Completeness of Cut-Free Sequent Calculus Modulo

Olivier Hermant[1]

INRIA Futurs and LIX
projet LOGICAL
École Polytechnique
91128 Palaiseau Cedex, France
ohermant@pauillac.inria.fr

Abstract. Deduction modulo is a powerful way to replace axioms by rewrite rules and allows to integrate computation in deduction. But adding rewrite rules is not always safe for properties of the deduction system such as consistency or cut elimination. Proving completeness of the cut-free calculus with respect to semantical models is a way to prove the redundancy of the cut rule. The result obtained this way is slightly weaker than that obtained with a normalization proof, but more general, and the proof is much simpler. We here give some conditions on rewrite rules and present the results and techniques that lead to the cut elimination theorem for the classical sequent calculus modulo. At last, we give a rewrite rule featuring cut-elimination, but non-normalizing.

Keywords : deduction modulo, sequent calculus modulo, model, rewrite rules, cut-free, cut elimination
An electronic version of the paper is available at :
`http://pauillac.inria.fr/~ohermant`

1 Introduction

Eliminating cuts is a way to prove some very important results about deduction systems, like constructivity, consistency, non-provability of some theorems, or completeness of proof search methods.

The introduction of axioms as hypothesis makes the cut elimination property of these systems in danger, introducing so-called axiomatic cuts.

Deduction modulo [1] is a way to integrate axioms into the deduction system, replacing them by rewrite rules. Adding rewrite rules allows us to express some powerful theories in first order logic, like Higher Order Logic [2] or Peano's Arithmetic [3].

A rewrite rule in deduction modulo is of the shape $l \rightarrow r$ where l can be any term, or an *atomic proposition*. For example, we can have the following rewrite rule, rewriting an atomic proposition to a non-atomic one : $x \times y = 0 \rightarrow (x = 0) \vee (y = 0)$. Eliminating cuts does not always succeed because of these kind of rules. For example, if we take a formulation of Crabbé's rule : $A \rightarrow B \wedge \neg A$, we are able to prove the propositions $\neg B$ but the proofs involves a cut that can't be eliminated. On the other hand, rules rewriting propositions allow us to express formalisms which power goes beyond first order.

The system on which we work here is the (classical) sequent calculus modulo, a deduction system based on sequent calculus LK [4], with the addition of term- and proposition-rewrite. But we do not have cut-elimination for all rewrite systems even when the rewrite rules are confluent and terminating [2]. We hence have to find some criterion to assure cut elimination in a wide range of cases. We here present two of them, namely an order condition, a positivity condition, and then we present cut-elimination for HOL expressed with the help of rewrite rules in sequent calculus.

Our goal is not to provide an algorithm to eliminate cuts and prove its termination [2] but to prove that every provable sequent has a cut-free proof. This result is slightly weaker than normalization, but it has simpler proofs and is more general. One of the motivations of this work was to study the link between these two approaches (pre-models versus models of the cut-free calculus). In this sense, the results given in section 6 answer partly this question. In all the cases, these results are sufficient to prove completeness result of proof search algorithms.

The way cut-elimination is obtained here is similar to the proof of Gödel's completeness theorem, proving a completeness theorem of the *cut-free* sequent calculus modulo with respect to semantical models. Associated with soundness of the full sequent calculus modulo, it entails directly the cut-elimination theorem. Such a method has already been used by Schütte, or in proving semantically that HOL has the cut-elimination property. In fact, the analogous result for HOL expressed in sequent calculus modulo we get here uses the same model construction as Andrews [5], Prawitz [6] and Takahashi [7].

There's an important point we should mention : although our proof follows the lines of Gödel, we cannot use the usual definitions of such terms as "complete" or "consistent", because we are now working in the cut-free calculus. This justifies the definitions we give in section 3. Other difficulties are given by the introduction of rewrite rules, that force use to prove again some results well-known for sequent calculus. Finally, the model constructions are singularly different from those of the completeness theorem.

2 Sequent Calculus Modulo

2.1 Deduction system

A sequent is a pair $\Gamma \vdash \Delta$, where Γ, Δ are multi-sets of proposition (a proposition can appear several time). We can derive (prove) a sequent with the help of deduction rules of the form :

$$\frac{\Gamma_1 \vdash \Delta_1, ..., \Gamma_1 \vdash \Delta_n}{\Gamma \vdash \Delta}$$

Some of these rules are given in the figure 1. The star on the $\forall$ quantifier means that we have a freshness condition on the constant c : this constant has to not appear in the sequent.

$$\frac{}{\Gamma, P \vdash P, \Delta}\text{axiom} \qquad \frac{\Gamma, P \vdash \Delta \quad \Gamma \vdash P, \Delta}{\Gamma \vdash \Delta}\text{cut}$$

$$\frac{\Gamma, P, Q \vdash \Delta}{\Gamma, P \wedge Q \vdash \Delta}\wedge\text{-l} \qquad \frac{\Gamma \vdash P, \Delta \quad \Gamma \vdash Q, \Delta}{\Gamma \vdash P \wedge Q, \Delta}\wedge\text{-r}$$

$$\frac{\Gamma, \{t/x\}P \vdash \Delta}{\Gamma, \forall x\ P \vdash \Delta}\forall\text{-l} \qquad \frac{\Gamma \vdash \{c/x\}P, \Delta}{\Gamma \vdash \forall x\ P, \Delta}\forall^*\text{-r}$$

Fig. 1. Some deduction rules of sequent calculus

To present the sequent calculus modulo, we need to give a precise definition of what is a rewrite rule. There is two kind of rewrite rules : rewrite rules on terms, and rewrite rules on propositions [1].

Definition 1. *A term rewrite rule is a pair of terms $l \to r$ such that the variables of r appears in l.*
A propositional rewrite rule is a pair of propositions $l \to r$ such that l is atomic and free variables of r appears in l.

Example of rewrite rule on a term:

$$x \times 0 \to 0$$

Example of rewrite rule on atomic proposition:

$$x \times y = 0 \to (x = 0) \vee (y = 0)$$

In this case, we notice that an atomic proposition can rewrite on a non-atomic proposition.

A rewrite system $\mathcal{R}$ is a set of propositional and term rewrite rules.

Definition 2. *Let $\mathcal{R}$ a rewrite system. The proposition P rewrites in one step to P' in $\mathcal{R}$ iff:*
$P_{|\omega} = \sigma(l)$ and $P' = P[\sigma(r)]_\omega$ for a rule $l \to r \in \mathcal{R}$, an occurence ω in P and a substitution σ. When we apply σ, we have to rename the bound variables in order to avoid capture.
We write $P \to_{\mathcal{R}} P'$.
$\to^*_{\mathcal{R}}$ stands for the reflexive transitive closure of relation $\to_{\mathcal{R}}$, and $=_{\mathcal{R}}$ is its reflexive, transitive, symmetric closure.

When we add a set of rewrite rules, we get an extra freedom : propositions involved in the premises and in the conclusion of a deduction rule have to be

$$\frac{}{\Gamma, P \vdash_{\mathcal{R}} Q, \Delta}\text{axiom if } P =_{\mathcal{R}} Q$$

$$\frac{\Gamma, P \vdash_{\mathcal{R}} \Delta \quad \Gamma \vdash_{\mathcal{R}} Q, \Delta}{\Gamma \vdash_{\mathcal{R}} \Delta}\text{cut if } P =_{\mathcal{R}} Q$$

$$\frac{\Gamma, P, Q \vdash_{\mathcal{R}} \Delta}{\Gamma, R \vdash_{\mathcal{R}} \Delta} \wedge\text{-l if } R =_{\mathcal{R}} P \wedge Q$$

$$\frac{\Gamma \vdash_{\mathcal{R}} P, \Delta \quad \Gamma \vdash_{\mathcal{R}} Q, \Delta}{\Gamma \vdash_{\mathcal{R}} R, \Delta} \wedge\text{-r if } R =_{\mathcal{R}} P \wedge Q$$

$$\frac{\Gamma, \{t/x\}P \vdash_{\mathcal{R}} \Delta}{\Gamma, Q \vdash_{\mathcal{R}} \Delta}\forall\text{-l if } Q =_{\mathcal{R}} \forall x\ P$$

$$\frac{\Gamma \vdash_{\mathcal{R}} \{c/x\}P, \Delta}{\Gamma \vdash Q, \Delta}\forall^{*}\text{-r if } Q =_{\mathcal{R}} \forall x\ P$$

Fig. 2. Some deduction rules of sequent calculus modulo

equal modulo the rewrite rules, as we can see in figure 2. The entire set of rules is given in [2], or in [1].

We add a subscript $\mathcal{R}$ to remind that we are working with a certain set of rewrite rules. In the following, we will mainly work in the cut-free sequent calculus. We will denote sequents in this calculus : $\Gamma \vdash^{cf}_{\mathcal{R}} \Delta$ to recall that we don't allow the cut rule to be employed. When we allow the cut rule, we will denote a sequent : $\Gamma \vdash_{\mathcal{R}} \Delta$.

As said before, we don't have cut-elimination for all sets of rewrite rules. Let's see Crabbé's counter-example. With the rewrite rule :

$$A \rightarrow B \vee \neg A$$

we have the following proofs π and π':

$$\dfrac{\dfrac{\dfrac{\dfrac{}{A \vdash_{\mathcal{R}} B, A}}{\vdash_{\mathcal{R}} B, \neg A, A}}{\vdash_{\mathcal{R}} B \vee \neg A, A}}{\vdash_{\mathcal{R}} A} \qquad\qquad \dfrac{\dfrac{}{B \vdash_{\mathcal{R}} B} \quad \dfrac{\dfrac{\pi}{\vdash_{\mathcal{R}} A, B}}{\neg A \vdash_{\mathcal{R}} B}}{A \vdash_{\mathcal{R}} B}$$

Combining these two proofs with a cut, we get a proof of $\vdash_{\mathcal{R}} B$. Considering the first rule applied to B, we can see that there exist no cut-free proof of this sequent. Hence in this system, cut-elimination fails, even if this system is consistent.

2.2 Example of rewriting theories

We restrict to first-order predicate logic, possibly with sorts. However, thanks to the rewrite rules on propositions, HOL can be embedded in deduction modulo.

We define the terms of the theory. We use a many-sorted logic, thus we first define the types of the terms :

- ι and o are type

- if T and U are types, $T \to U$ is a type.

