \), with constructors \( \text{nil} : \text{olist} \) and \( (: :) : o \rightarrow \text{olist} \rightarrow \text{olist} \) (written infix), and a membership relation \( \text{mem} : o \rightarrow \text{olist} \rightarrow \text{prop} \) that has the obvious inductive definition. In Abella, these two relations are displayed using the more evocative notation \( \{L \mid G\} \) and \( \{L, F \mid G\} \) for \( \text{seq} \ L \ G \) and \( \text{bch} \ L \ F \ G \). The final clause for \( \text{seq} \) uses a separate predicate \( \text{prog} : o \rightarrow \text{prop} \) that is true exactly for the clauses in the specification program. It is easy to see that with this syntax, the definitional clauses of figure 1 are precisely the inductive definition of a backchaining proof system.

2.3 Example: Type Uniqueness

The need for the two kinds of specification sequents and the mechanism for proving properties about the specification logic are best described with an example. Consider the simply typed \( \lambda \)-calculus, itself specified as an object logic in HOHH. The simple type system is represented using a new basic type \( \text{ty} \) with two constructors, \( i : \text{ty} \) (a basic sort), and \( \text{arr} : \text{ty} \rightarrow \text{ty} \rightarrow \text{ty} \) for constructing arrow types. The \( \lambda \)-terms are typed using a different basic type \( \text{tm} \) with two constructors: \( \text{app} : \text{tm} \rightarrow \text{tm} \rightarrow \text{tm} \) and \( \text{abs} : \text{ty} \rightarrow (\text{tm} \rightarrow \text{tm}) \rightarrow \text{tm} \). The \( \lambda \)-term \( \lambda x : i. \lambda f : i \rightarrow i. f x \) would be represented as \( \text{abs} \ i \ (\lambda x : i. \text{abs} \ i \ i) \ (\lambda f : \text{ty} \rightarrow \text{ty} \rightarrow \text{ty} \ (\lambda x : i. f x)) \). The relation between terms (of type \( \text{tm} \)) and types (of type \( \text{ty} \)) is usually expressed in the form of an inference system such as:

\[
\frac{\Gamma, x : A \vdash M : B}{\Gamma \vdash (\lambda x : A. M) : A \rightarrow B} \quad \frac{\Gamma \vdash M : A \rightarrow B \quad \Gamma \vdash N : A}{\Gamma \vdash M \ N : B} \quad \frac{\Gamma \vdash N : B}{\Gamma, x : A \vdash x : A^{\text{var}}} \quad (1)
\]
This relation is succinctly expressed as a pair of \texttt{HOHH} program clauses for the predicate \texttt{of} : \texttt{tm} \rightarrow \texttt{ty} \rightarrow \texttt{o}, which is used both for assumptions of the form \( x : A \) and for conclusions of the form \( M : A \) in the inference system above.

\[
\begin{align*}
\pi \text{ a:ty.} \text{ pi b:ty.} \text{ pi m:tm.} \text{ pi n:tm.} \text{ of m (arr a b) } \Rightarrow & \text{ of n a } \Rightarrow \text{ of (app m n) b.} \\
\pi \text{ a:ty.} \text{ pi b:ty.} \text{ pi r:tm } \Rightarrow & \text{ of (tm (pi x:tm x) tm) } \Rightarrow \text{ of (abs a r) (arr a b).}
\end{align*}
\]

Note that there is no clause for \texttt{var}; rather, it is folded into an assumption in the body of the \texttt{abs} case, which delimits its scope. It is generally easier to read such clauses when they are written using the standard \texttt{Prolog} syntactic convention of using capital letters for universally closed variables, writing implications in the reverse direction with the head first, and separating assumptions by commas rather than repeated implications. Thus, the above clauses correspond to:

\[
\begin{align*}
\text{of (app M N) B} & \Leftarrow \text{of M (arr A B), of N A.} \\
\text{of (abs A B) (arr A B)} & \Rightarrow \text{pi x\ of (R x) B } \Rightarrow \text{of (abs a r) (arr a b).}
\end{align*}
\]

The formula \( \pi \ (\lambda x. F) \) is rendered as \( \pi \ x : A \) in the concrete syntax, and the scope of \( x \) extends as far to the right as possible. Note that all the types are inferred.

