Consistency Implies Cut Admissibility

Guillaume Burel

Consistency Implies Cut Admissibility

Guillaume Burel

Énsiie/Cédric, 1 square de la résistance, 91025 Évry cedex, France
guillaume.burel@ensiie.fr   http://www.ensiie.fr/~guillaume.burel/

Abstract. For any finite and consistent first-order theory, we can find a presentation as a rewriting system that enjoys cut admissibility.

Since proofs are rarely built without context, it is essential to develop methods that are adapted to search for proofs in theories. For instance, SMT provers provide efficient tools. Nevertheless, they are restricted to some particular theories, such as linear arithmetic or arrays. We would like to have a generic and automated way of obtaining efficient methods for a given theory, provided it is consistent. A naive idea is to use an axiomatic presentation of the theory, but it is now folklore that this is not efficient enough. The theory should therefore be presented in a more effective manner. One solution is, starting from the axiomatic presentation, to automatically design a deductive system that is adapted to the theory. In [23], Negri and van Plato turn variable-free axioms into non-logical deduction rules that are added to a sequent calculus. Similarly, [10] transforms a large class of axioms into inference rules in sequent and hypersequent calculi. Deduction modulo [15] is a bit different: it presents the theory as computation, by means of a rewriting system, and the inference rules of an existing deductive system (natural deduction, sequent calculus, etc.) are applied modulo the congruence associated with this rewriting system. We have shown in [7] that presenting theories as rewriting systems improves indeed the search for proofs in the theory. If one wants these presentations to behave well, they should have the following proof-theoretical property: the cut rule must be admissible. Indeed, in the usual setting, cut admissibility implies the consistency of the theory, the subformula property (to find a proof, one can restrict oneself to the subformulas of the formula to be proved), the existence of proof normal forms, etc. Systems produced by [23, 10] all have the cut admissibility. However, in deduction modulo, it depends on the considered rewriting system. The question is: knowing that the theory is consistent, is it possible to present it as a rewriting system such that cut admissibility holds in deduction modulo? A presentation as a rewriting system with the cut admissibility was given for particular theories, such as arithmetic [17], simple type theory [14], and Zermelo's set theory [16]. Dowek designed a systematic way of transforming a consistent *propositional* theory into such a rewriting system, using a model of the theory. In [9], we gave a semi-algorithm that can handle any first-order theory: first, it produces a rewriting system that corresponds to the theory; second, it completes the rewriting system to ensure the cut admissibility. It is the second part that may not terminate. In this paper, we give a simple way to present any first-order theory as a rewriting system with cut admissibility. This is done by developing a recent characterization [8] of an extension of the resolution method based on deduction modulo as a combination of the set-of-support strategy [26] and selection of literals.

In the two next sections, we briefly present deduction modulo and refinements of resolution. Section 3 describes how a theory can be presented as a rewriting system, and why cut admissibility is implied by its consistency. As the rewriting system that is produced is too big in practice, we are led to restrict the number of rules are proposed in Section 4. We conclude by discussing further works.

1 Deduction Modulo

We use standard definitions for terms, predicates, propositions (with connectives $\neg, \Rightarrow, \wedge, \vee$ and quantifiers $\forall, \exists$), sequents, substitutions, term rewriting rules and term rewriting, as can be found in [1, 18] . The substitution of a variable x by a term t in a term or a proposition A is denoted by $\{t/x\}A$, and more generally the application of a substitution σ in a term or a proposition A by σA. A term t can be narrowed into s using substitution σ at position $\mathfrak{p}$ ($t \overset{\mathfrak{p},\sigma}{\rightsquigarrow} s$) if σt can be rewritten to s using substitution σ at position $\mathfrak{p}$. A literal is an atomic proposition or the negation of an atomic proposition. A proposition is in clausal form if it is the universal quantification of a disjunction of literals $\forall x_1, \ldots, x_n.\ L_1 \vee \ldots \vee L_p$ where $x_1, \ldots, x_n$ are the free variables of $L_1, \ldots, L_p$. In the following, we will often omit to write the quantifications, and we will identify propositions in clausal form with clauses (i.e. set of literals) as if $\vee$ was associative, commutative and idempotent. $\Box$ represents the empty clause. The polarity of a position in a proposition can be defined as follows: the root is positive, and the polarity switches when going under a $\neg$ or on the left of a $\Rightarrow$.

In deduction modulo, term rewriting and narrowing is extended to propositions by congruence on the proposition structure. In addition, there are also proposition rewriting rules whose left-hand side is an atomic proposition and whose right-hand side can be any proposition. Such rules can also be applied to non-atomic propositions by congruence on the proposition structure. We call a rewriting system the combination of a term rewriting system and a proposition rewriting system. Given a rewriting system $\mathcal{R}$, we denote by $A \underset{\mathcal{R}}{\longrightarrow} B$ the fact that A is rewritten in one step in B, either by a term rewriting rule or by a proposition rewriting rule, and by $A \underset{\mathcal{R}}{\rightsquigarrow} B$ the fact that A is narrowed to B. $\overset{*}{\underset{\mathcal{R}}{\longrightarrow}}$ is the reflexive transitive closure of $\underset{\mathcal{R}}{\longrightarrow}$.

