



ELSEVIER

Available online at www.sciencedirect.com



ScienceDirect

Electronic Notes in
Theoretical Computer
Science

Electronic Notes in Theoretical Computer Science 205 (2008) 137–144

www.elsevier.com/locate/entcs

On the Convergence of Reduction-based and Model-based Methods in Proof Theory

Gilles Dowek¹

École polytechnique and INRIA

LIX, École polytechnique, 91128 Palaiseau Cedex, France

Abstract

In the recent past, the reduction-based and the model-based methods to prove cut elimination have converged, so that they now appear just as two sides of the same coin. This paper details some of the steps of this transformation.

Keywords: Cut elimination, reducibility candidates, models, truth values algebras

Introduction

Many results of proof theory, such as unprovability results, completeness of various proof-search methods, the disjunction and the witness property of constructive proofs and the possibility to extract programs from such proofs, rely on cut elimination theorems, asserting that when a proposition is provable in some theory, it has a proof of a special form: a *cut free* proof.

The methods developed to prove such cut elimination theorems can be broadly divided into two categories: the reduction-based methods and the model-based ones. In the recent past, we have witnessed a convergence of these two kinds of methods. In this paper, I detail some of the steps of this transformation that has lead to consider reduction-based and model-based methods just as two sides of the same coin.

1 The problem of the axioms

A preliminary step to the convergence of reduction-based and model-based methods for proving cut elimination has been the definition of a sufficiently general notion

¹ Email: gilles.dowek@polytechnique.edu

of cut. And this has itself required a modification of the notion of theory.

Let us start with an example. A consequence of the cut elimination theorem is the disjunction property: in constructive logic, when a proposition of the form $A \vee B$ is provable in the empty theory, *i.e.* without axioms, then either A or B is provable. Indeed, by the cut elimination theorem, if the proposition $A \vee B$ is provable, it has a cut free proof. Then, a simple induction on proof structure shows that, in constructive natural deduction, the last rule of a cut free proof in the empty theory is an introduction. Thus a cut free proof of $A \vee B$ ends with an introduction of the disjunction and either A or B is provable.

The fact that the last rule of a cut free proof in an introduction does not extend when we add axioms. For instance, if $A \vee B$ is an axiom, then this proposition has a cut free proof that ends with the axiom rule. Thus, the disjunction property for theories such as arithmetic or simple type theory cannot be derived, in a simple way, from the cut elimination theorem for predicate logic. The attempts to characterize axioms, such as Harrop formulae, that preserve the usual properties of cut free proofs, such as the disjunction property, the witness property or the fact that the last rule is an introduction, have led to relatively small classes, that, for instance, never contain the axioms of arithmetic. Indeed, the cut elimination theorem for predicate logic without axioms can be proved in arithmetic and the property that all propositions provable in arithmetic have a proof ending with an introduction rule implies the consistency of arithmetic. Thus, this result cannot be derived in an elementary way from the cut elimination theorem of predicate logic.

Therefore, to prove the disjunction property for arithmetic or simple type theory, we need to extend the cut elimination theorem first. This explains why there are several cut elimination theorems for various theories of interest. For instance, in arithmetic, we usually introduce a new form of cut specific to the induction axiom, and we prove the cut elimination theorem again for this extended notion of cut.

This necessity to introduce a specific notion of cut for each theory of interest has been an obstacle to the development of a general theory of cut elimination. *Deduction modulo* [12,15] has been an attempt to partially solve this problem. In deduction modulo, the axioms of the form $\forall x_1 \dots \forall x_n (t = u)$ or $\forall x_1 \dots \forall x_n (P \Leftrightarrow A)$ where P is an atomic proposition are replaced by rewrite rules $t \longrightarrow u$ or $P \longrightarrow A$. Then, deduction is performed modulo the congruence generated by these rules. If not all, many theories can be formulated as rewrite systems: for instance arithmetic [16,1] and simple type theory [13].

In deduction modulo, not all theories have the cut elimination property. But, what is important is that the definition of the notion of cut is independent of the theory of interest and asking if some theory, formulated as a rewrite system, has the cut elimination property is now a well-formed question.

