Translating HOL to Dedukti

Ali Assaf, Guillaume Burel

Translating HOL to Dedukti

Ali Assaf
Inria, Paris, France
École Polytechnique, Palaiseau, France

Guillaume Burel
ENSIIE/Cédric, Évry, France

Dedukti is a logical framework based on the $\lambda\Pi$-calculus modulo rewriting, which extends the $\lambda\Pi$-calculus with rewrite rules. In this paper, we show how to translate the proofs of a family of HOL proof assistants to Dedukti. The translation preserves binding, typing, and reduction. We implemented this translation in an automated tool and used it to successfully translate the OpenTheory standard library.

1 Introduction

Dedukti is a logical framework for defining logics and expressing proofs in those logics [8]. Following the LF legacy [17], it is based on the $\lambda\Pi$-*calculus modulo rewriting*, which extends the $\lambda\Pi$-*calculus* with rewrite rules. Cousineau and Dowek [11] showed that functional *pure type systems* (PTS), a large class of calculi that are at the basis of many proof systems, can be embedded in the $\lambda\Pi$-calculus modulo rewriting in a way that is complete and that preserves reductions (i.e. program evaluation). This led to propose Dedukti as a universal proof framework.

In this paper, we focus on translating the proofs of HOL to Dedukti. HOL refers to a family of theorem provers built on a common logical system known as *higher-order logic* or *simple type theory* [10]. It includes systems such as HOL Light, HOL4, and ProofPower-HOL. These systems are fairly popular and a large number of important mathematical results have been formalized in them [15, 16, 29].

Universal proof checking

Using Dedukti as a logical framework serves two goals. First, in the short term, it serves as an alternative, independent proof checker, providing an additional layer of confidence over each system. The second, longer term goal, is interoperability. Proof systems are becoming increasingly important, both in the formalization of mathematics and in software engineering. However, they are usually developed separately, with very little interoperability in mind. As a result, it is currently very difficult to reuse a proof from one system in another one. Embedding these different systems in a single unified framework is the first step to bring them closer together, and opens the way for theory management systems [18, 27] to combine their proofs in order to construct and verify larger theories.

The $\lambda\Pi$-calculus as a logical framework

The $\lambda\Pi$-calculus, also known as LF, is a typed λ-calculus with dependent types. Through the *Curry–Howard correspondence*, it can express a wide variety of logics [17]. Several formalizations of HOL in LF have been proposed [2, 28, 26].

To appear in EPTCS.

The main concept behind this correspondence is the "*propositions as types*" principle. Typically, we define a context declaring the types, terms, and judgments of the original logic, in such a way that provability in the logic corresponds to type inhabitation in the context. For HOL, the signature would be:

$$\begin{array}{lcl}
\mathsf{type} & : & \mathsf{Type} \\
\mathsf{bool} & : & \mathsf{type} \\
\mathsf{arrow} & : & \mathsf{type} \to \mathsf{type} \to \mathsf{type} \\
\mathsf{term} & : & \mathsf{type} \to \mathsf{Type} \\
\mathsf{lam} & : & (\mathsf{term}\,\alpha \to \mathsf{term}\,\beta) \to \mathsf{term}\,(\mathsf{arrow}\,\alpha\,\beta) \\
\mathsf{app} & : & \mathsf{term}\,(\mathsf{arrow}\,\alpha\,\beta) \to \mathsf{term}\,\alpha \to \mathsf{term}\,\beta \\
\mathsf{proof} & : & \mathsf{term}\,\mathsf{bool} \\
\mathsf{rule_1} & : & \ldots \\
\mathsf{rule_2} & : & \ldots
\end{array}$$

For each proposition ϕ of the logic, we assign a type $\|\phi\|$ in the $\lambda\Pi$-calculus. The provability of the proposition ϕ corresponds to the inhabitation of the type $\|\phi\|$. Similarly, we translate proofs as terms inhabiting those types, and the correctness of the proof corresponds to the well-typedness of the term.

However, because the $\lambda\Pi$-calculus does not have polymorphism, we cannot translate propositions directly as types, as doing so would prevent us from quantifying over propositions for example. Instead, for each proposition ϕ, we have two translations: one translation $|\phi|$ *as a term*, and another $\|\phi\| = \mathsf{proof}\,|\phi|$ *as a type*. This correspondence has been successfully used to embed logics in the LF framework [17, 14], implemented in Twelf [25].

The $\lambda\Pi$-calculus vs. the $\lambda\Pi$-calculus modulo rewriting

An important limitation of LF is that these encodings do not preserve reduction (i.e. program evaluation), and therefore it does not preserve equivalence: if $M \equiv_\beta M'$ then $|M| \not\equiv_\beta |M'|$. For example, the term $(\lambda x : \alpha.x)\,x$ is encoded as $\mathsf{app}\,(\mathsf{lam}\,(\lambda x : \mathsf{term}\,\alpha.x))\,x$ which is not equivalent to x. This is problematic not only because it makes the representation larger and hence less efficient but also because conversion proofs may be very long.

By extending the $\lambda\Pi$-calculus with rewrite rules such as

$$\mathsf{term}\,(\mathsf{arrow}\,\alpha\,\beta) \hookrightarrow \mathsf{term}\,\alpha \to \mathsf{term}\,\beta\ ,$$

we can identify the type $\mathsf{term}\,(\mathsf{arrow}\,\alpha\,\beta)$ with the type $\mathsf{term}\,\alpha \to \mathsf{term}\,\beta$ and thus define a translation that is lighter and that preserves reductions. The encoding of the terms becomes more compact, as we represent λ-abstractions by λ-abstractions, applications by applications, etc. For example, the term $(\lambda x : \alpha.x)\,x$ is encoded as $(\lambda x : \mathsf{term}\,\alpha.x)\,x$. Such an encoding is impossible in LF for higher-order theories such as system F, HOL, or the calculus of constructions.

Moreover, our translation is modular enough so that we can extend the notion of reduction to the proofs of HOL and recover the pure type system nature of HOL [5]. This might be beneficial for several reasons:

1. It gives a reduction semantics for the proofs of HOL.
2. It allows compressing the proofs further by replacing conversion proofs with reflexivity.
3. Several other proof systems (Coq, Agda, etc.) are based on pure type systems, so expressing HOL as a PTS fits in the large scale of interoperability.