Deduction modulo consists in applying the inference rules of an existing proof system modulo such a rewriting system. This leads for instance to the asymmetric sequent calculus modulo [12], some of whose rules are presented in Figure 1.

Example 1. Consider the rewriting rule $A \subseteq B \to \forall x.\ x \in A \Rightarrow x \in B$. We can build the following proof of the transitivity of the inclusion in the asymmetric sequent calculus modulo this rule:

$$\overset{\frown}{\vdash}\ \frac{}{\Gamma, A \vdash B, \Delta}\ A \xrightarrow[\mathcal{R}]{*} C \xleftarrow[\mathcal{R}]{*} B \qquad \underset{\smile}{\vdash}\ \frac{\Gamma, A \vdash \Delta \qquad \Gamma \vdash B, \Delta}{\Gamma \vdash \Delta}\ A \xleftarrow[\mathcal{R}]{*} C \xrightarrow[\mathcal{R}]{*} B$$

$$\Rightarrow\vdash\ \frac{\Gamma, B \vdash \Delta \qquad \Gamma \vdash A, \Delta}{\Gamma, C \vdash \Delta}\ C \xrightarrow[\mathcal{R}]{*} A \Rightarrow B \qquad \vdash\forall\ \frac{\Gamma \vdash A, \Delta}{\Gamma \vdash B, \Delta}\ \begin{array}{l} B \xrightarrow[\mathcal{R}]{*} \forall x.\ A \\ x \text{ not free in } \Gamma, \Delta \end{array}$$

Fig. 1. Some inference rules of the Asymmetric Sequent Calculus Modulo $\mathcal{R}$

$$\overset{\frown}{\vdash}\ \frac{}{\Gamma, A \vdash B, \Delta}\ A \xrightarrow[\mathcal{R}]{*}{}^{-} C\ {}^{+}\!\xleftarrow[\mathcal{R}]{*} B \qquad \underset{\smile}{\vdash}\ \frac{\Gamma, A \vdash \Delta \qquad \Gamma \vdash B, \Delta}{\Gamma \vdash \Delta}\ A\ {}^{-}\!\xleftarrow[\mathcal{R}]{*} C \xrightarrow[\mathcal{R}]{*}{}^{+} B$$

$$\Rightarrow\vdash\ \frac{\Gamma, B \vdash \Delta \qquad \Gamma \vdash A, \Delta}{\Gamma, C \vdash \Delta}\ C \xrightarrow[\mathcal{R}]{*}{}^{-} A \Rightarrow B \qquad \vdash\forall\ \frac{\Gamma \vdash A, \Delta}{\Gamma \vdash B, \Delta}\ \begin{array}{l} B \xrightarrow[\mathcal{R}]{*}{}^{+} \forall x.\ A \\ x \text{ not free in } \Gamma, \Delta \end{array}$$

Fig. 2. Some inference rules of the Polarized Sequent Calculus Modulo $\mathcal{R}$

$$\vdash\forall\ \dfrac{\vdash\Rightarrow\ \dfrac{\forall\vdash\ \dfrac{\Rightarrow\vdash\ \dfrac{\forall\vdash\ \dfrac{\Rightarrow\vdash\ \dfrac{\overset{\frown}{\vdash}\ \dfrac{}{x \in C \vdash x \in C} \qquad \overset{\frown}{\vdash}\ \dfrac{}{x \in B \vdash x \in B}}{x \in B \Rightarrow x \in C, x \in B \vdash x \in C}}{B \subseteq C, x \in B \vdash x \in C} \qquad \overset{\frown}{\vdash}\ \dfrac{}{x \in A \vdash x \in A}}{x \in A \Rightarrow x \in B, B \subseteq C, x \in A \vdash x \in C}}{A \subseteq B, B \subseteq C, x \in A \vdash x \in C}}{A \subseteq B, B \subseteq C \vdash x \in A \Rightarrow x \in C}}{A \subseteq B, B \subseteq C \vdash A \subseteq C}$$

A rewriting rule can be applied indifferently to the left- or the right-hand side of a sequent. Consequently, they can be considered semantically as an equivalence between their left- and right-hand side. To be able to consider implications, a polarized version of deduction modulo was introduced [11]. Proposition rewriting rules are tagged with a polarity $+$ or $-$; they are then called polarized rewriting rules. A proposition A is rewritten positively into a proposition B ($A \longrightarrow{}^{+} B$) if it is rewritten by a positive rule at a positive position or by a negative rule at a negative position. It is rewritten negatively ($A \longrightarrow{}^{-} B$) if it is rewritten by a positive rule at a negative position or by a negative rule at a positive position. Term rewriting rules are considered as both positive and negative. $\xrightarrow{*}{}^{\pm}$ is the reflexive transitive closure of $\longrightarrow{}^{\pm}$. This gives the polarized sequent calculus modulo, some of whose rules are presented in Figure 2.

