

# Adequate and computational encodings in the logical framework Dedukti

Thiago Felicissimo ✉

Université Paris-Saclay, INRIA project Deducteam, Laboratoire de Méthodes Formelles, ENS  
Paris-Saclay, 91190 France

## Abstract

DEDUKTI is a very expressive logical framework which unlike most frameworks, such as the Edinburgh Logical Framework (ELF), allows for the representation of computation alongside deduction. However, unlike ELF encodings, DEDUKTI encodings proposed until now do not feature an adequacy theorem — *i.e.*, a bijection between terms in the encoded system and in its encoding. Moreover, many of them also do not have a conservativity one, which compromises the ability of DEDUKTI to check proofs written in such encodings. We propose a different approach for DEDUKTI encodings which do not only allow for simpler conservativity proofs, but which also restore the adequacy of encodings. More precisely, we propose in this work adequate (and thus conservative) encodings for Functional Pure Type Systems. However, in contrast with ELF encodings, ours is computational — that is, represents computation directly as computation. Therefore, our work is the first to present and prove correct an approach allowing for encodings that are both adequate and computational in DEDUKTI.

**2012 ACM Subject Classification** Theory of computation → Type theory; Theory of computation → Equational logic and rewriting

**Keywords and phrases** Type Theory, Logical Frameworks, Rewriting, Dedukti

**Digital Object Identifier** 10.4230/LIPIcs.CVIT.2016.23

**Acknowledgements** I would like to thank my PhD advisors Frédéric Blanqui and Gilles Dowek for the helpful discussions and comments on this paper.

## 1 Introduction

The research on proof-checking naturally leads to the proposal of many logical systems and theories. *Logical frameworks* are a way of addressing this heterogeneity by proposing a common foundation in which systems and theories can be defined. The *Edinburgh Logical Framework* (ELF)[17] is one of the milestones in the history of logical frameworks, and proposes the use of a dependently-typed lambda-calculus to express deduction. However, as modern proof assistants move from traditional logics to type theories, where computation plays an important role alongside deduction, it becomes essential for such frameworks to also be able to express computation, something that the ELF does not achieve.

The logical framework DEDUKTI[3] addresses this point by extending the ELF with rewriting rules, thus allowing for the representation of both deduction and computation. This framework has already proven itself as a very expressive system, and has been used to encode the logics of many proof assistants, such as COQ[13], AGDA[14], PVS[18] and others.

However, an unsatisfying aspect persists as, unlike ELF encodings, the DEDUKTI encodings proposed until now are not *adequate* — that is, feature a syntactical bijection between the terms of the encoded system and those of the encoding. Such property is key in ensuring that the framework faithfully represents the syntax on the encoded system. Moreover, proving that DEDUKTI encodings are *conservative* (*i.e.*, that if the translation of a type is inhabited, then this type is inhabited) is still a challenge, in particular for recent works such as [13][23][14][18]. This is a problem if one intends to use DEDUKTI to check the correctness of proofs coming from proof assistants: if conservativity does not hold then the fact that the translation of a



© Thiago Felicissimo;  
licensed under Creative Commons License CC-BY 4.0

42nd Conference on Very Important Topics (CVIT 2016).

Editors: John Q. Open and Joan R. Access; Article No. 23; pp. 23:1–23:18

Leibniz International Proceedings in Informatics



LIPICs Schloss Dagstuhl – Leibniz-Zentrum für Informatik, Dagstuhl Publishing, Germany

45 proof is checked correct in DEDUKTI does not imply that this proof is correct.

46 In the specific case of Pure Type Systems (PTS), a class of type systems which generalizes  
 47 many others, [9] was the first to propose an encoding of functional PTSs into DEDUKTI. One  
 48 of their main contributions is that, differently from ELF encodings, their one is *computational*  
 49 — that is, represents computation in the encoded system directly as computation. They then  
 50 showed that the encoding was conservative under the hypothesis of normalization of their  
 51 rewrite rules.

52 To address the issue of this unproven assumption, [11] proposed a notion of model of  
 53 DEDUKTI and showed using the technique of *reducibility candidates* that the existence of such  
 54 a model entails the normalization of the encoding. Using this result, they then showed the  
 55 conservativity of the encoding of Simple Type Theory and of the Calculus of Constructions.  
 56 This technique however is not very satisfying as the construction of such models is a very  
 57 technical task, and needs to be done case by case. One can also wonder why conservativity  
 58 should rely on normalization.

59 The cause of this difficulty in [9] and in all other traditional DEDUKTI encodings comes  
 60 from a choice made to represent the abstraction and application of the encoded system  
 61 directly by the abstraction and application of the framework. This causes a confusion as  
 62 redexes of the encoded system, that represent real computations, get confused with the  $\beta$   
 63 redexes of the framework, which in other frameworks such as the ELF are used exclusively  
 64 to represent binder substitution. As a non-normal term can contain both types of redexes,  
 65 it is impossible to inverse translate it as some of these redexes are ill-typed in the original  
 66 system, and the only way of eliminating these ill-typed redexes is by reducing all ones. One  
 67 then needs this process to be terminating, which is non-trivial to show as it involves proving  
 68 that the reduction of the redexes of the encoded system terminates.

69 The work of [2] first noted this problem and proposed a different approach to show  
 70 the conservativity of the encoding of PTSs. Instead of relying on the normalization of the  
 71 encoding, they proposed to directly inverse translate terms without normalizing them. As  
 72 this creates ill-typed terms, they then used reducibility candidates to show that these ill-typed  
 73 terms reduce to well-typed ones, thus proving conservativity for the encoding in [9]. Even  
 74 though this technique is a big improvement over [11], it is still unsatisfying that both of  
 75 them rely on involved arguments using reducibility, whereas the proofs of ELF encodings  
 76 were very natural. The technicality of these proofs may be a reason for recent works such as  
 77 [23], [18] and [14] to have left conservativity as conjecture. Moreover, none of such works  
 78 have addressed the lack of an adequacy theorem.

## 79 Our contribution

80 We propose to depart from the approach of traditional DEDUKTI encodings by restoring  
 81 the separation that existed in ELF encodings. Our paradigm represents the abstractions  
 82 and applications of the encoded system not by those of the framework, but by dedicated  
 83 constructions. Using this approach, we propose an encoding of functional PTSs that is not  
 84 only sound and conservative but also adequate. However, in contrast with ELF encodings,  
 85 ours is computational like other DEDUKTI encodings.

86 To show conservativity, we leverage the fact the computational rules of the encoded  
 87 system are not represented by  $\beta$  reduction anymore, but by dedicated rewrite rules. This  
 88 allows us to normalize only the framework's  $\beta$  redexes without touching the ones associated  
 89 with the encoded system, and thus performing no computation from its point of view.

90 To be able to  $\beta$  normalize terms, we generalize the proof in [17] to give a general criterion  
 91 for the normalization of  $\beta$  reduction in DEDUKTI. This criterion imposes rewriting rules

to be *arity preserving* (a definition we introduce). This is not satisfied by traditional DEDUKTI encodings, but poses no problem to ours. The proof uses the simple technique of defining an erasure map into the simply-typed lambda calculus, which is known to be normalizing.

## Outline

We start in Section 2 by recalling the preliminaries about DEDUKTI. We proceed in Section 3 by proposing a criterion for the normalization of  $\beta$  in DEDUKTI, which is used in our proofs of conservativity and adequacy. In Section 4 we introduce an explicitly-typed version of Pure Type Systems, which is used in our translation. We then present our encoding in Section 5, and proceed by showing it is sound in Section 6 and that it is conservative and adequate in Section 7. In Section 8 we discuss how our approach can be used together with already known techniques to represent systems with infinite sorts. Finally, in Section 9 we discuss more practical aspects by showing how our encoding can be instantiated and used in practice.

## 2 Dedukti

$$\begin{array}{c}
\frac{}{\Sigma; - \text{well-formed}} \text{Empty} \quad x \notin \Gamma \frac{\Sigma; \Gamma \vdash A : \text{TYPE}}{\Sigma; \Gamma, x : A \text{ well-formed}} \text{Decl} \\
\\
c[\Delta] : A \in \Sigma \frac{\Sigma; \Delta \vdash A : s \quad \Sigma; \Gamma \vdash \vec{M} : \Delta}{\Sigma; \Gamma \vdash c[\vec{M}] : A\{\vec{M}\}} \text{Cons} \quad \frac{\Sigma; \Gamma \text{ well-formed}}{\Sigma; \Gamma \vdash \text{TYPE} : \text{KIND}} \text{Sort} \\
\\
x : A \in \Gamma \frac{\Sigma; \Gamma \text{ well-formed}}{\Sigma; \Gamma \vdash x : A} \text{Var} \quad A \equiv_{\beta\mathcal{R}} B \frac{\Sigma; \Gamma \vdash M : A \quad \Sigma; \Gamma \vdash B : s}{\Sigma; \Gamma \vdash M : B} \text{Conv} \\
\\
\frac{\Sigma; \Gamma \vdash A : \text{TYPE} \quad \Sigma; \Gamma, x : A \vdash B : s}{\Sigma; \Gamma \vdash \Pi x : A. B : s} \text{Prod} \quad \frac{\Sigma; \Gamma \vdash M : \Pi x : A. B \quad \Sigma; \Gamma \vdash N : A}{\Sigma; \Gamma \vdash MN : B\{N/x\}} \text{App} \\
\\
\frac{\Sigma; \Gamma \vdash A : \text{TYPE} \quad \Sigma; \Gamma, x : A \vdash B : s \quad \Sigma; \Gamma, x : A \vdash M : B}{\Sigma; \Gamma \vdash \lambda x : A. M : \Pi x : A. B} \text{Abs}
\end{array}$$

Figure 1 Typing rules for DEDUKTI

The logical framework DEDUKTI [3] has the syntax of the  $\lambda$ -calculus with dependent types [17] ( $\lambda\Pi$ -calculus). Like works such as [18], we consider here a version with arities, with the following syntax.

$$A, B, M, N ::= x \mid c[\vec{M}] \mid \text{TYPE} \mid \text{KIND} \mid MN \mid \lambda x : A. M \mid \Pi x : A. B$$

Here,  $c$  ranges in an infinite set of constants  $\mathcal{C}$ , and  $x$  ranges in an infinite set of variables  $\mathcal{V}$ . Each constant  $c$  is assumed to have a fixed arity  $n_c$  and for each occurrence of  $c[\vec{M}]$  we should have  $\text{length}(\vec{M}) = n_c$ . We denote  $\Lambda_{\text{DK}}$  the set of terms generated by this grammar. We call a term of the form  $\Pi x : A. B$  a *dependent product*, and we write  $A \rightarrow B$  when  $x$  does not appear free in  $B$ . We allow ourselves sometimes to write  $c \vec{M}$  instead of  $c[\vec{M}]$  to ease the notation.