In fact, a similar idea had been investigated earlier by Dag Prawitz and others [26,7,8,20,17] who have proposed to replace the axioms of the form $\forall x_1 \dots \forall x_n (P \Leftrightarrow A)$ by non logical deduction rules allowing to unfold P into A and to fold A into P . More recently, Benjamin Wack has introduced a notion of super-natural deduction [30,3] where the unfolding of P into A is automatically followed by all the possible

elimination rules of the connectors and quantifiers of A and the folding of A into P preceded by the corresponding introduction rules. This leads to very natural deduction rules where, like in the usual mathematical practice, connectors and quantifiers almost disappear. Interestingly, the theories that have the cut elimination property in these three formalisms are the same [10,4]. This shows the robustness of this notion of cut.

In conclusion, it is possible to formulate a general notion of cut that applies to all the theories that can be expressed as a rewrite system and this notion of cut is quite robust. The definition of such a notion of cut independent of the theory of interest has been a pre-requisite to the convergence of reduction-based and model-based methods as, this way, a sufficiently large class of problems to which these methods apply, has been identified.

2 Models

2.1 Soundness and completeness

The soundness theorem asserts that for every proposition A , if A is provable in predicate logic, then for every model \mathcal{M} , A is valid in \mathcal{M} . Conversely, the completeness theorem asserts that for every proposition A , if for every model \mathcal{M} , A is valid in \mathcal{M} , then A is provable. In most of the proofs of the completeness theorem however, the classically equivalent statement is proved: for every proposition A , there exists a model \mathcal{M} such that if A is valid in \mathcal{M} , then A is provable.

With the usual notion of bi-valued model, it is not possible to permute the quantifiers and prove that there exists a uniform model \mathcal{M} such that for every proposition A , if A is valid in \mathcal{M} , then A is provable. But, if we extend the notion of model by allowing truth values to be elements of an arbitrary boolean algebra, then this statement becomes provable. An example of such model is the syntactic model, where the truth values are the elements of the Lindenbaum algebra of the language. In constructive logic, the boolean algebras need to be replaced by Heyting algebras, but this uniform completeness theorem can still be proved.

2.2 Model-based cut elimination proofs

The model-based cut elimination proofs — for instance [27,25,29,2,9,23] — proceed by proving a sharpened completeness theorem: for every proposition A , if for every model \mathcal{M} , A is valid in \mathcal{M} , then A has a cut free proof. The cut elimination theorem is then just a consequence of the soundness theorem and of this sharpened completeness theorem: if a proposition has a proof then, by the soundness theorem, it is valid in all models, hence, by the sharpened completeness theorem, it has a cut free proof.

Olivier Hermant has shown that such a model-based method could be used to prove cut elimination for a large class of theories in deduction modulo [21,22]. His sharpened completeness theorems are uniform: they proceed by constructing a model \mathcal{M} such that for all A , if A is valid in \mathcal{M} , then A has a cut free proof.

Notice that, when such a uniform sharpened completeness theorem is used, only one instance of the soundness theorem is needed in the proof of the cut elimination theorem: that corresponding to the model \mathcal{M} given by the sharpened completeness theorem. Provable propositions are valid in this particular model, hence they have a cut free proof.

3 Reductions

The reduction-based methods prove cut elimination theorems by exhibiting an algorithm that transforms a proof that is not cut free, into another that is “closer” to a cut free proof. This transformation process, called a *reduction* of the proof, can be iterated and if it terminates, it yields a cut free proof.

One of the first reduction-based cut elimination proofs is the proof of termination of proof reduction in arithmetic using Tait’s method [28]. The idea is to prove, by induction over proof structure, that all proofs terminate, but to let this induction go through, it is necessary, as usual in proofs by induction, to strengthen the induction hypothesis and to prove that all proofs verify a property stronger than termination, called *reducibility*. This notion of reducibility is parametrized by the proposition the proof is a proof of. Thus, in this proof, a notion of “being a *reducible* proof of A ” is defined by induction over the structure of the proposition A , and then, the fact that all proofs of A are reducible proofs of A is proved by induction over proof structure.

An equivalent formulation uses the set of reducible proofs of A instead of the predicate “being a reducible proof of A ”. The fact that the predicate “being a reducible proof of A ” is defined by induction on the structure of A then rephrases as the fact that the set of reducible proofs of $A \Rightarrow B$, for instance, is defined from the set of reducible proofs of A and that of reducible proofs of B , by applying to these sets a binary function \Rightarrow , and similarly for the other connectors and quantifiers.

