Regaining Cut Admissibility in Deduction Modulo using Abstract Completion

Guillaume Burel, Claude Kirchner

Regaining Cut Admissibility in Deduction Modulo using Abstract Completion

Guillaume Burel[a,c,*], Claude Kirchner[b,c]

[a] *Nancy-Université, Université Henri Poincaré*
[b] *INRIA, Centre de Recherche INRIA Bordeaux - Sud-Ouest*
[c] *LORIA, Équipe Pareo, Bâtiment B, Campus Scientifique, 54506 Vandœuvre-lès-Nancy Cedex*

Abstract

Deduction modulo is a way to combine computation and deduction in proofs, by applying the inference rules of a deductive system (e.g. natural deduction or sequent calculus) modulo some congruence that we assume here to be presented by a set of rewrite rules. Using deduction modulo is equivalent to proving in a theory corresponding to the rewrite rules, and leads to proofs that are often shorter and more readable. However, cuts may be not admissible anymore.

We define a new system, the unfolding sequent calculus, and prove its equivalence with the sequent calculus modulo, especially w.r.t. cut-free proofs. It permits to show that it is even undecidable to know if cuts can be eliminated in the sequent calculus modulo a given rewrite system.

Then, to recover the cut admissibility, we propose a procedure to complete the rewrite system such that the sequent calculus modulo the resulting system admits cuts. This is done by generalizing the Knuth-Bendix completion in a non-trivial way, using the framework of *abstract canonical systems*.

These results enlighten the entanglement between computation and deduction, and the power of abstract completion procedures. They also provide an effective way to obtain systems admitting cuts, therefore extending the applicability of deduction modulo in automated theorem proving.

Keywords: Automated deduction, rewriting, Knuth-Bendix completion, critical proofs, cut admissibility, deduction modulo, proof ordering, abstract canonical system, computational proof

*Corresponding author. Current address : Max Planck Institut für Informatik, Campus E1 4, 66123 Saarbrücken, Germany. Phone number: +49 681 9325 220. Fax number: +49 681 9325 999.

Email addresses: guillaume.burel@ens-lyon.org (Guillaume Burel), claude.kirchner@inria.fr (Claude Kirchner)

URL: http://www.mpi-inf.mpg.de/~burel/ (Guillaume Burel), http://www.loria.fr/~ckirchne/ (Claude Kirchner)

[1] LORIA is the UMR 7503 shared by CNRS–INPL–INRIA–Nancy2–UHP.

1. Introduction

Proof assistants like Coq, PVS or Isabelle-HOL are now well mastered systems both from the conceptual and implementation points of view. They allow for the development of large and even very large proofs like the one of the four-color theorem [1]. They allow also for a broad use of these techniques, making computer-aided proof development an approach now in use at the industrial level, for instance for making the formal proof of security issues of java card [2, 3].

This important activity in the use of current proof assistants enlightens the crucial lack of computing power easily combinable with the deductive capabilities of such systems. If the complementarity and interaction between computation and deduction is identified since at least Henri Poincaré, its formalization as deduction modulo [4] is an appropriate way to present first-order logic as well as any logic in general.

Deduction modulo should therefore be at the heart of proof assistants and proof search methods, either implicitly or explicitly [see for instance 4, 5, 6, 7] and getting a deep understanding of its logical behavior is of prime interest either for theoretical or practical purposes.

In deduction modulo, computations are modeled by a congruence relation between terms *and* between propositions. The logical deductions are done modulo this congruence that is represented by a rewrite relation over first-order terms and propositions. This permits to construct proofs that are often more readable, because the really deductive steps appear clearly, and also shorter, as was shown by Burel [8]. A first interesting question is to know which theories can be represented by such a congruence. It turns out, as we show in this paper, that any finitely presented first-order theory can be transformed into such a rewrite relation, as far as one is only concerned with classical logic. Nevertheless, the additional expressiveness capabilities added by the congruence entails that the Hauptsatz, *i.e.* the fact that cuts are not needed to build proofs, is no longer true. This can be seen in particular from an example derived from Crabbé's proof of the non-normalization of Zermelo's theory [9] (see for instance [4] and Footnote 3 below). And indeed the gap is important as we are proving in this paper that the admissibility of the cut rule is undecidable when one works modulo.

But cut elimination is fundamental for several related reasons: first, it implies the consistency of the logic, and in the case of deduction modulo the consistency of the theory associated with the rewrite relation. Second, it entails the subformula property[2], so that the search space is, in a sense, limited. The tableau method is based on this fact, and for instance TaMed [7, 10], a tableau method based on deduction modulo, is shown to be complete only for cut-free systems. Third, it has been shown by Hermant [11] that the proof search method

[2]In the case of deduction modulo, the intuitive notion of subformula must take the considered rewrite relation into account.

for deduction modulo ENAR [4]—which generalizes resolution and narrowing—is equivalent to the cut-free fragment of deduction modulo, i.e. a sequent has a cut-free proof in deduction modulo if and only if ENAR can find a proof. ENAR is therefore complete if and only if the cut rule is admissible. This is also the case in the more recently introduced Polarized Resolution Modulo [12].

So on the one hand, we like to have a powerful congruence but this may be at the price of losing cut admissibility. How can we get both? It has been shown by Dowek [13] that cut admissibility is equivalent to the confluence of the rewrite system, provided only first-order *terms* are rewritten. In case the term rewrite system we are considering is not confluent, we can apply standard (a.k.a. Knuth-Bendix [14]) completion to get an equivalent term rewrite system which is confluent, and that way, we regain the cut admissibility. It is however no longer true when *propositions* are also rewritten, and the cut admissibility is in that case a stronger notion than confluence. Dowek wanted therefore to build a generalized completion procedure whose input is a rewrite system over first-order terms and atomic propositions and computing a rewrite system such that the associated sequent calculus modulo admits cut. He proposed such a completion procedure for the quantifier free case [15], based on the construction of a model for the theory associated with the rewrite system.

To solve this question, including *unlimited* use of quantifiers, we use here a quite different approach based on the notion of *abstract canonical system and inference* introduced by Dershowitz and Kirchner [16], Bonacina and Dershowitz [17]. This abstract framework is based on a proof ordering whose goal is to apprehend the notion of proof quality from which the notions of canonicity, completeness and redundancy follow up. It is shown to be well adapted to existing completion procedures such as ground completion [18] and standard (a.k.a. Knuth-Bendix [14]) completion [19].

To present the general idea of our approach, let us consider the simple example of Crabbé's axiom [9] $A \Leftrightarrow B \wedge \neg A$[3]. Can we find, for the sequent calculus modulo the associated rewrite system $A \to B \wedge \neg A$, a provable sequent without any cut-free proof? Indeed, let us try to build a minimal example. We will show in Proposition 39 that such a proof, in its simplest form, is necessarily of the shape:

$$\dfrac{\dfrac{\dfrac{\vdots}{A, B \wedge \neg A \vdash}}{A \vdash}\uparrow\text{-l} \quad \dfrac{\dfrac{\vdots}{\vdash B \wedge \neg A, A}}{\vdash A}\uparrow\text{-r}}{\vdash}\,\mathsf{Cut}(A)$$

where the rules labeled "↑-r" and "↑-l" allow to unfold the oriented axioms respectively on the right or on the left. In order to validate this proof pattern, we have to check if it is possible to close both sides of the proof tree, possibly adding informations in the initial sequent.

[3]In Crabbé's manuscript, A represents $r_s \in r_s$ and B $r_s \in s$ where r_s is $\{x \in s : x \notin x\}$. Then, there is a proof of $r_s \notin s$ in Zermelo's set theory that is not normalizing.

First, we can trivially close the left part as follows:

$$\dfrac{\dfrac{\dfrac{}{A, B \vdash A}\ \mathsf{Axiom}}{A, B, \neg A \vdash}\ \neg\text{-}\mathsf{l}}{A, B \wedge \neg A \vdash}\ \wedge\text{-}\mathsf{l} \quad .$$

Second, to close the right part, we must have a proof in the form:

$$\dfrac{\vdash B, A \qquad \dfrac{\dfrac{}{A \vdash A}\ \mathsf{Axiom}}{\vdash \neg A, A}\ \neg\text{-}\mathsf{r}}{\vdash B \wedge \neg A, A}\ \wedge\text{-}\mathsf{r} \quad .$$

To enforce the proof of $\vdash B, A$, we must add either A or B to the left of the sequent, and we only have to consider B, since we have cut around A. We obtain the critical proof:

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{}{A, B \vdash A}\ \mathsf{Axiom}}{A, B, \neg A \vdash}\ \neg\text{-}\mathsf{l}}{B, A, B \wedge \neg A \vdash}\ \wedge\text{-}\mathsf{l}}{B, A \vdash}\ \uparrow\text{-}\mathsf{l} \qquad \dfrac{\dfrac{\dfrac{}{B \vdash B, A}\ \mathsf{Axiom} \qquad \dfrac{\dfrac{}{B, A \vdash A}\ \mathsf{Axiom}}{B \vdash \neg A, A}\ \neg\text{-}\mathsf{r}}{B \vdash B \wedge \neg A, A}\ \wedge\text{-}\mathsf{r}}{B \vdash A}\ \uparrow\text{-}\mathsf{r}}{B \vdash}\ \mathsf{Cut}(A) \quad .$$

We can also easily show that there are no cut-free proof of $B \vdash$, simply because no inference rule is applicable to it except Cut. If we want to have a cut-free proof, we need to make B reducible by the congruence, hence the idea to complete the initial system with a new rule which is a logical consequence of the current system. In our case, we must therefore add the rule $B \to \bot$.

With this new rule, we will show that there are no more critical proofs and that therefore the sequent calculus modulo the proposition rewrite system

$$\begin{cases} A \to B \wedge \neg A \\ B \to \bot \end{cases}$$

admits the cut rule and has the same expressive power as the initial one.

The study of this question indeed reveals general properties of the sequent calculus modulo and our contributions are the following:

- We define several variants of the sequent calculus modulo more adapted to prove the results of the paper (Section 2.2): the unfolding sequent calculus allows only atomic propositions to be rewritten, step by step; in addition, the polarized unfolding sequent calculus separates which rules can be applied to a proposition on the left and on the right of a sequent; both variants behave the same way, especially w.r.t. cut-free proofs, as the asymmetric sequent calculus modulo of Dowek [13], which in turn is equivalent to the original version of the sequent calculus modulo by Dowek et al. [4] when the rewrite system is confluent;

- We prove, using a semantical argument, that it is undecidable to know if the unfolding sequent calculus associated with a given proposition rewrite system admits cuts (Theorem 15);
- We show how to transform a finite set of axioms into a finite rewrite system, such that the theory induced by the set of axioms is the same as the one proved by the classical sequent calculus modulo the rewrite system (Section 4);
- We provide an appropriate Noetherian ordering on the proofs of the unfolding sequent calculus; This ordering allows us to set on the proof space of unfolding sequent calculus a structure of abstract canonical system (Theorem 37); We characterize the critical proofs in deduction modulo as simple cuts (Proposition 39); We establish a precise correspondence between the limit of a completion process and a cut-free sequent calculus (Theorem 41), therefore bypassing the undecidability of the cut admissibility in the same way as standard completion circumvents the undecidability of the confluence of a rewrite system;
- We show the applicability of the general results, in particular on sequent calculus modulo rewrite systems involving quantifiers, therefore generalizing all previously known results such as the ones of Dowek [15];

As an important by-product of these results, we demonstrate the expressive power of abstract canonical systems (ACS for short).

The next section presents basic notions on rewriting and introduces the variants of sequent calculi modulo that are used in the paper, proving their equivalence, in particular concerning cut admissibility. In Section 3, we show the undecidability of the cut admissibility in deduction modulo. The rest of the paper is therefore dedicated to ways to circumvent this. Section 4 describes an algorithm which transforms finitely presented first-order theories into rewrite systems such that the sequent calculus modulo proves the theory. It exhibits three important properties of the algorithm (Properties 16, 17 and 19) that are enough to define the completion procedure detailed in Section 5. This procedure is based on the framework of the ACS, which is recalled in Section 5.1. The unfolding sequent calculus is shown to be an instance of this framework (Section 5.2). This allows us in Section 5.3 to characterize the critical proofs of deduction modulo and to set-up the completion process as the appropriate (and indeed non-trivial) instance of the abstract completion process. We conclude after presenting in more details Crabbé's example as well as several examples involving quantifiers.

This paper is a profoundly revised and extended version of the paper presented at LFCS'07 [20] and it includes detailed proofs, examples and motivations.

2. Deduction modulo

2.1. Rewritings

We define here how propositions are rewritten in deduction modulo.

Bases on rewriting can be found in [21]. We present here briefly what we need for this paper to be self-contained, mainly by introducing notations. We denote by $\mathcal{T}(\Sigma, V)$ the set of first-order *terms* built from a signature Σ and a set of variables V. An *atomic proposition* is given by a predicate symbol A of arity n and by n terms $t_1, \ldots, t_n \in \mathcal{T}(\Sigma, V)$. It is denoted $A(t_1, \ldots, t_n)$. *Propositions* can be built using the following grammar[4]:

$$\mathcal{P} \quad \stackrel{!}{=} \quad A \mid \neg\mathcal{P} \mid \mathcal{P} \wedge \mathcal{P} \mid \mathcal{P} \vee \mathcal{P} \mid \mathcal{P} \Rightarrow \mathcal{P} \mid \forall x.\ \mathcal{P} \mid \exists x.\ \mathcal{P}$$

where A ranges over atomic propositions and x over variables. $P \Leftrightarrow Q$ will be used as a syntactic sugar for $(P \Rightarrow Q) \wedge (Q \Rightarrow P)$, as well as $\bigwedge \Gamma$ for $P_1 \wedge \ldots \wedge P_n$; $\bigvee \Gamma$ for $P_1 \vee \ldots \vee P_n$ and $\neg\Gamma$ for $\neg P_1, \ldots, \neg P_n$ when $\Gamma = P_1, \ldots, P_n$. Free variables of a proposition and substitutions are defined as usual. The replacement of a variable x by a term t in a proposition P is denoted by $\{t/x\}P$. A *position* in a term or a proposition t is a path in the tree representing t. The subterm or subproposition $t_{|\mathfrak{p}}$ of t at position $\mathfrak{p}$ is the term or proposition represented by the subtree of t whose root is the last node of $\mathfrak{p}$. The replacement in t of the subterm $t_{|\mathfrak{p}}$ by s is denoted by $t[s]_{\mathfrak{p}}$.

A *term rewrite rule* is the pair of terms l, r such that all free variables of r appear in l. It is denoted $l \to r$. A *term rewrite system* is a set of term rewrite rules.

A term s can be rewritten to a term t by a term rewrite rule $l \to r$ if there exists some substitution σ such that $\sigma l = s$ and $\sigma r = t$. This is extended to all terms, and then to all propositions 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.

An atomic proposition A can be rewritten to a proposition P by a proposition rewrite rule $B \to Q$ if there exists some substitution σ such that $\sigma B = A$ and $\sigma Q = P$. This is extended to all propositions by congruence. It should be noted that the proposition rewrite relation should be seen, at least at first approximation, as an equivalence between propositions, and not as an implication: We will see that proving using $A \to P$ is the same as proving with the extra assumption $A \Leftrightarrow P$.

A *rewrite system* will be the combination of a term rewrite system and a proposition rewrite system. In the following, the term rewrite system used in addition to all the proposition rewrite systems we will consider is fixed. It is supposed to be *terminating and confluent* and is denoted $R_{\mathcal{T}(\Sigma,V)}$.

[4] $\stackrel{!}{=}$ is used for definitions.

We denote by $P \underset{R}{\longrightarrow} Q$ the fact that P can be rewritten to Q in the rewrite system R in one step. R may be omitted if it is clear from the context. $\underset{R}{\xrightarrow{+}}$ (resp. $\underset{R}{\xrightarrow{*}}$) is the transitive (resp. reflexive transitive) closure of this rewrite relation.

