UNIVERSITÉ PARIS 7 – DENIS DIDEROT
UFR D'INFORMATIQUE

THÈSE

pour l'obtention du diplôme de

DOCTEUR DE L'UNIVERSITÉ PARIS 7
Spécialité programmation : sémantique, preuves, langages

présentée et soutenue publiquement

par

Olivier Hermant

le 6 Décembre 2005

TITRE :

MÉTHODES SÉMANTIQUES EN DÉDUCTION MODULO

Thèse dirigée par :

M. Gilles Dowek

Jury :

MM.	Thierry	Coquand	Rapporteurs
	Mitsuhiro	Okada	
MMes.	Thérèse	Hardin	Examinateurs
	Délia	Kesner	
MM.	Jean	Goubault-Larrecq	
	James	Lipton	

Жанне

Remerciements

Je tiens tout d'abord à remercier Thierry Coquand et Mitsuhiro Okada qui, malgré leur emploi du temps très chargé ont accepté de rapporter cette thèse. Leurs commentaires m'ont été très précieux, et ont éclairé mon travail sous un angle nouveau.

Mes remerciements vont ensuite aux membres du jury, pour la spontanéité avec laquelle ils ont accepté d'en faire partie. Merci donc à Thérèse Hardin, pour l'accueil qu'elle m' aréservé dans son équipe de recherche. Merci aussi à Délia Kesner, Jean Goubault-Larrecq et à James Lipton pour l'intérêt qu'ils portent à mon travail.

Gilles Dowek, qui a accepté d'encadrer cette thèse, a joué un rôle crucial dans son élaboration. Ses intuitions, ses commentaires et ses suggestions se sont toujours révélés extrêmement féconds. Que ces quelques mots puissent rendre compte ne serait-ce que d'un dixième de ce qu'il m'a apporté.

L'environnement de travail est souvent ce qu'il y a de plus important, mais on s'en aperçoit toujours trop tard. Merci donc à tous les membres de l'équipe Logical, en particulier Hugo Herbelin, Bruno Barras, Jean-Pierre Jouannaud et Benjamin Werner pour leurs conseils. Merci aussi à tous les thésards, en particulier à Florent Kirchner, Sylvain Lebresne, Julien Narboux, François-Régis Sinot, à Benjamin Grégoire ainsi qu'à tous ceux que je n'ai pas la place de citer.

Plusieurs équipes de recherche ont joué un rôle très important durant ces trois ans, en particulier le projet jumeau Proval, dont je remercie tous les membres. Merci aussi aux membres du laboratoire d'informatique de l'École polytechnique, qui m'a accueilli pendant plus de deux ans.

Cette thèse a le mérite d'être prête à temps grâce à Alexandre Miquel, que je remercie pour son entousiasme communicatif, mais aussi pour son lavage de cerveau à la suédoise.

Je dois aussi plusieurs fières chandelles aux secrétaires que j'ai pu rencontrer pendant ma thèse. Elles m'ont toujours aidé beaucoup plus que leur devoir ne le leur imposait. Merci, entre autres, à Catherine Moreau.

L'orthographe de cette thèse aurait pu être encore plus médiocre si elle n'avait reçu l'aide précieuse d'Anna Adamenko et de Guillaume Burel. Merci à eux.

Merci aussi à toute ma famille et à mes amis, pour leur soutien moral.

Je n'aurais jamais eu le courage de faire de la science sans le formidable soutien de ma femme Janna. Ce travail existe parce qu'elle l'a supporté de bout en bout. Je ne saurais la remercier assez. Cette thèse, bien plus qu'à moi ou à Gilles, lui appartient.

Introduction

Dès la fin du XIX$^{\text{ème}}$ siècle, des philosophes et des mathématiciens tels que Frege, ont ressenti le besoin de formaliser la notion de démonstration d'une manière plus profonde que ce que nous avons hérité de la Grèce Antique à travers la logique d'Aristote, par exemple.

Cette motivation est liée à l'apparition de preuves faisant appel à des raisonnements et des concepts de plus en plus abstraits, et aussi à la volonté de définir de manière rigoureuse la notion de nombre entier. Elle fut renforcée par la découverte de paradoxes comme ceux de Burali-Forti ou de Russell.

Ainsi, Frege puis Hilbert introduisirent la notion formelle de démonstration. Dans le système de déduction de Hilbert, existe un certain nombre d'axiomes logiques (tels que $A \Rightarrow B \Rightarrow A$) auxquels on ajoute des axiomes "impropres", c'est à dire spécifiques à la théorie considérée (par exemple, pour l'arithmétique, $x + S(y) = S(x) + y$). On y prouve une proposition P par l'utilisation d'axiomes ou de propositions déjà prouvées, au moyen de deux règles de déduction : le *Modus Ponens* et *Généralisation*.

Jaskowski apporta avec la *déduction naturelle* une notion de démonstration plus intuitive, sans axiomes logiques, mais avec un plus grand nombre de règles de déduction.

Formaliser ces différentes notions de démonstration, n'implique cependant pas leur cohérence : nous ne sommes toujours pas certains de ne pas pouvoir prouver n'importe quoi.

La théorie des modèles, formalisée par Tarski dans les année 30 du siècle dernier, permit de répondre d'une manière fine. La notion de modèle permit de mieux comprendre celle de cohérence et de démontrer la cohérence des règles de déduction. Supposons qu'il existe un modèle où toutes les règles de déduction et tous les axiomes sont valides (on dit qu'il est clos par déduction), alors tous les théorèmes sont valides (théorème de correction). Il s'ensuit non seulement qu'une proposition démontrable est vraie dans tous les modèles de la théorie, mais aussi qu'on ne peut démontrer les propositions non valides dans ce modèle.

Le développement de cette théorie, qui continue à ce jour (pour un nombre toujours plus important de systèmes de déduction), amena à poser la question de l'existence d'une réciproque au théorème de correction. En y répondant par l'affirmative, dans le cadre de la déduction naturelle, Gödel [23] prouva l'un des résultats majeurs (le théorème de complétude) de la branche des mathématiques qu'était devenue la logique.

Une avancée majeure dans la compréhension des preuves fut apportée par Gentzen en 1933 ([21]), lorsqu'il introduisit le calcul des séquents, un système de déduction dans lequel les preuves s'effectuent en travaillant à la fois sur les hypothèses et sur la conclusion, tandis que les systèmes précédents essayaient de former la conclusion à partir d'hypothèses quasi-immuables. Cela fait donc du calcul des séquents un système de déduction adapté à la démonstration automatique.

