Skolemization in intuitionistic first order logic

Olivier Hermant*

1 Introduction

Skolem theorem is a central result of proof theory. It simplifies many arguments and is heavily used in automatic deduction. However proving Skolem theorem requires great accurateness, and is difficult, specially in intuitionistic deduction systems [1, 2, 3], where we know only few proofs.

In this paper, we give a readable, elegant and understandable proof of Skolem theorem for Intuitionistic Logic by a semantic method. We therefore avoid the technical difficulties that one encounters when transforming by syntactical means a proof of $\Gamma, \forall x \exists y P(x, y) \vdash Q$ into a proof of $\Gamma, \forall x P(x, f(x)) \vdash Q$. Moreover, it applies uniformly to all deduction systems (sequent calculus, natural deduction, deduction à la Hilbert), as long as we have soundness and completeness of the chosen semantic w.r.t those calculi. Another advantage is that it extends readily to other intuitionistic calculi like intuitionistic HOL or Heyting Arithmetic, through Deduction Modulo.

The two main semantics for intuitionistic calculi are Heyting Algebras and Kripke structures. Unfortunately, it seems not to be possible to prove Skolem Theorem using these notions of model. Instead, we will use a restriction of Kripke structures, namely the Kripke trees that remain sound and complete w.r.t. intuitionistic calculi.

2 Preliminaries

We refer to [4] for instance to recall the intuitionistic sequent calculus deduction rules. If the reader is more familiar with natural deduction, he can reason in this system, presented for instance in [3]. As already said, this is not very relevant, since we are interested in proving Skolem Theorem in the semantical frame.

The theorem to prove is the following :

*Project PCRI Pôle Commun de Recherche en Informatique du plateau de Saclay, CNRS, École Polytechnique, INRIA, Université Paris-Sud.hermant@lix.polytechnique.fr http://lix.polytechnique.fr/~hermant

Theorem 1 (Skolem)**.** *Let Γ be a set of propositions, and $\forall x \exists y P(x,y), Q$ be propositions where the function symbol f does not appear. Then:*

$$\Gamma, \forall x \exists y P(x,y) \vdash Q \quad \textit{if and only if} \quad \Gamma, \forall x P(x, f(x)) \vdash Q$$

Note that the direct way of the equivalence is trivial, since the following sequent is provable:

$$\Gamma, \forall x P(x, f(x)) \vdash \forall x \exists y P(x,y)$$

we then end up constructing a proof of $\Gamma, \forall x P(x, f(x)) \vdash Q$ combining the two proofs of the sequents:

$$\Gamma, \forall x P(x, f(x)) \vdash \forall x \exists y P(x,y) \qquad \Gamma, \forall x \exists y P(x,y) \vdash Q$$

with a cut rule. □

The reverse way is much more complex. To achieve its proof we will switch into the semantic framework. We will use the following notion of model:

Definition 1 (Kripke structure)**.** *A Kripke structure $\mathcal{K}$ is a quadruple*

$$\langle K, \leq, D, \Vdash \rangle$$

where:

- *K is a non empty set, the set of worlds.*
- *$\leq$ is a partial order relation over K.*
- *D is a function from K to non empty sets, that is monotone. If $\alpha \leq \beta$, then $D_\alpha \subseteq D_\beta$.*
- *$\Vdash$ is a relation (the forcing relation) that verifies the following axioms:*
  - *for any atomic predicate A, worlds $\alpha \leq \beta$, and elements $a_1, ..., a_n \in D_\alpha$, $\alpha \Vdash A(a_1, ..., a_n) \Rightarrow \beta \Vdash A(a_1, ..., a_n)$.*
  - *$\alpha \Vdash A \vee B$ if and only if $\alpha \Vdash A$ or $\alpha \Vdash B$.*
  - *$\alpha \Vdash A \wedge B$ if and only if $\alpha \Vdash A$ and $\alpha \Vdash B$.*
  - *$\alpha \Vdash A \Rightarrow B$ if and only if for any $\beta \geq \alpha$ we have $\beta \Vdash A$ implies $\beta \Vdash B$.*
  - *$\alpha \Vdash \neg A$ if and only if for any $\beta \geq \alpha$, $\beta \nVdash B$.*
  - *$\alpha \Vdash \exists x A(x)$ if and only if there exists $a \in D_\alpha$ such that $\alpha \Vdash A(a)$.*
  - *$\alpha \Vdash \forall x A(x)$ if and only if for any world $\beta \geq \alpha$, and any $a \in D_\alpha$ we have $\beta \Vdash A(c)$.*