A *context*  $\Gamma$  is a finite sequence of pairs  $x : A$  with  $A \in \Lambda_{\text{DK}}$ . A *signature*  $\Sigma$  is a finite set of triples  $c[\Delta] : A$  where  $A \in \Lambda_{\text{DK}}$  and  $\Delta$  is a context containing at least all free variables of  $A$ . The main difference between DEDUKTI and the  $\lambda\Pi$ -calculus is that we also consider a set  $\mathcal{R}$  of *rewrite rules*, that is, of pairs of the form  $c[\vec{l}] \hookrightarrow r$  with  $l_1, \dots, l_k, r \in \Lambda_{\text{DK}}$ . A *theory* is a pair  $(\Sigma, \mathcal{R})$  such that all constants appearing in  $\mathcal{R}$  are declared in  $\Sigma$ .

We write  $\hookrightarrow_{\mathcal{R}}$  for the context and substitution closure of the rules in  $\mathcal{R}$  and  $\hookrightarrow_{\beta\mathcal{R}}$  for  $\hookrightarrow_{\beta} \cup \hookrightarrow_{\mathcal{R}}$ . We also consider the equivalence relation  $\equiv_{\beta\mathcal{R}}$  generated by  $\hookrightarrow_{\beta\mathcal{R}}$ . Finally, we may refer to  $\hookrightarrow_{\beta\mathcal{R}}$  and  $\equiv_{\beta\mathcal{R}}$  by just  $\hookrightarrow$  and  $\equiv$ .

Typing in DEDUKTI is given by the rules in Figure 1. In rule **Conv** we use the usual notation  $\Sigma; \Gamma \vdash \vec{M} : \Delta$  meaning that  $\Delta = x_1 : A_1, \dots, x_n : A_n$  and  $\Sigma; \Gamma \vdash M_i : A_i\{M_1/x_1\}\dots\{M_{i-1}/x_{i-1}\}$  is derivable for  $i = 1, \dots, n$ . We then also allow ourselves to write  $A\{\vec{M}\}$  instead of  $A\{M_1/x_1\}\dots\{M_n/x_n\}$ . We refer to Appendix A for a review of some basic metatheorems.

### 3 Strong Normalization of $\beta$ in Dedukti

In order to show conservativity of encodings, one often needs to be able to  $\beta$  normalize terms, thus requiring  $\beta$  to be normalizing for well-typed terms. In this section we present a criterion for the normalization of  $\beta$  in DEDUKTI. More precisely, we will see that if  $\beta\mathcal{R}$  is confluent and  $\mathcal{R}$  is *arity preserving* (a definition we will introduce in this section), then  $\beta$  is SN (strongly normalizing) in DEDUKTI for well-typed terms. The proof generalizes the one given in [17]. However, because of space constraints, we only give the intuition of the proof and refer to the long version for the proof.

Note that, unlike works such as [8], which provide syntactic criteria on the normalization of  $\beta\mathcal{R}$  in DEDUKTI, we only aim to show the normalization of  $\beta$ . In particular  $\beta\mathcal{R}$  may not be SN in our setting. Our work has more similar goals to [4], which provides criteria for the SN of  $\beta$  in the Calculus of Constructions when adding object-level rewrite rules. However, our work also allows for type-level rewrite rules, which will be needed in our encoding.

Our proof works by defining an erasure map into the simply-typed  $\lambda$ -calculus, which is known to be SN, and then showing that this map preserves typing and non-termination of  $\beta$ , thus implying that  $\beta$  is SN in DEDUKTI. Before proceeding, we introduce the following basic definitions.

#### ► Definition 1.

1. Given a signature  $\Sigma$ , a constant  $c$  is *type-level* (and referred by  $\alpha, \gamma$ ) if  $c[\Delta] : A \in \Sigma$  with  $A$  of the form  $\Pi \vec{x} : \vec{B}. \text{TYPE}$ , otherwise it is *object-level* (and referred by  $a, b$ ).
2. A rewrite rule  $c[\vec{l}] \hookrightarrow r$  is *type-level* if its head symbol  $c$  is a type-level constant.

We can now define the erasure map.

#### ► Definition 2 (Erasure map). Consider the simple types generated by the grammar

$$\sigma ::= * \mid \sigma \rightarrow \sigma.$$

Moreover, let  $\Gamma_{\pi}$  be the context containing for each  $\sigma$  the declaration  $\pi_{\sigma} : * \rightarrow (\sigma \rightarrow *) \rightarrow *$ . We define the partial functions  $\|-\|, |-|$  by the following equations.

$$\begin{array}{ll} \|\text{TYPE}\| = * & |x| = x \\ \|\alpha[\vec{M}]\| = * & |a[\vec{M}]| = a \mid \vec{M}| \\ \|\Pi x : A. B\| = \|A\| \rightarrow \|B\| & |\alpha[\vec{M}]| = \alpha \mid \vec{M}| \\ \|AN\| = \|A\| & |MN| = |M| \mid |N| \\ \|\lambda x : A. B\| = \|B\| & |\lambda x : A. M| = (\lambda z. \lambda x. |M|) |A| \text{ where } z \notin FV(M) \\ & |\Pi x : A. B| = \pi_{\|A\|} \mid |A| \mid (\lambda x. |B|) \end{array}$$

We also extend the definition of  $\|-\|$  (partially) on contexts and signatures by the following equations.

$$\begin{aligned} \|-\| &= - \\ \|x : A, \Gamma\| &= x : \|A\|, \|\Gamma\| \\ \|c[x_1 : A_1, \dots, x_n : A_n] : A; \Sigma\| &= (c : \|A_1\| \rightarrow \dots \rightarrow \|A_n\| \rightarrow \|A\|), \|\Sigma\| \end{aligned}$$

In order to show the normalization of  $\beta$ , we need the erasure to preserve typing. The main obstacle when showing this is dealing with the **Conv** rule. To make the proof go through, we would need to show that if  $A \equiv B$  then  $\|A\| = \|B\|$ . In the  $\lambda\Pi$ -calculus this can be easily shown, however because in DEDUKTI the relation  $\equiv$  also takes into account the rewrite rules in  $\mathcal{R}$ , we can easily build counterexamples in which this does not hold.

► **Example 3.** Let *El*, *Prod*, *Nat* be type-level constants, and consider the rule

$$\text{El } (\text{Prod } A B) \longleftrightarrow \Pi x : \text{El } A. \text{El } (B x)$$

traditionally used to build DEDUKTI encodings (as in [9]). Note that here we write  $\alpha \vec{I}$  for  $\alpha[\vec{I}]$ , to ease the notation. We then have

$$\text{El } (\text{Prod } \text{Nat } (\lambda x. \text{Nat})) \equiv \Pi x : \text{El } \text{Nat}. \text{El } ((\lambda x. \text{Nat}) x) \equiv \text{El } \text{Nat} \rightarrow \text{El } \text{Nat}$$

but  $\|\text{El } (\text{Prod } \text{Nat } (\lambda x : \text{Nat}))\| = *$  and  $\|\text{El } \text{Nat} \rightarrow \text{El } \text{Nat}\| = * \rightarrow *$ .

If we were to define the arity of a type<sup>1</sup> as the number of consecutive arrows (that is, of  $\Pi$ s), then we realize that the problem here is that rules such as  $\text{El } (\text{Prod } A B) \longleftrightarrow \Pi x : \text{El } A. \text{El } (B x)$  do not preserve the arity. Indeed,  $\text{El } (\text{Prod } A B)$  has arity 0 because it has no arrows, whereas  $\Pi x : \text{El } A. \text{El } (B x)$  has arity 1 as it has one arrow<sup>2</sup>. As the left-hand side of a type-level rule always has arity 0 (because it is of the form  $\alpha[\vec{I}]$ ), to remove these unwanted cases we need for their right-hand sides to also have arity 0. This motivates the following definition.

► **Definition 4** (Arity preserving).  $\mathcal{R}$  is said to be *arity-preserving*<sup>3</sup> if, for every type-level rewrite rule in  $\mathcal{R}$ , the right-hand side is in the following grammar, where  $\vec{M}, N, A$  are any.

$$R ::= \alpha[\vec{M}] \mid R N \mid \lambda x : A. R$$

It turns out that this condition, together with confluence of  $\beta\mathcal{R}$ , is enough to show that the translation preserves typing and non-termination. Using the fact that well-typed terms are strongly normalizing in the simply-typed  $\lambda$ -calculus, we get the following theorem. We refer to the long version in X for the proofs.

► **Theorem 5** ( $\beta$  is SN in DEDUKTI). *If  $\beta\mathcal{R}$  is confluent and  $\mathcal{R}$  is arity-preserving, then  $\beta$  is strongly normalizing for well-typed terms in DEDUKTI.*

<sup>1</sup> Note that this concept is different from the notion of arity of constants, as defined in Section 2.

<sup>2</sup> Using a different notation for the dependent product, we can write this type as  $(x : \text{El } A) \rightarrow \text{El } (B x)$ , which may help to clarify this assertion.

<sup>3</sup> More precisely, this definition also depends on the signature  $\Sigma$ , as this is used to define which constants are type-level.

## 4 Pure Type Systems

Pure type systems (or PTSs) is a class of type systems that generalizes many other systems, such as the Calculus of Constructions and System F. They are parameterized by a set of *sorts*  $\mathcal{S}$  and two relations  $\mathcal{A} \subseteq \mathcal{S}^2, \mathcal{R} \subseteq \mathcal{S}^3$ . In this work we restrict ourselves to functional PTSs, for which  $\mathcal{A}$  and  $\mathcal{R}$  are functional relations. This restriction covers almost all of PTSs used in practice, and gives a much more well behaved metatheory.