Example 2. Consider the polarized rewriting system

$$\begin{aligned} A \subseteq B &\to^{-} \forall x.\ x \in A \Rightarrow x \in B \\ A \subseteq B &\to^{+} \neg \mathit{diff}(A, B) \in A \\ A \subseteq B &\to^{+} \mathit{diff}(A, B) \in B \end{aligned}$$

We can build the following proof of the transitivity of the inclusion in the polarized sequent calculus modulo this rule:

$$
{\scriptstyle \vdash\because}\,\dfrac{{\scriptstyle \vdash\neg}\,\dfrac{{\scriptstyle \forall\vdash}\,\dfrac{{\scriptstyle \Rightarrow\vdash}\,\dfrac{{\scriptstyle \forall\vdash}\,\dfrac{{\scriptstyle \Rightarrow\vdash}\,\dfrac{{\scriptstyle \overset{\frown}{\vdash}}\,\dfrac{}{\mathit{diff}(A,C) \in C \vdash A \subseteq C} \qquad {\scriptstyle \overset{\frown}{\vdash}}\,\dfrac{}{\mathit{diff}(A,C) \in B \vdash \mathit{diff}(A,C) \in B}}{\mathit{diff}(A,C) \in B \Rightarrow \mathit{diff}(A,C) \in C, \mathit{diff}(A,C) \in B \vdash A \subseteq C}}{B \subseteq C, \mathit{diff}(A,C) \in B \vdash A \subseteq C} \qquad {\scriptstyle \overset{\frown}{\vdash}}\,\dfrac{}{\scriptstyle \mathit{diff}(A,C) \in A \vdash \mathit{diff}(A,C) \in A}}{\mathit{diff}(A,C) \in A \Rightarrow \mathit{diff}(A,C) \in B, B \subseteq C, \mathit{diff}(A,C) \in A \vdash A \subseteq C}}{A \subseteq B, B \subseteq C, \mathit{diff}(A,C) \in A \vdash A \subseteq C}}{A \subseteq B, B \subseteq C \vdash A \subseteq C, A \subseteq C}}{A \subseteq B, B \subseteq C \vdash A \subseteq C}
$$

To a rewriting system $\mathcal{R}$ corresponds a theory, which is the set of formulas that can be proved in the sequent calculus modulo $\mathcal{R}$. It was proved that this theory can always be presented by a traditional set of axioms, which is then called a compatible presentation [15]. In this paper, we are concerned with the opposite direction: is it possible to present any axiomatic first-order theory by a rewriting system? In [9, Corollary 25], we answered positively: it is possible to transform any first-order theory into a rewriting system. However, this rewriting system may not have all the good properties that ensure that deduction modulo behaves well, in particular the admissibility of the cut rule.

The cut rule is admissible in the sequent calculus modulo $\mathcal{R}$ if, whenever a sequent can be proved in it, then it can be proved without using the cut rule ($\underset{\smile}{\vdash}$ in Figure 1). Abusing terminology, we say that a rewriting system $\mathcal{R}$ admits cut if the cut rule is admissible in the sequent calculus modulo $\mathcal{R}$. The admissibility of the cut rule has a strong proof-theoretical as well as practical importance: it involves that normal forms exist for proofs; it implies the consistency of the theory associated to $\mathcal{R}$; it is equivalent to the completeness of the proof search procedures based on deduction modulo $\mathcal{R}$ (such as ENAR [15], extending the resolution method, and TaMed [4], extending the tableau method); etc. Cut admissibility can also be seen as the completeness of the cut-free sequent calculus w.r.t. the sequent calculus with cuts. In [9], to ensure the cut admissibility, we designed a procedure that completes the rewriting system. However, this procedure may not terminate (and produces too much rules in practice). In this paper, we propose another method to transform an axiomatic presentation of a theory into a cut-admitting rewriting system, that works for any finitely presented first-order theory.

2 Resolution Calculi

We briefly recall the resolution calculus and the set-of-support strategy, before presenting the extension of resolution with deduction modulo.

A derivation in resolution [25] tries to refute a set of clauses by inferring new clauses by means of the following inference rules

$$
\textsf{Resolution}\ \dfrac{P \vee C \qquad \neg Q \vee D}{\sigma(C \vee D)}\ {\scriptstyle \sigma = mgu(P,Q)} \qquad \textsf{Factoring}\ \dfrac{L \vee K \vee C}{\sigma(L \vee C)}\ {\scriptstyle \sigma = mgu(L,K)}
$$

until the empty clause is derived.