Then, we define some specific constants :

- $S_{T,U,V}$ is a symbol of the type $(T \to U \to V) \to (T \to U) \to T \to V$ for any types T, U, V
- $K_{T,U}$ is a symbol of type $T \to U \to T$ for any types T, U
- $\dot{\Rightarrow}, \dot{\vee}, \dot{\wedge}$ are symbols of type $o \to o \to o$
- $\dot{\neg}$ is a symbol of type $o \to o$
- $\dot{\exists}_T, \dot{\forall}_T$ are symbols of type $T \to o$ for any type T.
- For any types T, U, there's an application symbol, $\alpha_{T,U}$ of rank $\langle T \to U, T, U\rangle$, to combine terms. Thus, if f is a term of type $T \to U$ and x is a term of type T, $\alpha_{T,U}(f, x)$ is a term of type U

We will omit the types underscripts when there is no ambiguity. At last, we define an unique predicate symbol ε of rank $\langle o\rangle$.
Now, we have to define the rewrite rules of our theory :

- $\alpha(\alpha(\alpha(S, x), y), z) \to \alpha(\alpha(x, z), \alpha(y, z))$
- $\alpha(\alpha(K, x), y) \to x$
- $\varepsilon(\alpha(\alpha(\dot{\Rightarrow}, p), q)) \to \varepsilon(p) \Rightarrow \varepsilon(q)$
- $\varepsilon(\alpha(\dot{\neg}, p)) \to \neg\varepsilon(p)$
- $\varepsilon(\alpha(\alpha(\dot{\vee}, p), q)) \to \varepsilon(p) \vee \varepsilon(q)$
- $\varepsilon(\alpha(\alpha(\dot{\wedge}, p), q)) \to \varepsilon(p) \wedge \varepsilon(q)$
- $\varepsilon(\alpha(\dot{\forall}_T, p_{T\to o})) \to \forall x_T \varepsilon(\alpha(p, x))$
- $\varepsilon(\alpha(\dot{\exists}_T, p_{T\to o})) \to \exists x_T \varepsilon(\alpha(p, x))$

It can be proved that this rewrite system is confluent and terminating, see for example [8]. A term t is in β-normal form if it is in normal form (hence w.r.t. rules on combinators S and K). For any term t, we call $\beta(t)$ its normal form.

3 Definitions

Definition 3 (Confluence). *A rewrite system $\mathcal{R}$ is said to be* confluent *if for all proposition P such that $P \to^*_{\mathcal{R}} P'$ and $P \to^*_{\mathcal{R}} P''$, there exists Q such that $P' \to^*_{\mathcal{R}} Q$ and $P'' \to^*_{\mathcal{R}} Q$.*

Definition 4 (Termination). *Let $\mathcal{R}$ a rewrite system. He is said to be* terminating *if and only if for any term there exists a finite rewrite sequence starting from this term and ending in a normal term.*

He is said to be strongly terminating *if and only if all the rewrite sequences are finite.*

The following definitions are specific to the cut-free sequent calculus : instead of considering a theory with respect to provability in the sequent calculus, we consider it with respect to the cut-free calculus. This difference is visible in the cf superscript of the sequents. This difference reflects into the very formulation of these definitions : considering the cut-free calculus makes a distinction between formulations that were equivalents from the point of view of the calculus with cuts.

Definition 5 (Completeness). *A theory Γ is said to be complete iff for any proposition P: $\Gamma, P \vdash^{cf}_{\mathcal{R}}$ or $P \in \Gamma$.*

Definition 6 (Consistency). *A theory Γ is said to be consistent if and only if we can't prove the empty set of proposition.*
In our case, Γ is consistent iff $\Gamma \not\vdash^{cf}_{\mathcal{R}}$

Again, this definition is slightly different from the classical definitions of consistency:
Γ is inconsistent if and only if for any/at least one proposition P we have proofs of $\Gamma \vdash_{\mathcal{R}} P$ and of $\Gamma \vdash_{\mathcal{R}} \neg P$.
Proving equivalence between the two definitions requires the cut elimination theorem.

Definition 7. *A theory Γ admits Henkin witnesses iff for any proposition Q with one free variable x, there exists constants c, c' such that:*

$$\Gamma, \exists x Q \not\vdash^{cf}_{\mathcal{R}} \quad \textit{implies } Q[c/x] \in \Gamma$$
$$\Gamma \not\vdash^{cf}_{\mathcal{R}} \forall x Q \quad \textit{implies } \neg Q[c'/x] \in \Gamma$$

We will speak about a Henkin theory instead of a "theory that admits Henkin witnesses".

We quickly remind the definition of a structure for a one-sorted language:

Definition 8. *Let $\mathcal{L}$ be a language (a set of function, predicate and variable symbols), let P be a predicate symbol of rank n, and f a function of rank m of this language. A structure $\mathcal{M}$ is a set formed with a non empty set M (the domain), and for each predicate symbol P of rank n, and function f of rank m of the language $\mathcal{L}$:*

- *a function $\hat{P} : M^n \mapsto \{0, 1\}$*
- *a function $\hat{f} : M^m \mapsto M$*

Now for each term of the language, we define its interpretation under an assignment σ mapping any variable to a value in M:

Definition 9. *Let $\mathcal{L}$ a language, $\mathcal{V}$ its set of variables, $\mathcal{M}$ a structure. Let σ an assignment. We define by induction the interpretation of a term in $\mathcal{M}$ under this assignment :*

- *$|x|_\sigma = \sigma(x)$ where $x \in \mathcal{V}$*
- *$|f(t_1, ..., t_n)|_\sigma = \hat{f}(|t_1|_\sigma, ..., |t_n|_\sigma)$*

We define by induction the interpretation of a proposition under this assignment :

- *$|P(t_1, ..., t_n)|_\sigma = \hat{P}(|t_1|_\sigma, ..., |t_n|_\sigma)$*
- *$|\neg P|_\sigma = 1$ iff $|P|_\sigma = 0$ else $|\neg P|_\sigma = 0$*
- *$|P \vee Q|_\sigma = 1$ iff $|P|_\sigma = 1$ or $|Q|_\sigma = 1$, or else $|P \vee Q|_\sigma = 0$*

– $|P \wedge Q|_\sigma = 1$ *iff* $|P|_\sigma = 1$ *and* $|Q|_\sigma = 1$*, or else* $|P \wedge Q|_\sigma = 0$
– $|P \vee Q|_\sigma = 1$ *iff* $|P|_\sigma = 0$ *or* $|Q|_\sigma = 1$*, or else* $|P \vee Q|_\sigma = 0$
– $|\exists x P|_\sigma = 1$ *if there exists* $a \in M$ *such that* $|P|_{\sigma:\langle x,a\rangle} = 1$*, else* $|\exists x P|_\sigma = 0$
– $|\forall x P|_\sigma = 1$ *if for each* $a \in M$*,* $|P|_{\sigma:\langle x,a\rangle} = 1$*, else* $|\forall x P|_\sigma = 0$

We say that $\mathcal{M}$ is a model of a theory Γ is each proposition of Γ is interpreted by true (i.e. 1).

As we consider only ground propositions, it is easy to see that the interpretation of a proposition in the model does not depends on the assignment, so we will omit the subscript indicating the assignment, when it is not needed.

If the set M is the set (or a subset) of ground terms of $\mathcal{L}$, we won't speak about assignments, substituting on the fly the term to the free variable. For example, $|\forall x P| = 1$ iff for each ground term $|P[t/x]| = 1$. It can easily be shown to be an equivalent formulation.

We can extend smoothly this definition to many-sorted logic, adding a set M_s for each sort s, and interpreting propositions and functions accordingly.

When we construct a model, we see that it is necessary and sufficient to give the interpretation of each atom, and of any term. If we are not constructing a model in this way, then we have to prove the compatibility with definition 9.

The introduction of the rewrite rules justifies a new notion of model.

Definition 10 (Model for a rewrite system). *Let $\mathcal{M}$ be a structure. We say that it is a model of the rewrite rules if and only if for any propositions $P =_\mathcal{R} Q$ we have $\mathcal{M} \models P$ iff $\mathcal{M} \models Q$*

We will adopt the notation $\models_\mathcal{R}$ when a model is a model of the rewrite rules.

4 The cut elimination theorem

The cut elimination theorem is, as announced before, the result of the application of a soundness theorem with respect to semantical models, and a completeness theorem of the cut-free calculus with respect to these same models.

Proof of soundness is standard : all rules are valid, by a simple induction. For a complete proof, see [9].

Theorem 1 (Soundness). *If $\Gamma \vdash_\mathcal{R} \Delta$ then $\Gamma \models_\mathcal{R} \Delta$.*

The exact converse of this Soundness theorem is the Completeness theorem which was first proved by Gödel for natural deduction :

Theorem 2 (Completeness). *If $\Gamma \models_\mathcal{R} \Delta$ then $\Gamma \vdash_\mathcal{R} \Delta$*

If we add the more strict condition, that the sequent $\Gamma \vdash_\mathcal{R} \Delta$ must have a cut-free proof (replacing $\Gamma \vdash_\mathcal{R} \Delta$ with $\Gamma \vdash^{cf}_\mathcal{R} \Delta$), we get the :

Theorem 3 (Cut-elimination theorem). *Let $\mathcal{R}$ a set of rewrite rules such that $\Gamma \models_\mathcal{R} \Delta$ implies $\Gamma \vdash^{cf}_\mathcal{R} \Delta$*

$$\text{If } \Gamma \vdash_{\mathcal{R}} \Delta \text{ then } \Gamma \vdash^{cf}_{\mathcal{R}} \Delta$$

It now remains to find a condition on rewrite rules that assures that the completeness theorem for the cut-free calculus holds. Trying to prove it is, under the hypothesis of confluence of rewrite rules equivalent to prove the following result :

If a theory $\mathcal{T}$ (a possibly infinite set of axioms) is consistent (def. 6, then there exists a model of $\mathcal{T}$.

We now restrict ourselves to the construction of semantical models given a set of (cut-free) consistent axioms. We can narrow the problem even more and concentrate on building models of complete, consistent, Henkin theories. Indeed we will show in a first step that any consistent theory $\mathcal{T}$ is contained into a complete, consistent, Henkin theory Γ, provided that rewrite rules are confluent.

After having built such a theory, we will focus on the techniques for constructing models. In particular, defining a model is not self-evident, because we have to contstruct a model of the rewrite rules, following definition 10.

5 Key results in sequent calculus modulo

Note that in this whole section, we assume only confluence of the rewrite rules.

5.1 Some key lemmas

Since we are working in a new calculus (the *cut-free* sequent calculus *modulo*), we have to prove again even the most basic results. These results are very standard, maybe with exception of lemma 5.Some proofs lay in annex.

Under the hypothesis of confluence of the rewrite rules, we can by an easy induction prove the following lemma :

Lemma 1 (Connector). *let $P =_{\mathcal{R}} Q$ two non atomic proposition. P and Q have the same main connector.*

Proof : by confluence. The common reduct of P and Q has the same main connector than P and has the same main connector that Q, because we allowed rewrite rules only on atomic propositions. □

We can now prove the Kleene lemmas [10], that say that we can reverse rules. We distinguish the case of left rules and of right rules.