In the reasoning mode of \texttt{Abella}, the above \( \lambda \texttt{Prolog} \) specification is \texttt{imported} by reflecting all specification constants and types in the reasoning signature, and by generating a definition for \texttt{prog} that is true only for the two clauses for \texttt{of}. The typing judgement \( x : A, y : B \vdash M : C \) in the inference system (1), for instance, would be represented by \texttt{seq (of y B :: of x A :: nil) (of M C)}. As an example of reasoning on this specification, we can prove that \texttt{of} is deterministic in its second argument:

\[
\text{forall M A B, (| of M A) } \rightarrow \text{ (| of M B)} \rightarrow A = B.
\]

which is just concrete syntax for:

\[
\forall M: \text{tm.} \forall A: \text{ty.} \forall B: \text{ty. seq nil \ of (of M A) } \supset \text{ seq nil \ of (of M B)} \supset A = B.
\]

This theorem is proved by induction on the derivation of one of the \texttt{seq} assumptions, such as the first one. This induction would repeatedly \texttt{match} the form \texttt{seq nil M A} against the left hand sides of the definitional clauses in figure 1; for every successful match, the corresponding right hand side of the clause would give us new assumptions, which may then be used in the inductive hypothesis.

Initially, the only clause that matches is the final one for \texttt{seq} corresponding to backchaining on a program clause. In the case where the clause for \texttt{abs} is selected, the corresponding \texttt{bch} clause for it would in turn call \texttt{seq} with a different list of assumptions. Thus, the inductive argument cannot proceed with empty dynamic specification contexts (the first argument to \texttt{seq} and \texttt{bch}) alone: we must also allow for reasoning under an abstraction. This is achieved in the reasoning logic by inductively characterizing all such dynamic context extensions with a new atom, say \texttt{ctx : olist } \rightarrow \texttt{prop}, with the following inductive definitional clauses:

\[
\begin{align*}
\text{ctx nil } & \equiv \text{ true.} \\
\forall A. \forall G. (\forall x. \text{ctx \ (of x A :: G)) } & \equiv \text{ctx G.}
\end{align*}
\]

We can then prove a stronger lemma:

\[
\text{forall G M A B, ctx G } \rightarrow \{ G \vdash \text{of M A}\} \rightarrow \{ G \vdash \text{of M B}\} \rightarrow A = B.
\]

Now, when the dynamic context does grow when backchaining on the clause for \texttt{abs}, it will grow exactly by the form in the head of the second clause of \texttt{ctx}, \texttt{i.e.}, with a formula of the form \( \pi \ n A \) where \( n \) is a nominal constant that does not occur in \( A \) nor in the original context \( G \). Thus, when we in turn backchain on the dynamic clauses (using the penultimate clause for \texttt{ctx} in figure 1), we will know the precise form of the selected clause.
A Two-Level Logic Approach to Reasoning about Typed Specification Languages

\[ \phi(\Pi x : A. P) := \phi(A) \to \phi(P) \]

\[ \langle c \rangle := c \]

\[ \langle \lambda x : A. M \rangle := \lambda x : \phi(A). \langle M \rangle \]

\[ \phi(a \ M_1 \cdots M_n) := \text{lfobj} \]

\[ \langle x \rangle := x \]

\[ \phi(\text{type}) := \text{lftype} \]

\[ \langle M_1 \ M_2 \rangle := \langle M_1 \rangle \langle M_2 \rangle \]

**Figure 2** Encoding of LF types and kinds as simple types and LF objects as simply typed \( \lambda \)-terms.

### 3 An Adequate Translation of LF to HOHH

The Edinburgh Logical Framework (LF) is a dependently typed \( \lambda \)-calculus which is used for specifying formal systems. Terms of this language belong to one of the following three syntactic categories:

- **Kinds**: \( K ::= \text{type} \mid \Pi x : A. K \)
- **Types**: \( A, B ::= a \ M_1 \cdots M_n \mid \Pi x : A. B \)
- **Objects**: \( M, N ::= c \mid x \mid \lambda x : A. M \mid M \ N \)

Types, sometimes called *families*, classify objects and kinds classify types. Here \( a \) represents a type-level constant, \( c \) an object level constant, and \( x \) an object level variable. Following standard convention, we will write \( A \to B \) as a shorthand for \( \Pi x : A. B \) when \( x \) does not appear free in \( A \). We will use \( U \) to denote both types and objects and \( P \) for both kinds and types, so \( U : P \) will stand either for a typing or a kinding judgement. We will write \( U[M_1/x_1, \ldots, M_n/x_n] \) to denote the capture avoiding substitution of \( M_1, \ldots, M_n \) for free occurrences of \( x_1, \ldots, x_n \) respectively.