2.1 Set-of-Support Strategy

The set-of-support strategy for resolution [26] consists in restricting the clauses on which resolution can be applied. The input set of clauses is separated into a theory Γ and a set of support Δ. At least one of the clauses on which resolution is applied must be in the set of support, and the generated clause is put into the set of support. If the theory Γ is assumed to be consistent, this strategy is complete: if Γ, Δ is a unsatisfiable set of clauses, the empty clause can be derived from it using the set-of-support strategy. The set-of-support strategy can therefore be seen as proving a formula $\neg\Delta$ in a theory Γ without trying to find a contradiction in Γ because it is assumed to be consistent. In the following, we say that a set of clause Δ is refuted by the set-of-support strategy for Γ if the empty clause can be derived from the set Γ, Δ with set of support Δ.

2.2 (Polarized) Resolution Modulo

An extension of resolution based on deduction modulo, named Extended Narrowing and Resolution (ENAR), was defined in [15]. ENAR is a family of resolution calculi, each parametrized by a rewriting system $\mathcal{R}$.[1] It consists in adding a new inference rule, called Extended Narrowing, which produces the clauses obtained by narrowing a clause by $\mathcal{R}$. Since narrowing a clause with a proposition rewriting rule can produce a formula which is not in clausal normal form, the latter has to be computed to find the generated clauses. The Extended Narrowing rule is therefore:

$$\textsf{Ext. Narr.}\ \frac{C}{D}\ C \underset{\mathcal{R}}{\rightsquigarrow} A,\ D \in \mathcal{C}\ell(A)$$

where $\mathcal{C}\ell(A)$ is the set of clauses in the clausal normal form of A.

We say that ENAR for $\mathcal{R}$ is complete if, whenever $\vdash A$ can be proved in the sequent calculus modulo $\mathcal{R}$, the empty clause can be derived from $\mathcal{C}\ell(\neg A)$ in ENAR for $\mathcal{R}$. Hermant [20] proved that the empty clause can be derived from $\mathcal{C}\ell(\neg A)$ in ENAR for $\mathcal{R}$ if and only if $\vdash A$ can be proved *without cut* in the sequent calculus modulo $\mathcal{R}$. This implies that ENAR for a rewriting system $\mathcal{R}$ is complete if and only if the sequent calculus modulo $\mathcal{R}$ admits cut.

In ENAR, formulas have to be put in clausal normal form dynamically, which may require fresh Skolem symbols each time. To avoid this, Dowek introduced the Polarized Resolution Modulo (PRM) [13]. As ENAR, this is a family of resolution calculi parametrized by a rewriting system, but this system is assumed to be polarized, and clausal, i.e., each negative rule is of the form $P \to^- C$, and each positive rule is of the form $P \to^+ \neg C$, where C is in clausal form. In that case, the Extended Narrowing rule becomes:

[1] ENAR is originally parametrized by a rewriting system $\mathcal{R}$ and an equational theory $\mathcal{E}$, and the unification in the Resolution, Factoring and Extended Narrowing rules is performed modulo the equational theory $\mathcal{E}$, as in Equational Resolution [24]. To keep it simple, we choose not to consider equational theories in this paper.

$$\text{Ext. Narr.}^{-} \frac{P \vee C}{\sigma(D \vee C)} \; \sigma = mgu(P, Q),\ Q \rightarrow^{-} D \in \mathcal{R}$$

$$\text{Ext. Narr.}^{+} \frac{\neg Q \vee D}{\sigma(C \vee D)} \; \sigma = mgu(P, Q),\ P \rightarrow^{+} \neg C \in \mathcal{R}$$

Jianhua Gao recently proved that any rewriting system which admits cut can be transformed into an equivalent polarized and clausal rewriting system [19], so that PRM can be applied whenever ENAR can.

To each polarized clausal rewriting rule can be associated a clause in which one literal is selected. This clause is called a *one-way* clause [13]. For instance, to $P \rightarrow^{-} C$ is associated $\underline{\neg P} \vee C$, and to $P \rightarrow^{+} \neg C$ is associated $\underline{P} \vee C$ (the selected literals are underlined). Conversely, to a clause and a literal occurrence in this clause can be associated a polarized clausal rewriting rule: to $P \vee C$ and P is associated $P \rightarrow^{+} \neg C$, and to $\neg P \vee C$ and $\neg P$ is associated $P \rightarrow^{-} C$. The results of this paper exploit this isomorphism between polarized clausal rewriting rules and one-way clauses.

3 Cut-Admitting Presentations of Theories

3.1 Presenting a Theory as a Rewriting System

We suppose that the theory is presented by means of a set of clauses. If not, it has to be transformed into clausal normal form using standard techniques.

