Automating Theories in Intuitionistic Logic

Guillaume Burel

Automating Theories in Intuitionistic Logic

Guillaume Burel

Nancy-Université & LORIA*
guillaume.burel@ens-lyon.org http://www.loria.fr/~burel/

Abstract. Deduction modulo consists in applying the inference rules of a deductive system modulo a rewrite system over terms and formulæ. This is equivalent to proving within a so-called compatible theory. Conversely, given a first-order theory, one may want to internalize it into a rewrite system that can be used in deduction modulo, in order to get an analytic deductive system for that theory. In a recent paper, we have shown how this can be done in classical logic. In intuitionistic logic, however, we show here not only that this may be impossible, but also that the set of theories that can be transformed into a rewrite system with an analytic sequent calculus modulo is not co-recursively enumerable. We nonetheless propose a procedure to transform a large class of theories into compatible rewrite systems. We then extend this class by working in conservative extensions, in particular using Skolemization.

1 Introduction

Mathematical propositions are seldom proved in pure first-order logic, but more often within a particular theory, e.g. arithmetic or Euclidean geometry. In general, this is performed using an axiomatization of these theories, but this has drawbacks. First, this is rather inefficient from an automated-proof-search point of view, in particular when computations are involved. To be convinced of this, one may try to prove a simple result such as "2+2=4" in Peano's arithmetic. Second, some interesting properties of deductive systems may be lost when proving using axioms. In particular, in a constructive setting, the disjunction property, that says that from a proof of $P \vee Q$ one can find a proof of P or a proof of Q, and the witness property, that says that from a proof of $\exists x.\ P(x)$ one can find a witness term t and a proof of $P(t)$, no longer hold when using axioms.

Dowek, Hardin and Kirchner [11] proposed an alternative way of proving within a theory: in deduction modulo, the inference rules used to prove a formula are applied modulo a rewrite system. This system can rewrite terms, but also atomic formulæ to formulæ. For instance, given the (propositional) rule $x \times y = 0 \to x = 0 \vee y = 0$, we can build the following proof of $\forall x.\ x \times x = 0 \Rightarrow x = 0$ in the sequent calculus modulo:

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{}{x = 0 \vdash x = 0}\,\mathsf{Ax.} \quad \dfrac{}{x = 0 \vdash x = 0}\,\mathsf{Ax.}}{x \times x = 0 \vdash x = 0}\,\vee\!\vdash}{\vdash x \times x = 0 \Rightarrow x = 0}\,\vdash\!\Rightarrow}{\vdash \forall x.\ x \times x = 0 \Rightarrow x = 0}\,\vdash\!\forall}\ x \times x = 0 \longrightarrow x = 0 \vee x = 0$$

* UMR 7503 CNRS–INPL–INRIA–Nancy2–UHP

We can see that proving in the sequent calculus modulo this rule is equivalent to proving in the theory $\forall x\ y.\ x \times y = 0 \Leftrightarrow x = 0 \vee y = 0$. Propositions 1.6 and 1.8 of [11] tell us that given a rewrite system, it is always possible to find a theory such that proving modulo the rewrite system is equivalent to proving in the theory. Presentations of that theory are then called compatible with the rewrite system.

We are interested here in the converse problem: given a theory, how is it possible to internalize it into a rewrite system usable in deduction modulo? In which case, we will also say that the rewrite system is compatible with the theory. Proof search methods based on deduction modulo, e.g. ENAR [11] and TaMed [5] can then be used to find proofs in those theories. These methods are complete only if the sequent calculus modulo the compatible rewrite system admits cut. Indeed, it may not be the case in deduction modulo, as shown by the consistent example $A \to A \Rightarrow B$: B possesses the following proof

$$\dfrac{\dfrac{\dfrac{}{A \Rightarrow B \vdash B, A}\,\mathsf{Ax.}\ *}{\vdash\Rightarrow}\quad \dfrac{}{B \vdash B}\,\mathsf{Ax.}\ *}{\dfrac{A \vdash B \qquad\qquad \dfrac{\dfrac{A \vdash B}{\vdash B, A}\,\vdash\Rightarrow\ *}{\vdash B}\,\mathsf{Cut}}{}}$$

where the inference rules applied modulo $A \to A \Rightarrow B$ are marked by $*$. But B cannot be proved without cut. We therefore want to find compatible rewrite systems ensuring the cut admissibility. This was for instance successfully done by hand for arithmetic [13] and Zermelo's set theory [12]. However, to be sure that the deductive system modulo admits cuts, some tricks are used that seems difficult to automate. This paper studies the automation of the transformation of the presentation of an intuitionistic first-order theory into a rewrite system that is applied modulo.

In a submitted paper [7], we proposed a complete solution in the case of classical logic: First, we have shown how to transform any presentation of a theory into a compatible rewrite system; Then, we have defined a completion procedure that transforms the resulting rewrite system to ensure that the sequent calculus modulo the final rewrite system admits cut. In intuitionistic logic, however, there are theories that cannot be transformed into a compatible rewrite system, as we will soon show, and we cannot separate the production of the rewrite system and its completion that ensures the cut admissibility.

To better explain how we will proceed in the intuitionistic case, let us recall how theories can be internalized in classical logic. The main technical complication arises because in deduction modulo, left hand sides of proposition rewrite rules must be atomic formulæ. To transform an axiom into such a rule, the idea is therefore to apply the inference rules of a sequent calculus to decompose the axiom and pick out one of its atomic subformula. To remain in the same theory, the inference rules that we are using must preserve the provability. Therefore, we are only allowed to apply invertible rules —recall that an inference rule is called invertible if whenever its conclusion is derivable, its premises also are. Fortunately, there exists sequent calculi for classical logic where all inference rules are invertible, e.g. the system G4 of Kleene [19], so that the transformation is always

possible in classical logic. For instance, the theory presented by $\forall x.\ \exists y.\ A(x,y)$ is decomposed into the sequent $\vdash A(x,y), \exists y.\ A(x,y)$ which is in turn oriented into the rewrite rule $A(x,y) \to A(x,y) \vee \neg\exists y.\ A(x,y)$. The transformation of sequents into rewrite rules relies on classical tautologies, so that in intuitionistic logic, we cannot hope to obtain such a result. Indeed, if you consider the theory presented by the simple axiom $A \vee B$ with A and B some distinct atomic formulæ, you can prove neither A nor B. However, were it possible to find a rewrite system for that theory such that the sequent calculus modulo this system admits cuts, this deductive system would have the disjunction property (see Proposition 3). As by compatibility $A \vee B$ could be proven, either A or B should be provable, hence the contradiction. Note that in classical logic, the axiom $A \vee B$ would produce the rule $A \to A \vee \neg B$, but it is not intuitionistically equivalent to $A \vee B$. We would like to be able to characterize the presentations that have a compatible rewrite system such that the sequent calculus modulo this system admits cuts, but we prove that the set of such presentations is not co-recursively enumerable, that is, cannot be decided. Nevertheless, we propose a procedure that transforms a large class of theories into compatible rewrite systems. This procedure is a non-trivial generalization of the procedure for classical logic, because we have to mix the transformation into rewrite rules and the completion that ensures the cut admissibility, and because we must develop new techniques to avoid being stuck with examples such as $A \vee (B \Rightarrow A)$.

The same kind of counterexample as $A \vee B$ can be obtained from a theory presented by an axiom of the form $\exists x.\ A(x)$, using the witness property. In that case however, it is possible to use Skolemization to work in a conservative extension of the theory that has a compatible rewrite system such that the sequent calculus modulo this rewrite system admits cuts. As Skolemization does not always lead to a conservative extension in intuitionistic logic, this means that this will not always be possible. In this paper, we investigate in which cases it is possible to transform the presentation of a theory into a compatible rewrite system, possibly using conservative extensions of the theory.

In the following section we recall some sequent calculi for intuitionistic logic maximizing the number of invertible rules, and we introduce deduction modulo. In Section 3 we prove that the set of presentations that have a compatible rewrite system such that the sequent calculus modulo this system admits cut is not co-recursively enumerable. Section 4 presents a procedure that tries to transform a presentation into a compatible rewrite system. Then in Section 5, we extend the domain where this procedure succeeds by considering infinite presentations, equality and Skolemization. Finally, Section 6 provides an example application extracted from the Intuitionistic Logic Theorem Proving library [24].