An LF specification is a list of object or type constants together with their types or kinds, called a *signature*. Let us revisit the example of the simply typed \( \lambda \)-calculus and its associated typing relation used in section 2.3. The \( \lambda \)-terms are encoded using the following signature:

<table>
<thead>
<tr>
<th>( \text{ty} )</th>
<th>( \text{tm} )</th>
</tr>
</thead>
<tbody>
<tr>
<td>( i ) : ( \text{ty} )</td>
<td>( u ) : ( \text{tm} )</td>
</tr>
<tr>
<td>( \text{arr} : \text{ty} \to \text{ty} \to \text{ty} )</td>
<td>( \text{app} : \text{tm} \to \text{tm} \to \text{tm} )</td>
</tr>
<tr>
<td>( \text{abs} : \text{ty} \to (\text{tm} \to \text{tm}) \to \text{tm} )</td>
<td></td>
</tr>
</tbody>
</table>

For the typing relation \( \text{of} \), in LF we declare it as a dependent type rather than as a predicate as in HOHH. The clauses of the \( \text{of} \) type are then viewed as constructors for the dependent type, and are therefore also given names.

<table>
<thead>
<tr>
<th>( \text{of} )</th>
<th>( \text{ofU} )</th>
<th>( \text{ofApp} )</th>
<th>( \text{ofAbs} )</th>
</tr>
</thead>
<tbody>
<tr>
<td>( \text{of : tm} \to \text{ty} \to \text{type} )</td>
<td>( \text{ofU : of u i} )</td>
<td>( \text{ofApp : {A : \text{ty}} {B : \text{ty}} {M : \text{tm}} {\text{tm}} )</td>
<td>( \text{ofAbs : {A : \text{ty}} {B : \text{ty}} {\text{tm} \to \text{tm}} )</td>
</tr>
<tr>
<td>( \text{of (arr A B) = of N A \to of (app M N) B} )</td>
<td></td>
<td>( \text{ofAbs : {A : \text{ty}} {\text{tm} \to \text{tm}} \to \text{of (abs A B) (arr A B)} )</td>
<td></td>
</tr>
</tbody>
</table>

Here, the concrete syntax \( \{x:A\} \ B \) denotes \( \Pi x : A. B \).

The LF type system is formally defined in [7] and will not be repeated here. Instead, we will directly give an adequate encoding of the LF type system in terms of HOHH, based on the variant of [3] defined in [18], with the inverse mapping defined in [19].

The encoding proceeds in two steps. First, we transform our dependently typed terms into simply typed HOHH terms. The encoding of types and kinds is defined as a mapping, written \( \phi(-) \). These types indicate that the term is an encoding of an LF type and an LF object, respectively. For each constant \( c : P \) in the LF signature, we generate a simply typed term \( c \) of type \( \phi(P) \). Using this mapping, the dependently typed \( \lambda \)-terms are converted into simply typed \( \lambda \)-terms using the mapping \( (-) \). Figure 2 contains the rules for both \( (-) \) and \( \phi(-) \). Note that \( \phi(-) \) erases not just the type dependencies but also the identities of the types. For an atomic type \( A = a \ M_1 \cdots M_n \), we further write \( \langle A \rangle \) to stand for \( a \langle M_1 \rangle \cdots \langle M_n \rangle \).
\[
\begin{align*}
{\{\Pi x : A. P\}} &\iff \lambda m : \phi (\Pi x : A. P). p_1 x : \phi (A). {\{A\}} x \Rightarrow {\{P\}} (m x) \\
\{a \ M_1 \cdots \ M_n\} &\iff \lambda m : \text{lfo} \cdot \text{hastype} \ m \ (a \ (M_1) \cdots (M_n)) \\
\{\text{type}\} &\iff \lambda m : \text{lfo} \cdot \text{istype} \ m
\end{align*}
\]

Figure 3 Encoding of LF types and kinds using the hastype and istype predicates.