Definition 3. *Given a set of clauses Γ, we define the polarized rewriting system $\mathcal{R}_\Gamma$ consisting of, for each clause C in Γ, for each literal L in C,*

- *if $L = P$ is positive, a positive rewriting rule $P \rightarrow^{+} \neg\forall x_1, \ldots, x_n.\ L_1 \vee \cdots \vee L_m$ where $x_1, \ldots, x_n$ are the free variables of C that are not free in P and $L_1, \ldots, L_m$ are the literals of C different from P;*
- *if $L = \neg P$ is positive, a negative rewriting rule $P \rightarrow^{-} \forall x_1, \ldots, x_n.\ L_1 \vee \cdots \vee L_m$ where $x_1, \ldots, x_n$ are the free variables of C that are not free in P and $L_1, \ldots, L_m$ are the literals of C different from $\neg P$.*

Example 4. Let Γ be the set of clauses corresponding to the definition of the inclusion:

$$\neg A \subseteq B \vee \neg X \in A \vee X \in B$$
$$A \subseteq B \vee \mathit{diff}(A, B) \in A$$
$$A \subseteq B \vee \neg \mathit{diff}(A, B) \in B$$

Then $\mathcal{R}_\Gamma$ is

$$A \subseteq B \rightarrow^{-} \forall x.\ \neg x \in A \vee x \in B$$
$$X \in A \rightarrow^{-} \forall b.\ \neg A \subseteq b \vee X \in b$$
$$X \in B \rightarrow^{+} \neg\forall a.\ \neg a \subseteq B \vee X \in a$$

$$\begin{aligned} A \subseteq B &\rightarrow^{+} \neg \mathit{diff}(A,B) \in A \\ \mathit{diff}(A,B) \in A &\rightarrow^{+} \neg A \subseteq B \\ A \subseteq B &\rightarrow^{+} \neg\neg \mathit{diff}(A,B) \in B \\ \mathit{diff}(A,B) \in B &\rightarrow^{-} A \subseteq B \end{aligned}$$

Remark 5. The number of rewriting rules in $\mathcal{R}_\Gamma$ is equal to the number of literal occurrences in Γ.

3.2 From Consistency to Cut Admissibility

Theorem 6. *The consistency of a finite set of clauses Γ implies the completeness of the set-of-support strategy for Γ.*

Proof. This is the main theorem of [26].

Theorem 7. *The completeness of the set-of-support strategy for Γ implies the completeness of PRM for $\mathcal{R}_\Gamma$.*

Proof. This is a corollary of the following lemma.

Lemma 8. *A derivation of the empty clause from a set of clauses Δ with the set-of-support strategy for Γ can be transformed into a derivation of the empty clause from a set of clauses Δ in PRM for $\mathcal{R}_\Gamma$.*

Proof. By induction on the length of the derivation. If the first step resolves two clauses from the set of support (i.e. two clauses not in Γ), the same resolution can be performed in PRM. If the first step is

$$\mathsf{Resolution}\ \frac{C \vee P \qquad D \vee \neg Q}{\sigma(C \vee D)}\ \sigma = mgu(P,Q)$$

where $D \vee \neg Q$ is in Γ, we know that there is a rule $Q \rightarrow^{-} \forall x_1, \ldots, x_n.\ D$ in $\mathcal{R}_\Gamma$. Therefore, we have the following derivation in PRM:

$$\mathsf{Ext.\ Narr.}^{+}\ \frac{C \vee P}{\sigma(C \vee D)}\ \sigma = mgu(P,Q)$$

If the first step is

$$\mathsf{Resolution}\ \frac{C \vee \neg P \qquad D \vee Q}{\sigma(C \vee D)}\ \sigma = mgu(P,Q)$$

where $D \vee Q$ is in Γ, we know that there is a rule $Q \rightarrow^{+} \neg\forall x_1, \ldots, x_n.\ D$ in $\mathcal{R}_\Gamma$. Therefore, we have the following derivation in PRM:

$$\mathsf{Ext.\ Narr.}^{-}\ \frac{C \vee \neg P}{\sigma(C \vee D)}\ \sigma = mgu(P,Q)$$

Theorem 9. *The completeness of PRM for $\mathcal{R}_\Gamma$ implies the admissibility of the cut rule in the polarized sequent calculus modulo $\mathcal{R}_\Gamma$.*

Proof. Either direct proof by adapting Hermant's one for unpolarized deduction modulo [20], or combination of the following lemmas.

As in [9], Section 2.2, from the polarized rewriting system $\mathcal{R}_\Gamma$ we define the unpolarized rewriting system $\mathcal{R}_\Gamma^\mp$ consisting of:

- a rule $P \to P \vee \neg C$ for each positive rule $P \to^+ \neg C$ in $\mathcal{R}_\Gamma$;
- a rule $P \to P \wedge C$ for each negative rule $P \to^- C$ in $\mathcal{R}_\Gamma$.

Lemma 10. *A derivation of the empty clause from a set of clauses Δ in PRM for $\mathcal{R}_\Gamma$ can be transformed into a derivation of the empty clause from a set of clauses Δ in ENAR for $\mathcal{R}_\Gamma^\mp$.*

Proof. By induction on the derivation length, the only interesting case is Extended Narrowing.

Suppose that we have

$$\text{Ext. Narr.}^- \ \frac{P \vee C}{\sigma(D \vee C)} \ \sigma = mgu(P, Q),\ Q \to^- D$$

To $Q \to^- D$ corresponds the unpolarized rule $Q \to Q \wedge D$. Hence, $P \vee C$ can be narrowed to $\sigma((Q \wedge D) \vee C)$, whose clausal normal form is $(\sigma(Q \vee C)) \wedge (\sigma(D \vee C))$. Hence, the Extended Narrowing rule of ENAR can infer the clause $\sigma(D \vee C)$.