2 Preliminaries

2.1 Sequent Calculi for Intuitionistic Logic

We use standard definitions for terms, predicates, propositions (with connectors $\bot, \top, \Rightarrow, \wedge, \vee$ and quantifiers $\forall, \exists$), substitutions, term rewrite rules and term

rewriting, as can be found in [1, 14]. The set of terms built from a signature Σ and a set of variables V is denoted by $\mathcal{T}(\Sigma, V)$, the replacement of a variable x by a term t in a proposition P by $\{t/x\}P$, the application of a substitution σ in a proposition P by σP, the free variables occurring in P by $FV(P)$. $\neg P$ is a shorthand for $P \Rightarrow \bot$, and when $\Gamma = P_1, \ldots, P_n$, then $\bigwedge \Gamma$, $\bigvee \Gamma$ and $\neg\Gamma$ are notations for $P_1 \wedge \cdots \wedge P_n$, $P_1 \vee \cdots \vee P_n$ and $\neg P_1, \ldots, \neg P_n$. $P \Leftrightarrow Q$ denotes $(P \Rightarrow Q) \wedge (Q \Rightarrow P)$.

The reader is referred to [14] for an introduction to sequent calculi. A sequent is a pair (Γ, Δ) of multisets of formulæ, denoted by $\Gamma \vdash \Delta$. A logical rule of a sequent calculus decomposes a formula, which is called *principal*, appearing in a sequent, into its direct subformulæ, which are called the *side formulæ*. For instance, in

$$\Rightarrow\vdash \frac{\Gamma \vdash X, \Delta \qquad \Gamma, Y \vdash \Delta}{\Gamma, X \Rightarrow Y \vdash \Delta}$$

$X \Rightarrow Y$ is the principal formula, X and Y are the side formulæ, and the other formulæ, those appearing in Γ and Δ, are called the *extra formulæ*. An inference rule $\dfrac{H_1 \quad \cdots \quad H_n}{C}$ is said *invertible* if whenever C can be proved, then so can all H_i for $1 \leq i \leq n$. A logical rule r permutes over a logical rule $\mathsf{r'}$ if whenever there is a proof ending with

$$\mathsf{r}\,\frac{\mathsf{r'}\,\dfrac{H_1 \quad \cdots \quad H_n}{C} \qquad I_1 \quad \cdots \quad I_m}{D}$$

where the principal formula of r is not a side formula of $\mathsf{r'}$, it is possible to build a proof with r below $\mathsf{r'}$. If an inference rule permutes with all the other rules, it can be proved that it is invertible. A double horizontal line indicates several application of an inference rule. We will also consider *derivations*, that is, partial proofs where leafs are not all closed by Ax. The sequents appearing in the open leafs of a derivation are called its *premises*.

The usual sequent calculus for intuitionistic logic, LJ, was introduced by Gentzen [15]. It consists in allowing at most one formula to the right of the sequents of the sequent calculus for classical logic LK. However, this has drawbacks, because many rules cannot be permuted contrarily to classical logic, so that almost all rules are not invertible. Therefore, it has been proposed to keep multiple conclusions in the sequents, but to restrict only the rules where it is needed, i.e. for the right rules for $\Rightarrow$ and $\forall$. The resulting system is called L'J [21], LB [26] or LJm [23], with little differences between versions. We represent the system LB in Fig. 1, as it appears in [26]. It is shown [26] that the only cases of rules that do not permute are $\forall\vdash$ over $\vdash\forall$; $\forall\vdash$ and $\vdash\exists$ over $\exists\vdash$; and $\Rightarrow\vdash$ over $\vdash\Rightarrow$ and $\vdash\forall$. This means that the only logical rules that are not invertible are $\forall\vdash$, $\vdash\exists$ and $\Rightarrow\vdash$.

To make these rules invertible, one solution is to apply a contraction ($\cdot,\cdot\vdash$ or $\vdash\cdot,\cdot$) to the active formula just before applying the logical rule. This is what is done in classical logic to obtain the system G4 [19] from LK. It can be shown [23]

Identity rules

$$\mathsf{Ax.}\ \frac{}{\Gamma, X \vdash X, \Delta} \qquad \mathsf{Cut}\ \frac{\Gamma, X \vdash \Delta \qquad \Gamma \vdash X, \Delta}{\Gamma \vdash \Delta}$$

Structural rules

$$\because\vdash\ \frac{\Gamma, X, X \vdash \Delta}{\Gamma, X \vdash \Delta} \qquad \vdash\because\ \frac{\Gamma \vdash X, X, \Delta}{\Gamma \vdash X, \Delta}$$

$$\cdot\vdash\ \frac{\Gamma \vdash \Delta}{\Gamma, X \vdash \Delta} \qquad \vdash\cdot\ \frac{\Gamma \vdash \Delta}{\Gamma \vdash X, \Delta}$$

Logical rules

$$\Rightarrow\vdash\ \frac{\Gamma \vdash X, \Delta \qquad \Gamma, Y \vdash \Delta}{\Gamma, X \Rightarrow Y \vdash \Delta} \qquad \vdash\Rightarrow\ \frac{\Gamma, X \vdash Y}{\Gamma \vdash X \Rightarrow Y}$$

$$\wedge\vdash\ \frac{\Gamma, X, Y \vdash \Delta}{\Gamma, X \wedge Y \vdash \Delta} \qquad \vdash\wedge\ \frac{\Gamma \vdash X, \Delta \qquad \Gamma \vdash Y, \Delta}{\Gamma \vdash X \wedge Y, \Delta}$$

$$\vee\vdash\ \frac{\Gamma, X \vdash \Delta \qquad \Gamma, Y \vdash \Delta}{\Gamma, X \vee Y \vdash \Delta} \qquad \vdash\vee 1\ \frac{\Gamma \vdash X, Y, \Delta}{\Gamma \vdash X \vee Y, \Delta}$$

$$\forall\vdash\ \frac{\Gamma, X(t) \vdash \Delta}{\Gamma, \forall x,\ X(x) \vdash \Delta} \qquad \vdash\forall\ \frac{\Gamma \vdash X(y)}{\Gamma \vdash \forall x,\ X(x)}\ \begin{array}{l}y \text{ not free in} \\ \Gamma, X(x), \Delta\end{array}$$

$$\exists\vdash\ \frac{\Gamma, X(y) \vdash \Delta}{\Gamma, \exists x, X(x) \vdash \Delta}\ \begin{array}{l}y \text{ not free in} \\ \Gamma, X(x), \Delta\end{array} \qquad \vdash\exists\ \frac{\Gamma \vdash X(t), \Delta}{\Gamma \vdash \exists x, X(x), \Delta}$$

$$\bot\vdash\ \frac{}{\bot \vdash C} \qquad \vdash\top\ \frac{}{\vdash \top}$$

Fig. 1. Inference rules of LB [26]

$$\Rightarrow\vdash\ \frac{\Gamma, X \Rightarrow Y \vdash X, \Delta \qquad \Gamma, Y \vdash \Delta}{\Gamma, X \Rightarrow Y \vdash \Delta} \qquad \vdash\Rightarrow\ \frac{\Gamma, X \vdash Y}{\Gamma \vdash X \Rightarrow Y, \Delta}$$

$$\forall\vdash\ \frac{\Gamma, X(t), \forall x,\ X(x) \vdash \Delta}{\Gamma, \forall x,\ X(x) \vdash \Delta} \qquad \vdash\forall\ \frac{\Gamma \vdash X(y)}{\Gamma \vdash \forall x,\ X(x), \Delta}\ \begin{array}{l}y \text{ not free in} \\ \Gamma, X(x), \Delta\end{array}$$

$$\exists\vdash\ \frac{\Gamma, X(y) \vdash \Delta}{\Gamma, \exists x, X(x) \vdash \Delta}\ \begin{array}{l}y \text{ not free in} \\ \Gamma, X(x), \Delta\end{array} \qquad \vdash\exists\ \frac{\Gamma \vdash X(t), \exists x, X(x), \Delta}{\Gamma \vdash \exists x, X(x), \Delta}$$

$$\bot\vdash\ \frac{}{\Gamma, \bot \vdash \Delta} \qquad \vdash\bot\ \frac{\Gamma \vdash \Delta}{\Gamma \vdash \bot, \Delta}$$

$$\top\vdash\ \frac{\Gamma \vdash \Delta}{\Gamma, \top \vdash \Delta} \qquad \vdash\top\ \frac{}{\Gamma \vdash \top, \Delta}$$