4 From reductions to models

Bridging the gap between reduction-based methods and model-based ones has required several steps.

4.1 Reducibility candidates

The first has been the introduction, by Jean-Yves Girard, of the notion of *reducibility candidate* in his reduction-based proof of cut elimination for simple type theory [18,19].

In this proof, to define the set of reducible proofs of some proposition A , it is necessary to quantify on the sets of reducible proofs of all propositions B . Thus, a naive attempt leads to a circular definition and a way to avoid this circularity is to introduce *a priori* a set of sets of proofs, the set of *reducibility candidates*, and quantify over all such reducibility candidates instead. Then, it is possible to define

the set of reducible proofs of all propositions and it happens *a posteriori* that these sets are reducibility candidates.

Introducing this set of reducibility candidates, Jean-Yves Girard has defined the place where sets of reducible proofs live. Michel Parigot [24] has shown later that this set of reducibility candidate could be defined in a simple way, as the smallest set of set of proofs closed by the operations \Rightarrow , $\tilde{\vee}$, ...

4.2 Reducibility candidates as truth values

In the cut elimination proofs for various formulations of type theory, in particular in Benjamin Werner’s proof of cut elimination for the *Calculus of inductive constructions* [31], the similarity of this assignment of a set of proofs to each proposition and the assignment of a truth value to each proposition in a model was noticed.

In particular, it is interesting to remark that the model theoretic notation $\llbracket A \rrbracket$ has progressively replaced the notation R_A for the set of reducible proofs of a proposition A and that the expressions “the interpretation of A ” and “the denotation of A ” have progressively replaced the expression “the set of reducible proofs of A ”.

4.3 Introducing domains

In [15], we have proposed together with Benjamin Werner a reduction-based cut elimination proof for a large class of theories in deduction modulo. In deduction modulo, unlike in type theory, the terms of the theory and the proof-terms are entities of different kinds, as well as the sorts of the language and the propositions. Thus, it was natural to interpret not only propositions, using reducibility candidates for truth values, but also terms.

This simplified our cut elimination proof, in particular because, instead of defining the interpretation of a predicate symbol as a function mapping terms to truth values, it was possible to decompose this function in two steps and first interpret the terms in a domain and then define the interpretation of a predicate symbol as a function mapping elements of the domain to truth values, as it is usual in models.

This way, a notion of domain of interpretation of terms was introduced in reduction-based cut elimination proofs and this materialized in a notion of reducibility candidate valued model, called *pre-models*.

4.4 Truth values algebras and super-consistency

As already said, the usual notion of bi-valued model can be extended to notions where the truth values form a boolean algebra or a Heyting algebra. This raises the question of the possibility to view pre-models as such Heyting algebra valued models, *i.e.* the question of the possibility to define an order on the set of reducibility candidates that makes it a Heyting algebra. Unfortunately, this is not possible, as in all Heyting algebras $(\tilde{\top} \Rightarrow \tilde{\top}) = \tilde{\top}$, but not in the algebra of reducibility candidates. Thus, to include the algebra of reducibility candidates, the notion of Heyting algebra had to be generalized to a notion of *Truth values algebra* [11].

What relations and operations are needed to use a set as a set of truth values ? Actually, there is no need for this set to be equipped with an order relation. What are needed are operations $\Rightarrow, \tilde{\vee}, \tilde{\wedge}, \dots$ so that propositions can be interpreted and a notion of *positive truth value* to characterize valid propositions. For the soundness theorem to hold, this set of positive truth values must be closed by deduction rules. For instance, if $a \Rightarrow b$ and a are positive truth values, then b also must be a positive truth value.

Thierry Coquand [5] has suggested that in such an algebra, it is always possible to define a relation \leq by $a \leq b$ if $a \Rightarrow b$ is a positive truth value. And he has noticed that a truth value algebra equipped with such a relation verifies all the properties of Heyting algebras except one: the antisymmetry of the relation \leq . Thus, truth values algebras can alternatively be defined as pre-ordered structures with greatest lower bounds, least upper bounds and relative complementation. Unlike in ordered structures, greatest lower bounds and least upper bounds are not unique in pre-ordered structures and, besides the pre-order, the operations $\Rightarrow, \tilde{\vee}, \tilde{\wedge}, \dots$ must be given in the definition of the algebra, as it has to be specified which greatest lower bound of a and b the element $a \tilde{\wedge} b$ is.