In this paper we consider a variant of PTSs with explicit parameters. That is, just like when taking the projection of a pair  $\pi^1(p)$  we can explicit all parameters and write  $\pi^1(A, B, p)$  where  $p : A \times B$ , we can also write  $\lambda(A, [x]B, [x]M)$  instead of  $\lambda x : A. M$  and  $\mathcal{O}(A, [x]B, M, N)$  instead of  $MN$ . Moreover, if  $- \times -$  is a universe-polymorphic definition, we should also write  $\pi_{s_A, s_B}^1(A, B, p)$  to explicit the sort parameters. As in PTSs the dependent product is used across sorts, we then should also write  $\lambda_{s_A, s_B}(A, [x]B, [x]M)$ ,  $\mathcal{O}_{s_A, s_B}(A, [x]B, M, N)$  and  $\Pi_{s_A, s_B}(A, [x]B)$ . To be more technical, we render explicit the parameters on the dependent product type and on its constructor (abstraction) and eliminator (application). Because of this interpretation in which we are rendering the parameters of  $\lambda$  and  $\mathcal{O}$  explicit, we name this version of PTSs as Explicitly-typed Pure Type Systems (EPTSs).

Reduction is then defined by the context closure of the  $\beta$  rules<sup>4</sup>

$$\mathcal{O}_{s_1, s_2}(A, [x]B, \lambda_{s_1, s_2}(A', [x]B', [x]M), N) \longleftrightarrow M\{N/x\}$$

given for each  $(s_1, s_2, s_3) \in \mathcal{R}$ . Typing is given by the rules in Figure 2.

$$\begin{array}{c} \frac{}{- \text{ well-formed}} \text{ EMPTY} \quad x \notin \Gamma \frac{\Gamma \vdash A : s}{\Gamma, x : A \text{ well-formed}} \text{ DECL} \\ \\ A \equiv B \frac{\Gamma \vdash M : A \quad \Gamma \vdash B : s}{\Gamma \vdash M : B} \text{ CONV} \quad (s_1, s_2) \in \mathcal{A} \frac{\Gamma \text{ well-formed}}{\Gamma \vdash s_1 : s_2} \text{ SORT} \\ \\ x : A \in \Gamma \frac{\Gamma \text{ well-formed}}{\Gamma \vdash x : A} \text{ VAR} \quad (s_1, s_2, s_3) \in \mathcal{R} \frac{\Gamma \vdash A : s_1 \quad \Gamma, x : A \vdash B : s_2}{\Gamma \vdash \Pi_{s_1, s_2}(A, [x]B) : s_3} \text{ PROD} \\ \\ (s_1, s_2, s_3) \in \mathcal{R} \frac{\Gamma \vdash A : s_1 \quad \Gamma, x : A \vdash B : s_2 \quad \Gamma, x : A \vdash M : B}{\Gamma \vdash \lambda_{s_1, s_2}(A, [x]B, [x]M) : \Pi_{s_1, s_2}(A, [x]B)} \text{ ABS} \\ \\ (s_1, s_2, s_3) \in \mathcal{R} \frac{\Gamma \vdash A : s_1 \quad \Gamma, x : A \vdash B : s_2 \quad \Gamma \vdash N : A \quad \Gamma \vdash M : \Pi_{s_1, s_2}(A, [x]B)}{\Gamma \vdash \mathcal{O}_{s_1, s_2}(A, [x]B, M, N) : B\{N/x\}} \text{ APP} \end{array}$$

■ **Figure 2** Typing rules for Explicitly-typed Pure Type Systems

This modification is just a technical change that will help us during the translation, as our encoding needs the data of such parameters often left implicit. Other works such as [20] and [21] also consider similar variants, though none of them correspond exactly to ours. Therefore, we had to develop the basic metatheory of our version in [12], and we have found that the usual meta-theoretical properties of functional PTSs are preserved when moving to the explicitly-typed version (see Appendix B). More importantly, by a proof that uses ideas present in [21], we have shown the following equivalence.

<sup>4</sup> We consider a linearized variant of the expected non-left linear rule  $\mathcal{O}_{s_1, s_2}(A, [x]B, \lambda_{s_1, s_2}(A, [x]B, [x]M), N) \longleftrightarrow M\{N/x\}$ , which is non-confluent in untyped terms. By linearizing it, we get a much more well-behaved rewriting system, where confluence holds for all terms. Moreover, whenever the left hand side is well-typed, the typing constraints impose  $A \equiv A'$  and  $B \equiv B'$ .

213 ▶ **Theorem 6** (Equivalence between PTSs and EPTSs[12]). *Let  $|-|$  be the erasure map defined*  
 214 *in the most natural way from a functional EPTS to its corresponding functional PTS. Given*  
 215  *$\Gamma, M, A$  in a PTS, we have*

$$216 \quad \Gamma \vdash_{PTS} M : A \iff \exists \Gamma', M', A' \text{ st } \Gamma' \vdash_{EPTS} M' : A' \wedge |\Gamma'| = \Gamma \wedge |M'| = M \wedge |A'| = A.$$

## 217 5 Encoding EPTSs in Dedukti

218 This section presents our encoding of functional EPTSs in DEDUKTI. In order to ease the  
 219 notation, from now on we write  $c \vec{M}$  for  $c[\vec{M}]$ . The basis for the encoding is given by a  
 220 theory  $(\Sigma_{EPTS}, \mathcal{R}_{EPTS})$  which we will construct step by step here.

221 Pure Type Systems (explicitly-typed or not) feature two kinds of types: dependent  
 222 products and universes. We start by building the representation of the latter. For each  
 223  $s \in \mathcal{S}$  we declare a type  $U_s$  to represent the type of elements of  $s$ . However, as the terms  $A$   
 224 with  $\Gamma \vdash_{EPTS} A : s$  are themselves types, we also need to declare a function  $El_{s_1}$  which maps  
 225 each such  $A$  to its corresponding type. As for each  $(s_1, s_2) \in \mathcal{A}$  we have  $\vdash_{EPTS} s_1 : s_2$ , we  
 226 also declare a constant  $u_{s_1}$  in  $U_{s_2}$  to represent this. Finally, as the sorts  $s_1$  with  $(s_1, s_2) \in \mathcal{A}$   
 227 now can be represented by both  $U_{s_1}$  and  $El_{s_2} u_{s_1}$ , we add a rewrite rule to identify these  
 228 representations. This encoding resembles the definition of universes in type theories *à la*  
 229 Tarski, and also follows traditional representations of universes in DEDUKTI as in [9].

$$230 \quad \left| \begin{array}{l} U_s : \text{TYPE} \\ El_s[A : U_s] : \text{TYPE} \end{array} \right| \quad \text{for } s \in \mathcal{S} \quad \left| \begin{array}{l} u_{s_1} : U_{s_2} \\ El_{s_2} u_{s_1} \hookrightarrow_{u_{s_1}\text{-red}} U_{s_1} \end{array} \right| \quad \text{for } (s_1, s_2) \in \mathcal{A}$$

231 We now move to the representation of the dependent product type. We first declare a  
 232 constant to represent the type formation rule for the dependent product.

$$233 \quad \left| \text{Prod}_{s_1, s_2}[A : U_{s_1}; B : El_{s_1} A \rightarrow U_{s_2}] : U_{s_3} \right| \quad \text{for } (s_1, s_2, s_3) \in \mathcal{R}$$

234 Traditional DEDUKTI encodings would normally continue here by introducing the rule  
 235  $El_{s_3}(\text{Prod}_{s_1, s_2} A B) \hookrightarrow \Pi x : El_{s_1} A. El_{s_2}(B x)$ , identifying the dependent product of the  
 236 encoded theory with the one of DEDUKTI, thus allowing for the use of the framework's  
 237 abstraction, application and  $\beta$  to represent the ones of the encoded system. We instead keep  
 238 them separate and declare constants representing the introduction and elimination rules for  
 239 the dependent product being encoding, that is, representing abstraction and application.

$$240 \quad \left| \begin{array}{l} abs_{s_1, s_2}[A : U_{s_1}; B : El_{s_1} A \rightarrow U_{s_2}; M : \Pi x : El_{s_1} A. El_{s_2}(B x)] : El_{s_3}(\text{Prod}_{s_1, s_2} A B) \\ app_{s_1, s_2}[A : U_{s_1}; B : El_{s_1} A \rightarrow U_{s_2}; M : El_{s_3}(\text{Prod}_{s_1, s_2} A B); N : El_{s_1} A] : El_{s_2}(B N) \\ app_{s_1, s_2} A B (abs_{s_1, s_2} A' B' M) N \hookrightarrow_{beta_{s_1, s_2}} M N \end{array} \right| \quad \text{for } (s_1, s_2, s_3) \in \mathcal{R}$$

241 We note that this idea is also hinted in [1], though they did not pursue it further.  
 242 This approach also reassembles the one of the Edinburgh Logical Framework (ELF) [17] in  
 243 which the framework's abstraction is used exclusively for binding. We are however able to  
 244 encode computation directly as computation with the rule  $beta_{s_1, s_2}$ , whereas the ELF handles  
 245 computation by encoding it as an equality judgment, thus introducing explicit coercions in  
 246 the terms. Some other variants such as [16] prevent the introduction of such coercions, but  
 247 computation is still represented by an equality judgment instead of being represented by  
 248 computation.

249 We are now ready to define the translation function  $\llbracket - \rrbracket$ .

250  $\llbracket x \rrbracket = x$

251  $\llbracket s \rrbracket = u_s$

252  $\llbracket \Pi_{s_1, s_2}(A, [x]B) \rrbracket = \text{Prod}_{s_1, s_2} \llbracket A \rrbracket (\lambda x : \text{El}_{s_1} \llbracket A \rrbracket. \llbracket B \rrbracket)$

253  $\llbracket \lambda_{s_1, s_2}(A, [x]B, [x]M) \rrbracket = \text{abs}_{s_1, s_2} \llbracket A \rrbracket (\lambda x : \text{El}_{s_1} \llbracket A \rrbracket. \llbracket B \rrbracket) (\lambda x : \text{El}_{s_1} \llbracket A \rrbracket. \llbracket M \rrbracket)$

254  $\llbracket \mathcal{C}_{s_1, s_2}(A, [x]B, M, N) \rrbracket = \text{app}_{s_1, s_2} \llbracket A \rrbracket (\lambda x : \text{El}_{s_1} \llbracket A \rrbracket. \llbracket B \rrbracket) \llbracket M \rrbracket \llbracket N \rrbracket$

256 We also extend  $\llbracket - \rrbracket$  to well-formed contexts by the following definition. Note that because  
257 we are dealing with functional EPTSs, the sort of  $A$  in  $\Gamma$  is unique, hence the following  
258 definition makes sense.

