Cut Elimination in Deduction Modulo by Abstract Completion

Guillaume Burel, Claude Kirchner

Cut Elimination in Deduction Modulo by Abstract Completion

Guillaume Burel[1] and Claude Kirchner[2]

[1] Université Henri Poincaré & LORIA[3]
[2] INRIA & LORIA[3]
[3] UMR 7503 CNRS-INPL-INRIA-Nancy2-UHP

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 has been shown to be 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. Moreover, we prove that it is even undecidable.
To recover this crucial property, computation rules can be added following the classical idea of completion *a la* Knuth and Bendix on terms. But of course in this case the objects are much more elaborated and it becomes essential to use an abstract framework which in our case is the *abstract canonical systems* one.
We show how, under appropriate hypothesis, the sequent calculus modulo can be seen as an instance of abstract canonical systems and that therefore, cuts correspond to critical proofs that abstract completion allows us to eliminate.
In addition to a deeper understanding of the interaction between deduction and computation and of the expressive power of abstract canonical systems, this provides a mechanical way to transform a sequent calculus modulo a given proposition rewrite system into an equivalent one having the cut elimination property, therefore extending in a significant way the applicability of mechanized proof search in deduction modulo.

1 Introduction

The complementarity and interaction between computation and deduction is known since at least Henri Poincaré and deduction modulo [14] 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 [24, 2, 14, 4]) 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 [12].

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 [6] (see for instance [14]). But we know that this cut-elimination property is fundamental for at least two related reasons: first, if a system has the cut-elimination property, then the formulæ needed to build a sequent calculus proof of some sequent are subformulæ[4] of the ones appearing in it, so that the search space is, in a sense, limited. Such proofs are sometimes called *analytic* [12]. The tableaux method is based on this fact, and for instance TaMeD [4], 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 [21] that a proof search method for deduction modulo like ENAR [14]—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-elimination property holds.

So on the one hand, we like to have a powerful congruence but this may be at the price of loosing cut-elimination. How can we get both? It has been shown in [12] that cut-elimination 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-elimination 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 in [11], based on the construction of a model for the theory associated with the rewrite system.

To solve this question, including a limited use of quantifiers, we use here a quite different approach based on the notion of abstract canonical system and inference introduced in [10, 3]. 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 [8] and standard (a.k.a. Knuth-Bendix [23]) completion [5].

To present the general idea of our approach, let us consider the simple example of Crabbé's axiom [6] $A \Leftrightarrow B \wedge \neg A$[5]. 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 Prop. 4 that such a proof, in its simplest form, is necessarily of the shape:

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

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

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

where the rules labeled "↑-r" and "↑-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:

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

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

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

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:

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

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

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

has the cut-elimination property and 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;
– We establish the boundaries of our approach by proving the undecidability of cut-elimination and of the search for critical proofs;

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 states the undecidability of the cut-elimination 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 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. All proofs will be found in the appendix.

2 Prerequisites

2.1 Rewritings

We define here how propositions are rewritten in deduction modulo.

We use standard definitions for terms, predicates, propositions (with connectors $\neg, \Rightarrow, \wedge, \vee$ and quantifiers $\forall, \exists$), substitutions, term rewrite rules and term rewriting, as can be found in [1, 17]. The set of terms built from a signature Σ and a set of variables V is denoted by $\mathcal{T}(\Sigma, V)$, the replacement of a variable x by a term t in a proposition P by $\{t/x\}P$, the application of a substitution σ in a proposition P by σP.

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

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. 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 $B \to Q$ 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 [14], because this can be simulated in the sequent calculus modulo we present in the next section.

Identity Group: $\dfrac{}{\Gamma, P \vdash P, \Delta}\ \mathsf{Axiom}$ $\qquad$ $\dfrac{\Gamma, P \vdash \Delta \quad \Gamma \vdash P, \Delta}{\Gamma \vdash \Delta}\ \mathsf{Cut}(P)$

Logical Rules: $\dfrac{\Gamma, \neg P \vdash P, \Delta}{\Gamma, \neg P \vdash \Delta}\ \neg\text{-}\mathsf{l}$ $\qquad$ $\dfrac{\Gamma \vdash \exists x.\ P, \{t/x\}P, \Delta}{\Gamma \vdash \exists x.\ P, \Delta}\ \exists\text{-}\mathsf{r},\ t \in \mathcal{T}(\Sigma, V)$

Rewrite Rules: if A can be rewritten to P, either by a term or a proposition rewrite rule (in one step),

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

Fig. 1. Sequent calculus modulo

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 [18]. We will use the denominations of [17].