Suppose that we have

$$\text{Ext. Narr.}^+ \ \frac{\neg P \vee C}{\sigma(D \vee C)} \ \sigma = mgu(P, Q),\ Q \to^+ \neg D$$

To $Q \to^+ \neg D$ corresponds the unpolarized rule $Q \to Q \vee \neg D$. Hence, $\neg P \vee C$ can be narrowed to $\sigma(\neg(Q \vee \neg D) \vee C)$, whose clausal normal form is $(\sigma(\neg Q \vee C)) \wedge (\sigma(D \vee C))$. Hence, the Extended Narrowing rule of ENAR can infer the clause $\sigma(D \vee C)$.

Corollary 11. *The completeness of PRM for $\mathcal{R}_\Gamma$ implies the completeness of ENAR for $\mathcal{R}_\Gamma^\mp$.*

Lemma 12. *The completeness of ENAR for $\mathcal{R}_\Gamma^\mp$ implies the admissibility of the cut rule in the asymmetric sequent calculus modulo $\mathcal{R}_\Gamma^\mp$.*

Proof. This is a corollary of Theorems 1 and 2 of [20].

Lemma 13. *The admissibility of the cut rule in the asymmetric sequent calculus modulo $\mathcal{R}_\Gamma^\mp$ implies the admissibility of the cut rule in the polarized sequent calculus modulo $\mathcal{R}_\Gamma$.*

Proof. This is a direct consequence of the equivalence theorem between the polarized sequent calculus modulo $\mathcal{R}_\Gamma$ and the asymmetric sequent calculus modulo $\mathcal{R}_\Gamma^\mp$ (Corollary 10 of [9]): a sequent is provable (resp. provable without cut) in the polarized sequent calculus modulo a polarized proposition rewriting system $\mathcal{R}$ iff it is provable (resp. provable without cut) in the asymmetric sequent calculus modulo the rewriting system $\mathcal{R}^\mp$.

By combining Theorems 6, 7, and 9, we obtain:

Theorem 14. *The consistency of a finite set of clauses Γ implies the admissibility of the cut rule in the polarized sequent calculus modulo $\mathcal{R}_\Gamma$.*

4 Restricting the Number of Rules

The method described in this paper produces a number of rules equals to the number of literal occurrences of the input theory, so that the size of the input is multiplied by the number of literals in clauses. In this section, we discuss how to reduce the number of rules with the help of the following example: consider the theory

$$\begin{gathered} P(x) \vee Q(x) \\ \neg P(x) \vee Q(x) \\ P(x) \vee \neg Q(x) \end{gathered}$$

This paper's method gives the system $\mathcal{R}_1$

$$\begin{aligned} &P(x) \rightarrow^{+} \neg Q(x) \\ &Q(x) \rightarrow^{+} \neg P(x) \\ &P(x) \rightarrow^{-} Q(x) \\ &Q(x) \rightarrow^{+} \neg\neg P(x) \\ &P(x) \rightarrow^{+} \neg\neg Q(x) \\ &Q(x) \rightarrow^{-} P(x) \end{aligned}$$

A first solution to lower the number of rules is to consider ordered resolution with selection [3]. Ordered resolution with selection is parametrized by an ordering $\succ$ on atoms which is stable by substitution and total on ground atoms, and by a selection function S that associates to each clause a subset of the negative literals of this clause. It consists in restricting the literals on which resolution can be applied: if $S(C)$ is not empty, then only the literals in $S(C)$ can be used; in the other case, only the maximal literals w.r.t. $\succ$ can be used. In the same spirit as in Section 3.1, it is possible to associate a polarized rewriting system to a set of clauses for ordered resolution with selection by only considering as left-hand sides the literals that are selected (or maximal if none are selected) in a clause.

However, ordered resolution with selection is not compatible with the set-of-support strategy, in the sense that their combination jeopardizes the completeness. Consequently, the rewriting system corresponding to the clauses may not admit cut. Nevertheless, a sufficient condition to ensure the completeness is the saturation of the set of clauses used as complement of the set of support (i.e. the theory): the clauses that can be inferred from it must either be in it or be redundant. In our example, whatever the ordering and selection function used, the set of clauses is not saturated: at least one of $P(x)$ or $Q(x)$ is maximal in $P(x) \vee Q(x)$. By symmetry, we can suppose that $P(x)$ is maximal. Then $\neg P(x)$ is maximal in $\neg P(x) \vee Q(x)$ (and it can also be selected). Thus, $Q(x)$ can be inferred, and it is not redundant. A saturated set of clauses could be:

$$\underline{P(x)} \vee Q(x)$$

$$\underline{\neg P(x)} \vee Q(x)$$
$$\underline{P(x)} \vee \neg Q(x)$$
$$\underline{Q(x)}$$

which corresponds to a rewriting system

$$\begin{aligned}
&P(x) \rightarrow^{+} \neg Q(x)\\
&P(x) \rightarrow^{-} Q(x)\\
&P(x) \rightarrow^{+} \neg\neg Q(x)\\
&Q(x) \rightarrow^{+} \neg\bot
\end{aligned}$$

By completeness of the combination of ordered resolution and polarized resolution modulo [6], this system admits cut, and has less rules than $\mathcal{R}_1$.