HOL and OpenTheory

The theorem provers of the HOL family (HOL Light, HOL4, ProofPower-HOL, etc.) are built on a common logical formalism known as *higher-order logic*, and have fairly similar core implementations.

A recurrent issue when trying to retrieve proofs from these systems is that they do not keep a trace of their proofs [18, 20, 24]. Following the LCF architecture, they represent their theorems using an abstract datatype and thus guarantee their safety without the need to remember their proofs. This approach reduces memory consumption but hinders their ability to share proofs.

Fortunately, several proposals have already been made to solve this problem [18, 24]. Among them is the OpenTheory project. It defines a standard format called the *article format* for recording and sharing HOL theorems. An article file contains a sequence of elementary commands to reconstruct proofs. Importing a theorem requires only a mechanical execution of the commands.

The format is limited to the HOL family, and cannot be used to communicate the proofs of Coq for example. However, it is an excellent starting point for our translation. Choosing OpenTheory as a front-end has several advantages:

- We cover all the systems of the HOL family that can export their proofs to OpenTheory with a single implementation. As of today, this includes HOL Light, HOL4, and ProofPower-HOL.[1]
- The implementation of a theorem prover can change, so the existence of this standard, documented proof format is extremely helpful, if not necessary.
- The OpenTheory project also defines a large common standard theory library, covering the development of common datatypes and mathematical theories such as lists and natural numbers. This substantial body of theories was used as a benchmark for our implementation.

Related work

Several formalizations of HOL in LF have been proposed [2, 26, 28]. To our knowledge, they lack an actual implementation of the translation. Other translations have been proposed to automatically extract the proofs of HOL to other systems such as Isabelle/HOL [19, 24], Nuprl [23], or Coq [20]. With the exception of the implementation of Kalyszyk and Krauss [19], these tools suffer from scalability problems. Our translation is lightweight enough to be scalable and provides promising results. The implementation of Kalyszyk and Krauss is the first efficient and scalable translation of HOL Light proofs, but its target is Isabelle/HOL, a system that, unlike Dedukti, is foundationally very close to HOL Light.

ProofCert [9] is another project like Dedukti that aims at providing a universal framework for checking proofs. Unlike Dedukti, it is based on sequent calculus. It can handle linear, intuitionistic, and classical logics. To our knowledge, there are no automated translations of systems like HOL to ProofCert that have been implemented yet.

A project complementary to ours is Coqine [7], which proposes a translation of the *calculus of inductive constructions* (CIC), the formalism behind Coq, to Dedukti. The translation has been implemented in an automated tool that translates the proofs compiled by Coq to Dedukti. It can handle most of the features of Coq, and has been used to translate a part of its standard library.

[1] Isabelle/HOL can currently read from but not write to OpenTheory.

Contributions

We define a translation of the types, terms and proofs of HOL to Dedukti. We use the rewriting techniques of Cousineau and Dowek [11] to obtain a shallow embedding that is lightweight and modular. We implemented this translation in an automated tool called Holide, which automatically translates the proofs of HOL written in the OpenTheory format to Dedukti. We used it to successfully translate the OpenTheory standard library.

Outline

The rest of this paper is organized as follows. Section 2 presents Dedukti and the $\lambda\Pi$-calculus modulo rewriting. Section 3 presents HOL and the logical system behind it. Section 4 defines the translation of HOL to Dedukti. In Section 5, we show that the translation is correct. Section 6 discusses the details of our implementation and the results obtained by translating the OpenTheory standard library. Section 7 discusses some additional applications of rewriting. Finally, Section 8 summarizes and considers future work.

2 Dedukti

Dedukti is essentially a type checker for the $\lambda\Pi$-calculus modulo rewriting [8], which extends the $\lambda\Pi$-calculus with rewrite rules. We choose a presentation based on pure type systems [5], which makes no syntactic distinction between terms, usually denoted by M or N, and types, usually denoted by A or B.

We assume countably infinite sets of variables and constants. There are two sorts, Type and Kind. The sort Type is the type of types and the sort Kind is the type of Type. We write $\lambda x : A.M$ for abstractions and MN for applications. The type of functions is written $\Pi x : A.B$, or $A \to B$ when x does not appear free in B. Application is left-associative while the arrow $\to$ is right-associative. Terms are considered up to α-equivalence. Contexts contain the types of variables while signatures contain the types of constants and their rewrite rules. Each rewrite rule is accompanied by a context Γ to ensure it is well-typed.

Definition 2.1. The syntax of the $\lambda\Pi$-calculus modulo rewriting is:

variables	x, y		
constants	c		
sorts	s	$::=$	$\mathsf{Type} \mid \mathsf{Kind}$
terms	M, N, A, B	$::=$	$x \mid c \mid s \mid \Pi x : A.B \mid \lambda x : A.M \mid MN$
contexts	Γ, Δ	$::=$	$\cdot \mid \Gamma, x : A$
signatures	Σ	$::=$	$\cdot \mid \Sigma, c : A \mid \Sigma, [\Gamma]\ M \rightsquigarrow N$

If R is a set of rewrite rules, we write $\longrightarrow_R$ for the induced reduction relation, $\longrightarrow_R^+$ for its transitive closure, $\longrightarrow_R^*$ for its reflexive transitive closure, and $\equiv_R$ for its reflexive symmetric transitive closure. Given a signature Σ, we write $\beta\Sigma$ for the union of the β rule with the rewrite rules of Σ.

The typing judgments $\Sigma \mid \Gamma \vdash M : A$ are accompanied by context formation judgments $\Sigma \mid \Gamma$ *context* and signature formation judgments Σ *signature*. We write $\Gamma \vdash M : A$ and Γ *context* instead of $\Sigma \mid \Gamma \vdash M : A$ and $\Sigma \mid \Gamma$ *context* when the signature is not ambiguous. The rules are presented in Figure 1.