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 $x_1, \ldots, x_n$ are the free variables of Γ, Δ, we will denote by $\mathcal{P}(\Gamma \vdash \Delta)$ the proposition $\forall x_1, \ldots, x_n.\ (\bigwedge \Gamma \Rightarrow \bigvee \Delta)$.

In Fig. 1 we present some inference rules of our *sequent calculus modulo*. They differ from the ones of [12] because the congruence is externalized through specific inference rules $\uparrow$-l and $\uparrow$-r (as can be found in [21]), whereas contraction is internalized. The other logical rules are the one of the standard sequent calculus where the principal proposition is contracted before application. *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 use only rules that appear in $R \cup R_{\mathcal{T}(\Sigma,V)}$. The set of all proofs will be denoted by $\mathcal{SQM}$.

$\mathsf{Cut}(P)$ 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 have the *cut elimination property* 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 [18], or more accuratly [12] because of $R_{\mathcal{T}(\Sigma,V)}$) that $\emptyset$ has the cut-elimination property.

It is important to be aware that free variables appearing in a sequent 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 in [14, 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 $\Gamma \vdash P, P, \Delta$.

Proposition 1 (Equivalence). *The sequent calculus modulo (partly) presented in Fig. 1 is equivalent to the Asymmetric Sequent Calculus Modulo of [12].*

Our system also satisfies the Kleene Lemma:

Lemma 1 (Kleene Lemma [21, Lemme 3.3]).

If $\Gamma, P \vdash \Delta$ has a proof (resp. cut-free proof) in R, where P is neither atomic nor of the form $\forall x.\ Q$, then there exists a proof (resp. cut-free proof) in R of the same sequent whose first rule is a logical rule with principal proposition P.

If $\Gamma \vdash P, \Delta$ has a proof (resp. cut-free proof) in R, where P is neither atomic nor of the form $\exists x.\ Q$, then there exists a proof (resp. cut-free proof) in R of the same sequent whose first rule is a logical rule with principal proposition P.

We prove also the following new result:

Theorem 1 (Undecidability of the Cut Elimination Property). *Given a propositional rewrite system $\mathcal{R}$, it is undecidable to know if $\mathcal{R}$ has the cut-elimination property.*

2.3 Abstract Canonical Systems and Inference

The results in this section are extracted from [9, 10, 3], 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: $[\cdot]^{Pm} : \mathbb{P} \to 2^{\mathbb{A}}$ 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 $A \subseteq \mathbb{A}$ is denoted by

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

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). 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:

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

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 $p \trianglerighteq q \Rightarrow p = q$, 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 $\widehat{A}$ 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 (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:

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

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

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

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

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

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

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 $A_0 \rightsquigarrow A_1 \rightsquigarrow \cdots$ is called a *derivation*. The *result* of the derivation is, as usual, its *persisting* formulæ:

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

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

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

Theorem 2 ([3, Lemma 5.13]). *A deduction mechanism is completing if and only if for all derivations $A_0 \rightsquigarrow A_1 \rightsquigarrow \cdots$,*

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

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

$$Crit(A) \quad \stackrel{!}{=} \quad \{p \in \mu Pf(A) \setminus Nf(A) : \forall q \in Pf(A).\ p \rhd q \Rightarrow q \in Nf(A)\}$$

Completing formulæ are conclusions of proofs smaller than critical proofs:

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

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

$$A \rightsquigarrow A \cup \mathsf{C}(A)$$

where $Comp(A) \subseteq \mathsf{C}(A) \subseteq Th\, A$.