Un autre avantage du calcul des séquents de Gentzen est qu'il met en avant une notion qui était jusque là mal définie : la notion de coupure, qui correspond à celle de preuve en forme normale (en déduction naturelle). Dans la formulation de Gentzen, cette notion apparaît comme une règle distincte, ce qui en facilite la compréhension.

La règle de coupure est une règle de déduction utilisée dans quasiment toutes les démonstrations en mathématiques, en particulier lorsqu'on utilise un lemme intermédiaire. Le théorème d'élimination des coupures énonce que l'on peut se passer de démontrer ce lemme, et qu'il suffit de redémontrer le lemme dans notre cas particulier.

Dans [20], Gentzen prouve que la règle de coupure dans son calcul des séquents est redondante en trouvant une façon de transformer les démonstrations du calcul des séquents. Ce résultat a pour corollaire le fait que le calcul des séquents est cohérent (et de ce fait, la déduction naturelle et les systèmes de déduction *à la* Hilbert). Ce résultat est obtenu de manière purement syntaxique. C'est la base de ce qui devint ensuite, développée par Prawitz, Tait puis Girard en 1972, la méthode de normalisation des démonstrations.

Une autre méthode d'élimination de la règle de coupure, différente de la normalisation et qui s'appuie sur la notion de modèle, fit sont apparition dans les années 50. On remarqua (Beth, Hintikka, Kanger et Schütte) que des méthodes sémantiques pouvaient être appliquées à l'élimination de la règle de coupure en prouvant un théorème de complétude renforcé : si une proposition est vraie dans tous les modèles, alors elle est démontrable sans la règle de coupure. Ces techniques furent développées ensuite par Tait pour la Logique du Second Ordre puis Takahashi, Prawitz et Andrews pour la Logique d'Ordre Supérieur.

Le théorème de normalisation est plus fort que celui d'élimination des coupures sémantique puisqu'il l'implique. Cependant, dans de nombreux cas, par

exemple la démonstration automatique, seul importe le fait que la règle de coupure soit redondante, de manière à pouvoir travailler sans la règle de coupure. La résolution ou la méthode des tableaux ont besoin de ce résultat pour être complètes.

On peut donc espérer avoir des démonstrations d'élimination des coupures plus simples que celles de normalisation. De plus, il est théoriquement possible de savoir prouver l'élimination des coupures sans avoir la propriété de normalisation. Nous reviendrons sur ce point par la suite.

Inversement, il est dans certains cas possible de définir une translation des méthodes de normalisation vers les méthodes sémantiques, ce que fait Okada [35]. L'existence de la réciproque est un problème ouvert, dont la résolution permettrait d'unifier les deux approches d'élimination des coupures.

Une des difficultés dans cette approche est que l'élimination des coupures a été étudiée pour la logique des prédicats, pour la logique d'ordre supérieur et pour certaines théories comme l'arithmétique sans qu'on puisse en tirer une étude uniforme qui puisse s'appliquer à n'importe quelle théorie axiomatique. La notion de coupure dans ces différents systèmes est en effet loin d'être uniforme.

L'axiome de l'arithmétique dont nous avons parlé plus haut ($x + S(y) = S(x) + y$) n'est pas une définition très heureuse. Quel écolier, si on lui donne $3 + 5$ nous répondra $4 + 4$? C'est un exemple de la régression obtenue lors de la formalisation des mathématiques par les logiciens. En voulant trop abstraire, toute notion de calcul a été oubliée, alors qu'elle est au coeur des mathématiques depuis des millénaires.

Le calcul revint sur le devant de la scène à partir du milieu du XX$^{\text{ème}}$ siècle, avec l'apparition des ordinateurs, l'invention du λ-calcul et de ses versions typées. De plus, l'échec de la réalisation d'un programme qui pourrait prouver tous les théorèmes mathématiques fit progressivement comprendre que pour qu'un ordinateur soit capable de démontrer un théorème, il ne fallait pas, lors de la résolution de problèmes simples comme $2 + 2 = 4$, essayer de tout prouver par la déduction, mais de laisser la place au calcul. En effet, on se priverait alors de ce que les ordinateurs savent faire mille fois mieux qu'aucun être humain, fût-il Jacques Inaudi.

Ainsi, les axiomes peuvent être remplacés par des règles de réécriture. Par exemple, on peut définir la règle :

$$x + S(y) \rightarrow S(x + y)$$

Il faut ensuite se préoccuper d'intégrer les règles de réécriture dans les systèmes de déduction. Ce paradigme se retrouve dans de nombreux travaux tels que ceux de Church, Andrews, Plotkin, Huet ou Boyer-Moore.

Ces notions ont abouti à la formulation de Dowek, Hardin et Kirchner [16], la Déduction Modulo. Elle représente une manière la plus générale possible d'introduire des règles de réécriture dans les règles de déduction. L'idée est que

tout ce qui relève du calcul n'est pas pertinent pour un être humain (comme par exemple le fait que $2 + 2$ s'évalue en 4). Ainsi, la déduction modulo est un formalisme où les règles de réécriture sont intégrées aux règles de déduction, plutôt que de former un ensemble de règles à part. Les preuves deviennent alors plus compactes et plus lisibles.

Puisqu'une notion de calcul y est explicitement introduite, la déduction modulo se prête bien à la démonstration automatique. Une recherche automatique de preuve est ainsi beaucoup plus orientée que dans le cas où nous avons des axiomes. On pourrait par exemple passer des heures à prouver que la proposition $2 + 2 = 4$ est équivalente à $1 + 3 = 4$ elle-même équivalente à $2 + 2 = 4$, ce que nous évitons en déduction modulo.

Une idée centrale de la Déduction Modulo a été la possibilité de réécrire non seulement des termes (comme $2 + 2$), mais aussi des propositions (comme "2 est pair"). Cette possibilité permet d'exprimer des théories telles que la Logique d'Ordre Supérieur ou la théorie des ensembles de Zermelo dans le cadre de la Déduction Modulo, c'est à dire dans une formulation au premier ordre, et sans axiomes.

La Déduction Modulo permet de traiter de manière uniforme le problème des coupures axiomatiques. Dans les théories axiomatiques il existe en effet plusieurs types de coupure *ad hoc* (coupures de récurrence, coupures d'égalité). Les méthodes d'élimination des coupures dont nous avons précédemment parlé doivent ainsi démontrer que toutes les formes de coupures peuvent être éliminées.

