Proofs for Free in the $\lambda\Pi$-Calculus Modulo Theory

LFMTP 2024

Thomas Traversié

The landscape of proof systems

- Many different proof systems, data structures and encodings

Proof systems

Data structures and encodings

Natural numbers   Integers

Reals   Sets

- Improve **interoperability** and re-usability of proofs
  - Easily exchange proofs between proof systems
  - Easily exchange proofs between encodings

Improving interoperability

- The $\lambda\Pi$-calculus modulo theory [Cousineau and Dowek, 2007]
  - Logical framework used for **exchanging proofs between systems**
  - Implemented in the Dedukti proof language
- Parametricity [Bernardy *et al.*, 2010]
  - Method used for **transferring proofs between encodings**
  - TROCQ, a COQ plugin for proof transfer [Cohen *et al.*, 2024]

Goal: transfer proofs between different theories of the $\lambda\Pi$-calculus modulo theory

Contribution

- We define an **interpretation of theories** of the $\lambda\Pi$-calculus modulo theory
  - For theories that feature basic notions
  - When the source theory can be **embedded** into the target theory

- We show how the proofs of the source can be **transferred** to the target

- We give examples of interpretations in Dedukti

`https://github.com/thomastraversie/InterpDK`

Outline

Outline

The $\lambda\Pi$-calculus modulo theory

- λ-calculus extended with **dependent types** and **rewrite rules**

- Syntax

Sorts	$s ::= \texttt{TYPE} \mid \texttt{KIND}$
Terms	$t, u, A, B ::= c \mid x \mid s \mid \Pi(x : A).\ B \mid \lambda(x : A).\ t \mid t\ u$
Signatures	$\Sigma ::= \langle\rangle \mid \Sigma, c : A \mid \Sigma, \ell \hookrightarrow r$
Contexts	$\Gamma ::= \langle\rangle \mid \Gamma, x : A$

$\Pi x : A.\ B$ written $A \to B$ if x not in B

- Theory $\mathbb{T}$ given by a well-defined signature Σ

Typing rules

$$\frac{\Gamma \vdash A : \texttt{TYPE} \qquad \Gamma, x : A \vdash B : s \qquad \Gamma, x : A \vdash t : B}{\Gamma \vdash \lambda(x : A).\ t : \Pi(x : A).\ B}\ [\textsc{Abs}]$$

$$\frac{\Gamma \vdash t : \Pi(x : A).\ B \qquad \Gamma \vdash u : A}{\Gamma \vdash t\ u : B[x \mapsto u]}\ [\textsc{App}]$$

Conversion $\equiv_{\beta\Sigma}$ generated by β-reduction and the rewrite rules of Σ

$$\frac{\Gamma \vdash t : A \qquad \Gamma \vdash B : s}{\Gamma \vdash t : B}\ [\textsc{Conv}]\ A \equiv_{\beta\Sigma} B$$

Prelude encoding (1)

- Notions of proposition and proof [Blanqui et al, 2023]

- Universe of **sorts** $\mathit{Set} : \mathtt{TYPE}$, injection $\mathit{El} : \mathit{Set} \to \mathtt{TYPE}$
  Sort nat : Set, natural number $n : \mathit{El}$ nat
  Sort $o : \mathit{Set}$, proposition $P : \mathit{El}\ o$

- Universe of **propositions** $\mathit{El}\ o : \mathtt{TYPE}$, injection $\mathit{Prf} : \mathit{El}\ o \to \mathtt{TYPE}$
  A proof of proposition P is of type $\mathit{Prf}\ \ P$

Prelude encoding (2)