The second pass uses two new predicates, hastype : lfo \rightarrow lfo \rightarrow o and istype : lfo \rightarrow o, to encode the type and kind judgements of LF. Whenever \( M : A \) in LF from a given signature, it must be the case that \( \{\{A\}\}(M) \) is derivable in \( \text{HOHH} \) from the clauses for hastype and istype produced from encoding the signature. Likewise, when \( A : K \), it should be the case that \( \{\{K\}\}(A) \) is derivable. The rules determining this encoding are shown in figure 3.

\begin{itemize}
\item [\textbf{Theorem 1 (Adequacy, [18]).}] The LF hypothetical judgement \( x_1 : P_1, \ldots, x_n : P_n \vdash M : A \) is derivable in the LF type theory \[?] from an LF signature \( \Sigma \) if and only if the \( \text{HOHH} \) formula \( \{\{P_1\}\} x_1 \Rightarrow \cdots \Rightarrow \{\{P_n\}\} x_n \Rightarrow \{\{A\}\}(M) \) is derivable from the \( \text{HOHH} \) encoding of \( \Sigma \) according to the rules in figures 2 and 3.
\end{itemize}

Because this encoding is adequate, it is possible to define a right-inverse that maps a \( \text{HOHH} \) formula in the image of the translation in figure 3 back to an LF judgement. This inverse will be very useful in the next section where we will use the encoding of LF to extend the 2LL via translations. The user of the system will not need to be aware of the details of the encoding as the \( \text{HOHH} \) formulas will be inverted into their corresponding LF judgements.

Defining such an inverse requires a small amount of care. We obviously cannot invert every \( \text{HOHH} \) formula, just those that correspond to a given signature. However, even for formulas constructed using the encodings of an LF signature, we may not necessarily be able to invert them; for instance, the formula may be the translation of a malformed or ill-typed LF judgement. This inverse will also not necessarily recover exactly the LF judgement used to construct the \( \text{HOHH} \) formula in the first place; rather, the inversion will only produce a unique inverse (if one exists) up to \( \beta\eta \)-conversion.

The general structure of the inversion operation is defined in terms of the following four sequent forms:

\[
\begin{align*}
\Gamma &\vdash \text{hastype} \ m \ a \rightarrow M : A & \text{inverting typing; } M, A \ output \\
\Gamma &\vdash \text{istype} \ a \rightarrow A : \text{type} & \text{inverting kinding; } A \ output \\
\Gamma &\vdash m : A \rightsquigarrow M & \text{inverting canonical terms; } M \ output \\
\Gamma &\vdash m \rightsquigarrow M : A & \text{inverting atomic terms; } M, A \ output
\end{align*}
\]

In each case, \( \Gamma \) contains the type and kind information for the signature constants and the typing assumptions for the bound variables in the input terms. \( A \) and \( B \) range over LF types, \( M \) and \( N \) over LF terms, \( F \) and \( G \) over \( \text{HOHH} \) formulas, and \( a, m \) and \( n \) over simply typed \( \lambda \)-terms produced by \( \langle \rangle \). The rules are shown in figure 4. The latter two rules for inverting simply typed \( \lambda \)-terms to LF terms are standard from bidirectional type-checking, and was already been developed in [19] (in a slightly more general form). The former two rules for inverting judgements are novel.

\begin{itemize}
\item [\textbf{Theorem 2 (Right inverse).}] If \( \{\{P\}\}(U) = F \) under the translation of \( \Gamma \) and \( \Gamma \vdash F \longrightarrow U' : P \), then \( \Gamma \vdash U : \text{\(\beta\eta\)} U' : P \) in LF.
\end{itemize}

\textbf{Proof.} Straightforward structural induction. Note the requirement for \( \eta \)-contraction of the term to a variable in the second premise of inv-nest is necessary, for otherwise the rule would produce an unsound abstraction. If the formula \( F \) was generated from the translation of figures 2 and 3, then this \( \eta \)-contraction check will always succeed.  

A Two-Level Logic Approach to Reasoning about Typed Specification Languages

In addition, we add the following clauses to redexes in the clauses, reason on

\[ \phi_i : \text{lfobj} \rightarrow \text{lfobj} \]

ofU : \text{lfobj}.

\[ \text{lfhas} (\text{abs } Z1 Z2) \rightarrow \text{lfhas } Z1 \text{ ty}, \text{lfhas } Z2 \text{ ty}. \]

\[ \text{lfhas} \text{ tm}. \]

\[ \text{lfhas } (\text{arr } Z1 Z2) \rightarrow \text{lfhas } Z1 \text{ ty}, \text{lfhas } Z2 \text{ ty}. \]

\[ \text{lfhas} \text{ u } \text{ tm}. \]

\[ \text{lfhas} (\text{app } Z1 Z2) \rightarrow \text{lfhas } Z1 \text{ tm}, \text{lfhas } Z2 \text{ tm}. \]

\[ \text{lfhas} (\text{abs } Z1 Z2) \rightarrow \text{lfhas } Z1 \text{ ty}, (\text{pi } x) \text{ lfhas } x \text{ tm } \Rightarrow \text{lfhas } (Z2 x) \text{ tm}). \]
The variables named $Z_i$ are generated by the translator for those variables that are omitted from the input signature by the use of $\rightarrow$ instead of $\Pi$.