En Déduction Modulo, le fait de ne pas avoir d'axiomes, mais des règles de réécriture intègre dans la règle de coupure "usuelle" toutes les coupures *ad hoc*. Ainsi, le problème de l'élimination des coupures devient bien posé, puisque nous n'avons plus qu'une sorte de coupure à étudier, et montrer l'élimination des coupures en Déduction Modulo implique l'élimination de toutes les coupures dans les théories axiomatiques correspondant.

Comme dans tous les systèmes de déduction, la propriété d'élimination des coupures en Déduction Modulo implique des propriétés essentielles telles que la cohérence du calcul, celle du témoin ou l'analyticité. Cette dernière propriété est importante dans le cadre du développement de programmes de démonstration automatique.
Une discussion plus détaillée de la règle de coupure est effectuée au chapitre 1, lorsque nous définirons le calcul des séquents.

Ce sont les raisons pour lesquelles il est primordial d'étudier l'élimination des coupures en Déduction Modulo. Cependant – contrepartie de la puissance théorique de la Déduction Modulo – le théorème d'élimination des coupures n'est pas valable pour toutes les ensembles de règle de réécriture. Des méthodes pour prouver la normalisation ont été définies par Dowek et Werner dans [17], dans la ligne de celles de Girard.

Un des buts de notre travail a été de développer des méthodes sémantiques

permettant de prouver la propriété d'élimination des coupures, qui soient assez générales pour être appliquées à de vastes classes de systèmes de réécriture. La définition de telles méthodes forme la contribution principale de cette thèse, dont l'ordre supérieur est un cas particulier.

Parmi ces conditions, nous pourrons retrouver les conditions "standard" telles que confluence et terminaison. Cependant, elles ne sont pas suffisantes, comme le montre un contre-exemple développé par Gilles Dowek et Benjamin Werner [17]. Nous reprendrons cet exemple plus loin, et l'étendrons pour montrer que certaines théories cohérentes n'ont pas la propriété d'élimination des coupures, puis exhiber une théorie n'ayant pas la propriété d'élimination des coupures bien que possédant celle de normalisation.

Après une partie où nous rappellerons les définitions du calcul des séquents modulo et de sa sémantique, nous prouverons quelques résultats élémentaires sur ce calcul. En particulier, nous démontrerons que le théorème de Skolem s'étend à la déduction modulo, ce qui constituera une première application des méthodes sémantiques en déduction modulo.

Ces chapitres formeront la base de ce qui est la partie centrale de notre thèse, où nous montrerons nos deux théorèmes principaux : une théorème d'élimination des coupures pour le calcul des séquents modulo classique, et son alter ego pour le calcul des séquents modulo intuitionniste. Nous conclurons cette partie par un chapitre qui discutera des liens entre les propriétés de normalisation et d'élimination des coupures.

Enfin, nous nous intéresserons à un système utilisé en démonstration automatique : la résolution modulo. Nous prouverons l'équivalence de ce dernier système avec le fragment sans coupures du calcul des séquents modulo.

Première partie

Syntaxe et Sémantique de la Déduction Modulo

Chapitre 1

Le Calcul des Séquents

Dans ce chapitre, nous présentons la syntaxe des calculs des séquents modulo classique et intuitionniste. Nous en donnons plusieurs formulations, ainsi que les preuves de leur équivalence.

1.1 Le langage

1.1.1 Les propositions et les termes

Comme dans la logique des prédicats, nous considérons un langage $\mathcal{L}$ formé :
- de symboles de prédicat, notés : $P, Q, R, ...$, d'arité n quelconque.
- de symboles de fonction d'arité n (les constantes sont des symboles de fonction d'arité 0)

Et un ensemble dénombrable $\mathcal{V}$ de symboles de variables, notés : $x, y, ...$

Enfin, nous avons des symboles de connecteurs, permettant de connecter les propositions entre elles. Nous avons trois connecteurs propositionnels :

$$\wedge \quad \vee \quad \Rightarrow$$

qui sont d'arité 2 (et sont habituellement respectivement nommés `et`, `ou` et `implique`), et un connecteur propositionnel :

$$\neg$$

qui est d'arité 1 et se nomme `non`. Nous avons aussi deux quantificateurs universels et existentiels (quel que soit, il existe) :

$$\forall \qquad \exists$$

Nous pouvons combiner ces différents éléments ensemble, nous donnons les règles de combinaisons dans les deux définition 1.1 et 1.2 ci-dessous. Par exemple avec P, Q prédicat à une variable, $+$ symbole de fonction à deux variables, nous pouvons former $P(+)$ mais nous ne pouvons par former $P + Q$ (qui n'est

pas un terme bien formé). Pour les fonctions et les prédicats d'arité n, nous représenterons en générale ses arguments entre parenthèses ($P(f(b), a)$ au lieu de $Pfba$), et nous utiliserons une notation infixe pour les connecteurs logiques, quitte à utiliser des parenthèses. Nous noterons $A \vee (B \wedge C)$ au lieu de $\vee A \wedge BC$. Lorsque nous parlerons d'un connecteur propositionnel sans le préciser, nous utiliserons la notation $\underline{c}$, de même que pour les quantificateurs nous utiliserons la notation $\underline{\mathcal{Q}}$.

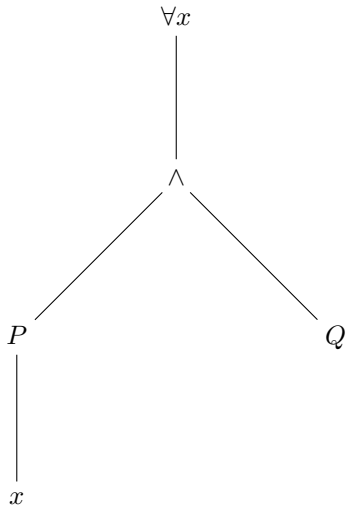
Puisque tous les termes ne sont pas bien formés, voici les définitions de ce que sont un terme bien formé, puis une formule bien formée :

Définition 1.1 (Terme bien formé). *Un terme est bien formé si :*
- *c'est une variable,*
- *c'est un symbole de fonction f d'arité n appliqué à n arguments qui sont eux-mêmes des termes bien formés.*

Définition 1.2 (Formule bien formée). *Une formule est bien formée si :*
- *c'est un symbole de prédicat d'arité n appliqué à n termes bien formés (définition 1.1),*
- *c'est un connecteur propositionnel $\underline{c}$ d'arité n appliqué à n arguments qui sont eux-même des formules bien formées ($A \vee B$ par ex.),*
- *c'est un quantificateur, suivi d'un symbole de variable, et suivi d'une formule bien formée ($\forall x P$).*

Nous emploierons très souvent le terme proposition au lieu de formule bien formée. De même le terme atome, ou proposition atomique est une abréviation de prédicat d'arité n appliqué à n arguments.