Fig. 2. Logical rules of LBi

that for $\Rightarrow\vdash$ it is only necessary to apply a contraction in the left premise. We also want to get rid of the weakening rules ($.\vdash$ and $\vdash.$), that are of course non invertible. To do so, we have to allow extra formulæ in $\bot\vdash$ and $\vdash\top$, to add a left rule for $\top$ and a right rule for $\bot$, and to allow weakening below an application of $\vdash\Rightarrow$ and $\vdash\forall$ and into premises of derivations. In so doing, it can be proved that all structural rules are admissible (see Appendix A). The system that we use here will be called LBi ("i" standing for invertible and not intuitionistic). Its logical rules are presented in Fig. 2, except the rules for $\wedge$ and $\vee$ that are the same than in LB. Note that LBi has *no* structural rules. However, LBi is equivalent to LB (see the proof in Appendix A).

Proposition 1. *All inference rules of LBi but* $\vdash\Rightarrow$ *and* $\vdash\forall$ *are invertible. Nonetheless, when there is no extra formula on the right hand side of their conclusion,* $\vdash\Rightarrow$ *and* $\vdash\forall$ *are also invertible.*

2.2 Deduction Modulo

An introduction on term rewriting can be found in [1]. We consider two kinds of rules: the usual term rewrite rules, and proposition rewrite rules defined below. An atomic formula $A(s_1, \ldots, s_i, \ldots, s_n)$ can be rewritten to the atomic formula $A(s_1, \ldots, t_i, \ldots, s_n)$ by a term rewrite rule $l \to r$ if s_i can be rewritten to t_i by $l \to r$. This rewrite relation is extended to non-atomic formulæ by congruence.

A *proposition rewrite rule* is the pair of an atomic proposition A and a proposition P, such that all free variables of P appear in A. It is denoted $A \to P$. A *proposition rewrite system* is a set of proposition rewrite rules. A formula P can be rewritten to a formula Q by the rule $A \to O$ at the position p with substitution σ if the subterm of P at position p equals σA and Q is P where its subterm at position p is replaced by σO.

In the following, a *rewrite system* $\mathcal{R}$ will be the disjoint union of a term rewrite system and a proposition rewrite system. $P \underset{\mathcal{R}}{\longrightarrow} Q$ denotes the fact that P can be rewritten to Q by some term or proposition rewrite rule in $\mathcal{R}$, and $\underset{\mathcal{R}}{\overset{*}{\longrightarrow}}$ (resp. $\underset{\mathcal{R}}{\overset{*}{\longleftrightarrow}}$) denotes the reflexive and transitive (resp. reflexive, symmetric and transitive) closure of $\underset{\mathcal{R}}{\longrightarrow}$.

As said above, deduction modulo consists in applying the inference rules of a deductive system modulo a rewrite system. For instance, in LBi modulo $\mathcal{R}$, the left rule for $\Rightarrow$ becomes

$$\Rightarrow\vdash \frac{\Gamma, Z \vdash X, \Delta \qquad \Gamma, Y \vdash \Delta}{\Gamma, Z \vdash \Delta}\ Z \underset{\mathcal{R}}{\overset{*}{\longleftrightarrow}} X \Rightarrow Y$$

Proving modulo a rewrite system $\mathcal{R}$ is equivalent to proving inside some theory whose presentations are called compatible with $\mathcal{R}$:

Definition 2. *A presentation is a set of formulæ with no free variables. The theory presented by a presentation* Γ *is the set of formulæ* P *such that* $\Gamma' \vdash P$ *can be proved in the sequent calculus for some finite subset* Γ' *of* Γ*.*

Given a rewrite system $\mathcal{R}$, its associated theory is the set of formulæ P such that $\vdash P$ can be proved in the sequent calculus modulo $\mathcal{R}$.

A presentation and a rewrite system $\mathcal{R}$ are said to be compatible *if they are associated with the same theory.*

Note that these definitions depend on the considered logic (e.g. classical or intuitionistic). Propositions 1.6 and 1.8 of [11] prove that a rewrite system always has a compatible presentation. This shows that the theory associated with a rewrite system is a theory in the standard meaning, that is, a deductively closed set of formulæ.

Some automated theorem-proving procedures have been designed based on deduction modulo, e.g. ENAR [11], generalizing resolution, as well as Tamed [5], a tableau method. These methods are complete only if the sequent calculus modulo admits cut. In fact, as proved by Hermant [17], the proofs found by these methods are exactly the cut-free proofs of the asymmetric sequent calculus modulo [9], a variant of the sequent calculus modulo where rewriting can only be applied from bottom to top in the proofs. For instance the left rule for $\Rightarrow$ becomes

$$\Rightarrow\vdash \frac{\Gamma, X \Rightarrow Y \vdash X, \Delta \qquad \Gamma, Y \vdash \Delta}{\Gamma, Z \vdash \Delta}\ Z \xrightarrow[\mathcal{R}]{*} X \Rightarrow Y$$

It can also be useful to distinguish which rules can be applied to the left and to the right of a sequent, or more precisely at positive and negative position in a sequent. Recall that a position in a formula is positive (resp. negative) if it is in the left subformula of an even (resp. odd) number of $\Rightarrow$. Suppose that the rewrite rules are associated with polarities. We denote by $A \rightarrow^{+} P$ the rewrite rule $A \rightarrow P$ associated with a positive polarity, and dually for $-$. A proposition P can be positively rewritten to Q in $\mathcal{R}$ $\left(P \underset{\mathcal{R}\ +}{\longrightarrow} Q\right)$ if P can be rewritten to Q by a positive rule at a positive position or by a negative rule at a negative position. A proposition P can be negatively rewritten to Q in $\mathcal{R}$ $\left(P \underset{\mathcal{R}\ -}{\longrightarrow} Q\right)$ if P can be rewritten to Q by a negative rule at a positive position or by a positive rule at a negative position. In the polarized sequent calculus modulo [8], formulæ in the left (resp. right) of a sequent can only be negatively (resp. positively) rewritten, so that the Ax. rule, for instance, becomes

$$\mathsf{Ax.}\ \frac{}{\Gamma, X \vdash Y, \Delta}\ X \underset{\mathcal{R}\ -}{\longrightarrow} \underset{\mathcal{R}\ +}{\longleftarrow} Y$$

In [7] we proved that for classical logic, the polarized sequent calculus is equivalent to the asymmetric sequent calculus, also w.r.t. the cut admissibility. This also holds for LBi (see Appendix B). The latter is equivalent to the original version of the sequent calculus modulo, but if we are also concerned with cut admissibility, they are equivalent if and only if the rewrite system is confluent. Given a sequent $\Gamma \vdash \Delta$, we denote by $\Gamma \vdash^{S}_{\mathcal{R}} \Delta$ the fact that for finite subsets Γ' and Δ' of Γ and Δ, the sequent $\Gamma' \vdash \Delta'$ can be derived from premises in the set of sequents S, in the polarized LBi modulo $\mathcal{R}$. If S and $\mathcal{R}$ are empty, we write

$\Gamma \vdash \Delta$, which therefore means that there is a proof of $\Gamma' \Vdash \Delta'$ in LBi without modulo.

A (polarized) rewrite system $\mathcal{R}$ is called *analytic* if the polarized sequent calculus modulo $\mathcal{R}$ admits cut, that is, if $\Gamma \vdash_{\mathcal{R}} \Delta$ then $\Gamma \Vdash \Delta$ can be proved in the polarized LBi modulo $\mathcal{R}$ without Cut. In other words, adding Cut does not increase the set of theorems.

