An Abstract Completion Procedure for Cut Elimination in Deduction Modulo

Guillaume Burel
École Normale Supérieure de Lyon & LORIA*
guillaume.burel@ens-lyon.org

Claude Kirchner
INRIA & LORIA
Claude.Kirchner@loria.fr

The complementarity and interaction between computation and deduction is known since at least Henri Poincaré and deduction modulo [7] 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 (for instance see [7, 2]) 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 [6].

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 price: the Hauptsatz, *i.e.* the fact that cuts are not needed to build proofs, is not always true as one can see from an example derived from Crabbé's proof of the non-normalization of Zermelo's theory [3] (see for instance [7]). 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[1] of the ones appearing in it, so that the search space is, in a sense, limited. Such proofs are sometimes called *analytic* [6]. The tableaux method is based on this fact, and for instance TaMeD [2], 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 [8] that a proof search method for deduction modulo like ENAR [7]—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 [6] 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 [5], 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 [4, 1]. 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, saturation and redundancy follow up.

To present the general idea of our approach, let us consider the simple example of Crabbé's axiom [3] $A \Leftrightarrow B \wedge \neg A$. 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 can prove that such a proof, in its simplest form, is necessarily of the shape:

$$\dfrac{\dfrac{\begin{matrix}\vdots\\ A, B\wedge\neg A \vdash\end{matrix}}{A\vdash}\uparrow\text{-l} \qquad \dfrac{\begin{matrix}\vdots\\ \vdash B\wedge \neg A, A\end{matrix}}{\vdash A}\uparrow\text{-r}}{\vdash}\text{Cut}(A)$$

where the rules labeled "$\uparrow$ -r" and "$\uparrow$ -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:

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

*UMR 7503 CNRS-INPL-INRIA-Nancy2-UHP

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

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

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

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

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

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

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

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

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;

As an important by-product of these results, we demonstrate the expressive power of the abstract canonical systems.

References

[1] M. Bonacina and N. Dershowitz. Abstract canonical inference. *ACM Trans. Comput. Logic*, 8(1), 2007.

[2] R. Bonichon. TaMeD: A tableau method for deduction modulo. In D. A. Basin and M. Rusinowitch, editors, *IJCAR*, volume 3097 of *LNCS*, pages 445–459. Springer, 2004.

[3] M. Crabbé. Non-normalisation de la théorie de Zermelo. Manuscript, 1974.

[4] N. Dershowitz and C. Kirchner. Abstract canonical presentations. *Theoretical Computer Science*, 357:53–69, 2006.

[5] G. Dowek. What is a theory? In H. Alt and A. Ferreira, editors, *STACS*, volume 2285 of *LNCS*, pages 50–64. Springer, 2002.

[6] G. Dowek. Confluence as a cut elimination property. In R. Nieuwenhuis, editor, *RTA*, volume 2706 of *LNCS*, pages 2–13. Springer, 2003.

[7] G. Dowek, T. Hardin, and C. Kirchner. Theorem proving modulo. *Journal of Automated Reasoning*, 31(1):33–72, 2003.

[8] O. Hermant. *Méthodes Sémantiques en Déduction Modulo*. PhD thesis, École Polytechnique, 2005.