Les deux définitions 1.1 et 1.2 définissent formellement un terme (respectivement, une formule) comme un arbre. Par exemple, la proposition $\forall x(P(x) \wedge Q)$ représente en fait l'arbre suivant :



Une variable x est dite libre lorsqu'elle ne dépend d'aucun quantificateur, c'est à dire que dans l'arbre de dérivation de la formule, n'est pas située sous un quantificateur ayant comme argument x.

Si une variable n'est pas libre, on dit qu'elle est liée. Par exemple x est libre dans $\exists y P(x, y)$, mais y y est liée (par le quantificateur $\exists$).

Pour avoir une définition formelle de ce que nous avons présenté ci-dessus, il faut commencer par définir ce qu'est l'occurrence d'une variable (ou d'un terme, ou d'une constante, ou d'une proposition) dans une formule : c'est l'endroit à laquelle on le rencontre dans l'arbre de dérivation (donc, si l'on code les chemins de l'arbre par une suite de 0 et de 1, c'est une suite d'entiers). Par exemple, dans la formule :

$$P(x, x) \vee Q(x, y)$$

le symbole de prédicat Q a une occurrence, de même que l'atome $Q(x, y)$. Par contre la variable x en a trois. Nous parlerons de la première occurrence de x, de la deuxième, etc, en fonction de l'ordre d'apparition de x dans le parcours en profondeur d'abord, avec priorité à gauche de l'arbre de dérivation de la formule (qui correspond au parcours gauche-droite classique dans notre notation des formules).

Les notations préfixes, infixes et postfixes ne modifient pas l'ordre des occurrences.

Définition 1.3. *Si x a une occurrence dans P, cette occurrence est dite libre dans P ssi :*

- *P est un atome.*
- *P est une formule du type $\underline{Q}yR$ ($\underline{Q}$ est un quantificateur), $x \neq y$, et l'occurrence de x est libre dans R.*
- *P est une formule du type $Q\underline{c}R$, où $\underline{c}$ est un connecteur propositionnel, et si l'occurrence de x est dans Q, alors celle-ci est libre dans Q (resp. si elle est dans R, alors celle-ci est libre dans R).*

L'occurrence d'une variable qui n'est pas libre est dite liée.

Une formule est close si et seulement si toutes les occurrences de toutes ses variables sont liées.

Un terme est clos si et seulement si il ne comporte pas de variables.

Une variable z est fraîche *par rapport à une formule ssi elle n'a aucune occurrence (ni libre, ni liée) dans cette formule.*

Une constante c est fraîche *par rapport à une formule ssi elle n'a aucune occurrence dans cette formule.*

Un terme t est frais *par rapport à une formule F ssi tous les termes de $\mathcal{L} \cup \mathcal{V}$ qui le composent sont frais dans F.*

Si nous avons une formule du type $P(x) \vee (\forall x Q(x))$, alors la première occurrence de x est libre, mais la seconde est liée. Même si ce genre de formule est bien formé, nous éviterons de les écrire sous cette forme. Il vaudra mieux considérer la formule $P(x) \vee (\forall y Q(y))$. Ces deux formules sont équivalentes, et ce problème est connu sous le nom d'α-équivalence (équivalence alphabétique) en théorie de

la démonstration, et sous le nom de variable muette en mathématiques usuelles.

Dans la formule précédente, nous pourrions avoir envie de remplacer les occurrences libres de x par un terme quelconque t. Cela se fait en définissant la notion de substitution. Commençons par définir la notion de remplacement, qui ne fonctionne bien que pour les termes t clos :

Définition 1.4 (Remplacement). *Soit u, t des termes bien formés, x une variable. Nous définissons le terme $\langle u/x\rangle t$ par induction sur la structure de t :*
- *Si t est une variable y différente de x, $\langle u/x\rangle y = y$.*
- *Si t est x, alors $\langle u/x\rangle x = u$.*
- *Si t est un symbole de fonction appliqué à ses arguments $f(t_1, ..., t_n)$ (n peut être nul), alors $\langle u/x\rangle f(t_1, ..., t_n) = f(\langle u/x\rangle t_1, ..., \langle u/x\rangle t_n)$.*

Soit P une proposition bien formée, nous définissons de même :
- *Si P est un prédicat d'arité n, alors nous posons $\langle u/x\rangle P(t_1, ..., t_n) = P(\langle u/x\rangle t_1, ..., \langle u/x\rangle t_n)$.*
- *Si P est une formule du type $\underline{Q}yR$, alors $\langle u/x\rangle \underline{Q}yR = \underline{Q}y\langle u/x\rangle R$. Avec $x \neq y$.*
- *Si P est une formule du type $\underline{Q}xR$, alors $\langle u/x\rangle \underline{Q}xR = \underline{Q}xR$.*
- *Si P est une formule du type $Q\underline{c}R$, où $\underline{c}$ est un connecteur propositionnel, alors $\langle u/x\rangle (Q\underline{c}R) = (\langle u/x\rangle Q)\underline{c}(\langle u/x\rangle R)$.*

Nous remarquons que nous ne remplaçons pas les variables liées. Par contre, le problème suivant peut survenir :
$\langle y/x\rangle(\forall y Q(x, y)) = \forall y Q(y, y)$, ce qui n'est pas la même chose que la proposition initiale, car l'occurrence de x qui était libre devient une occurrence liée de y. Ce phénomène s'appelle la capture, et pour s'en débarrasser, il faudrait renommer y en z par exemple, pour d'abord obtenir la proposition (alphabétiquement équivalente) $\forall z Q(x, z)$ puis seulement ensuite remplacer.

Ce problème n'apparaît nulle part dans notre travail, car nous ne substituerons à x que des termes t clos, non sujet à la capture de variable. C'est pourquoi une définition comme la définition 1.4 nous convient tout à fait.