- Desired behavior: functionality and implication

$$El\ (a \rightsquigarrow b) \hookrightarrow El\ a \rightarrow El\ b$$

$$Prf\ (a \Rightarrow b) \hookrightarrow Prf\ a \rightarrow Prf\ b$$

- Dependent functionality and implication

$$El\ (a \rightsquigarrow_d b) \hookrightarrow \Pi z : El\ a.\ El\ (b\ z)$$

$$Prf\ (a \Rightarrow_d b) \hookrightarrow \Pi z : Prf\ a.\ Prf\ (b\ z)$$

- Universal quantifiers over object-terms and proof-terms

$$Prf\ (\forall\ a\ b) \hookrightarrow \Pi z : El\ a.\ Prf\ (b\ z)$$

$$El\ (\pi\ a\ b) \hookrightarrow \Pi z : Prf\ a.\ El\ (b\ z)$$

Theories with prelude encoding

- $\mathbb{T} = \Sigma_{pre} \cup \Sigma_{\mathbb{T}}$
- Constants and rewrite rules Σ_{pre} of the prelude encoding
- Constants and rewrite rules $\Sigma_{\mathbb{T}}$ **defined by the user**
- Constraint: for every $c : A \in \Sigma_{\mathbb{T}}$, we have $\vdash A : \texttt{TYPE}$

Example: theory of natural numbers $\mathbb{T}_n$

$$\mathsf{nat} : \mathit{Set} \qquad 0_n : \mathit{El}\ \mathsf{nat} \qquad \mathsf{succ}_n : \mathit{El}\ \mathsf{nat} \to \mathit{El}\ \mathsf{nat} \qquad \geq_n : \mathit{El}\ \mathsf{nat} \to \mathit{El}\ \mathsf{nat} \to \mathit{El}\ o$$

- $\geq_n$ is reflexive, transitive and $\mathsf{succ}_n\ x \geq_n x$
- Induction principle

$$\begin{aligned} \mathsf{rec}_n : \quad & \Pi(P : \mathit{El}\ \mathsf{nat} \to \mathit{El}\ o).\ \mathit{Prf}\ (P\ 0_n) \to \\ & [\Pi(x : \mathit{El}\ \mathsf{nat}).\ \mathit{Prf}\ (P\ x) \to \mathit{Prf}\ (P\ (\mathsf{succ}_n\ x))] \to \\ & \Pi(x : \mathit{El}\ \mathsf{nat}).\ \mathit{Prf}\ (P\ x) \end{aligned}$$

- Theorem

$$\Pi(x : \mathit{El}\ \mathsf{nat}).\ \mathit{Prf}\ (\mathsf{succ}_n\ x \geq_n 0_n) \quad \checkmark$$

Example: theory of integers $\mathbb{T}_i$

$$\mathrm{int} : \mathit{Set} \qquad 0_i : \mathit{El}\ \mathrm{int} \qquad \mathrm{succ}_i : \mathit{El}\ \mathrm{int} \to \mathit{El}\ \mathrm{int} \qquad \mathrm{pred}_i : \mathit{El}\ \mathrm{int} \to \mathit{El}\ \mathrm{int}$$

$$\geq_i : \mathit{El}\ \mathrm{int} \to \mathit{El}\ \mathrm{int} \to \mathit{El}\ o$$

- Generalized induction principle

$$\begin{aligned} \mathrm{rec}_i : \quad & \Pi(x_0 : \mathit{El}\ \mathrm{int})(P : \mathit{El}\ \mathrm{int} \to \mathit{El}\ o).\ \mathit{Prf}\ (P\ x_0) \to \\ & [\Pi(x : \mathit{El}\ \mathrm{int}).\ \mathit{Prf}\ (x \geq_i x_0) \to \mathit{Prf}\ (P\ x) \to \mathit{Prf}\ (P\ (\mathrm{succ}_i\ x))] \to \\ & \Pi(x : \mathit{El}\ \mathrm{int}).\ \mathit{Prf}\ (x \geq_i x_0) \to \mathit{Prf}\ (P\ x) \end{aligned}$$

- Theorems

$$\Pi(x : \mathit{El}\ \mathrm{int}).\ \mathit{Prf}\ (\mathrm{succ}_i\ x \geq_i 0_i) \quad ✗$$

$$\Pi(x : \mathit{El}\ \mathrm{int}).\ \mathit{Prf}\ (x \geq_i 0_i) \to \mathit{Prf}\ (\mathrm{succ}_i\ x \geq_i 0_i) \quad ✓$$