It is instructive to compare these clauses to those for the pure HOHH version in section 2.3. Although, on the surface, these two look quite different, there are similarities in the kinds of subgoals that are produced for the three constructors of $\text{of}$. For example, consider the case of $\text{ofApp}$. Two of the formulas, $\text{hastype } Z_1 (\text{of } M (\text{arr } A B))$ and $\text{hastype } Z_2 (\text{of } N A)$ are already present in nearly this form in the HOHH specification. The additional assumptions are just repetitions of the typing assumptions for the arguments to $\text{ofApp}$; indeed, many of them are redundant since the $\text{ofApp}$ term is already assumed to be type-correct. This kind of redundancy analysis can be used to further improve the translation, making it nearly identical to the simply typed one [18, 19].

4.2 Representing LF Hypothetical Judgements

We use the concrete syntax $\langle M : A \rangle$ or $\langle A : K \rangle$ to depict $\{\{A\}\} M$ or $\{\{K\}\} A$, respectively. In fact, since the LF type system is given in terms of hypothetical derivations, we generalize this syntax to the form: $\langle x_1 : P_1, \ldots, x_n : P_n \vdash U : P \rangle$ as an abbreviation for: $\text{seq}(\langle x_1 : P_1 \rangle :: \cdots :: \langle x_n : P_n \rangle) (\langle U : P \rangle)$. As an example, the uniqueness theorem for the $\text{of}$ relation is (eliding types):

$$\forall G, M, A, B, P_1, P_2, \text{ctx } G \supset (G \vdash P_1 : \text{of } M A) \supset (G \vdash P_2 : \text{of } M B) \supset A = B. \quad (2)$$

or, in the equivalent concrete syntax,

$$\forall G, M, A, B, P_1, P_2, \text{ctx } G \rightarrow (G \vdash P_1 : \text{of } M A) \rightarrow (G \vdash P_2 : \text{of } M B) \rightarrow A = B.$$ 

Here, $P_1$ and $P_2$ are (encodings of) the LF proof-terms for the judgements of $M A$ and of $M B$ respectively; these proof terms are built out of the constructors for the $\text{of}$ relation, viz. $\text{ofU}$, $\text{ofApp}$ and $\text{ofAbs}$.

Of course, in order to prove this theorem we would require a suitable $\text{ctx}$ definition. Unlike in the simply typed case, the recursive case for $\lambda$-abstractions not only introduces a new variable but also a proof that it has a given LF type at the same time. This gives us the following definitional clauses.

$$\text{ctx nil } \triangleq \text{true}.$$ 

$$\forall x : \text{lfobj}. \forall p : \text{lfobj}. \text{ctx } ((x : \text{tm}) :: (p : \text{of } x A) :: G) \triangleq \text{ctx } G.$$ 

It is interesting to note that, because variables are introduced (bound) in a different place than their typing assumptions, it would be just as valid to use the following clause instead for the second clause above:

$$\forall x : \text{lfobj}. \forall p : \text{lfobj}. \text{ctx } ((p : \text{of } x A) :: (x : \text{tm}) :: G) \triangleq \text{ctx } G.$$ 

\footnote{The full Abella/LF development is found in appendix A, which may also be interactively browsed online at \url{http://abella-prover.org/lf}.}
This reordering of the context that is not strictly allowed in the \( \text{LF} \) type system poses no problems for us. Indeed, when we reason about the elements of the context, we can always recover these two assumptions that are always simultaneously added to the context.

\[
\begin{align*}
\text{forall } G, A, \ nabla \ p \ x, \\
\text{ctx } (G x p) & \rightarrow \text{member } (x : \text{tm}) (G x p) \\
\exists A, \text{member } (p : \text{of } x A) (G x p) & \land \text{fresh } p A \land \text{fresh } x A.
\end{align*}
\]

The dependency of \( G \) on \( x \) and \( p \) is indicated explicitly using application. For \( A \), this dependency is implicit, because the \( \exists \) occurs in the scope of the corresponding \( \nabla s \), so we use the predicate \( \text{fresh} : \text{lfobj} \rightarrow \text{lfobj} \rightarrow \text{prop} \) to further assert that its first arguments are nominal constants that do not occur in its second arguments. This is definable simply as:

\[
\forall A. (\nabla x. \text{fresh } x A) \triangleq \text{true}.
\]