La solution à ce problème est obtenu en définissant une substitution qui évite la capture, comme par exemple dans [12], ce qui est la définition standard d'une substitution :

Définition 1.5 (Substitution). *Soit u, t deux termes bien formés, x une variable, nous définissons le terme substitué $(u/x)t$ de la façon suivante :*
- *si t est x, alors $(u/x)x = u$*
- *si t est une autre variable y, alors $(u/x)y = y$*
- *Si $t = f(t_1, ..., t_n)$, alors $(u/x)f(t_1, ..., t_n) = f((u/x)t_1, ..., (u/x)t_n)$*

Soit P une formule bien formée, nous définissons $(u/x)P$ de manière inductive :
- *Si P est un prédicat d'arité n, alors nous posons $(u/x)A(t_1, ..., t_n) = A((u/x)t_1, ..., (u/x)t_n)$,*

- *Si P est une formule du type $\underline{\mathcal{Q}}yR$, alors $(u/x)\underline{\mathcal{Q}}yR = \underline{\mathcal{Q}}z(u/x)(z/y)R$. Avec $x \neq y$, et z une variable fraîche par rapport à u et R.*
- *Si P est une formule du type $\underline{\mathcal{Q}}xR$ alors, $(u/x)\underline{\mathcal{Q}}xR = \underline{\mathcal{Q}}xR$.*
- *Si P est une formule du type $Q\underline{c}R$, où $\underline{c}$ est un connecteur propositionnel, alors $(u/x)(Q\underline{c}R) = ((u/x)Q)\underline{c}((u/x)R)$*

Définition 1.6 (Substitution parallèle). *Soit t un terme. Soit une substitution parallèle $\{u_1/x_1, ..., u_n/x_n\}$ (en abrégé σ), qui à un nombre fini de variables $x_1, ..., x_n$ associe les termes $u_1, ..., u_n$. Nous définissons le terme substitué σt par induction sur t :*

- *Si t est x_i, alors $\sigma x = u_i$.*
- *Si t est une autre variable y alors $\sigma y = y$.*
- *Si $t = f(t_1, ..., t_n)$, alors $\sigma f(t_1, ..., t_n) = f(\sigma t_1, ..., \sigma t_n)$.*

Soit P une formule bien formée, nous définissons σP par induction sur P :

- *P est un prédicat à n variables $\sigma A(t_1, ..., t_n) = A(\sigma t_1, ..., \sigma t_n)$.*
- *P est une formule du type $\underline{\mathcal{Q}}yR$, $\sigma\underline{\mathcal{Q}}yR = \underline{\mathcal{Q}}z\sigma((z/y)R)$. Avec $x \neq y$, et z une variable n'ayant aucune occurrence ni dans R ni dans u.*
- *P est une formule du type $Q\underline{c}R$, où $\underline{c}$ est un connecteur propositionnel, $\sigma(Q\underline{c}R) = (\sigma Q)\underline{c}(\sigma R)$.*

Nous noterons nos substitutions de la manière suivante :

$$\{t/x\}$$

Nous savons parler des occurrences de variables et de termes dans une formule. Et même d'occurrence de propositions. Cela ne nous suffit pas, car nous voulons être capable de dire que $P(0)$ est une sous-formule de $\forall x P(x)$:

Définition 1.7 (Sous-formule). *Soit P une formule. On dit que Q est une sous-formule de P dans les cas suivants :*

- *$Q = P$*
- *$P = \underline{\mathcal{Q}}xR$, et Q est une sous-formule de $\{t/x\}R$ pour un certain terme t.*
- *$P = R\underline{c}S$, et Q est une sous formule de R ou de S.*

Il nous reste à définir les occurrences positives et négatives dans une formule :

Définition 1.8 (Occurrences positives). *Soit P une formule, et l'occurrence d'un atome A. Nous définissons la positivité et la négativité de cette occurrence de la manière suivante :*

- *si P est l'atome A, alors elle est positive,*
- *si $P = Q \vee R$, alors les occurrences positives de A dans Q et R sont positives dans P,*
- *si $P = Q \wedge R$, alors les occurrences positives de A dans Q et R sont positives dans P,*
- *si $P = \forall xQ$, les occurrences positives de A dans Q ont positives dans P,*
- *si $P = \exists xQ$, les occurrences positives de A dans Q sont positives dans P,*
- *si $P = Q \Rightarrow R$, les occurrences positives de A dans R et négatives de A dans Q sont positives dans P,*
- *si $P = \neg Q$, les occurrences négatives de A dans Q sont positives dans P,*
- *dans tous les cas contraires, les occurrences de A dans P sont négatives.*

1.1.2 Langages à plusieurs sortes

Lors de la définition du langage $\mathcal{L}$ on peut vouloir définir plusieurs sortes (ce sera le cas au chapitre 7 par exemple). Les définitions sont alors modifiées en conséquence. $\mathcal{L}$ contient :

- des sortes $\iota, s, ...$ (nous ne donnons pour l'instant aucune précision sur la formation de ces sortes),
- des symboles de fonction d'arité n, de rang $\langle s_1, ..., s_n, s_{n+1}\rangle$,
- des symboles de prédicat, de rang $\langle s_1, ..., s_n\rangle$ où s_i est une sorte.

Pour chaque sorte s, nous avons un ensemble dénombrable de variables $\mathcal{V}_s$.

La définition d'un terme bien formé s'étend immédiatement :

Définition (Terme bien formé). *Un terme de sorte s est bien formé si :*

- *c'est une variable de sorte s,*
- *c'est un symbole de constante de sorte s,*
- *c'est un symbole de fonction f de rang $\langle s_1, ..., s_n, s_{n+1}\rangle$ appliqué à n arguments, chacun étant respectivement bien formé de sorte s_i.*

Toutes les autres définitions (formule bien formée, remplacement, substitution) s'étendent de la même manière.

Dans le chapitre 7 nous définirons nos sortes de la manière suivante :

- deux sortes élémentaires ι (les termes) et o (les propositions),
- une règle pour former de nouvelles sortes : si ι_1, ι_2 sont des sortes, alors $\iota_1 \to \iota_2$ est une sorte.

Il n'y a que quelques symboles de fonction et un symbole de prédicat :

- α_{s_1,s_2} de rang $\langle s_1 \to s_2, s_1, s_2\rangle$, symbole d'application,
- ε de rang $\langle o\rangle$, symbole d'encapsulement.

Et il y a des symboles de constantes distinguées :

- S, K, les combinateurs,
- $\dot\wedge, \dot\vee, ...$ les connecteurs logiques,
- $\forall_s, \exists_s$ les quantificateurs.

1.2 Systèmes de déduction

Nous venons de donner les règles de formation des propositions. Il faut maintenant répondre à la question "que pouvons nous en faire ?", "comment prouver $P \Rightarrow P$?", ou encore "comment écrire des preuves ?".

Plusieurs formalismes de construction de preuve existent, comme rappelé en introduction. Ils sont équivalent entre eux. On peut citer la déduction naturelle, les systèmes de déduction à la Hilbert, la résolution, les tableaux, et celui que nous allons utiliser principalement dans notre travail, le calcul des séquents, introduit par Gentzen dans [20].