The *subformula relation* $\succ$ is the least transitive relation such that:

- $P \succ P_i$ $(i = 1, 2)$ if $P = P_1 \wedge P_2$, $P = P_1 \vee P_2$ or $P = \neg P_1$;
- $P \succ \{t/x\}Q$ if $P = \forall x.\ Q$ or $P = \exists x.\ Q$;
- $P \succ Q$ if $P \underset{R_{\mathcal{T}(\Sigma,V)}}{\longrightarrow} Q$

for all terms t, variables x and propositions P, Q, P_1, P_2. It is well-founded: the lexicographic combination of the comparison of the number of connectors and quantifiers in the propositions and the relation $\underset{R_{\mathcal{T}(\Sigma,V)}}{\longrightarrow}$ contains $\succ$: if $P \succ Q$, then either P contains more connectors and quantifier than Q ($R_{\mathcal{T}(\Sigma,V)}$ rewrites only terms, so it cannot add connectors or quantifiers), or as much and in that case $P \underset{R_{\mathcal{T}(\Sigma,V)}}{\xrightarrow{+}} Q$. As we know that $R_{\mathcal{T}(\Sigma,V)}$ terminates, the lexicographic combination is well founded. Note that this is not the subformula relation that we are talking about in Footnote 2: for the subformula property to hold we need to also include proposition rewriting, in which case the wellfoundedness may be lost even for terminating rewrite systems (for instance for $A(c) \to \exists x.\ A(x)$).

2.2. Sequent Calculi Modulo

Sequent calculi modulo can be seen as extensions of the sequent calculus of Gentzen [22]. We will use the denominations of Gallier [23]. There exist several variations of sequent calculi modulo, depending on whether rewrite steps are explicit or not, or whether they are applied to atomic propositions only or not. We propose here two variants, the unfolding sequent calculus and the polarized unfolding sequent calculus. We link them with other variants defined by Dowek [13, 15].

A *sequent* is a pair of multisets of propositions Γ, Δ. It is denoted by $\Gamma \vdash \Delta$. The sets of all sequents is denoted $\mathcal{S}$. For a sequent $\Gamma \vdash \Delta$, if $x_1, \ldots, x_n$ are the free variables of Γ, Δ, we denote $\mathcal{P}(\Gamma \vdash \Delta)$ the proposition $\forall x_1, \ldots, x_n.\ (\bigwedge \Gamma \Rightarrow \bigvee \Delta)$.

In Fig. 1 we present the inference rules of the *unfolding sequent calculus*, which is an extension of the system G4 of Kleene [24] with unfolding rules that apply a rewrite rule to an atomic proposition. *Proofs* are trees labeled by sequents built using these rules, and where all leaves are Axioms. The root sequent is called the *conclusion*. In the following, a double horizontal bar will mean several applications of an inference rule. A proof is said to be *built in the proposition rewrite system* R if all $\uparrow$-l and $\uparrow$-r steps use only rules that appear in $R \cup R_{\mathcal{T}(\Sigma,V)}$.

Identity Group:

$$\frac{}{\Gamma, P \vdash P, \Delta}\ \mathsf{Axiom}(P) \qquad \frac{\Gamma, P \vdash \Delta \quad \Gamma \vdash P, \Delta}{\Gamma \vdash \Delta}\ \mathsf{Cut}(P)$$

Logical Rules:

$$\frac{\Gamma \vdash P, \Delta}{\Gamma, \neg P \vdash \Delta}\ \neg\text{-l} \qquad \frac{\Gamma, P \vdash \Delta}{\Gamma \vdash \neg P, \Delta}\ \neg\text{-r}$$

$$\frac{\Gamma, P, Q \vdash \Delta}{\Gamma, P \wedge Q \vdash \Delta}\ \wedge\text{-l} \qquad \frac{\Gamma \vdash P, \Delta \quad \Gamma \vdash Q, \Delta}{\Gamma \vdash P \wedge Q, \Delta}\ \wedge\text{-r}$$

$$\frac{\Gamma, P \vdash \Delta \quad \Gamma, Q \vdash \Delta}{\Gamma, P \vee Q \vdash \Delta}\ \vee\text{-l} \qquad \frac{\Gamma \vdash P, Q, \Delta}{\Gamma \vdash P \vee Q, \Delta}\ \vee\text{-r}$$

$$\frac{\Gamma, Q \vdash \Delta \quad \Gamma, \vdash P, \Delta}{\Gamma, P \Rightarrow Q \vdash \Delta}\ \Rightarrow\text{-l} \qquad \frac{\Gamma, P \vdash Q, \Delta}{\Gamma \vdash P \Rightarrow Q, \Delta}\ \Rightarrow\text{-r}$$

$$\frac{\Gamma, \forall x.\ P, \{t/x\}P \vdash \Delta}{\Gamma, \forall x.\ P \vdash \Delta}\ \forall\text{-l} \qquad \frac{\Gamma \vdash \{y/x\}P, \Delta}{\Gamma \vdash \forall x.\ P, \Delta}\ \forall\text{-r}$$

$$\frac{\Gamma, \{y/x\}P \vdash \Delta}{\Gamma, \exists x.\ P \vdash \Delta}\ \exists\text{-l} \qquad \frac{\Gamma \vdash \exists x.\ P, \{t/x\}P, \Delta}{\Gamma \vdash \exists x.\ P, \Delta}\ \exists\text{-r}$$

In $\forall$-l and $\exists$-r, $t \in \mathcal{T}(\Sigma, V)$; in $\exists$-l and $\forall$-r, y is not free in Γ, Δ.

Unfolding Rules:
$A \underset{\{r\}}{\longrightarrow} P$, A atomic:

$$\frac{\Gamma, A, P \vdash \Delta}{\Gamma, A \vdash \Delta}\ \uparrow\text{-l}(r) \qquad \frac{\Gamma \vdash A, P, \Delta}{\Gamma \vdash A, \Delta}\ \uparrow\text{-r}(r)$$

Figure 1: Unfolding Sequent Calculus

$\mathsf{Cut}(P)$ permits essentially to extend the proof search space with the proposition P. Logical Rules decompose some proposition which is called *principal*. Unfolding Rules, that do not appear in Gentzen's sequent calculus, introduce proposition rewriting into the proof system. They are parametrized by a rewrite rule. Note that only atomic propositions are rewritten, in one step. It can also be remarked that the Unfolding Rules contain an implicit contraction. This is needed to prove that contractions are admissible in the Cut-free Unfolding Sequent Calculus (see Lemma 5 below), even when the rewrite system is confluent, as shown by proving A modulo the rule $A \to A \Rightarrow B$.

Definition 1 (Cut admissibility). A proposition rewrite system R is said to *admit* Cut if for all sequents $s \in \mathcal{S}$, s has a proof in R if and only if s has a proof in R without using Cut.

It is well-known (Gentzen's Hauptsatz [22], or more accurately [13, Proposition 8] because of $R_{\mathcal{T}(\Sigma,V)}$) that $\emptyset$ admits Cut.

The unfolding sequent calculus is slightly different from the asymmetric sequent calculus modulo of Dowek [13], which consists in applying identity and logical rules modulo the rewrite system. For instance, it contains the following inference rules

$$\frac{}{\Gamma, P \vdash Q, \Delta}\ \mathsf{Axiom}\ {}_{P \xrightarrow{*} R \xleftarrow{*} Q} \qquad \frac{\Gamma, Q \vdash \Delta \quad \Gamma \vdash P, \Delta}{\Gamma, R \vdash \Delta}\ \Rightarrow\text{-}\mathsf{l}\ {}_{R \xrightarrow{*} P \Rightarrow Q}\ .$$

The asymmetric sequent calculus modulo also contains explicit contraction and weakening inference rules. Unfolding sequent calculus is to the asymmetric sequent calculus modulo what natural deduction with folding/unfolding rules is to natural deduction modulo (see [25]). We will show that they are equivalent, in particular w.r.t. Cut.

From a logical point of view, deduction modulo is not problematic, because proving in a rewrite system R is the same as proving using some set of first-order axioms, which is then called compatible [see 4, Proposition 1.8]. In particular, a compatible axiom for the rewrite rule $A \to P$ is the proposition $\forall x_1, \ldots, x_n.\ A \Leftrightarrow P$ where $x_1, \ldots, x_n$ are the free variables of A. To be able to do the same with implications instead of equivalences, Dowek [12, 15] introduced the polarized sequent calculus modulo. In this, rewrite rules are distinguished by a (positive or negative) polarity written on the arrow of the rule. A polarity is also defined for the positions of propositions: the root is positive, and we switch polarity under $\neg$ and at the left of $\Rightarrow$. A proposition is *positively rewritten* if it is rewritten by a positive rule at a positive position, or by a negative rule at a negative position. A proposition is *negatively rewritten* if it is rewritten by a negative rule at a positive position, or by a positive rule at a negative position. The polarized sequent calculus is similar to the asymmetric calculus modulo, but propositions on the right of a sequent can only be positively rewritten, and propositions on the left only negatively. Term rewrite rules can be indifferently applied to the left or the right. We will denote by $\mathcal{PRR}$ the set of all polarized rewrite rules.

If we try to do the same with the unfolding sequent calculus, we simply have to restrain $\uparrow$-l to negative rules, and $\uparrow$-r to positive rules. We obtain that way what we call the *polarized unfolding sequent calculus*. The set of proof of the polarized unfolding sequent calculus is denoted by $\mathcal{PUSC}$. We show now that it is equivalent to the polarized sequent calculus modulo.

First, we show that weakening and contraction are admissible in the polarized unfolding sequent calculus.

Lemma 2 (Weakening Lemma). *For all proposition rewrite system R, if there exist a proof of $\Gamma \vdash \Delta$ in R, then for all propositions P there exists proofs of $\Gamma, P \vdash \Delta$ and $\Gamma \vdash P, \Delta$ in R of the same size.*

Proof. By induction on the proof, P can be propagated in the first proof until Axioms, which accept side propositions. □

Lemma 3 (Kleene Lemma [11, Lemme 3.3]). *If a sequent, containing the non-atomic proposition P, has a proof (resp.* Cut*-free proof) in R, then it has a proof (resp.* Cut*-free proof) in R whose first rule is a logical rule with principal proposition P.*

Proof. This is slightly more general than Hermant [11, Lemme 3.3], because we also consider $\forall$-l and $\exists$-r. But, for instance, if there is a proof $\Gamma, \forall x.\ P \vdash \Delta$, by weakening there is a proof of the same size of $\Gamma, \forall x.\ P, \{t/x\}P \vdash \Delta$. The lemma can be proved by simple induction on the size of the proof. □

Corollary 4. *For all sequents $\Gamma \vdash \Delta$, the sequent $\vdash \mathcal{P}(\Gamma \vdash \Delta)$ has a* Cut*-free proof in R iff the sequent $\Gamma \vdash \Delta$ has one.*

Note. It should be remarked that all inference rules r but $\forall$-l and $\exists$-r (even $\uparrow$-l and $\uparrow$-r) can be permuted from above, in the sense that if there is an application of r above some other inference rule r' that do not decompose a principal proposition into the principal proposition of r, then we can build a valid proof by permuting the inference rules, applying therefore r' above r. This can also be proved by induction on the proof.

Lemma 5 (Contraction Lemma). *For all proposition rewrite system R, the two following statements hold:*

- *There exist a proof of $\Gamma, P \vdash \Delta$ in R if and only if there exists a proof of $\Gamma, P, P \vdash \Delta$ in R.*
- *There exist a proof of $\Gamma \vdash P, \Delta$ in R if and only if there exists a proof of $\Gamma \vdash P, P, \Delta$ in R.*

Proof. One direction is a direct corollary of the Weakening Lemma.

The other one is a consequence of Kleene's Lemma, and can be proved by lexicographic induction on the structure of the proposition P and the size of the proof of $\Gamma, P, P \vdash \Delta$.

In the case of an atomic proposition A: suppose there exists a proof of $\Gamma, A, A \vdash \Delta$. If the principal proposition of the last inference rule is not one of the A, then by we can just apply the induction hypothesis to the subproof. If the last inference rule is Axiom, we can prune one of the A in it. The resulting proof has the same size. If the last inference rule is $\uparrow$-l for some rewrite rule $A \rightarrow^{-} P$, then we have a strictly smaller proof of $\Gamma, A, A, P \vdash \Delta$ to which we can apply the induction hypothesis to get a proof of $\Gamma, A, P \vdash \Delta$. Apply $\uparrow$-l to this proof gives a proof of $\Gamma, A \vdash \Delta$.

In the case of $\vee$: suppose there exists a proof of $\Gamma, P \vee Q, P \vee Q \vdash \Delta$. By Kleene's Lemma there exist proofs of $\Gamma, P, P \vee Q \vdash \Delta$ and $\Gamma, Q, P \vee Q \vdash \Delta$. We can apply Kleene Lemma twice again to get proofs of $\Gamma, P, P \vdash \Delta$; $\Gamma, Q, P \vdash \Delta$; $\Gamma, P, Q \vdash \Delta$ and $\Gamma, Q, Q \vdash \Delta$. By induction hypothesis, we have proofs of $\Gamma, P \vdash \Delta$ and $\Gamma, Q \vdash \Delta$, and therefore a proof of $\Gamma, P \vee Q \vdash \Delta$.

In the case of $\exists$: suppose there exists a proof of $\Gamma, \exists x.\ Q, \exists x.\ Q \vdash \Delta$. By applying Kleene's Lemma twice there exists a proof of $\Gamma, \{y/x\}Q, \{y'/x\}Q \vdash \Delta$

where y and y' are not free in Γ, Δ. Then, we can replace y' by y in this proof to get a valid proof of $\Gamma, \{y/x\}Q, \{y/x\}Q \vdash \Delta$. By induction hypothesis, there exists a proof of $\Gamma, \{y/x\}Q \vdash \Delta$ where y is not free in Γ and Δ. Therefore we have a proof of $\Gamma, \exists x.\ Q \vdash \Delta$.

In the case of $\forall$: we proceed by induction on the proof of $\Gamma, \forall x.\ Q, \forall x.\ Q \vdash \Delta$. If no $\forall x.\ Q$ is the principal proposition of the last rule, this is a simple induction. If it is principal, the direct subproof proves $\Gamma, \{t/x\}Q, \forall x.\ Q, \forall x.\ Q \vdash \Delta$ for some $t \in \mathcal{T}(\Sigma, V)$. By induction hypothesis, we have a proof of $\Gamma, \{t/x\}Q, \forall x.\ Q \vdash \Delta$, and therefore a proof of $\Gamma, \forall x.\ Q \vdash \Delta$. □

NOTE. The premises Γ and conclusions Δ of sequent $\Gamma \vdash \Delta$ can therefore be considered as sets.

Lemma 6 (Rewrite Lemma). *For all proposition rewrite systems R_1 and R_2, the two following statements hold:*

- *If $P \xrightarrow[R_1 \cup R_{\mathcal{T}(\Sigma,V)}]{*} Q$ negatively and there exists a proof of $\Gamma, Q \vdash \Delta$ in R_2, then there exists a proof of $\Gamma, P \vdash \Delta$ in $R_1 \cup R_2$.*
- *If $P \xrightarrow[R_1 \cup R_{\mathcal{T}(\Sigma,V)}]{*} Q$ positively and there exists a proof of $\Gamma \vdash Q, \Delta$ in R_2, then there exists a proof of $\Gamma \vdash P, \Delta$ in $R_1 \cup R_2$.*

PROOF. We proceed by induction on the length of the rewrite derivation $P \xrightarrow[R_1 \cup R_{\mathcal{T}(\Sigma,V)}]{*} Q$. We therefore only have to show it for a single step of rewriting.

If $P \xrightarrow[R_1 \cup R_{\mathcal{T}(\Sigma,V)}]{} Q$ negatively, then there exists some context $C[]$, an atomic proposition A and a proposition Q' such that $P = C[A]$ and $Q = C[Q']$ and $A \xrightarrow[R_1 \cup R_{\mathcal{T}(\Sigma,V)}]{} Q'$ negatively if the position of the hole in the context is positive or positively in the other case. We proceed by induction on the context. Suppose there exists a proof of $\Gamma, C[Q'] \vdash \Delta$. We can transform it into a proof of $\Gamma, C[A] \vdash \Delta$ by applying the same inference rules, except when these rules are directly applied to Q', because it is replaced by A. In this case, if the hole in $C[]$ is at a positive position, then A is on the left of the sequent, and we can apply $\uparrow$-l (the rewrite rule that rewrites A into Q' is indeed negative in that case). In the other case, it is on the right and we can apply $\uparrow$-r (the rewrite rule is indeed positive). We can then carry on the proof. The resulting proof uses then rewrite rules in $R_1 \cup R_2 \cup R_{\mathcal{T}(\Sigma,V)}$, and is thus in $R_1 \cup R_2$.