Proposition 3 (Disjunction and witness property). *Consider an analytic rewrite system $\mathcal{R}$.*

- *If $\vdash_{\mathcal{R}} P \vee Q$ then either $\vdash_{\mathcal{R}} P$ or $\vdash_{\mathcal{R}} Q$.*
- *If $\vdash_{\mathcal{R}} \exists x.\ P$ then for some $t \in \mathcal{T}(\Sigma, V)$, we have $\vdash_{\mathcal{R}} \{t/x\}P$.*

Proof. If $\vdash_{\mathcal{R}} P \vee Q$, because $\mathcal{R}$ is analytic there is a cut-free proof of $\Vdash P \vee Q$ in the polarized LBi modulo $\mathcal{R}$, and therefore also in the polarized LJ modulo $\mathcal{R}$ (see Appendix B). As the left hand side of proposition rewrite rules are atomic formulæ, if $P \vee Q \xrightarrow[\mathcal{R}\ +]{*} O$ then the connector at the root of O has to be $\vee$, so that the only rule that can be applied is $\Vdash\vee$, hence the conclusion. The proof of the witness property is similar. □

3 Undecidability of the Automation

As we saw in the introduction, the theory $A \vee B$ with A and B atomic cannot be transformed into an analytic compatible rewrite system. Therefore, we may want to characterize the theories that have an analytic compatible rewrite system, and to find an algorithm to build such rewrite systems. We prove in this section that it cannot be done through a decidable characterization, because the set of such theories is no co-recursively enumerable. In other words, if we have a procedure that transforms a presentation into an analytic compatible rewrite system, it would either be incomplete, that is, the procedure would not answer for some theories that do have an analytic compatible rewrite system, or it would not always terminate.

Theorem 4. *The set of presentations that can be transformed into an analytic compatible rewrite system is not co-recursively enumerable.*

Proof. Recall that the set of valid formulæ in classical first-order logic is not co-recursively enumerable. Using the double-negation translation, neither is the set of valid formulæ in intuitionistic first-order logic. We prove that a formula P is intuitionistically valid iff the presentation $\{(A \Rightarrow P) \vee A\}$ can be transformed into an analytic compatible rewrite system.

Let P be a formula and A an atomic formula not appearing in P. We do not have $(A \Rightarrow P) \vee A \vdash A$: it does not hold in classical logic, so neither does it hold in intuitionistic logic.

Suppose that P is intuitionistically valid. Then so is $(A \Rightarrow P) \vee A$. Consequently, the theory presented by $(A \Rightarrow P) \vee A$ is the theory presented by an

empty set of axioms. Consider the empty rewrite system. It is therefore compatible with $(A \Rightarrow P) \vee A$, and the sequent calculus modulo the empty rewrite system admits cuts. Thus, the theory presented by $(A \Rightarrow P) \vee A$ has an analytic compatible rewrite system.

Conversely, suppose that the theory presented by $(A \Rightarrow P) \vee A$ has an analytic compatible rewrite system $\mathcal{R}$. By compatibility, $\vdash_{\mathcal{R}} (A \Rightarrow P) \vee A$. By Proposition 3, either $\vdash_{\mathcal{R}} A \Rightarrow P$ or $\vdash_{\mathcal{R}} A$. In the latter case, that would mean by compatibility that $(A \Rightarrow P) \vee A \vdash A$, but this does not hold as mentioned above. Hence $\vdash_{\mathcal{R}} A \Rightarrow P$ and by compatibility $(A \Rightarrow P) \vee A \vdash A \Rightarrow P$. Because $\vee\vdash$ is invertible, $A \vdash A \Rightarrow P$. Because $\vdash\Rightarrow$ is invertible when there is only one formula on the right hand side, $A \vdash P$. Because A is atomic and does not appear in P, it cannot be used in this proof, so that $\vdash P$. By soundness of LBi, P is valid.

We therefore reduced the problem of deciding validity in intuitionistic first-order logic to the problem of deciding whether a theory has an analytic compatible rewrite system. The set of theories having one is therefore not co-recursively enumerable. □

4 A Procedure to Produce Compatible Rewrite Systems

In this section, we try to find a way to transform the presentation of a theory into a compatible rewrite system, whishing this rewrite system to be analytic. Because of Theorem 4, it is not possible to find a terminating algorithm producing such a rewrite system in all cases where it is possible to find one. The procedure that we propose does not contradict this because it may not terminate. However, we try to avoid cases where it would unnecessarily fail.

To ease the description, we present the procedure by a set of transition rules as is traditional for completion procedures, e.g. in [3]. The procedure is therefore non-deterministic and may not terminate, in particular when the theory does not have a compatible rewrite system. Transition rules, which are given below in Procedure 1, transform a set of sequents S and a set of polarized rewrite rules $\mathcal{R}$. Given a presentation Θ, the input to the procedure is $\{\vdash P \ : \ P \in \Theta\}$ for the set of sequents, and the empty rewrite system. Let us describe the transition rules. **Orient**+ and **Orient**− transform a sequent containing an atomic formula into rewrite rules. These are the base cases. Note that in **Orient**+ the right hand side only contains one formula. Sequents with several formulæ on the right and no atomic formula on the left are therefore the potential failure cases. To obtain sequents in which there are atomic formulæ, one may apply the inference rules of LBi. This is what **Decompose** does, with the proviso that the inference rules are invertible to remain in the same theory. Contrary to classical logic, there remains sequents that cannot be transformed into rewrite rules even though there exists a compatible rewrite system. **Discard** and **Delete** permit to deal with these sequents. **Delete** is not really necessary, but it permits to eliminate redundancies in the construction of the rewrite system. In particular, it gets rid of tautologies such as those used in the proof of Theorem 4. The rewrite systems

Procedure 1 Transition rules to compute a compatible rewrite system

Orient+	$S \cup \{\Gamma \vdash A\}, \mathcal{R} \rightsquigarrow S, \mathcal{R} \cup \{A \rightarrow^{+} \exists x_1, \ldots, x_n.\ \bigwedge \Gamma\}$ if A atomic and $\{x_1, \ldots, x_n\} = FV(\Gamma) \setminus FV(A)$
Orient−	$S \cup \{\Gamma, A \vdash \Delta\}, \mathcal{R} \rightsquigarrow S, \mathcal{R} \cup \{A \rightarrow^{-} \forall x_1, \ldots, x_n.\ \bigwedge \Gamma \Rightarrow \bigvee \Delta\}$ if A atomic and $\{x_1, \ldots, x_n\} = FV(\Gamma, \Delta) \setminus FV(A)$
Decompose	$S \cup \{\Gamma \vdash \Delta\}, \mathcal{R} \rightsquigarrow S \cup \bigcup_{1 \leq i \leq n} \{\Gamma_i \vdash \Delta_i\}, \mathcal{R}$ if $\mathsf{r}\ \dfrac{\Gamma_1 \vdash \Delta_1 \quad \cdots \quad \Gamma_n \vdash \Delta_n}{\Gamma \vdash \Delta}$ is invertible
Discard	$S \cup \{\Gamma \vdash P, \Delta\}, \mathcal{R} \rightsquigarrow S \cup \{\Gamma \vdash \Delta\}, \mathcal{R}$ if $\Gamma, P \vdash^{S}_{\mathcal{R}} \Delta$
Delete	$S \cup \{\Gamma \vdash \Delta\}, \mathcal{R} \rightsquigarrow S, \mathcal{R}$ if $\Gamma \vdash^{S}_{\mathcal{R}} \Delta$ without Cut
Deduce	$S, \mathcal{R} \rightsquigarrow S \cup \{\Gamma \vdash \Delta\}, \mathcal{R}$ if $\Gamma \vdash \Delta \in CP(\mathcal{R})$

produced by all these rules may nevertheless not admit cuts, as shown by the example $A \Leftrightarrow A \Rightarrow B$ which can lead to the rewrite rules $A \rightarrow^{+} A \Rightarrow B$ and $A \rightarrow^{-} A \Rightarrow B$ (see the introduction). **Deduce** completes the theory to recover the cut admissibility. The set $CP(\mathcal{R})$ is the set of conclusions of critical proofs of $\mathcal{R}$. A critical proof of $\mathcal{R}$ is a proof of the form $\mathsf{Cut}\ \dfrac{\overset{\pi}{\Gamma, P \vdash \Delta} \qquad \overset{\pi'}{\Gamma \vdash Q, \Delta}}{\Gamma \vdash \Delta}$ where

- P, Q is a critical pair of $\mathcal{R}$, i.e. there exists A atomic such that $P \underset{\mathcal{R}}{\longleftarrow} A \underset{\mathcal{R}}{\longrightarrow} Q$;
- π and π' are cut-free;
- P (resp. Q) is the principal formula of the last inference rule of π (resp. π');
- all formulæ in Γ, Δ are principal in one of the inference rules of π or π';
- there is no cut-free proof of $\Gamma \vdash \Delta$ modulo $\mathcal{R}$.