Outline

Theories in the $\lambda\Pi$-calculus modulo theory

Interpretation of theories

Examples of interpretations

Conclusion

Intuition

- Goal: represent every term t of type A in the source theory $\mathbb{S}$
  by a term t^* of type A^* in the target theory $\mathbb{T}$

- Example: natural numbers and integers
  – Represent El nat by $\Sigma(z : El \text{ int}).\ Prf\ (z \geq_i 0_i)$ ✗
  – Represent El nat by El int and introduce a **predicate** ✓

- We interpret $\Pi(x : El \text{ nat}).\ Prf\ (\text{succ}_n\ x \geq_n 0_n)$ into

$$\Pi(x^* : El \text{ int}).\ \underbrace{Prf\ (x^* \geq_i 0_i)}_{\text{new assumption}} \to Prf\ (\text{succ}_i\ x^* \geq_i 0_i)$$

Interpretation of terms (1)

- We define **two translations** $t \mapsto t^*$ and $t \mapsto t^+$
  such that if $t : A$ then $t^* : A^*$ and $t^+ : A^+\ t^*$

- Definition of $t \mapsto t^*$

$$(x)^* := x^* \text{ (variable)}$$
$$(c)^* := c^* \text{ (parameter)}$$
$$\texttt{TYPE}^* := \texttt{TYPE}$$
$$\texttt{KIND}^* := \texttt{KIND}$$
$$(t\ u)^* := t^*\ u^*\ u^+$$
$$(\lambda(x : A).\ t)^* := \lambda(x^* : A^*)(x^+ : A^+\ x^*).\ t^*$$
$$(\Pi(x : A).\ B)^* := \Pi(x^* : A^*)(x^+ : A^+\ x^*).\ B^*$$

Interpretation of terms (2)

- Definition of $t \mapsto t^+$

$$
\begin{aligned}
(x)^+ &:= x^+ \text{ (variable)} \\
(c)^+ &:= c^+ \text{ (parameter)} \\
\mathtt{KIND}^+ &:= \mathtt{KIND} \\
(t\ u)^+ &:= t^+\ u^*\ u^+ \\
(\lambda(x : A).\ t)^+ &:= \lambda(x^* : A^*)(x^+ : A^+\ x^*).\ t^+
\end{aligned}
$$

Interpretation of terms (3)

- If $B : \texttt{TYPE}$,

$$(\Pi(x : A).\ B)^{+} := \lambda(f : (\Pi(x : A).\ B)^{*}).\ \Pi(x^{*} : A^{*})(x^{+} : A^{+}\ x^{*}).\ B^{+}\ (f\ x^{*}\ x^{+})$$

- If $B : \texttt{KIND}$, we **cannot** abstract on f
  - We write $T\{X\}$ when the **metavariable** X occurs in T
  - We write $T\{f\}$ when X is substituted by f

$$(\Pi(x : A).\ B)^{+}\{X\} := \Pi(x^{*} : A^{*})(x^{+} : A^{+}\ x^{*}).\ B^{+}\{X\ x^{*}\ x^{+}\}$$

- Definition of $\texttt{TYPE}^{+}$

$$\texttt{TYPE}^{+}\{X\} := X \to \texttt{TYPE}$$

Interpretation of theories

$\mathbb{S}$ has an **interpretation** in $\mathbb{T}$ when:

1. for each constant $c : A \in \mathbb{S}$, we have in $\mathbb{T}$
   - a term c^* such that $\vdash c^* : A^*$,
   - a term c^+ such that
   $$\begin{array}{ll} \vdash c^+ : A^+\ c^* & \text{if } \vdash A : \texttt{TYPE} \\ \vdash c^+ : A^+\{c^*\} & \text{if } \vdash A : \texttt{KIND} \end{array}$$
2. for each rewrite rule $\ell \hookrightarrow r \in \mathbb{S}$, we have $\ell^* \equiv_{\beta\Sigma} r^*$ and $\ell^+ \equiv_{\beta\Sigma} r^+$ in $\mathbb{T}$.