The second sentence is dual. □

Note that in all the previous lemmata, we do not introduce extra Cuts in the resulting proofs. This allows to prove the equivalence with the polarized sequent calculus modulo, also w.r.t. Cut-free proofs.

Proposition 7 (Equivalence). *The polarized unfolding sequent calculus is equivalent to the polarized sequent calculus modulo of Dowek [15], that is, a sequent is provable (resp. provable without* Cut*) in the polarized unfolding sequent calculus in a proposition rewrite system R iff it is provable (resp. provable without* Cut*) in the polarized sequent calculus modulo the rewrite system $R \cup R_{\mathcal{T}(\Sigma,V)}$.*

Proof. It is quite clear that the inference rules of the polarized unfolding sequent calculus can be derived in Dowek's one, by integrating each unfolding step into the inference rules above through the modulo.

Conversely, using Lemma 6, we can extract the rewriting from the logical rules. For instance, if we have a proof whose root is

$$\frac{\Gamma, Q \vdash \Delta \quad \Gamma \vdash P, \Delta}{\Gamma, O \vdash \Delta} \Rightarrow\text{-l}\ O \xrightarrow{*} P \Rightarrow Q \text{ negatively},$$

we use the premises to get a proof $\Gamma, P \Rightarrow Q \vdash \Delta$ without implicit rewriting, and we use Lemma 6 to get the proof of $\Gamma, O \vdash \Delta$.

Then, Lemmata 2 and 5 proves that weakening and contraction are admissible.

Of course, as we have seen, both system are also equivalent regarding Cut-free proofs, since we did not need to add any Cut in the proofs of the previous lemmata. □

Corollary 8. *The unfolding sequent calculus is equivalent (in the same sense) to the asymmetric sequent calculus modulo.*

Proof. A non-polarized rewrite system R can easily be seen as a polarized rewrite system $R^{\pm}$ with for each rule $A \to P$ in R a positive rule $A \to^{+} P$ and a negative rule $A \to^{-} P$. The unfolding sequent calculus for R (resp. the asymmetric sequent calculus modulo for R) is then the polarized unfolding sequent calculus for $R^{\pm}$ (resp. the polarized sequent calculus modulo for $R^{\pm}$).

This translation also permits to know that every lemma above holds also for the unfolding sequent calculus. □

Given a polarized rewrite system R, we can transform it into a non-polarized rewrite system $R^{\mp}$:

- a positive rule $A \to^{+} P$ is translated into $A \to A \vee P$;
- a negative rule $A \to^{-} P$ is translated into $A \to A \wedge P$.

The polarized unfolding sequent calculus for R is then equivalent to the unfolding sequent calculus for $R^{\mp}$:

Proposition 9. *A sequent is provable (resp. provable without* Cut*) in the polarized unfolding sequent calculus in a polarized proposition rewrite system R iff it is provable (resp. provable without* Cut*) in the unfolding sequent calculus in the rewrite system $R^{\mp}$.*

Proof. By induction on the structure of the proofs. Only the cases with unfolding rules are interesting.

If we have a proof ending with

$$\frac{\Gamma, \sigma A, \sigma P \vdash \Delta}{\Gamma, \sigma A \vdash \Delta} \uparrow\text{-l}(A \to^{-} P)$$

then by induction hypothesis we have a proof of $\Gamma, \sigma A, \sigma P \vdash \Delta$ in the unfolding sequent calculus. Using Lemma 2, and applying $\wedge$-l we obtain a proof of $\Gamma, \sigma A, \sigma A \wedge \sigma P \vdash \Delta$. We therefore can build the derivation

$$\dfrac{\dfrac{\Gamma, \sigma A, \sigma A, \sigma P \vdash \Delta}{\Gamma, \sigma A, \sigma(A \wedge P) \vdash \Delta}\ \wedge\text{-l}}{\Gamma, \sigma A \vdash \Delta}\ \uparrow\text{-l}(A \to A \wedge P)$$

in the unfolding sequent calculus. This is dual for the polarized $\uparrow$-r.

Conversely, there are two cases: either the rewrite rule is applied on the side corresponding to the polarity of the polarized rule that produced it, or on the other side. In the first case, suppose for instance that we have the proof

$$\dfrac{\begin{array}{c}\pi\\ \vdots\\ \Gamma \vdash \sigma(A \vee P), \sigma A, \Delta\end{array}}{\Gamma \vdash \sigma A, \Delta}\ \uparrow\text{-r}(A \to A \vee P)\ .$$

By induction hypothesis on π we have a proof of $\Gamma \vdash \sigma(A \vee P), \sigma A, \Delta$ in the polarized unfolding sequent calculus. By Lemmata 3 and 5, we have a proof of $\Gamma \vdash \sigma P, \sigma A, \Delta$. Because $\sigma A \underset{A \to^+ P}{\longrightarrow} \sigma P$ positively, we can apply $\uparrow$-r to get a proof of $\Gamma \vdash \sigma A, \Delta$. In the second case, suppose for instance that we have the proof

$$\dfrac{\begin{array}{c}\pi\\ \vdots\\ \Gamma, \sigma A, \sigma(A \vee P) \vdash \Delta\end{array}}{\Gamma, \sigma A \vdash \Delta}\ \uparrow\text{-l}(A \to A \vee P)\ .$$

By induction hypothesis on π we have a proof of $\Gamma, \sigma A, \sigma(A \vee P) \vdash \Delta$ in the polarized unfolding sequent calculus. By Lemmata 3 and 5, we have a proof of $\Gamma, \sigma A \vdash \Delta$. □

Corollary 10. *The polarized sequent calculus modulo and the asymmetric sequent calculus modulo are equivalent.*

This somehow answers a question of Dowek [15, end of Section 4] who asked which polarized rewrite system can be represented as a non-polarized rewrite system. We can also prove the equivalence for intuitionistic logic, with the same translation. To be able to do this, one needs a multi-conclusion sequent calculus for intuitionistic logic, see [26] (the translation is in the appendix of the full version of that paper, available at `http://hal.inria.fr/inria-00395934`). However, the non-polarized system is not necessarily confluent, and therefore, we may not have the equivalence with the original sequent calculus modulo of Dowek et al. [4], at least concerning Cut admissibility. Nevertheless, this should not be a problem. Indeed, the proving procedures based on deduction modulo, TaMed and ENAR, are actually complete for the cut-free part of the *asymmetric* sequent calculus modulo, regardless of the confluence of the rewrite system.

3. Undecidability of the cut admissibility

We present here some properties of the unfolding sequent calculus, which are slight generalizations of Hermant [11, 27]. In particular, we introduce the notion of semantically sound rewrite systems, which implies Cut admissibility, and we prove that the Cut admissibility is not decidable.

We need the following definitions, whose motivations can be found in Hermant [27]:

Definition 11 (Properties of a theory). Given a rewrite system R, a theory Γ:

- is *complete* iff for all propositions P, either $\Gamma, P \vdash$ or $\Gamma \vdash P$ has a Cut-free proof in R;
- is *consistent* iff there is no Cut-free proof of $\Gamma \vdash$ in R;
- *admits Henkin witnesses* iff for all propositions Q with one free variable x, there is a constant c of the language such that
  - if $\Gamma, \exists x.\ Q \vdash$ has no Cut-free proof in R, then $\{c/x\}Q$ is in Γ;
  - if $\Gamma \vdash \forall x.\ Q$ has no Cut-free proof in R, then $\neg\{c/x\}Q$ is in Γ.

Models in deduction modulo are standard first-order models, except that they are compatible with the rewrite system:

Definition 12 (Model for a rewrite system). A Boolean model $\mathcal{M}$ is a *model for the rewrite system* R if for all rewrite rules $A \to P$ in R, A and P are interpreted the same way in $\mathcal{M}$.

We introduce the new notion of semantically sound rewrite system:

Definition 13 (Semantical soundness). A rewrite system R is said *semantically sound* if every complete, consistent theory Γ which admits Henkin witnesses has a model $\mathcal{M}$ for R.

Proposition 14 (Semantical soundness implies Cut admissibility). *If R is semantically sound, then R admits* Cut.

Proof. As proved by Hermant [27, Lemma 3], if $\Gamma \vdash \Delta$ has a proof in R, then any model $\mathcal{M}$ for R interprets $\mathcal{P}(\Gamma \vdash \Delta)$ as true.

It remains to be proved that if any model $\mathcal{M}$ for R interprets $\mathcal{P}(\Gamma \vdash \Delta)$ as true then $\Gamma \vdash \Delta$ has a Cut-*free* proof in R.

If $\neg\mathcal{P}(\Gamma \vdash \Delta)$ is consistent, then using Hermant [27, Section 6.1], we can complete it into a consistent, complete theory Θ which admits Henkin witnesses. By hypothesis (semantical soundness), Θ has a model $\mathcal{M}$ for R. Furthermore, by construction of Θ this model is also a model for $\neg\mathcal{P}(\Gamma \vdash \Delta)$. Consequently, this model for R does not interpret $\mathcal{P}(\Gamma \vdash \Delta)$ as true, which contradicts our hypothesis.

Hence $\neg\mathcal{P}(\Gamma \vdash \Delta)$ is not consistent, by definition there is a Cut-free proof of $\neg\mathcal{P}(\Gamma \vdash \Delta) \vdash$ in R, and using Lemma 3 there is a Cut-free proof of $\Gamma \vdash \Delta$. □

This proposition permits to prove the main theorem of this first section:

Theorem 15 (Undecidability of the Cut Admissibility). *The problem*

> *Input: A propositional rewrite system R*
> *Decide if R admits* Cut.

is undecidable.

Proof. We reduce to the validity problem in first-order logic (given a proposition, decide whether it is valid in all first-order models). We recall the reader that this problem is undecidable in the empty theory when the language contains at least a binary predicate.

Let P be a first-order proposition.

Let A be a nullary predicate not appearing in P. Consider the propositional rewrite system

$$R = \{\, A \to A \Rightarrow P \,\} \ .$$

It is always possible to build a proof of $\vdash P$ in R:

$$\dfrac{\dfrac{\dfrac{\dfrac{}{A, P \vdash P}\ \textsf{Axiom} \quad \dfrac{}{A \vdash A, P}\ \textsf{Axiom}}{A, A \Rightarrow P \vdash P}\ \Rightarrow\textsf{-l}}{A \vdash P}\ \uparrow\textsf{-l} \qquad \dfrac{\dfrac{\dfrac{}{A \vdash P, A, P}\ \textsf{Axiom}}{\vdash A \Rightarrow P, A, P}\ \Rightarrow\textsf{-r}}{\vdash A, P}\ \uparrow\textsf{-r}}{\vdash P}\ \textsf{Cut}(A)$$

Then we show that P is valid if and only if R admits Cut:

If P is valid, then R is semantically sound: given a complete, consistent theory Γ which admits Henkin witnesses, let $\mathcal{M}$ be the model defined as follows: Its domain is the set of closed terms. An atomic predicate B is interpreted as true by $\mathcal{M}$ iff $\Gamma \vdash B$ has a Cut-free proof in R. Because the theory is complete and because it admits Henkin witnesses, this permits to define the model for all propositions [see 27, Lemma 8]. This process is well-defined by consistency. Then $\vdash A$ has a Cut-free proof (the right part of the proof above where P is pruned). By weakening $\Gamma \vdash A$ has a Cut-free proof in R, and A is therefore interpreted as true by $\mathcal{M}$. As P is valid, it is interpreted as true in particular in $\mathcal{M}$. Consequently, the interpretation of $A \Rightarrow P$ is also true. Thus, the left-hand side and the right-hand side of the rules in R have the same interpretation in $\mathcal{M}$, which is therefore a model for R. Consequently, R is semantically sound and by Proposition 14 it admits Cut.

Conversely, if R admits Cut, because of the existence of the proof above, there exists a Cut-free proof of $\vdash P$ in R. Because P does not contain A, no unfolding rules can be applied in this proof (simple proof by induction). Therefore, there exists a proof of $\vdash P$ in Gentzen's sequent calculus, and as it is complete for first-order logic, P is valid. □

Note. This proof is deeply inspired by the proof of Hermant [11, Chapter 8] that there exists terminating and confluent rewrite systems that admits Cut, but in which some proof is not normalizing. Cut admissibility remains undecidable

even when considering only terminating and confluent rewrite system, by using the system $r \in r \to \forall y.\ (\forall x.\ y \in x \Rightarrow r \in x) \Rightarrow y \in r \Rightarrow P$ in the proof above.

NOTE. In fact, this problem seems to be Π^0_2-complete in the arithmetical hierarchy (see [28, Chapter C.1] for an introduction on the arithmetical hierarchy), i.e. it is not even semi-decidable. This could be proved by merging the proof above with techniques used in [29] to prove in particular that the confluence of a rewrite system is Π^0_2-complete.

4. Construction of a rewrite system compatible with a theory

We now present an algorithm transforming a finitely presented first-order theory into a polarized rewrite system such that, proving in the theory is equivalent to proving modulo the rewrite system. We first define the good properties that such an algorithm should have, and then provide an example of such an algorithm.

4.1. Desired properties

We want to build an algorithm that translates a finite presentation of a first-order theory into a rewrite system. This algorithm may be seen as a function from sequents to polarized rewrite systems: $\mathit{Rew} :\ \mathcal{S}\ \to \mathcal{PRR}$.

First, we require that each polarized rewrite rule can be produced by the algorithm. This is not really useful here, but we need this for the completion procedure in the next section.

Property 16. For all polarized rewrite rule r there exists a sequent s such that $\mathit{Rew}(s) = \{r\}$.

Then we want that the theory is compatible with the rewrite system produced from it. Moreover, we would like that at least the axioms in the presentation of the theory are provable without Cut in the produced rewrite system.

Property 17 (Strong Compatibility). For all sequents $\Gamma \vdash \Delta$, $\mathit{Rew}(\Gamma \vdash \Delta)$ and $\mathcal{P}(\Gamma \vdash \Delta)$ are strongly compatible:

(a) for all positive rewrite rule $A \to^+ P$ in $\mathit{Rew}(\Gamma \vdash \Delta)$, there exists a proof of $\mathcal{P}(\Gamma \vdash \Delta) \vdash P \Rightarrow A$ in $\emptyset$ (i.e. using only term rewrite rules of $R_{\mathcal{T}(\Sigma,V)}$);
(b) for all negative rewrite rule $A \to^- P$ in $\mathit{Rew}(\Gamma \vdash \Delta)$, there exists a proof of $\mathcal{P}(\Gamma \vdash \Delta) \vdash A \Rightarrow P$ in $\emptyset$ (i.e. using only term rewrite rules of $R_{\mathcal{T}(\Sigma,V)}$);
(c) there exists a Cut-free proof of $\vdash \mathcal{P}(\Gamma \vdash \Delta)$ in $\mathit{Rew}(\Gamma \vdash \Delta)$.

Property 17 is a stronger notion than the compatibility in the sense of Definition 1.4 of Dowek et al. [4]: it imposes Cut-*free* proof in (c) and it does not care about term rewrite rules. Property 17(a) and 17(b) implies the following:

Proposition 18. *For all sequents $\Gamma \vdash \Delta$, for all rewrite systems R, if there is a proof of a sequent $\Gamma' \vdash \Delta'$ in the rewrite system $\mathit{Rew}(\Gamma \vdash \Delta) \cup R$, there is a proof of $\mathcal{P}(\Gamma \vdash \Delta), \Gamma' \vdash \Delta'$ in R.*

PROOF. We prove it by induction on the proof of $\Gamma' \vdash \Delta'$. The only interesting case is when the last inference rule is an unfolding rule. If it is $\uparrow$-l with a rule in $Rew(\Gamma \vdash \Delta) \setminus R$, we have

$$\dfrac{\begin{array}{c}\vdots\\ \Gamma', A, P \vdash \Delta'\end{array}}{\Gamma', A \vdash \Delta'}\ \uparrow\text{-l}(B \rightarrow^{-} Q)$$

with $B \rightarrow^{-} Q$ in $Rew(\Gamma \vdash \Delta)$ and $A = \sigma B$, $P = \sigma Q$ for some substitution σ. By induction hypothesis, there exists a proof π of $\mathcal{P}(\Gamma \vdash \Delta), \Gamma', A, P \vdash \Delta'$ in $\emptyset$. By Property 17(b), there is a proof ϖ of $\mathcal{P}(\Gamma \vdash \Delta) \vdash B \Rightarrow Q$ in $\emptyset$. We can apply σ to ϖ to get a valid proof ϖ' of $\mathcal{P}(\Gamma \vdash \Delta) \vdash A \Rightarrow P$.