Example 5. Given the axiom $A \vee (B \Rightarrow A)$, we apply **Decompose** to get $\vdash A, B \Rightarrow A$. Because $A \vdash B \Rightarrow A$, we can apply **Discard** to change $\vdash A, B \Rightarrow A$ into $\vdash B \Rightarrow A$. We apply **Decompose** to get $B \vdash A$. We have the choice between **Orient**+ and **Orient**− to get either the rewrite rule $B \rightarrow^{-} A$ or the rule $A \rightarrow^{+} B$, both of them which are analytical rewrite systems compatible with $A \vee (B \Rightarrow A)$.

Example 6. Consider the axioms $A \Rightarrow B \Rightarrow \bot$ and $(A \Rightarrow B \Rightarrow \bot) \Rightarrow A$. If we apply **Decompose** and **Orient**− on the former, we obtain the rule 1: $A \rightarrow^{-} B \Rightarrow \bot$. On the latter, we can apply **Decompose** and **Orient**+ to get the rule 2: $A \xrightarrow{+} A \Rightarrow B \Rightarrow \bot$. There is a critical proof with the two rules we have obtained (numbers indicate which rewrite rules are used modulo):

$$\dfrac{\dfrac{\mathsf{Ax}.\ \dfrac{}{B \Rightarrow \bot, B \vdash B} \quad \bot\vdash \dfrac{}{\bot, B \vdash}}{\Rightarrow\vdash\ B \Rightarrow \bot, B \vdash} \quad \dfrac{\mathsf{Ax}.\ \dfrac{}{B, A \vdash B \Rightarrow \bot}\ 1}{\vdash\Rightarrow\ B \vdash A \Rightarrow B \Rightarrow \bot}}{\mathsf{Cut}\ \dfrac{}{B \vdash}}\ 1{,}2$$

Using **Deduce**, we therefore add $B \vdash$ to S. It can be oriented into 3: $B \xrightarrow{-} \bot$. The resulting rewrite system, consisting of the rules 1 to 3, is compatible with the input axioms and is analytical.

We first prove that the procedure produces compatible rewrite systems:

Proposition 7. *If $S, \mathcal{R} \rightsquigarrow S', \mathcal{R}'$ then for all sequents $\Gamma \vdash \Delta$, we have $\Gamma \vdash^S_{\mathcal{R}} \Delta$ iff $\Gamma \vdash^{S'}_{\mathcal{R}'} \Delta$.*

Moreover, if the derivation of $\Gamma \vdash^S_{\mathcal{R}} \Delta$ is Cut*-free, so is the derivation of $\Gamma \vdash^{S'}_{\mathcal{R}'} \Delta$.*

Proof. We prove it by cases on the transition rules. For **Orient**+, for the "only if" direction, it is enough to show that $\Gamma \vdash A$ can be proved without Cut in $A \to^+ \exists x_1, \ldots, x_n.\ \bigwedge \Gamma$, which is easy. For the "if" direction, we proceed by induction on the lexicographic order of the number of rewrite steps using the rule $A \to^+ \exists x_1, \ldots, x_n.\ \bigwedge \Gamma$ and the structure of the proof. Except for Cut, the application of an inference rule in LBi modulo $\mathcal{R}$ can be decomposed into an application of r without modulo followed by an explicit conversion rule (two for Ax.) of the form

$$\uparrow^* \vdash \frac{\Gamma, Q \vdash \Delta}{\Gamma, P \vdash \Delta}\, P \xrightarrow[\mathcal{R}\ -]{*} Q \qquad \text{or} \qquad \vdash \uparrow^* \frac{\Gamma \vdash Q, \Delta}{\Gamma \vdash P, \Delta}\, P \xrightarrow[\mathcal{R}\ +]{*} Q \quad .$$

For Cut, we need two explicit conversions above the application of Cut without modulo. Consider the last application of an inference rule in a derivation of $\Gamma' \vdash \Delta'$ modulo $\mathcal{R} \cup \{A \to^+ \exists x_1, \ldots, x_n.\ \bigwedge \Gamma\}$, and decompose it as shown above. If the explicit conversion step does not use $A \to^+ \exists x_1, \ldots, x_n.\ \bigwedge \Gamma$, then we proceed by structural induction on the proof. Otherwise, suppose that $\Gamma' = P, \Sigma$ where P is negatively rewritten by $A \to^+ \exists x_1, \ldots, x_n.\ \bigwedge \Gamma$ into Q. By the induction hypothesis, we obtain a derivation of $Q, \Sigma \vdash \Delta$ in $\mathcal{R}$. From $\Gamma \vdash A$ we can derive $\exists x_1, \ldots, x_n.\ \bigwedge \Gamma \vdash A$, and using Lemma 15, we know how to build a derivation of $P \vdash Q$. Using a Cut, we therefore have a derivation of $P, \Sigma \vdash \Delta$, as expected. The case where the rewriting occurs in Δ is dual.

The case of **Orient**− is dual.

For **Decompose**, this results from the fact that r is supposed invertible.

For **Discard**, for the "only if" part is obtained by weakening. For the "if" direction, we replace the premise $\Gamma \vdash \Delta$ by a Cut between the premise $\Gamma \vdash P, \Delta$ and the derivation of $\Gamma, P \vdash^S_{\mathcal{R}} \Delta$.

For **Delete**, the "if" part is trivial. For the "only if" direction, replace the premises $\Gamma \vdash \Delta$ by the cut-free derivation $\Gamma \vdash^S_{\mathcal{R}} \Delta$.

For **Deduce**, the "only if" part is trivial. For the "if" direction, because $\Gamma \vdash \Delta \in CP(\mathcal{R})$, it is the conclusion of a proof modulo $\mathcal{R}$. We can therefore replace the premises $\Gamma \vdash \Delta$ by this proof.

Remark that for the "only if" direction, we never added Cuts. □

Corollary 8. *Given a presentation Θ, if $\{\vdash P : P \in \Theta\}, \emptyset \rightsquigarrow^* \emptyset, \mathcal{R}$, then Θ and $\mathcal{R}$ are compatible.*

Proof. A proof $\Theta \vdash Q$ can be seen as a derivation $\vdash^{\{\vdash P : P \in \Theta\}} Q$ by replacing $\mathsf{Ax.}\ \dfrac{}{\Theta \vdash P}$ where $P \in \Theta$ by the premise $\vdash P$. □

As usual in completion procedures, we need a fairness condition to ensure that all critical proofs are dealt with. This condition is the following: at any moment, if $\Gamma \vdash \Delta \in CP(\mathcal{R}) \setminus S$ then **Deduce** will eventually add $\Gamma \vdash \Delta$ in the set of sequents.