Un séquent est formé de deux multi-ensembles finis de propositions, que nous nommerons Γ et Δ, séparés par le symbole $\vdash$ (à lire "thèse"). La différence entre un ensemble et un multi-ensemble est que dans un multi-ensemble on peut avoir

plusieurs occurrences d'un même élément.
La sémantique informelle de cette notation est la suivante. $\Gamma \vdash \Delta$ veut dire "à partir des hypothèses Γ, je peux prouver la disjonction des (*une des*) propositions de Δ". Dans la formulation intuitionniste du calcul des séquents Δ contient au plus une proposition.

Mais séquent n'est pas synonyme de preuve. Nous pouvons écrire par exemple $\neg A \vdash A$. C'est un séquent bien formé. Par contre, il n'a pas de preuve. Les preuves valides de séquents sont engendrées par les règles définies dans les deux sections 1.2.1 et 1.2.2. C'est à ces ensemble de règles que l'on fait référence sous le vocable "calcul des séquents intuitionniste" (respectivement "calcul des séquents classique").

La terminologie est la suivante, et la même pour toutes les règles :

$$\frac{\Gamma, A \vdash B}{\Gamma \vdash A \Rightarrow B} \Rightarrow\text{-d}$$

Le séquent $\Gamma \vdash A \Rightarrow B$ est la conclusion de la règle $\Rightarrow$-g, et $\Gamma, A \vdash B, \Delta$ en est sa prémisse principale. La proposition $A \Rightarrow B$ sur laquelle s'applique effectivement la règle s'appelle la proposition active. Le sens de cette règle est que si on veut démontrer $A \Rightarrow B$ à partir des hypothèses Γ, alors il est suffisant de démontrer B à partir des hypothèses Γ, A.

Il y a deux sortes de règles : les règles gauches notées avec le suffixe "-g", qui s'appliquent aux hypothèses Γ, et les règles droites, notées avec un suffixe "-d" qui s'appliquent aux propositions de Δ.

Notons que nous n'avons pas de règle d'échange entre propositions, puisque nous considérons un séquent comme une paire d'ensembles non ordonnés, et non des listes. Cela diffère de la présentation habituelle du calcul des séquents, que l'on peut par exemple trouver dans [46].

1.2.1 Le calcul des séquents intuitionniste

Les règles d'inférence du calcul des séquents intuitionniste sont présentées figure 1.1.

Ces calculs sont équivalents à la déduction naturelle et au calcul des prédicats de Hilbert (voir par exemple les notes de cours de Dowek [14]).

Un séquent $\Gamma \vdash P$ a une preuve si et seulement si on peut construire un arbre à partir des règles de la figure 1.1 dont chacune des feuilles est soit une règle axiome, soit une règle $\bot$-g.

Un preuve d'un séquent (une assertion) $\Gamma \vdash P$ est une dérivation de ce séquent grâce aux règles d'inférences de la figure 1.2. Lors de l'application d'une règle, par exemple $\vee$-gauche :

$$\frac{\Gamma, A \vdash P \quad \Gamma, B \vdash P}{\Gamma, A \vee B \vdash P} \vee\text{-gauche}$$

nous avons démontré l séquent $\Gamma, A \vee B \vdash P$ si et seulement si nous savons démontrer les séquents $\Gamma, A \vdash P$ et $\Gamma, A \vdash P$. C'est à dire, informellement, j'ai prouvé P sous les hypothèses $A \vee B$ si je peux prouver P sous les hypothèses A et B indépendamment.

Les seules règles qui permettent de "fermer" une preuve (c'est à dire obtenir une branche sans prémisse) sont les règles axiome et $\bot$-g. Une preuve bien formée est une preuve qui est fermée. Voici des exemples de preuve :

$$\frac{}{A \vdash A} \qquad \frac{\dfrac{}{A \vdash A}}{\vdash A \Rightarrow A} \Rightarrow\text{-d}$$

Un point de vocabulaire doit être ici précisé :

Définition 1.9. *Soit $\mathcal{T}$ une théorie infinie. Nous écrirons :*

$$\mathcal{T} \vdash_{\mathcal{R}} P$$

si et seulement si un sous-ensemble fini $\Gamma \subset \mathcal{T}$ *est tel que le séquent* $\Gamma \vdash_{\mathcal{R}} P$ *a une preuve.*

En effet, dans une preuve valide du calcul des séquents, seul un nombre fini de propositions interviennent, les autres ne servant à rien. Comme un nombre infini de propositions dans un séquent pose problème (en particulier lors du choix d'une constante fraîche), nous nous restreignons à des séquents finis.

1.2.2 Calcul des séquents classique

Dans le calcul des séquents intuitionniste, il n'est pas possible d'avoir une démonstration du tiers-exclu (*tertium non datur*), dont une formulation est la suivante. Pour toute proposition A, on a :

$$A \vee (\neg A)$$

Si on essaie de prouver $\vdash A \vee \neg A$ en calcul des séquents intuitionniste sans utiliser la règle de coupure, alors on s'aperçoit que la seule règle qui puisse s'appliquer est $\vee$-d. Mais, que l'on essaie de prouver $\vdash A$ ou $\vdash \neg A$, la tentative échoue.

L'autorisation de la règle de coupure ne change rien, car elle est redondante, comme nous le verrons plus tard.

Des arguments sémantiques (il existe des contre-modèles de $A \vee \neg A$) que nous ne pouvons encore invoquer donnent une idée plus claire sur la question.

Pour pallier à ce manque, quand on veut autoriser l'axiome du tiers-exclu, on pourrait rajouter une règle d'inférence :

$$\frac{}{\vdash A \vee \neg A}\ \text{tiers-exclu}$$

$$\frac{}{\Gamma, P \vdash P}\ \text{axiome}$$

$$\frac{\Gamma, P \vdash Q \quad \Gamma \vdash P}{\Gamma \vdash Q}\ \text{coupure}$$

$$\frac{\Gamma, P, P \vdash Q}{\Gamma, P \vdash Q}\ \text{contr-g}$$

$$\frac{}{\Gamma, \bot \vdash Q}\ \bot\text{-g}$$

$$\frac{\Gamma \vdash Q}{\Gamma, P \vdash Q}\ \text{affaiblissement-g}$$

$$\frac{\Gamma \vdash}{\Gamma \vdash P}\ \text{affaiblissement-d}$$

$$\frac{\Gamma, P, Q \vdash R}{\Gamma, P \wedge Q \vdash R}\ \wedge\text{-g}$$

$$\frac{\Gamma \vdash P \quad \Gamma \vdash Q}{\Gamma \vdash P \wedge Q}\ \wedge\text{-d}$$