We can therefore build the proof

$$\dfrac{\dfrac{\begin{array}{c}\pi\\ \vdots\\ \mathcal{P}(\Gamma \vdash \Delta), \Gamma', A, P \vdash \Delta'\end{array} \quad \dfrac{}{\mathcal{P}(\Gamma \vdash \Delta), \Gamma', A \vdash A, \Delta'}\ \mathsf{Axiom}}{\mathcal{P}(\Gamma \vdash \Delta), \Gamma', A, A \Rightarrow P \vdash \Delta'}\ \Rightarrow\text{-l} \qquad \varpi'}{\mathcal{P}(\Gamma \vdash \Delta), \Gamma', A \vdash \Delta'}\ \mathsf{Cut}(A \Rightarrow P)$$

which is indeed in R.

The case of $\uparrow$-r is very similar. □

The next property will also be useful for the completion procedure. It essentially says that Rew should be modular, i.e. for all sequents s, s_1, s_2, if $Rew(s) = Rew(s_1) \cup Rew(s_2)$ then having a cut-free proof of s_1 and s_2 implies having a cut-free proof of s, whatever the rewrite system used in the modulo.

Property 19. For all proposition rewrite system R, for all sequents s, if for all rewrite rules $r \in Rew(s)$ there exists a sequent s_r which is provable without Cut in R and such that $r \in Rew(s_r)$, then s has a Cut-free proof in R.

4.2. An Algorithm ...

We now present one possible algorithm having the required properties. It is quite simple to describe: it consists in applying rules of the sequent calculus to the sequent until an atomic proposition appears in the sequent. This atomic proposition will be the left-hand side of the polarized rewrite rule, the polarity of the rule will depend on the side of the sequent in which A appears, and the right-hand side will contain all other propositions.

More precisely, the algorithm can be described by the non-deterministic steps below. To decompose universally quantified propositions on the left and existentially quantified propositions on the right only once, we mark that they have already been decomposed by underlining them.

Step 1. Choose a sequent. Push all negated propositions on the other side of the sequent. For instance, $A, \neg B \vdash \neg C, \neg\neg D$ becomes $A, C \vdash B, D$. If the new Γ contains only underlined propositions (or no proposition), go to step 2. If the new Δ contains only underlined propositions (or no proposition), go to step 3. Else, go to either Step 2 or Step 3.

Step 2. Decompose the last proposition iteratively:

$P_1, \ldots, P_n \vdash Q_1, \ldots, Q_m$ becomes $P_1, \ldots, P_n, \neg Q_1, \ldots, \neg Q_{m-1} \vdash Q_m$

$P_1, \ldots, P_n \vdash Q_1 \wedge Q_2$ " $P_1, \ldots, P_n \vdash Q_1$; $P_1, \ldots, P_n \vdash Q_2$

$P_1, \ldots, P_n \vdash Q_1 \vee Q_2$ " $P_1, \ldots, P_n, \neg Q_1 \vdash Q_2$

$P_1, \ldots, P_n \vdash Q_1 \Rightarrow Q_2$ " $P_1, \ldots, P_n, Q_1 \vdash Q_2$

$P_1, \ldots, P_n \vdash \forall x.\ Q$ " $P_1, \ldots, P_n \vdash \{y/x\}Q$
where y does not appear in $P_1, \ldots, P_n$

$P_1, \ldots, P_n \vdash \exists x.\ Q$ " $P_1, \ldots, P_n, \underline{\neg \exists x.\ Q} \vdash \{t/x\}Q$
where t can be any term

$P_1, \ldots, P_n \vdash A$ " $A \rightarrow^+ \exists x_1, \ldots, x_p.\ (P_1 \wedge \cdots \wedge P_n)$

(A atomic, and the x_i are the free variables appearing in $P_1, \ldots, P_n$ but not in A)

for $P_1, \ldots, P_n \vdash \neg Q$, return to Step 1

Step 3. Decompose the first proposition iteratively, dually from step 2. For instance,

$P_1 \Rightarrow P_2 \vdash Q_1, \ldots, Q_m$ becomes $P_2 \vdash Q_1, \ldots, Q_m$; $\neg P_1 \vdash Q_1, \ldots, Q_m$

$\forall x.\ P \vdash Q_1, \ldots, Q_m$ " $\{t/x\}P \vdash \neg \underline{\forall x.\ P}, Q_1, \ldots, Q_m$
where t can be any term

$A \vdash Q_1, \ldots, Q_m$ " $A \rightarrow^- \forall x_1, \ldots, x_p.\ (Q_1 \vee \cdots \vee Q_m)$

(A atomic, and the x_i are the free variables appearing in $Q_1, \ldots, Q_m$ but not in A)

for $\neg P \vdash Q_1, \ldots, Q_m$, return to Step 1.

In practice, we can for instance choose x for t, so that no substitution is needed in those cases. All other choices are also correct. Of course, at the end, the underlines are removed.

This algorithm clearly terminates, because each times a step 2 or 3 begins, either a rewrite rule is generated, or a proposition is decomposed into subformulæ, so that the number of connectors in the non-underlined propositions in a sequent different from $\neg$ strictly diminishes. Of course, we do not pretend that this algorithm is the most optimized for our purpose.

We denote $Rew(\Gamma \vdash \Delta)$ the function returning the rewrite system obtained by applying the algorithm to $\{\Gamma \vdash \Delta\}$.

To get an intuition on this algorithm, it may be seen as the attempt to build a Cut-free proof of a sequent, adding rewrite rules to close the branches where an atomic proposition appears.

4.3. ... with the Good Properties

We first prove Property 17 using three lemmata.

Lemma 20. *If the sequent $\Gamma \vdash \Delta$ is transformed to the set of sequents $\{\Gamma' \vdash \Delta'\} \cup S'$ by the algorithm described in Section 4.2, then the sequent*

$$\mathcal{P}(\Gamma \vdash \Delta) \vdash \mathcal{P}(\Gamma' \vdash \Delta')$$

can be proved (without proposition rewrite rules).

PROOF. By case analysis on the transformation. For instance, in Step 2, $P_1, \ldots, P_n \vdash Q_1 \wedge Q_2$ is transformed into $P_1, \ldots, P_n \vdash Q_1; P_1, \ldots, P_n \vdash Q_2$. Suppose $x_1, \ldots, x_n$ (resp. $y_1, \ldots, y_m$) are the free variables of $P_1, \ldots, P_n, Q_1 \wedge Q_2$ (resp.$P_1, \ldots, P_n, Q_1$). $\{y_1, \ldots, y_m\} \subseteq \{x_1, \ldots, x_n\}$ so that we can suppose $y_i = x_i$ for $i \in \{1, \ldots, m\}$. We have the following proof (only relevant propositions are written, and the substitutions are forgotten in the above part of the proof):

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{}{Q_1, Q_2 \vdash Q_1}\,\textsf{Axiom}}{Q_1 \wedge Q_2 \vdash Q_1}\,\wedge\textsf{-l} \qquad \dfrac{}{\bigwedge_i P_i \vdash \bigwedge_i P_i}\,\textsf{Axiom}}{\bigwedge_i P_i \Rightarrow (Q_1 \wedge Q_2), \bigwedge_i P_i \vdash Q_1}\,\Rightarrow\textsf{-l}}{\bigwedge_i P_i \Rightarrow (Q_1 \wedge Q_2) \vdash \bigwedge_i P_i \Rightarrow Q_1}\,\Rightarrow\textsf{-r}}{\forall x_1, \ldots, x_n.\ (\bigwedge_i P_i \Rightarrow (Q_1 \wedge Q_2)) \vdash (\bigwedge_i P_i \Rightarrow Q_1)}\,\forall\textsf{-l}}{\forall x_1, \ldots, x_n.\ (\bigwedge_i P_i \Rightarrow (Q_1 \wedge Q_2)) \vdash \forall y_1, \ldots, y_m.\ (\bigwedge_i P_i \Rightarrow Q_1)}\,\forall\textsf{-r}$$

It can be checked that the side conditions of the rules $\exists$-l and $\forall$-r are verified. □

Lemma 21. *For all propositions $A, P_1, \ldots, P_n$, if $x_1, \ldots, x_p$ are the free variables of $P_1, \ldots, P_n$ not appearing freely in A, then the sequents*

$$\mathcal{P}(P_1, \ldots, P_n \vdash A) \vdash (\exists x_1, \ldots, x_p.\ \bigwedge_i P_i) \Rightarrow A$$

$$\mathcal{P}(A \vdash P_1, \ldots, P_n) \vdash A \Rightarrow \forall x_1, \ldots, x_p.\ \bigvee_i P_i$$

can be proved (without proposition rewrite rules).

PROOF. Suppose $y_1, \ldots, y_m$ are the free variables of $A, P_1, \ldots, P_n$. Note that $\{x_1, \ldots, x_p\} \subseteq \{y_1, \ldots, y_m\}$ so that we can suppose $y_i = x_i$ for $i \in \{1, \ldots, p\}$. We can construct the following proof (only relevant propositions are written):

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{}{A \vdash A}\,\textsf{Axiom} \qquad \dfrac{}{\bigwedge_i P_i \vdash \bigwedge_i P_i}\,\textsf{Axiom}}{(\bigwedge_i P_i \Rightarrow A), \bigwedge_i P_i \vdash A}\,\Rightarrow\textsf{-l}}{\forall y_1, \ldots, y_m.\ (\bigwedge_i P_i \Rightarrow A), \bigwedge_i P_i \vdash A}\,\forall\textsf{-l}}{\forall y_1, \ldots, y_m.\ (\bigwedge_i P_i \Rightarrow A), \exists x_1, \ldots, x_p.\ \bigwedge_i P_i \vdash A}\,\exists\textsf{-l}}{\forall y_1, \ldots, y_m.\ (\bigwedge_i P_i \Rightarrow A) \vdash (\exists x_1, \ldots, x_p.\ \bigwedge_i P_i) \Rightarrow A}\,\Rightarrow\textsf{-r}$$

The proof of the other sequent is dual. □

Note that although the proofs given by Lemmata 20 and 21 are Cut-free, we will need Cuts to link them and prove Properties 17(a) and 17(b).

Lemma 22. *For all atomic propositions A and propositions $P_1, \ldots, P_n$, if $x_1, \ldots, x_p$ are the free variables of $P_1, \ldots, P_n$ not appearing freely in A, then we can prove without* Cut *the sequent*

$$\vdash \mathcal{P}(P_1, \ldots, P_n \vdash A)$$

in the rewrite system consisting of the rule $A \rightarrow^{+} \exists x_1, \ldots, x_p.\ (P_1 \wedge \cdots \wedge P_n)$*, and the sequent*

$$\vdash \mathcal{P}(A \vdash P_1, \ldots, P_n)$$

in the rewrite system consisting of the rule $A \rightarrow^{-} \forall x_1, \ldots, x_p.\ (P_1 \vee \cdots \vee P_n)$*.*

PROOF. Suppose $y_1, \ldots, y_m$ are the free variables of $A, P_1, \ldots, P_n$. Note that $\{x_1, \ldots, x_p\} \subseteq \{y_1, \ldots, y_m\}$ so that we can suppose $y_i = x_i$ for $i \in \{1, \ldots, p\}$. Because $x_1, \ldots, x_p$ do not appear in A, $\{t_i/y_i\}A = \{t_i/y_i : i > p\}A$. Only relevant propositions are written:

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{}{P_1 \vdash P_1}\ \mathsf{Axiom} \quad \cdots \quad \dfrac{}{P_n \vdash P_n}\ \mathsf{Axiom}}{P_1, \ldots, P_n \vdash A, P_1 \wedge \cdots \wedge P_n}\ \wedge\text{-}\mathsf{r}}{\bigwedge_i P_i \vdash A, P_1 \wedge \cdots \wedge P_n}\ \wedge\text{-}\mathsf{l}}{\bigwedge_i P_i \vdash A, \exists x_1, \ldots, x_p.\ (P_1 \wedge \cdots \wedge P_n)}\ \exists\text{-}\mathsf{r}}{\bigwedge_i P_i \vdash A}\ \uparrow\text{-}\mathsf{r}}{\vdash \bigwedge_i P_i \Rightarrow A}\ \Rightarrow\text{-}\mathsf{r}}{\vdash \forall y_1, \ldots, y_m.\ (\bigwedge_i P_i \Rightarrow A)}\ \forall\text{-}\mathsf{r}$$

□

We can prove Property 19 using the following lemma:

Lemma 23. *For all proposition rewrite system R, if the set of sequents S is transformed into the set of sequents S' by the algorithm of Section 4.2 without the production of a rewrite rule, then all sequents of S have a (resp.* Cut*-free) proof in R iff all sequents of S' have a (resp.* Cut*-free) proof in R.*

PROOF. By case analysis on the transformation. The "if" part is the application of logical rules, whereas the "only if" part is a consequence of Lemma 3.

For instance, $P_1, \ldots, P_n \vdash \forall x.\ Q$ is transformed into $P_1, \ldots, P_n \vdash \{y/x\}Q$ where y does not appear in $P_1, \ldots, P_n$. If $P_1, \ldots, P_n \vdash \{y/x\}Q$ has a proof in R, then because y does not appear in $P_1, \ldots, P_n$, $P_1, \ldots, P_n \vdash \forall x.\ Q$ has a proof in R by application of $\forall$-r. Conversely, if $P_1, \ldots, P_n \vdash \forall x.\ Q$ has a proof in R, then by Lemma 3 there exists a proof of $P_1, \ldots, P_n \vdash \{y/x\}Q$ in R for y not free in $P_1, \ldots, P_n$. Therefore $P_1, \ldots, P_n \vdash \{y/x\}Q$ has a proof in R.

In the preceding paragraph, if proofs are supposed Cut-free, then the resulting proofs have the same property. □

We can now prove the main result of this subsection:

Proposition 24. *The Rew function defined in Section 4.2 has the Properties 16, 17 and 19.*

PROOF. We proceed by induction on the execution of the algorithm of Section 4.2.

Property 16 directly follows from the fact that $Rew(A \vdash P) = \{A \rightarrow^{-} P\}$ and $Rew(P \vdash A) = \{A \rightarrow^{+} P\}$.

For Properties 17(a) and 17(b), Lemma 21 permits to prove the properties at the end of the algorithm, when sequents are transformed into rules. Lemma 20 permits to prove the inductive case: suppose $\Gamma \vdash \Delta$ is transformed into $\{\Gamma' \vdash \Delta'\} \cup \cdots$. Suppose $\mathcal{P}(\Gamma' \vdash \Delta') \vdash A \Rightarrow P$ has a proof π without proposition rewrite rules. By Lemma 20, there is a proof π' of $\mathcal{P}(\Gamma \vdash \Delta) \vdash \mathcal{P}(\Gamma' \vdash \Delta')$ in $\emptyset$. Therefore, we can construct the proof

$$\dfrac{\begin{array}{cc}\vdots\,\pi & \vdots\,\pi' \\ \mathcal{P}(\Gamma \vdash \Delta), \mathcal{P}(\Gamma' \vdash \Delta') \vdash A \Rightarrow P & \mathcal{P}(\Gamma \vdash \Delta) \vdash \mathcal{P}(\Gamma' \vdash \Delta'), A \Rightarrow P\end{array}}{\mathcal{P}(\Gamma \vdash \Delta) \vdash A \Rightarrow P}\ \mathsf{Cut}(\mathcal{P}(\Gamma' \vdash \Delta'))$$

without proposition rewrite rules.

For Property 17(c), the base case is a consequence of Lemma 22, whereas the inductive case is a consequence of Lemma 3. For instance, suppose $P_1, \ldots, P_n \vdash Q_1 \wedge Q_2$ is transformed into $P_1, \ldots, P_n \vdash Q_1; P_1, \ldots, P_n \vdash Q_2$. For $i \in \{1, 2\}$, suppose $\vdash \mathcal{P}(P_1, \ldots, P_n \vdash Q_i)$ has a Cut-free proof in some rewrite system R_i. By Lemma 3, there is a Cut-free proof π_i of $P_1, \ldots, P_n \vdash Q_i$ in R_i. Consequently we can construct the Cut-free proof

$$\dfrac{\begin{array}{cc}\vdots\,\pi_1 & \vdots\,\pi_2 \\ P_1, \ldots, P_n \vdash Q_1 & P_1, \ldots, P_n \vdash Q_2\end{array}}{\vdash \mathcal{P}(P_1, \ldots, P_n \vdash Q_1 \wedge Q_2)}\ \forall\text{-}\mathsf{r}, \Rightarrow\text{-}\mathsf{r}, \wedge\text{-}\mathsf{l}, \wedge\text{-}\mathsf{r}$$

in $R_1 \cup R_2$.