Proposition 9. *Under this fairness condition, if the procedure terminates and produces $\emptyset, \mathcal{R}$, then $\mathcal{R}$ is analytic.*

Proof. Suppose that $\mathcal{R}$ is not analytic. There exists a sequent that can be proved with Cut but not without. Consider proofs as trees of couple of inference rules and principal formula, and define the recursive path ordering defined by the following precedence: $(\mathsf{Cut}, P) > (\mathsf{Ax.}, Q) > (\mathsf{r}, R)$ for all inference rules r different from Cut and $\mathsf{Ax.}$, and all formulæ P, Q, R; and $(\mathsf{Cut}, P) > (\mathsf{Cut}, Q)$ and $(\mathsf{Ax.}, P) > (\mathsf{Ax.}, Q)$ if Q is a subformula of P. As the precedence is well-founded, so is this ordering. By induction on this ordering, and following the cut-elimination procedure as described in [16], we can find a proof of the form $\mathsf{Cut}\ \dfrac{\overset{\pi}{\Gamma, P \vdash \Delta} \qquad \overset{\pi'}{\Gamma \vdash Q, \Delta}}{\Gamma \vdash \Delta}$ where

- P, Q is a critical pair of $\mathcal{R}$, i.e. there exists A atomic such that $P \underset{\mathcal{R}}{\longleftarrow} A \underset{\mathcal{R}}{\longrightarrow} Q$;
- π and π' are cut-free;
- P (resp. Q) is the principal formula of the last inference rule of π (resp. π');
- there is no cut-free proof of $\Gamma \vdash \Delta$ modulo $\mathcal{R}$.

In this proof, we can prune all formulæ that are not principal in one of the inference rules of π or π', and we therefore obtain a critical proof. By the fairness assumption, the sequent $\Gamma \vdash \Delta$ has been added to S during the procedure. By Proposition 7, the Cut-free derivation $\Gamma \vdash \Delta$ using the premise $\Gamma \vdash \Delta$ has been transformed by the procedure into a Cut-free derivation using premises in $\emptyset$ and rewrite rules in $\mathcal{R}$. We therefore have a Cut-free *proof* of $\Gamma \vdash \Delta$ modulo $\mathcal{R}$, hence the contradiction. □

Note that Procedure 1 is not computable, in the sense that **Discard**, **Delete** and **Deduce** use oracles that are not recursive. Indeed, the sets $\vdash^S_{\mathcal{R}}$ and $CP(\mathcal{R})$ are not co-recursively enumerable in general. Nonetheless, we believe that it is not possible to do better, because we conjecture the set described in Theorem 4 to be Σ^0_3-complete in the arithmetical hierarchy (see [4, Chapter C.1] for an introduction on the arithmetical hierarchy), that is, it is not even recursively enumerable. Once this conjecture has been proved, we could try to prove that our procedure with oracles is complete, that is, for all presentations that can be transformed into an analytic rewrite system, the procedure terminates without failure. Of course, in the case where the procedure fails, we can keep the remaining sequents in S and use them either as premises, or, if we only want to work with proofs and not derivations, we can transform these sequents $\Gamma \vdash \Delta$ into axioms $\forall x_1, \ldots, x_n.\ \bigwedge \Gamma \Rightarrow \bigvee \Delta$ with $\{x_1, \ldots, x_n\} = FV(\Gamma, \Delta)$.

5 Extensions

In this section, we present some extensions to the procedure presented in the previous section. For lack of space, we only briefly discuss them.

Axiom Schemata. Theories are often presented not only by axioms but also by axiom schemata. An axiom schema is a formula in which proposition variables can appear. The instance of an axiom schema are the formulæ where these proposition variables are substituted by formulæ. For instance, the induction principle in Peano's arithmetic $\forall x.\ (X(0) \wedge \forall y.\ X(y) \Rightarrow X(s(y))) \Rightarrow X(x)$ is an axiom schema with the proposition variable $X(x)$. An instance of this axiom schema is $\forall x.\ (0 + 0 = 0 \wedge \forall y.\ y + 0 = y \Rightarrow s(y) + 0 = s(y)) \Rightarrow x + 0 = x$ where $X(x)$ being substituted by $x + 0 = x$.

Axiom schemata can be seen as the infinite set of their instances, so that our procedure works on such presentations. However, in that case, $\mathcal{R}$ may be infinite. The rewrite relation would therefore not be implementable as it is. If the theory is presented by a finite set of axiom schemata, we can use the work of Kirchner [18] who shows how to get a finitely presented conservative extension of the theory. We can then apply Procedure 1 to this finite presentation and obtain a finite rewrite system if it terminates.

Equalities. First-order theories often use equality, for instance in Peano's arithmetic we have the axiom $\forall x.\ 0 + x = x$. Such axioms are better represented by term rewrite rules instead of proposition rewrite rules. In this example, $0+x \to x$ is better than $0 + x = x \to \top$. Therefore, given a presentation, before applying our procedure, a better approach is to take away the equational logic subset of the presentation (axioms of the form $\forall x_1, \ldots, x_n.\ s = t$) and to apply standard tools to it, for instance Knuth-Bendix completion [20], to obtain a compatible confluent term rewrite system for that subset. Then, we apply Procedure 1 to the remaining axioms.

Skolemization. The theory presented by $\exists x.\ A(x)$ has no analytic compatible rewrite system, because it does not have the witness property. However, for some new constant c not appearing in the original signature, $A(c)$ is a presentation of a conservative extension of this theory that does have an analytic compatible rewrite system, e.g. $A(c) \to^+ \top$. Nevertheless, contrary to classical logic, Skolemization does not always lead to a conservative extension in intuitionistic logic. Mints [22] characterizes the presentations that can be correctly Skolemized. One improvement is therefore to apply Skolemization on those cases before applying Procedure 1. Nevertheless, even doing so, we will not be able to handle presentations such as $\neg\neg\exists x.\ A(x)$.

Baaz and Iemhoff [2] propose a generalization of Skolemization which works every time. To sum up the idea, formulæ are translated into their semantic in a Kripke structure. As the semantic of a Kripke model is defined in classical logic, the translated formulæ can be Skolemized. For our purpose, we do not even need to Skolemize these formulæ. Instead, we can apply the completion procedure for

classical logic described in [7] to the translated presentation. Indeed, Baaz and Iemhoff proved that a formula is valid in intuitionistic logic iff its translation is valid in classical logic [2, Lemma 11]. However, we think that this is probably highly inefficient, in particular because of the transitivity of the accessibility relation in Kripke structures.

6 Example of Application

We can apply Procedure 1 to one of the axiom sets proposed in the Intuitionistic Logic Theorem Proving library [24], for instance the presentation of constructive geometry derived from [25] (files `GEJxxx+1.ax`). We obtain an analytic compatible rewrite system including among others the three following rules:

$$x \neq_p y \rightarrow^{-} \neg x \notin ln(x,y) \qquad (\texttt{GEJ002+1.ax}, \text{a1})$$

$$x \neq_p y \rightarrow^{-} \neg y \notin ln(x,y) \qquad (\texttt{GEJ002+1.ax}, \text{a2})$$

$$x \neq_p y \rightarrow^{-} \forall u\ v.\ u \neq_l v \Rightarrow (x \notin u \vee x \notin v \vee y \notin u \vee y \notin v) \qquad (\texttt{GEJ003+1.ax}, \text{a1})$$

The theorem proposed in the problem `GEJ001+1.p` therefore has the following proof in which Γ stands for $x \neq_p y, \neg x \notin z, \neg y \notin z, z \neq_l ln(x,y)$ and the inference rules that are applied modulo are marked by *:

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{}{z \neq_l ln(x,y) \vdash z \neq_l ln(x,y)}\,\text{Ax.}}{\Rightarrow\vdash} \quad \dfrac{\dfrac{\dfrac{}{x \notin z \vdash x \notin z}\,\text{Ax.}}{\neg\vdash} \quad \dots \quad \dfrac{\dfrac{}{y \notin ln(x,y) \vdash y \notin ln(x,y)}\,\text{Ax.}}{\neg\vdash}\,*}{\vee\vdash}}{z \neq_l ln(x,y) \Rightarrow (x \notin z \vee x \notin ln(x,y) \vee y \notin z \vee y \notin ln(x,y)), \Gamma \vdash}}{\forall\vdash}\,*}{\vdash\Rightarrow}}{\wedge\vdash}}{\vdash\Rightarrow}}{\vdash\forall}$$

7 Conclusion

We have proposed a method to find automated theorem proving procedures adapted to proof search in a particular intuitionistic theory. The idea is to transform a presentation of the theory into a rewrite system, and to combine the inference rules of a sequent calculus with rewriting. We first proved that it is not decidable to transform the presentation of a theory into a rewrite system with an analytic sequent calculus modulo. We nonetheless proposed a (possibly nonterminating) procedure to do so, covering a large class of presentations. We then extended the domain of applicability of this procedure by working in conservative extensions of the theories we want to automate, to get finite presentations, to better handle equality and to partially authorize Skolemization. This work opens new challenges that we are now considering.

