



HAL
open science

Cut Elimination in Deduction Modulo by Abstract Completion (Full Version)

Guillaume Burel, Claude Kirchner

► **To cite this version:**

Guillaume Burel, Claude Kirchner. Cut Elimination in Deduction Modulo by Abstract Completion (Full Version). [Research Report] 2007, pp.16. inria-00132964v1

HAL Id: inria-00132964

<https://inria.hal.science/inria-00132964v1>

Submitted on 23 Feb 2007 (v1), last revised 18 Nov 2009 (v2)

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.

Cut Elimination in Deduction Modulo by Abstract Completion (Full Version)

Guillaume Burel

Claude Kirchner

February 23, 2007

Abstract

Deduction Modulo implements Poincaré’s principle by identifying deduction and computation as different paradigms and making their interaction possible. This leads to logical systems like the sequent calculus or natural deduction modulo. Even if deduction modulo is logically equivalent to first-order logic, proofs in such systems are quite different and dramatically simpler with one cost: cut elimination may not hold anymore. We prove first that it is even undecidable to know, given a congruence over propositions, if cuts can be eliminated in the sequent calculus modulo this congruence.

Second, to recover the cut admissibility, we show how computation rules can be added following the classical idea of completion *a la* Knuth and Bendix. Because in deduction modulo, rewriting acts on terms as well as on propositions, the objects are much more elaborated than for standard completion. Under appropriate hypothesis, we prove that the sequent calculus modulo is an instance of the powerful framework of *abstract canonical systems* and that therefore, cuts correspond to critical proofs that abstract completion allows us to eliminate.

In addition to an original and deep understanding of the interactions between deduction and computation and of the expressivity of abstract canonical systems, this provides a mechanical way to transform a sequent calculus modulo into an equivalent one admitting the cut rule, therefore extending in a significant way the applicability of mechanized proof search in deduction modulo.

Keywords: Automated deduction and interactive theorem proving, Knuth-Bendix completion, critical proofs, cut elimination, deduction modulo, proof ordering

1 Introduction

The complementarity and interaction between computation and deduction is known since at least Henri Poincaré and deduction modulo (Dowek, Hardin, and Kirchner, 2003) is a way to present first-order logic taking advantage from this complementarity. Deduction modulo is at the heart of proof assistants and proof search methods, either implicitly or explicitly (see for instance Peterson and Stickel, 1981; Barendregt and Barendsen, 2002; Dowek et al., 2003; Bonichon, 2004) 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 often better represented by a rewrite relation over first-order terms and propositions, leading to the asymmetric sequent calculus (Dowek, 2003).

In the sequent calculus modulo, the Hauptsatz, *i.e.*

the fact that cuts are not needed to build proofs, is no longer true as one can see from an example derived from Crabbé’s proof of the non-normalization of Zermelo’s theory (1974) (see for instance Dowek et al., 2003). But we know that the admissibility of the cut rule is fundamental for at least two related reasons: first, if a system admits it, then the formulæ needed to build a sequent calculus proof of some sequent are subformulæ¹ of the ones appearing in it, so that the search space is, in a sense, limited. Such proofs are sometimes called *analytic* (Dowek, 2003). The tableaux method is based on this fact, and for instance TaMeD (Bonichon, 2004), a tableaux method based on deduction modulo, is shown to be complete only for cut-free systems. On the other hand, it has been shown by Hermant (2005a) that a proof search method for deduction modulo like ENAR (Dowek et al., 2003)—which generalizes resolution and narrowing—is equivalent to the cut-free fragment of deduction modulo. ENAR is therefore complete if and only if the cut rule is admissible.

So on the one hand, we like to have a powerful con-

¹In the case of deduction modulo, the intuitive notion of subformula must take the considered rewrite relation into account.

gruence but this may be at the price of loosing cut admissibility. How can we get both? It has been shown by Dowek (2003) that cut admissibility is equivalent to the confluence of the rewrite system, provided only first-order terms are rewritten. It is no longer true when *propositions* are also rewritten, and the cut admissibility property is in that case a stronger notion than confluence. Gilles 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 has the cut-elimination property. Such a completion procedure was proposed for the quantifier free case by Dowek (2002), 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 (2006); Bonacina and Dershowitz (2007). 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 adapted to existing completion procedures such as ground completion Dershowitz (2003) and standard (a.k.a. Knuth-Bendix Knuth and Bendix (1970)) completion Burel and Kirchner (2006).

To present the general idea of our approach, let us consider the simple example of Crabbé's axiom (1974) $A \Leftrightarrow B \wedge \neg A^2$. Can we find, for the sequent calculus modulo the associated rewrite system $A \rightarrow B \wedge \neg A$, a provable sequent without any cut-free proof? Indeed, let us try to build a minimal example. We will show in Prop. 9 that such a proof, in its simplest form, is necessarily of the shape:

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

where the rules labeled “ $\uparrow\text{-r}$ ” and “ $\uparrow\text{-l}$ ” allow to apply 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.

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

$$\frac{\frac{\frac{\overline{A, B \vdash A} \text{Ax}}{A, B, \neg A \vdash} \neg\text{-l}}{A, B \wedge \neg A \vdash} \wedge\text{-l}}{\vdash}$$

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

$$\frac{\frac{\frac{\overline{A \vdash A} \text{Ax}}{\vdash B, A \quad \vdash \neg A, A} \neg\text{-r}}{\vdash B \wedge \neg A, A} \wedge\text{-r}}{\vdash}$$

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:

$$\frac{\frac{\frac{\overline{A, B \vdash A} \text{Ax}}{A, B, \neg A \vdash} \neg\text{-l} \quad \frac{\frac{\overline{B, A \vdash A} \text{Ax}}{B \vdash \neg A, A} \neg\text{-r}}{B \vdash B \wedge \neg A, A} \wedge\text{-l}}{\frac{B, A \vdash \quad \vdash B \wedge \neg A, A} \uparrow\text{-l}}{B \vdash A} \uparrow\text{-r}}{\text{Cut}(A)} B \vdash$$

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 $B \rightarrow \perp$.

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

$$\left\{ \begin{array}{l} A \rightarrow B \wedge \neg A \\ B \rightarrow \perp \end{array} \right.$$

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 provide an appropriate Noetherian ordering on the proofs of the sequent calculus modulo a rewrite system; This ordering allows us to set on the proof space of sequent calculus modulo a structure of abstract canonical system;
- We characterize the critical proofs in deduction modulo as simple cuts;
- By an appropriate correspondence between sequents and rewrite systems, we establish a precise correspondence between the limit of a completion process and a cut free sequent calculus;
- We show the applicability of the general results, in particular on sequent calculus modulo rewrite systems involving quantifiers, therefore generalizing all previously known results;

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

The next section will present the minimal knowledge needed on deduction modulo and abstract canonical systems to make the paper self-contained, and gives a proof of the undecidability of the cut admissibility in deduction modulo. In Sect. 3, we show how to set, on the proof space of sequent calculus modulo, a structure of abstract canonical system. In particular we make precise why the postulates of ACS are fulfilled. This allows us in Sect. 4 to characterize the critical proofs of deduction modulo and to set-up the completion process as the appropriate (and indeed

²In 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.

non-trivial) instance of the abstract completion process. We also provide an algorithm to systematically transform a set of sequents into an appropriate set of proposition rewrite rule, therefore making the whole framework operational. We conclude after presenting in more details Crabbé's example as well as several examples involving quantifiers.

2 Prerequisites

2.1 Rewritings

We define here how propositions are rewritten in deduction modulo.

We denote by $\mathcal{T}(\Sigma, V)$ the set of *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 $t_1, \dots, t_n \in \mathcal{T}(\Sigma, V)$. It is denoted $A(t_1, \dots, t_n)$. *Propositions* can be built using the following grammar³:

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

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 $P_1 \wedge \dots \wedge P_n$, and $\bigvee \Gamma$ for $P_1 \vee \dots \vee P_n$ if $\Gamma = P_1, \dots, P_n$. Free variables 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 *term rewrite rule* is the pair of terms l, r such that all free variables of r appear in l . It is denoted $l \rightarrow r$. 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 $l \rightarrow r$ if there exists some substitution σ and some position \mathbf{p} in s such that $\sigma l = s|_{\mathbf{p}}$ and $t = s[\sigma r]_{\mathbf{p}}$.

An atomic proposition $A(s_1, \dots, s_i, \dots, s_n)$ can be rewritten to the atomic proposition $A(s_1, \dots, t_i, \dots, s_n)$ by a term rewrite rule $l \rightarrow r$ if s_i can be rewritten to t_i by $l \rightarrow r$.

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 $A \rightarrow P$. A *proposition rewrite system* is a set of proposition rewrite rules. The set of all proposition rewrite systems is denoted \mathcal{PRS} .

An atomic proposition A can be rewritten to a proposition P by a proposition rewrite rule $B \rightarrow Q$ if there exists some substitution σ such that $\sigma B = A$ and $\sigma Q = P$. Semantically, this proposition rewrite relation must be seen as a logical equivalence between propositions.