It is well-known that the relation defined on propositions by $A \leq B$ if $A \Rightarrow B$ is provable is reflexive and transitive, but that to make it antisymmetric and define the Lindenbaum algebra of a language, it is necessary to take the quotient of the set of propositions by the relation \simeq defined by $A \simeq B$ if $A \Leftrightarrow B$ is provable. An alternative “solution” is to drop this antisymmetry requirement.

The set of reducibility candidates equipped with the operations $\Rightarrow, \tilde{\vee}, \tilde{\wedge}, \dots$ is a truth values algebra and the models valued in this algebra are exactly the pre-models we had constructed with Benjamin Werner.

Surprisingly, in these constructions, no specific properties of the algebra of reducibility candidates were used. Thus, they generalize to all truth values algebras. This has lead to introduce a notion of *super-consistency*: a theory is super-consistent if it has a \mathcal{B} -valued model, not only for one, but for all truth values algebras \mathcal{B} .

Super-consistency is a model theoretic sufficient condition for termination of proof reduction. Whether this condition is necessary is still an open problem.

4.5 From super-consistency to model-based cut elimination proofs

We have noticed with Olivier Hermant that the proof that super-consistency implies the termination of proof reduction can be simplified, if we restrict to the goal to prove that super-consistency implies that all provable propositions have a cut free proof [14]. In this case, we do not need to establish a property of proofs but merely a property of propositions and sequents. Thus instead of using an algebra whose elements are sets of proofs, we can use a simpler algebra whose elements are sets of sequents: in a reducibility candidate, each proof collapses to its conclusion.

Tait’s lemma, that if π is a proof of a proposition A , then it is an element of the set $\llbracket A \rrbracket$ of reducible proofs of A , collapses to the fact that if a sequent $\Gamma \vdash A$ is provable then it is a element of $\llbracket A \rrbracket$. This model can further be transformed into a model where truth values are sets of contexts, that form a Heyting algebra, in such

a way that if $\Gamma \in \llbracket A \rrbracket$ then $\Gamma \vdash A$ has a cut free proof, and Tait's lemma rephrases as the fact that if a sequent $\Gamma \vdash A$ is provable then $\Gamma \in \llbracket A \rrbracket$.

It is possible to prove that if a sequent $\Gamma \vdash A$ is valid in this model, then $\Gamma \in \llbracket A \rrbracket$ and Tait's lemma boils down to the fact that if a sequent $\Gamma \vdash A$ is provable then it is valid in this model. Like in model-based proofs, this is just the instance of the soundness lemma corresponding to this model. And indeed the fact that if a sequent $\Gamma \vdash A$ is valid in this model, then the $\Gamma \in \llbracket A \rrbracket$ and thus $\Gamma \vdash A$ has a cut free proof is a uniform sharpened completeness theorem.

Conclusion

Step by step, the gap between reduction-based methods and model-based methods to prove cut elimination has been bridged and, along the way, cut eliminations has been proved for new theories. Both types of proofs can be decomposed in two steps, first a proof that the theory of interest is super-consistent, then a proof, independent of the theory of interest, that super-consistency implies cut elimination. The only difference is in the choice of the truth value algebra used to deduce cut elimination from super-consistency: the algebra of reducibility candidates to prove the termination of proof reduction, the simpler algebra of sequents to construct a model where validity implies cut free provability.

Once this convergence is achieved, several directions may be worth exploring. First, we may want to deduce directly proof theoretical results from super-consistency, without proving cut elimination first. Second, we may want to extend the notion of super-consistency to type theory. The recent [6] that relates deduction modulo and type theory may be a good starting point.