First, we would like to know the precise hardness in the arithmetical hierarchy of the transformation of a presentation into a compatible analytic rewrite system , and to prove that Procedure 1 is complete, or to find a complete procedure, in order to be able to transform all presentations that can be. Besides, the procedure only guarantees the Cut admissibility, and not the strong normalization. It would be interesting to refine the procedure to also have it, for instance because strong normalization helps at conceiving proof checkers. Note that if we are only interested in automated proof search, the normalization is less crucial, because the admissibility of cuts suffices to ensure the completeness of the proof-search procedures. Also, remark that the rewrite system produced by Procedure 1 may be not confluent. The original version of the sequent calculus modulo may therefore not be equivalent to the polarized version. Nonetheless, this is not problematic because we are mainly interested in the automated proving procedures based on deduction modulo, which are equivalent to the cut-free portion of the polarized version. Another interesting point is the combination of theories. Given two theories whose presentations have been transformed into analytic compatible rewrite systems, in which cases would the union of the rewrite system still be analytic? Investigating this question implies the study of modularity in deduction modulo.

We also need to implement Procedure 1. To control its non-termination, we can resort to iterative deepening, that is, incrementally limiting the number of times that $\Rightarrow\vdash$, $\forall\vdash$ and $\vdash\exists$ can be applied. We should link this implementation with a theorem prover based on deduction modulo that will serve as an oracle to compute $\vdash^S_{\mathcal{R}}$ and $CP(\mathcal{R})$.

Finally, we have researched how theories can be presented in deduction modulo. We could also examine how deductive systems can be encoded in it, in order to use deduction modulo as a logical framework. It was already proven that deduction modulo can encode HOL [10] and every functional pure type system [6]. An interesting issue is to automate how to find out such encodings.

Acknowledgments This work was partly supported by the Inria ARC Corias. The author wishes to thank C. Kirchner for his support and helpful discussions about this topic, and M. Boespflug for his useful comments.

References

1. Baader, F., Nipkow, T.: Term *Re*writing and *all That*. Cambridge University Press (1998)
2. Baaz, M., Iemhoff, R.: On Skolemization in constructive theories. The Journal of Symbolic Logic **73** (2008) 969–998
3. Bachmair, L., Dershowitz, N.: Completion for rewriting modulo a congruence. In: Proceedings 2nd Conference on Rewriting Techniques and Applications, Bordeaux (France). LNCS, Vol. 256., Bordeaux (France), Springer (1987) 192–203
4. Barwise, J. (ed.): Handbook of Mathematical Logic. 4th printing edn. Elsevier Science Publishers B. V. (North-Holland) (1985)

5. Bonichon, R., Hermant, O.: On constructive cut admissibility in deduction modulo. In: Altenkirch, T., McBride, C. (eds.): TYPES. LNCS, Vol. 4502. Springer (2006) 33–47
6. Burel, G.: A first-order representation of pure type systems using superdeduction. In: Pfenning, F. (ed.): LICS. IEEE Computer Society (2008) 253–263
7. Burel, G., Kirchner, C.: Regaining cut admissibility in deduction modulo using abstract completion. Submitted (2008)
8. Dowek, G.: What is a theory? In: Alt, H., Ferreira, A. (eds.): STACS. LNCS, Vol. 2285. Springer (2002) 50–64
9. Dowek, G.: Confluence as a cut elimination property. In: Nieuwenhuis, R. (ed.): RTA. LNCS, Vol. 2706. Springer (2003) 2–13
10. Dowek, G., Hardin, T., Kirchner, C.: HOL-$\lambda\sigma$ an intentional first-order expression of higher-order logic. Mathematical Structures in Computer Science **11** (2001) 1–25
11. Dowek, G., Hardin, T., Kirchner, C.: Theorem proving modulo. Journal of Automated Reasoning **31** (2003) 33–72
12. Dowek, G., Miquel, A.: Cut elimination for Zermelo's set theory. Available on authors' web page (2006)
13. Dowek, G., Werner, B.: Arithmetic as a theory modulo. In: Giesl, J. (ed.): RTA. LNCS, Vol. 3467. Springer (2005) 423–437
14. Gallier, J.H.: Logic for Computer Science: Foundations of Automatic Theorem Proving. Computer Science and Technology Series, Vol. 5. Harper & Row, New York (1986) Revised On-Line Version (2003), `http://www.cis.upenn.edu/~jean/gbooks/logic.html`.
15. Gentzen, G.: Untersuchungen über das logische Schliessen. Mathematische Zeitschrift **39** (1934) 176–210, 405–431
16. Girard, J.Y., Lafont, Y., Taylor, P.: Proofs and Types. Cambridge Tracts in Theoretical Computer Science, Vol. 7. Cambridge University Press (1989)
17. Hermant, O.: Semantic cut elimination in the intuitionistic sequent calculus. In: Urzyczyn, P. (ed.): TLCA. LNCS, Vol. 3461. Springer (2005) 221–233
18. Kirchner, F.: A finite first-order theory of classes. In: Altenkirch, T., McBride, C. (eds.): TYPES. LNCS, Vol. 4502. Springer (2006) 188–202
19. Kleene, S.C.: Mathematical Logic. John Wiley, New York, USA (1967)
20. Knuth, D.E., Bendix, P.B.: Simple word problems in universal algebras. In: Leech, J. (ed.): Computational Problems in Abstract Algebra. Pergamon Press, Oxford (1970) 263–297
21. Maehara, S.: Eine Darstellung der intuitionistischen Logik in der klassischen. Nagoya Mathematical Journal **7** (1954) 45–64
22. Mints, G.: The Skolem method in intuitionistic calculi. Proc. Steklov Inst. Math. **121** (1974) 73–109
23. Mints, G.: A Short Introduction to Intuitionistic Logic. The University series in mathematics. Kluwer Academic Publishers (2000)
24. Raths, T., Otten, J., Kreitz, C.: The ILTP problem library for intuitionistic logic, release v1.1. Journal of Automated Reasoning **38** (2007) 261–271 Website: `http://www.iltp.de/`.
25. von Plato, J.: The axioms of constructive geometry. Annals of Pure and Applied Logic **76** (1995) 169–200
26. Waaler, A., Wallen, L.: Tableaux for Intutionistic Logics. In: Handbook of Tableau Methods. Kluwer Academic Publishers, Boston (1999)

A Properties of LBi

We introduce the notion of proof skeleton. Indeed, we need to prove some lemmata by induction on the proof structure, but without caring about formulæ that can be pruned.

Definition 10. *The* proof skeleton *associated with a proof is the tree whose nodes are the inference rules of the proof. Proof skeletons are ordered by the subtree relation, which is well-founded.*

We first prove that LBi admits the structural rules:

Lemma 11. *If $\Gamma \vdash \Delta$ then $\Gamma, P \vdash \Delta$ and $\Gamma \vdash P, \Delta$ with the same proof skeleton.*

Proof. By induction on the proof structure. □

Proposition 12. *All inference rules of LBi but $\vdash\Rightarrow$ and $\vdash\forall$ are invertible, and the proofs of their premises is smaller or equal for the proof skeleton ordering. Nonetheless, when there is no extra formula on the right hand side of their conclusion, $\vdash\Rightarrow$ and $\vdash\forall$ are also invertible, with the same property about the proof skeleton ordering.*

Proof. We prove it by induction on the proof skeleton ordering. We only detail the most relevant cases.

For all rules r but $\forall\vdash$, $\vdash\exists$, $\Rightarrow\vdash$, $\vdash\Rightarrow$ and $\vdash\forall$, either the last inference rule in the proof of the conclusion of r is r, in which case this is trivial, or we can proceed by induction. For instance, if we have a proof finishing by

$$\vee\vdash \frac{\Gamma, P, R \wedge S \vdash \Delta \qquad \Gamma, Q, R \wedge S \vdash \Delta}{\Gamma, P \vee Q, R \wedge S \vdash \Delta}$$

then by induction hypothesis we have proofs of $\Gamma, P, R, S \vdash \Delta$ and $\Gamma, Q, R, S \vdash \Delta$ and therefore we can build a proof of $\Gamma, P \vee Q, R, S \vdash \Delta$.