$$\frac{\Gamma, P \vdash R \quad \Gamma, Q \vdash R}{\Gamma, P \vee Q \vdash R}\ \vee\text{-g}$$

$$\frac{\Gamma \vdash P}{\Gamma \vdash P \vee Q}\ \vee\text{-d} \qquad \frac{\Gamma \vdash Q}{\Gamma \vdash P \vee Q}\ \vee\text{-d}$$

$$\frac{\Gamma \vdash P \quad \Gamma, Q \vdash R}{\Gamma, P \Rightarrow Q \vdash R}\ \Rightarrow\text{-g}$$

$$\frac{\Gamma, P \vdash Q}{\Gamma \vdash P \Rightarrow Q}\ \Rightarrow\text{-d}$$

$$\frac{\Gamma \vdash P}{\Gamma, \neg P \vdash Q}\ \neg\text{-g}$$

$$\frac{\Gamma, P \vdash}{\Gamma \vdash \neg P}\ \neg\text{-d}$$

$$\frac{\Gamma, \{t/x\}P \vdash Q}{\Gamma, \forall x P \vdash Q}\ \forall\text{-g}, t \text{ clos}$$

$$\frac{\Gamma \vdash \{c/x\}P}{\Gamma \vdash \forall x P}\ \forall\text{-d}, c \text{ constante fraîche, i.e. qui n'apparaît pas dans } \Gamma \vdash \forall x P$$

$$\frac{\Gamma, \{c/x\}P \vdash Q}{\Gamma, \exists x P \vdash Q}\ \exists\text{-g}, c \text{ constante fraîche, qui n'apparaît pas dans } \Gamma \vdash \exists x P$$

$$\frac{\Gamma \vdash \{t/x\}P}{\Gamma \vdash \exists x P}\ \exists\text{-d}, t \text{ clos}$$

FIG. 1.1 – Règles d'inférence du calcul des séquents intuitionniste

ou bien celle-ci, équivalente :

$$\frac{\Gamma \vdash \neg\neg A}{\Gamma \vdash A}$$

Le problème de cette règle est que quand nous voulons nous en servir, nous sommes obligés d'introduire (via la règle de coupure) une proposition plus grosse que la proposition de départ. Ainsi, on a la démonstration suivante (qui se lit mieux de bas en haut) :

$$\dfrac{\dfrac{}{\neg\neg P \vdash P \vee \neg P} \qquad \dfrac{\dfrac{}{\neg\neg P, P \vdash P} \qquad \dfrac{\dfrac{}{\neg P \vdash \neg P}}{\neg\neg P, \neg P \vdash P}\,\neg\text{-g}}{\neg\neg P, P \vee \neg P \vdash P}}{\neg\neg P \vdash P}\,\text{coupure}$$

Dans cette démonstration, le point important est la manière dont nous avons utilisé la règle ¬-g. On ne peut pas l'appliquer telle-quelle sur le séquent $\neg\neg P \vdash P$ car nous écraserions la proposition P, par $\neg P$.

Au lieu de cela, nous nous sommes servis de la règle du tiers-exclu par le biais de la règle de coupure (on ne peut l'éviter dans ce cas-là) et nous avons mis en réserve $\neg P$ dans les hypothèses (c'est à dire le dual de P par le tiers-exclu), puis nous avons appliqué la règle ¬-g.

En quelque sorte, nous avons mis P en réserve à gauche du séquent. Cela revient au même d'autoriser plusieurs conclusions à la droite du séquent, mais en n'autorisant plus la nouvelle règle tiers-exclu (qui serait de toutes façons redondante).

Les règles du calcul des séquents modulo classique sont présentées figure 1.2. Dans cette figure, comme dans la suite de cette thèse, Γ et Δ dénotent des ensembles finis de propositions.

Il est maintenant facile d'avoir une démonstration des séquents :

$$\neg\neg P \vdash P \qquad \vdash A \vee \neg A$$

L'avantage de ce système de déduction par rapport au calcul des séquents intuitionniste avec règle du tiers-exclu est multiple : nous n'avons pas besoin de règle supplémentaire, nous n'introduisons plus de proposition par la règle de coupure, et nous n'augmentons pas la taille des propositions introduites.

1.2.3 Présentation alternative

Très souvent, par exemple dans [46, 14], le calcul des séquents est présenté avec des termes non clos. Les règles modifiées en sont ∀-d et ∃-g (x doit être non libre dans Γ, Δ) :

$$\frac{\Gamma \vdash P, \Delta}{\Gamma \vdash \forall x P, \Delta}\forall\text{-d} \qquad \frac{\Gamma, P \vdash \Delta}{\Gamma, \exists x P \vdash \Delta}\exists\text{-g}$$

$$\frac{}{P \vdash P}\text{axiome}$$

$$\frac{\Gamma, P \vdash \Delta \quad \Gamma \vdash P, \Delta}{\Gamma \vdash \Delta}\text{coupure}$$

$$\frac{\Gamma, P, P \vdash \Delta}{\Gamma, P \vdash \Delta}\text{contr-g}$$

$$\frac{\Gamma \vdash P, P, \Delta}{\Gamma \vdash P, \Delta}\text{contr-d}$$

$$\frac{\Gamma \vdash \Delta}{\Gamma, P \vdash \Delta}\text{affaiblissement-g}$$

$$\frac{\Gamma \vdash \Delta}{\Gamma \vdash P, \Delta}\text{affaiblissement-d}$$

$$\frac{\Gamma, P, Q \vdash \Delta}{\Gamma, P \wedge Q \vdash \Delta} \wedge\text{-g}$$

$$\frac{\Gamma \vdash P, \Delta \quad \Gamma \vdash Q, \Delta}{\Gamma \vdash P \wedge Q, \Delta} \wedge\text{-d}$$

$$\frac{\Gamma, P \vdash \Delta \quad \Gamma, Q \vdash \Delta}{\Gamma, P \vee Q \vdash \Delta} \vee\text{-g}$$

$$\frac{\Gamma \vdash P, Q, \Delta}{\Gamma \vdash P \vee Q, \Delta} \vee\text{-d}$$

$$\frac{\Gamma \vdash P, \Delta \quad \Gamma, Q \vdash \Delta}{\Gamma, P \Rightarrow Q \vdash \Delta} \Rightarrow\text{-g}$$

$$\frac{\Gamma, P \vdash Q, \Delta}{\Gamma \vdash P \Rightarrow Q, \Delta} \Rightarrow\text{-d}$$

$$\frac{\Gamma \vdash P, \Delta}{\Gamma, \neg P \vdash \Delta}\neg\text{-g}$$

$$\frac{\Gamma, P \vdash \Delta}{\Gamma \vdash \neg P, \Delta}\neg\text{-d}$$

$$\frac{}{\Gamma, \bot \vdash \Delta}\bot\text{-g}$$

$$\frac{\Gamma, \{t/x\}P \vdash \Delta}{\Gamma, \forall x P \vdash \Delta}\forall\text{-g, } t \text{ clos}$$

$$\frac{\Gamma \vdash \{c/x\}P, \Delta}{\Gamma \vdash \forall x P, \Delta}\forall\text{-d, } c \text{ constante fraîche}$$

$$\frac{\Gamma, \{c/x\}P \vdash \Delta}{\Gamma, \exists x P \vdash \Delta}\exists\text{-g, } c \text{ constante fraîche}$$

$$\frac{\Gamma \vdash \{t/x\}P, \Delta}{\Gamma \vdash \exists x P, \Delta}\exists\text{-d, } t \text{ clos}$$