Proposition 2 ([9, 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 $Rew : \mathcal{S} \to \mathcal{PRS}$ 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, $P \xleftrightarrow[R]{*} Q$ 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 [14], which is the same except that we need here a *cut-free* proof in b).

Section 4.3 provides an instance of such a function Rew, but only for a restricted set of sequents.

With respect to the definitions of ACSs (see Sect. 2.3) 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:

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

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

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

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

— 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,

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

— 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,

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

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 formulæ P, Q, if P is greater than Q for the subformula relation, then $\mathsf{Cut}(P) > \mathsf{Cut}(Q)$, and for all other inference rules r of Fig. 1, $\mathsf{Cut}(P) > \mathsf{r}$.

We order proofs using the RPO [7] based on this precedence. Since the precedence is well-founded, so is the RPO [7]. 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 $\uparrow$-l or $\uparrow$-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 $\mathbb{P} \cup \widehat{\mathbb{A}}$, where formulæ 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 $\mathbb{P} \cup \widehat{\mathbb{A}}$ is the same relation as $>$ over the original $\mathbb{P}$.)

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

$$p \trianglerighteq q \quad \text{if } - \; q \text{ is a subproof modulo weakening of } p \text{ in } \mathcal{SQM}, \text{ or}$$
$$- \text{ if } q = \widehat{a} \text{ with } a \in [p]^{Pm}.$$

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 3 (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* $\rhd$ *given above.*

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 which has the cut-elimination property.

4.1 Normal-form Proofs and Critical Proofs in Deduction Modulo

Proposition 3 (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.*

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

Proposition 4 (Critical Proofs in Deduction Modulo). *Critical proofs in deduction modulo are of the form*

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

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

Note 1. If we suppose, as in the order condition of [22], 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 cut-elimination property is verified.

The main difference with [22] is that Hermant gives a semantic proof of the cut-elimination property, 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 in [15] that such an order condition provides normalization in the quantifier-free case.

4.2 The Completion Procedure

As we wrote in Sect. 2.3, we want to define a completing deduction mechanism by adding to a presentation A a presentation $\mathsf{C}(A)$ such that $Comp(A) \subseteq \mathsf{C}(A) \subseteq Th\ A$. So we have to find proofs smaller than critical proofs. Here, using Property 1(b) and Lemma 1, we can find for all sequents $\Gamma \vdash \Delta$ a cut-free proof in $Rew(\Gamma \vdash \Delta)$ with conclusion $\Gamma \vdash \Delta$, which will be smaller than any proof containing a cut proving the same sequent, in particular any critical proof. The premises of this proof are in $Rew(\Gamma \vdash \Delta) = [p]_{Cl}$. The best procedure is thus to add only the conclusions of critical proofs. Nevertheless, it is not possible:

Theorem 4 (Undecidability of Critical Proof Search). *Given a propositional rewrite system R and a sequent $\Gamma \vdash \Delta$, it is undecidable to know if $\Gamma \vdash \Delta$ is the conclusion of a critical proof in R.*

We must therefore add a superset of these conclusions. Here we will add the conclusion of the proofs in the form of Proposition 4, 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 4. 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 [4], 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 5 (Cut-Elimination 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_∞.*

4.3 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.

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:

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

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

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

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

$P_1, \ldots, P_n \vdash A$ " $A \to A \vee \exists x_1, \ldots, x_p.\ (P_1 \wedge \cdots \wedge P_n)$

(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 $P_2 \vdash Q_1, \ldots, Q_m$; $\neg P_1 \vdash Q_1, \ldots, Q_m$

$A \vdash Q_1, \ldots, Q_m$ " $A \to A \wedge \forall x_1, \ldots, x_p.\ (Q_1 \vee \cdots \vee Q_m)$

(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.

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 subformulæ, 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 $\{\Gamma \vdash \Delta\}$.