259  $\llbracket - \rrbracket = -$

260  $\llbracket \Gamma, x : A \rrbracket = \llbracket \Gamma \rrbracket, x : \text{El}_{s_A} \llbracket A \rrbracket$  where  $\Gamma \vdash A : s_A$

262 ▶ **Remark 7.** Note that in the definitions of  $\llbracket - \rrbracket$  it was essential for  $\lambda$  and  $\mathcal{C}$  to explicit the  
263 types  $A$  and  $B$ , as the constants  $\text{abs}_{s_1, s_2}$  and  $\text{app}_{s_1, s_2}$  require their translations. Had we had  
264 for instance just  $\lambda x : A.M$ , we could then make the translation dependent on  $\Gamma$  and take a  
265  $B$  such that  $\Gamma, x : A \vdash M : B$ . However, because  $\llbracket - \rrbracket$  is defined by induction and  $B$  is not  
266 a subterm of  $\lambda x : A.M$ , we cannot apply  $\llbracket - \rrbracket$  to  $B$ . Therefore, when doing an encoding in  
267 DEDUKTI one should first render explicit the needed data before translating, and then show  
268 an equivalence theorem between the explicit and implicit versions (in our case, Theorem 6).

269 Moreover, note that by also making the sorts explicit in  $\lambda_{s_1, s_2}, \mathcal{C}_{s_1, s_2}, \Pi_{s_1, s_2}$  our translation  
270 can be defined purely syntactically. If this information were not in the syntax, we could still  
271 define  $\llbracket - \rrbracket$  by making it dependent on  $\Gamma$ . Nevertheless, this complicates many proofs, as each  
272 time we apply  $\llbracket - \rrbracket_\Gamma$  to a term we need to know it is well-typed in  $\Gamma$ .

273 In order to understand more intuitively how the encoding works, let's look at an example.

274 ▶ **Example 8.** Recall that System F can be defined by the sort specification  $\mathcal{S} = \{\text{Type}, \text{Kind}\}$ ,  $\mathcal{A} =$   
275  $\{\text{Type} : \text{Kind}\}$ ,  $\mathcal{R} = \{(\text{Type}, \text{Type}, \text{Type}), (\text{Kind}, \text{Type}, \text{Type})\}$ . In this EPTS, we can express  
276 the polymorphic identity function, traditionally written as  $\lambda A : \text{Type}. \lambda x : A. x$ , by

277  $\lambda_{\text{Kind}, \text{Type}}(\text{Type}, [A]\Pi(A, [x]A), [A]\lambda_{\text{Type}, \text{Type}}(A, [x]A, [x]x))$

278 This term is represented in our encoding by

279  $\text{abs}_{\text{Kind}, \text{Type}} \ u_{\text{Type}} (\lambda A. \text{Prod}_{\text{Type}, \text{Type}} A (\lambda x. A)) (\lambda A. \text{abs}_{\text{Type}, \text{Type}} A (\lambda x. A) (\lambda x. x))$

280 where we omit the type annotations in the abstractions, to improve readability.

## 281 6 Soundness

282 An encoding is said to be sound when it preserves the typing relation of the original system.  
283 In this section we will see that our encoding has this fundamental property. We start by  
284 establishing some conventions in order to ease notations.

285 ▶ **Convention 9.** We establish the following notations.

286 ■ We write  $\Sigma; \Gamma \vdash_{\text{DK}} M : A$  for a DEDUKTI judgment and  $\Gamma \vdash M : A$  (not  $\vdash_{\text{EPTS}}$ ) for an  
287 EPTS judgment

288 ■ As the same signature  $\Sigma_{\text{EPTS}}$  is used everywhere, when writing  $\Sigma_{\text{EPTS}}; \Gamma \vdash_{\text{DK}} M : A$  we omit  
289 it and write  $\Gamma \vdash_{\text{DK}} M : A$ .



Before showing soundness, we start by establishing some basic results.

► **Proposition 10** (Basic properties). *We have the following basic properties.*

1. *Confluence: The rewriting rules of the encoding are confluent with  $\beta$ .*
2. *Well-formedness of the signature: For all  $c[\Delta] : A \in \Sigma_{\text{EPTS}}$ , we have  $\Delta \vdash_{\text{DK}} A : s$ .*
3. *Subject reduction for  $\beta$ : If  $\Gamma \vdash_{\text{DK}} M : A$  and  $M \hookrightarrow_{\beta} M'$  then  $\Gamma \vdash_{\text{DK}} M' : A$ .*
4. *Strong normalization for  $\beta$ : If  $\Gamma \vdash_{\text{DK}} M : A$ , the  $\beta$  is strongly normalizing for  $M$ .*
5. *Compositionality: For all  $M, N \in \Lambda_{\text{EPTS}}$  we have  $\llbracket M \rrbracket \{ \llbracket N \rrbracket / x \} = \llbracket N \{ N/x \} \rrbracket$ .*

**Proof.** 1. The considered rewrite rules form an orthogonal combinatory reduction system, and therefore are confluent[19].

2. Can be shown for instance with LAMBDAP1[10], an implementation of DEDUKTI.

3. Subject reduction of  $\beta$  is implied by confluence of  $\beta\mathcal{R}_{\text{EPTS}}$ [6].

4.  $\mathcal{R}_{\text{EPTS}}$  is arity preserving and  $\beta\mathcal{R}_{\text{EPTS}}$  is confluent, thus  $\beta$  is SN in DEDUKTI (Theorem 5) applies.

5. By induction on  $M$ . ◀

► **Remark 11.** We could also show subject reduction of our encoding, either using the method in [7] or LAMBDAP1[10]. However, we will see that our proof does not actually require subject reduction of  $\mathcal{R}_{\text{EPTS}}$ . Therefore, we conjecture that our proof method can also be adapted to systems that do not satisfy subject reduction.

► **Lemma 12** (Preservation of computation). *Let  $M, N \in \Lambda_{\text{EPTS}}$ . We have*

1.  *$M \hookrightarrow N$  implies  $\llbracket M \rrbracket \hookrightarrow^* \llbracket N \rrbracket$*
2.  *$M \equiv N$  implies  $\llbracket M \rrbracket \equiv \llbracket N \rrbracket$*

**Proof.** The first part is shown by induction on the rewriting context, using compositionality of  $\llbracket - \rrbracket$  for the base case. The second part follows by induction on  $\equiv$  and uses part 1. ◀

Recall that a sort  $s \in \mathcal{S}$  is said to be a top-sort if there is no  $s'$  with  $(s, s') \in \mathcal{A}$ . The following auxiliary lemma allows us to switch between sort representations and is heavily used in the proof of soundness.

► **Lemma 13** (Equivalence for sort representations). *If  $s$  is not a top-sort, then*

$$\Gamma \vdash_{\text{DK}} M : U_s \iff \Gamma \vdash_{\text{DK}} M : El_{s'} u_s$$

where  $(s, s') \in \mathcal{A}$ .

With all these results in hand, we can now show the soundness of our encoding.

► **Theorem 14** (Soundness). *Let  $\Gamma$  be a context and  $M, A$  terms in an EPTS. We have*

- *If  $\Gamma$  well-formed then  $\llbracket \Gamma \rrbracket$  well-formed*
- *If  $\Gamma \vdash M : A$  then*
  - *if  $A$  is a top-sort then  $\llbracket \Gamma \rrbracket \vdash_{\text{DK}} \llbracket M \rrbracket : U_A$*
  - *else  $\llbracket \Gamma \rrbracket \vdash_{\text{DK}} \llbracket M \rrbracket : El_{s_A} \llbracket A \rrbracket$ , where  $\Gamma \vdash A : s_A$*

**Proof.** By structural induction on the proof of the judgment. We present here only the case PROD to show the idea, the other cases are detailed in the long version.

**Case Prod:** The proof ends with

$$(s_1, s_2, s_3) \in \mathcal{R} \frac{\Gamma \vdash A : s_1 \quad \Gamma, x : A \vdash B : s_2}{\Gamma \vdash \Pi_{s_1, s_2} (A, [x]B) : s_3} \text{PROD}$$

By the IH and Lemma 13, we have  $\llbracket \Gamma \rrbracket \vdash_{\text{DK}} \llbracket A \rrbracket : U_{s_1}$  and  $\llbracket \Gamma \rrbracket, x : El_{s_1} \llbracket A \rrbracket \vdash_{\text{DK}} \llbracket B \rrbracket : U_{s_2}$ .  
 By **Abs** we get  $\llbracket \Gamma \rrbracket \vdash_{\text{DK}} \lambda x : El_{s_1} \llbracket A \rrbracket. \llbracket B \rrbracket : El_{s_1} \llbracket A \rrbracket \rightarrow U_{s_2}$ , therefore it suffices to apply **Cons**  
 with  $Prod_{s_1, s_2}$  to conclude

$$\llbracket \Gamma \rrbracket \vdash_{\text{DK}} Prod_{s_1, s_2} \llbracket A \rrbracket_{\Gamma} (\lambda x : El_{s_1} \llbracket A \rrbracket. \llbracket B \rrbracket) : U_{s_3}$$

If  $s_3$  is not a top-sort, we then apply Lemma 13.  $\blacktriangleleft$

## 7 Conservativity and Adequacy

Many works proposing DEDUKTI encodings often stop after showing soundness and leave conservativity as a conjecture. This is because, when mixing the rules  $\beta$  with  $\beta_{\text{eta}}$ , as done in traditional DEDUKTI encodings, one needs to show the termination of both, given that to show conservativity one often considers terms in normal form [9]. However this problem is non-trivial, and in particular the normalization of  $\beta \cup \beta_{\text{eta}}$  implies the termination (and thus normally also the consistency) of the encoded system. This is also unnatural, as logical frameworks should be agnostic to the fact that a system is consistent or not, and thus this shouldn't be required to show conservativity.

In this section we will show how conservativity can be shown without difficulties when we distinguish the rules  $\beta$  and  $\beta_{\text{eta}}$ . In particular, our proof does not need  $\beta \cup \beta_{\text{eta}}$  to be normalizing, and thus also applies to non-normalizing and non-consistent systems.

We start by defining a notion of invertible forms and an inverse translation which allows to invert them into the original system. After proving some basic properties about them, we then proceed with the proof of conservativity.