Example 2.2. Let Σ be the signature containing

$$\alpha : \mathsf{Type}, c : \alpha, f : \alpha \to \mathsf{Type}$$

$$\frac{\Gamma \ \mathit{context} \qquad (x:A)\in\Gamma}{\Gamma\vdash x:A}\ \textsc{Var} \qquad \frac{\Gamma \ \mathit{context} \qquad (c:A)\in\Sigma}{\Gamma\vdash c:A}\ \textsc{Const} \qquad \frac{\Gamma \ \mathit{context}}{\Gamma\vdash \mathsf{Type}:\mathsf{Kind}}\ \textsc{Type}$$

$$\frac{\Gamma\vdash A:\mathsf{Type} \qquad \Gamma,x:A\vdash B:s}{\Gamma\vdash \Pi x:A.B:s}\ \textsc{Prod} \qquad \frac{\Gamma\vdash A:\mathsf{Type} \qquad \Gamma,x:A\vdash M:B}{\Gamma\vdash \lambda x:A.M:\Pi x:A.B}\ \textsc{Abs}$$

$$\frac{\Gamma\vdash M:\Pi x:A.B \qquad \Gamma\vdash N:A}{\Gamma\vdash MN:[N/x]B}\ \textsc{App} \qquad \frac{\Gamma\vdash M:A \qquad \Gamma\vdash B:\mathsf{Type} \qquad A\equiv_{\beta\Sigma} B}{\Gamma\vdash M:B}\ \textsc{Conv}$$

$$\frac{\Sigma \ \mathit{signature}}{\cdot \ \mathit{context}}\ \textsc{EmptyCtx} \qquad \frac{\Gamma\vdash A:\mathsf{Type} \qquad x\notin\Gamma}{\Gamma,x:A \ \mathit{context}}\ \textsc{VarCtx}$$

$$\frac{}{\cdot \ \mathit{signature}}\ \textsc{EmptySig} \qquad \frac{\Sigma \mid \cdot\vdash A:s \qquad c\notin\Sigma}{\Sigma,c:A \ \mathit{signature}}\ \textsc{ConstSig}$$

$$\frac{\Sigma \mid \Gamma\vdash M:A \qquad \Sigma \mid \Gamma\vdash N:A}{\Sigma,[\Gamma]\ M\rightsquigarrow N \ \mathit{signature}}\ \textsc{RewriteSig}$$

Figure 1: Typing rules of the $\lambda\Pi$-calculus

and the rewrite rule

$$[\cdot]\ f\,c \rightsquigarrow \Pi y:\alpha.\ f\,y\to f\,y.$$

The term $\lambda x:f\,c.\ x\,c\,x$ is well-typed in Σ and has the type $f\,c\to f\,c$. Notice that this term would not be well-typed without the rewrite rule, even if we replace all occurences of $f\,c$ by $\Pi y:\alpha.\ f\,y\to f\,y$.

Dedukti imposes some additional restrictions on the rewrite rules to keep type-checking decidable. In particular, the left side of a rewrite rule must belong to the higher-order pattern fragment [21, 22] and the free variables of the right side must appear on the left side. Moreover, the reduction relation $\longrightarrow_{\beta\Sigma}$ should be confluent and strongly normalizing. This property is not verified by the system and it is up to the user to ensure that it is indeed the case. We discuss this in Section 5.

3 HOL

There are many different formulations for higher-order logic. The intuitionistic formulation is based on implication and universal quantification as primitive connectives, but the current systems generally use a formulation called Q_0 [1] based on equality as a primitive connective. We take as reference the logical system used by OpenTheory [18], which we will now briefly present.

The terms of the logic are terms of the simply typed λ-calculus, with a base type bool representing the type of propositions and a type ind of individuals. The terms can contain constant symbols such as $(=)$, the symbol for equality, or select, the symbol of choice. The logic supports a restricted form of polymorphism, known as ML-style polymorphism, by allowing type variables, such as α or β, to appear in types. For example, the type of $(=)$ is $\alpha\to\alpha\to\mathsf{bool}$.

$$\frac{}{\vdash M = M}\ \textsc{Refl}\ M \qquad \frac{\Gamma \vdash M = N}{\Gamma \vdash \lambda x : A.M = \lambda x : A.N}\ \textsc{AbsThm}\ x \qquad \frac{\Gamma \vdash F = G \qquad \Delta \vdash M = N}{\Gamma \cup \Delta \vdash FM = GN}\ \textsc{AppThm}$$

$$\frac{}{\vdash (\lambda x : A.M)x = M}\ \textsc{Beta}\ x\ M \qquad \frac{}{\{\phi\} \vdash \phi}\ \textsc{Assume} \qquad \frac{\Gamma \vdash \phi = \psi \qquad \Delta \vdash \phi}{\Gamma \cup \Delta \vdash \psi}\ \textsc{EqMp}$$

$$\frac{\Gamma \vdash \phi \qquad \Delta \vdash \psi}{(\Gamma - \{\psi\}) \cup (\Delta - \{\phi\}) \vdash \phi = \psi}\ \textsc{DeductAntiSym} \qquad \frac{\Gamma \vdash \phi}{\Gamma[\sigma] \vdash \phi[\sigma]}\ \textsc{Subst}\ \sigma$$

Figure 2: Derivation rules of HOL

Types can be parameterized through type operators of the form $p(A_1, \ldots, A_n)$. For example, list is a type operator of arity 1, and list(bool) is the type of lists of booleans. Type variables and type operators are enough to describe all the types of HOL, because bool can be seen as a type operator of arity 0, and the arrow $\to$ as a type operator of arity 2. Hence the type of $(=_\alpha)$ is in fact $\to(\alpha, \to(\alpha, \text{bool}()))$. We still write $A \to B$ instead of $\to(A,B)$ for arrow types, p instead of $p()$ for type operators of arity 0, and $M = N$ instead of $(=)MN$ when it is more convenient.

Definition 3.1. The syntax of HOL is:

type variables	α, β		
type operators	p		
types	A, B	$::=$	$\alpha \mid p(A_1, \ldots, A_n)$
term variables	x, y		
term constants	c		
terms	M, N	$::=$	$x \mid \lambda x : A.M \mid MN \mid c$

The propositions of the logic are the terms of type bool and the predicates are the terms of type $A \to \text{bool}$. We use letters such as ϕ or ψ to denote propositions. The contexts, denoted by Γ or Δ, are sets of propositions, and the judgments of the logic are of the form $\Gamma \vdash \phi$. The derivation rules are presented in Figure 2.