Proposition 5. *The function Rew has the Properties 1 and 2.*

This algorithm can be extended to a certain limit to the case with quantifiers, in particular when for each sequent, at least one formula of the left part of the sequent is a member of grammar L, or one formula of the right part of the sequent is a member of grammar R, where:

$$\begin{array}{rcl} R & \stackrel{!}{=} & A \mid \neg L \mid R \wedge R \mid R \vee R \mid L \Rightarrow R \mid \forall x.\ R \\ L & \stackrel{!}{=} & A \mid \neg R \mid L \wedge L \mid L \vee L \mid R \Rightarrow L \mid \exists x.\ L \end{array} .$$

The formula chosen in step 2 must be in R, and the one chosen in step 3 must be in L. We also have to add the following decomposition steps:

- (2) $P_1, \ldots, P_n \vdash \forall x.\ Q$ becomes $P_1, \ldots, P_n \vdash \{y/x\}Q$ where y does not appear in $P_1, \ldots, P_n$;
- (3) $\exists x.\ P \vdash Q_1, \ldots, Q_m$ becomes $\{y/x\}P \vdash Q_1, \ldots, Q_m$ where y does not appear in $Q_1, \ldots, Q_m$.

We can show that the sets of sequents produced in each step belong to our restriction, and that this algorithm also has Properties 1 and 2.

This algorithm does not allow all rewrite systems to be considered as formulæ. Nevertheless, one can transform all rewrite systems to equivalent rewrite systems that are images of sequents by Rew, by splitting the rules: $A \to P$ becomes $A \to A \vee P$ and $A \to A \wedge P$. This is equivalent to the polarized rewrite systems of [11].

4.4 Examples

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

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

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

has the cut-elimination property.

The next example deals with quantifiers and is extracted from [22]:

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

where $y \simeq z \quad \stackrel{!}{=} \quad \forall x.\ (y \in x \Rightarrow z \in x)$. It is terminating and confluent, but does not have the cut-elimination property.

The critical proofs have the form

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

The left part can be developed as

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

and the right part as

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

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

$$\begin{cases} R \in R \ \to\ \forall y.\ y \simeq R \Rightarrow y \in R \Rightarrow C \\ C \to C \vee \top \end{cases}$$

has the cut-elimination property.

One can also think of another example, where free variables have to be looked at: one can think of a rule derived from Crabbé's example $A \to (\exists x.\ B \wedge P(x)) \wedge \neg A$ where A and B are atomic propositions, and P a predicate of arity 1. The conclusion of one of the critical proofs is $\exists x.\ B \wedge P(x) \vdash$. This leads to the rewrite rule $B \to B \wedge \forall x.\ \neg P(x)$.

5 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 cut-elimination property. This reveals a deep logical correspondence between the sequent calculus, proof orderings and completion. This also opens many questions that we are now considering.

For the completed proposition rewrite system, the cut-elimination property holds only for sequents that can be transformed into a rewrite system. We have to look further if this property does hold in fact for all sequents, or if we have to extend the notion of proposition rewriting. One way to do this may be to

allow rewriting not only on atomic propositions but also on some quantified propositions. We must in fact determine what theories can be defined using the original notion of proposition rewrite system, and how this notion could be extended to cover all first-order theories.

Moreover, the ordering on proofs we are using is adapted to consider cut-elimination 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 $A \to A \vee \exists x.\ P(x)$ subsumes $A \to A \vee P(t)$ 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 has the cut-elimination property. Indeed, if a proposition rewrite system is a fixpoint of this procedure, then we know that it has the cut-elimination property. 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 have the cut-elimination property, like Higher Order Logic [13] or arithmetic [16].

Lastly, our procedure only guarantees the cut-elimination property, 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 (as in standard completion) 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

1. Baader, F., Nipkow, T.: Term *Re*writing and *all That*. Cambridge University Press (1998)
2. Barendregt, H., Barendsen, E.: Autarkic computations in formal proofs. Journal of Automated Reasoning **28** (2002) 321–336
3. Bonacina, M.P., Dershowitz, N.: Abstract Canonical Inference. ACM Transactions on Computational Logic (2006) To appear.
4. Bonichon, R.: TaMeD: A tableau method for deduction modulo. In Basin, D.A., Rusinowitch, M., eds.: IJCAR. Volume 3097 of Lecture Notes in Computer Science., Springer-Verlag (2004) 445–459
5. Burel, G., Kirchner, C.: Completion is an instance of abstract canonical system inference. In Futatsugi, K., et al., eds.: Algebra, Meaning and Computation. Volume 4060 of Lecture Notes in Computer Science., Springer-Verlag (2006) 497–520
6. Crabbé, M.: Non-normalisation de la théorie de Zermelo. Manuscript (1974)
7. Dershowitz, N.: Orderings for term-rewriting systems. Theoretical Computer Science **17** (1982) 279–301
8. Dershowitz, N.: Canonicity. In Dahn, I., Vigneron, L., eds.: FTP. Volume 86 of Electronic Notes in Theoretical Computer Science., Elsevier Science Publishers B. V. (North-Holland) (2003)