For Property 19, using Lemma 23 by induction on the execution of the algorithm, we obtain that a sequent s is provable without Cut in a rewrite system R iff the sequents eventually producing all rules of $Rew(s)$ are provable without Cut in R. Suppose that for all $r \in Rew(s)$ there exists a sequent s_r provable without Cut in R such that $r \in Rew(s')$. Then the sequent producing each r can be proved without Cut in R. Therefore s can be proved without Cut in R. □

NOTE. $\mathcal{P}(\Gamma \vdash \Delta)$ is compatible with $Rew(\Gamma \vdash \Delta)$ in classical logic, but it is not true for intuitionistic logic. For instance, $Rew(\vdash \exists x.\ B(x)) = \{B(x) \rightarrow^{+} \neg\exists x.\ B(x)\}$. Then, $\vdash \exists x.\ B(x)$ has the following proof in $Rew(\vdash \exists x,\ B(x))$

$$\dfrac{\dfrac{\dfrac{\dfrac{}{\exists x.\ B(x) \vdash \exists x.\ B(x), B(x)}\ \mathsf{Axiom}}{\vdash \exists x.\ B(x), B(x), \neg\exists x.\ B(x)}\ \neg\text{-}\mathsf{r}}{\vdash \exists x.\ B(x), B(x)}\ \uparrow\text{-}\mathsf{r}}{\vdash \exists x.\ B(x)}\ \exists\text{-}\mathsf{r}$$

in the classical polarized unfolding sequent calculus but it has no proof in, for instance, the polarized natural deduction of Dowek [15], which is an intuitionistic system. As pointed out by a referee, it is not possible to transform an axiom

$\exists x.\ B(x)$ into a rewrite system admitting Cut and compatible in intuitionistic logic, because the theory formed with the axiom do not enjoy the witness property, but it would using the rewrite system. Notice also that, as shown by Hermant [11], Cut admissibility in classical and intuitionistic logic are not equivalent in deduction modulo.

NOTE. It is possible that the produced rewrite system does not admit Cut. For instance, on $\vdash A \Leftrightarrow B \wedge \neg A$ the algorithm returns Crabbé's system of the introduction.

As a nice consequence of the properties of Rew, we obtain a way to internalize in the congruence any first-order theory:

Corollary 25. *For all finite set of formulæ Γ and rewrite systems R, there exists a rewrite system R' such that for all finite set of formulæ Δ: $\Gamma \vdash \Delta$ is derivable in R iff $\vdash \Delta$ is derivable in R'.*

PROOF. Simply take $R' = R \cup \bigcup_{P \in \Gamma} Rew(\vdash P)$. □

5. Abstract Completion for Cut Admissibility

We present in this section the completion procedure which permits to transform a rewrite system into one admitting Cut. It is based on an abstract completion procedure introduced in the framework of the Abstract Canonical Systems and Inference, that we are first presenting.

5.1. Abstract Canonical Systems and Inference

The results in this section are extracted from Dershowitz and Kirchner [16, 30] and Bonacina and Dershowitz [17], which should be consulted for motivations, details and proofs. We define a framework with abstract notions of formulæ, proofs, etc. These should not be confused with the first-order propositions and sequent-calculus proofs used before, although the framework *could* be instantiated with those. In Section 5.2 we will see which exact instance we will be using. In this section, to give intuitions, we will use standard completion as an example of instance, but without going into details (that can be found in Burel and Kirchner [19]).

Let $\mathbb{A}$ be the set of all (abstract) formulæ over some fixed vocabulary. Let $\mathbb{P}$ be the set of all (abstract) proofs. These sets are linked by two functions: $[\cdot]^{Pm} : \mathbb{P} \to 2^{\mathbb{A}}$ gives the *premises* in a proof, and $[\cdot]_{Cl} : \mathbb{P} \to \mathbb{A}$ gives its *conclusion*. Both are extended to sets of proofs in the usual fashion. The set of proofs built using assumptions in $R \subseteq \mathbb{A}$ is denoted by

$$Pf(R) \quad \stackrel{!}{=} \quad \left\{p \in \mathbb{P} : [p]^{Pm} \subseteq R\right\} \ .$$

The framework described here is predicated on two *well-founded* partial orderings over $\mathbb{P}$: a *proof ordering* $>$ and a *subproof relation* $\rhd$. They are related by a monotonicity requirement (postulate E). The proof ordering expresses the

quality of proofs, whereas the subproof relation translates their structures. We assume for convenience that the proof ordering only compares proofs with the same conclusion ($p > q \Rightarrow [p]_{Cl} = [q]_{Cl}$), rather than mention this condition each time we have cause to compare proofs.

Example 26. For standard completion, formulæ are rewrite rules or equations, proofs are proofs by rewriting (for instance $a \underset{s\to t}{\longleftarrow} b \underset{u\to v}{\longrightarrow} c \underset{e=f}{\longleftrightarrow} d$ as a proof of $a = d$ in $Pf(\{s \to t; u \to v; e = f\})$). The proof ordering is chosen so that $a \underset{s\to t}{\longleftarrow} b \underset{u\to v}{\longrightarrow} c$ is greater than $a \underset{a=c}{\longleftrightarrow} c$, which is greater than a proof of the form $a \overset{*}{\longrightarrow} \overset{*}{\longleftarrow} c$.

We will use the term *presentation* to mean a set of formulæ, and *justification* to mean a set of proofs. We reserve the term *theory* for deductively closed presentations:

$$Th\ R \quad \overset{!}{=} \quad [Pf(R)]_{Cl} \quad = \quad \{[p]_{Cl} : p \in \mathbb{P},\ [p]^{Pm} \subseteq R\}\ .$$

In addition to this, we assume the two following postulates:

Postulate A (Reflexivity). For all presentations R:

$$R \subseteq Th\ R$$

Postulate B (Closure). For all presentations R:

$$Th\ Th\ R \subseteq Th\ R$$

We call a proof *trivial* when it proves only its unique assumption and has no subproofs other than itself, that is, if $[p]^{Pm} = \{[p]_{Cl}\}$ and $p \trianglerighteq q \Rightarrow p = q$, where $\trianglerighteq$ is the reflexive closure of the subproof ordering $\triangleright$. We denote by $\widehat{a}$ such a trivial proof of $a \in \mathbb{A}$ and by $\widehat{R}$ the set of trivial proofs of each $a \in R$.

Example 27. For standard completion, the trivial proof of $s \to t$ is just $s \underset{s\to t}{\longrightarrow} t$.

We assume that proofs use their assumptions (postulate C), that subproofs don't use non-existent assumptions (postulate D), and that proof orderings are monotonic with respect to subproofs (postulate E):

Postulate C (Trivia). For all proofs p and formulæ a:

$$a \in [p]^{Pm} \Rightarrow p \trianglerighteq \widehat{a}$$

Postulate D (Subproofs Premises Monotonicity). For all proofs p and q:

$$p \trianglerighteq q \Rightarrow [p]^{Pm} \supseteq [q]^{Pm}$$

Postulate E (Replacement). For all proofs p, q and r:

$$p \triangleright q > r \Rightarrow \exists v \in Pf([p]^{Pm} \cup [r]^{Pm}).\ p > v \triangleright r$$

We make no other assumptions regarding proofs or their structure and the proof ordering $>$ is lifted to a quasi-ordering $\gtrsim$ over presentations:

$$R_1 \gtrsim R_2 \text{ if } Th\, R_1 = Th\, R_2 \text{ and } \forall p \in Pf(R_1).\ \exists q \in Pf(R_2).\ p \geq q \ .$$

A *normal-form proof* for R will be a proof that is minimal whatever the presentation of the theory build on R, i.e. it is one of the minimal proofs of $Pf(Th\, R)$:

$$\begin{array}{lcl} Nf(R) & \stackrel{!}{=} & \mu Pf(Th\, R) \\ & \stackrel{!}{=} & \{p \in Pf(Th\, R) \ :\ \neg\exists q \in Pf(Th\, R).\ p > q\} \end{array}$$

Normal form proofs are the best, the one we wish we can build from our current presentation.

Example 28. For standard completion, normal proofs are valley proofs, that is, proofs of the form $a \stackrel{*}{\longrightarrow} \stackrel{*}{\longleftarrow} c$.

The *canonical presentation* contains those formulæ that appear as assumptions of normal-form proofs:

$$R^\sharp \quad \stackrel{!}{=} \quad [Nf(R)]^{Pm} \ .$$

So, we will say that R is *canonical* if $R = R^\sharp$. Intuitively, the canonical presentation of R contains the formulæ that are necessary to build all the best proofs of the theory of R, and only these formulæ.

A presentation R is *complete* if every theorem has a normal-form proof:

$$Th\, R = [Pf(R) \cap Nf(R)]_{Cl}$$

Canonicity implies completeness, but the converse is not true. Intuitively, R is complete iff it contains enough to build all the theory using only its own best proofs.

Example 29. For standard completion, completeness means that every equality provable with a rewrite system can be proved with this rewrite system using a valley proof. In other words, a complete rewrite system is confluent.

We now consider inference and deduction mechanisms. A *deduction mechanism* $\rightsquigarrow$ is a function from presentations to presentations and we call the relation $R_1 \rightsquigarrow R_2$ a *deduction step*.

A sequence of presentations $R_0 \rightsquigarrow R_1 \rightsquigarrow \cdots$ is called a *derivation*.

The *result* of the derivation is, as usual, its *persisting* formulæ:

$$R_\infty \quad \stackrel{!}{=} \quad \liminf_{j\to\infty} R_j \ = \ \bigcup_{j>0} \bigcap_{i>j} R_i \ .$$

A deduction mechanism is *completing* if for each step $R_1 \rightsquigarrow R_2$, $R_1 \gtrsim R_2$ and the limit R_∞ is complete.

A completing mechanism can be used to build normal-form proofs of theorems of the initial presentation:

Theorem 30 (Bonacina and Dershowitz [17, Lemma 5.13]). *A deduction mechanism is completing if and only if for all derivations $R_0 \rightsquigarrow R_1 \rightsquigarrow \cdots$,*

$$Th\, R_0 \subseteq [Pf(R_\infty) \cap Nf(R_0)]_{Cl} \ .$$

A *critical proof* is a minimal proof which is not in normal form, but whose strict subproofs are:

$$Crit(R) \quad \stackrel{!}{=} \quad \left\{ \begin{array}{l} p \in \mu Pf(R) \setminus Nf(R) : \\ \forall q \in Pf(R).\ p \rhd q \Rightarrow q \in Nf(R) \end{array} \right\}$$

Intuitively, a critical proof of R is a minimal (in terms of quality and structure) counter-example that shows that R is not complete.

Example 31. For standard completion, critical proofs correspond to non-confluent critical pairs, that is, proofs $a \underset{s[b] \to a}{\longleftarrow} s[b] \underset{b \to c}{\longrightarrow} s[c]$ with no valley proof $a \stackrel{*}{\longrightarrow} \stackrel{*}{\longleftarrow} s[c]$. Standard completion adds the equation $a = s[c]$ to the presentation, so that it is possible to build the smaller proof $a \underset{a = s[c]}{\longleftrightarrow} s[c]$.

The idea to obtain a complete presentation is therefore to enhance the current presentation with formulæ that permits to build proofs smaller than the critical ones. *Completing formulæ* are then premises of proofs smaller than critical proofs:

$$Comp(R) \quad \stackrel{!}{=} \quad \bigcup_{\substack{p \in Crit(R) \\ p' \text{ is any proof such that } p > p'}} [p']^{Pm}$$

To get a completing procedure, we therefore need to add at least these proofs, and we can only add formulæ that are in the theory. In this paper, given some function C from presentations to presentations such that $Comp(R) \subseteq \mathsf{C}(R) \subseteq Th\, R$ for all presentations R, the deduction mechanism is therefore:

$$R \rightsquigarrow R \cup \mathsf{C}(R) \ .$$

Proposition 32 (Dershowitz and Kirchner [30, Lemma 10]). *This deduction mechanism is completing.*

Example 33. For standard completion, the deduction mechanism is more evolved, because there are also simplification steps. Burel and Kirchner [19] give remaining details.

5.2. Deduction Modulo is an Instance of ACS

We want to show that the polarized unfolding sequent calculus can be seen as an instance of ACS. For this purpose, we have to define what the (abstract) formulæ, proofs, premises and conclusions are, and to give the appropriate orderings. After this, we need to check that the postulates are verified by the defined instance.

5.2.1. Proofs and Formulae

We aim to obtain Cut-free proofs, so that the natural candidate for abstract proofs are polarized-unfolding-sequent-calculus proofs.

The completion procedure we want to establish deals with polarized rewrite rules over atomic propositions. Nevertheless, the conclusions of the proofs, from which we want to generate the rewrite rules added by the completion mechanism, are sequents. In other words, sequents must be related to rewrite rules. We therefore assume that we have a function Rew satisfying Properties 16, 17 and 19. Only these properties are important, so that we do not need to use the particular algorithm given in Section 4.2.

Then, ACS formulæ will be polarized rewrite rules (similarly as for standard completion), and proofs will be polarized-unfolding-sequent-calculus proofs. The premises of a proof are the rewrite rules used in that proof. For the conclusion, as a sequent may be associated by Rew to several rewrite rules, we would need proofs with several conclusions. However, we can bypass this by considering several instances of a proof of $\Gamma \vdash \Delta$, one for each rules in $Rew(\Gamma \vdash \Delta)$. The conclusion of a proof will therefore be this particular rule.

5.2.2. Orderings on Proofs

To define an ordering on proofs, we need the concept of proof skeleton:

Definition 34. The *skeleton* of a proof p is the tree labeled by the inference rules used p, with the active proposition in the case of Cut and Axiom.

We define the following precedence $>$ on inference rules: for all propositions P, Q, O, if P is greater than Q for the subformula relation, then $\mathsf{Cut}(P) > \mathsf{Cut}(Q)$ and $\mathsf{Axiom}(P) > \mathsf{Axiom}(Q)$, and for all other inference rules r of Fig. 1, $\mathsf{Cut}(P) > \mathsf{Axiom}(O) > \mathsf{r}$. This precedence is infinite, but it is well founded because the subformula relation is.

We order the proof skeletons with the RPO [31] based on this precedence. Since the precedence is well-founded, so is the RPO [31]. We define the ordering over proofs by saying that a proof is strictly greater than another if this holds for their skeletons. This defines therefore a well-founded ordering on proofs.

We restrict this ordering to proofs which have the same conclusion.

Notice that with this ordering, a Cut-free proof is always strictly smaller than a proof with at least one Cut at root.

NOTE. To get a completion procedure producing rewrite systems admitting Cut, it should have been possible to use a coarser ordering, the essential property being that proofs with Cut are bigger than proofs without. Nevertheless, the finer the ordering is, the fewer the critical proofs are. To be able to better characterize the critical proofs, the ordering we are using seems convenient. Moreover, we use an RPO because it is a simplification ordering and Postulate E is therefore easier to prove.

Subproofs of a proof p are for a part defined as the subproofs of p for the sequent calculus. We also want to say that if a proof do not use a proposition (i.e.

it is the weakened version of another proof), then the strengthened proof should be smaller for the subproof relation. We therefore consider the transitive closure of the subproof ordering in the unfolding sequent calculus and this "weakening" ordering.

Definition 35. We say that $\pi \rhd_{sp} \pi'$ iff π' is a strict subproof of π in the sequent calculus.

We say that $\pi \rhd_w \pi'$ if there is a proposition in π that can be pruned from all sequents in π to produce the valid proof π'.

$\rhd_{\mathcal{PUSC}}$ will be the transitive closure of $\rhd_{sp} \cup \rhd_w$.