Notation. In the remainder of this note, $\Gamma \vDash P$ stands for the following: for any Kripke structure K, for any node α such that $\alpha \Vdash \Gamma$, $\alpha \Vdash P$.

A key property of the Kripke structure is that the forcing relation is monotonic. This is known by definition for the atoms, and can be extended to any proposition:

Proposition 2. *In a Kripke structure, for any worlds $\beta \geq \alpha$, $\alpha \Vdash P$ implies $\beta \Vdash P$.*

Proof. By an induction on the propositions structure. See [5]. $\square$

Theorem 3 (Soundness and Completeness)**.** $\Gamma \vdash P$ *if and only if* $\Gamma \vDash P$

Proof. See for instance [5, 4]. It is standard, and presented in two parts (completeness following soundness). $\square$

As said in the introduction, thanks to soundness and completeness theorems, we can transform the if part of theorem 1 into the following proposition:

Proposition 4. *If* $\Gamma, \forall x P(x, f(x)) \vDash Q$ *then* $\Gamma, \forall x \exists y P(x, y) \vDash Q$

To prove 4, it would be sufficient to prove that any model $\mathcal{M}$ of $\forall x \exists y P(x, y)$ can be extended to a model of $\forall x P(x, f(x))$, without changing anything in the model itself, that is, giving the interpretation of the new function symbol f in the model $\mathcal{M}$. Unfortunately, this is not always possible, as shown by the following counter example, where the arrow represents the partial order over Kripke worlds.

$$
\begin{tikzcd}
& A_{\{a,b,c\}} \Vdash P(a,b), P(a,c), P(b,b), P(c,c) & \\
B_{\{a,c\}} \Vdash P(a,c), P(c,c) \arrow[ur] & & C_{\{a,b,c\}} \Vdash P(a,b), P(b,b), P(c,c) \arrow[ul] \\
& D_{\{c\}} \Vdash P(c,c) \arrow[ul] \arrow[ur] &
\end{tikzcd}
$$

Here, the domain of the worlds A, B, C, D is denoted as a subscript of the world, and we have indicated the forced atomic propositions. We can check that $D \Vdash \forall x \exists y P(x, y)$.

We would like to prove $D \Vdash Q$, knowing by assumption that $\forall x P(x, f(x)) \vDash Q$.

The simplest idea is to try to extend the $\Vdash$ forcing relation, without changing the domain, to take into account the new symbol f, such that $D \Vdash \forall x P(x, f(x))$ holds. In order to have a conservative extension, we should interpret f as $\widehat{f}$ such that:

$$
\begin{array}{lcl}
\widehat{f}(D)(c) & := & c \\
\widehat{f}(B)(a) & := & c \\
\widehat{f}(B)(c) & := & c \\
\widehat{f}(C)(a) & := & b \\
\widehat{f}(C)(b) & := & b \\
\widehat{f}(C)(c) & := & c
\end{array}
$$

But we can not define $\widehat{f}(A)(a)$, since $\widehat{f}(A)$ has to agree with both $\widehat{f}(B)$ and $\widehat{f}(C)$. So $D \nVdash \forall x P(x, f(x))$, in any case.

If we analyse the cause of the impossibility to interpet the function symbol f as we would haved liked to, it turns out that this is because $a \in \mathcal{D}_B \cap \mathcal{D}_C$ and $a \notin \mathcal{D}_D$. To overcome this difficulty, we have two ways. Both of them are base on a slight restriction of definition 1:

- Either we can enforce that if $a \in \mathcal{D}_B \cap \mathcal{D}_C$, a then $a \in \mathcal{D}_D$ (two parallel worlds share only the domain of their common predecessor, and nothing else).
- either we can forbid such a partial order on the nodes, so as to have only trees. This is the choice made here, because it is more natural and elegant. Furthermore it underlines the fact that Kripke structures lacks some good ordering.