### 7.1 The inverse translation

► **Definition 15** (Invertible forms). *We call the terms generated by the following grammar the invertible forms. The  $s_i$  are any sorts in  $S$ , whereas the  $T_1, T_2$  are any terms.*

$$\begin{aligned} M, N, A, B ::= & x \mid c \mid u_s \mid abs_{s_1, s_2} A (\lambda x : T_1. B) (\lambda x : T_2. M) \mid (\lambda x : T. M) N \\ & \mid Prod_{s_1, s_2} A (\lambda x : T_1. B) \mid app_{s_1, s_2} A (\lambda x : T_1. B) M N \end{aligned}$$

Note that this definition includes some terms which are not in  $\beta$  normal form. The next definition justifies the name of invertible forms: we know how to invert them.

► **Definition 16.** *We define the inverse translation function  $| - | : \Lambda_{\text{DK}} \rightarrow \Lambda_{\text{EPTS}}$  on invertible forms by structural induction.*

$$\begin{aligned} |x| &= x & |(\lambda x : \_ . M) N| &= |M| \{ |N| / x \} \\ |c| &= c & |Prod_{s_1, s_2} A (\lambda x : \_ . B)| &= \Pi_{s_1, s_2} (|A|, [x] |B|) \\ |u_s| &= s & |abs_{s_1, s_2} A (\lambda x : \_ . B) (\lambda x : \_ . M)| &= \lambda_{s_1, s_2} (|A|, [x] |B|, [x] |M|) \\ & & |app_{s_1, s_2} A (\lambda x : \_ . B) M N| &= \mathcal{O}_{s_1, s_2} (|A|, [x] |B|, |M|, |N|) \end{aligned}$$

We can show, as expected, that the terms in the image of the translation are invertible forms and that  $| - |$  is a left inverse of  $\llbracket - \rrbracket$ . The proof is a simple induction on  $M$ .

► **Proposition 17.** *For all  $M \in \Lambda_{\text{EPTS}}$ ,  $\llbracket M \rrbracket$  is an invertible form and  $\llbracket \llbracket M \rrbracket \rrbracket = M$ .*

The following lemma shows that invertible forms are closed under rewriting and that this rewriting can also be inverted into the EPTS.

365 ▶ **Proposition 18.** *Let  $M$  be a invertible form.*

- 366 1. *If  $N$  is an invertible form, then  $M(N/x)$  is also and  $|M|\{|N|/x\} = |M\{N/x\}|$ .*
- 367 2. *If  $M \hookrightarrow_{\text{beta}_{s_1, s_2}} N$  then  $N$  is an invertible form and  $|M| \hookrightarrow_{\beta}^* |N|$*
- 368 3. *If  $M \hookrightarrow_{\beta, u_{s_1} \text{-red}} N$  then  $N$  is an invertible form and  $|M| = |N|$ .*
- 369 4. *If  $M \hookrightarrow^* N$  then  $N$  is an invertible form and  $|M| \hookrightarrow^* |N|$ .*

370 **Proof.** The property 1 is shown by induction on  $M$ , whereas 2, 3 follow by induction on the  
 371 rewrite context and 4 follows directly from 2, 3. ◀

372 ▶ **Remark 19.** Note that this last proposition explains the difference between the  $\beta$  and  
 373  $\text{beta}_{s_1, s_2}$  steps. Whereas  $\text{beta}_{s_1, s_2}$  steps represents the real computation steps that take place  
 374 in the encoded system,  $\beta$  steps are invisible because they correspond to the framework's  
 375 substitution, an administrative operation that is implicit in the encoded system. Therefore,  
 376 it was expected that  $\text{beta}_{s_1, s_2}$  steps would be reflected into the original system, whereas  $\beta$   
 377 steps would be silent.

378 Putting all this together, we deduce that computation and conversion in DEDUKTI is  
 379 reflected in the encoded system.

380 ▶ **Corollary 20** (Reflection of computation). *For  $M, N \in \Lambda_{EPTS}$ , we have*

- 381 1. *If  $\llbracket M \rrbracket \hookrightarrow^* \llbracket N \rrbracket$  then  $M \hookrightarrow^* N$ .*
- 382 2. *If  $\llbracket M \rrbracket \equiv \llbracket N \rrbracket$  then  $M \equiv N$ .*

383 **Proof.** 1. Immediate consequence of Proposition 18 and Proposition 17.

384 2. Follows from confluence of  $\beta\mathcal{R}_{EPTS}$  and also Proposition 18 and Proposition 17. ◀

385 Note that for part 2 we really need  $\beta\mathcal{R}_{EPTS}$  to be confluent. Indeed, If  $\llbracket M \rrbracket \hookleftarrow N$  then  
 386 we cannot apply  $|-|$  to  $N$  because it might not be an invertible form.

## 387 7.2 Conservativity

388 Before showing conservativity, we show the following auxiliary result, saying that every  $\beta$   
 389 normal term  $M$  that has type  $\Pi x : A.B$  in  $\llbracket \Gamma \rrbracket$  is an abstraction.

390 ▶ **Lemma 21.** *Let  $M$  be in  $\beta$ -normal form. If  $\llbracket \Gamma \rrbracket \vdash_{DK} M : \Pi x : A.B$  then  $M = \lambda x : A'.N$  with  
 391  $A' \equiv A$  and  $\llbracket \Gamma \rrbracket, x : A \vdash_{DK} N : B$ .*

392 **Proof.** By induction on  $M$ .  $M$  cannot neither be a variable or constant, as there is no  
 393  $x : C \in \llbracket \Gamma \rrbracket$  or  $c[\Delta] : C \in \Sigma_{EPTS}$  with  $C \equiv \Pi x : A.B$ . If  $M = M_1 M_2$ , then  $M_1$  has a type of the  
 394 form  $\Pi x' : A'.B'$ . By IH we get that  $M_1$  is an abstraction, which contradicts the fact that  $M$   
 395 is in  $\beta$  normal form.

396 Therefore,  $M$  is an abstraction, of the form  $M = \lambda x : A'.N$ . By inversion of typing, we  
 397 thus have  $\llbracket \Gamma \rrbracket, x : A' \vdash_{DK} N : B'$  with  $A' \equiv A$  and  $B' \equiv B$ . We can then use *Conv in context*  
 398 for DK (Theorem 30) and *Conv* to derive  $\llbracket \Gamma \rrbracket, x : A \vdash_{DK} N : B$ . ◀

399 We are now ready to show conservativity for  $\beta$  normal forms. However, if we also want to  
 400 show adequacy latter, we also need to show that  $|-|$  is a kind of right inverse to  $\llbracket - \rrbracket$ . However,  
 401 because the inverse translation does not capture the information in the type annotations of  
 402 binders,  $\llbracket |M| \rrbracket = M$  does not hold.

403 ▶ **Example 22.** Take any invertible forms  $A, B$  and a term  $T$  with  $T \neq \text{El}_{s_1} A$ . Then the term  
 404  $M = \text{Prod}_{s_1, s_2} A (\lambda x : T.B)$  is sent by  $|-|$  into  $\Pi_{s_1, s_2} (|A|, [x]|B|)$ , which is then sent by  $\llbracket - \rrbracket$   
 405 into  $\text{Prod}_{s_1, s_2} \llbracket |A| \rrbracket (\lambda x : \text{El}_{s_1} \llbracket |A| \rrbracket. \llbracket |B| \rrbracket)$ . Therefore, even if have  $\llbracket |B| \rrbracket = B$  and  $\llbracket |A| \rrbracket = A$ ,  
 406 we still have  $T \neq \text{El}_{s_1} A$ , implying  $M \neq \llbracket |M| \rrbracket$ . However, if  $M$  is typable, then by typing  
 407 constraints we should nevertheless have  $T \equiv \text{El}_{s_1} A$ .

Therefore, while proving conservativity we will show a weaker property: for the well-typed terms we are interested in,  $|-|$  is a right inverse up to the following “hidden” conversion.

► **Definition 23** (Hidden step). *We say that a rewriting step  $M \hookrightarrow N$  is hidden when it happens on the type annotation of a binder. More formally, we should have a rewriting context  $C(-)$  and terms  $A, A', P$  such that  $A \hookrightarrow A'$ ,  $M = C(\lambda x : A.P)$  and  $N = C(\lambda x : A'.P)$ . We denote the conversion generated by such rules by  $\equiv_H$ .*

We now have all ingredients to show that the encoding is conservative for  $\beta$  normal forms.

► **Theorem 24** (Conservativity of  $\beta$  normal forms). *Suppose  $\Gamma \vdash A$  type and let  $M \in \Lambda_{\text{DK}}$  be a  $\beta$  normal form st  $\llbracket \Gamma \rrbracket \vdash_{\text{DK}} M : T$ , with  $T = \text{El}_{s_A} \llbracket A \rrbracket$  or  $T = U_A$ . Then  $M$  is an invertible form,  $\Gamma \vdash |M| : A$  and  $\llbracket |M| \rrbracket \equiv_H M$ .*

**Proof.** By induction on  $M$ .

**Case  $M = \lambda x : A'.M'$**  : By inversion we have  $M : \Pi x : A'_1.A'_2$  with  $T \equiv \Pi x : A'_1.A'_2$ . Because  $\mathcal{R}_{\text{EPTS}}$  is arity preserving, this implies that  $T$  is of the form  $\Pi x : A_1.A_2$ , which cannot hold. Thus, this case is impossible.

**Case  $M = M_1 M_2$**  : As  $M$  is in beta normal form, its head symbol is a constant or variable. However, there is no  $c[\Delta] : C \in \Sigma$  or  $x : C \in \Gamma$  with  $C$  convertible to a dependent product type. Hence, this case is impossible.

**Case  $M = x$**  : If  $M = x$ , by inversion of typing there is  $x : \text{El}_{s_B} \llbracket B \rrbracket \in \llbracket \Gamma \rrbracket$  with  $T \equiv \text{El}_{s_B} \llbracket B \rrbracket$ . Therefore, we deduce  $A \equiv B$  and thus we can derive  $\Gamma \vdash x : A$  by applying VAR with  $x : B \in \Gamma$ , then CONV with  $A \equiv B$  and  $\Gamma \vdash A$  type.

**Case  $M = c[\vec{M}]$**  : We proceed by case analysis on  $c$ . We present only case  $c = \text{Prod}_{s_1, s_2}$  here and refer to the long version for all the details.

► **Note 25.** In the following, to improve readability we omit the typing hypothesis when applying CONV. However, all such uses can be justified.