Example 3.2. Here is a derivation of the transitivity of equality: if $\Gamma \vdash x = y$ and $\Delta \vdash y = z$, then $\Gamma \cup \Delta \vdash x = z$.

$$\dfrac{\dfrac{\dfrac{}{\vdash ((=)x) = ((=)x)}\ \textsc{Refl} \qquad \Delta \vdash y = z}{\Delta \vdash (x = y) = (x = z)}\ \textsc{AppThm} \qquad \Gamma \vdash x = y}{\Gamma \cup \Delta \vdash x = z}\ \textsc{EqMp}$$

HOL supports mechanisms for defining new types and constants in a conservative way. We will not consider them here. In addition to the core derivation rules, three axioms are assumed:

- η-equality, which states that $\lambda x : A.\ Mx = M$,
- the axiom of choice, with a predeclared symbol of choice called select,
- the axiom of infinity, which states that the type ind is infinite.

It is important to note that from η-convertibility and the axiom of choice, we can derive the excluded middle [6], making HOL a classical logic.

4 Translation

In this section we show how to translate HOL to Dedukti. We define a signature Σ containing primitive declarations and definitions, and a translation function assigning, to every construct of the logic, a term that is well-typed in the signature Σ.

HOL Types

To translate the simple types of HOL, we declare a new Dedukti type called type and three constructors bool, ind and arrow.

$$\begin{array}{lcl} \mathsf{type} & : & \mathsf{Type} \\ \mathsf{bool} & : & \mathsf{type} \\ \mathsf{ind} & : & \mathsf{type} \\ \mathsf{arrow} & : & \mathsf{type} \to \mathsf{type} \to \mathsf{type} \end{array}$$

One should not confuse type, which is the type of Dedukti terms that represent HOL types, with Type, which is the type of Dedukti types. The translation of a HOL type as a Dedukti term is defined inductively on the structure of the type.

Definition 4.1 (Translation of a HOL type as a Dedukti term)**.** For any HOL type A, we define $|A|$, the translation of A as a term, to be

$$\begin{array}{lcl} |\alpha| & = & \alpha \\ |\mathsf{bool}| & = & \mathsf{bool} \\ |\mathsf{ind}| & = & \mathsf{ind} \\ |A \to B| & = & \mathsf{arrow}\,|A|\,|B| \ . \end{array}$$

More generally, if we have an n-ary HOL type operator p, we declare a constant p of type $\underbrace{\mathsf{type} \to \ldots \to \mathsf{type}}_{n} \to \mathsf{type}$, and we translate an instance $p\,(A_1, \ldots, A_n)$ of this type operator to the term $p\,|A_1| \cdots |A_n|$.

HOL Terms

We declare a new dependent type called term indexed by a type, and we identify the terms of type $\mathsf{term}(\mathsf{arrow}\,A\,B)$ with the functions of type $\mathsf{term}\,A \to \mathsf{term}\,B$ by adding a rewrite rule. We also declare a constant eq for HOL equality and a constant select for the choice operator.

$$\begin{array}{lcl} \mathsf{term} & : & \mathsf{type} \to \mathsf{Type} \\ \mathsf{eq} & : & \Pi\alpha : \mathsf{type}.\ \mathsf{term}\,(\mathsf{arrow}\,\alpha\,(\mathsf{arrow}\,\alpha\,\mathsf{bool})) \\ \mathsf{select} & : & \Pi\alpha : \mathsf{type}.\ \mathsf{term}\,(\mathsf{arrow}\,(\mathsf{arrow}\,\alpha\,\mathsf{bool})\,\alpha) \end{array}$$

$$[\alpha : \mathsf{type}, \beta : \mathsf{type}]\ \mathsf{term}\,(\mathsf{arrow}\,\alpha\,\beta) \rightsquigarrow \mathsf{term}\,\alpha \to \mathsf{term}\,\beta$$

The symbol term can be seen as a decoding function that assigns a Dedukti type to every HOL type. The translation of a term M of type A will then be a term of type $\mathsf{term}\,|A|$.

Definition 4.2 (Translation of a HOL type as a Dedukti type)**.** For any HOL type A, we define

$$\|A\| = \mathsf{term}\,|A|\,.$$

Definition 4.3 (Translation of a HOL term as a Dedukti term)**.** For any HOL term M, we define $|M|$, the translation of M as a term to be

$$\begin{array}{lcl} |x| & = & x \\ |MN| & = & |M|\ |N| \\ |\lambda x : A.M| & = & \lambda x : \|A\| .\ |M| \\ |(=_A)| & = & \mathsf{eq}\,|A| \\ |\mathsf{select}_A| & = & \mathsf{select}\,|A|\ . \end{array}$$

More generally, for every HOL constant c of type A, if $\alpha_1, \ldots, \alpha_n$ are the free type variables that appear in A, we declare a new constant c of type

$$\Pi\alpha_1 : \mathsf{type}. \ldots \Pi\alpha_n : \mathsf{type}. \|A\|$$

and we translate an instance $c_{A_1,\ldots,A_n}$ of this constant by the term $c\,|A_1| \cdots |A_n|$.

Example 4.4. The term $(\lambda x : \alpha.x)x$ is translated to

$$|(\lambda x : \alpha.x)x| \quad = \quad (\lambda x : \mathsf{term}\,\alpha.x)x$$

which is convertible to x.

HOL Proofs

We declare a new type proof, to express the proof judgments of HOL. It is a dependent type, indexed by the proposition ϕ that it is proving.

$$\mathsf{proof} \quad : \quad \mathsf{term}\,\mathsf{bool} \to \mathsf{Type}$$

Definition 4.5 (Translation of HOL propositions as Dedukti types)**.** For any HOL proposition ϕ (i.e. a HOL term of type bool), we define

$$\|\phi\| = \mathsf{proof}\,|\phi|\,.$$

For any HOL context $\Gamma = \phi_1, \ldots, \phi_n$, we define

$$\|\Gamma\| = h_{\phi_1} : \|\phi_1\|, \ldots, h_{\phi_n} : \|\phi_n\|$$

where $h_{\phi_1}, \ldots, h_{\phi_n}$ are fresh variables.

We now take care of the derivation rules of HOL (Figure 2). In the following, we write $\Pi x, y : A.B$ as a shortcut for $\Pi x : A.\Pi y : A.B$.