The idea behind this is that we should view A not as a single world, but as two distinct worlds: one that possesses B as antecedent, another that possesses C as an antecedent, as in the following tree:

$$\begin{tikzcd}
A_l \Vdash P(a,b), P(a,c), P(b,b), P(c,c) & & A_r \Vdash P(a,b), P(a,c), P(b,b), P(c,c) \\
B \Vdash P(a,c), P(c,c) \arrow[u] & & C \Vdash P(a,b), P(b,b), P(c,c) \arrow[u] \\
& D \Vdash P(c,c) \arrow[ul] \arrow[ur] &
\end{tikzcd}$$

Here we can set $\widehat{f}(A_l)(a) = b$ and $\widehat{f}(A_r)(a) = c$, so $D \Vdash \forall x P(x, f(x))$, therefore $D \Vdash Q$ by hypothesis.

At this point, we should be very careful, because if we shift the definition of our semantical frame, we have to check that soundness ans completeness theorem 3 still hold for "Kripke trees".

We process now with the details, and first define what is a Kripke tree. We then prove soundness and completeness w.r.t. this semantic. A direct proof could have been done, re-proving soundness and completeness from scratch, just checking that the proofs of [5] for example still hold. Instead of doing that, we give here an alternate proof, that is semantical, as simple as the above checking, and of independent interest.

Definition 2. *A Kripke structure $\langle K, \leq, D, \Vdash \rangle$ is called a Kripke tree if the order on K is well-founded and for any worlds α, β, γ, if $\gamma \leq \alpha$ and $\delta \leq \alpha$, we can compare γ and β, i.e.:*

$$\beta \leq \gamma \quad \textit{or} \quad \gamma \leq \beta$$

The two semantics are eqquivalent:

Proposition 5. *$\Gamma \vDash A$ for the Kripke tree semantics if and only if $\Gamma \vDash A$ in the Kripke structure semantics.*

Proof. The converse statement is trivial, since a Kripke tree *is* a Kripke structure with some more properties. $\square$

Regarding the direct way, we can define the unravelling of a Kripke structure into a Kripke tree that is conservative w.r.t. the Kripke structure.

Let $\langle K, \leq, \mathcal{D}, \Vdash \rangle$ be a Kripke structure. we define the following Kripke structure $\langle K', \preceq, \mathcal{D}', \Vdash \rangle$:

- K' is the set of increasing finite sequences of nodes of K: $(a_1 ... a_j a_{j+1} ... a_n) \in K'$ if and only if $a_j < a_{j+1}$ and $a_j \in K$ for any index j.
- We define the partial ordering relation $\preceq$ as follows: we say that $(a_1 ... a_n) \preceq (a'_1 ... a'_m)$ if and only if $n \leq m$ and $\forall i \leq n, a_i = a'_i$ (the former is an initial sequence of the later).
- We set $\mathcal{D}'_{(a_1 ... a_n)} = \mathcal{D}_{a_n}$.
- The forcing relation is *defined* as follows: $(a_1 ... a_n) \Vdash' P$ if and only if $a_n \Vdash P$ (for any proposition, even non atomic ones).

It is routine to prove that the order on K' defines a tree, and to check that axioms for a Kripke structure (of definition 1) are preserved. $\square$

Notice that this transformation doesn't transform a tree into itself. The order $\preceq$ is well-founded, event if the intial order of $\mathcal{K}$ is not.