Note that we do not define how to rewrite non-atomic propositions by proposition rewrite rules, as in Dowek et al. (2003), because this can be simulated in the sequent calculus modulo we present in the next section.

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*. It will be denoted $R_{\mathcal{T}(\Sigma, V)}$.

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

- $P \succ P_i$ 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 can be rewritten to Q by $R_{\mathcal{T}(\Sigma, V)}$

for all terms t , variables x and propositions P, Q, P_1, P_2 . It is well-founded because of the termination of $R_{\mathcal{T}(\Sigma, V)}$.

2.2 Sequent Calculus Modulo

Sequent calculus modulo can be seen as an extension of the sequent calculus of Gentzen (1934). We will use the denominations of Gallier (1986).

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

In Fig. 1 we present the inference rules of our *sequent calculus modulo*. They differ from the ones of Dowek (2003) because the congruence is externalized through specific inference rules $\uparrow\text{-l}$ and $\uparrow\text{-r}$ (as can be found Hermant, 2005a; Wack, 2005), whereas contraction is internalized. *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 $\uparrow\text{-l}$ and $\uparrow\text{-r}$ use only rules that appear in $R \cup R_{\mathcal{T}(\Sigma, V)}$. The set of all proofs will be denoted by \mathcal{SQM} .

$\text{Cut}(P)$ permits essentially to extend the proof search space with the proposition P . Logical Rules decompose some proposition which is called *principal*. Rewrite Rules, that do not appear in Gentzen's sequent calculus, introduce proposition rewriting into the proof system. Note that only atomic propositions are rewritten.

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 (1934), or more accurately Dowek (2003) because of $R_{\mathcal{T}(\Sigma, V)}$) that \emptyset admits Cut .

It is important to be aware that free variables appearing in a sequents play the same role as fresh constants, because no inference rules can modify them. As a consequence, one can restrict oneself to closed sequents, as indicated by Dowek et al. (2003, Proposition 1.5).

This sequent calculus has the weakening and the contraction properties:

- if there exist a proof of $\Gamma \vdash \Delta$, then for all propositions P there exists proofs of $\Gamma, P \vdash \Delta$ and $\Gamma \vdash P, \Delta$;
- there exist a proof of $\Gamma, P \vdash \Delta$ if and only if there exists a proof of $\Gamma, P, P \vdash \Delta$, and there exist a proof of $\Gamma \vdash P, \Delta$ if and only if there exists a proof of $\Gamma \vdash P, P, \Delta$.

³ \perp is used for definitions.

Identity Group:	
$\frac{}{\Gamma, P \vdash \Delta, P} \text{Ax}$	$\frac{\Gamma, P \vdash \Delta \quad \Gamma \vdash P, \Delta}{\Gamma \vdash \Delta} \text{Cut}(P)$
Logical Rules:	
$\frac{\Gamma \vdash P, \Delta}{\Gamma, \neg P \vdash \Delta} \neg\text{-l}$	$\frac{\Gamma, P \vdash \Delta}{\Gamma \vdash \neg P, \Delta} \neg\text{-r}$
$\frac{\Gamma, P, Q \vdash \Delta}{\Gamma, P \wedge Q \vdash \Delta} \wedge\text{-l}$	$\frac{\Gamma \vdash P, \Delta \quad \Gamma \vdash Q, \Delta}{\Gamma \vdash P \wedge Q, \Delta} \wedge\text{-r}$
$\frac{\Gamma, P \vdash \Delta \quad \Gamma, Q \vdash \Delta}{\Gamma, P \vee Q \vdash \Delta} \vee\text{-l}$	$\frac{\Gamma \vdash P, Q, \Delta}{\Gamma \vdash P \vee Q, \Delta} \vee\text{-r}$
$\frac{\Gamma, Q \vdash \Delta \quad \Gamma, \vdash P, \Delta}{\Gamma, P \Rightarrow Q \vdash \Delta} \Rightarrow\text{-l}$	$\frac{\Gamma, P \vdash Q, \Delta}{\Gamma \vdash P \Rightarrow Q, \Delta} \Rightarrow\text{-r}$
$\frac{\Gamma, \forall x. P, \{t/x\}P \vdash \Delta}{\Gamma, \forall x. P \vdash \Delta} \forall\text{-l}, t \in \mathcal{T}(\Sigma, V)$	$\frac{\Gamma \vdash \{c/x\}P, \Delta}{\Gamma \vdash \forall x. P, \Delta} \forall\text{-r},$ $c \text{ free constant } (c \notin \Sigma \cup V)$
$\frac{\Gamma, \{c/x\}P \vdash \Delta}{\Gamma, \exists x. P \vdash \Delta} \exists\text{-l},$ $c \text{ free constant } (c \notin \Sigma \cup V)$	$\frac{\Gamma \vdash \exists x. P, \{t/x\}P, \Delta}{\Gamma \vdash \exists x. P, \Delta} \exists\text{-r}, t \in \mathcal{T}(\Sigma, V)$
Rewrite Rules:	
if A can be rewritten to P , either by a term or a proposition rewrite rule (in one step),	
$\frac{\Gamma, A, P \vdash \Delta}{\Gamma, A \vdash \Delta} \uparrow\text{-l}$	$\frac{\Gamma \vdash A, P, \Delta}{\Gamma \vdash A, \Delta} \uparrow\text{-r}$

Figure 1: Sequent Calculus Modulo

Proposition 1 (Equivalence). *The sequent calculus modulo presented in Figure 1 is equivalent to the Asymmetric Sequent Calculus Modulo of Dowek (2003) (also w.r.t to cut-free proofs).*

Proof. It is quite clear that the inference rules of our system can be derived in G. Dowek's one.

Conversely, the absence of a weakening rule can be solved by the fact that our Axiom rule accepts side propositions, so that the weakened propositions can be kept until the Axioms.

The absence of contraction rule is not a problem, because the only inference rules where it could be problematic are $\forall\text{-l}$, $\exists\text{-r}$, $\uparrow\text{-l}$ and $\uparrow\text{-r}$, and the contraction is integrated in them.

Then, one can show that for a proposition rewrite rule $A \rightarrow P$, if there exists a proof of $\Gamma, C[P] \vdash \Delta$ for some propositional context C , then there exists a proof of $\Gamma, C[A] \vdash \Delta$: we can apply to $C[A]$ all the logical rules applied to $C[P]$ in the proof of $\Gamma, C[P] \vdash \Delta$, except the one applying to P because it is replaced by A . We must here first apply the rewrite rule $A \rightarrow P$, and then follow

on. We obtain by this process a proof of $\Gamma, C[A] \vdash \Delta$. The same is true at the right of a sequent. Consequently one can simulate rewriting non-atomic proposition.

Using this, one can transform the side conditions of G. Dowek's system into applications of $\uparrow\text{-l}$ and $\uparrow\text{-r}$. This implies that a proof in Dowek's system can be transformed into a proof in our system.

Of course, as we have seen, both system are also equivalent regarding cut-free proofs, since we did not need any Cut. \square

2.3 Properties of the Sequent Calculus Modulo

We present here some properties of the sequent calculus modulo, mainly extracted from Hermant (2005a), and we prove that the cut admissibility is not decidable.

Our system satisfies the Kleene Lemma:

Lemma 2 (Kleene Lemma (Hermant, 2005a, Lemme 3.3)). *If a sequent, containing the non-atomic formula 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 (2005a, Lemme 3.3), because we also look at \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 $\Gamma, \forall x. P, \{t/x\}P \vdash \Delta$. \square

The reader should consult Hermant (2003) for the definitions of the terms in the next proposition:

Proposition 3 (Condition for Cut Admissibility (Hermant, 2003, Lemma 8)). *Let \mathcal{R} be a proposition rewrite system.*

If there exists a complete, consistent theory Γ admitting Henkin witnesses, and a model of this theory such that for all $A \rightarrow P \in \mathcal{R}$, A and P have the same interpretation, then \mathcal{R} admits Cut.

Theorem 4 (Undecidability of the Cut Admissibility).

The problem

Input: A propositional rewrite system \mathcal{R}

Decide if \mathcal{R} admits Cut.

is undecidable.

Proof. We reduce to the validity problem in first-order logic. 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 R be a constant and \in a 2-ary predicate not appearing in P . Consider the propositional rewrite system (inspired from Hermant (2005a))

$$\mathcal{R} = \left\{ R \in R \rightarrow \forall y. (\forall x. y \in x \Rightarrow R \in x) \Rightarrow y \in R \Rightarrow P \right\}.$$

Then one can show that P is valid if and only if \mathcal{R} admits Cut.

If P is valid, then define a model as in Hermant (2005a, Definition 8.3). As P is valid, it is also in this model, so that $|P| = 1$. We can therefore use the same proof as in Hermant (2005a, Section 8.3) to prove the admissibility of Cut, replacing $A \vee \neg A$ by P .