Lemma 2 (Kleene). *Let $A_1 =_{\mathcal{R}} ... =_{\mathcal{R}} A_n =_{\mathcal{R}} A$ be propositions. If the sequent :*

$$\Gamma, A_1, ..., A_n \vdash^{cf}_{\mathcal{R}} \Delta$$

is provable, then we can construct a proof of :

- *if $A = \neg P$: $\Gamma \vdash^{cf}_{\mathcal{R}} P, \Delta$*

- *if* $A = P \vee Q$ *:* $\Gamma, P \vdash^{cf}_{\mathcal{R}} \Delta$ *and* $\Gamma, Q \vdash^{cf}_{\mathcal{R}} \Delta$
- *if* $A = P \wedge Q$ *:* $\Gamma, P, Q \vdash^{cf}_{\mathcal{R}} \Delta$
- *if* $A = P \Rightarrow Q$ *:* $\Gamma, Q \vdash^{cf}_{\mathcal{R}} \Delta$ *and* $\Gamma \vdash^{cf}_{\mathcal{R}} P, \Delta$
- *if* $A = \exists x P$ *:* $\Gamma, P[c/x] \vdash^{cf}_{\mathcal{R}} \Delta$*, where* c *is a fresh constant.*

Lemma 3. *Let* $A_1 =_{\mathcal{R}} ... =_{\mathcal{R}} A_n =_{\mathcal{R}} A$ *be propositions. If the sequent :*

$$\Gamma \vdash^{cf}_{\mathcal{R}} A_1, ..., A_n, \Delta$$

is provable, then we can construct a proof of :

- *if* $A = \neg P$ *:* $\Gamma, P \vdash^{cf}_{\mathcal{R}} \Delta$
- *if* $A = P \wedge Q$ *:* $\Gamma \vdash^{cf}_{\mathcal{R}} P, \Delta$ *and* $\Gamma \vdash^{cf}_{\mathcal{R}} Q, \Delta$
- *if* $A = P \vee Q$ *:* $\Gamma \vdash^{cf}_{\mathcal{R}} P, Q, \Delta$
- *if* $A = P \Rightarrow Q$ *:* $\Gamma, P \vdash^{cf}_{\mathcal{R}} Q, \Delta$
- *if* $A = \forall x P$ *:* $\Gamma \vdash^{cf}_{\mathcal{R}} P[c/x], \Delta$*, where* c *is a fresh constant.*

Proof : By the the same induction over the proof structure as in 2. □

These lemmas stands for any connector rules of the sequent calculus, with exception of the ∀-left (in lemma 2 and of the ∃-right in lemma 3. That's the reason why we introduce lemma 5.

The following lemma can be taken as a remark on complete consistent Henkin theories and will be helpful in many cases :

Lemma 4. *Let* Γ *be a complete consistent Henkin theory. Then :*

- *if* $P \in \Gamma$ *and* $P =_{\mathcal{R}} Q$ *then* $Q \in \Gamma$
- *if* $\neg A \in \Gamma$ *then* $\Gamma \not\vdash^{cf}_{\mathcal{R}} A$
- *if* $A \vee B \in \Gamma$ *then* $A \in \Gamma$ *or* $B \in \Gamma$
- *if* $A \wedge B \in \Gamma$ *then* $A \in \Gamma$ *and* $B \in \Gamma$
- *if* $A \Rightarrow B \in \Gamma$ *then* $\Gamma \not\vdash^{cf}_{\mathcal{R}} A$ *or* $B \in \Gamma$
- *if* $\forall x A \in \Gamma$ *then for any term* t $A[t/x] \in \Gamma$
- *if* $\exists x A \in \Gamma$ *then there exists a* c *such that* $A[c/x] \in \Gamma$

on the same way, we have :

- *if* $\Gamma \not\vdash^{cf}_{\mathcal{R}} P$ *and* $P =_{\mathcal{R}} Q$, $\Gamma \not\vdash^{cf}_{\mathcal{R}} Q$
- *if* $\Gamma \not\vdash^{cf}_{\mathcal{R}} \neg A$ *then* $A \in \Gamma$
- *if* $\Gamma \not\vdash^{cf}_{\mathcal{R}} A \wedge B$ *then* $\Gamma \not\vdash^{cf}_{\mathcal{R}} A$ *or* $\Gamma \not\vdash^{cf}_{\mathcal{R}} B$
- *if* $\Gamma \not\vdash^{cf}_{\mathcal{R}} A \vee B$ *then* $\Gamma \not\vdash^{cf}_{\mathcal{R}} A$ *and* $\Gamma \not\vdash^{cf}_{\mathcal{R}} B$
- *if* $\Gamma \not\vdash^{cf}_{\mathcal{R}} A \Rightarrow B$ *then* $A \in \Gamma$ *and* $\Gamma \not\vdash^{cf}_{\mathcal{R}} B$
- *if* $\Gamma \not\vdash^{cf}_{\mathcal{R}} \exists x A$ *then for any term* t $\Gamma \not\vdash^{cf}_{\mathcal{R}} A[t/x]$
- *if* $\Gamma \not\vdash^{cf}_{\mathcal{R}} \forall x A$ *then there exists a* c *such that* $\Gamma \not\vdash^{cf}_{\mathcal{R}} A[c/x]$

Proof : We see only some significant cases, because proof is easy.

- The first case is very easy. If Γ, Q is inconsistent, Γ, P is inconsistent too.

- The last two cases are the definition of a Henkin theory.
- Let's focus on the fifth case : Γ is consistent, hence $\Gamma, A \Rightarrow B \nvdash^{cf}_{\mathcal{R}}$. Now, suppose that we have : $\Gamma \vdash^{cf}_{\mathcal{R}} A$ and $B \notin \Gamma$. That means that we have proofs of the following sequents (because Γ is complete) : $\Gamma \vdash^{cf}_{\mathcal{R}} A$ and $\Gamma, B \vdash^{cf}_{\mathcal{R}}$ Applying the $\Rightarrow$-left rule, we get that $\Gamma, A \Rightarrow B \vdash^{cf}_{\mathcal{R}}$ that is in contradiction with our hypothesis.
- The proof for the remaining cases are on the same way. □

We now introduce as announced, for complete Henkin theories, a more powerful lemma than the Kleene lemmas 2 and 3, because it works with all the rules (including $\forall$-left and $\exists$-right). The subtle point to understand is that when Γ is a theory with an infinite set of axioms, and when we write $\Gamma \vdash^{cf}_{\mathcal{R}} P$, we mean *a finite subset of* Γ entails P. And this subset will change within the proof of the lemma.

For example, let Γ_0 a finite subset of a complete Henkin theory Γ. if there exists a proof of $\Gamma_0 \vdash^{cf}_{\mathcal{R}} \exists x P$, lemma 5 gives us a proof of the sequent $\Gamma_1 \vdash^{cf}_{\mathcal{R}} \exists x P$ with a first rule on $\exists x P$, where Γ_1 is a finite subset of Γ.

As often in sequent calculus, we have to prove the result in a symmetric formulation of it, but further we will use a non-symmetric corollary (without the Δ set). We add some extra conditions that will be useful later in the proof, but that are unnecessary to the comprehension of the lemma :

Lemma 5. *Let Γ a complete consistent Henkin theory, and let $\Delta = \{P | \neg P \in \Gamma\}$. Then, if we have a proof of :*

$$\Gamma, \Gamma_1 \vdash^{cf}_{\mathcal{R}} \Delta_1, \Delta \tag{1}$$

we can construct a proof of this sequent whose first rule is on a proposition of Γ_1, Δ_1, whose number of rules on propositions coming from Γ_1, Δ_1 is preserved, and which height is less or equal than the height of (1).

5.2 Completion of a theory

Now, given a consistent theory $\mathcal{T}$, we construct a complete consistent Henkin theory containing $\mathcal{T}$, with respect to provability in the cut-free classical sequent calculus modulo. We suppose the theory is expressed in a denumerable language $\mathcal{L}$, to which we add a denumerable set of new constants $\mathcal{C}$, giving a new language $\mathcal{L}'$.

Definition 11 (Theory construction). *We let $\Gamma_0 = \mathcal{T}$, and we enumerate all the proposition of the language $\mathcal{L}'$:*

$$P_0, ..., P_n, ...$$

We define Γ_{n+1} by induction:

- *If* $P_n = \exists x Q$ *and if* $\Gamma_n, \exists x Q \nvdash^{cf}_{\mathcal{R}}$ *then let* $c \in \mathcal{C}$ *a constant that doesn't appear in* Γ_n. *This is possible, because a finite number of these constants appear in* $P_0, ..., P_n$, *and none appears in* $\Gamma_0 = \mathcal{T}$. *We let* $\Gamma_{n+1} = \Gamma_n \cup \{Q[c/x], P_n\}$.
- *If* $\Gamma_n, P_n \nvdash^{cf}_{\mathcal{R}}$ *then* $\Gamma_{n+1} = \Gamma_n \cup \{P_n\}$
- *If* $P_n = \forall x Q$, *if* $\Gamma_n, \forall x Q \vdash^{cf}_{\mathcal{R}}$ *and if* $\Gamma_n \nvdash^{cf}_{\mathcal{R}} \forall x Q$ *then we let* $\Gamma_{n+1} = \Gamma_n \cup \{\neg Q[c/x]\}$, c *being a fresh constant (with respect to* Γ_n*) of* $\mathcal{C}$. *There exists such a constant because* Γ_n *contains at most a finite number of constants in* $\mathcal{C}$ *: they can appear only in* $P_0, ..., P_n$.
- *Else, we let* $\Gamma_{n+1} = \Gamma_n$.

Finally, we take $\Gamma = \bigcup_{n=0}^{\infty} \Gamma_n$.

We easily check by induction that Γ_n is consistent for any n, so Γ itself is consistent. We then prove easily that Γ is complete and admits Henkin witnesses (if no, there exists a proposition P that contradicts these assertions, and by our former enumeration there exists an n such that $P = P_n$).

So, we get the result :

Any consistent theory is contained into a complete, consistent, Henkin theory

This construction is very similar to the one that can be found in [11], at one major difference : we have done it in the cut-free calculus (and some definitions have been changed on this purpose).

In sequent calculus without rewrite rules, once one has constructed a complete Henkin theory, one immediately gets a model. This is also the case here. But there's a problem we haven't addressed yet : will this model be a model of the rewrite rules ? This is the point that bears logical complexity, because rewrite rules add theoretical power to the calculus.

6 Model construction

Since there exists counter-example to cut-elimination for confluent rewrite systems (Crabbé's rule, and there's other counter-examples even for terminating cases [2]), we have to strengthen our hypothesis on rewrite rules. That's why in this section we need additionnal hypothesis. But they remain general enough to embed some large classes of rewrite rules.

6.1 An order condition

We suppose the existence of an order on propositions that have the following properties:

- for any proposition $P = A\ \mathcal{C}\ B$ where $\mathcal{C}$ is a binary connector $(\wedge, \vee, \Rightarrow)$, $P \succ A$ and $P \succ B$,
- $\neg P \succ P$,

- $\exists x P \succ P[t/x]$ for any ground term t,
- $\forall x P \succ P[t/x]$ for any ground term t,
- let t and t' be two propositions or ground terms such that $t \to_{\mathcal{R}} t'$. $t \succ t'$ (compatibility of the rewrite system and the order),
- $\succ$ is a well-founded order.

We will additionally suppose the rewrite system to be confluent. By the well-foundedness of the order, we get that the rewrite rules are terminating. Hence the normal form of a proposition exists and is unique.

A rewrite rule that fits these condition is for example $x*0 \to 0$. J. Stuber [12] gives a more extended example, formulating a piece of set theory with rewrite rules that satisfies this condition. The quantifier-free rewrite rules of [2] fits this condition too. We now construct the model, like in [12], using techniques inspired by L. Bachmair and H. Ganzinger for resolution.