A second solution to lower the number of rules is to consider subsystems of the one obtained by this paper's method, i.e., to only take some of the rules produced by it. It can be shown that the system $\mathcal{R}_1$ can be restricted to the four rules

$$\begin{aligned}
&P(x) \rightarrow^{+} \neg Q(x)\\
&Q(x) \rightarrow^{+} \neg P(x)\\
&P(x) \rightarrow^{-} Q(x)\\
&P(x) \rightarrow^{+} \neg\neg Q(x)
\end{aligned}$$

and still admits cut.

Consequently, starting from a rewriting system

$$\begin{aligned}
&P(x) \rightarrow^{+} \neg Q(x)\\
&P(x) \rightarrow^{-} Q(x)\\
&P(x) \rightarrow^{+} \neg\neg Q(x)
\end{aligned}$$

which does not admit cut, we can think of two ways of completing it to ensure cut admissibility. In one case, we add a new rule corresponding to a clause obtain by resolving (the clauses corresponding) to the rules ($Q(x) \rightarrow^{+} \neg\bot$, obtained by resolving $P(x) \rightarrow^{+} \neg Q(x)$ with $P(x) \rightarrow^{-} Q(x)$). In the other case, we add a new rule corresponding to the selection of another literal in an existing clause ($Q(x) \rightarrow^{+} \neg P(x)$, obtained by selecting $Q(x)$ instead of $P(x)$ in $P(x) \rightarrow^{+} \neg Q(x)$). In our example, in both cases, it was sufficient to obtain a cut-admitting system. Nevertheless, in general, we may have to reiterate the process. The completion by saturation may generate an unbounded number of clauses, whereas the completion by reselection is bounded by the number of literal occurrences in the initial clauses. However, we currently do not know how to tell when the second method can be stopped before generating all reselections. It remains to be investigated what method, or their combination, behaves the best in practice.

5 Further Work

5.1 Logical Strength

Since cut admissibility implies consistency, Gödel's second incompleteness theorem implies that it cannot be proved in the theory itself. But we may wonder whether it can be proved in the theory plus the assumption of its consistency. To this purpose, we have to investigate the proof of Section 3.2. We conjecture that "consistency implies cut admissibility" can be proved in first-order arithmetic.

5.2 Equality

In this paper, we only considered theories of first-order logic without equality. However, theories are often presented in first-order logic with equality. Adding the axioms for the equality (reflexivity, symmetry, transitivity and congruence w.r.t. the function symbols and the predicates), and transforming them as presented in this paper, is a theoretical way to obtain presentations of such theories. However, it does not take into account the specificity of the equality, and the way it can be integrated into a deduction system thanks to deduction modulo. A first improvement is to put the equational axioms into an equational theory modulo which rewriting and unification is performed (see Footnote 1). Nevertheless, existing provers perform unification and rewriting modulo only specific equational theories, such as commutativity of a function symbol. Only such axioms should therefore be presented this way. The other equational axioms should be transformed into *term* rewriting rules. It remains to be proved that using term rewriting rules for equational axioms and proposition rewriting rules as obtained as in this paper for the other axioms is complete. We conjecture that it is the case as long as the term rewriting system is confluent and commutes with the proposition rewriting system. The confluence of the term rewriting system can be ensured by the standard completion of Knuth and Bendix [22].

The next step is to design proof-search procedures based on deduction modulo for first-order logic with equality. A good candidate would be an extension of the superposition calculus [2] with an Extended Narrowing rule, but we currently do not know if it is complete.

5.3 Axiom Schemata

This paper only considers finite theories, but usual theories, such as for instance arithmetic, use axiom schemata. A way to handle such theories is to consider the work of Kirchner [21] who transforms an axiom schema into a finite number of axioms, most of them being directly orientable into rewriting rules.

5.4 Termination

Cut admissibility is not the only property of interest for a rewriting system. The termination is another good requirement, since it implies for instance the decidability of proof checking. However, note that even if the rewriting systems terminates, the narrowing may not. The systems produced by this paper's method may not terminate in general. We have to investigate if we can restrict the number of rules to ensure the termination of the rewriting system as well as its cut admissibility.

In the same line of work, we should investigated whether we can obtain rewriting systems that provide decision procedures for some theories.