Reciprocally, suppose P is not valid. By soundness of the sequent calculus of Gentzen, $\vdash P$ does not have any proof in \emptyset . Consequently, it does not have any cut-free proof in \mathcal{R} . Indeed, since R and \in do not appear in P , they cannot appear in a cut-free proof of $\vdash P$, so that no rewrite rule could be applied in a cut-free proof of $\vdash P$.

Nevertheless, there is a proof of P in \mathcal{R} : this is the same proof as in Hermant (2005a, Section 8.1), replacing C by P . Consequently, \mathcal{R} does not admit Cut. \square

2.4 Abstract Canonical Systems and Inference

The results in this section are extracted from Dershowitz and Kirchner (2003, 2006); Bonacina and Dershowitz

(2007), which should be consulted for motivations, details and proofs.

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

$$Pf(A) \stackrel{\dagger}{=} \{p \in \mathbb{P} : [p]^{Pm} \subseteq A\}.$$

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

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:

$$Th A \stackrel{\dagger}{=} [Pf(A)]_{Cl} = \{[p]_{Cl} : p \in \mathbb{P}, [p]^{Pm} \subseteq A\}.$$

Presentations A and B are *equivalent* ($A \equiv B$) if their theories are identical: $Th A = Th B$. In addition to this, we assume the two following postulates:

Postulate A (Reflexivity).

For all presentations A :

$$A \subseteq Th A$$

Postulate B (Closure).

For all presentations A :

$$Th Th A \subseteq Th A$$

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 $p \triangleright q \Rightarrow p = q$, where \triangleright is the reflexive closure of the subproof ordering \triangleright . We denote by \hat{a} such a trivial proof of $a \in \mathbb{A}$ and by \hat{A} the set of trivial proofs of each $a \in A$.

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 (Trivial).

For all proofs p and formulæ a :

$$a \in [p]^{Pm} \Rightarrow p \triangleright \hat{a}$$

Postulate D (Subproofs Premises Monotonicity).

For all proofs p and q :

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

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 \succsim over presentations:

$$A \succsim B \text{ if } A \equiv B \text{ and } \forall p \in Pf(A). \exists q \in Pf(B). p \geq q .$$

We define what a *normal-form proof* is, i.e. one of the minimal proofs of $Pf(Th A)$:

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

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

$$A^\# \stackrel{!}{=} [Nf(A)]^{Pm} .$$

So, we will say that A is *canonical* if $A = A^\#$.

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

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

Canonicity implies completeness, but the converse is not true.

We now consider inference and deduction mechanisms. A *deduction mechanism* \rightsquigarrow is a function from presentations to presentations and we call the relation $A \rightsquigarrow B$ a *deduction step*. A sequence of presentations $A_0 \rightsquigarrow A_1 \rightsquigarrow \dots$ is called a *derivation*. The *result* of the derivation is, as usual, its *persisting* formulæ:

$$A_\infty \stackrel{!}{=} \liminf_{j \rightarrow \infty} A_j = \bigcup_{j > 0} \bigcap_{i > j} A_i .$$

A deduction mechanism is *completing* if for each step $A \rightsquigarrow B$, $A \succsim B$, and the limit A_∞ is complete.

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

Theorem 5 (Bonacina and Dershowitz (2007, Lemma 5.13)).

A deduction mechanism is completing if and only if for all derivations $A_0 \rightsquigarrow A_1 \rightsquigarrow \dots$,

$$Th A_0 \subseteq [Pf(A_\infty) \cap Nf(A_0)]_{Cl} .$$

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

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

Completing formulæ are conclusions of proofs smaller than critical proofs:

$$Comp(A) \stackrel{!}{=} \bigcup_{p \in Crit(A) \wedge p' \text{ is any proof such that } p \triangleright p'} [p']^{Pm}$$

In this paper, we use a completing deduction mechanism in the following way:

$$A \rightsquigarrow A \cup C(A)$$

where $Comp(A) \subseteq C(A) \subseteq Th A$.

Proposition 6 (Dershowitz and Kirchner (2003, Lemma 10)). *This deduction mechanism is completing.*

3 Deduction Modulo is an Instance of ACS

We want to show that the sequent calculus modulo can be seen as an instance of ACS. For this purpose, we have to define what the formulæ, the proofs, the 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.

3.1 Proofs and Formulae

We aim to obtain cut-free proofs, so that the natural candidate for ACS proofs are sequent calculus proofs. Because of the weakening and contraction properties, we can restrict ourselves to proofs using minimal sets of propositions in their conclusions. More precisely, we can consider only proofs where all the propositions appearing in the conclusion are used as principal propositions somewhere in the proof, or in one of the Axioms.

The completion procedure we want to establish deals with 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 identified with proposition rewrite systems.

Therefore we suppose that there exists a function between sequents and proposition rewrite systems $Rew : \mathcal{S} \rightarrow \mathcal{PRS}$ such that:

Property 1: For all sequents $\Gamma \vdash \Delta$, $R = Rew(\Gamma \vdash \Delta)$ and $\mathcal{P}(\Gamma \vdash \Delta)$ are strongly compatible:

- (a) for all propositions P, Q , $P \xleftarrow[R]{*} Q$ implies that there exists a proof of $\mathcal{P}(\Gamma \vdash \Delta) \vdash P \Leftrightarrow Q$ in \emptyset (i.e. without rewrite rules);
- (b) there exists a cut-free proof of $\vdash \mathcal{P}(\Gamma \vdash \Delta)$ in R .

Property 2: For all proposition rewrite system R , for all sequents s and s' , if $Rew(s) = Rew(s')$ then s has a proof (resp. cut-free proof) in R iff s' has a proof (resp. cut-free proof) in R .

Property 1 implies compatibility in the sense of Definition 1.4 of Dowek et al. (2003), which is the same except that we need here a *cut-free* proof in b).

Section 5 provides an instance of such a function Rew .

With respect to the definitions of ACSs (see Sect. 2.4) deduction modulo can be seen as an ACS, in the following way:

— \mathbb{P} : *proofs* are sequent calculus proofs using minimal sets of propositions in their conclusion:

$$\mathbb{P} \stackrel{!}{=} \{p \in \mathcal{SQM} : \neg(\exists q \in \mathcal{SQM}. \text{Weak}(q, p))\}$$

where $\text{Weak}(q, p)$ says that the proof p can be obtained from q by weakening.

— \mathbb{A} : *formulae* are proposition rewrite systems corresponding to some sequent:

$$\mathbb{A} \stackrel{!}{=} \text{Rew}(\mathcal{S}) \subseteq \mathcal{PRS} .$$

— The *conclusion* of an ACS proof is the rewrite system associated by Rew to the conclusion of the sequent calculus proof: for all proofs p ,

$$[p]_{Cl} \stackrel{!}{=} \text{Rew}(\Gamma \vdash \Delta) \text{ when } p = \frac{\vdots}{\Gamma \vdash \Delta} .$$

— The *premises* of a proof are the rewrite system consisting in the proposition rewrite rules appearing in the proof or its subproofs: for all proofs p ,

$$[p]^{Pm} \stackrel{!}{=} \left\{ \left\{ \begin{array}{l} A \rightarrow P : \text{there exists a } \uparrow\text{-l or} \\ \uparrow\text{-r using } A \rightarrow P \text{ in } q \end{array} \right\} : \right. \\ \left. q \text{ is a subproof of } p \right\}$$

This definition implies that we consider only proofs using proposition rewrite systems corresponding to some sequent.

3.2 Orderings on Proofs

We define the following (infinite, but Noetherian) precedence $>$: for all formulae P, Q , if P is greater than Q for the subformula relation, then $\text{Cut}(P) > \text{Cut}(Q)$, and for all other inference rules r of Fig. 1, $\text{Cut}(P) > r$.

We order proofs using the RPO (Dershowitz, 1982) based on this precedence. Since the precedence is well-founded, so is the RPO (Dershowitz, 1982). We restrict this ordering to proofs which have the same *sequent* as conclusion, modulo weakening.

Because we work modulo weakening and contraction, it is important to note that a proof and its weakened and contracted versions are equivalent with respect to the ordering we have just defined, because they have the same cuts and the same labeled tree structure.

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

Subproofs of a proof p are defined as the subproofs of p for the sequent calculus, modulo weakening and contraction (subproofs may use less propositions than their parents).

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

To solve this problem, we can add manually the trivial proofs, i.e. \mathbb{P} is in fact $\mathbb{P} \cup \hat{\mathbb{A}}$, where formulae are identified with their trivial proof.

We have to extend the ordering $>$ to trivial proofs: it can be simply done by saying that they cannot be compared with other proofs. ($>$ over $\mathbb{P} \cup \hat{\mathbb{A}}$ is the same relation as $>$ over the original \mathbb{P} .)

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

$p \supseteq q$ if — q is a subproof modulo weakening of p in \mathcal{SQM}
— or $q = \hat{a}$ with $a \in [p]^{Pm}$.

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

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

Theorem 7 (Instance of ACS).