**Case  $c = \text{Prod}_{s_1, s_2}$**  : By inversion of typing, we have

1.  $\vec{M} = M_1 M_2$
2.  $\llbracket \Gamma \rrbracket \vdash_{\text{DK}} M_1 : U_{s_1}$
3.  $\llbracket \Gamma \rrbracket \vdash_{\text{DK}} M_2 : \text{El}_{s_1} M_1 \rightarrow U_{s_2}$
4.  $T \equiv U_{s_3}$

As  $M_1$  is in  $\beta$  normal form, by IH  $M_1$  is an invertible form,  $\Gamma \vdash |M_1| : s_1$  and  $\llbracket |M_1| \rrbracket \equiv_H M_1$ .

By Lemma 21 applied to 2, we get  $M_2 = \lambda x : B.N$  and  $B \equiv \text{El}_{s_1} M_2$  with  $\llbracket \Gamma \rrbracket, x : \text{El}_{s_1} M_1 \vdash N : U_{s_2}$ . Because  $M_1 \equiv \llbracket |M_1| \rrbracket$ , we have  $\llbracket \Gamma \rrbracket, x : \text{El}_{s_1} \llbracket |M_1| \rrbracket \vdash N : U_{s_2}$ . As  $\Gamma \vdash |M_1| : s_1$  we have  $\Gamma, x : |M_1|$  well-formed and thus by IH  $N$  is an invertible form and we have  $\llbracket |N| \rrbracket \equiv_H N$  and  $\Gamma, x : |M_1| \vdash |N| : s_2$ .

Therefore, by PROD we have  $\Gamma \vdash \Pi_{s_1, s_2}(|M_1|, [x]|N|) : s_3$ , and then by CONV with  $A \equiv s_3$  we conclude  $\Gamma \vdash \Pi_{s_1, s_2}(|M_1|, [x]|N|) : A$ . Finally, as  $M_1 \equiv_H \llbracket |M_1| \rrbracket$ ,  $N \equiv_H \llbracket |N| \rrbracket$  and  $B \equiv \text{El}_{s_1} M_1 \equiv \text{El}_{s_1} \llbracket |M_1| \rrbracket$ , we conclude

$$\begin{aligned} M &= \text{Prod}_{s_1, s_2} M_1 M_2 = \text{Prod}_{s_1, s_2} M_1 (\lambda x : B.N) \\ &\equiv_H \text{Prod}_{s_1, s_2} \llbracket |M_1| \rrbracket (\lambda x : \text{El}_{s_1} \llbracket |M_1| \rrbracket. \llbracket |N| \rrbracket) = \llbracket \Pi_{s_1, s_2}(|M_1|, [x]|N|) \rrbracket = \llbracket |M| \rrbracket \quad \blacktriangleleft \end{aligned}$$

By *Basic properties* (Proposition 10),  $\beta$  is strongly normalizing and type preserving. Therefore from the previous result we can immediately get full conservativity.

► **Theorem 26** (Conservativity). *Let  $\Gamma \vdash A$  type,  $M \in \Lambda_{\text{DK}}$  such that  $\llbracket \Gamma \rrbracket \vdash_{\text{DK}} M : T$ , with  $T = \text{El}_{s_A} \llbracket A \rrbracket$  or  $T = U_A$ . We have  $\Gamma \vdash |NF_{\beta}(M)| : A$  and  $M \hookrightarrow_{\beta}^* NF_{\beta}(M) \equiv_H \llbracket |NF_{\beta}(M)| \rrbracket$ .*

452 Note that this also gives us a straightforward algorithm to invert terms: it suffices to  
 453 normalize with  $\beta$  and then apply  $|-|$ .

### 454 7.3 Adequacy

455 If we write  $\Lambda(\Gamma \vdash_{EPTS} \_ : A)$  for the set of  $M \in \Lambda_{EPTS}$  st  $\Gamma \vdash M : A$  and  $\Lambda_{NF}(\Gamma \vdash_{DK} \_ : T)$  for  
 456 the set of  $M \in \Lambda_{DK}$  in  $\beta$  normal form st  $\Gamma \vdash_{DK} M : T$ , we can show our adequacy theorem. This  
 457 result follows by simply putting together *Basic properties* (Proposition 10), *Preservation of*  
 458 *computation* (Lemma 12), *Soundness* (Theorem 14), *Reflection of computation* (Corollary 20)  
 459 and *Conservativity* (Theorem 26).

460 ▶ **Theorem 27** (Computational adequacy). *For  $A, \Gamma$  with  $\Gamma \vdash A$  type, let  $T = U_A$  if  $A$  is a top*  
 461 *sort, otherwise  $T = El_{s_A} \llbracket A \rrbracket$ . We have a bijection*

$$462 \quad \Lambda(\Gamma \vdash_{EPTS} \_ : A) \simeq \Lambda_{NF}(\llbracket \Gamma \rrbracket \vdash_{DK} \_ : T) / \equiv_H$$

463 *given by  $\llbracket - \rrbracket$  and  $|-|$ . It is compositional in the sense that  $\llbracket - \rrbracket$  commutes with substitution. It*  
 464 *is computational in the sense that  $M \hookrightarrow^* N$  iff  $\llbracket M \rrbracket \hookrightarrow^* \llbracket N \rrbracket$ . Moreover, any  $M$  satisfying*  
 465  *$\llbracket \Gamma \rrbracket \vdash_{DK} M : T$  has such a  $\beta$  normal form.*

## 466 8 Representing systems with infinite sorts

467 We have presented an encoding of EPTSs in DEDUKTI that is sound, conservative and  
 468 adequate. However when using it in practice with DEDUKTI implementations we run into  
 469 problems when representing systems with infinite sorts, such as in Martin-Löf's Type Theory  
 470 or the Extended Calculus of Constructions. Indeed, in this case our encoding needs an  
 471 infinite number of constant and rule declarations, which cannot be made in practice.

472 One possible solution is to approximate the infinite sort structure by a finite one. Most  
 473 proofs in infinite sort systems probably do not use more than 10 sorts, therefore we could  
 474 truncate the representation while still providing a good encoding of the system.

475 A different approach proposed in [1][23] is to internalize the indices of  $Prod_{s_1, s_2}, El_{s_1}, \dots$   
 476 and represent them inside DEDUKTI. In order to apply this method, we chose to stick with  
 477 systems in which  $\mathcal{A}, \mathcal{R}$  are total functions  $\mathcal{S} \rightarrow \mathcal{S}$  and  $\mathcal{S} \times \mathcal{S} \rightarrow \mathcal{S}$  respectively. Note that  
 478 this is true for almost all infinite sort systems used in practice, and this will greatly simplify  
 479 our presentation.

480 We can now declare a constant  $\hat{\mathcal{S}}$  to represent the type of sorts in  $\mathcal{S}$  and two constants  
 481  $\hat{\mathcal{A}}, \hat{\mathcal{R}}$  to represent the functions  $\mathcal{A}, \mathcal{R}$ . Then, each of our previously declared families of  
 482 constants now becomes a single one, by taking arguments of type  $\hat{\mathcal{S}}$ . The same happens with  
 483 the rewrite rules. This leads to the theory presented in Figure 3, which we call  $(\Sigma_{EPTS}^{\mathcal{S}}, \mathcal{R}_{EPTS}^{\mathcal{S}})$ .

484 This theory needs of course to be completed case by case, so that  $\hat{\mathcal{S}}, \hat{\mathcal{A}}, \hat{\mathcal{R}}$  correctly  
 485 represent  $\mathcal{S}, \mathcal{A}, \mathcal{R}$ . For this to hold, each sort  $s \in \mathcal{S}$  should have a representation  $\dot{s} : \hat{\mathcal{S}}$ , and  
 486 this should restrict to a bijection when considering only the closed normal forms of type  $\hat{\mathcal{S}}$ .  
 487 Moreover, we should add rewrite rules such that  $\mathcal{A}(s_1) = s_2$  iff  $\hat{\mathcal{A}} \dot{s}_1 \equiv \dot{s}_2$  and  $\mathcal{R}(s_1, s_2) = s_3$   
 488 iff  $\hat{\mathcal{R}} \dot{s}_1 \dot{s}_2 \equiv \dot{s}_3$ .

489 In order to understand intuitively these conditions, let's look at an example.

490 ▶ **Example 28.** The sort structure of Martin-Löf's Type Theory is given by the specification  
 491  $\mathcal{S} = \mathbb{N}$ ,  $\mathcal{A}(x) = x + 1$  and  $\mathcal{R}(x, y) = \max\{x, y\}$ . We can represent this in DEDUKTI by  
 492 declaring constants  $z : \hat{\mathcal{S}}$ ,  $s[n : \hat{\mathcal{S}}] : \hat{\mathcal{S}}$  and rewrite rules  $\hat{\mathcal{A}} x \hookrightarrow s x$ ,  $\hat{\mathcal{R}} z x \hookrightarrow x$ ,  $\hat{\mathcal{R}} x z \hookrightarrow x$   
 493 and  $\hat{\mathcal{R}} (s x) (s y) \hookrightarrow s (\hat{\mathcal{R}} x y)$ . Then the closed normal forms of type  $\hat{\mathcal{S}}$  are in bijection  
 494 with  $\mathcal{S}$ , and we have  $\mathcal{A}(s_1) = s_2$  iff  $\hat{\mathcal{A}} s_1 \equiv s_2$  and  $\mathcal{R}(s_1, s_2) = s_3$  iff  $\hat{\mathcal{R}} s_1 s_2 \equiv s_3$ .

$$\begin{array}{ll}
\hat{S} : \text{TYPE} & U[s : \hat{S}] : \text{TYPE} \\
\hat{\mathcal{A}}[s_1 : \hat{S}] : \hat{S} & El[s : \hat{S}; A : U s] : \text{TYPE} \\
\hat{\mathcal{R}}[s_1 : \hat{S}; s_2 : \hat{S}] : \hat{S} & u[s : \hat{S}] : U (\hat{\mathcal{A}} s) \\
& El s' (u s) \hookrightarrow_{u\text{-red}} U s \\
\\
Prod[s_1 : \hat{S}; s_2 : \hat{S}; A : U s_1; B : El s_1 A \rightarrow U s_2] : U (\hat{\mathcal{R}} s_1 s_2) & \\
abs[s_1 : \hat{S}; s_2 : \hat{S}; A : U s_1; B : El s_1 A \rightarrow U s_2; N : \Pi x : El s_1 A. El s_2 (B x)] & \\
& : El (\hat{\mathcal{R}} s_1 s_2) (Prod s_1 s_2 A B) \\
app[s_1 : \hat{S}; s_2 : \hat{S}; A : U s_1; B : El s_1 A \rightarrow U s_2; M : El (\hat{\mathcal{R}} s_1 s_2) (Prod s_1 s_2 A B); N : El s_1 A] & \\
& : El s_2 (B N) \\
app s_1 s_2 A B (abs s'_1 s'_2 A' B' M) N \hookrightarrow_{beta} M N
\end{array}$$

■ **Figure 3** Definition of the theory  $(\Sigma_{\text{EPTS}}^S, \mathcal{R}_{\text{EPTS}}^S)$

Now one can proceed as before with the proofs of soundness, conservativity and adequacy, which follow the same idea as the previously presented ones. However, it is quite unsatisfying that we have to redo all the work of Sections 6 and 7 another time, and therefore one can wonder if we can reuse the results we already have about the first encoding.