We only consider the ground propositions of the language. For the domain of the structure $\mathcal{M}$ we take all ground normal terms. We naturally interpret a ground term by its normal form. We now define the interpretation of each atom, begining with normal atoms. For each normal atom, we let :

$$\begin{cases} \text{if } \Gamma, A \vdash^{cf}_{\mathcal{R}}, |A|_{\mathcal{M}} = 0 \\ \text{if } A \in \Gamma, |A|_{\mathcal{M}} = 1 \end{cases}$$

This definition is valid, because the theory is consistent. This definition holds for any normal atom A because Γ is a complete theory in the sense of definition 5.

Now we have defined the value for normal atoms, we define the interpretation of all the propositions of the language, beginning with the normal ones. For each normal proposition, we construct its tree.

- The tree for the proposition $A \vee B$ is a tree which root is $\vee$ and which sons are the two trees of the normal forms of A and B
- The tree of the normal proposition $\exists x A$ is a tree which root is labeled $\exists$ and which sons are the trees of the *normal* forms of $A[t/x]$, for each ground term t
- and so on for other connectors.

The tree is finite (in the sense that we can't find an infinite path), because each time we go down in the tree, we decrease the well-founded order $\succ$.

All the leaves are normal atoms, and we know how to assign a truth value of a normal atom. Thus we can give a truth value for the entire tree of a (normal) proposition :

- To a tree which root is $\vee$, we assign the 1 truth value if and only if at least one of its sons has the 1 thruth value, else we assign the 0 truth value.
- We assign the 1 truth value to a tree which root is $\exists$ if and only if at least one of its sons has the 1 truth value.

– and so on for the other connectors.

Finally, the truth value of a non-normal proposition is set as the truth value of its normal form.

We can easily check that the structure $\mathcal{M}$ constructed defines an interpretation, and that this is a model of the rewrite rules. Now, we have to check that $\mathcal{M}$ is a model of Γ. This is done by induction over the order $\succ$, using the fact that we have for each normal atom :

$$\Gamma, A \nvdash^{cf}_{\mathcal{R}} \text{ iff } \mathcal{M} \models A$$

We then use lemma 4, and use the fact that at every step time, we deconstruct a proposition or we rewrite it, so we decrease the well-founded order. □

6.2 Positive rewrite systems

In this section we suppose that the rewrite rules are confluent, terminating and that they verify the positivity condition [2] :

Definition 12. *A rewrite system is said to be positive if an atomic proposition rewrites into a proposition which atoms have only positive occurrences.*

This definition can be seen as following : an atomic proposition A rewrites to a proposition P which clausal form does not contain the $\neg$ connector. For example, the following rewrite rules is *not* positive, because B has a negative occurence :

$$A \rightarrow B \Rightarrow C$$

But the following are positive :

$$A \rightarrow (\forall x B[x]) \vee C$$
$$A' \rightarrow (\neg B') \Rightarrow C'$$

We already have a complete consistent Henkin theory, and we have to construct a model of it. The point is to construct a model not taking into account rewrite rules and to prove later that this is really a model of the rewrite rules. The domain of $\mathcal{M}$ is composed of all equivalence classes (modulo the rewrite rules) of ground terms.

For each ground atom (even *non-normal* ones) we define :

Definition 13.
– *if* $A \in \Gamma$ *then* $|A|_{\mathcal{M}} = 1$
– *if* $\Gamma \nvdash^{cf}_{\mathcal{R}} A$ *then* $|A|_{\mathcal{M}} = 0$
– *if* $\Gamma \vdash^{cf}_{\mathcal{R}} A$ *and* $\Gamma, A \vdash^{cf}_{\mathcal{R}}$ *then, we arbitrarly put* $|A|_{\mathcal{M}} = 0$

This definition is well formed. Indeed, the three cases are mutually exclusive, and describe all the possibility, since Γ is a complete, consistent theory. We have defined an interpretation, because we have defined it on each ground atom.

This is not hard to prove that $\mathcal{M}$ is a model of Γ using lemma 4. Indeed, when we break a proposition, we get *in fine* some (non-normal) atoms, that are already interpreted (this is the main difference with the previous construction of section 6.1).

Lemma 6. *$\mathcal{M}$ is a model of Γ*

Proof : In fact, we have to prove simultaneously the following. If P is a predicate, then :

$$\begin{cases} P \in \Gamma \text{ implies } |P|_{\mathcal{M}} = 1 \\ \Gamma \not\vdash^{cf}_{\mathcal{R}} P \text{ implies } |P|_{\mathcal{M}} = 0 \end{cases}$$

We prove it by induction over P. Let's see some key cases.

- If P is an atom, then we refer to the definition 13
- If $P = \neg Q$ and $P \in \Gamma$ that implies $\Gamma, P \not\vdash^{cf}_{\mathcal{R}}$ (by consistency), hence, by a contrapposition of Kleene lemma 3, we have $\Gamma \not\vdash^{cf}_{\mathcal{R}} Q$, hence $|Q| = 0$ by induction hypothesis, so $|P| = 1$ by definition 9.
- If $P = \neg Q$ and $\Gamma \not\vdash^{cf}_{\mathcal{R}} P$ then we use lemma 4.
- If $P = \forall x Q$ and $P \in \Gamma$, then by lemma 4 and induction hypothesis we get that for any term t we have $|Q[t/x]| = 1$ hence $|P| = 1$ because $\mathcal{M}$ is a model.
- If $P = \forall x Q$ and $\Gamma \not\vdash^{cf}_{\mathcal{R}} \forall x Q$, by lemma 4 we get (thanks to the fact that Γ is a Henkin theory, see definition 7) that there exists a constant c such that $\Gamma \not\vdash^{cf}_{\mathcal{R}} Q[c/x]$. So, $|Q[c/x]| = 0$ by induction hypothesis, and therefore $|P| = 0$. $\square$

We can remark that the third case of definition 13 doesn't occur at any time, just because of the cut elimination theorem (having the two proofs simultaneaously would imply that $\Gamma \vdash^{cf}_{\mathcal{R}}$). But since we are proving this very theorem, we are forced to take into account such cases.

It remains now to prove that $\mathcal{M}$ is a model of the rewrite rules. We can focus on rewriting atoms, because rewrite rules occurs on atoms. Thus, we have to check that if $A \to_{\mathcal{R}} P$, then $|A| = |P|$.

We distinguish three cases :

- if $A \in \Gamma$ then $|A|_{\mathcal{M}} = 1$, and $|P|_{\mathcal{M}} = 1$ because $\mathcal{M}$ is a model of Γ, and $P \in \Gamma$ by lemma 4
- if $\Gamma \not\vdash^{cf}_{\mathcal{R}} A$ then $|A|_{\mathcal{M}} = 0$ and $|P|_{\mathcal{M}} = 0$ because $\mathcal{M}$ is a model of Γ.
- if $\Gamma \vdash^{cf}_{\mathcal{R}} A$ and $\Gamma, A \vdash^{cf}_{\mathcal{R}}$, we can say nothing for now on $|P|_{\mathcal{M}}$, but we know that $|A|_{\mathcal{M}} = 0$, by definition 13.

To prove last case, we need the following lemma :

Lemma 7. *If $\Gamma, P^+ \vdash^{cf}_{\mathcal{R}}$ and $\Gamma \vdash^{cf}_{\mathcal{R}} P^+$ then $|P^+| = 0$.
If $\Gamma, P^- \vdash^{cf}_{\mathcal{R}}$ and $\Gamma \vdash^{cf}_{\mathcal{R}} P^-$ then $|P^-| = 1$.*

Here P^+ denotes a proposition having only positive occurence of atoms, and P^- a proposition having only negative occurence of atoms. For proof considerations, we need to prove it in a symmetric formulation, though only the positive part is of interest for us.

This lemma represents a new way to see cut-elimination for positive rewrite systems. It replaces the fixpoint construction in [2].

Proof of lemma is done by induction on the structure of P, using Kleene lemmas 2 and 3, and the following corollary of lemma 5, when Kleene lemma can't apply (so, in the $\forall$-left and $\exists$-right cases).

Corollary 1. *Let Γ be a complete consistent Henkin theory. Then, is we have a proof of the sequent $\Gamma, \Gamma_1 \vdash^{cf}_{\mathcal{R}} \Delta_1$, then we can find a proof of this same sequent such that :*

- *The number of rule applied to proposition coming from Γ_1, Δ_1 is preserved.*
- *the first rule is either a rule on a proposition of Γ_1, Δ_1 either a $\neg$-left rule on a proposition of Γ followed by an axiom rule on a proposition of Γ_1, Δ_1.*

Proof of lemma 7 : By induction over the structure of P. We will see only some significative results (the others are on the same way). We will note P^* and $\overline{P^*}$ a signed proposition when we don't care of its sign. (If $P^* = P^+$ then $\overline{P^*} = P^-$ and conversely).

- P^* is an atom A. That's the base case, and the definition of the model : $|P^*| = |P^+| = 0$
- $P* = A^* \vee B^*$. Then, we get, by Kleene lemmas 3, 2 proofs of :

$$\Gamma, A^* \vdash^{cf}_{\mathcal{R}}$$
$$\Gamma, B^* \vdash^{cf}_{\mathcal{R}}$$
$$\Gamma \vdash^{cf}_{\mathcal{R}} A^*, B^*$$

  If $* = +$, we have either $\Gamma \vdash^{cf}_{\mathcal{R}} A^+$ and by induction hypothesis $|A^+| = 0$, either $\Gamma \not\vdash^{cf}_{\mathcal{R}} A^+$, and by the proof of 6, $|A^+| = 0$. We can replace A by B, and hence we get $|A+ \vee B^+| = 0$.
  If $* = -$, we will prove that $|A^- \wedge B^-| = 1$. If there exists a proof of $\Gamma \vdash^{cf}_{\mathcal{R}} A^-$ we get the result by induction hypothesis ($|A \vee B| = |A^-| = 1$). Else $\Gamma \not\vdash^{cf}_{\mathcal{R}} A^-$ and thus, by Kleene lemma 2, $\Gamma, \neg A^- \not\vdash^{cf}_{\mathcal{R}}$. Equivalently, by 5, $\neg A \in \Gamma$. So, we turn back to the proof of $\Gamma \vdash^{cf}_{\mathcal{R}} A^-, B^-$ we have, add a $\neg$-right rule, and a contraction rule, and get a proof of $\Gamma \vdash^{cf}_{\mathcal{R}} B^-$. By induction hypothesis, we then have $|B^-| = 1$.
- $P^* = \neg\overline{Q^*}$. We can apply Kleene lemmas 3 and 2. We get two proofs of the sequents $\Gamma, \overline{Q^*} \vdash^{cf}_{\mathcal{R}}$ and $\Gamma \vdash^{cf}_{\mathcal{R}} \overline{Q^*}$. We can apply induction hypothesis and we get $|P^*| = \overline{|\overline{Q^*}|}$. So, $|P^+| = 0$ and $|P^-| = 1$.
- $P^* = \forall x Q^*[x]$. Kleene lemma 3 give us a proof π of $\Gamma \vdash^{cf}_{\mathcal{R}} Q^*[c/x]$ where c is a fresh constant.