5.5 Intuitionistic Logic

Since it is based on resolution, the method described in this paper only works for classical logic. In intuitionistic logic, it is known that some theories cannot be transformed into a rewriting system with cut admissibility. In [5], we have proposed a procedure inspired from our work in [9] that is able to transform a large class of intuitionistic theories into a rewriting system admitting cuts. Since it is undecidable to know if such a transformation is possible, the procedure is of course non-terminating. We need to investigate whether the method proposed here can improve the transformation of intuitionistic theories, but it does not seem plausible.

References

1. Baader, F., Nipkow, T.: Term *Re*writing and *all That*. Cambridge University Press (1998)
2. Bachmair, L., Ganzinger, H.: Rewrite-based equational theorem proving with selection and simplification. Journal of Logic and Computation 4(3), 1–31 (1994)
3. Bachmair, L., Ganzinger, H.: Resolution theorem proving. In: Handbook of Automated Reasoning, pp. 19–99. Elsevier and MIT Press (2001)
4. Bonichon, R., Hermant, O.: A semantic completeness proof for TaMed. In: Hermann, M., Voronkov, A. (eds.) LPAR. Lecture Notes in Computer Science, vol. 4246, pp. 167–181. Springer (2006)
5. Burel, G.: Automating theories in intuitionistic logic. In: Ghilardi, S., Sebastiani, R. (eds.) FroCoS. Lecture Notes in Artificial Intelligence, vol. 5749, pp. 181–197. Springer (2009)
6. Burel, G.: Embedding deduction modulo into a prover. In: Dawar, A., Veith, H. (eds.) CSL. Lecture Notes in Computer Science, vol. 6247, pp. 155–169. Springer (2010)
7. Burel, G.: Experimenting with deduction modulo. In: Sofronie-Stokkermans, V., Bjørner, N. (eds.) CADE 2011. Lecture Notes in Artificial Intelligence, vol. 6803, pp. 162–176. Springer (2011)
8. Burel, G., Dowek, G.: How can we prove that a proof search method is not an instance of another? In: LFMTP'09. pp. 84–87. ACM International Conference Proceeding Series, ACM (2009)
9. Burel, G., Kirchner, C.: Regaining cut admissibility in deduction modulo using abstract completion. Information and Computation 208(2), 140–164 (2010)
10. Ciabattoni, A., Galatos, N., Terui, K.: From axioms to analytic rules in nonclassical logics. In: Pfenning, F. (ed.) LICS. IEEE Computer Society (2008)

11. Dowek, G.: What is a theory? In: Alt, H., Ferreira, A. (eds.) STACS. Lecture Notes in Computer Science, vol. 2285, pp. 50–64. Springer (2002)
12. Dowek, G.: Confluence as a cut elimination property. In: Nieuwenhuis, R. (ed.) RTA. Lecture Notes in Computer Science, vol. 2706, pp. 2–13. Springer (2003)
13. Dowek, G.: Polarized resolution modulo. In: Calude, C.S., Sassone, V. (eds.) IFIP TCS. IFIP AICT, vol. 323, pp. 182–196. Springer (2010)
14. Dowek, G., Hardin, T., Kirchner, C.: HOL-$\lambda\sigma$ an intentional first-order expression of higher-order logic. Mathematical Structures in Computer Science 11(1), 1–25 (2001)
15. Dowek, G., Hardin, T., Kirchner, C.: Theorem proving modulo. Journal of Automated Reasoning 31(1), 33–72 (2003)
16. Dowek, G., Miquel, A.: Cut elimination for Zermelo's set theory (2006), available on authors' web page
17. Dowek, G., Werner, B.: Arithmetic as a theory modulo. In: Giesl, J. (ed.) RTA. Lecture Notes in Computer Science, vol. 3467, pp. 423–437. Springer (2005)
18. Gallier, J.H.: Logic for Computer Science: Foundations of Automatic Theorem Proving, Computer Science and Technology Series, vol. 5. Harper & Row, New York (1986)
19. Gao, J.: Clausal presentation of theories in deduction modulo (2011), presented in this workshop.
20. Hermant, O.: Resolution is cut-free. Journal of Automated Reasoning 44(3), 245–276 (2009)
21. Kirchner, F.: A finite first-order theory of classes. In: Altenkirch, T., McBride, C. (eds.) TYPES. Lecture Notes in Computer Science, vol. 4502, pp. 188–202. Springer (2006)
22. Knuth, D.E., Bendix, P.B.: Simple word problems in universal algebras. In: Leech, J. (ed.) Computational Problems in Abstract Algebra, pp. 263–297. Pergamon Press, Oxford (1970)
23. Negri, S., von Plato, J.: Cut elimination in the presence of axioms. The Bulletin of Symbolic Logic 4(4), 418–435 (1998)
24. Plotkin, G.: Building-in equational theories. Machine Intelligence 7, 73–90 (1972)
25. Robinson, J.A.: A machine-oriented logic based on the resolution principle. Journal of the ACM 12, 23–41 (1965)
26. Wos, L., Robinson, G.A., Carson, D.F.: Efficiency and completeness of the set of support strategy in theorem proving. J. ACM 12(4), 536–541 (1965)