9. Dershowitz, N., Kirchner, C.: Abstract saturation-based inference. In: LICS, IEEE Computer Society (2003) 65–74
10. Dershowitz, N., Kirchner, C.: Abstract Canonical Presentations. Theoretical Computer Science **357** (2006) 53–69
11. Dowek, G.: What is a theory? In Alt, H., Ferreira, A., eds.: STACS. Volume 2285 of Lecture Notes in Computer Science., Springer-Verlag (2002) 50–64
12. Dowek, G.: Confluence as a cut elimination property. In Nieuwenhuis, R., ed.: RTA. Volume 2706 of Lecture Notes in Computer Science., Springer-Verlag (2003) 2–13
13. Dowek, G., Hardin, T., Kirchner, C.: HOL-$\lambda\sigma$ an intentional first-order expression of higher-order logic. Mathematical Structures in Computer Science **11** (2001) 1–25
14. Dowek, G., Hardin, T., Kirchner, C.: Theorem proving modulo. Journal of Automated Reasoning **31** (2003) 33–72
15. Dowek, G., Werner, B.: Proof normalization modulo. The Journal of Symbolic Logic **68** (2003) 1289–1316
16. Dowek, G., Werner, B.: Arithmetic as a theory modulo. In Giesl, J., ed.: RTA. Volume 3467 of Lecture Notes in Computer Science., Springer-Verlag (2005) 423–437
17. Gallier, J.H.: 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`.
18. Gentzen, G.: 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".
19. Girard, J.Y., Lafont, Y., Taylor, P.: Proofs and Types. Volume 7 of Cambridge Tracts in Theoretical Computer Science. Cambridge University Press (1989)
20. Hermant, O.: A model-based cut elimination proof. In: 2nd St-Petersburg Days of Logic and Computability. (2003)
21. Hermant, O.: Méthodes Sémantiques en Déduction Modulo. PhD thesis, École Polytechnique (2005)
22. Hermant, O.: Semantic cut elimination in the intuitionistic sequent calculus. In Urzyczyn, P., ed.: TLCA. Volume 3461 of Lecture Notes in Computer Science., Springer-Verlag (2005) 221–233
23. Knuth, D.E., Bendix, P.B.: Simple word problems in universal algebras. In Leech, J., ed.: Computational Problems in Abstract Algebra. Pergamon Press, Oxford (1970) 263–297
24. Peterson, G., Stickel, M.E.: Complete sets of reductions for some equational theories. Journal of the ACM **28** (1981) 233–264

A Proofs of Sect. 2

Proposition 1 (Equivalence). *The sequent calculus modulo (partly) presented in Fig. 1 is equivalent to the Asymmetric Sequent Calculus Modulo of [12].*

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, since it is integrated in every of our inference rules (except of course the identity group).

Then, one can show that for a proposition rewrite rule $A \to P$, 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 $A \to P$, 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 $\uparrow$-l and $\uparrow$-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. □

The reader should consult [20] for the definitions of the terms in the next proposition:

Proposition 6 (Condition for Cut Elimination [20, 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 $A \to P \in \mathcal{R}$, A and P have the same interpretation, then $\mathcal{R}$ has the cut elimination property.

Theorem 1 (Undecidability of the Cut Elimination Property). *The problem*

Input: A propositional rewrite system $\mathcal{R}$
Decide if $\mathcal{R}$ has the cut-elimination property.

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 in such a language.