We can replace c with any term t, provided a renaming of some other fresh constant of π, so we have for any ground term t proofs of :

$$\Gamma, \forall x Q^*[x] \vdash_{\mathcal{R}}^{cf} \tag{2}$$

$$\Gamma \vdash_{\mathcal{R}}^{cf} Q^*[t/x] \tag{3}$$

Let's consider the negative case first. Let t be a ground term. Either we have $\Gamma, A^-[t/x] \nvdash_{\mathcal{R}}^{cf}$ and we can conclude that $|A^-[t/x]| = 1$, either we have $\Gamma, A^-[t/x] \vdash_{\mathcal{R}}^{cf}$, and we get the same conclusion by induction hypothesis. So, for each ground term t, $|A^-[t/x]| = 1$, hence $|P^-| = 1$ by definition 9.

The positive case doesn't work in the same way. If there exists a ground term t such that $\Gamma, Q^+[t/x] \vdash_{\mathcal{R}}^{cf}$, we can apply induction hypothesis. $|Q^+[t/x]| = 0$, hence $|P^+| = 0$.
Else for any ground term t, $Q^+[t/x] \in \Gamma$, because Γ is complete. Suppose this is the case, we will derive a contradiction with the help of corollary 1. So, we have three hypothesis. This one, proofs of (2), and (3) for any ground t.
Having to deal with this contraction rule, we must be a little bit careful to derive a contradiction. We will derive this contradiction on the number of rules that we apply in a proposition derived from P in the sequent $\Gamma, P^+ \vdash_{\mathcal{R}}^{cf}$. Take a proof of such a sequent and call N the number of rules applied on propositions derived from P^+.

We can apply corollary 1. If we have a $\neg$-left followed by an axiom rule, then we would have $\neg P^+ \in \Gamma$ and we could derive the inconsistency of Γ from the proof of $\Gamma \vdash_{\mathcal{R}}^{cf} P^+$. We could do the same thing if this were a $\forall$-left rule on P, viz. for any ground t, $Q^+[t/x] \in \Gamma$ by hypothesis. So we must have a contraction on P as first rule, and we get the following proof :

$$\dfrac{\dfrac{\pi}{\Gamma, P_1^+, P_2^+ \vdash_{\mathcal{R}}^{cf}}}{\Gamma, P^+ \vdash_{\mathcal{R}}^{cf}}$$

Note that the number of rules applied on proposition derived from P_1, P_2 is $N - 1$, thanks to corollary 1.
We can apply on the same way $N - 1$ times corollary on the proof of $\Gamma, P_1^+, P_2^+ \vdash_{\mathcal{R}}^{cf}$. At the end, we get a proof π' of the sequent $\Gamma, P_1^+, ..., P_n^+ \vdash_{\mathcal{R}}^{cf}$ with no rule on $P_1^+ = P_2^+ = ... = P_n^+ = P^+$, not even an axiom rule. So they don't play any role in π' : we can delete them from the proof and we get a proof of the sequent $\Gamma \vdash_{\mathcal{R}}^{cf}$, that is, the inconsistency of Γ.
So in all the cases, we get a contradiction, and there must exists a ground term t such that $\Gamma, Q^+[t/x] \vdash_{\mathcal{R}}^{cf}$.

- The other cases are treated in the same way.

$\square$

Now it is easy to check that our model $\mathcal{M}$ is a model of rewrite rules. It is sufficent to check it on atomic propositions. Since we have $A \rightarrow_{\mathcal{R}} P^+$ for each rewrite rule (positive rewrite system), we have $|A|_{\mathcal{M}} = |P|_{\mathcal{M}}$ in the three cases :

$$\begin{array}{r} \Gamma, A \nvdash^{cf}_{\mathcal{R}} \\ \Gamma \nvdash^{cf}_{\mathcal{R}} A \\ \Gamma, A \vdash^{cf}_{\mathcal{R}} \text{ and } \Gamma \vdash^{cf}_{\mathcal{R}} A \end{array}$$

thanks to lemmas 7 and 6. □

6.3 HOL

We consider the rewrite rules of the section 2.2.

We first construct for the *terms* of the theory a structure following the construction of Andrews [5], Prawitz [6] and Takahashi [7]. Our construction is slightly different from the one of [5], because we consider another formulation of HOL (without λ binder but with combinators). Thus we don't have problems like α-equivalence, but we are forced to define the interpretation of $S_{T,U,V}$, $K_{T,U}$, and $\alpha(f,t)$ for any f,t.

To follow the construction of Andrews [5], we need to have a semi-valuation on terms.

Definition 14. *A semi-valuation $\parallel . \parallel$ on propositional terms (i.e. terms of type o) is a function which domain is a subset of the terms of type o and range $\{0,1\}$ such that :*

- *if $p \rightarrow^*_{\mathcal{R}} q$ then $\parallel p \parallel = \parallel q \parallel$*
- *if $\parallel \alpha(\dot{\neg}, p) \parallel = 0$ then $\parallel p \parallel = 1$*
- *if $\parallel \alpha(\dot{\neg}, p) \parallel = 1$ then $\parallel p \parallel = 0$*
- *if $\parallel \alpha(\alpha(\dot{\vee}, p), q) \parallel = 0$ then $\parallel p \parallel = \parallel q \parallel = 0$*
- *if $\parallel \alpha(\alpha(\dot{\vee}, p), q) \parallel = 1$ then $\parallel p \parallel = 1$ or $\parallel q \parallel = 1$*
- *if $\parallel \alpha(\dot{\forall}, p_{T\rightarrow o}) \parallel = 0$ then there exists a term t_T such that $\parallel \alpha(p,t) \parallel = 0$*
- *if $\parallel \alpha(\dot{\forall}, p_{T\rightarrow o}) \parallel = 1$ then for each term t_T, $\parallel \alpha(p,t) \parallel = 1$*

The definition is in the same way for the other quantifiers.

A term p of type o can rewrite into q only by the mean of rewrite rules on α symbol.

We can construct on the same model a semi-valuation definition on propositions. For example the condition on $\forall$ becomes :

if $\parallel \forall x_T P \parallel = 0$ then there exists a term t_T such that $\parallel P[x/t] \parallel = 0$.

With the help of lemma 4, this is very easy to construct a semi-valuation on propositions using Γ. Let :

$$P \in \Gamma \Rightarrow \| P \|= 1$$
$$\Gamma \nvdash^{cf}_{\mathcal{R}} P \Rightarrow \| \neg P \|= 0$$

Now we have to propagate this definition to the terms of type o (i.e. propositional terms) :

$$\| p_o \| \text{ is set to } \| \varepsilon(p_o) \|$$

This is easy to check that this is a semi-valuation on terms. For example if we have $\| \alpha(\dot{\neg}, p_o) \|= 1$ then we have $\| \varepsilon(\alpha(\dot{\neg}, p)) \|= 1$ hence $\| \neg\varepsilon(p) \|= 1$ by definition of our semi-valuation on propositions, hence $\| \varepsilon(p) \|= 0$, hence $\| p_o \|= 0$. We reason on the same way for all the other connectors. □

In fact, this is even a partial valuation, but this is of no interest here.

Having this semi-valuation on terms, we can now step by step follow the construction in Andrews [5], erasing the treatment of λ and adding definitions for S, K symbols. $\alpha(,)$ replaces the treatment of application.

We first define what a V-complex is, as in [5] :

Definition 15 (V-complex). *For each type T We define the set $\mathcal{D}_T$ of V-complexes as a pair by induction over the type structure :*

- *if T is o, then $\mathcal{D}_o = \{\langle t_o, v\rangle$, such that v is 1 or 0 and if $\| t_o \|$ is defined, then $v =\| t \|$ and t is in β normal form $\}$*
- *if α is ι, $\mathcal{D}_\iota = \{\langle t_\iota, \iota\rangle\}$ for each t_ι in β-normal form.*
- *ifα is $A \to B$, then $\mathcal{D}_{A\to B} = \{\langle t_{A\to B}, f_{\mathcal{D}_A \to \mathcal{D}_B}\rangle\}$, where t is in β-normal form, and f is a function from $\mathcal{D}_A$ into $\mathcal{D}_B$ such that for each V-complex $\langle t'_A, g\rangle \in \mathcal{D}_A$, we have $f(\langle t'_A, g\rangle) = \langle \beta(\alpha(t, t')_B), h\rangle \in \mathcal{D}_B$.*

ι in the second member of $\mathcal{D}_\iota$ doesn't play any role further. It should be understand as a dummy constant. $\mathcal{D}_{\mathcal{T}}$ is the domain of the type T. The key point of the construction is that when the semi-valuation can't decide the truth value of a term of type o, then we give it both.

First of all, we associate to each ground term of type T a cannonical element in $\mathcal{D}_T$:

Lemma 8 (Cannonical elements). *To each term t_A, we can associate a V-complex $\langle \beta t, f_{t_A}\rangle \in \mathcal{D}_A$*

Proof : By induction over the type structure of A. For ι, to any t_ι we associate $\langle \beta(t_\iota), \iota\rangle$. To each t_o we associate $\langle \beta(t_o), v\rangle$ if $v =\| t_o \|$ if defined. Else we put arbitrarly $v = 1$.

Consider the case of a term t of type $A \to B$. We let $f_{t_{A\to B}}$ be the function from $\mathcal{D}_A$ to $\mathcal{D}_B$ such that for any $\langle t'_A, g\rangle \in \mathcal{D}_A$:

$$f_{t_{A\to B}}(\langle t'_A, g\rangle) = \langle \beta(\alpha(t_{A\to B}, t'_A,)), f_{\beta(\alpha(t_{A\to B}, t'_A,)B)}\rangle$$

which is a V-complex defined by construction.

It is easy to check that these elements are V-complexes. □

Now we can define interpretation of all terms modulo an assignment σ mapping variables of type T into $\mathcal{D}_T$, let $|t_T|_\sigma$.
We let C^1 and C^2 the first and second components of a V-complex C, and σ^1 an assignment mapping variables x of type T to $\sigma(x)^1$ (hence to a ground term in β-normal form in $\mathcal{D}_T$).

Not surprisingly, we define the first component of $|t_A|_\sigma$ in the following way :

$$|t_A|^1_\sigma = \beta(\sigma^1 t_A)$$

We then define the second component of $|t_A|_\sigma$ by induction over the structure of the term t_A. At each step, we will have to check that we really get a V-complex.