Parameters for the prelude encoding (1)

- We must find the **parameters for the prelude encoding**

- If nat : Set, then nat^* : Set and $\text{nat}^+ : El\ \text{nat}^* \to El\ o$

$$
\begin{aligned}
Set^* &:= Set \\
Set^+ &:= \lambda(z : Set).\ El\ z \to El\ o
\end{aligned}
$$

- If $n : El\ \text{nat}$, then $n^* : El\ \text{nat}^*$ and $n^+ : Prf\ (\text{nat}^+\ n^*)$

$$
\begin{aligned}
El^* &:= \lambda(x^* : Set)(x^+ : El\ x^* \to El\ o).\ El\ x^* \\
El^+ &:= \lambda(u^* : Set)(u^+ : El\ u^* \to El\ o)(z : El\ u^*).\ Prf\ (u^+\ z)
\end{aligned}
$$

Parameters for the prelude encoding (2)

- If $P : El\ o$, then $P^* : El\ o$ and $P^+ : Prf\ P^* \to Prf\ P^*$

$$
\begin{aligned}
o^* &:= o \\
o^+ &:= \lambda(z : El\ o).\ z \Rightarrow_d (\lambda(x : Prf\ z).\ z)
\end{aligned}
$$

- If $t : Prf\ P$, then $t^* : Prf\ P^*$ and $t^+ : Prf\ P^*$

$$
\begin{aligned}
Prf^* &:= \lambda(x^* : El\ o)(x^+ : Prf\ (o^+\ x^*)).\ Prf\ x^* \\
Prf^+ &:= \lambda(u^* : El\ o)(u^+ : Prf\ (o^+\ u^*))(z : Prf\ u^*).\ Prf\ u^*
\end{aligned}
$$

Main theorems

Suppose that $\mathbb{S}$ has an interpretation in $\mathbb{T}$.

- **Interpretation theorem**: If $\Gamma \vdash t : A$ in $\mathbb{S}$ then $\Gamma^{*,+} \vdash t^* : A^*$ in $\mathbb{T}$

  $\hookrightarrow$ We can **transfer** proofs from $\mathbb{S}$ to $\mathbb{T}$

- **Relative consistency theorem**: If $\mathbb{T}$ is consistent, then $\mathbb{S}$ is **consistent**

Outline

Example: natural numbers and integers

- Natural numbers can be **embedded** into integers
  $\mathsf{nat}^* := \mathsf{int}$
  $\mathsf{nat}^+ := \lambda(z : El\ \mathsf{int}).\ z \geq_i 0_i$
  $\mathsf{succ}_n^* := \lambda(x^* : El\ \mathsf{int})(x^+ : Prf\ (x^* \geq_i 0_i)).\ \mathsf{succ}_i\ x^*$

- The theorems of $\mathbb{T}_n$

$$\vdash \mathsf{thm} : \Pi(x : El\ \mathsf{nat}).\ Prf\ (\mathsf{succ}_n\ x \geq_n 0_n)$$

can be derived in $\mathbb{T}_i$

$$\vdash \mathsf{thm}^* : \Pi(x^* : El\ \mathsf{int}).\ Prf\ (x^* \geq_i 0_i) \to Prf\ (\mathsf{succ}_i\ x^* \geq_i 0_i)$$

Example: sets and pointed graphs

- Zermelo set theory can be represented by pointed graphs [Dowek and Miquel, 2007]
- We can **interpret** the theory of sets in the theory of pointed graphs
  $\hookrightarrow$ The theory of pointed graphs is computational
- Every pointed graph represents a set
  $\hookrightarrow$ The predicates asserting that a graph represents a set are **unnecessary**

Outline

Takeaway message

- Interpretation for theories
  - With prelude encoding
  - When the source $\mathbb{S}$ can be **embedded** in the target $\mathbb{T}$

- Interpretation of a type A of $\mathbb{S}$ by a **more general** type A^* of $\mathbb{T}$
  But we introduce the **predicate** A^+

- Well-suited when the target is larger than the source
  May insert unnecessary predicates

Perspectives

- Practical application: **implementation** in Dedukti
- Theoretical application: **relative normalization**
  - Result in deduction modulo theory using an interpretation [Dowek and Miquel, 2007]
  - Possible for the $\lambda\Pi$-calculus modulo theory?

Thank you for your attention!