We then prove the direct way of proposition 5:

Proposition. *If $\Gamma \vDash A$ for the Kripke tree semantics then $\Gamma \vDash A$ in the Kripke structure semantics.*

Proof. Let $\mathcal{K}$ be a Kripke structure, and $\alpha \in K$ a world such that $\alpha \Vdash \Gamma$. Define $\mathcal{K}'$ as the unravelling of $\mathcal{K}$. From the conservativity of $\mathcal{K}'$ over $\mathcal{K}$, we get that $(\alpha) \Vdash' \Gamma$. So, by hypothesis, $(\alpha) \Vdash' A$, and by conservativity again $\alpha \Vdash A$. $\square$ $\square$

As a corollary, we get the soundness and completeness theorem of Intuitionistic Sequent Calculus w.r.t. Kripke trees. Notice that a direct proof could have be done, as already said.

3 Proof of Skolem theorem

Let us turn back into the proof of the Skolem theorem 1. What we have to do is to prove proposition 4, but with respect to Kripke trees semantic now. Thanks to that, we are now able to extend the forcing relation $\Vdash$ so that any node $\alpha \Vdash \forall x \exists y P(x, y)$ is also such that $\alpha \Vdash \forall x P(x, f(x))$.

Proof. Suppose we have $\Gamma, \forall x P(x, f(x)) \models Q$.

Let $\mathcal{K}$ be a tree , and $\alpha \in K$ a world such that $\alpha \Vdash \Gamma, \forall x \forall y P(x, y)$. We have to prove that $\alpha \Vdash Q$.

Consider now the skolemized form $P(x, f(x))$. We have to deal with a fresh symbol f in the language $\mathcal{L}$ in which are expressed Γ, P, Q. So, we are to extend the forcing relation to take into account this new symbol, *without changing the domain function*. Notice that we are not interested in worlds other than those that are greater than α because we want to prove $\alpha \Vdash Q$, and a Kripke structure is causal. We can therefore consider α as a root.

In other words, given a world $\beta \succ \alpha$ and an element $a \in D_\beta$, we will give the interpretation of $\widehat{f}(\beta)(a)$ in D_β, knowing that the symbol f does not appear in Γ nor in Q by hypothesis.

So for any $\beta \succ \alpha$, and $a \in D_\beta$, we have two choices:

- a is a new term that does not appear in any world below. As $\beta \Vdash \forall x \exists y P$ (the forcing relation is monotone, and $\alpha \Vdash \forall x \exists y P$), we have a term $a' \in \mathcal{D}_\beta$ such that $\beta \Vdash P(a, a')$. We set $\widehat{f}(\beta)(a)$ equal to a'.

- a appears in $\gamma \prec \beta$. Because we have a tree structure, and the order is well-founded, we can consider the unique least $\delta \prec \beta$, such that $a \in \mathcal{D}_\delta$. $\widehat{f}(\delta)(a)$ is already interpreted by a term in $\mathcal{D}_\delta$, such that $\delta \Vdash P(a, \widehat{f}(\delta)(a))$. Hence $\gamma \Vdash P(a, \widehat{f}(\delta)(a))$ by monotonicity of the forcing relation. So, we set $\widehat{f}(\beta)(a)$ equal to $\widehat{f}(\delta)(a))$.

Now, it is easy to check that for any node $\beta \succ \alpha$, any term $a \in \mathcal{D}_\beta$, $\beta \Vdash P(a, \widehat{f}(\beta)(a))$. Hence, $\alpha \Vdash \Gamma, \forall x P(x, f(x))$.

We hence have, by hypothesis $\alpha \Vdash Q$.

So we have checked that for any Kripke tree, for any node such that $\alpha \Vdash \Gamma, \forall x \exists y P(x, y)$, we have $\alpha \Vdash Q$. So we proved proposition 4. □

To end up the proof of Skolem theorem 1, let's now suppose we have a proof of the sequent $\Gamma, \forall x P(x, f(x)) \vdash Q$. We have by the soundness theorem $\Gamma, \forall x P(x, f(x)) \models Q$.