References

- [1] L. Allali. Algorithmic equality in Heyting arithmetic modulo. *Higher Order Rewriting*, 2007.
- [2] P.B. Andrews. Resolution in type theory. *The Journal of Symbolic Logic*, 36(3):414–432, 1971.
- [3] P. Brauner, C. Houtmann, and C. Kirchner. Superdeduction at work. *Rewriting, Computation and Proof, Essays dedicated to Jean-Pierre Jouannaud on the occasion of his 60th birthday*, Lectures Notes in Computer Science 4600, Springer, 132–166, 2007.
- [4] P. Brauner, G. Dowek, and B. Wack. Normalization in supernatural deduction and in deduction modulo. Manuscript, 2007.
- [5] Th. Coquand, Personal communication.
- [6] D. Cousineau and G. Dowek. Embedding Pure Types Systems in the lambda Pi-calculus modulo, *Typed Lambda calculi and Applications*, Lecture Notes in Computer Science 4583, Springer, 102–117, 2007.
- [7] M. Crabbé. Non-normalisation de la théorie de Zermelo. Manuscript, 1974.
- [8] M. Crabbé. Stratification and cut-elimination. *The Journal of Symbolic Logic*, 56(1): 213–226, 1991.
- [9] M. De Marco and J. Lipton. Completeness and cut-elimination in the intuitionistic theory of types. *Journal of Logic and Computation*, 15:821–854, 2005.
- [10] G. Dowek. About folding-unfolding cuts and cuts modulo. *Journal of Logic and Computation*, 11(3):419–429, 2001.

- [11] G. Dowek, Truth values algebras and proof normalization, *TYPES 2006*, Lecture Notes in Computer Science 4502, Springer, 2007.
- [12] G. Dowek, T. Hardin, and C. Kirchner. Theorem proving modulo. *Journal of Automated Reasoning*, 31:32–72, 2003.
- [13] G. Dowek, T. Hardin, and C. Kirchner. HOL-lambda-sigma: an intentional first-order expression of higher-order logic. *Mathematical Structures in Computer Science*, 11:1–25, 2001.
- [14] G. Dowek and O. Hermant. A simple proof that super-consistency implies cut elimination. *Rewriting techniques and applications*, Lecture Notes in Computer Science, 4533, 96–106, 2007.
- [15] G. Dowek and B. Werner. Proof normalization modulo. *The Journal of Symbolic Logic*, 68(4):1289–1316, 2003.
- [16] G. Dowek and B. Werner. Arithmetic as a theory modulo. *Term rewriting and applications*, Lecture Notes in Computer Science 3467, Springer, 423–437, 2005.
- [17] J. Ekman. *Normal proofs in set theory*. Doctoral thesis, Chalmers university of technology and University of Göteborg, 1994.
- [18] J.-Y. Girard. Une extension de l'interprétation de Gödel à l'analyse, et son application à l'élimination des coupures dans l'analyse et la théorie des types. *2nd Scandinavian Logic Symposium*, North Holland, 63–92, 1971.
- [19] J.-Y. Girard, *Interprétation fonctionnelle et élimination des coupures dans l'arithmétique d'ordre supérieur*. Doctoral thesis, Université de Paris 7, 1972.
- [20] L. Hallnäs. *On normalization of proofs in set theory*. Doctoral thesis, University of Stockholm, 1983.
- [21] O. Hermant. *Méthodes sémantiques en déduction modulo*. Doctoral Thesis, Université de Paris 7, 2005.
- [22] O. Hermant. Semantic cut elimination in the intuitionistic sequent calculus. *Typed Lambda Calculi and Applications*, Lecture Notes in Computer Science 3461, Springer, 221–233, 2005.
- [23] M. Okada. A uniform semantic proof for cut elimination and completeness of various first and higher order logics. *Theoretical Computer Science*, 281:471–498, 2002.
- [24] M. Parigot. Strong normalization for the second orclassical natural deduction. *Logic in Computer Science*, 39–46, 1993.
- [25] D. Prawitz. Hauptsatz for higher order logic. *The Journal of Symbolic Logic*, 33:452–457, 1968.
- [26] D. Prawitz. *Natural Deduction. A Proof-Theoretical Study*. Almqvist and Wiksell, 1965.
- [27] W. W. Tait. A non constructive proof of Gentzen's Hauptsatz for second order predicate logic. *Bulletin of the American Mathematical Society*, 72:980–983, 1966.
- [28] W. W. Tait. Intentional interpretations of functionals of finite type I. *The Journal of Symbolic Logic*, 32:198–212, 1967.
- [29] M. o. Takahashi. A proof of cut-elimination theorem in simple type theory. *Journal of the Mathematical Society of Japan*, 19:399–410, 1967.
- [30] B. Wack. *Typage et déduction dans le calcul de réécriture*. Doctoral Thesis, Université Henri Poincaré Nancy 1, 2005.
- [31] B. Werner. *Une théorie des constructions inductives*. Doctoral Thesis, Université de Paris 7, 1994.