- t is a variable x_A, then we put $|x|^2_\sigma = \sigma(x)^2$. Thus, we have $|x|_\sigma = \sigma(x)$.
- t is a constant c_A. Following lemma 8, we let $|c_A|^2_\sigma$ be the function f_{c_A}. Then we have $|c_A| = \langle c_A, f_{c_A}\rangle$, the cannonical element of $\mathcal{D}_A$ associated to c_A.
- t is a $K_{A,B}$ symbol. Let $|K_{A,B}|^2_\sigma$ be the following function f :

  $$\begin{aligned} \mathcal{D}_A &\longrightarrow \mathcal{D}_{B\to A} \\ \langle t_A, g\rangle &\longmapsto \langle \alpha(K, t_A), h\rangle \end{aligned}$$

  where h is the following function :

  $$\begin{aligned} \mathcal{D}_B &\longrightarrow \mathcal{D}_A \\ \langle t'_B, i\rangle &\longmapsto \langle t_A, g\rangle \end{aligned}$$

  It remains now to prove that $|K|_\sigma = \langle K, f\rangle$ is a V-complex of type $A \to B \to A$. We know that $\langle t_A, g\rangle$ is in $\mathcal{D}_A$ by definition. So h is really a function from $\mathcal{D}_B$ to $\mathcal{D}_A$. Moreover, $\beta\alpha(\alpha(K, t_A), t'_B) = t_A$ because t_A is in normal form.
  Thus $\langle \alpha(K, t_A), h\rangle \in \mathcal{D}_{B\to A}$, and f is really a function from $\mathcal{D}_A$ to $\mathcal{D}_{A\to B}$. At last $\alpha(K, t_A)$ is in normal form, because t_A is. So f is the expected function, and $\langle K, f\rangle$ is in $\mathcal{D}_{A\to B\to A}$.
- t is a $S_{T,U,V}$ symbol. Things are the same as in the previous case. We let $|S_{T,U,V}|^2_\sigma$ be the following function f :

  $$\begin{aligned} \mathcal{D}_{T\to U\to V} &\longrightarrow \mathcal{D}_{(T\to U)\to T\to V} \\ \langle t_{T\to U\to V}, g\rangle &\longmapsto \langle \alpha(S, t), h\rangle \end{aligned}$$

  where h is the following function :

  $$\begin{aligned} \mathcal{D}_{T\to U} &\longrightarrow \mathcal{D}_{T\to V} \\ \langle t'_{T\to U}, i\rangle &\longmapsto \langle \alpha(\alpha(S, t), t'), j\rangle \end{aligned}$$

where j is the following function :

$$\begin{aligned} \mathcal{D}_T &\longrightarrow \mathcal{D}_V \\ \langle t''_T, k\rangle &\longmapsto \langle \beta\alpha(\alpha(t,t''),\alpha(t',t''))_V, l\rangle \end{aligned}$$

where $l = (g(\langle t''_T, k\rangle)^2\,(i(\langle t''_T, k\rangle)))^2$.

We check on the same way as in the previous case that the defined terms are V-complexes.

- t is a $\dot{\neg}$ connector. We let $\mid \dot{\neg} \mid^2_\sigma = f$ a function from $\mathcal{D}_o$ to $\mathcal{D}_o$ such that :

  $$f(\langle P_o, v\rangle) = \langle \dot{\neg}\ P_o, \overline{v}\rangle$$

  where $\overline{v}$ is 1 if $v = 0$ and 0 if $v = 1$. So we have $\mid \dot{\neg} \mid_\sigma = \langle \dot{\neg}, f\rangle$

  It remains to prove that when we apply f to a V-complex of type o, we get back a V-complex of the right shape (see definition 15). If P_o is in normal form, then $\dot{\neg}\ P_o$ is in n.f. too, so the first member is as expected. If $\|\dot{\neg}\ P_o\|$ is not defined, then by definition, we have a V-complex.

  If, say $\|\dot{\neg}\ P_o\| = 1$, by definition of a semi-valuation, we must have $\|\ P_o\| = 0$, and we see that, for $\langle P_o, v\rangle$ to be a V-complex, we must have $v = 0$, so $\langle \dot{\neg}\ P_o, \overline{v}\rangle$ is a V-complex too, because compatible with the semi-valuation.
- t is a $\dot{\vee}$ connector. On the same way, we have $\mid \dot{\vee} \mid_\sigma = \langle \dot{\vee}, f\rangle$, where f is define as follows :

  $$\begin{aligned} \mathcal{D}_o &\longrightarrow \mathcal{D}_{o\to o} \\ \langle A_o, v\rangle &\longmapsto \langle \alpha(\dot{\vee}, A_o)_{o\to o}, g\rangle \end{aligned}$$

  where g is the following function :

  $$\begin{aligned} \mathcal{D}_o &\longrightarrow \mathcal{D}_o \\ \langle B_o, w\rangle &\longmapsto \langle \alpha(\alpha(\dot{\vee}, A_o), B_o), v \vee w\rangle \end{aligned}$$

  $v \vee w$ stands is 1 if one at least of the v and w is 1 else it is 0. As in the previous case, we have to check that we really have a V-complex. This is done in the same way.
- t is a $\dot{\forall}_A$ connector. Then, we have $\mid \dot{\forall} \mid_\sigma = \langle \dot{\forall}_A, f\rangle$, where f is defined as follows :

  $$\begin{aligned} \mathcal{D}_{A\to o} &\longrightarrow \mathcal{D}_o \\ \langle p_{A\to o}, g\rangle &\longmapsto \langle \dot{\forall}_A\ p, v\rangle \end{aligned}$$

  Where $v = 1$ iff $g(\langle t_A, h\rangle) = \langle \_, 1\rangle$ for each V-complex $\langle t, h\rangle \in \mathcal{D}_A$.

  We yet have to prove that $\langle \dot{\forall}\ p, v\rangle$ is a V-complex of type o, and of the expected shape. The first component is not a problem. We just consider the case when $\|\dot{\forall}\ p_o\|$ is defined, the other is trivial.

  Suppose it's equal to 1, that means that for each term t_A, we have $\|\ \alpha(p_{A\to o}, t_A)_o\ \| = 1$, and, because semi-valuations are compatible with rewrite rules, we have $\|$

$\beta(\alpha(p_{A\to o}, t_A)_o) \| = 1$ So, each V-complex of the form $\langle \beta(\alpha(p_{A\to o}, t_{A,)}\ o), w\rangle$ is such that $w = 1$, by definition 15.
$\langle p_{A\to o}, g\rangle$ is a V-complex, so we have $g(\langle t_A, h\rangle) = \langle \beta(\alpha(p_{A\to o}, t_A)), w\rangle$ hence $w = 1$. By our definition, we set $v = 1$, and $\langle \dot{\forall}_p, v\rangle$ is a V-complex.

Suppose now $\|\dot{\forall}\ p_o \| = 0$. Let t_{0_A} a term such that $\|\ \alpha(p_{A\to o}, t_0) \| = 0$. Any V-complex $\langle q_o, w\rangle$ such that $q_o =_{\mathcal{R}} \alpha(p_{A\to o}, t_{O_A})$ must have $w = 0$.
This is in particular the case for $g(\langle t_0, f_{t_0}\rangle) = \langle \beta(\alpha(p_{A\to o}, t_{O_A},)), w\rangle$, where f_{t_0} is th cannonical function defined in lemma 8. Hence we set $v = 0$, and $\langle \dot{\forall}_p, v\rangle$ is a V-complex.

In conclusion, f is really a function from $\mathcal{D}_{A\to o}$ to $\mathcal{D}_o$, and gives the expected results. $\langle \dot{\forall}_,\ f\rangle$ is a V-complex.

- The remaining logical connectors are treated on the same way as these three ones.
- t_B is $\alpha(t_{A\to B}, t'_{A,)}\ B$. We let $|t_B|^2_\sigma = (|t_{A\to B}|^2_\sigma\ |t'_A|_\sigma)^2$. The definition is correct because $|t_{A\to B}|_\sigma$ and $|t'_A|_\sigma$ are defined by induction. We can check that $(|t_{A\to B}|^2_\sigma\ |t'_A|_\sigma)^1 = \beta\alpha(t_{A\to B}, t'_A)$, because $|t_{A\to B}|_\sigma, |t'_A|_\sigma$ are V-complex respectively of the shape $\langle \beta(t), f\rangle, \langle \beta(t'), g\rangle$, and because $\beta\alpha(t, t') = \beta(\alpha(\beta(t), \beta(t')))$.

  So, we have he following statement, that we will re-use : $|\alpha(t, t')|_\sigma = |t|^2_\sigma |t'|_\sigma$

We have intepreted all terms. Hence, by a standard model interpretation, we are ready to interpret the proposition :

Definition 16. *Let P be a proposition of the language and σ an assignment mapping free variables into V-complexes. We define $|P|_\sigma$ by induction over the structure of the proposition:*

- *if $P = \varepsilon(p)$ we let $|P|_\sigma = |p|^2_\sigma$*
- *if $P = A \vee B$ we let $|P|_\sigma = 1$ iff $|A|_\sigma = 1$ or $|B|_\sigma = 1$*
- *if $P = \exists_A x Q$ we let $|P|_\sigma = 1$ iff there exists a V-complex $c \in \mathcal{D}_A$, such that : $|Q|_{\sigma:(c/x)} = 1$*
- *and so on for other connectors, as in definition 9*

We could have chose another definition, proving that for any proposition P, there corresponds a unique term t_o such that $P = \varepsilon(t_o)$ and setting $|P|_\sigma = |p|^2_\sigma$. Definition 16 avoids the problem of proving existence of p, but raises another problem : is the model constructed a model of rewrite rules ? The answer is given by the following lemma.

Lemma 9. *Let p be a term or a proposition, and σ an assignment. If $p \to_{\mathcal{R}} q$ then $|p|_\sigma = |q|_\sigma$.*

The model constructed is a model of Γ, because interpretation in the models fits with the interpretation with semi-valuation (where it is defined), so every proposition in Γ is true in the model, and the model is a model of the rewrite rules.

6.4 A counterexample to normalization

We here consider a modification of the terminating, confluent rewrite rule of [2]. The rule is the following :

$$R \in R \to_{\mathcal{R}} \forall y(y \simeq R \Rightarrow \neg y \in R)$$

where $\neg A$ is equivalent to $A \Rightarrow \bot$, and $y \simeq z$ stands for $\forall x(y \in x \Rightarrow z \in x)$.

We can refine this rule, replacing $\neg A$ with $A \Rightarrow C$, where C is a proposition (for the moment unspecified) :

$$R \in R \to_{\mathcal{R}} \forall y(y \simeq R \Rightarrow (y \in R \Rightarrow C)) \tag{4}$$

As in [2], we can construct intuitionnistic cut-free proofs π and π' of the sequents $R \in R \vdash^{cf}_{\mathcal{R}} C$, and $\vdash^{cf}_{\mathcal{R}} R \in R$.