Lemma 36. *If $\pi_1 \trianglerighteq_{\mathcal{PUSC}} \pi_2$ then there exists π_3 such that $\pi_1 \rhd_{sp}^* \pi_3 \rhd_w^* \pi_2$.*

Proof. We only need to show that if $\pi_1 \rhd_w \pi_2 \rhd_{sp} \pi_3$ then there exist some π_2' such that $\pi_1 \rhd_{sp} \pi_2' \rhd_w \pi_3$. If $\pi_1 \rhd_w \pi_2$ there exists some proposition P that can be pruned in the sequents in π_1 to get π_2. Let π_2' be π_3 in which P is added in each sequents by weakening in the same side as in π_1. Then π_2' is a subproof of π_1. □

Unfortunately, this definition is not sufficient to define trivial proofs, because if we use a premise through a $\uparrow$-l or $\uparrow$-r rule, there will always be a strict subproof, so that there are no proofs using premises without strict subproofs. For instance,

$$\dfrac{\dfrac{}{P \vdash P}\ \mathsf{Axiom}}{A \vdash P}\ \uparrow\text{-}\mathsf{l}$$

seems a good candidate for the trivial proof $\widehat{A \rightarrow^- P}$, but is contains the subproof $\dfrac{}{P \vdash P}\ \mathsf{Axiom}$.

To solve this problem, we can manually add the trivial proofs. We therefore consider proofs $\widehat{a}$ for each formula $a \in \mathbb{A}$.

We have to extend the ordering $>$ to trivial proofs: it can be simply done by saying that they cannot be compared with other proofs.

For Postulate C to be verified, we have to extend the subproof relation:

$$p \trianglerighteq q \quad \begin{array}{l} \text{if } - \ q \text{ is a subproof of } p \text{ for } \trianglerighteq_{\mathcal{PUSC}} \\ \quad - \text{ or } q = \widehat{a} \text{ with } a \in [p]^{Pm}. \end{array}$$

This relation is well-founded because of the wellfoundedness of the subproof relation in the sequent calculus, and because trivial proofs cannot have strict subproofs.

To summarize, with respect to the definitions of ACSs (see Section 5.1) deduction modulo can be seen as an ACS, in the following way:

- $\mathbb{A}$: *formulæ* are polarized rewrite rules

$$\mathbb{A} \quad \overset{!}{=} \quad \mathcal{PRR} \quad (= Rew(\mathcal{S}) \text{ by Property 16})$$

- $\mathbb{P}$: *proofs* are either couples formed with a sequent calculus proof and a polarized rule in the rewrite system associated with its conclusion, or trivial proofs:

$$\mathbb{P} \stackrel{!}{=} \left\{ \left\langle \frac{\vdots}{\Gamma \vdash \Delta}, A \rightarrow^{\pm} P \right\rangle \in \mathcal{PUSC} \times \mathbb{A} : (A \rightarrow^{\pm} P) \in Rew(\Gamma \vdash \Delta) \right\} \cup \{\widehat{a} : a \in \mathbb{A}\}$$

- $[\cdot]^{Pm}$: *premises* of a non-trivial proof are the rewrite rules used in its first component, the unique premise of a trivial proof is the formula it corresponds to.

- $[\cdot]_{Cl}$: the *conclusion* of a non-trivial proof is its second component, the conclusion of a trivial proof is the formula it corresponds to.

- $>$: the ordering on proofs is defined by $p > q$ if p and q are not trivial, their second component is the same as well as the conclusion of their first component, and the skeleton of the first component of p is greater than the one of q for the RPO based on the precedence defined by: for all propositions P, Q, O, if P is greater than Q for the subformula relation, then $\mathsf{Cut}(P) > \mathsf{Cut}(Q)$ and $\mathsf{Axiom}(P) > \mathsf{Axiom}(Q)$, and for all other inference rules r of Fig. 1, $\mathsf{Cut}(P) > \mathsf{Axiom}(O) > \mathsf{r}$.

- $\rhd$: the subproof ordering is defined by $p \trianglerighteq q$ if
  - neither p nor q are trivial and the first component of p is greater than the first component of q for $\trianglerighteq_{\mathcal{PUSC}}$;
  - or $q = \widehat{a}$ with $a \in [p]^{Pm}$.

With these definitions we can prove the main theorem of this section:

Theorem 37 (Instance of ACS). *The unfolding sequent calculus is an instance of ACS, with the definitions of* $\mathbb{A}$, $\mathbb{P}$, $[\cdot]^{Pm}$, $[\cdot]_{Cl}$, $>$ *and* $\rhd$ *given above.*

Proof. First we need to show that $>$ and $\rhd$ are strict and well-founded orderings. It is not too difficult to prove that $>$ is irreflexive and transitive. It is well founded because the RPO on skeleton is, because the subformula relation is. Concerning $\rhd$, first remark that $\widehat{a} \trianglerighteq q$ iff $q = \widehat{a}$. Then, we only need to show that $\rhd_{\mathcal{PUSC}}$ is a strict ordering: indeed, it is trivially irreflexive, and transitive by definition. To show that $\rhd$ is well founded we also only need to show that $\rhd_{\mathcal{PUSC}}$ is. This is less trivial, but can be shown using Lemma 36 which says that if $p \rhd_{\mathcal{PUSC}} q$, then q can be obtained by pruning some propositions in a subproof of p. Then we only need to show that $\rhd_{sp}$ and $\rhd_{w}$ are well founded, which holds because the first relation makes the skeleton of proof decrease whereas the second makes the number of propositions in the conclusion decrease.

We then show the postulates:

- Postulate A: suppose $a \in R$, we want to show that a is the conclusion of a proof built with R. $\widehat{a}$ is such a proof.

- Postulate B: let a be in $Th\,Th\,R$. By definition there is a proof $p \in Pf(Th\,R)$ such that $[p]_{Cl} = a$. If p is trivial, then $\{a\} = [p]^{Pm} \subseteq Th\,R$ therefore $a \in Th\,R$. If p is not trivial, then its first component $\pi_p \in \mathcal{PUSC}$ proves $\Gamma \vdash \Delta$ in $Th\,R$ for some $\Gamma \vdash \Delta$ such that $a \in Rew(\Gamma \vdash \Delta)$. Rewrite rules used in π_p are therefore in $Th\,R$. Let $b \in [p]^{Pm}$ be such a rule. There exists $q \in Pf(R)$ such that $[q]_{Cl} = b$. If q is trivial, then $\{b\} = [p]^{Pm} \subseteq R$ therefore $b = [p]_{Cl} \in R$. Else, its first component $\pi_q \in \mathcal{PUSC}$ proves s in R for some s such that $b \in Rew(s)$. Using Property 17 and Proposition 18, we can transform π_p into a proof ϖ_p of $\Gamma, \mathcal{P}rop(s) \vdash \Delta$ in $[p]^{Pm} \setminus Rew(s)$. One can apply $\wedge$-l, $\vee$-r, $\Rightarrow$-r and $\forall$-r to π_q to get a proof of $\vdash \mathcal{P}rop(s)$ in R. By applying Cut to this proof and ϖ_p we obtain a proof of $\Gamma \vdash \Delta$ in $[p]^{Pm} \setminus Rew(s) \cup R$. By repeating this process to every premises of p not in R, we eventually obtain a proof π in R whose conclusion is $\Gamma \vdash \Delta$. Then, $a = [\langle \pi, a \rangle]_{Cl} \in [Pf(R)]_{Cl} = Th\,R$.

- Postulate C: it holds by definition of the subproof relation $\trianglerighteq$.

- Postulate D: suppose $p \trianglerighteq q$. If $q = \widehat{a}$ then by definition of $\trianglerighteq$, we have $[q]^{Pm} = \{a\} \subseteq [p]^{Pm}$. If q is not trivial, neither is p. In that case, by definition of $\rhd_{\mathcal{PUSC}}$ the first component of q use a subset of the rules used in the first component of p.

- Postulate E: suppose $p \rhd q > r$. Because q is comparable with r, none of them is trivial, and p neither. We call π_p, π_q and π_r their first components. Because of Lemma 36, π_q can be obtained by pruning some first-order propositions in a subproof π' of π_p. By definition of $>$, π_q and π_r have the same conclusion. We can therefore add the propositions pruned in π' in π_r, and replace π' by this proof in π_p to get a valid proof π_v. If a is the second component of p, then let $v \overset{!}{=} \langle \pi_v, a \rangle$, which is a correct ACS proof because π_p and π_v have the same conclusion. Then $p > v$ because the RPO is a simplification ordering and because if $\pi_1 \rhd_w \pi_2$, then π_1 and π_2 have the same skeleton. Moreover, by definition of π_v, $v \rhd r$. Furthermore, the rewrite rules used in π_v are included in the ones used in π_p and π_r, therefore $v \in Pf([p]^{Pm} \cup [r]^{Pm})$.

□

5.3. A Generalized Completion Procedure

We want to define a completion procedure through critical proofs. For this, we first need some characterizations of the normal-form proofs and the critical proofs. The limit of this completion procedure will be an equivalent rewrite system modulo which the sequent calculus admits Cut.

5.3.1. Normal-form Proofs and Critical Proofs in Deduction Modulo

Proposition 38 (Characterization of Normal-Form Proofs). *A proof in the unfolding sequent calculus is in normal form iff it is either a trivial proof or its first component is a* Cut*-free proof with no unneeded logical rules, where* Axiom *is applied only to atomic propositions.*

Proof. If a proof p in $Pf(R)$ is not a trivial proof, and its first component π_p possesses a Cut at position $\mathfrak{p}$, then using Property 17(c), we know that there exists a Cut-free proof of the sequent $\vdash \mathcal{P}(\Gamma \vdash \Delta)$ in $Rew(\Gamma \vdash \Delta)$ where $\Gamma \vdash \Delta$ is the conclusion of $\pi_{p_{|\mathfrak{p}}}$. Using Lemma 3 we obtain a Cut-free proof π_q of $\Gamma \vdash \Delta$. Because π_q is Cut-free and $\pi_{p_{|\mathfrak{p}}}$ has a Cut at root, the skeleton of $\pi_{p_{|\mathfrak{p}}}$ is greater than the one of π_q for the RPO. Replacing $\pi_{p_{|\mathfrak{p}}}$ by π_q in p using Postulate E, we obtain a smaller proof than p which is in $Pf(ThR)$ because π_q is by assumption in $Rew(\Gamma \vdash \Delta) = \bigcup_{a \in Rew(\Gamma \vdash \Delta)} [\langle \pi_{p_{|\mathfrak{p}}}, a \rangle]_{Cl}$, and each $\langle \pi_{p_{|\mathfrak{p}}}, a \rangle$ is in $Pf(R)$. Therefore p cannot be in normal form.

If a proof p is not a trivial proof, and its first component π_p has a unneeded logical rule at position $\mathfrak{p}$, then the direct subproofs of $\pi_{p_{|\mathfrak{p}}}$ shows the same conclusion as $\pi_{p_{|\mathfrak{p}}}$ when weakened, and are smaller because an RPO is a simplification ordering and the weakening of a proof does not change its skeleton. By using Postulate E we can obtain a proof smaller than p, and therefore p cannot be in normal form.

If a proof p is not a trivial proof, and its first component apply Axiom to a non-atomic proposition, then it is always possible to replace this application by some proof where Axiom is applied only to atomic propositions. Given the definition of the precedence, this proof is smaller than the original application of Axiom and p is therefore not minimal.

Due to our definition of the precedence of the RPO, if a non-trivial proof p is not minimal in every presentation of a theory, i.e. there exists a smaller proof q, then either the first component of p contains a Cut, or it applies Axiom on a non-atomic proposition, or the first component of q is a weakened subproof of the one of p, i.e. unneeded rules were applied in p.

A trivial proof in $Pf(R)$ is not comparable with any other proof, in particular in $Pf(Th\,R)$, so that it is in normal form. □

We give now a characterization of the critical proofs in deduction modulo.

Proposition 39 (Critical Proofs in Deduction Modulo). *Critical proofs in deduction modulo are non trivial and their first component is of the form*

$$\dfrac{\dfrac{\begin{array}{c}\pi\\ \vdots\\ \Gamma, A, P \vdash \Delta\end{array}}{\Gamma, A \vdash \Delta}\uparrow\text{-}\mathsf{l}(B \to^{-} P_1) \quad \dfrac{\begin{array}{c}\pi'\\ \vdots\\ \Gamma \vdash Q, A, \Delta\end{array}}{\Gamma \vdash A, \Delta}\uparrow\text{-}\mathsf{r}(C \to^{+} P_2)}{\Gamma \vdash \Delta}\,\mathsf{Cut}(A)$$

where

- π *and* π' *are* Cut*-free;*
- π *and* π' *do not use unneeded logical rules;*
- π *and* π' *apply* Axiom *only to atomic propositions;*
- Γ *contains only universally quantified propositions and atomic propositions different from* A*;*
- Δ *contains only existentially quantified propositions and atomic propositions different from* A*;*
- *all propositions of* $\Gamma \cup \Delta$ *are principal proposition either in some* Axiom *(and not* $\uparrow$-l *nor* $\uparrow$-r*),* $\forall$-l *or* $\exists$-r *in* π *or* π'*.*
- *at least one of* $B \to^- P_1$ *or* $C \to^+ P_2$ *is not a* term *rewriting.*

Proof. We essentially follow the proof of the Hauptsatz of Girard, Lafont, and Taylor [32, Chapter 13].

Because of Proposition 38, subproofs of a critical proof (which are by definition in normal form) that are not trivial must be Cut-free. Furthermore, because a critical proof is not in normal form, then it possesses either a Cut, a unneeded logical rule or apply Axiom to a non atomic proposition. In the second and third cases, we can find a smaller proof in the same presentation, contradicting the minimality of critical proofs. Therefore a critical proof has a Cut at its root. It is a proof of the form

$$\dfrac{\pi \left\{ \dfrac{\pi_1 \quad \cdots \quad \pi_n}{\Gamma, P \vdash \Delta}\,\mathsf{r} \qquad \dfrac{\pi'_1 \quad \cdots \quad \pi'_m}{\Gamma \vdash P, \Delta}\,\mathsf{r'} \right\} \pi'}{\Gamma \vdash \Delta}\,\mathsf{Cut}(P)$$

where π and π' are in normal form, so are cut-free, do not use unneeded rules and apply Axiom only to atomic propositions. Moreover, if $A \in \Gamma \cup \Delta$, then Cut is unneeded. Furthermore, if Γ contains a non-atomic proposition which is not universally quantified, then either it can be pruned, in which case we can obtain a proof smaller for $\triangleright$ which is not in normal form (It contains a Cut.); or it is the principal proposition of some inference rule (different from $\forall$-l and $\uparrow$-l) in π or π'. But it is possible to permute this inference rule with all other inference rules until Cut (see Note 1), in which case we obtain a proof smaller for $>$ in the same presentation. This is also the case if some atomic proposition is rewritten using $\uparrow$-l. For Δ this is dual. All propositions in $\Gamma \cup \Delta$ are used somewhere, else they could be pruned and we could obtain a proof smaller for $\triangleright$ which would not be in normal form.

In the following, $\varpi, \varpi', \varpi_1, \ldots, \varpi_n, \varpi'_1, \ldots, \varpi'_m$ are proof obtained from $\pi, \pi', \pi_1, \ldots, \pi_n, \pi'_1, \ldots, \pi'_m$ by weakening.