The sequent calculus modulo is an instance of ACS, with the definitions of \mathbb{A} , \mathbb{P} , $[\cdot]^{Pm}$, $[\cdot]_{Cl}$, $>$ and \supseteq given above.

Proof.

- Postulate A: suppose $R \in A$, we want to show that R is the conclusion of a proof built with A . Because $R \in \mathbb{A} = \text{Rew}(\mathcal{S})$, there exists some sequent $\Gamma \vdash \Delta$ such that $\text{Rew}(\Gamma \vdash \Delta) = R$. Using Property 1b), we know that there is a proof of $\mathcal{P}(\Gamma \vdash \Delta)$ in R . As a consequence of Lemma 2, we know that there is a proof of $\Gamma \vdash \Delta$ in R , i.e. a proof in A proving $\text{Rew}(\Gamma \vdash \Delta) = R$. (Remember that free variables can be treated as fresh constants in the construction of a proof.)
- Postulate B: let R be in $\text{Th } \text{Th } A$. By definition there is a proof $p \in \text{Pf}(\text{Th } A)$ such that $[p]_{Cl} = \text{Rew}(\Gamma \vdash \Delta) = R$ for some sequent $\Gamma \vdash \Delta$. Let R' be the rewrite system used in p , therefore $R' \in [p]^{Pm} \subseteq \text{Th } A$. By definition, there is a proof $q \in \text{Pf}(A)$ such that $[q]_{Cl} = \text{Rew}(\Gamma' \vdash \Delta') = R'$ for some sequent $\Gamma' \vdash \Delta'$. Using Property 1, we know that R' is compatible with $\mathcal{P}(\Gamma' \vdash \Delta')$. Using Proposition 1.8 of Dowek et al. (2003), because p is a proof of $\Gamma \vdash \Delta$ in R' , we know that there exists a proof r of $\mathcal{P}(\Gamma' \vdash \Delta'), \Gamma \vdash \Delta$ in \emptyset (i.e. without rewriting). The proof

$$\frac{\frac{\frac{\vdots}{\Gamma, P' \vdash \Delta} \quad \frac{\frac{\frac{\vdots}{\Gamma, \sigma\Gamma' \vdash \sigma\Delta', \Delta}}{\Gamma \vdash P', \Delta} \text{ Logical rules}}{\Gamma \vdash \Delta} \text{ Cut}(P')}{\Gamma \vdash \Delta}}$$

where P' means $\mathcal{P}(\Gamma' \vdash \Delta')$ and σ is a substitution replacing the free variables of Γ', Δ' by fresh constants, is a proof of $\text{Rew}(\Gamma \vdash \Delta) = R$ in $\text{Pf}(A)$, because it uses the same rewrite system as q which is in $\text{Pf}(A)$. (q is indeed a proof of $\sigma\Gamma' \vdash \sigma\Delta'$, because free variables can be considered as fresh constants.) Therefore $R \in \text{Th } A$.

- Postulate C: it holds by definition of the subproof relation \supseteq .
- Postulate D: suppose $p \supseteq q$. If q is a subproof of p in the sequent calculus modulo, then by definition of $[\cdot]^{Pm}$ and by transitivity of the subproof relation, $[p]^{Pm} \supseteq [q]^{Pm}$. If $q = \hat{a}$ with $a \in [p]^{Pm}$, $[q]^{Pm} = \{a\} \subseteq [p]^{Pm}$.

- Postulate E: suppose $p \triangleright q > r$. Because q is comparable with r , both of them are sequent calculus proofs, and not trivial proofs. As q is a subproof of p in the sequent calculus modulo, we can replace q by r in p to obtain some proof v , because $q > r$ implies that they have the same sequent as conclusion, modulo weakening. Because an RPO is reduction ordering, $p > v$.

□

4 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 whom the sequent calculus admits Cut.

4.1 Normal-form Proofs and Critical Proofs in Deduction Modulo

Proposition 8 (Characterization of Normal-Form Proofs). *A proof in deduction modulo is in normal form iff it is either a trivial proof or a cut-free proof with no useless logical rules.*

Proof. If a proof p in $Pf(A)$ is not a trivial proof, and possesses a cut at position \mathfrak{p} , then using Property 1(b), we know that there exists a cut-free proof of the sequent $\vdash \mathcal{P}(\Gamma \vdash \Delta)$ where $\Gamma \vdash \Delta$ is the conclusion of $p|_{\mathfrak{p}}$. Using Lemma 2 we obtain a cut-free proof q of $\Gamma \vdash \Delta$. Replacing $p|_{\mathfrak{p}}$ by q in p using Postulate E, we obtain a smaller proof

than p which is in $Pf(ThA)$ because q is by assumption in $Rew(\Gamma \vdash \Delta) = [p|_{\mathfrak{p}}]_{cl}$. Therefore p cannot be in normal-form.

If a proof p is not a trivial proof, is cut-free, and has a useless logical rule at position \mathfrak{p} , then the direct subproofs of $p|_{\mathfrak{p}}$ shows the same conclusion as $p|_{\mathfrak{p}}$ (because we work modulo weakening, and because the propositions resulting from the logical rule are not needed), and are smaller because an RPO is a simplification ordering. By using Postulate E we can obtain a proof smaller than p , and therefore p cannot be in normal-form.

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 p contains a Cut or q is a subproof of p , i.e. useless rules were applied in p .

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

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

Proposition 9 (Critical Proofs in Deduction Modulo). *Critical proofs in deduction modulo are of the form*

$$\frac{\frac{\frac{\pi}{\vdots}}{\Gamma, A, P \vdash \Delta} \uparrow\text{-l} \quad \frac{\frac{\pi'}{\vdots}}{\Gamma \vdash Q, A, \Delta} \uparrow\text{-r}}{\Gamma \vdash \Delta} \text{Cut}(A)$$

where π and π' are cut-free and do not use unneeded logical rules, and at least one of $A \rightarrow P$ or $A \rightarrow Q$ is not a term rewriting.

Proof. We essentially follow the proof of the Hauptsatz of Girard, Lafont, and Taylor (1989, Chapter 13).

Because of Proposition 8, 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, or a unneeded logical rule. In the second case, we can find a smaller proof in the same presentation, contradicting the minimality of critical proofs. Therefore a cut-free proof has a cut at its root. It is a proof of the form

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

where π and π' are cut-free without useless rules.

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

We can now check the different cases that can be found in Section 13.2 of Girard et al. (1989) (note that we do not have to consider structural rules in our 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 $\overline{\Gamma \vdash \Delta}^{Ax}$ 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 formula 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 . The proof

$$\frac{\frac{\frac{\varpi_1 \vdots \Gamma, \Gamma_1, P \vdash \Delta, \Delta_1}{\Gamma, \Gamma_1 \vdash \Delta, \Delta_1} \text{Cut}(P) \quad \frac{\varpi' \vdots \Gamma, \Gamma_1 \vdash P, \Delta, \Delta_1}{\Gamma, \Gamma_1 \vdash \Delta, \Delta_1} \text{Cut}(P)}{\Gamma, \Gamma_1 \vdash \Delta, \Delta_1} \quad \frac{\frac{\varpi_n \vdots \Gamma, \Gamma_n, P \vdash \Delta, \Delta_n}{\Gamma, \Gamma_n \vdash \Delta, \Delta_n} \text{Cut}(P) \quad \frac{\varpi' \vdots \Gamma, \Gamma_n \vdash P, \Delta, \Delta_n}{\Gamma, \Gamma_n \vdash \Delta, \Delta_n} \text{Cut}(P)}{\Gamma, \Gamma_n \vdash \Delta, \Delta_n} r}{\Gamma, \Gamma \vdash \Delta, \Delta}$$

is smaller than the initial proof, contradicting its minimality.

4. r' is a logical rule other than a right one with principal formula 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. (1989) : by replacing the cut over P by cuts over subformulae 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

$$\frac{\frac{\frac{\pi_1 \vdots \Gamma, P_1, P_2 \vdash \Delta}{\Gamma, P_1 \wedge P_2 \vdash \Delta} \wedge\text{-l} \quad \frac{\frac{\pi'_1 \vdots \Gamma \vdash P_1, \Delta}{\Gamma \vdash P_1, \Delta} \wedge\text{-r} \quad \frac{\pi'_2 \vdots \Gamma \vdash P_2, \Delta}{\Gamma \vdash P_2, \Delta} \wedge\text{-r}}{\Gamma \vdash P_1 \wedge P_2, \Delta} \text{Cut}(P_1 \wedge P_2)}{\Gamma \vdash \Delta}$$

is greater than the proof

$$\frac{\frac{\frac{\pi_1 \vdots \Gamma, P_1, P_2 \vdash \Delta}{\Gamma, P_1 \vdash \Delta} \text{Cut}(P_2) \quad \frac{\varpi'_2 \vdots \Gamma, P_1 \vdash P_2, \Delta}{\Gamma, P_1 \vdash P_2, \Delta} \text{Cut}(P_2)}{\Gamma, P_1 \vdash \Delta} \quad \frac{\pi'_1 \vdots \Gamma \vdash P_1, \Delta}{\Gamma \vdash P_1, \Delta} \text{Cut}(P_1)}{\Gamma \vdash \Delta}$$