The proof of (2) proceeds by induction on the second assumption, \( \langle G \vdash P_1 : \text{of } M A \rangle \), using the clauses added to \( \text{prog} \) when importing the specification. There are exactly three backchaining possibilities for \( \text{prog} \) clauses, corresponding to the \( \text{ofU} \), \( \text{ofApp} \), and \( \text{ofAbs} \) cases, respectively. Finally, when backchaining on the dynamic clauses in \( G \), we use the \( \text{ctx} \) definition to characterize the shape of the selected clause: if the selected clause is \( (x : \text{tm}) \), then the branch immediately succeeds since \( (x : \text{tm}) \) will not unify with \( (P_1 : \text{of } M A) \). Thus, the only backchaining case worth considering is when the selected dynamic clause is of the form \( (p : \text{of } x A') \). In this case, we continue by case-analysis of the second derivation, \( \langle P_2 : \text{of } M B \rangle \), in which case again the only possibility that is not immediately ruled out by unification is the case of \( (p' : \text{of } x B') \) being selected from \( G \). In this case, we appeal to a uniqueness lemma [1] of the following form:

\[
\forall G, X, A, B, P_1, P_2, \text{ctx } G \supset \text{mem } (P : \text{of } X A) G \supset \text{mem } (P_2 : \text{of } X B) G \supset A = B.
\]

The rest of the proof is fairly systematic, and largely identical in structure to that of the \( \text{HOHH} \) case. It is also worth remarking that once we have shown that the types \( A \) and \( B \) are identical in (2), we can then also show that the proof terms \( P_1 \) and \( P_2 \) must also be equal (up to \( \alpha \beta \eta \), of course).

\[
\begin{align*}
\text{forall } G, M \ A \ B \ P_1 \ P_2, \text{ctx } G & \rightarrow \\
(G \vdash P_1 : \text{of } M A) & \rightarrow (G \vdash P_2 : \text{of } M B) \rightarrow P_1 = P_2.
\end{align*}
\]

This is expected from the \( \text{LF} \) type theory, but would be difficult to state in \( \text{LF} \) itself because of the lack of equality as a built-in relation.

### 4.3 The Implementation

The implementation of the translational \textit{2LL} can be found in the \textit{lf} branch of the \textit{Abella} repository.\footnote{Details for downloading and building this branch can be found in \url{http://abella-prover.org/lf}.} This implementation also comes with a few examples of reasoning on \( \text{LF} \) specifications that can be browsed online without needing to run \textit{Abella}. We have made the following observations about these developments:

- The user of the system never needs to look at the encoding of \( \text{LF} \) in \( \text{HOHH} \) directly.
- The system always translates \( \text{LF} \) judgements, written using \( \langle \cdot \rangle \), transparently to \( \text{HOHH} \), and also inverts any \( \text{HOHH} \) formulas in the image of the translation back into an \( \text{LF} \) (hypothetical) judgement. Hence, the only “domain knowledge” the user needs to use the system is the tactics-based proof language of \textit{Abella} itself.
Our implementation currently does not perform type-checking on the \( LF \) judgements written by the user, either in the specification itself or as part of reasoning. This is not as such a problem, since we can never prove anything false about well-typed judgements. However, without type checking we have no way to verify that the theorem which has been proved is really meaningful since we are allowed to reason about ill-formed \( LF \) judgements. It would also be useful for users to have a type-checker as a sanity check. For the time being, we run the input specification through the Twelf system [15], both to type-check it and to get an explicit form of the specification.

5 Related Work and Conclusion

We have proposed here a translational extension to the two-level logic approach for reasoning about specifications. By adding a translation layer to the Abella theorem prover we have been able to reason over dependently typed \( LF \) specifications without needing to change the reasoning logic, and allowing \( LF \) to co-exist with the HOHH specification logic. We are already in the process of extending this implementation to arbitrary pure type systems instead of just \( LF \); in particular, extending the type system with polymorphism, which is the most common feature request for Abella, should nevertheless be encodable via our translation that reifies specification types as reasoning terms.