We can now check the different cases that can be found in Section 13.2 of Girard et al. [32] (note that we do not have to consider structural rules in the polarized unfolding sequent calculus):

1. r is Axiom. There are two cases :
   - the principal proposition of the Axiom is P, then we have necessarily $P \in \Delta$ and π' is therefore a proof of $\Gamma \vdash \Delta$ which is smaller than the initial proof, contradicting its minimality;
   - the principal proposition of the Axiom is another proposition Q, then $Q \in \Gamma$ and $Q \in \Delta$, so that we can build the proof $\dfrac{}{\Gamma \vdash \Delta}\ \mathsf{Axiom}$ which is smaller than the initial proof, contradicting its minimality.
2. r' is Axiom. This case is handled as case 1.
3. r is a logical rule other than a left one with principal proposition P. In this case, the conclusion of a subproof π_i has the form $\Gamma_i, P \vdash \Delta_i$, because r does not touch P. We can build the proof

$$\dfrac{\dfrac{\varpi_1 \quad \varpi'}{\dfrac{\Gamma, \Gamma_1, P \vdash \Delta, \Delta_1 \qquad \Gamma, \Gamma_1 \vdash P, \Delta, \Delta_1}{\Gamma, \Gamma_1 \vdash \Delta, \Delta_1}\ \mathsf{Cut}(P)} \quad \dfrac{\dfrac{\varpi_n \quad \varpi'}{\Gamma, \Gamma_n, P \vdash \Delta, \Delta_n \qquad \Gamma, \Gamma_n \vdash P, \Delta, \Delta_n}\ \mathsf{Cut}(P)}{\Gamma, \Gamma_n \vdash \Delta, \Delta_n}}{\Gamma, \Gamma \vdash \Delta, \Delta}\ \mathsf{r}$$

   and then use Lemma 5. If we look at the proof of this lemma, we can show by induction that the skeleton of the contracted proofs is smaller than the original one for the RPO. We therefore have a smaller proof than the initial proof, contradicting its minimality.
4. r' is a logical rule other than a right one with principal proposition P. This case is handled as case 3.
5. Both r and r' are logical rules, r a left one and r' a right one, of principal proposition P. This is one of the key cases as given in Section 13.1 of Girard et al. [32] : by replacing the Cut over P by Cuts over subformulæ of P we obtain a smaller proof, thus contradicting the minimality of the original proof. For instance, if $P = P_1 \wedge P_2$, the initial proof

$$\dfrac{\dfrac{\dfrac{\pi_1}{\Gamma, P_1, P_2 \vdash \Delta}}{\Gamma, P_1 \wedge P_2 \vdash \Delta}\ \wedge\text{-l} \qquad \dfrac{\dfrac{\pi'_1 \qquad \pi'_2}{\Gamma \vdash P_1, \Delta \qquad \Gamma \vdash P_2, \Delta}}{\Gamma \vdash P_1 \wedge P_2, \Delta}\ \wedge\text{-r}}{\Gamma \vdash \Delta}\ \mathsf{Cut}(P_1 \wedge P_2)$$

is greater than the proof

$$\dfrac{\dfrac{\begin{array}{c}\pi_1\\ \vdots\\ \Gamma, P_1, P_2 \vdash \Delta\end{array} \quad \begin{array}{c}\varpi_2'\\ \vdots\\ \Gamma, P_1 \vdash P_2, \Delta\end{array}}{\Gamma, P_1 \vdash \Delta}\,\mathsf{Cut}(P_2) \quad \begin{array}{c}\pi_1'\\ \vdots\\ \Gamma \vdash P_1, \Delta\end{array}}{\Gamma \vdash \Delta}\,\mathsf{Cut}(P_1)$$

6. r or r' is an unfolding rule applying to another proposition than P. This case can in fact be handled as case 3.
7. r is an unfolding rule and r' is a logical rule, both applying to P. This case cannot occur, because only atomic propositions are unfolded, so that no logical rule can be applied to P.
8. r is a logical rule and r' is an unfolding rule, both applying to P. This case is handled as case 7.
9. r and r' are both unfolding rules applying to P. Therefore P has to be atomic, and is rewritten by $B \to^- P_1$ to the left and $C \to^+ P_2$ to the right. If both of this rewriting are term rewriting, then, because of confluence of $R_{\mathcal{T}(\Sigma,V)}$, we know that there is some P' such that $P_1 \underset{R_{\mathcal{T}(\Sigma,V)}}{\overset{*}{\longrightarrow}} P' \underset{R_{\mathcal{T}(\Sigma,V)}}{\overset{*}{\longleftarrow}} P_2$. The proof

$$\dfrac{\begin{array}{c}\pi_1\\ \vdots\\ \Gamma, P_1 \vdash \Delta\end{array} \quad \dfrac{\dfrac{\dfrac{}{\Gamma, P' \vdash P', \Delta}\,\mathsf{Axiom}}{\Gamma, P_2 \vdash P_1, \Delta}\,\mathsf{Unfolding\ Rules} \quad \begin{array}{c}\varpi_1'\\ \vdots\\ \Gamma \vdash P_1, P_2, \Delta\end{array}}{\Gamma \vdash P_1, \Delta}\,\mathsf{Cut}(P_2)}{\Gamma \vdash \Delta}\,\mathsf{Cut}(P_1)$$

is smaller than the initial proof (remind that the term rewrite relation is by definition included in the subformula relation), contradicting its minimality. Otherwise, we are exactly in the case stated in the theorem.

□

NOTE. If we suppose, as in the order condition of Hermant [33], that the proposition rewrite system is confluent, and that it is included in an well-founded ordering compatible with the subformula relation, then we can take this ordering instead of the subformula relation to compare Cuts in the precedence. Doing this, we can prove that there are no minimal proofs of this form, and consequently *no critical proofs*. Therefore the admissibility of Cut is verified, as a by-product of the completion procedure.

The main difference with Hermant [33] is that he gives a semantic proof of the admissibility of Cut, whereas we have here a Cut elimination algorithm, i.e. a terminating syntactical process that transforms a proof into a Cut-free one. It is proved by Dowek and Werner [34] that such an order condition provides normalization.

The fact that the compatibility of the rewrite system with the subformulæ relation implies the Cut-admissibility was also independently found by Aiguier, Boin, and Longuet [35], with the same kind of ordering over proofs.

Theorem 40 (Undecidability of Critical Proof Search). *The problem*

> *Input: A propositional rewrite system R and a sequent $\Gamma \vdash \Delta$.*
>
> *Decide if $\Gamma \vdash \Delta$ is the conclusion of a critical proof in R.*

is undecidable.

Proof. We reduce to the problem of validity in first-order logic.

Let P be a first-order proposition.

Let A, B be atomic propositions not appearing in P. Consider the following propositional rewrite system:

$$\begin{cases} A \to^- B \\ A \to^+ P \end{cases} .$$

We can check that $\vdash B$ is the conclusion of a critical proof in it if and only if P is valid.

Indeed, a critical proof is necessarily of the form

$$\dfrac{\dfrac{\dfrac{}{A, B \vdash B}\ \mathsf{Axiom}}{A \vdash B}\ \uparrow\text{-l} \qquad \dfrac{\begin{array}{c}\text{Proof of } P \text{ with no } \uparrow\text{-l nor } \uparrow\text{-r} \\ \vdots \\ \vdash P, A, B\end{array}}{\vdash A, B}\ \uparrow\text{-r}}{\vdash B}\ \mathsf{Cut}(A)$$

□

Of course, in the quantifier-free case, this problem is decidable. It remains to be investigated for what fragments of first-order logic it is decidable, in particular if these fragments are the same that for the validity problem.

5.3.2. The Completion Procedure

As we wrote in Section 5.1, we want to define a completing deduction mechanism by adding to a presentation A a presentation $\mathsf{C}(A)$ such that $Comp(A) \subseteq \mathsf{C}(A) \subseteq Th\, A$.

Here, using Property 17(c), we know that for all proofs p whose first component is a proof π of a sequent $\Gamma \vdash \Delta$ there exists a Cut-free proof of the sequent $\vdash \mathcal{P}(\Gamma \vdash \Delta)$ in $Rew(\Gamma \vdash \Delta)$. Using Lemma 3 we obtain a Cut-free proof π of $\Gamma \vdash \Delta$ in $Rew(\Gamma \vdash \Delta)$. If the proof p is critical, π has a Cut at its root and thus it is greater than π', so that we can use this particular π' in the definition of $Comp$. Note that if p is critical, so are the proofs with the same first component π but another conclusion (that is, another rule in $Rew(\Gamma \vdash \Delta)$). We therefore have to add the premises of π', but these premises are in fact in $Rew(\Gamma \vdash \Delta)$,

and we obtain all $Rew(\Gamma \vdash \Delta)$ by considering the conclusion of all the critical proofs whose first component is π:

$$Comp(A) \quad \stackrel{!}{=} \quad \bigcup_{p \in Crit(A)} [p]_{Cl} \ .$$

The best procedure is thus to add only the conclusions of critical proofs. Nevertheless, searching for these conclusions is undecidable, so that we must use a superset of them. Here we will add the conclusion of the proofs in the form of Proposition 39. (Note that this proposition is only a necessary condition for being critical.)

We must consider proofs of the form of Proposition 39. As π and π' are Cut-free and do not use unneeded logical rules, they could be found using for instance a tableau method modulo, like TaMed [7, 10], which is complete with respect to Cut-free proofs, if we knew Γ and Δ. The idea is therefore to apply a tableau method for the deduction modulo on $A, P \vdash$ and $\vdash A, Q$ until they are either proved or the method terminates, and to complete the sequents to close all branches. Of course, the tableau method may not terminate, in which case we have to arbitrarily decide to stop it. If we stop it too early, then maybe there remains some open branch that could be closed, and therefore Γ and Δ in the critical-proof candidate will not be minimal. This is not a problem because the generated rewrite rules for this will be more general than the one for the real critical proof. However, the longer the tableau method runs, the more accurate the additional rules will be.

Then, we have to close all remaining open branches by adding some propositions in Γ and Δ. We know we do not need to add A. The formulæ in Γ and Δ can be non-atomic formulæ, in which case they could be further decomposed by the tableau method. However, if we use a tableau method with meta-variables (see [36]), the order in which formulas are decomposed in no longer relevant, only the unification of meta-variables is, so that they could have occurred before the decomposition of $A, P \vdash$ or $\vdash A, Q$. As Axioms are applied only to atomic propositions, we only need to consider such cases to close the branches, and then, we may need to recompose the atomic formulæ added to the branches to get the actual Γ and Δ. In particular, if we added some atomic formula in which there is a variable which was introduced in the proof by some $\exists$-l or $\forall$-r (an Eigenvariable)[5], then it cannot appear in $\Gamma \cup \Delta$. It therefore has to be introduced using a quantification. For instance, if we wanted to add $B(x)$ in Γ and x is such an Eigenvariable, we have to add $\forall x.\ B(x)$ instead. We need to do so for all possible choices of atomic propositions different from A to close the branches, and *a priori* for all choices of recompositions. We would obtain that way all possible conclusions $\Gamma \vdash \Delta$ of proofs of the form of Proposition 39, and $C(A)$ would be the union of $Rew(\Gamma \vdash \Delta)$ for each of them. However, it seems that we only need to recompose the formulæ to add the quantifications

[5] Working using meta-variables, this would mean that the formula contains a Skolem symbol.

protecting the Eigenvariables. Indeed, by applying other recompositions, we obtain sequents $\Gamma \vdash \Delta$ whose rules in $Rew(\Gamma \vdash \Delta)$ are redundant w.r.t. the rules obtained without the recomposition — this is due to the fact that Rew is working by decomposing the formulæ in the sequent.

We repeatedly complete the rewrite system until a fixpoint is reached. The limit admits Cut.

Theorem 41 (Cut Admissibility of the Limit). *For all sequents $\Gamma \vdash \Delta$, for all proposition rewrite systems R_0, $\Gamma \vdash \Delta$ has a proof in R_0 if and only if it has a* Cut*-free proof in R_∞.*

Proof. By Proposition 32, we know that our deduction mechanism is completing, and therefore by Theorem 30

$$Th\, R_0 \subseteq [Pf(R_\infty) \cap Nf(R_0)]_{Cl} \ . \tag{1}$$

The "if" part comes from the fact that we only add rules that corresponds to sequents provable in R_0. For the "only if", suppose that $\Gamma \vdash \Delta$ has a proof in R_0, then using (1) there exists a proof p_a of conclusion a in $Pf(R_\infty) \cap Nf(R_0)$ for all rules $a \in Rew(\Gamma \vdash \Delta)$. If p_a is trivial, then we can use Property 17(c) to find a Cut-free proof with the same conclusion, otherwise Proposition 38 shows that p_a is Cut-free. We can therefore conclude with Property 19. □

6. Examples

In the case of Crabbé's example presented in the introduction, the input is the rewrite system $\{A \to^+ B \wedge \neg A; A \to^- B \wedge \neg A\}$ and the completion procedure generates $B \to^- \bot$.

With this new rule, we can show that there are no more critical proofs. The proposition rewrite system

$$\begin{cases} A \to B \wedge \neg A \\ B \to \bot \end{cases}$$

admits Cut.

The next example deals with quantifiers and is extracted from Hermant [33]:

$$r \in r \ \to \ \forall y.\ y \simeq r \Rightarrow y \in r \Rightarrow C$$

where $y \simeq z \quad \stackrel{!}{=} \quad \forall x.\ (y \in x \Rightarrow z \in x)$. It is terminating and confluent, but does not admits Cut.

The critical proofs have the form

$$\dfrac{\dfrac{\dfrac{\vdots}{r \in r, \forall y.\ y \simeq r \Rightarrow y \in r \Rightarrow C \vdash}}{r \in r \vdash} \uparrow\text{-l} \qquad \dfrac{\dfrac{\vdots}{\vdash r \in r, \forall y.\ y \simeq r \Rightarrow y \in r \Rightarrow C}}{\vdash r \in r} \uparrow\text{-l}}{\vdash} \ \mathsf{Cut}(r \in r)$$

The left part can be developed as

$$\dfrac{\dfrac{\dfrac{r \in r, C \vdash \quad r \in r \vdash t_1 \in r}{r \in r, t_1 \in r \Rightarrow C \vdash}\ \Rightarrow\text{-l} \qquad \dfrac{\dfrac{r \in r, t_1 \in z \vdash r \in z}{r \in r \vdash t_1 \in z \Rightarrow r \in z}\ \Rightarrow\text{-r}}{r \in r \vdash t_1 \simeq r}\ \forall\text{-r}}{r \in r, t_1 \simeq r \Rightarrow t_1 \in r \Rightarrow C \vdash}\ \Rightarrow\text{-l}}{r \in r, \forall y.\ y \simeq r \Rightarrow y \in r \Rightarrow C \vdash}\ \forall\text{-l}$$

and the right part as

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{r \in t_0, z \in r \vdash r \in r, C \quad z \in r \vdash z \in t_0, r \in r, C}{z \in t_0 \Rightarrow r \in t_0, z \in r \vdash r \in r, C}\ \Rightarrow\text{-l}}{z \simeq r, z \in r \vdash r \in r, C}\ \forall\text{-l}}{z \simeq r \vdash r \in r, z \in r \Rightarrow C}\ \Rightarrow\text{-r}}{\vdash r \in r, z \simeq r \Rightarrow z \in r \Rightarrow C}\ \Rightarrow\text{-r}}{\vdash r \in r, \forall y.\ y \simeq r \Rightarrow y \in r \Rightarrow C}\ \forall\text{-r}$$

.

To close the proofs, we can for instance have $t_0 = r = t_1$, and C in the right part of the sequent (to close $r \in r, C \vdash$). One can see that other choices will not produce critical proofs. The resulting sequent is therefore $\vdash C$, and the added rule is $C \rightarrow^+ \top$. This rule does not generate new critical proofs, and consequently, the proposition rewrite system

$$\begin{cases} r \in r \ \rightarrow^+ \ \forall y.\ y \simeq r \Rightarrow y \in r \Rightarrow C \\ r \in r \ \rightarrow^- \ \forall y.\ y \simeq r \Rightarrow y \in r \Rightarrow C \\ C \rightarrow^+ \top \end{cases}$$

admits Cut.

One can also think of another example, where there remains quantifiers in the conclusion: one can replace B by $\exists x.\ \forall y.\ B \wedge C(x, y)$ in Crabbé's example to get the rule: $A \rightarrow (\exists x.\ \forall y.\ B \wedge C(x, y)) \wedge \neg A$ where A and B are atomic propositions, and C a predicate of arity 2.