6. r or r' is a rewrite rule applying to another proposition than P . This case can in fact be handled as case 3.
7. r is a rewrite rule and r' is a logical rule, both applying to P . This case cannot occur, because if we rewrite P , it implies that P is atomic so that no logical rule can be applied to it.
8. r is a logical rule and r' is a rewrite rule, both applying to P . This case is handled as case 7.
9. r and r' are both rewrite rules applying to P . Therefore P has to be atomic, and is rewritten by $P \rightarrow P_1$ to the left and $P \rightarrow P_2$ to the right. If both of this rewriting are term rewriting, then, because of confluence of $R_{\mathcal{T}(\Sigma, \mathcal{V})}$, we know that there is some P' such that $P_1 \xrightarrow{*}_{R_{\mathcal{T}(\Sigma, \mathcal{V})}} P' \xleftarrow{*}_{R_{\mathcal{T}(\Sigma, \mathcal{V})}} P_2$. The proof

$$\frac{\frac{\frac{\pi_1 \vdots \Gamma, P_1 \vdash \Delta}{\Gamma, P_1 \vdash \Delta} \text{Cut}(P_1) \quad \frac{\frac{\frac{\Gamma, P' \vdash P', \Delta}{\Gamma, P_2 \vdash P_1, \Delta} \text{Ax} \quad \text{Rewrite Rules}}{\Gamma \vdash P_1, \Delta} \text{Cut}(P_2)}{\Gamma \vdash P_1, \Delta} \text{Cut}(P_2)}{\Gamma \vdash \Delta} \quad \frac{\varpi'_1 \vdots \Gamma \vdash P_1, P_2, \Delta}{\Gamma \vdash P_1, P_2, \Delta} \text{Cut}(P_2)}{\Gamma \vdash \Delta}$$

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. \square

Note: If we suppose, as in the order condition of Hermant (2005b), 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.

The main difference with Hermant (2005b) 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 remains to be investigated how this process is related with normalization, i.e. β -reduction. (The last case corresponds in fact to an η -expansion.) It is proved

by Dowek and Werner (2003) that such an order condition provides normalization in the quantifier-free case.

This result was also independently found by Aiguier, Boin, and Longuet (2005), with the same kind of ordering over proofs.

Theorem 10 (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 formula.

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

$$\left\{ \begin{array}{l} A \rightarrow A \wedge B \\ A \rightarrow A \vee P \end{array} \right. .$$

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

$$\frac{\frac{\frac{\overline{A, B \vdash B} \text{ Ax}}{A, A \wedge B \vdash B} \wedge\text{-I}}{A \vdash B} \uparrow\text{-I}}{\vdash B} \text{ Cut}(A) \quad \frac{\frac{\vdots}{\vdash P, A, B} \text{ Proof of } P \text{ in } \emptyset}{\vdash A \vee P, A, B} \vee\text{-r}}{\vdash A, B} \uparrow\text{-r}$$

□

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.

4.2 The Completion Procedure

As we wrote in Sect. 2.4, we want to define a completing completion procedure by adding to a presentation A a presentation $C(A)$ such that $Comp(A) \subseteq C(A) \subseteq Th A$.

Here, using Property 1(b), we know that for all proofs p 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 2 we obtain a cut-free proof p' of $\Gamma \vdash \Delta$ in $Rew(\Gamma \vdash \Delta)$. If the proof p is critical, it has a cut at its root and thus it is than p' , so that we can use this particular p' in the definition $Comp()$. We therefore have to add the premises of q , but these premises are in fact in $Rew(\Gamma \vdash \Delta) = [p]_{cl}$:

$$Comp(A) \stackrel{!}{=} \{[p]_{cl} : p \in Crit(A)\} .$$

Step 1. Choose a sequent. Push all negated formulæ on the other side of the sequent. For instance, $A, \neg B \vdash \neg C, D$ becomes $A, C \vdash B, D$. If the new Γ is empty, go to step 2. If the new Δ is empty, go to step 3. If neither are

The best procedure is thus to add only the conclusions of critical proofs. Nevertheless, searching for these proofs 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 9 (note that it is only a necessary condition for being critical), except the one that we know for sure that they are not minimal (for instance if $A \in \Gamma \cup \Delta$).

We must consider proofs of the form of Proposition 9. As π and π' are cut-free and do not use unneeded logical rules, they could be found using for instance a tableaux method modulo, like TaMeD (Bonichon, 2004), which is complete with respect to cut-free proofs, if we knew Γ and Δ , hence the idea to apply the tableaux method to $A, P \vdash$ and $\vdash Q, A$, and to complete Γ and Δ in order to close the remaining tableaux. Because we work modulo weakening, we can restrict ourselves to the minimal Γ and Δ closing the tableaux. We can then sort the obtained $\Gamma \vdash \Delta$ to remove sequents where $A \in \Gamma \cup \Delta$. The resulting rewrite system is obtained by adding all $Rew(\Gamma \vdash \Delta)$ to our rewrite system.

Theorem 11 (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 6, we know that R_∞ is complete, and therefore by Lemma 5

$$Th R_0 \subseteq [Pf(R_\infty) \cap Nf(R_0)]_{cl} . \quad (1)$$

The “if” part comes from the fact that our completion is sound. For the “only if”, suppose that $\Gamma \vdash \Delta$ has a proof in R_0 , then using (1) it has a proof p in $Pf(R_\infty) \cap Nf(R_0)$. If p is a trivial proof, then we can use 1(b) to find a cut-free proof with the same conclusion, otherwise Proposition 8 shows that p is cut-free. The conclusion of the cut-free proof is not necessarily $\Gamma \vdash \Delta$ but a sequent $\Gamma' \vdash \Delta'$ such that $Rew(\Gamma \vdash \Delta) = Rew(\Gamma' \vdash \Delta')$, so we can conclude with Property 2. □

5 Sequents and Rewrite Systems

For deduction modulo to be an instance of ACS, we have to define some function Rew having Properties 1 and 2. We also want to know how to build proofs that use the rewrite system associated with some sequent, and therefore this function has to be effective.

5.1 An Algorithm ...

If we consider only propositional logic (i.e. without quantifier), we can use the following (non-deterministic) algorithm to transform a set of sequents $\Gamma \vdash \Delta$ into a set of rewrite rules:

empty, go to either Step 2 or Step 3.

Step 2. Decompose the last proposition iteratively:

$$\begin{array}{lcl}
P_1, \dots, P_n \vdash Q_1, \dots, Q_m & \text{becomes} & P_1, \dots, P_n, \neg Q_1, \dots, \neg Q_{m-1} \vdash Q_m \\
P_1, \dots, P_n \vdash Q_1 \wedge Q_2 & \text{"} & P_1, \dots, P_n \vdash Q_1 ; P_1, \dots, P_n \vdash Q_2 \\
P_1, \dots, P_n \vdash Q_1 \vee Q_2 & \text{"} & P_1, \dots, P_n, \neg Q_1 \vdash Q_2 \\
P_1, \dots, P_n \vdash Q_1 \Rightarrow Q_2 & \text{"} & P_1, \dots, P_n, Q_1 \vdash Q_2 \\
P_1, \dots, P_n \vdash A & \text{"} & A \rightarrow A \vee \exists x_1, \dots, x_p. (P_1 \wedge \dots \wedge P_n)
\end{array}$$

(A atomic, and the x_i are the free variables appearing in P_1, \dots, P_n but not in A)
for $P_1, \dots, P_n \vdash \neg Q$, return to Step 1

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

$$\begin{array}{lcl}
P_1 \Rightarrow P_2 \vdash Q_1, \dots, Q_m & \text{becomes} & P_2 \vdash Q_1, \dots, Q_m ; \neg P_1 \vdash Q_1, \dots, Q_m \\
A \vdash Q_1, \dots, Q_m & \text{"} & A \rightarrow A \wedge \forall x_1, \dots, x_p. (Q_1 \vee \dots \vee Q_m)
\end{array}$$

(A atomic, and the x_i are the free variables appearing in Q_1, \dots, Q_m but not in A)
for $\neg P \vdash Q_1, \dots, Q_m$, return to Step 1.

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

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

This algorithm can be extended to the case with quan-

tifiers. In the case of a \forall on the left of the sequent, or a \exists on the right, we will keep the formula in the sequent, but will not decompose it further. We will therefore denote by \underline{P} the fact that P was already decomposed. Then we do not consider underlined formula in Step 1 to choose between Step 2 or Step 3, and at the beginning of Step 2 (resp. Step 3), one keep a non-underlined formula to the right (resp. left) side.