Equality proofs

We declare Refl, FunExt, and AppThm:

$$\begin{array}{lcl} \mathsf{Refl} & : & \Pi\alpha : \mathsf{type}.\,\Pi x : \mathsf{term}\,\alpha.\ \mathsf{proof}\,(\mathsf{eq}\,\alpha\,x\,x) \\ \mathsf{FunExt} & : & \Pi\alpha,\beta : \mathsf{type}.\,\Pi f, g : \mathsf{term}\,(\mathsf{arrow}\,\alpha\,\beta)\,. \\ & & (\Pi x : \mathsf{term}\,\alpha.\ \mathsf{proof}\,(\mathsf{eq}\,\beta\,(f\,x)\,(g\,x))) \to \mathsf{proof}\,(\mathsf{eq}\,(\mathsf{arrow}\,\alpha\,\beta)\,f\,g) \\ \mathsf{AppThm} & : & \Pi\alpha,\beta : \mathsf{type}.\,\Pi f, g : \mathsf{term}\,(\mathsf{arrow}\,\alpha\,\beta)\,.\,\Pi x, y : \mathsf{term}\,\alpha. \\ & & \mathsf{proof}\,(\mathsf{eq}\,(\mathsf{arrow}\,\alpha\,\beta)\,f\,g) \to \mathsf{proof}\,(\mathsf{eq}\,\alpha\,x\,y) \to \mathsf{proof}\,(\mathsf{eq}\,\beta\,(f\,x)\,(g\,y)) \end{array}$$

The constant FunExt corresponds to *functional extensionality*, which states that if two functions f and g of type $A \to B$ are equal on all values x of type A, then f and g are equal. We can use it to translate both the ABSTHM rule and the η axiom. Finally, since our encoding is shallow, β-equality can be proved by reflexivity.

Definition 4.6. The rules REFL, ABSTHM, APPTHM, and BETA are translated to

$$\left|\frac{}{\vdash M = M}\ \textsc{Refl}\right| = \mathsf{Refl}\,|A|\ |M| \quad \text{(where } A \text{ is the type of } M\text{)}$$

$$\left|\frac{\mathscr{D}}{\Gamma \vdash \lambda x : A.M = \lambda x : A.N}\ \textsc{AbsThm}\right| = \mathsf{FunExt}\,|A|\ |B|\ |\lambda x : A.M|\ |\lambda x : A.N|\ (\lambda x : |A|\,.\,|\mathscr{D}|)$$

$$\left|\frac{\mathscr{D}_1 \qquad \mathscr{D}_2}{\Gamma \cup \Delta \vdash F\,M = G\,N}\ \textsc{AppThm}\right| = \mathsf{AppThm}\,|A|\ |B|\ |F|\ |G|\ |M|\ |N|\ |\mathscr{D}_1|\ |\mathscr{D}_2|$$

$$\left|\frac{}{(\lambda x : A.M)\,x = M}\ \textsc{Beta}\right| = \mathsf{Refl}\,|B|\ |M| \quad \text{(where } B \text{ is the type of } M\text{)}\ .$$

Boolean proofs

We declare the constants PropExt and EqMp:

$$\begin{array}{lcl} \mathsf{PropExt} & : & \Pi p, q : \mathsf{term\,bool}. \\ & & (\mathsf{proof}\,q \to \mathsf{proof}\,p) \to (\mathsf{proof}\,q \to \mathsf{proof}\,p) \to \mathsf{proof}\,(\mathsf{eq\,bool}\,p\,q) \\ \mathsf{EqMp} & : & \Pi p, q : \mathsf{term\,bool}.\ \mathsf{proof}\,(\mathsf{eq\,bool}\,p\,q) \to \mathsf{proof}\,p \to \mathsf{proof}\,q \end{array}$$

The constant PropExt corresponds to *propositional extensionality* and, together with EqMp, states that equality on booleans in HOL behaves like the connective "*if and only if*".

Definition 4.7. The rules ASSUME, DEDUCTANTISYM, and EQMP are translated to

$$\left|\frac{}{\{\phi\} \vdash \phi}\ \textsc{Assume}\right| = h_\phi \quad \text{(where } h_\phi \text{ is a fresh variable)}$$

$$\left|\frac{\mathscr{D}_1 \qquad \mathscr{D}_2}{(\Gamma - \{\psi\}) \cup (\Delta - \{\phi\}) \vdash \phi = \psi}\ \textsc{DeductAntiSym}\right| =$$

$$\mathsf{PropExt}\,|\phi|\ |\psi|\ \left(\lambda h_\psi : \|\psi\|\,.\,|\mathscr{D}_1|\right)\ \left(\lambda h_\phi : \|\phi\|\,.\,|\mathscr{D}_2|\right)$$

$$\left|\frac{\mathscr{D}_1 \qquad \mathscr{D}_2}{\Gamma \cup \Delta \vdash \psi}\ \textsc{EqMp}\right| = \mathsf{EqMp}\,|\phi|\ |\psi|\ |\mathscr{D}_1|\ |\mathscr{D}_2|\ .$$

Substitution proofs

The HOL rule SUBST derives $\Gamma[\sigma] \vdash \phi[\sigma]$ from $\Gamma \vdash \phi$. In OpenTheory, the substitution can substitute for both term and type variables but type variables are instantiated first. For the sake of clarity, we split this rule in two steps: one for term substitution of the form $\sigma = M_1/x_1, \ldots, M_n/x_n$, and one for type substitution of the form $\theta = A_1/\alpha_1, \ldots, A_m/\alpha_m$. In Dedukti, we have to rely on β-reduction to express substitution. We can correctly translate a parallel substitution $M[M_1/x_1, \ldots, M_n/x_n]$ as

$$(\lambda x_1 : B_1. \ldots \lambda x_n : B_n.M)\,M_1 \ldots M_n$$

where B_i is the type of M_i.

Definition 4.8. The rule SUBST is translated to

$$\left|\frac{\mathscr{D}}{\Gamma[\theta]\vdash\phi[\theta]}\ \textsc{TypeSubst}\right| = (\lambda\,\alpha_1 : \mathsf{type}.\ldots\lambda\,\alpha_m : \mathsf{type}.\,|\mathscr{D}|)\,|A_1|\ldots|A_m|$$

$$\left|\frac{\mathscr{D}}{\Gamma[\sigma]\vdash\phi[\sigma]}\ \textsc{TermSubst}\right| = (\lambda x_1 : \|B_1\|.\ldots\lambda x_n : \|B_n\|.\,|\mathscr{D}|)\,|M_1|\ldots|M_n|$$

5 Correctness

The correctness of the translation is expressed by two properties: *completeness* and *soundness*. The first states that all the generated terms have the correct type. For example, the translation of a term of type A has type $\|A\|$ while the translation of a proof of ϕ has type $\|\phi\|$. The second states that if a proof term is well-typed in Dedukti, then the proof is correct in the original logic. These two properties ensure that we can use Dedukti as an independent proof checker: we can use it to re-verify the proofs of OpenTheory, and moreover we can be sure that, if a proof is accepted by Dedukti, then it is also valid in OpenTheory.