Note that one may intuitively think of the  $(\Sigma_{\text{EPTS}}^S, \mathcal{R}_{\text{EPTS}}^S)$  as a “hidden implementation” of  $(\Sigma_{\text{EPTS}}, \mathcal{R}_{\text{EPTS}})$ . In this case, it should be possible to take a proof written in the  $(\Sigma_{\text{EPTS}}, \mathcal{R}_{\text{EPTS}})$  and “implement” it in the  $(\Sigma_{\text{EPTS}}^S, \mathcal{R}_{\text{EPTS}}^S)$ . Following this intuition, we define in the long version a notion of *theory morphism* which allows us to show the soundness of this new encoding by means of morphism from  $(\Sigma_{\text{EPTS}}, \mathcal{R}_{\text{EPTS}})$  to  $(\Sigma_{\text{EPTS}}^S, \mathcal{R}_{\text{EPTS}}^S)$ .

Nevertheless, this definition has too strong requirements and cannot be used to define a morphism in the other direction to show conservativity. Therefore, it is still an open problem for us to find a notion of morphism allowing to show the equivalence between the encodings. For the time being, in order to show conservativity of this new encoding one unfortunately has to redo the work of Section 7, which is doable but unsatisfying.

## 9 The encoding in practice

Our encoding satisfies very nice theoretical properties, but when using it in practice it becomes quite annoying to have to explicit all the information needed in  $app_{s_1, s_2}$  and  $abs_{s_1, s_2}$ . Worst, when performing translations from other systems where those parameters are not explicit we would then have to compute them during the translation. Thankfully, LAMBD-API[10], an implementation of DEDUKTI, allows us to solve this by declaring some arguments as implicit, so they are only calculated internally.

Using the encoding of Figure 3 we can mark for instance the arguments  $s_1, s_2, A$  of  $Prod$  as implicit. We can then also rename  $Prod$  into  $\Pi'$ ,  $abs$  into  $\lambda'$ ,  $app$  into  $\blacksquare$  and use another LAMBD-API feature allowing to mark  $\Pi', \lambda'$  as quantifier and  $\blacksquare$  as infix left. This then allows us to represent  $\Pi x : A.B$  as  $\Pi' x : El \llbracket A \rrbracket. \llbracket B \rrbracket$ ,  $\lambda x : A.B$  as  $\lambda' x : El \llbracket A \rrbracket. \llbracket B \rrbracket$  and  $M N$  as  $\llbracket M \rrbracket \blacksquare \llbracket N \rrbracket$ . Using these notations, we can write terms in the encoding in a very natural way,

521 and we refer to <sup>5</sup> for a set of examples of this.

522 However, as DEDUKTI also aims to be used in practice for sharing real libraries between  
 523 proof assistants, we also tested how our approach copes with more practical scenarios. We  
 524 provide in <sup>6</sup> a benchmark of Fermat's little theorem library in DEDUKTI[22], where we  
 525 compare the traditional encoding with an adequate version that applies the ideas of our  
 526 approach.<sup>7</sup> As we can see, the move from the traditional to the adequate version introduces a  
 527 considerable performance hit. The standard DEDUKTI implementation, which is our reference  
 528 here, takes 17 times more time to typecheck the files. This is probably caused by the insertion  
 529 of type parameters  $A$  and  $B$  in  $abs_{s_A, s_B}$  and  $app_{s_A, s_B}$ , which are not needed in traditional  
 530 encodings.

531 Nevertheless, DEDUKTI is still able to typecheck our encoding in a very reasonable time,  
 532 showing that our approach is indeed usable in practical scenarios, even if it is not the most  
 533 performing one. Moreover, as our encoding is mainly intended to be used to check proofs,  
 534 and not with interactive proof development, immediacy of the result is not essential and thus  
 535 it can be reasonable to trade performance for better theoretical properties. Still, we plan in  
 536 the future to look at techniques to improve our performances. In particular, DEDUKTI does  
 537 not implement sharing, and doing so would probably improve drastically our performance,  
 538 as the parameter annotations in  $app_{s_A, s_B}$  and  $abs_{s_A, s_B}$  carry a lot of repetition.

## 539 10 Conclusion

540 By separating the framework's abstraction and application from the ones of the encoded  
 541 system, we have proposed a new paradigm for DEDUKTI encodings. Our approach offers  
 542 much more well-behaved encodings, whose conservativity can be showed in a much more  
 543 straightforward way and which feature adequacy theorems, something that was missing from  
 544 traditional DEDUKTI encodings. However, differently from the ELF approach, our encoding  
 545 is also computational. Therefore, our method combines the adequacy of ELF encodings  
 546 with the computational aspect of DEDUKTI encodings.

547 By decoupling the framework's  $\beta$  from the rewriting of the encoded system, our approach  
 548 allows to show the expected properties of the encoding without requiring to show that the  
 549 encoded system terminates. Indeed, our adequacy result concerns all functional EPTS, even  
 550 non terminating ones, such as the one with  $Type : Type$ . This sets our work apart from [9],  
 551 whose conservativity proof requires the encoded system to be normalizing.

552 This work opens many other directions we would like to explore. We believe that our  
 553 technique can be extended to craft adequate and computational encodings of type theories with  
 554 much more complex features, such as (co)inductive types, universe polymorphism, predicate  
 555 subtyping and others. For instance, in the case of inductive types no type-level rewriting  
 556 rules need to be added, thus  $\beta$  is SN in DEDUKTI (Theorem 5) would apply. Therefore, we  
 557 could repeat the same technique of normalizing only with  $\beta$  to show conservativity.

558 However, we would be particularly interested to see if we could take a general definition  
 559 of type theories covering most of these features (maybe in the lines of [5]). This would allow  
 560 us to define a single encoding which could be applied to encode various features, and thus  
 561 would saves us from redoing similar proofs multiple times.

<sup>5</sup> <https://github.com/thiagofelicissimo/examples-encodigs>

<sup>6</sup> <https://github.com/thiagofelicissimo/encoding-benchmarking>

<sup>7</sup> Because the underlying logic of the library is not a PTS, this encoding is not exactly the one we present here. However, it uses the same ideas discussed, and the same proof strategy to show adequacy applies.



## References

- 1 Ali Assaf. *A framework for defining computational higher-order logics*. Theses, École polytechnique, September 2015. URL: <https://pastel.archives-ouvertes.fr/tel-01235303>.
- 2 Ali Assaf. Conservativity of embeddings in the lambda pi calculus modulo rewriting. In *13th International Conference on Typed Lambda Calculi and Applications (TLCA 2015)*. Schloss Dagstuhl-Leibniz-Zentrum fuer Informatik, 2015.
- 3 Ali Assaf, Guillaume Burel, Raphaël Cauderlier, D Delahaye, G Dowek, C Dubois, F Gilbert, P Halmagrand, O Hermant, and R Saillard. Dedukti: a logical framework based on the  $\lambda$   $\pi$ -calculus modulo theory. Manuscript, 2016.
- 4 Gilles Barthe. The relevance of proof-irrelevance. In Kim G. Larsen, Sven Skyum, and Glynn Winskel, editors, *Automata, Languages and Programming*, pages 755–768, Berlin, Heidelberg, 1998. Springer Berlin Heidelberg.
- 5 Andrej Bauer, Philipp G. Haselwarter, and Peter LeFanu Lumsdaine. A general definition of dependent type theories, 2020. [arXiv:2009.05539](https://arxiv.org/abs/2009.05539).
- 6 Frédéric Blanqui. *Théorie des types et réécriture. (Type theory and rewriting)*. PhD thesis, University of Paris-Sud, Orsay, France, 2001. URL: <https://tel.archives-ouvertes.fr/tel-00105522>.
- 7 Frédéric Blanqui. Type safety of rewrite rules in dependent types. In *FSCD 2020 - 5th International Conference on Formal Structures for Computation and Deduction*, volume 167, page 14, Paris, France, June 2020. URL: <https://hal.inria.fr/hal-02981528>, doi: 10.4230/LIPIcs.FSCD.2020.13.
- 8 Frédéric Blanqui, Guillaume Genestier, and Olivier Hermant. Dependency pairs termination in dependent type theory modulo rewriting. In Herman Geuvers, editor, *4th International Conference on Formal Structures for Computation and Deduction, FSCD 2019, June 24-30, 2019, Dortmund, Germany*, volume 131 of *LIPIcs*, pages 9:1–9:21. Schloss Dagstuhl - Leibniz-Zentrum für Informatik, 2019. doi:10.4230/LIPIcs.FSCD.2019.9.
- 9 Denis Cousineau and Gilles Dowek. Embedding pure type systems in the lambda-pi-calculus modulo. In Simona Ronchi Della Rocca, editor, *Typed Lambda Calculi and Applications*, pages 102–117, Berlin, Heidelberg, 2007. Springer Berlin Heidelberg.
- 10 Deducteam. *Lambdapi*. <https://github.com/Deducteam/lambdapi>.
- 11 Gilles Dowek. Models and termination of proof reduction in the lambda pi-calculus modulo theory. In *ICALP*, 2017.
- 12 Thiago Felicissimo. No need to be implicit!
- 13 Gaspard Ferey. *Higher-Order Confluence and Universe Embedding in the Logical Framework*. Theses, Université Paris-Saclay, June 2021. URL: <https://tel.archives-ouvertes.fr/tel-03418761>.
- 14 Guillaume Genestier. *Dependently-Typed Termination and Embedding of Extensional Universe-Polymorphic Type Theory using Rewriting*. PhD thesis, 2020. Thèse de doctorat dirigée par Blanqui, Frédéric et Hermant, Olivier Informatique université Paris-Saclay 2020. URL: <http://www.theses.fr/2020UPASG045>.
- 15 Jan Herman Geuvers. *Logics and type systems*. [Sl: sn], 1993.
- 16 Robert Harper. An equational logical framework for type theories. *arXiv preprint arXiv:2106.01484*, 2021.
- 17 Robert Harper, Furio Honsell, and Gordon Plotkin. A framework for defining logics. *J. ACM*, 40(1):143–184, January 1993. doi:10.1145/138027.138060.
- 18 Gabriel Hondet and Frédéric Blanqui. Encoding of Predicate Subtyping with Proof Irrelevance in the  $\lambda\Pi$ -Calculus Modulo Theory. In Ugo de'Liguoro, Stefano Berardi, and Thorsten Altenkirch, editors, *26th International Conference on Types for Proofs and Programs (TYPES 2020)*, volume 188 of *Leibniz International Proceedings in Informatics (LIPIcs)*, pages 6:1–6:18, Dagstuhl, Germany, 2021. Schloss Dagstuhl – Leibniz-Zentrum für Informatik. URL: <https://drops.dagstuhl.de/opus/volltexte/2021/13885>, doi:10.4230/LIPIcs.TYPES.2020.6.