Let R be a constant and $\in$ a 2-ary predicate not appearing in P. Consider the propositional rewrite system (inspired from [22])

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

Then one can show that P is valid if and only if $\mathcal{R}$ has the cut elimination property.

If P is valid, then define a model as in [21, 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 [21, Section 8.3] to prove the cut elimination property, 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 [21, Section 8.1], replacing C by P. Consequently, $\mathcal{R}$ has not the cut-elimination property.

□

B Proof of Theorem 3

Theorem 3 (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 $\rhd$ given in Sect. 3.*

Proof.

– Postulate A: suppose $R \in A$, we want to show that R is the conclusion of a proof built with A. Because $R \in \mathbb{A} = Rew(\mathcal{S})$, there exists some sequent $\Gamma \vdash \Delta$ such that $Rew(\Gamma \vdash \Delta) = R$. Using Property 1b), we know that there is a proof of $\mathcal{P}(\Gamma \vdash \Delta)$ in R. As a consequence of Lemma 1, we know that there is a proof of $\Gamma \vdash \Delta$ in R, i.e. a proof in A proving $Rew(\Gamma \vdash \Delta) = R$. (Remember that free variables can be treated as fresh constants in the construction of a proof.)

– Postulate B: let R be in $Th\,Th\,A$. By definition there is a proof $p \in Pf(Th\,A)$ such that $[p]_{Cl} = Rew(\Gamma \vdash \Delta) = R$ for some sequent $\Gamma \vdash \Delta$. Let R' be the rewrite system used in p, therefore $R' \in [p]^{Pm} \subseteq Th\,A$. By definition, there is a proof $q \in Pf(A)$ such that $[q]_{Cl} = Rew(\Gamma' \vdash \Delta') = R'$ 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 [14], 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

$$\dfrac{\dfrac{\begin{array}{c}\vdots\\ r\end{array}}{\Gamma, \mathcal{P}(\Gamma' \vdash \Delta') \vdash \Delta} \quad \dfrac{\dfrac{\begin{array}{c}\vdots\\ q\end{array}}{\Gamma, \sigma\Gamma' \vdash \sigma\Delta', \Delta}}{\Gamma \vdash \mathcal{P}(\Gamma' \vdash \Delta'), \Delta}\ \mathsf{Logical\ rules}}{\Gamma \vdash \Delta}\ \mathsf{Cut}(\mathcal{P}(\Gamma' \vdash \Delta'))$$

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

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

– Postulate D: suppose $p \trianglerighteq q$. 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 $q = \widehat{a}$ with $a \in [p]^{Pm}$, $[q]^{Pm} = \{a\} \subseteq [p]^{Pm}$.

– Postulate E: suppose $p \rhd q > r$. 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, $p > v$.

□

C Proofs of Sect. 4

C.1 Normal-form and Critical Proofs, Cut-elimination of the Limit

Proposition 3 (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 1 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 $Pf(Th\,A)$, so that it is in normal form. □

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

Proposition 4 (Critical Proofs in Deduction Modulo). *Critical proofs in deduction modulo are of the form*

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

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

Proof. We essentially follow the proof of the Hauptsatz of [19, Chapter 13].

Because of Proposition 3, 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

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

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

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 [19] (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 $\dfrac{}{\Gamma \vdash \Delta}\ \mathsf{Axiom}$ which is smaller than the initial proof, contradicting its minimality.
2. $\mathsf{r'}$ 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

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

   is smaller than the initial proof, contradicting its minimality.
4. $\mathsf{r'}$ is a logical rule other than a right one with principal formula P. This case is handled as case 3.
5. Both r and $\mathsf{r'}$ are logical rules, r a left one and $\mathsf{r'}$ a right one, of principal proposition P. This is one of the key cases as given in Section 13.1 of [19] : 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