We also have to add the following decomposition steps:

- (2) $P_1, \dots, P_n \vdash \forall x. Q$ becomes $P_1, \dots, P_n \vdash \{y/x\}Q$ where y does not appear in P_1, \dots, P_n ;
- (2) $P_1, \dots, P_n \vdash \exists x. Q$ becomes $P_1, \dots, P_n, \neg \exists x. \underline{Q} \vdash \{t/x\}Q$ where t can be any ground term;
- (3) $\exists x. P \vdash Q_1, \dots, Q_m$ becomes $\{y/x\}P \vdash Q_1, \dots, Q_m$ where y does not appear in Q_1, \dots, Q_m .
- (3) $\forall x. QP_1, \dots, P_n \vdash$ becomes $\{t/x\}P \vdash \underline{\forall x. Q}, Q_1, \dots, Q_m$ where t can be any ground term.

Of course, at the end, the underlines are removed.

This algorithm does not allow all rewrite systems to be considered as formulae. Nevertheless, one can transform all rewrite systems to equivalent rewrite systems that are images of sequents by Rew , by splitting the rules: $A \rightarrow P$ becomes $A \rightarrow A \vee P$ and $A \rightarrow A \wedge P$. This is equivalent

to the polarized rewrite systems of Dowek (2002).

This algorithm can be seen as the attempt to build a cut-free proof of the conclusion of a critical proof, adding rewrite rules to close the branches were an atomic formula appears.

5.2 ... with the Good Properties

We first prove Property 1 using three lemmata.

Lemma 12. *If the sequent $\Gamma \vdash \Delta$ is transformed to the set of sequents $\{\Gamma' \vdash \Delta'\} \cup S'$ by the algorithm described in Sect. 5, then the sequent*

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

can be proved (without rewrite rules).

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

$$\begin{array}{c}
\frac{}{Q_1, Q_2 \vdash Q_1} \text{Ax} \\
\frac{}{Q_1 \wedge Q_2 \vdash Q_1} \wedge\text{-I} \quad \frac{}{\bigwedge_i P_i \vdash \bigwedge_i P_i} \text{Ax} \\
\frac{}{\bigwedge_i P_i \Rightarrow (Q_1 \wedge Q_2), \bigwedge_i P_i \vdash Q_1} \Rightarrow\text{-I} \\
\frac{}{\{c_i/x_i\} \bigwedge_i P_i \Rightarrow (Q_1 \wedge Q_2) \vdash \{c_i/y_i\} \bigwedge_i P_i \Rightarrow Q_1} \Rightarrow\text{-r} \\
\frac{}{\forall x_1, \dots, x_n. (\bigwedge_i P_i \Rightarrow (Q_1 \wedge Q_2)) \vdash \{c_i/y_i\} (\bigwedge_i P_i \Rightarrow Q_1)} \forall\text{-I} \\
\frac{}{\forall x_1, \dots, x_n. (\bigwedge_i P_i \Rightarrow (Q_1 \wedge Q_2)) \vdash \forall y_1, \dots, y_m. (\bigwedge_i P_i \Rightarrow Q_1)} \forall\text{-r}
\end{array}$$

where c_i are fresh constants. \square

Lemma 13. For all propositions A, P_1, \dots, P_n , if x_1, \dots, x_p the free variables of P_1, \dots, P_n not appearing freely in A , then the sequents

$$\begin{aligned} \mathcal{P}(P_1, \dots, P_n \vdash A) \vdash A &\Leftrightarrow A \vee \exists x_1, \dots, x_p. \bigwedge_i P_i \\ \mathcal{P}(A \vdash P_1, \dots, P_n) \vdash A &\Leftrightarrow A \wedge \forall x_1, \dots, x_p. \bigvee_i P_i \end{aligned}$$

can be proved (without rewrite rules).

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

$$\frac{\frac{\frac{\forall y_1, \dots, y_m. (\bigwedge_i P_i \Rightarrow A), A \vdash A, \exists x_1, \dots, x_p. \bigwedge_i P_i}{\forall y_1, \dots, y_m. (\bigwedge_i P_i \Rightarrow A), A \vdash A \vee \exists x_1, \dots, x_p. \bigwedge_i P_i} \text{Ax}}{\forall y_1, \dots, y_m. (\bigwedge_i P_i \Rightarrow A), A \vdash A \vee \exists x_1, \dots, x_p. \bigwedge_i P_i} \text{V-r}}{\forall y_1, \dots, y_m. (\bigwedge_i P_i \Rightarrow A) \vdash A \Rightarrow A \vee \exists x_1, \dots, x_p. \bigwedge_i P_i} \Rightarrow \text{-r} \quad (2)$$

$$\frac{\frac{\frac{\frac{\frac{A \vdash A}{A \vdash A} \text{Ax}}{\sigma \bigwedge_i P_i \vdash \sigma \bigwedge_i P_i} \text{Ax}}{\sigma(\bigwedge_i P_i \Rightarrow A), \sigma \bigwedge_i P_i \vdash A} \Rightarrow \text{-I}}{\forall y_1, \dots, y_m. (\bigwedge_i P_i \Rightarrow A), \sigma \bigwedge_i P_i \vdash A} \forall \text{-I}}{\frac{\frac{A \vdash A}{\forall y_1, \dots, y_m. (\bigwedge_i P_i \Rightarrow A), \exists x_1, \dots, x_p. \bigwedge_i P_i \vdash A} \text{Ax}}{\forall y_1, \dots, y_m. (\bigwedge_i P_i \Rightarrow A), A \vee \exists x_1, \dots, x_p. \bigwedge_i P_i \vdash A} \exists \text{-I}}{\forall y_1, \dots, y_m. (\bigwedge_i P_i \Rightarrow A) \vdash A \vee \exists x_1, \dots, x_p. \bigwedge_i P_i \Rightarrow A} \Rightarrow \text{-r}} \quad (3)$$

$$\frac{\begin{array}{c} (2) \\ \vdots \end{array} \quad \begin{array}{c} (3) \\ \vdots \end{array}}{\forall y_1, \dots, y_m. (\bigwedge_i P_i \Rightarrow A) \vdash A \Leftrightarrow A \vee \exists x_1, \dots, x_p. \bigwedge_i P_i} \wedge \text{-r}$$

where σ is the substitution replacing x_i by a fresh constant c_i for $i \in \{1, \dots, p\}$, leaving all other variables unchanged.

The proof of the other sequent is dual. \square

Lemma 14. For all atomic propositions A and propositions P_1, \dots, P_n , if x_1, \dots, x_p the free variables of P_1, \dots, P_n not appearing freely in A , then we can prove the sequent

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

in the rewrite system consisting of the rule $A \rightarrow A \vee \exists x_1, \dots, x_p. (P_1 \wedge \dots \wedge P_n)$, and the sequent

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

in the rewrite system consisting of the rule $A \rightarrow A \wedge \exists x_1, \dots, x_p. (P_1 \vee \dots \vee P_n)$.

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

$$\frac{\frac{\frac{\frac{\frac{\frac{\{c_i/y_i\}P_1 \vdash \{c_i/y_i\}P_1}{\{c_i/y_i\}P_1, \dots, \{c_i/y_i\}P_n, \vdash \{c_i/y_i\}A, \{c_i/y_i\}P_1 \wedge \dots \wedge P_n} \text{Ax}}{\{c_i/y_i\} \bigwedge_i P_i \vdash \{c_i/y_i\}A, \{c_i/y_i : i > p\}(\{c_i/x_i\}P_1 \wedge \dots \wedge P_n)} \wedge \text{-I}}{\{c_i/y_i\} \bigwedge_i P_i \vdash \{c_i/y_i\}A, \{c_i/y_i : i > p\} \exists x_1, \dots, x_p. (P_1 \wedge \dots \wedge P_n)} \exists \text{-r}}{\{c_i/y_i\} \bigwedge_i P_i \vdash \{c_i/y_i : i > p\}(A \vee \exists x_1, \dots, x_p. (P_1 \wedge \dots \wedge P_n))} \vee \text{-r}}{\frac{\{c_i/y_i\} \bigwedge_i P_i \vdash \{c_i/y_i : i > p\}A}{\vdash \{c_i/y_i\} \bigwedge_i P_i \Rightarrow A} \Rightarrow \text{-r}} \uparrow \text{-r}}{\vdash \forall y_1, \dots, y_m. (\bigwedge_i P_i \Rightarrow A)} \forall \text{-r}$$

\square

We can prove Property 2 using the following lemma:

Lemma 15. *For all proposition rewrite system R , if the set of sequents S is transformed into the set of sequents S' by the algorithm of Sect. 5, 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 2.

For instance, $P_1, \dots, P_n \vdash \forall x. Q$ is transformed into $P_1, \dots, P_n \vdash \{y/x\}Q$ where y does not appear in

P_1, \dots, P_n . If $P_1, \dots, P_n \vdash \{y/x\}Q$ has a proof in R , then because y does not appear in P_1, \dots, P_n , $P_1, \dots, P_n \vdash \{c/x\}Q$ has a proof in R for any fresh constant c , so that $P_1, \dots, P_n \vdash \forall x. Q$ has a proof in R by application of \forall -r. Conversely, if $P_1, \dots, P_n \vdash \forall x. Q$ has a proof in R , then by Lemma 2 there exists a proof of $P_1, \dots, P_n \vdash \{c/x\}Q$ in R for a fresh constant c . As c is fresh, it can be replaced by a variable y which does not appear in P_1, \dots, P_n , so that $P_1, \dots, P_n \vdash \{y/x\}Q$ has a proof in R .