For $\forall\vdash$, $\vdash\exists$, the premises of the inference rule can be obtained by weakening the proof of its conclusion.

For $\Rightarrow\vdash$, for the left premise we use weakening, for the right we use induction with permutations as above.

For $\vdash\Rightarrow$ and $\vdash\forall$ when there is no extra formula on the right hand side of their conclusion, either the formula on the right hand side is principal somewhere in the proof of the conclusion, in which case we can permute rules to put it at the end of the proof, or it is nowhere principal, so that we can prune it and add the side formulæ by weakening to get the premise. □

Lemma 13. *If $\Gamma, P, P \vdash \Delta$ then $\Gamma, P \vdash \Delta$ with a smaller or equal proof skeleton. and if $\Gamma \vdash P, P, \Delta$ then $\Gamma \vdash P, \Delta$ with a smaller or equal proof skeleton.*

Proof. By induction on the proof skeleton ordering. For all cases but when P is $Q \Rightarrow S$ or $\forall x.\, Q$ on the right hand side, we can use the invertibility of the rule to decompose P twice, apply the induction hypothesis on the resulting proofs and

then apply the inference rule to recompose P. For instance, if we have $\Gamma, P \vee Q, P \vee Q \vdash \Delta$, we use the invertibility of $\vee\vdash$ twice to obtain $\Gamma, P, Q, P, Q \vdash \Delta$. We apply the induction hypothesis twice to get $\Gamma, P, Q, \vdash \Delta$ (note the importance to state that the contracted proof is smaller or equal for the proof skeleton ordering). We apply $\vee\vdash$ to get $\Gamma, P \vee Q \vdash \Delta$.

If P is $Q \Rightarrow S$ or $\forall x.\ Q$, we reason by case: Either the principal formula of the last inference rule in $\Gamma \vdash P, P, \Delta$ is P, in which case the other P and Δ are discarded in the proof above. We can therefore discard the other P in the conclusion. For instance if we have

$$\vdash\Rightarrow \frac{\Gamma, R \vdash S}{\Gamma \vdash R \Rightarrow S, R \Rightarrow S, \Delta}$$

we can build

$$\vdash\Rightarrow \frac{\Gamma, R \vdash S}{\Gamma \vdash R \Rightarrow S, \Delta}$$

Or we can use the induction hypothesis on the subproofs and apply the last inference rule to get $\Gamma \vdash P, \Delta$. For instance, if we have

$$\vee\vdash \frac{\Gamma, P \vdash R \Rightarrow S, R \Rightarrow S, \Delta \qquad \Gamma, Q \vdash R \Rightarrow S, R \Rightarrow S, \Delta}{\Gamma, P \vee Q \vdash R \Rightarrow S, R \Rightarrow S, \Delta}$$

then by induction hypothesis we have $\Gamma, P \vdash R \Rightarrow S, \Delta$ and $\Gamma, Q \vdash R \Rightarrow S, \Delta$ and we can apply $\vee\vdash$ to get $\Gamma, P \vee Q \vdash R \Rightarrow S, \Delta$. □

Proposition 14. *LBi and LB are equivalent.*

Proof. We first consider how LB rules are admissible in LBi:

- The lemmata above shows that structural rules are admissible in LBi.
- $\Rightarrow\vdash$(LB) is admissible by using weakening and applying $\Rightarrow\vdash$(LBi). This is the same for $\forall\vdash$, $\vdash\exists$, $\bot\vdash$ and $\vdash\top$.
- $\vdash\Rightarrow$(LB) is a particular case of $\vdash\Rightarrow$(LBi) where $\Delta = \emptyset$. This is the same for $\vdash\forall$.
- $\wedge\vdash$, $\vdash\wedge$, $\vee\vdash$, $\vdash\vee$ and $\exists\vdash$ are the same in LB and LBi.

Conversely, we consider how LBi rules are admissible in LB:

- $\Rightarrow\vdash$(LBi) is admissible by using weakening on the right, applying $\Rightarrow\vdash$(LB) and applying $\cdot\cdot\vdash$. This is the same for $\forall\vdash$ and $\vdash\exists$.
- $\vdash\Rightarrow$(LBi) is obtained by applying $\vdash\Rightarrow$(LB) and applying weakenings. This is the same for $\vdash\forall$, $\bot\vdash$ and $\vdash\top$.
- $\vdash\bot$ and $\top\vdash$ are particular instances of $\cdot\vdash$ and $\vdash\cdot$.

□

B Properties of polarized LBi

Lemma 15.
If $P \underset{+}{\longrightarrow} Q$ *using the rule* $A \to^+ R$*, then we can derive* $Q \vdash P$ *from* $R \vdash A$.
If $P \underset{+}{\longrightarrow} Q$ *using the rule* $A \to^- R$*, then we can derive* $Q \vdash P$ *from* $A \vdash R$.
If $P \underset{-}{\longrightarrow} Q$ *using the rule* $A \to^+ R$*, then we can derive* $P \vdash Q$ *from* $R \vdash A$.
If $P \underset{-}{\longrightarrow} Q$ *using the rule* $A \to^- R$*, then we can derive* $P \vdash Q$ *from* $A \vdash R$.

Proof. By mutual induction on the position where the rewriting occurs. □

We now prove the equivalence between polarized and asymmetric sequent calculi modulo: Given a non-polarized rewrite system $\mathcal{R}$, it is trivial to find a polarized rewrite system $\mathcal{R}^{\pm}$ such that the asymmetric LBi modulo $\mathcal{R}$ is equivalent to the polarized LBi modulo $\mathcal{R}^{\pm}$: simply consider two rules $A \to^+ P$ and $A \to^- P$ for each rule $A \to P$ in $\mathcal{R}$.

Conversely, given a polarized rewrite system $\mathcal{R}$, we can define a non-polarized rewrite system $\mathcal{R}^{\mp}$:

- $A \to^+ P$ becomes $A \to A \vee P$;
- $A \to^- P$ becomes $A \to A \wedge P$.

Proposition 16. *$\Gamma \vdash \Delta$ can be proved in the polarized LBi modulo $\mathcal{R}$ iff it can be proved in the asymmetric LBi modulo $\mathcal{R}^{\mp}$.*

Proof. A formal proof would require an induction on the structure of the proof. The proof for classical logic, as can be found in [7], can easily be adapted for LBi. To give the idea, suppose that a rule $A \to^+ P$ is used somewhere in the proof. If P is the principal formula elsewhere in the proof, it is necessarily on the right of the sequent because of the polarity conditions. If we rewrite A into $A \vee P$ instead, we can first apply $\vdash\vee$ in the place where P is principal. This is dual for the negative rule.

Conversely, suppose that $A \to A \vee P$ is used somewhere in the proof. If $A \vee P$ is principal on the right of a sequent, it means that the rewriting occurred at a positive position. We can instead use weakening and the rewrite by $A \to^+ P$ in the position where $A \vee P$ is principal. If $A \vee P$ is principal on the left of a sequent, we get a proof where A appears on the left, so that its rewriting into $A \vee P$ was not necessary. □

Finally, let us remark that polarized LJ, polarized LB and polarized LBi are equivalent. Indeed, working in a polarized sequent calculus modulo $\mathcal{R}$ can be seen as working in the same sequent calculus without modulo but with explicit conversion rules:

$$\uparrow^* \vdash \frac{\Gamma, Q \vdash \Delta}{\Gamma, P \vdash \Delta}\, P \underset{\mathcal{R}\ -}{\overset{*}{\longrightarrow}} Q \qquad \text{and} \qquad \vdash \uparrow^* \frac{\Gamma \vdash Q, \Delta}{\Gamma \vdash P, \Delta}\, P \underset{\mathcal{R}\ +}{\overset{*}{\longrightarrow}} Q \quad .$$

As LJ, LB and LBi are equivalent, adding these conversion rules does not break this equivalence. (One has to be careful with LJ, because the right conversion rule is not exactly the same because the right hand side of the sequent contains at most one formula, but it works.)