Completeness

Let Σ be the signature of HOL containing the declarations and rewrite rules of the previous sections.

Lemma 5.1. *For any HOL type A,*

$$\Sigma \mid \alpha_1 : \mathsf{type},\ldots,\alpha_n : \mathsf{type} \vdash |A| : \mathsf{type}$$

where $\alpha_1,\ldots,\alpha_n$ are the free type variables appearing in A.

Lemma 5.2. *For any HOL term M of type A,*

$$\Sigma \mid \alpha_1 : \mathsf{type},\ldots,\alpha_n : \mathsf{type}, x_1 : \|A_1\|,\ldots x_n : \|A_n\| \vdash |M| : \|A\|$$

where $\alpha_1,\ldots,\alpha_n$ are the free type variables and $x_1 : A_1,\ldots,x_n : A_n$ are the free term variables appearing in M.

Theorem 5.3. *For any HOL proof $\mathscr{D}$ of $\Gamma\vdash\phi$,*

$$\Sigma \mid \alpha_1 : \mathsf{type},\ldots,\alpha_n : \mathsf{type}, x_1 : \|A_1\|,\ldots x_n : \|A_n\|, \|\Gamma\| \vdash |\mathscr{D}| : \|\phi\|$$

where $\alpha_1,\ldots,\alpha_n$ are the free type variables and $x_1 : A_1,\ldots,x_n : A_n$ are the free term variables appearing in $\mathscr{D}$.

Proof. By induction on the structure of $\mathscr{D}$. □

Soundness

Proving the soundness of the embedding is less straightforward than proving completeness. In fact, it is closely related to the confluence and normalization properties of the system. We state the results here and refer the reader to the works of Assaf, Cousineau, and Dowek [3, 11, 12] for the complete proofs.[2]

Lemma 5.4. *The reduction relation $\longrightarrow_{\beta\Sigma}$ is confluent.*

Lemma 5.5. *The reduction relation $\longrightarrow_{\beta\Sigma}$ is strongly normalizing.*

Theorem 5.6. *If $\Sigma \mid \|\Gamma\| \vdash M : \|A\|$ then M corresponds to a valid proof of $\Gamma\vdash A$ in HOL.*

[2] The terms *soundness* and *completeness* are interchanged in Cousineau and Dowek's paper [11].

Package	Size (kB)		Time (s)	
	OpenTheory	Dedukti	Translation	Verification
unit	5	13	0.2	0.0
function	16	53	0.3	0.2
pair	38	121	0.8	0.5
bool	49	154	0.9	0.5
sum	84	296	2.1	1.1
option	93	320	2.2	1.2
relation	161	620	4.6	2.8
list	239	827	5.7	3.2
real	286	945	6.5	3.1
natural	343	1065	6.8	3.2
set	389	1462	10.2	5.8
Total	1702	5877	40.3	21.6

Table 1: Translation of the OpenTheory standard library

6 Implementation

We implemented our translation in an automated tool called Holide. It works as an OpenTheory virtual machine that additionally keeps track of the corresponding proof terms for theorems. The program reads a HOL proof written in the OpenTheory article format (`.art`) and outputs a Dedukti file (`.dk`) containing its translation. We can run Dedukti on the generated file to verify it. All generated files are linked with a hand-written file `hol.dk` containing the signature Σ that we defined in Section 4. Our software is available online at https://www.rocq.inria.fr/deducteam/Holide/.

HOL proofs are known to be very large [19, 20, 24], and we needed to implement sharing of proofs, terms, and types in order to reduce them to a manageable size. OpenTheory already provides some form of proof sharing but we found it easier to completely factorize the derivations into individual steps.

We used Holide to translate the OpenTheory standard library. The library is organized into logical packages, each corresponding to a theory such as lists or natural numbers. We were able to verify all of the generated files. The results are summarized in Table 1. We list the size of both the source files and the files generated by the translation after compression using gzip. The reason we use the size of the compressed files for comparison is because it provides a more reasonable measure that is less affected by syntax formatting and whitespace. We also list the time it takes to translate and verify each package. These tests were done on a 64-bit Intel Xeon(R) CPU @ 2.67GHz × 4 machine with 4 GB of RAM.

Overall, the size of the generated files is about 3 to 4 times larger than the source files. Given that this is an encoding in a logical framework, an increase in the size is to be expected, and we find that this factor is very reasonable. There are no similar translations to compare to except the one of Keller and Werner [20]. The comparison is difficult because they work with a slightly different form of input, but they produce several hundred megabytes of proofs. Similary, an increase in verification time is to be expected compared to verifying OpenTheory directly, but our results are still very reasonable given the nature of the translation. Our time is about 4 times larger than OpenTheory, which takes about 5 seconds to verify the standard library. It is in line with the scalable translation of Kalyszyk and Krauss to Isabelle/HOL, which takes around 30 seconds [19]. In comparison, Keller and Werner's translation takes several hours, although we should note that our work greatly benefited from their experience.

7 Extensions

In this section we show some additional advantages of having a translation which preserves reduction.

Compressing conversion proofs

One of the reasons why HOL proofs are so large is that conversion proofs have to traverse the terms using the congruence rules ABSTHM and APPTHM. Since we now prove β-reduction using reflexivity, large conversion proofs could be reduced to a single reflexivity step, therefore reducing the size of the proofs.[3]

Example 7.1. The following proof of $f(g((\lambda x : A.x)x)) = f(g(x))$,

$$\dfrac{\dfrac{}{\vdash f = f}\,\textsc{Refl}\ f \qquad \dfrac{\dfrac{}{\vdash g = g}\,\textsc{Refl}\ g \qquad \dfrac{}{\vdash (\lambda x : A.x)x = x}\,\textsc{Beta}}{\vdash g((\lambda x : A.x)x) = gx}\,\textsc{AppThm}}{\vdash f(g((\lambda x : A.x)x)) = f(gx)}$$

can be translated simply as $\mathsf{Refl}\, C(f(gx))$, where $A \to B$ is the type of g and $B \to C$ is the type of f.