We first search for a proof of $A, (\exists x.\ \forall y.\ B \wedge C(x, y)) \wedge \neg A \vdash$, and we get

$$\dfrac{\dfrac{\dfrac{}{A, (\exists x.\ \forall y.\ B \wedge C(x, y)) \vdash A}\ \mathsf{Axiom}(A)}{A, (\exists x.\ \forall y.\ B \wedge C(x, y)), \neg A \vdash}\ \neg\text{-l}}{A, (\exists x.\ \forall y.\ B \wedge C(x, y)) \wedge \neg A \vdash}\ \wedge\text{-l}$$

We try do the same for the right part

$$\dfrac{\dfrac{\dfrac{\vdash \exists x.\ \forall y.\ B \wedge C(x, y), B, A \quad \vdash \exists x.\ \forall y.\ B \wedge C(x, y), C(x, y), A}{\vdash \exists x.\ \forall y.\ B \wedge C(x, y), B \wedge C(x, y), A}\ \wedge\text{-r}}{\vdash \exists x.\ \forall y.\ B \wedge C(x, y), \forall y.\ B \wedge C(x, y), A}\ \forall\text{-r}}{\vdash \exists x.\ \forall y.\ B \wedge C(x, y), A}\ \exists\text{-r} \qquad \dfrac{\dfrac{}{A \vdash A}\ \mathsf{Axiom}(A)}{\vdash \neg A, A}\ \neg\text{-r}}{\vdash (\exists x.\ \forall y.\ B \wedge C(x, y)) \wedge \neg A, A}\ \wedge\text{-r}$$

$A \to (\exists x.\ \forall y.\ B \wedge C(x,y)) \wedge \neg A$ has already been applied in the right part of the sequent, so it is not useful to do it again, and so we cannot close the derivation. We see that we have to add propositions in the context to close the remaining branches. As we do not add A, and Axiom is only applied to atomic propositions, there remains only the choice to add B in Γ for the left branch and $C(x,y)$ in Γ for the right branch. However, in $C(x,y)$, the variable y is an Eigenvariable, so we need in fact to add $\forall y.\ C(x,y)$. Finally, the conclusion of the critical proof is $B, \forall y.\ C(x,y) \vdash$ which gives for instance the rewrite rule $B \to^- \forall x.\ \neg\forall y.\ C(x,y)$. With this new rule, there are no longer critical proofs. In particular we have the following Cut-free proof of $\exists x.\ \forall y.\ B \wedge C(x,y) \vdash$, corresponding to the conclusion $B \vdash$ of the critical proof in the original Crabbé system:

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{}{\forall y.\ B \wedge C(x,y), C(x,y_0), B, \forall x.\ \neg\forall y.\ C(x,y), C(x,y) \vdash C(x,y_0)}\,\text{Axiom}}{\forall y.\ B \wedge C(x,y), B \wedge C(x,y_0), B, \forall x.\ \neg\forall y.\ C(x,y), C(x,y) \vdash C(x,y_0)}\,\wedge\text{-l}}{\forall y.\ B \wedge C(x,y), B, \forall x.\ \neg\forall y.\ C(x,y), C(x,y) \vdash C(x,y_0)}\,\forall\text{-l}}{\forall y.\ B \wedge C(x,y), B, \forall x.\ \neg\forall y.\ C(x,y), C(x,y) \vdash \forall y.\ C(x,y)}\,\forall\text{-r}}{\forall y.\ B \wedge C(x,y), B, \forall x.\ \neg\forall y.\ C(x,y), \neg\forall y.\ C(x,y), C(x,y) \vdash}\,\neg\text{-l}}{\forall y.\ B \wedge C(x,y), B, \forall x.\ \neg\forall y.\ C(x,y), C(x,y) \vdash}\,\forall\text{-l}}{\forall y.\ B \wedge C(x,y), B, C(x,y) \vdash}\,\uparrow\text{-l}}{\forall y.\ B \wedge C(x,y), B \wedge C(x,y) \vdash}\,\wedge\text{-l}}{\forall y.\ B \wedge C(x,y) \vdash}\,\forall\text{-l}}{\exists x.\ \forall y.\ B \wedge C(x,y) \vdash}\,\exists\text{-l}$$

In these three examples, only one step was needed to produce a complete system. But the system

$$R = \begin{cases} A \to^- B \\ A \to^+ C \\ D \to^- B \\ D \to^+ E \end{cases}$$

may need two steps to produce the completed system

$$R \ \cup \ \begin{cases} B \to^- C \\ B \to^+ E \\ C \to^+ E \end{cases} .$$

Indeed, the first two rules of R create the critical proof

$$\dfrac{\dfrac{\dfrac{}{B, A, C \vdash C}\,\text{Axiom}}{B, A \vdash C}\,\uparrow\text{-l} \qquad \dfrac{\dfrac{}{B \vdash A, B, C}\,\text{Axiom}}{B \vdash A, C}\,\uparrow\text{-r}}{B \vdash C}\,\text{Cut}(A)$$

that leads for instance to the rewrite rule $B \to^- C$. Similarly the two other rules may complete the system by the rewrite rule $B \to^+ E$. Consequently,

after one step the system has a critical proof

$$\dfrac{\dfrac{\dfrac{}{E, B, C \vdash C}\ \mathsf{Axiom}}{E, B \vdash C}\ \uparrow\text{-}\mathsf{l} \qquad \dfrac{\dfrac{}{E \vdash B, E, C}\ \mathsf{Axiom}}{E \vdash B, C}\ \uparrow\text{-}\mathsf{r}}{E \vdash C}\ \mathsf{Cut}(B)$$

and may be completed by the rewrite rule $C \to^{+} E$.

We nevertheless conjecture that if the initial proposition rewrite system is confluent, the completion procedure is terminating, possibly in one step.

7. Conclusion and Perspectives

This paper reveals a deep logical correspondence between the sequent calculus, proof orderings and completion. We have first shown the boundaries of the research for an optimal criterion which ensures the Cut admissibility of a rewrite system by proving its undecidability in general. Then, we have proposed how to circumvent this issue by transforming the rewrite systems we are working with into an equivalent one which admits Cut. This is done by setting the right abstract canonical system structure on the proof space of the unfolding sequent calculus modulo, which is equivalent to the asymmetric sequent calculus modulo, in particular concerning Cut admissibility. This permits to use abstract completion to recover the admissibility of Cut. This abstract completion is precise enough to be operational, and it is actually implemented, based on a prototype of the tableau method modulo TaMed [10], and coded in the language TOM+OCaml [`http://tom.loria.fr/`, `http://caml.inria.fr/ocaml/index.en.html`]. The implementation is available on the SVN distribution of TOM (see `http://gforge.inria.fr/scm/?group_id=78`) in the directory `trunk/jtom/application/completion`. Note that because the implemented tableau method is for non-polarized deduction modulo, the completion procedure adds non-polarized rewrite rules thanks to the translation $\cdot^{\mp}$ given in Section 2.2 before Proposition 9.

All this opens many questions that we are now considering.

The limit of the completion procedure admits Cut in the polarized sequent calculus, and therefore we can translate it by Corollary 8 and Proposition 9 into a non-polarized rewrite system that admits Cut in the asymmetric sequent calculus modulo. However, this system may be non-confluent, so we do not know if it admits Cut in the original version of the sequent calculus modulo of Dowek et al. [4]. However, if we begin with a confluent rewrite system R_0, then the original sequent calculus modulo R_0 is equivalent to the asymmetric sequent calculus modulo $R_\infty^{\mp}$ without Cut. This is exactly what we wanted, since the asymmetric sequent calculus modulo without Cut is analytic, in the sense that rewriting is oriented from the bottom to the top of proofs, which induces that the asymmetric sequent calculus modulo is well adapted for proof search. The usual restriction of deduction modulo to confluent rewrite system was mainly imposed to be able to check the congruence using only rewritings, and is no

longer needed as far as we know that the final system prove the same that the original one.

The ordering on proofs we are using is adapted to consider Cut admissibility as a normal-form property of an ACS, but produces too many critical proofs, in particular when quantifiers are involved, because some of the rules produced by the completion procedure subsumes other ones. (For instance $A \to^+ \exists x.\ P(x)$ subsumes $A \to^+ P(t)$ for a particular $t \in \mathcal{T}(\Sigma, V)$.) This ordering has therefore to be refined in order to restrict oneself to the more relevant critical proofs.

Furthermore, our procedure can be used to determine if a system admits Cut. Indeed, if a proposition rewrite system is a fixpoint of this procedure, then we know that it admits Cut. Nevertheless, the converse is not true, essentially because we have to use a superset of the critical proofs. It will be interesting to check what results this procedure will give on system that are proved to admits Cut, like Higher Order Logic [37] or arithmetic [38], or for systems for which the admissibility of Cut is unknown yet, such as Pure Type Systems [39].

Indeed, we have shown that the *Rew* algorithm provides a constructive way to transform a first-order theory into a proposition rewrite system. Up to efficiency questions, this closes the problem of transforming proofs in a theory into proofs modulo, i.e. to replace deduction steps by computational ones. What remains still open and challenging is to understand how to systematically build first-order theories out of general ones (e.g. HOL or arithmetic) and how to balance the amount of computations on term versus the one on propositions.

Moreover, our procedure only guarantees the admissibility of Cut, and does not provide a Cut elimination procedure. In other words, we do not have a process that transform proofs with Cuts to Cut-free ones, so that we have to build the Cut-free proofs from scratch. In particular, for the completed system, normalization may not hold. For instance, with Crabbé's rule, once the system is completed, the initial proof of $B \vdash$ can still be constructed, and it is still not normalizing, i.e. the λ-term that is associated to the proof can be infinitely β-reduced. We can notice that, even if Cut is admissible, the proof of Proposition 39 does not give a cut elimination procedure: we know that there are no critical proofs, but we do not know how to transform a proof in the form of Proposition 39 into a smaller one (without building a Cut-free proof from scratch). We probably have to introduce some simplification rules in order to suppress the possibility to build non-normalizing proofs. For instance, in our example, we could simplify $A \to B \wedge \neg A$ into $A \to \bot \wedge \neg A$ using $B \to \bot$, and then simplify it to $A \to \bot$, the system $\{A \to \bot\ ;\ B \to \bot\}$ being normalizing. Besides, with such simplification rules, we may obtain the canonical presentation of the system.

Lastly, it will be interesting to understand how the results presented here can be transferred to intuitionistic logic. In particular, the impossibility to build a *Rew* function without breaking the witness property shows that it is not trivial. We tackle this issue in [26].

Acknowledgements. We had many fruitful discussions with Nachum Dershowitz and Gilles Dowek on the topics of this paper. Many thanks also to the anony-

mous referees for their careful reading and clever suggestions.

References

[1] G. Gonthier, A computer-checked proof of the Four Colour Theorem, unpublished, available at `http://research.microsoft.com/~gonthier/4colproof.pdf`, 2005.

[2] B. Chetali, A world-first smart card CC certificate with formal assurances, presented at the Third Franco-Japanese Computer Security Workshop. Nancy, France, 2008.

[3] B. Chetali, Q. H. Nguyen, Industrial Use of Formal Methods for a High-Level Security Evaluation, in: J. Cuéllar, T. S. E. Maibaum, K. Sere (Eds.), FM, vol. 5014 of *LNCS*, Springer, ISBN 978-3-540-68235-6, 198–213, 2008.

[4] G. Dowek, T. Hardin, C. Kirchner, Theorem Proving Modulo, Journal of Automated Reasoning 31 (1) (2003) 33–72.

[5] G. Peterson, M. E. Stickel, Complete Sets of Reductions for Some Equational Theories, Journal of the ACM 28 (1981) 233–264.

[6] H. Barendregt, E. Barendsen, Autarkic Computations in Formal Proofs, Journal of Automated Reasoning 28 (3) (2002) 321–336.

[7] R. Bonichon, TaMeD: A Tableau Method for Deduction Modulo., in: D. A. Basin, M. Rusinowitch (Eds.), IJCAR, vol. 3097 of *LNCS*, Springer, 445–459, 2004.

[8] G. Burel, Unbounded Proof-Length Speed-up in Deduction Modulo, in: J. Duparc, T. A. Henziger (Eds.), CSL 2007, vol. 4646 of *LNCS*, Springer, 496–511, 2007.

[9] M. Crabbé, Non-normalisation de la théorie de Zermelo, manuscript, 1974.

[10] R. Bonichon, O. Hermant, A Semantic Completeness Proof for TaMed, in: M. Hermann, A. Voronkov (Eds.), LPAR, vol. 4246 of *LNCS*, Springer, 167–181, 2006.

[11] O. Hermant, Méthodes Sémantiques en Déduction Modulo, Ph.D. thesis, École Polytechnique, 2005.

[12] G. Dowek, Polarized resolution modulo, manuscript, 2009.

[13] G. Dowek, Confluence as a Cut Elimination Property., in: R. Nieuwenhuis (Ed.), RTA, vol. 2706 of *LNCS*, Springer, 2–13, 2003.

[14] D. E. Knuth, P. B. Bendix, Simple word problems in universal algebras, in: J. Leech (Ed.), Computational Problems in Abstract Algebra, Pergamon Press, Oxford, 263–297, 1970.

[15] G. Dowek, What Is a Theory?, in: H. Alt, A. Ferreira (Eds.), STACS, vol. 2285 of *LNCS*, Springer, 50–64, 2002.

[16] N. Dershowitz, C. Kirchner, Abstract Canonical Presentations, Theoretical Computer Science 357 (2006) 53–69.

[17] M. P. Bonacina, N. Dershowitz, Abstract canonical inference, ACM Trans. Comput. Logic 8 (1).

[18] N. Dershowitz, Canonicity, in: I. Dahn, L. Vigneron (Eds.), FTP, vol. 86 of *Electronic Notes in Theoretical Computer Science*, Elsevier Science Publishers B. V. (North-Holland), 147–158, 2003.

[19] G. Burel, C. Kirchner, Completion Is an Instance of Abstract Canonical System Inference, in: K. Futatsugi, et al. (Eds.), Algebra, Meaning and Computation, vol. 4060 of *LNCS*, Springer, 497–520, 2006.

[20] G. Burel, C. Kirchner, Cut Elimination in Deduction Modulo by Abstract Completion, in: S. Artemov, A. Nerode (Eds.), LFCS, LNCS, Springer, 115–131, 2007.

[21] F. Baader, T. Nipkow, Term *Re*writing and *all That*, Cambridge University Press, 1998.

[22] G. Gentzen, Untersuchungen über das logische Schliessen, Mathematische Zeitschrift 39 (1934) 176–210, 405–431, translated in Szabo, editor., *The Collected Papers of Gerhard Gentzen* as "Investigations into Logical Deduction".

[23] J. H. Gallier, Logic for Computer Science: Foundations of Automatic Theorem Proving, vol. 5 of *Computer Science and Technology Series*, Harper & Row, New York, revised On-Line Version (2003), `http://www.cis.upenn.edu/~jean/gbooks/logic.html`, 1986.

[24] S. C. Kleene, Mathematical Logic, John Wiley, New York, USA, 1967.

[25] G. Dowek, About folding-unfolding cuts and cuts modulo, Journal of Logic and Computation 11 (3) (2001) 419–429.

[26] G. Burel, Automating Theories in Intuitionistic Logic, in: S. Ghilardi, R. Sebastiani (Eds.), FroCoS, Lecture Notes in Artificial Intelligence, Springer, 181–197, 2009.

[27] O. Hermant, A Model-based Cut Elimination Proof, in: 2nd St-Petersburg Days of Logic and Computability, 2003.

[28] J. Barwise (Ed.), Handbook of Mathematical Logic, Elsevier Science Publishers B. V. (North-Holland), 4th printing edn., 1985.

[29] J. Endrullis, H. Geuvers, H. Zantema, Degrees of Undecidability in Term Rewriting, in: E. Grädel, R. Kahle (Eds.), CSL, vol. 5771 of *Lecture Notes in Computer Science*, Springer, 255–270, 2009.

[30] N. Dershowitz, C. Kirchner, Abstract Saturation-Based Inference, in: LICS, IEEE Computer Society, 65–74, 2003.

[31] N. Dershowitz, Orderings for Term-Rewriting Systems, Theoretical Computer Science 17 (1982) 279–301.

[32] J.-Y. Girard, Y. Lafont, P. Taylor, Proofs and Types, vol. 7 of *Cambridge Tracts in Theoretical Computer Science*, Cambridge University Press, 1989.

[33] O. Hermant, Semantic Cut Elimination in the Intuitionistic Sequent Calculus., in: P. Urzyczyn (Ed.), TLCA, vol. 3461 of *LNCS*, Springer, 221–233, 2005.

[34] G. Dowek, B. Werner, Proof Normalization Modulo, The Journal of Symbolic Logic 68 (4) (2003) 1289–1316.

[35] M. Aiguier, C. Boin, D. Longuet, On Generalized Theorems for Normalization of Proofs, Tech. Rep., LaMI - CNRS and Université d'Evry Val d'Essonne, 2005.

[36] M. Fitting, First-order logic and automated theorem proving (2nd ed.), Springer, Secaucus, NJ, USA, ISBN 0-387-94593-8, 1996.

[37] G. Dowek, T. Hardin, C. Kirchner, HOL-$\lambda\sigma$ an intentional first-order expression of higher-order logic, Mathematical Structures in Computer Science 11 (1) (2001) 1–25.

[38] G. Dowek, B. Werner, Arithmetic as a Theory Modulo, in: J. Giesl (Ed.), RTA, vol. 3467 of *LNCS*, Springer, 423–437, 2005.

[39] G. Burel, A First-Order Representation of Pure Type Systems using Superdeduction, in: F. Pfenning (Ed.), LICS, IEEE Computer Society, 253–263, 2008.