In the preceding paragraph, if proofs are supposed cut-free, then the resulting proofs have the same property. \square

We can now prove the main result of this subsection:

Proposition 16. *The Rew function defined in Sect. 5.1 has the Properties 1 and 2.*

Proof. We proceed by induction on the execution of the algorithm of Sect. 5

For Property 1a), one can restrict oneself to one step rewrite for $P \xrightarrow[R]{*} Q$. Lemma 13 permits to prove the property at the end of the algorithm, when sequents are transformed into rules. Lemma 12 permits to prove the inductive case: suppose $\Gamma \vdash \Delta$ is transformed into $\{\Gamma' \vdash \Delta'\} \cup \dots$. Suppose $\mathcal{P}(\Gamma' \vdash \Delta') \vdash A \Leftrightarrow P$ has a proof p without rewrite rules. By Lemma 12, there is a proof q of $\mathcal{P}(\Gamma \vdash \Delta) \vdash \mathcal{P}(\Gamma' \vdash \Delta')$. Therefore, we can construct the proof

$$\frac{\begin{array}{c} p \\ \vdots \\ \mathcal{P}(\Gamma \vdash \Delta), \mathcal{P}(\Gamma' \vdash \Delta') \vdash A \Leftrightarrow P \end{array} \quad \begin{array}{c} q \\ \vdots \\ \mathcal{P}(\Gamma \vdash \Delta) \vdash \mathcal{P}(\Gamma' \vdash \Delta'), A \Leftrightarrow P \end{array}}{\mathcal{P}(\Gamma \vdash \Delta) \vdash A \Leftrightarrow P} \text{Cut}(\mathcal{P}(\Gamma' \vdash \Delta'))$$

without rewrite rules.

For Property 1b), the base case is a consequence of Lemma 14, whereas the inductive case is a consequence of Lemma 2. For instance, suppose $P_1, \dots, P_n \vdash Q_1 \wedge Q_2$ is transformed into $P_1, \dots, P_n \vdash Q_1; P_1, \dots, P_n \vdash Q_2$. For $i \in \{1, 2\}$, suppose $\vdash \mathcal{P}(P_1, \dots, P_n \vdash Q_i)$ has a cut-free proof in some rewrite system R_i . By Lemma 2, there is a cut-free proof p_i of $\sigma P_1, \dots, \sigma P_n \vdash \sigma Q_i$ in R_i , where σ is a substitution replacing the free variables of P_1, \dots, P_n, Q_i by fresh constants. Consequently we can construct the cut-free proof

$$\frac{\begin{array}{c} p_1 \\ \vdots \\ \sigma P_1, \dots, \sigma P_n \vdash \sigma Q_1 \end{array} \quad \begin{array}{c} p_2 \\ \vdots \\ \sigma P_1, \dots, \sigma P_n \vdash \sigma Q_2 \end{array}}{\vdash \mathcal{P}(P_1, \dots, P_n \vdash Q_1 \wedge Q_2)} \forall\text{-r}, \Rightarrow\text{-r}, \wedge\text{-l}, \wedge\text{-r}$$

in $R_1 \cup R_2$.

For Property 2, the base case is trivial, and the inductive case is a consequence of Lemma 15. \square

6 Examples

In the case of Crabbé’s example presented in the introduction, the input is the rewrite system $A \rightarrow B \wedge \neg A$ and the completion procedure generates $B \rightarrow B \wedge \perp$ which is equivalent to $B \rightarrow \perp$.

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

$$\left\{ \begin{array}{l} A \rightarrow B \wedge \neg A \\ B \rightarrow \perp \end{array} \right.$$

The critical proofs have the form

$$\frac{\begin{array}{c} \vdots \\ R \in R, \forall y. y \simeq R \Rightarrow y \in R \Rightarrow C \vdash \end{array}}{R \in R \vdash} \uparrow\text{-l} \quad \frac{\begin{array}{c} \vdots \\ \vdash R \in R, \forall y. y \simeq R \Rightarrow y \in R \Rightarrow C \end{array}}{\vdash R \in R} \uparrow\text{-l}}{\vdash} \text{Cut}(R \in R)$$

admits Cut.

The next example deals with quantifiers and is extracted from Hermant (2005b):

$$R \in R \rightarrow \forall y. y \simeq R \Rightarrow y \in R \Rightarrow C$$

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

The left part can be developed as

$$\frac{\frac{\frac{R \in R, C \vdash R \in R \vdash t_1 \in R}{R \in R, t_1 \in R \Rightarrow C \vdash} \Rightarrow -l \quad \frac{\frac{R \in R, t_1 \in c_1 \vdash R \in c_1}{R \in R \vdash t_1 \in c_1 \Rightarrow R \in c_1} \Rightarrow -r}{R \in R \vdash t_1 \simeq R} \forall -r}{\frac{R \in R, t_1 \simeq R \Rightarrow t_1 \in R \Rightarrow C \vdash}{R \in R, \forall y. y \simeq R \Rightarrow y \in R \Rightarrow C \vdash} \forall -l} \Rightarrow -l$$

and the right part as

$$\frac{\frac{\frac{\frac{R \in t_0, c_0 \in R \vdash R \in R, C \quad c_0 \in R \vdash c_0 \in t_0, R \in R, C}{c_0 \in t_0 \Rightarrow R \in t_0, c_0 \in R \vdash R \in R, C} \Rightarrow -l}{c_0 \simeq R, c_0 \in R \vdash R \in R, C} \forall -l}{c_0 \simeq R \vdash R \in R, c_0 \in R \Rightarrow C} \Rightarrow -r}{\frac{\frac{\frac{\frac{\vdash R \in R, c_0 \simeq R \Rightarrow c_0 \in R \Rightarrow C}{\vdash R \in R, c_0 \simeq R \Rightarrow c_0 \in R \Rightarrow C} \Rightarrow -r}{\vdash R \in R, \forall y. y \simeq R \Rightarrow y \in R \Rightarrow C} \forall -r}} \Rightarrow -l$$

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 $C \rightarrow C \vee \top$. This rule does not generate new critical proofs, and consequently, the proposition rewrite system

$$\left\{ \begin{array}{l} R \in R \rightarrow \forall y. y \simeq R \Rightarrow y \in R \Rightarrow C \\ C \rightarrow C \vee \top \end{array} \right.$$

admits Cut.

One can also think of another example, where there remains quantifiers in the conclusion: one can think of a rule derived from Crabbé's example $A \rightarrow (\exists x. \forall y. B \wedge P(x, y)) \wedge \neg A$ where A and B are atomic propositions, and P a predicate of arity 2. We have a critical proof

$$\frac{\frac{\frac{\frac{A, \exists x. \forall y. B \wedge P(x, y) \vdash A}{A, \exists x. \forall y. B \wedge P(x, y), \neg A \vdash} \text{Ax} \quad \frac{\frac{\frac{\exists x. \forall y. B \wedge P(x, y), A \vdash A}{\exists x. \forall y. B \wedge P(x, y) \vdash \neg A, A} \text{Ax}}{\exists x. \forall y. B \wedge P(x, y) \vdash \neg A, A} \text{Ax}}{\exists x. \forall y. B \wedge P(x, y) \vdash (\exists x. \forall y. B \wedge P(x, y)) \wedge \neg A, A} \wedge -r}{\exists x. \forall y. B \wedge P(x, y), A, (\exists x. \forall y. B \wedge P(x, y)) \wedge \neg A \vdash} \wedge -l}{\exists x. \forall y. B \wedge P(x, y), A \vdash} \uparrow -l}{\exists x. \forall y. B \wedge P(x, y) \vdash A} \text{Cut}(A)$$

The sequent of the conclusion is transformed into a rewrite rule:

$$\begin{aligned} \exists x. \forall y. B \wedge P(x, y) \vdash & \text{ becomes } \forall y. B \wedge P(z, y) \vdash \\ & \text{ becomes } B \wedge P(z, a) \vdash \neg \forall y. B \wedge P(z, y) \\ & \text{ becomes } B \vdash \neg P(z, a), \neg \forall y. B \wedge P(z, y) \\ & \text{ becomes } B \rightarrow B \wedge \forall z. (\neg P(z, a) \vee \neg \forall y. B \wedge P(z, y)). \end{aligned}$$