HOL as a pure type system

It turns out that HOL can be seen as a pure type system called λ_{HOL} with three sorts [5, 13]. This formulation corresponds to intuitionistic higher-order logic. However, this structure is lost in the Q_0 formulation used by the HOL systems. Our shallow embedding can be adapted to recover this structure, and thus obtain a constructive and computational version of HOL.

Instead of equality, we declare implication and universal quantification as primitive connectives, and we define what provability means through rewriting.

$$\begin{array}{lcl} \mathsf{imp} & : & \mathsf{term}\,(\mathsf{arrow}\,\mathsf{bool}\,(\mathsf{arrow}\,\mathsf{bool}\,\mathsf{bool})) \\ \mathsf{forall} & : & \Pi\alpha : \mathsf{type}.\ \mathsf{term}\,(\mathsf{arrow}\,(\mathsf{arrow}\,\alpha\,\mathsf{bool})\,\mathsf{bool}) \end{array}$$

$$\begin{array}{llcl} [p : \mathsf{term}\,\mathsf{bool}, q : \mathsf{term}\,\mathsf{bool}] & \mathsf{proof}\,(\mathsf{imp}\,p\,q) & \rightsquigarrow & \mathsf{proof}\,p \to \mathsf{proof}\,q \\ [\alpha : \mathsf{type}, p : \mathsf{term}\,(\mathsf{arrow}\,\alpha\,\mathsf{bool})] & \mathsf{proof}\,(\mathsf{forall}\,p) & \rightsquigarrow & \Pi x : \mathsf{term}\,\alpha.\ \mathsf{proof}\,(p\,x) \end{array}$$

However, this time we do not even need to declare constants like Refl and AppThm for the derivation rules, because they are derivable. Here is a derivation of the introduction and elimination rules for implication for example:

$$\begin{array}{lcl} \mathsf{imp\_intro} & : & \Pi p, q : \mathsf{term}\,\mathsf{bool}.\ (\mathsf{proof}\,p \to \mathsf{proof}\,q) \to \mathsf{proof}\,(\mathsf{imp}\,p\,q) \\ & = & \lambda p, q : \mathsf{term}\,\mathsf{bool}.\,\lambda h : (\mathsf{proof}\,p \to \mathsf{proof}\,q).\,h \\ \mathsf{imp\_elim} & : & \Pi p, q : \mathsf{term}\,\mathsf{bool}.\ \mathsf{proof}\,(\mathsf{imp}\,p\,q) \to \mathsf{proof}\,p \to \mathsf{proof}\,q \\ & = & \lambda p, q : \mathsf{term}\,\mathsf{bool}.\,\lambda h : \mathsf{proof}\,(\mathsf{imp}\,p\,q).\,\lambda x : \mathsf{proof}\,p.\,hx \end{array}$$

By translating the introduction rules as λ-abstractions, and the elimination rules as applications, we recover the reduction of the proof terms, which corresponds to *cut elimination* in the original proofs.

[3] This also applies to conversions involving constant definitions, which we did not cover here but are also assumed as an axiom in HOL.

As for equality, it is also possible to define it in terms of these connectives. For example, we could use the Leibniz definition of equality, which is the one used by Coq:

$$\begin{array}{lcl} \mathsf{eq} & : & \Pi\alpha : \mathsf{type}.\ \mathsf{term}\,(\mathsf{arrow}\,\alpha\,(\mathsf{arrow}\,\alpha\,\mathsf{bool})) \\ & = & \lambda\alpha : \mathsf{type}.\,\lambda x : \mathsf{term}\,\alpha.\,\lambda y : \mathsf{term}\,\alpha. \\ & & \mathsf{forall}\,(\mathsf{arrow}\,\alpha\,\mathsf{bool})\ (\Pi p : \mathsf{term}\,(\mathsf{arrow}\,\alpha\,\mathsf{bool}).\ \mathsf{imp}\,(p\,x)\ (p\,y)) \end{array}$$

We would still need to assume some axioms to prove all the rules of OpenTheory, namely FunExt and PropExt [20], but at least this definition is closer to that of Coq. Since the λ_{HOL} PTS is a strict subset of the calculus of inductive constructions, we can adapt our translation to inject HOL directly into an embedding of Coq in Dedukti [7], or to combine HOL proofs with Coq proofs in Dedukti [4]. Further research into ways to eliminate these axioms (and thus maintain the constructive aspect) when possible is the subject of ongoing work.

8 Conclusion

We showed how to translate HOL to Dedukti by adapting techniques from Cousineau and Dowek [11] to define an embedding that is sound, complete, and reduction preserving. Using our implementation, we were able to translate the OpenTheory standard library and verify it in Dedukti.

Future work

The translation we have presented can be improved in several ways. The current implementation suffers from a lack of linking: if a package makes use of a type, constant, or theorem defined in another package, we do not have a reference to the original definition. This is due to a limitation of the OpenTheory article format. In OpenTheory, this problem is resolved by adding a theory management layer, which is responsible for composing and linking theories together [18]. It would be beneficial to integrate this layer in our translation so that we can properly link the resulting files together.

While we used several optimizations including term sharing in our implementation, there is still room for reducing the time and memory consumption of the translation and the size of the generated files. The caching techniques of Kaliszyk and Krauss [19] could be used in this regard to handle larger libraries and formalizations.

Finally, we can study how to combine the proofs obtained by this translation with the proofs obtained from the translation of Coq [7]. That will require a careful examination of the compatibility of the two embeddings. First, the types of the two theories must coincide, so that a natural number from HOL is the same as a natural number from Coq for example. Second, we must make sure that the resulting theory is consistent. For instance, we know that every type in HOL is inhabited, which is inconsistent with the existence of empty types in Coq, so we will need to modify the translations to avoid this. A solution is to parameterize each HOL type variable by a witness ensuring that it is non-empty. Our translation can be adapted for this solution without much trouble. Some work has already been done in this direction [4].

Acknowledgments

We thank Gilles Dowek for his support, as well as Mathieu Boespflug and Chantal Keller for their comments and suggestions.

References

[1] Peter B. Andrews (1986): *An introduction to mathematical logic and type theory: to truth through proof*. Academic Press Professional, Inc., San Diego, CA, USA.

[2] Andrew W. Appel (2001): *Foundational Proof-Carrying Code*. In: *LICS*, IEEE Computer Society, Washington, DC, USA, p. 247–256, doi:10.1109/LICS.2001.932501.