- 613 19 Jan Willem Klop, Vincent van Oostrom, and Femke van Raamsdonk. Combinatory reduction  
 614 systems: introduction and survey. *Theoretical Computer Science*, 121(1):279–308, 1993. URL:  
 615 <https://www.sciencedirect.com/science/article/pii/0304397593900917>, doi:[https://doi.org/10.1016/0304-3975\(93\)90091-7](https://doi.org/10.1016/0304-3975(93)90091-7).  
 616
- 617 20 Paul-André Mellies and Benjamin Werner. A generic normalisation proof for pure type systems.  
 618 In Eduardo Giménez and Christine Paulin-Mohring, editors, *Types for Proofs and Programs*,  
 619 pages 254–276, Berlin, Heidelberg, 1998. Springer Berlin Heidelberg.
- 620 21 Vincent Siles and Hugo Herbelin. Pure type system conversion is always typable. *Journal of*  
 621 *Functional Programming*, 22:153 – 180, 2012.
- 622 22 François Thiré. Sharing a library between proof assistants: Reaching out to the HOL family. In  
 623 Frédéric Blanqui and Giselle Reis, editors, *Proceedings of the 13th International Workshop on*  
 624 *Logical Frameworks and Meta-Languages: Theory and Practice, LFMTP@FSCD 2018, Oxford,*  
 625 *UK, 7th July 2018*, volume 274 of *EPTCS*, pages 57–71, 2018. doi:10.4204/EPTCS.274.5.
- 626 23 François Thiré. *Interoperability between proof systems using the logical framework Dedukti*.  
 627 PhD thesis, ENS Paris-Saclay, 2020.

## 628 A Typing rules and metatheory of Dedukti

- 629 ▶ **Proposition 29** (Basic properties). *Suppose  $\hookrightarrow_{\beta\mathcal{R}}$  is confluent.*
- 630 1. *Weakening: If  $\Sigma; \Gamma \vdash M : A$  and  $\Gamma \sqsubseteq \Gamma'$  then  $\Sigma; \Gamma' \vdash M : A$*
- 631 2. *Well-typedness of contexts: If  $\Sigma; \Gamma$  well-formed then for all  $x : B \in \Gamma$ ,  $\Sigma; \Gamma \vdash B : \text{TYPE}$*
- 632 3. *Inversion of typing: Suppose  $\Sigma; \Gamma \vdash M : A$*
- 633 ■ *If  $M = x$  then  $x : A' \in \Gamma$  and  $A \equiv A'$*
- 634 ■ *If  $M = c[\vec{N}]$  then  $c[\Delta] : A' \in \Sigma$ ,  $\Sigma; \Delta \vdash A' : s$ ,  $\Sigma; \Gamma \vdash \vec{N} : \Delta$  and  $A'(\vec{N}/\Delta) \equiv A$*
- 635 ■ *If  $M = \text{TYPE}$  then  $A \equiv \text{KIND}$*
- 636 ■  *$M = \text{KIND}$  is impossible*
- 637 ■ *If  $M = \Pi x : A_1. A_2$  then  $\Sigma; \Gamma \vdash A_1 : \text{TYPE}$ ,  $\Sigma; \Gamma, x : A_1 \vdash A_2 : s$  and  $s \equiv A$*
- 638 ■ *If  $M = M_1 M_2$  then  $\Sigma; \Gamma \vdash M_1 : \Pi x : A_1. A_2$ ,  $\Sigma; \Gamma \vdash M_2 : A_1$  and  $A_2(M_2/x) \equiv A$*
- 639 ■ *If  $M = \lambda x : B. N$  then  $\Sigma; \Gamma \vdash B : \text{TYPE}$ ,  $\Sigma; \Gamma, x : B \vdash C : s$ ,  $\Sigma; \Gamma, x : B \vdash N : C$  and*  
 640  *$A \equiv \Pi x : B. C$*
- 641 4. *Uniqueness of types: If  $\Sigma; \Gamma \vdash M : A$  and  $\Sigma; \Gamma \vdash M : A'$  then  $A \equiv A'$*
- 642 5. *Well-sortedness: If  $\Sigma; \Gamma \vdash M : A$  then  $\Sigma; \Gamma \vdash A : s$  or  $A = \text{TYPE}$ ,  $s = \text{KIND}$*
- 643 ▶ **Theorem 30** (Conv in context for DK). *Let  $A \equiv A'$  with  $\Sigma; \Gamma \vdash A' : s$ . We have*
- 644 ■  $\Sigma; \Gamma, x : A, \Gamma' \text{ WF} \Rightarrow \Sigma; \Gamma, x : A', \Gamma' \text{ WF}$
- 645 ■  $\Sigma; \Gamma, x : A, \Gamma' \vdash M : B \Rightarrow \Sigma; \Gamma, x : A', \Gamma' \vdash M : B$

646 **Proof.** Structural induction on the derivation tree, using weakening for the case **Var**. ◀

- 647 ▶ **Proposition 31** (Reduce type in judgement). *Suppose  $\hookrightarrow_{\beta\mathcal{R}}$  is confluent and satisfies*  
 648 *subject reduction. Then if  $\Sigma; \Gamma \vdash_{\lambda\Pi} M : A$  and  $A \hookrightarrow^* A'$  we have  $\Sigma; \Gamma \vdash_{\lambda\Pi} M : A'$ .*

## 649 B Metatheory of Explicitly-typed Pure Type Systems

650 We have the following properties for functional EPTSs. We refer to [12] for the proofs.

- 651 ▶ **Proposition 32** (Weakening). *Let  $\Gamma \sqsubseteq \Gamma'$ . We have*
- 652 ■  $\Gamma, x : A \text{ well-formed} \Rightarrow \Gamma', x : A \text{ well-formed when } x \notin \Gamma'$
- 653 ■  $\Gamma \vdash M : A \Rightarrow \Gamma' \vdash M : A$
- 654 ▶ **Proposition 33** (Inversion). *If  $\Gamma \vdash M : C$  then*
- 655 ■ *If  $M = x$ , then*

## 23:18 Adequate and computational encodings in the logical framework Dedukti

- 656     ■  $\Gamma$  well-formed *with a smaller derivation tree*
- 657     ■ *there is  $x$  with  $x : A \in \Gamma$  and  $C \equiv A$*
- 658 ■ *If  $M = s$ , then there is  $s'$  with  $(s, s') \in \mathcal{A}$  and  $C \equiv s'$*
- 659 ■ *If  $M = \Pi_{s_1, s_2}(A, [x]B)$  then*
  - 660     ■  $\Gamma \vdash A : s_1$  *with a smaller derivation tree*
  - 661     ■  $\Gamma, x : A \vdash B : s_2$  *with a smaller derivation tree*
  - 662     ■ *there is  $s_3$  with  $(s_1, s_2, s_3) \in \mathcal{R}$  and  $C \equiv s_3$*
- 663 ■ *If  $M = \lambda_{s_1, s_2}(A, [x]B, [x]N)$  then*
  - 664     ■  $\Gamma \vdash A : s_1$  *with a smaller derivation tree*
  - 665     ■  $\Gamma, x : A \vdash B : s_2$  *with a smaller derivation tree*
  - 666     ■ *there is  $s_3$  with  $(s_1, s_2, s_3) \in \mathcal{R}$*
  - 667     ■  $\Gamma, x : A \vdash N : B$  *with a smaller derivation tree*
  - 668     ■  $C \equiv \Pi_{s_1, s_2}(A, [x]B)$
- 669 ■ *If  $M = \mathcal{O}_{s_1, s_2}(A, [x]B, N_1, N_2)$  then*
  - 670     ■  $\Gamma \vdash A : s_1$  *with a smaller derivation tree*
  - 671     ■  $\Gamma, x : A \vdash B : s_2$  *with a smaller derivation tree*
  - 672     ■ *there is  $s_3$  with  $(s_1, s_2, s_3) \in \mathcal{R}$*
  - 673     ■  $\Gamma \vdash N_1 : A$  *with a smaller derivation tree*
  - 674     ■  $\Gamma \vdash N_2 : \Pi_{s_1, s_2}(A, [x]B)$  *with a smaller derivation tree*
  - 675     ■  $C \equiv B(N_2/x)$
- 676 ▶ **Proposition 34** (Uniqueness of types). *If  $\Gamma \vdash M : A$  and  $\Gamma \vdash M : B$  we have  $A \equiv B$ .*
- 677 ▶ **Corollary 35** (Uniqueness of sorts). *If  $\Gamma \vdash M : s$  and  $\Gamma \vdash M : s'$  we have  $s = s'$ .*
- 678 ▶ **Proposition 36** (Conv in context). *Let  $A \equiv A'$  and  $\Gamma \vdash A' : s$ . We have*
  - 679     ■  $\Gamma, x : A, \Gamma'$  well-formed  $\Rightarrow \Gamma, x : A', \Gamma'$  well-formed
  - 680     ■  $\Gamma, x : A, \Gamma' \vdash M : B \Rightarrow \Gamma, x : A', \Gamma' \vdash M : B$
- 681 ▶ **Proposition 37** (Substitution in judgment). *Let  $\Gamma \vdash N : A$ . We have*
  - 682     ■  $\Gamma, x : A, \Gamma'$  well-formed  $\Rightarrow \Gamma, \Gamma'(N/x)$  well-formed
  - 683     ■  $\Gamma, x : A, \Gamma' \vdash M : B \Rightarrow \Gamma, \Gamma'(N/x) \vdash M(N/x) : B(N/x)$