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{}{R \in R, C \vdash^{cf}_{\mathcal{R}} C} \quad \dfrac{}{R \in R \vdash^{cf}_{\mathcal{R}} R \in R}}{R \in R, (R \in R \Rightarrow C) \vdash^{cf}_{\mathcal{R}} C} \quad \dfrac{\dfrac{\dfrac{}{R \in R, R \in R_0 \vdash^{cf}_{\mathcal{R}} R \in R_0}}{R \in R \vdash^{cf}_{\mathcal{R}} R \in R_0 \Rightarrow R \in R_0}}{R \in R \vdash^{cf}_{\mathcal{R}} R \simeq R}}{R \in R, R \simeq R \Rightarrow (R \simeq R \Rightarrow C) \vdash^{cf}_{\mathcal{R}} C}}{R \in R, R \in R \vdash^{cf}_{\mathcal{R}} C}}{R \in R \vdash^{cf}_{\mathcal{R}} C}$$

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\pi}{R \in R, R_0 \in R \vdash^{cf}_{\mathcal{R}} C} \quad \dfrac{}{R_0 \in R \vdash^{cf}_{\mathcal{R}} R_0 \in R}}{(R_0 \in R \Rightarrow R \in R), R_0 \in R \vdash^{cf}_{\mathcal{R}} C}}{R_0 \simeq R, R_0 \in R \vdash^{cf}_{\mathcal{R}} C}}{R_0 \simeq R \vdash^{cf}_{\mathcal{R}} R_0 \in R \Rightarrow C}}{\vdash^{cf}_{\mathcal{R}} (R_0 \simeq R \Rightarrow (R_0 \in R \Rightarrow C))}}{\vdash^{cf}_{\mathcal{R}} R \in R}$$

Proofs terms are the same as in [2]. So we can have a proof of $\vdash_{\mathcal{R}} C$ combining π and π'. But this involves a cut :

$$\dfrac{\pi \quad \pi'}{\vdash_{\mathcal{R}} C}\ \text{cut}$$

This is not hard to see that we don't have any mean to prove intuitionnistically $\vdash^{cf}_{\mathcal{R}} C$ without a cut : there is no rule applyable but the cut rule. So the normalization algorithm fails, although this calculus may be consistent (depending on proposition C).

As C is unspecified in 4, we can replace C by any proposition, including a classical tautology that is *not an intuitionnistic tautology*, for example the standard one $A \vee \neg A$ for some A. We get a specialized rule (4_A). We don't have any mean to prove $\vdash^{cf}_{\mathcal{R}} A \vee \neg A$ in cut-free intuitionnistic sequent calculus : this is the excluded middle rule, and no rule other than $\vee$-right can apply. So the intuitionnistic calculus doesn't have the cut-elimination property and doesn't normalize.

But in classical sequent calculus, we have a (trivial) cut-free proof :

$$\dfrac{\dfrac{\overline{A \vdash^{cf}_{\mathcal{R}} A}}{\vdash^{cf}_{\mathcal{R}} A, \neg A}}{\vdash^{cf}_{\mathcal{R}} A \vee \neg A}$$

In fact, we are going to see that the classical calculus features the cut elimination property, constructing as before a model for any complete, consistent Henkin theory with the rewrite rule (4_A).

Let Γ be such a theory. We define our model not taking into account the rewrite rule, just like in section 6.2, by defining the truth value of each atomic predicate :

$$|B| = 1 \text{ if } B \in \Gamma$$
$$|B| = 0 \text{ if } \Gamma \not\vdash^{cf}_{\mathcal{R}} B$$
$$|B| = 1 \text{ if } \Gamma \vdash^{cf}_{\mathcal{R}} B \text{ and } \Gamma, B \vdash^{cf}_{\mathcal{R}}$$

The domain for the term is the set of ground terms. We have obviously constructed a model of Γ. It remains to prove that this is a model of the rewrite rules. We check it only on atoms. In fact, there is only one atom in non-normal form : $R \in R$. Note that $|R \in R| = 1$ since we have a proof of the empty sequent $\vdash^{cf}_{\mathcal{R}} R \in R$ (so a proof of $\Gamma \vdash^{cf}_{\mathcal{R}} R \in R$ for any Γ). We have to prove that $|\forall y(y \simeq R \Rightarrow (y \in R \Rightarrow C))| = 1$, with $C = A \vee \neg A$.

The key point is that $|C| = 1$, because either $|A| = 1$, either $|\neg A| = 1$ (we have a classical model). So, $t \in R \Rightarrow C$ is true for any ground term t. Hence, whatever the truth value of $|t \simeq R|$, we get that, for any ground term t, $|(t \simeq R \Rightarrow (t \in R \Rightarrow C))| = 1$, and finally $|\forall y(y \simeq R \Rightarrow (y \in R \Rightarrow C))| = 1$. $\square$

7 Conclusion

Deduction modulo is a uniform way to study cut elimination of axiomatic theories, integrating axioms into the deduction rules. It enhances the power of the deduction system, as we have seen, we can express powerful theories and remain into first-order logic.

The link between cut-elimination and normalization is not as simple as it appeared, although the model constructions have many common points with pre-model construction [2]. The method employed seems a little bit more general, since we are able to prove cut-elimination even for non normalizing systems. It even seems that we can extend this result to the intuitionnistic logic.

References

1. Dowek, G., Hardin, T., Kirchner, C.: Theorem proving modulo. Journal of Automated Reasoning **31** (2003) 33–72
2. Dowek, G., Werner, B.: Proof normalization modulo. The Journal of Symbolic Logic **68** (2003) 1289–1316
3. Dowek, G., Werner, B.: Peano's arithmetic as a theory modulo. Types for Proofs and Programs 98 (1999) 62–77
4. Gentzen, G.: Untersuchungen uber das logische Schliessen. Mathematische Zeitschrift (1934) 176–210, 405–431
5. Andrews, P.B.: Resolution in type theory. The Journal of Symbolic Logic **36** (1971) 414–432
6. Prawitz, D.: Hauptsatz for higher order logic. The Journal of Symbolic Logic **33** (1968) 452–457
7. Takahashi, M.o.: A proof of cut-elimination theorem in simple type-theory. Journal of the Mathematical Society of Japan **19** (1967) 399–410
8. Dowek, G.: Introduction to proof theory. Course notes for the 13th European Summer School in Logic, Language and Information (2001)
9. Hermant, O.: A model-based cut elimination proof. 2nd St-Petersburg Days of Logic and Computability (2003)
10. Kleene, A.C.: Permutability of inferences in Gentzen's calculi LK and LJ. Memoirs of the American Mathematical Society **10** (1952) 1–26, 27–68
11. Cori, R., Lascar, D.: Logique mathématique. Masson (1993)
12. Stuber, J.: A model-based completness proof of extended narrowing and resolution. IJCAR-2001 (2001) 195–210
13. Szabo, M.E., ed.: Collected Papers of Gerhard Gentzen. Studies in Logic and the Foundation of Mathematics. North Holland Publishing Company, Amsterdam (1969)
14. Schűtte, K.: Syntactical and semantical properties of simple type theory. The Journal of Symbolic Logic **25** (1960) 305–326
15. Smullyan, R.M.: First-Order Logic. Springer-Verlag, Berlin Heidelberg New York (1968)

Annex

7.1 Proof of lemma 2

By induction over the proof structure, considering the first rule applied.

If the first rule is a rule r on a proposition of Γ, Δ, then we apply the induction hypothesis on the premises of this rule, and obtain proofs to which we apply the same rule r. Let's give the example for the last point of the lemma (this is the most difficult) :

– If the first rule is, say, a $\vee$-left on $B \vee C \in \Gamma$, then by induction hypothesis, we get two proofs :

$$\frac{\pi}{\Gamma', B, P[c/x] \vdash^{cf}_{\mathcal{R}} \Delta} \qquad\qquad \frac{\pi'}{\Gamma', C, P[c'/x] \vdash^{cf}_{\mathcal{R}} \Delta}$$

We take a constant d fresh in both proofs π and π'. We replace c by d everywhere in π and c' by d everywhere in π'. Hence we get proofs of $\Gamma', B, P[d/x] \vdash^{cf}_{\mathcal{R}} \Delta$ and $\Gamma', C, P[d/x] \vdash^{cf}_{\mathcal{R}} \Delta$. We can then apply the rule $\vee$-left on these two sequents and get the required proof.

– If the first rule is a $\forall$-left, then, applying the induction hypothesis, we get a proof of $\Gamma', B[t/x], P[c/x] \vdash^{cf}_{\mathcal{R}} \Delta$, c being a fresh constant, hence, does not appear in t. We can apply the rule $\forall$-left without problem.

– If the first rule is an $\exists$-left, we apply the induction hypothesis on the premise and get a proof of $\Gamma', B[c/x], P[d/x] \vdash^{cf}_{\mathcal{R}} \Delta$. c and d are fresh constants and are different. Hence, we can apply the rule $\exists$-left.

– We handle the other rules in the same way.

If the first rule is a rule on one of the $A_1, ..., A_n$ (suppose it is A_1) :

– If it's a weak-left, then we apply induction hypothesis on the premise and get the needed proof(s). In the case $n = 1$, we have no more propositions $A_1, ..., A_n$. We just have to apply a weak rule (maybe 2 different times) to get the needed proof(s).

– If it's a contraction, then we apply the induction hypothesis.

– If it's an axiome rule, let's see the case where A is of the shape $\exists x P$. We have :

$$\frac{}{\Gamma, A_1, ..., A_n \vdash^{cf}_{\mathcal{R}} B, \Delta'}\ \text{axiom}$$

with $B \cup \Delta' = \Delta$. We replace this proof by the following proof :

$$\frac{\dfrac{}{\Gamma, P[c/x] \vdash^{cf}_{\mathcal{R}} P[c/x], \Delta'}\ \text{axiom}}{\Gamma, P[c/x] \vdash^{cf}_{\mathcal{R}} B, \Delta'}\ \exists\text{-right}$$

we can do that because we don't have any freshness condition when applying $\exists$-right. We can do the same for any connector, but the $\forall$-left, because this one needs a fresh constant. That's the reason why we don't have the Kleene lemma for the $\forall$-left rule.

– If it is a connector rule. Suppose $A = B \vee C$. Then we have the following premises :
$\Gamma, B, A_2, ..., A_n \vdash^{cf}_{\mathcal{R}} \Delta$ $\qquad\qquad$ $\Gamma, C, A_2, ..., A_n \vdash^{cf}_{\mathcal{R}} \Delta$
we apply the induction hypothesis, get proofs of :

$$\Gamma, B, C \vdash^{cf}_{\mathcal{R}} \Delta \qquad\qquad \Gamma, C, C \vdash^{cf}_{\mathcal{R}} \Delta$$
$$\Gamma, B, B \vdash^{cf}_{\mathcal{R}} \Delta \qquad\qquad \Gamma, C, B \vdash^{cf}_{\mathcal{R}} \Delta$$

and we apply a contraction rule on the two useful proofs to get proofs of what we needed.
We have the same things for all the other connectors, but $\exists$. Here, we do the following : the premise is $\Gamma, P[c/x], A_2, ..., A_n \vdash^{cf}_{\mathcal{R}} \Delta$. Applying the inductive hypothesis, we get a proof π of $\Gamma, P[c/x], P[d/x] \vdash^{cf}_{\mathcal{R}} \Delta$, where d is fresh. In order to apply the contraction rule, we replace in π th constant d by c.
– We can't have other rules on $A_1, ..., A_n$, because of lemma 1.

□

7.2 Proof of lemma 5

By induction over the proof height, considering the last rule applied, and lemma 4 or definition 7 if this last rule is applied on Γ of Δ. We check that we have $\Gamma = \{P, \neg P \in \Delta\}$, because Γ is complete, and if $P \in \Gamma$, $\neg\neg P \in \Gamma$, by lemma 2 and 3, and we note that hypothesis that height is less or equal is essential, because this is our induction hypothesis.