[3] Ali Assaf (2015): *Conservativity of embeddings in the lambda-Pi calculus modulo rewriting*. Available at https://hal.archives-ouvertes.fr/hal-01084165. To appear in TLCA 2015.

[4] Ali Assaf & Raphaël Cauderlier (2015): *Mixing HOL and Coq in Dedukti (Rough Diamond)*. Available at https://hal.inria.fr/hal-01141789. To appear in PxTP 2015.

[5] H. P. Barendregt (1992): *Lambda Calculi with Types, Handbook of Logic in Computer Science Vol. II*. Oxford University Press.

[6] Michael Beeson (1985): *Foundations of Constructive Mathematics*. Springer-Verlag, doi:10.1007/978-3-642-68952-9.

[7] M. Boespflug & G. Burel (2012): *CoqInE: Translating the calculus of inductive constructions into the lambda-Pi-calculus modulo*. In: *PxTP*, pp. 44–50.

[8] M. Boespflug, Q. Carbonneaux & O. Hermant (2012): *The lambda-Pi-calculus modulo as a universal proof language*. In: *PxTP*, pp. 28–43.

[9] Zakaria Chihani, Dale Miller & Fabien Renaud (2013): *Foundational proof certificates in first-order Logic*. In Maria Paola Bonacina, editor: *Automated Deduction – CADE-24*, *Lecture Notes in Computer Science* 7898, Springer Berlin Heidelberg, pp. 162–177, doi:10.1007/978-3-642-38574-2_11.

[10] Alonzo Church (1940): *A formulation of the simple theory of types*. *Journal of Symbolic Logic* 5(02), pp. 56–68, doi:10.2307/2266170.

[11] Denis Cousineau & Gilles Dowek (2007): *Embedding Pure Type Systems in the Lambda-Pi-Calculus Modulo*. In Simona Ronchi Della Rocca, editor: *TLCA*, *LNCS* 4583, Springer Berlin Heidelberg, pp. 102–117, doi:10.1007/978-3-540-73228-0_9.

[12] Gilles Dowek (2014): *Models and termination of proof-reduction in the $\lambda\Pi$-calculus modulo theory*. Available at https://who.rocq.inria.fr/Gilles.Dowek/Publi/superpi.pdf.

[13] Herman Geuvers (1993): *Logics and type systems*. PhD thesis, University of Nijmegen.

[14] Herman Geuvers & Erik Barendsen (1999): *Some logical and syntactical observations concerning the first-order dependent type system lambda-P*. *Mathematical Structures in Computer Science* 9(04), pp. 335–359, doi:10.1017/S0960129599002856.

[15] Thomas C. Hales (2007): *The Jordan Curve Theorem, Formally and Informally*. *American Mathematical Monthly* 114(10), pp. 882–894.

[16] Thomas C. Hales, John Harrison, Sean McLaughlin, Tobias Nipkow, Steven Obua & Roland Zumkeller (2011): *A Revision of the Proof of the Kepler Conjecture*. In Jeffrey C. Lagarias, editor: *The Kepler Conjecture*, Springer New York, pp. 341–376, doi:10.1007/978-1-4614-1129-1_9.

[17] Robert Harper, Furio Honsell & Gordon Plotkin (1993): *A framework for defining logics*. *J. ACM* 40(1), p. 143–184, doi:10.1145/138027.138060.

[18] Joe Hurd (2011): *The OpenTheory Standard Theory Library*. In Mihaela Bobaru, Klaus Havelund, Gerard J. Holzmann & Rajeev Joshi, editors: *NFM*, *LNCS* 6617, Springer, pp. 177–191, doi:10.1007/978-3-642-20398-5_14.

[19] Cezary Kaliszyk & Alexander Krauss (2013): *Scalable LCF-Style Proof Translation*. In Sandrine Blazy, Christine Paulin-Mohring & David Pichardie, editors: *ITP*, *LNCS* 7998, Springer Berlin Heidelberg, pp. 51–66, doi:10.1007/978-3-642-39634-2_7.

[20] Chantal Keller & Benjamin Werner (2010): *Importing HOL Light into Coq*. In Matt Kaufmann & Lawrence C. Paulson, editors: *ITP*, *LNCS* 6172, Springer Berlin Heidelberg, pp. 307–322, doi:10.1007/978-3-642-14052-5_22.

[21] Dale Miller (1991): *Unification of simply typed lambda-terms as logic programming*. *Technical Reports (CIS)*.

[22] Dale A. Miller (2004): *Proofs in higher-order logic*. Ph.D. thesis, University of Pennsylvania.

[23] Pavel Naumov, Mark-Oliver Stehr & José Meseguer (2001): *The HOL/NuPRL Proof Translator*. In Richard J. Boulton & Paul B. Jackson, editors: *TPHOLs*, *LNCS* 2152, Springer Berlin Heidelberg, pp. 329–345, doi:10.1007/3-540-44755-5_23.

[24] Steven Obua & Sebastian Skalberg (2006): *Importing HOL into Isabelle/HOL*. In Ulrich Furbach & Natarajan Shankar, editors: *Automated Reasoning*, *LNCS* 4130, Springer Berlin Heidelberg, pp. 298–302, doi:10.1007/11814771_27.

[25] Frank Pfenning & Carsten Schürmann (1999): *System Description: Twelf — A Meta-Logical Framework for Deductive Systems*. In: *CADE-16*, *LNCS* 1632, Springer Berlin Heidelberg, pp. 202–206, doi:10.1007/3-540-48660-7_14.

[26] Florian Rabe (2010): *Representing Isabelle in LF*. *EPTCS* 34, pp. 85–99, doi:10.4204/EPTCS.34.8. arXiv: 1009.2794.

[27] Florian Rabe & Michael Kohlhase (2013): *A scalable module system*. *Inf. Comput.* 230, pp. 1–54, doi:10.1016/j.ic.2013.06.001.

[28] Carsten Schürmann & Mark-Oliver Stehr (2006): *An Executable Formalization of the HOL/Nuprl Connection in the Metalogical Framework Twelf*. In Miki Hermann & Andrei Voronkov, editors: *LPAR*, *LNCS* 4246, Springer Berlin Heidelberg, pp. 150–166, doi:10.1007/11916277_11.

[29] Freek Wiedijk (2007): *The QED manifesto revisited*. *Studies in Logic, Grammar and Rhetoric* 10(23), pp. 121–133.