The translation of \( LF \) to HOHH used in this work is a minor variant of the simple translation from [18], which is itself based on earlier work [3], while the inversion on terms is similar to the definition in [19], omitting meta-variables. Various optimized versions of this translation have been used to use \( \lambda Prolog \) as an engine for logic programming with \( LF \) specifications; in particular, the Parinati system [18] and its extension to meta-variables in [19]. The meta-theory of the optimized translation is not as immediate as for the simple translation, but it would be interesting to investigate its use for the Abella/LF variant in the future. The combination of Parinati and Abella/LF gives us both an efficient execution model for dependently typed logic programs and a mechanism to reason about the meta-theory of such specifications in the extended 2LL. In effect, \( LF \) becomes as much a first class citizen of the Abella ecosystem as HOHH and \( \lambda Prolog \) have traditionally been.

There are many other systems designed to reason with and about \( LF \) specifications. The most mature implementation is Twelf [15], which has a very efficient type-checker incorporating sophisticated term and type reconstruction. As mentioned in section 4.3, we use Twelf to type-check and elaborate the \( LF \) specifications we import in Abella. In addition to the type-checker, Twelf has a suite of meta-theoretic tools that can verify certain properties of \( LF \) specifications, such as that a declared relation determines a total function. Twelf is, however, not powerful enough to reason inductively on arbitrary \( LF \) derivations. For example, although Twelf can check coverage, it cannot express the logical formula that corresponds to the coverage property.

Some of these expressive deficiencies of Twelf have been addressed in the Delphin [17] and Beluga [16] systems that add a functional programming language that can manipulate and reason inductively on \( LF \) syntax. The Beluga system, in particular, extends the \( LF \) type theory with contextual modal types [13] that give a type-theoretic treatment for meta-variables and explicit substitutions; in more recent work, Beluga also allows abstraction over contexts and substitutions [2]. The type-checker of Beluga is therefore very sophisticated and performs many kinds of reasoning on contexts automatically that must be done manually in Abella. On the flip-side, Abella has a small trusted core based on the logic \( G \) with a well-understood and—importantly!—stable proof system [11, 5]. It would be interesting to formally compare
the representational abilities of Abella/LF and Beluga. Moreover, Abella has recently acquired a Plugin architecture that allows arbitrary (but soundness-preserving) user-written extensions to its automation capabilities [1], which might help us add more automation in the future.

Acknowledgements

Thanks to Dale Miller and Gopalan Nadathur for many discussions about all aspects of this work, and to Gopalan especially for many useful comments on earlier drafts. This work has been partially supported by the NSF Grant CCF-0917140 and by the ERC Advanced Grant ProofCert. Opinions, findings, and conclusions or recommendations expressed in this paper are those of the authors and do not necessarily reflect the views of the National Science Foundation.

References


A Two-Level Logic Approach to Reasoning about Typed Specification Languages

A Type-Uniqueness for an LF Specification in Abella/LF

We give here the complete formalization of type-uniqueness for the LF specification file below, unique.elf, which was type-checked by Twelf version 1.7.1.

\[
\begin{align*}
\text{ty} & : \text{type}. \\
i & : \text{ty}. \\
\text{arr} & : \text{ty} \rightarrow \text{ty} \rightarrow \text{ty}. \\
\text{tm} & : \text{type}. \\
u & : \text{tm}. \\
\text{abs} & : \text{ty} \rightarrow (\text{tm} \rightarrow \text{tm}) \rightarrow \text{tm}. \\
\text{app} & : \text{tm} \rightarrow \text{tm} \rightarrow \text{tm}. \\
of & : \text{tm} \rightarrow \text{ty} \rightarrow \text{type}. \\
ofU & : \text{of} \ u \ i. \\
ofApp & : \{A:\text{ty}\} \{B:\text{ty}\} \{M:\text{tm}\} \{N:\text{tm}\} \\
& \text{of} \ M \ (\text{arr} \ A \ B) \rightarrow \text{of} \ N \ A \rightarrow \\
& \text{of} \ (\text{app} \ M \ N) \ B. \\
ofAbs & : \{A:\text{ty}\} \{B:\text{ty}\} \{R:\text{tm} \rightarrow \text{tm}\} \\
& \{x:\text{tm}\} \text{of} \ x \ A \rightarrow \text{of} \ (R \ x) \ B \rightarrow \\
& \text{of} \ (\text{abs} \ A \ ((x:\text{tm}) \ R \ x)) \ (\text{arr} \ A \ B).
\end{align*}
\]

The generated simply typed signature and type-checking clauses are already displayed in section 4.1. Below is the reasoning file, unique.thm, that proves type and proof uniqueness for typing in Abella/LF.

%%% Import unique.elf (i.e., perform the translation)
Specification "unique.elf".