If the first rule is a rule on Γ_1, Δ_1, there's nothing to do and we get the proof we wanted.

If the fisrt rule is an axiom, then it applies at least to one proposition of Γ_1, Δ_1. Else we would have $P \in \Gamma$ and $P =_{\mathcal{R}} Q \in \Delta$. By definition of Δ, $\neg P \in \Gamma$, so we can prove $\Gamma \vdash^{cf}_{\mathcal{R}}$ (inconsistency of Γ).

Now, we consider the case of a first rule on Γ or on Δ, that doesn't touch any of the propositions in Γ_1, Δ_1. This can't be an axiom, by the upper argument. Then :

– if it's a contraction or a weakening, we apply the induction hypothesis on the premise and we get what we wanted, because we continue to have a subset of Γ (or Δ), so the premise is of the shape $\Gamma, \Gamma_1 \vdash^{cf}_{\mathcal{R}} \Delta_1, \Delta$.
– If it is a $\vee$-left on a proposition of Γ, then we get proofs of the sequent $\Gamma, A, \Gamma_1 \vdash^{cf}_{\mathcal{R}} \Delta_1, \Delta$ and of $\Gamma, B, \Gamma_1 \vdash^{cf}_{\mathcal{R}} \Delta_1, \Delta$. By lemma 4 we get that either $A \in \Gamma$, either $B \in \Gamma$. Hence one of these two proofs is in fact a proof of $\Gamma, \Gamma_1 \vdash^{cf}_{\mathcal{R}} \Delta_1, \Delta$, and we can apply the induction hypothesis to this proof and get what we wanted.

– If it is a $\vee$-right on a proposition, we can on the same way apply the induction hypothesis to the sequent $\Gamma, \Gamma_1 \vdash_{\mathcal{R}}^{cf} \Delta_1, A, B, \Delta$, because $A, B \in \Delta$: since $A \vee B \in \Delta$ we have $\neg(A \vee B) \in \Gamma$, and so, $\Gamma, \neg(A \vee B) \not\vdash_{\mathcal{R}}^{cf}$. Hence $\Gamma \not\vdash_{\mathcal{R}}^{cf} A \vee B$, and by lemma 4 we get that $\Gamma \not\vdash_{\mathcal{R}}^{cf} A$ and $\Gamma \not\vdash_{\mathcal{R}}^{cf} B$. Applying Kleene's lemma 2 we get the conclusion that $\Gamma, \neg A \not\vdash_{\mathcal{R}}^{cf}$ and $\Gamma, \neg B \not\vdash_{\mathcal{R}}^{cf}$, hence by definition 5 that $\neg A, \neg B \in \Gamma$, and eventually $A, B \in \Delta$ by definition of Δ.
– The other cases are treated exactly in the same way, except from the $\exists$-left and $\forall$-right, that don't use lemma 4, but that use the definition 7 of Henkin witnesses instead.

It's now easy to check that the number of rules on Γ_1, Δ_1 is less or equal, that the height is less or equal and that the first rule is on a proposition of Γ_1, Δ_1. As said before, the trick of the lemma is that when we write Γ, we mean only a subset Γ. Of course, we strongly used the three properties that Γ is complete, consistent and admits Henkin witnesses. □

7.3 Proof of corollary 1

We apply lemma 5 and get a proof of $\Gamma, \Gamma_1 \vdash_{\mathcal{R}}^{cf} \Delta_1, \Delta$ (Remember that we have finite subsets of Γ and Δ). We distinguish cases on the first rule applied (that concerns, in any cases, at least one proposition of Γ_1, Δ_1).

– It's an axiom on some common proposition of Γ and Δ_1. That's what we wanted : the subset of Δ plays no role, so take it empty.
– It's an axiom on the proposition P of Γ_1 and Δ. Since $P \in \Delta$, we have that $\neg P \in \Gamma$ by definition of Δ. Hence, we can have a proof of $\Gamma, \Gamma_1 \vdash_{\mathcal{R}}^{cf} \Delta_1$ with a $\neg$-left rule on $\neg P$ and an axiom. That's what we wanted.
– It's an axiom on a common proposition of Γ_1, Δ_1. Then we have a proof of $\Gamma_1 \vdash_{\mathcal{R}}^{cf} \Delta_1$
– Else, we have a rule r on one proposition of Γ_1, Δ_1, and a non-empty proof π over this rule. The subsets of Γ, Δ are left unchanged when passing through this rule. We can hence insert $\neg$-right rules at the bottom of π and apply the same rule r and we get a proof of $\Gamma, \neg\Delta, \Gamma_1 \vdash_{\mathcal{R}}^{cf} \Delta_1$. We now remember the definition of Δ and check that $\neg\Delta \subset \Gamma$. So, we have a proof of $\Gamma, \Gamma_1 \vdash_{\mathcal{R}}^{cf} \Delta_1$ with a first rule on Γ_1, Δ_1.

In all these cases, we check that we didn't changed the number of rules on Γ_1, Δ_1 (we only moved them within the proof), so that the announced property is true. But we could have increased proof height (we don't care). □

7.4 Proof of lemma 9

By induction over the structure of p. We distinguish cases if P is a proposition or if p is a term. Let's begin with the proposition case.

– if $P = \varepsilon(p) \to_{\mathcal{R}} Q = \varepsilon(q)$ then $p \to_{\mathcal{R}} q$ and by induction hypothesis, $|p|_\sigma = |q|_\sigma$, then by definition of $|.|_\sigma$ on propositions, $|P|_\sigma = |Q|_\sigma$.

- if $P = A \vee B$ then, either $A \to_{\mathcal{R}} A'$, either $B \to_{\mathcal{R}} B'$ ($\to_{\mathcal{R}}$ is a one-step reduct). By induction hypothesis $|A|_\sigma = |A'|_\sigma$ in the first case, and $|B|_\sigma = |B'|_\sigma$ in the second case. Thus by definition of $|.|_\sigma$ on propositions, $|P|_\sigma = |Q|_\sigma$.
- if $P = \forall_A x P'$ then $P' \to_{\mathcal{R}} P''$, and $|P'|_{\sigma:(c/x)} = |P''|_{\sigma:(c/x)}$ for all V-complex $c \in \mathcal{D}_A$ by induction hypothesis. Then $|P|_\sigma = |Q|_\sigma$.
- we apply the same methods for the other connectors.

Now, we have the base cases.

- if $P = \varepsilon(\alpha(\dot{\neg}, p)) \to_{\mathcal{R}} \neg\varepsilon(p)$. We set $Q = \varepsilon(p)$. Then, let $|p|_\sigma = \langle \beta(p), w\rangle$, and $|\alpha(\dot{\neg}, p)|_\sigma = |\dot{\neg}|^2_\sigma |p|_\sigma = \langle \beta(\dot{\neg}\ p), \overline{w}\rangle$, by definition. Thus, $|P|_\sigma = \overline{|Q|_\sigma}$, that is what we wanted.
- if $P = \varepsilon(\alpha(\alpha(\dot{\vee}, a), b)) \to_{\mathcal{R}} \varepsilon(a) \vee \varepsilon(b)$ then $|\varepsilon(a) \vee \varepsilon(b)|_\sigma = 1$ iff $|a|^2_\sigma = 1$ or $|b|^2_\sigma = 1$. Let's now look at $|\alpha(\alpha(\dot{\vee}, a), b)|^2_\sigma$. We have :
$$\begin{aligned} |\alpha(\alpha(\dot{\vee}, a), b)|^2_\sigma &= (|\alpha(\dot{\vee}, a)|^2_\sigma |b|_\sigma)^2 \\ &= ((|\dot{\vee}|^2_\sigma |a|_\sigma)^2 |b|_\sigma)^2 \end{aligned}$$
And this is equal to 1 iff, by definition of $|\dot{\vee}|^2_\sigma$, $|a|^2_\sigma = 1$ or $|b|^2_\sigma = 1$.
- if $P = \varepsilon(\alpha(\dot{\forall}_A, p_{A\to o},)) \to_{\mathcal{R}} \forall_A x \varepsilon(\alpha(p, x))$. First notice that x should not be free in p.
Then $|\forall x \varepsilon(\alpha(p, x))|_\sigma = 1$ iff for all V-complex $c \in \mathcal{D}_A$, we have $|\varepsilon(\alpha(p, x))|_{\sigma:(c/x)} = 1$, that is to say $|\alpha(p, x)|^2_{\sigma:(c/x)} = (|p|^2_{\sigma:(c/x)} |x|_{\sigma:(c/x)})^2 = 1$. But $|x|_{\sigma:(c/x)} = c$ hence, the condition for $|\forall x \varepsilon(\alpha(p, x))|_\sigma$ to be equal to 1 becomes that for each $c \in \mathcal{D}_A$, we have $(|p|^2_{\sigma:(c/x)} c)^2 = 1$.
Since x is not free in p, this is easy to check that $|p|_{\sigma:(c/x)} = |p|_\sigma$.
The condition transforms into : $|\forall x \varepsilon(\alpha(p, x))|_\sigma = 1$ iff $(|p|^2_\sigma c)^2 = 1$ for any $c \in \mathcal{D}_A$. This is the definition of $(|\dot{\forall}|^2_\sigma |p|_\sigma)^2 = 1$.
But, by our former remark, we have $|\alpha(\dot{\forall}, p)|_\sigma = |\dot{\forall}|^2_\sigma |p|_\sigma$. So the proof is done : $|\forall x \varepsilon(\alpha(p, x))|_\sigma = 1$ iff $(|\dot{\forall}|^2_\sigma |p|^2_\sigma)^2 = |\alpha(\dot{\forall}, p)|^2_\sigma = 1$
- The other connectors are treated in a similar way.

Now suppose p is a term of type A. We could apply to it only two kind of rewrite rules : those on S terms, and those on K terms. Thus we have the following cases :

- p is $\alpha(t, u)$ with $t \to_{\mathcal{R}} t'$, $u \to_{\mathcal{R}} u'$ (either $t = t'$ either $u = u'$). By induction hypothesis (or by identity), we have $|t|_\sigma = |t'|_\sigma$ and $|u|_\sigma = |u'|_\sigma$. This is a property of the application α that we have $|\alpha(t, u)|_\sigma = |t|^2_\sigma |u|_\sigma = |t'|^2_\sigma |u'|_\sigma = |\alpha(t', u')|_\sigma$.
- $\alpha(\alpha(K_{T,U}, x), y) \to_{\mathcal{R}} x$. By definition of $|K|_\sigma$ we have :
$$\begin{aligned} |\alpha(\alpha(K, x), y)|_\sigma &= (|K|^2_\sigma |x|_\sigma)^2 |y|_\sigma \\ &= |x|_\sigma \end{aligned}$$
- $\alpha(\alpha(\alpha(S, x), y), z) \to_{\mathcal{R}} \alpha(\alpha(x, z), \alpha(y, z))$. We have :
$$|\alpha(\alpha(\alpha(S, x), y), z)|_\sigma = ((|S|^2_\sigma |x|_\sigma)^2 |y|_\sigma)^2 |z|_\sigma$$

□