Then, a cut free proof of $\exists x. \forall y. B \wedge P(x, y) \vdash$ can be:

$$\frac{\frac{\frac{\frac{\frac{B \wedge P(c, d), B, P(c, a) \vdash B \wedge P(c, d)}{\forall y. B \wedge P(c, y), B, P(c, a) \vdash B \wedge P(c, d)} \text{Ax}}{\forall y. B \wedge P(c, y), B, P(c, a) \vdash \forall y. B \wedge P(c, y)} \forall -l}{\forall y. B \wedge P(c, y), B, \neg P(c, a), P(c, a) \vdash} \forall -l}{\forall y. B \wedge P(c, y), B, \neg P(c, a) \vee \neg \forall y. B \wedge P(c, y), P(c, a) \vdash} \forall -l}{\forall y. B \wedge P(c, y), B, \forall z. (\neg P(z, a) \vee \neg \forall y. B \wedge P(z, y)), P(c, a) \vdash} \forall -l}{\forall y. B \wedge P(c, y), B, B \wedge \forall z. (\neg P(z, a) \vee \neg \forall y. B \wedge P(z, y)), P(c, a) \vdash} \wedge -l}{\forall y. B \wedge P(c, y), B, P(c, a) \vdash} \uparrow -l}{\forall y. B \wedge P(c, y), B \wedge P(c, a) \vdash} \wedge -l}{\forall y. B \wedge P(c, y) \vdash} \forall -l}{\exists x. \forall y. B \wedge P(x, y) \vdash} \exists -l$$

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

$$R = \left\{ \begin{array}{l} A \rightarrow A \vee B \\ A \rightarrow A \wedge C \\ D \rightarrow D \wedge B \\ D \rightarrow D \vee E \end{array} \right.$$

may need two step to produce the completed system

$$R \cup \left\{ \begin{array}{l} B \rightarrow B \wedge C \\ B \rightarrow B \vee E \\ C \rightarrow C \vee E \end{array} \right. .$$

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

$$\frac{\frac{\overline{B, A, C \vdash C} \text{Ax}}{B, A, A \wedge C \vdash C} \wedge\text{-l} \quad \frac{\overline{B \vdash A, B, C} \text{Ax}}{B \vdash A \vee B, A, C} \vee\text{-r}}{\frac{B, A \vdash C}{B \vdash C} \uparrow\text{-l} \quad \frac{B \vdash A, C}{B \vdash A, C} \uparrow\text{-r}} \text{Cut}(A)$$

that leads for instance to the rewrite rule $B \rightarrow B \wedge C$. Similarly the two other rules may complete the system by the rewrite rule $B \rightarrow B \vee E$. Consequently, after one step the system has a critical proof

$$\frac{\frac{\overline{E, B, C \vdash C} \text{Ax}}{E, B, B \wedge C \vdash C} \wedge\text{-l} \quad \frac{\overline{E \vdash B, E, C} \text{Ax}}{E \vdash B \vee E, B, C} \vee\text{-r}}{\frac{E, B \vdash C}{E \vdash C} \uparrow\text{-l} \quad \frac{E \vdash B, C}{E \vdash B, C} \uparrow\text{-r}} \text{Cut}(B)$$

and may be completed by the rewrite rule $C \rightarrow C \vee E$.

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

We have shown how, by setting the right abstract canonical system structure on the proof space of a sequent calculus modulo, we can use abstract completion to recover the admissibility of Cut. This abstract completion is precise enough to be operational, and it is actually implemented. It also reveals a deep logical correspondence between the sequent calculus, proof orderings and completion. This opens many questions that we are now considering.

The ordering on proofs we are using is adapted to consider cut-freeness as a normal-form property of an ACS, but produces too much critical proofs, in particular in the case when quantifiers are involved, because some of the rules produced by the completion procedure subsumes other one. (For instance $A \rightarrow A \vee \exists x. P(x)$ subsumes $A \rightarrow A \vee P(t)$ 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. We have to check what results this procedure will give on system that are proved to admits Cut, like Higher Order Logic (Dowek, Hardin, and Kirchner, 2001) or arithmetic (Dowek and Werner, 2005).

Lastly, our procedure only guarantees the admissibility of Cut, not the normalization. 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. In other words, we do not have a process that transform proofs with cuts to cut-free ones. We probably have to introduce some simplification rules in order to suppress the possibility to build non-normalizing proofs.

Moreover, with such simplification rules, we may obtain the canonical presentation of the system.

References

- Marc Aiguier, Clément Boin, and Delphine Longuet. On generalized theorems for normalization of proofs. Technical report, LaMI - CNRS and Université d'Evry Val d'Essonne, 2005.
- Henk Barendregt and Erik Barendsen. Autarkic computations in formal proofs. *Journal of Automated Reasoning*, 28(3):321–336, 2002.
- Maria Paola Bonacina and Nachum Dershowitz. Abstract canonical inference. *ACM Trans. Comput. Logic*, 8(1), 2007. ISSN 1529-3785.
- Richard Bonichon. TaMeD: A tableau method for deduction modulo. In David A. Basin and Michaël Rusinowitch, editors, *IJCAR*, volume 3097 of *Lecture Notes in Computer Science*, pages 445–459. Springer-Verlag, 2004. ISBN 3-540-22345-2.
- Guillaume Burel and Claude Kirchner. Completion is an instance of abstract canonical system inference. In Kōkichi Futatsugi et al., editors, *Algebra, Meaning and Computation*, volume 4060 of *Lecture Notes in Computer Science*, pages 497–520. Springer-Verlag, 2006.
- Marcel Crabbé. Non-normalisation de la théorie de Zermelo. Manuscript, 1974.
- N. Dershowitz. Orderings for term-rewriting systems. *Theoretical Computer Science*, 17:279–301, 1982.
- Nachum Dershowitz. Canonicity. In Ingo Dahn and Laurent Vigneron, editors, *FTP*, volume 86 of *Electronic Notes in Theoretical Computer Science*. Elsevier Science Publishers B. V. (North-Holland), 2003.
- Nachum Dershowitz and Claude Kirchner. Abstract saturation-based inference. In *LICS*, pages 65–74. IEEE Computer Society, 2003. ISBN 0-7695-1884-2.
- Nachum Dershowitz and Claude Kirchner. Abstract Canonical Presentations. *Theoretical Computer Science*, 357:53–69, 2006.
- Gilles Dowek. What is a theory? In Helmut Alt and Afonso Ferreira, editors, *STACS*, volume 2285 of *Lecture Notes in Computer Science*, pages 50–64. Springer-Verlag, 2002. ISBN 3-540-43283-3.
- Gilles Dowek. Confluence as a cut elimination property. In Robert Nieuwenhuis, editor, *RTA*, volume 2706 of *Lecture Notes in Computer Science*, pages 2–13. Springer-Verlag, 2003. ISBN 3-540-40254-3.
- Gilles Dowek, Thérèse Hardin, and Claude Kirchner. HOL- $\lambda\sigma$ an intentional first-order expression of higher-order logic. *Mathematical Structures in Computer Science*, 11(1):1–25, 2001.

- Gilles Dowek, Thérèse Hardin, and Claude Kirchner. Theorem proving modulo. *Journal of Automated Reasoning*, 31(1):33–72, 2003. ISSN 0168-7433.
- Gilles Dowek and Benjamin Werner. Proof normalization modulo. *The Journal of Symbolic Logic*, 68(4):1289–1316, 2003.
- Gilles Dowek and Benjamin Werner. Arithmetic as a theory modulo. In Jürgen Giesl, editor, *RTA*, volume 3467 of *Lecture Notes in Computer Science*, pages 423–437. Springer-Verlag, 2005. ISBN 3-540-25596-6.
- Jean H. Gallier. *Logic for Computer Science: Foundations of Automatic Theorem Proving*, volume 5 of *Computer Science and Technology Series*. Harper & Row, New York, 1986. Revised On-Line Version (2003), <http://www.cis.upenn.edu/~jean/gbooks/logic.html>.
- Gerhard Gentzen. Untersuchungen über das logische Schliessen. *Mathematische Zeitschrift*, 39:176–210, 405–431, 1934. Translated in Szabo, editor., *The Collected Papers of Gerhard Gentzen* as “Investigations into Logical Deduction”.
- J.-Y. Girard, Y. Lafont, and P. Taylor. *Proofs and Types*, volume 7 of *Cambridge Tracts in Theoretical Computer Science*. Cambridge University Press, 1989.
- Olivier Hermant. A model-based cut elimination proof. In *2nd St-Petersburg Days of Logic and Computability*, 2003.
- Olivier Hermant. *Méthodes Sémantiques en Dédution Modulo*. PhD thesis, École Polytechnique, 2005a.
- Olivier Hermant. Semantic cut elimination in the intuitionistic sequent calculus. In Pawel Urzyczyn, editor, *TLCA*, volume 3461 of *Lecture Notes in Computer Science*, pages 221–233. Springer-Verlag, 2005b. ISBN 3-540-25593-1.
- Donald E. Knuth and P. B. Bendix. Simple word problems in universal algebras. In J. Leech, editor, *Computational Problems in Abstract Algebra*, pages 263–297. Pergamon Press, Oxford, 1970.
- G. Peterson and M. E. Stickel. Complete sets of reductions for some equational theories. *Journal of the ACM*, 28:233–264, 1981.
- Benjamin Wack. *Typage et Dédution dans le Calcul de Réécriture*. PhD thesis, Université Henri Poincaré – Nancy 1, 2005.