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

   is greater than the proof

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

6. r or $\mathsf{r'}$ 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 $\mathsf{r'}$ 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 $\mathsf{r'}$ is a rewrite rule, both applying to P. This case is handled as case 7.
9. r and $\mathsf{r'}$ are both rewrite rules applying to P. Therefore P has to be atomic, and is rewritten by $P \to P_1$ to the left and $P \to P_2$ 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

$$\dfrac{\dfrac{\vdots\,\pi_1}{\Gamma, P_1 \vdash \Delta} \qquad \dfrac{\dfrac{\dfrac{}{\Gamma, P' \vdash P', \Delta}\,\mathsf{Axiom}}{\Gamma, P_2 \vdash P_1, \Delta}\,\mathsf{Rewrite\ Rules} \quad \dfrac{\vdots\,\varpi'_1}{\Gamma \vdash P_1, P_2, \Delta}\,\mathsf{Cut}(P_2)}{\Gamma \vdash P_1, \Delta}\,\mathsf{Cut}(P_1)}{\Gamma \vdash \Delta}$$

   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.

□

Theorem 4 (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:

$$\begin{cases} A \to A \wedge B \\ A \to A \vee P \end{cases} .$$

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

$$\dfrac{\dfrac{\dfrac{\dfrac{}{A, B \vdash B}\,\mathsf{Axiom}}{A, A \wedge B \vdash B}\,\wedge\text{-}\mathsf{l}}{A \vdash B}\,\uparrow\text{-}\mathsf{l} \qquad \dfrac{\dfrac{\text{Proof of } P \text{ in } \emptyset}{\vdash P, A, B}}{\vdash A \vee P, A, B}\,\vee\text{-}\mathsf{r}}{\vdash A, B}\,\uparrow\text{-}\mathsf{r}}{\vdash B}\,\mathsf{Cut}(A)$$

□

Theorem 5 (Cut-Elimination 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 2, we know that R_∞ is complete, and therefore by Lemma 2

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

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 3 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. □

C.2 Proof of Proposition 5

We first prove Property 1 using three lemmata.

Lemma 2. *If the sequent $\Gamma \vdash \Delta$ is transformed to the set of sequents $\{\Gamma' \vdash \Delta'\} \cup S'$ by the algorithm described in Sect. 4.3, 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, $P_1, \ldots, P_n \vdash Q_1 \wedge Q_2$ 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):

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{}{Q_1, Q_2 \vdash Q_1}\,\mathsf{Axiom}}{Q_1 \wedge Q_2 \vdash Q_1}\,\wedge\text{-}\mathsf{l} \qquad \dfrac{}{\bigwedge_i P_i \vdash \bigwedge_i P_i}\,\mathsf{Axiom}}{\bigwedge_i P_i \Rightarrow (Q_1 \wedge Q_2), \bigwedge_i P_i \vdash Q_1}\,\Rightarrow\text{-}\mathsf{l}}{\{c_i/x_i\} \bigwedge_i P_i \Rightarrow (Q_1 \wedge Q_2) \vdash \{c_i/y_i\} \bigwedge_i P_i \Rightarrow Q_1}\,\Rightarrow\text{-}\mathsf{r}}{\forall x_1, \ldots, x_n.\ (\bigwedge_i P_i \Rightarrow (Q_1 \wedge Q_2)) \vdash \{c_i/y_i\}(\bigwedge_i P_i \Rightarrow Q_1)}\,\forall\text{-}\mathsf{l}}{\forall x_1, \ldots, x_n.\ (\bigwedge_i P_i \Rightarrow (Q_1 \wedge Q_2)) \vdash \forall y_1, \ldots, y_m.\ (\bigwedge_i P_i \Rightarrow Q_1)}\,\forall\text{-}\mathsf{r}$$

where c_i are fresh constants. □

Lemma 3. *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*

$$\mathcal{P}(P_1, \dots, P_n \vdash A) \vdash A \Leftrightarrow A \vee \exists x_1, \dots, x_p.\ \bigwedge_i P_i$$

$$\mathcal{P}(A \vdash P_1, \dots, P_n) \vdash A \Leftrightarrow A \wedge \forall x_1, \dots, x_p.\ \bigvee_i P_i$$