We then use proposition 4. And by the completeness theorem , we get $\Gamma, \forall x \exists y P(x, y) \vdash Q$, that proves the reverse way of the Skolem theorem 1. □

4 Extension to Deduction Modulo

A complete introduction to Deduction Modulo can be found in [6]. The idea is to mix rewrite rules ans a deduction system. The main feature is that rewrite rules are allowed also on *atomic formulas*:

$$A(0) \quad \rightarrow \quad \forall x (A(x) \wedge B)$$

Deduction rules are modified accordingly. Let $\mathcal{R}$ be a set of rewrite rules. For instance, the axiom rule becomes:

$$\frac{}{\Gamma, A \vdash_{\mathcal{R}} B} \text{ if and only if } A \equiv_{\mathcal{R}} B$$

where $\equiv_{\mathcal{R}}$ is the symmetric-reflexive-transitive closure of the one-step rewrite relation of $\mathcal{R}$.

This feature allows to express many powerful theories in a first order frame, without any addition axiom. For instance, we can express Heyting arithmetic [7], Intuitionistic HOL [8], or Zermelo's set theory in deduction modulo.

Semantics for Deduction Modulo are the very same that those for usual deduction systems, except that we add a condition that if $A \equiv B$, then they should have the same interpretation. So we modify the Kripke structure definition 1 adding the following statement:

For any node α, any propositions $A \equiv_{\mathcal{R}} B$, $\alpha \Vdash A \Leftrightarrow \alpha \Vdash B$

With this definition, we are able to prove soundness and completeness theorem under the hypothesis that $\mathcal{R}$ is confluent. Not modifying any line of our proof, we can show equivalence between Kripke structures for deduction modulo and Kripke trees for deduction modulo:

Theorem 6 (Skolem theorem in Deduction Modulo)**.** *Let Γ be a set of propositions, $\mathcal{R}$ a set of (confluent) rewrite rules, and $\forall x \exists y P(x, y), Q$ be propositions. Let f a function symbol that doesn't appear anywhere else. Then:*

$$\Gamma, \forall x \exists y P(x, y) \vdash_{\mathcal{R}} Q \quad \textit{if and only if} \quad \Gamma, \forall x P(x, f(x)) \vdash_{\mathcal{R}} Q$$

Proof. It is essential to consider a Skolem symbol not appearing nor in Γ, nor in Q, nor in the set $\mathcal{R}$ of rewrite rules. This is sufficient to check that our proof remains valid with no further modification. □

5 Conclusion

We have proved Skolem Theorem in the intuitionistic frames. The good point of the method is that it is much more simpler than syntactic methods, like [3]. Another advantage is that the result extends to other formalisms without difficulties, as shown. It readily extends to Skolemization in Deduction Modulo, and with this help, we got a proof of Skolem theorem for intuitionistic HOL, Heyting Arithmetic and Zermelo's Set theory for instance. This method could also be applied in classical frames, considering this time boolean models.

Beth models is a semantic that already have a tree structure [4], remains sound and complete, but that is yet more specific than the definition we gave. We believe that we could have used this semantic, although modifying the Kripke structure one seems more interesting, since it points the fact that Kripke structures have to be considered as trees.

6 Acknowledgements

The author is grateful to Gilles Dowek and Thierry Coquand for an accurate reading of the paper and for their invaluable comments and discussions.

References

[1] Maehara, S.: The predicate calculus with ε symbol. Journal of the Mathematical Society of Japan **7** (1955) 323–344

[2] Mints, G.E.: Skolem's method of elimination of positive quantifiers in sequential calculi. Soviet. Math. Dokl. **7** (1966) 861–864

[3] Dowek, G., Benjamin, W.: A constructive proof of skolem theorem for constructive logic. to appear (2005)

[4] Troelstra, A.S., van Dalen, D.: Constructivism in Mathematics, An Introduction. North-Holland (1988)

[5] Troelstra, A.S.: Metamathematical Investigation of Intuitionistic Arithmetic and Analysis. Springer-Verlag (1973)

[6] Dowek, G., Hardin, T., Kirchner, C.: Theorem proving modulo. Journal of Automated Reasoning **31** (2003) 33–72

[7] Dowek, G., Werner, B.: Arithmetic as a theory modulo. Term rewriting and applications (2005) 423–437

[8] Dowek, G., Werner, B.: Proof normalization modulo. The Journal of Symbolic Logic **68** (2003) 1289–1316