Define \(\text{ctx} : \text{olist} \rightarrow \text{prop}\) by
\[
\text{ctx} \ nill = \text{ctx} \ (\langle \text{p} : \text{of} \ x \ A \rangle :: \langle x : \text{tm} \rangle :: G) = \text{ctx} \ G.
\]

%%% The next three theorems are standard in Abella
%%% developments for HOAS representations.
Theorem member_prune : forall \(G \ E\), \(\text{nabla} \ (n: \text{lfobj})\),
member \(E \ n\) \(G\) \rightarrow \exists \(X\), \(E = \langle X : \text{tm} \rangle \land \text{name} \ X\).
induction on \(1\). intros. case \(H1\).
search.
apply \(\text{IH}\) to \(H2\). search.

Define fresh : \(\text{lfobj} \rightarrow \text{lfobj} \rightarrow \text{prop}\) by
\(\text{nabla} \ x, \text{fresh} \ x \ A\).

Define name : \(\text{lfobj} \rightarrow \text{prop}\) by
\(\text{nabla} \ x, \text{name} \ x\).

%%% How to reason about an arbitrary element of \(G\)
Theorem ctx_mem : forall \(G \ E\),
\(\text{ctx} \ G \rightarrow \text{member} \ E \ G\) \rightarrow \\
\((\exists X, E = \langle X : \text{tm} \rangle \land \text{name} X) \lor \\
(\exists P \ X \ A, E = \langle P : \text{of} \ X \ A \rangle \land \text{fresh} \ X \ A \land \text{fresh} \ P \ A)\).
induction on \(1\). intros. case \(H1\).
case \(H2\).
case \(H3\). search.
case \(H4\). search.
apply \(\text{IH}\) to \(H5\). case \(H6\).
search. search.

%%% The same variable cannot have two different declarations in \(G\)
Theorem ctx_unique : forall \(G \ P \ Q \ X \ A \ B\),
\(\text{ctx} \ G \rightarrow \text{member} \ (P : \text{of} \ X \ A) \ G \rightarrow \text{member} \ (Q : \text{of} \ X \ B) \ G \rightarrow \\
(\text{of} \ P \ A \rightarrow \text{of} \ Q \ B)\)
\[ A = B \land P = Q. \]

**induction on 1. intros. case H1.**

- case H2.
- case H2.
- case H3.
  - search.
    - case H5. apply member_prune to H6.
    - case H3.
      - case H5. apply member_prune to H6.
      - case H5. case H6. apply IH to H4 H7 H8. search.

\%\% Type-uniqueness

**Theorem** unique_ty : \(\forall G M A B P1 P2,\)
\(< G \vdash P1 : of M A > \to < G \vdash P2 : of M B > \to A = B.\)

**induction on 2. intros. case H2.**

- case H3. search.
  - apply ctx_mem to H1 H5. case H6.
  - case H4.
  - case H7. case H4.
  - case H3.
  - apply IH to H1 H8 H14. search.
    - apply ctx_mem to H1 H11. case H12.
      - case H10.
  - case H3.
    - apply IH to _ H7 H11. search.
      - apply ctx_mem to H1 H9. case H10.
      - case H8.
      - case H11. case H8.
      - apply ctx_mem to H1 H5. case H6.
      - case H4.
      - case H3.
        - case H7. case H4.
        - case H7. case H4.
        - apply ctx_mem to H1 H10. case H11.
          - case H9.
          - case H4. case H9.
            - apply ctx_unique to H1 H5 H10. search.

\%\% Proof-uniqueness

**Theorem** unique_proof : \(\forall G M A B P1 P2,\)
\(< G \vdash P1 : of M A > \to < G \vdash P2 : of M B > \to P1 = P2.\)

**induction on 2. intros. case H2.**

- case H3. search.
  - apply ctx_mem to H1 H5. case H6.
  - case H4. case H7. case H4.
  - case H3.
    - apply IH to H1 H8 H14.
      - apply IH to H1 H9 H15.
        - apply unique_ty to H1 H8 H14. search.
      - apply ctx_mem to H1 H11. case H12.
        - case H10.
  - case H3.
    - apply IH to _ H7 H11.
      - apply unique_ty to _ H7 H11.
        - search.
      - apply ctx_mem to H1 H9. case H10.
        - case H8.
        - case H11. case H8.
    - apply ctx_mem to H1 H5. case H6.
      - case H4.
      - case H3.
case H7. case H4.
case H7. case H4.
case H7. case H4.
apply ctx_mem to H1 H10. case H11.
case H9.
case H4. case H9.
apply ctx_unique to H1 H5 H10. search.