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):

$$\dfrac{\dfrac{\dfrac{}{\forall y_1, \dots, y_m.\ (\bigwedge_i P_i \Rightarrow A), A \vdash A, \exists x_1, \dots, x_p.\ \bigwedge_i P_i}\ \text{Axiom}}{\forall y_1, \dots, y_m.\ (\bigwedge_i P_i \Rightarrow A), A \vdash A \vee \exists x_1, \dots, x_p.\ \bigwedge_i P_i}\ \vee\text{-r}}{\forall y_1, \dots, y_m.\ (\bigwedge_i P_i \Rightarrow A) \vdash A \Rightarrow A \vee \exists x_1, \dots, x_p.\ \bigwedge_i P_i}\ \Rightarrow\text{-r} \tag{2}$$

$$\dfrac{\dfrac{\dfrac{\dfrac{}{A \vdash A}\ \text{Axiom} \quad \dfrac{\dfrac{}{\sigma \bigwedge_i P_i \vdash \sigma \bigwedge_i P_i}\ \text{Axiom}}{\sigma(\bigwedge_i P_i \Rightarrow A), \sigma \bigwedge_i P_i \vdash A}\ \Rightarrow\text{-l}}{\forall y_1, \dots, y_m.\ (\bigwedge_i P_i \Rightarrow A), \sigma \bigwedge_i P_i \vdash A}\ \forall\text{-l}}{\dfrac{\dfrac{}{A \vdash A}\ \text{Axiom} \quad \forall y_1, \dots, y_m.\ (\bigwedge_i P_i \Rightarrow A), \exists x_1, \dots, x_p.\ \bigwedge_i P_i \vdash A}\ \exists\text{-l}}{\forall y_1, \dots, y_m.\ (\bigwedge_i P_i \Rightarrow A), A \vee \exists x_1, \dots, x_p.\ \bigwedge_i P_i \vdash A}\ \vee\text{-l}}{\forall y_1, \dots, y_m.\ (\bigwedge_i P_i \Rightarrow A) \vdash A \vee \exists x_1, \dots, x_p.\ \bigwedge_i P_i \Rightarrow A}\ \Rightarrow\text{-r} \tag{3}$$

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

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. □

Lemma 4. *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 $A \to A \vee \exists x_1, \dots, x_p.\ (P_1 \wedge \dots \wedge P_n)$, and the sequent

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

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

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:

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

□

We can prove Property 2 using the following lemma:

Lemma 5. *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. 4.3, 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 1.

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 1 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. □

We can now prove the main result of this subsection:

Proposition 5. *The Rew function defined in Sect. 4.3 has the Properties 1 and 2.*

Proof. We proceed by induction on the execution of the algorithm of Sect. 4.3

For Property 1a), one can restrict oneself to one step rewrite for $P \xleftrightarrow[R]{*} Q$. Lemma 3 permits to prove the property at the end of the algorithm, when sequents are transformed into rules. Lemma 2 permits to prove the inductive case: suppose $\Gamma \vdash \Delta$ is transformed into $\{\Gamma' \vdash \Delta'\} \cup \cdots$. Suppose $\mathcal{P}(\Gamma' \vdash \Delta') \vdash A \Leftrightarrow P$ has a proof p without rewrite rules. By Lemma 2, there is a proof q of $\mathcal{P}(\Gamma \vdash \Delta) \vdash \mathcal{P}(\Gamma' \vdash \Delta')$. Therefore, we can construct the proof

$$\dfrac{\begin{array}{cc}\overset{p}{\vdots} & \overset{q}{\vdots} \\ \mathcal{P}(\Gamma \vdash \Delta), \mathcal{P}(\Gamma' \vdash \Delta') \vdash A \Leftrightarrow P & \mathcal{P}(\Gamma \vdash \Delta) \vdash \mathcal{P}(\Gamma' \vdash \Delta'), A \Leftrightarrow P\end{array}}{\mathcal{P}(\Gamma \vdash \Delta) \vdash A \Leftrightarrow P}\ \mathsf{Cut}(\mathcal{P}(\Gamma' \vdash \Delta'))$$

without rewrite rules.

For Property 1b), the base case a consequence of Lemma 4, whereas the inductive case is a consequence of Lemma 1. 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 1, 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

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

in $R_1 \cup R_2$.

For Property 2, the base case is trivial, and the inductive case is a consequence of Lemma 5. □