FIG. 1.2 – règles d'inférence du calcul des séquents classique

Cette présentation a certains avantages (dans la preuve du théorème de correction 5.1 du chapitre suivant, en particulier), mais a aussi un inconvénient majeur : comment prouve-t-on le séquent $\exists x P(x), \exists x Q(x) \vdash \exists x \exists y (P(x) \wedge Q(y))$ par exemple ?

Le lecteur intéressé peut vérifier qu'une telle preuve est très facile dans le calcul des séquents de la figure 1.2.

Or ici, ce séquent tel quel n'a pas de preuve. Il faut en fait renommer la variable x en z dans la proposition $\exists x Q(x)$. Cela revient à *identifier* les propositions suivantes :

$$\exists x Q(x) \quad \equiv \quad \exists z Q(z)$$

On peut maintenant vérifier que le séquent $\exists x P(x), \exists z Q(z) \vdash \exists x \exists y (P(x) \wedge Q(y))$ a une preuve dans le système précédent.

C'est la deuxième fois que nous rencontrons le problème de l'α-conversion depuis la section 1.1.

Soulignons que le calcul des séquents présenté figure 1.2 a l'avantage de résoudre ce problème d'α-conversion de la manière la plus simple : il n'existe pas. C'est pour cette raison entre autres que nous pouvons nous contenter de la définition 1.4 pour nos substitutions, car nous substituerons toujours des termes clos.

1.2.4 Restrictions sur les règles d'inférence

À des fins syntaxiques, nous pouvons restreindre le champs d'application de certaines règles du calcul des séquents. Nous ne parlerons que des règles du calcul des séquents classique de la figure 1.2, car nous n'aurons besoin de ces restrictions que dans ce cas. Mais elles sont tout aussi valides dans le cas du calcul des séquents intuitionniste.

– Tout d'abord, dans le calcul des séquents de la figure 1.2, nous pouvons nous restreindre à des règles axiome portant uniquement sur des propositions atomiques :

$$\frac{}{\Gamma, A \vdash A, \Delta} \quad \text{axiome si } A \text{ atomique}$$

Le calcul ainsi obtenu reste équivalent. En effet, les preuves du nouveau calcul sont déjà des preuves du calcul des séquents classique, et inversement, étant donné une preuve du calcul des séquents classiques, il suffit de remplacer chaque règle axiome :

$$\frac{}{\Gamma, P \vdash P, \Delta} \quad \text{axiome}$$

par le morceau de démonstration :

$$\frac{\vdots}{\Gamma, P \vdash P, \Delta}$$

qui se définit par induction sur le nombre de connecteurs de P. Par exemple, si $P = \forall x Q$, alors voici le morceau de preuve à rajouter :

$$\dfrac{\dfrac{\dfrac{\pi}{\Gamma, Q(c) \vdash Q(c), \Delta}}{\Gamma, \forall x Q(x) \vdash Q(c), \Delta}}{\Gamma, \forall x Q(x) \vdash \forall x Q(x), \Delta}$$

avec π obtenue par induction (puisque $Q(c)$ a un connecteur de moins que P).

- De même, on peut remplacer les règles d'affaiblissement par des règles d'affaiblissement atomiques. Nous ne développons pas la preuve d'équivalence, elle est similaire à celle présentée ci-dessus.
- Enfin, nous pouvons aussi restreindre la règle $\bot$-gauche en ne l'autorisant à s'appliquer qu'à un contexte vide. Pour obtenir de nouveau une preuve de $\Gamma, \bot \vdash \Delta$, nous pouvons nous servir des règles d'affaiblissement :

$$\dfrac{\dfrac{}{\bot \vdash}\bot - \mathrm{g}}{\dfrac{\vdots}{\Gamma, \bot \vdash \Delta}}\ \text{affaiblissements}$$

- Enfin, nous pouvons, mais ceci est plus difficile à démontrer, restreindre les règles de contraction aux propositions dont le connecteur principal est $\forall$ pour les propositions à gauche du séquent ou $\exists$ à droite. Ceci est dû au lemme de Kleene 3.3. Informellement, nous pouvons "pousser" plus haut dans la démonstration n'importe quelle règle de contraction, sauf celles sur les propositions quantifiées existentiellement à droite et universellement à gauche. La raison étant que le lemme de Kleene n'est pas valide pour ces deux cas.
  La preuve formelle est laissée au lecteur intéressé, car nous ne nous servirons pas de ce fait dans la suite.

Ces restrictions ont en général pour but de définir un calcul des séquents dans lequel les récurrences sur la hauteur des preuves se font facilement (parfois, il est même impossible de les effectuer dans le calcul des séquents de la figure 1.2), nous les utiliserons au chapitre 9.

La règle de coupure

Nous continuons ici la discussion de l'introduction, que nous pouvons affiner puisque nous savons maintenant à quoi ressemble le calcul des séquents.

La règle de coupure est la seule qui introduise une proposition P qui n'a aucun rapport ni avec Γ, ni avec Δ. Du point de vue de la recherche automatique de preuve, c'est une très mauvaise règle. Comme nous cherchons toujours à construire une preuve du bas vers le haut (de la conclusion vers les prémisses), nous n'avons aucune information sur la proposition P que nous devons introduire. Dans le cadre d'une recherche exhaustive de preuve, nous devrions donc

toutes les énumérer, ce qui n'est pas efficace du tout.

Si la règle de coupure est interdite (car redondante), nous sommes absolument sûrs que les prémisses du séquent $\Gamma \vdash \Delta$ seront composées uniquement de sous-formules de Γ, Δ (le lecteur intéressé peut le vérifier dans la figure 2.4). Ainsi, tous les éléments nécessaires à la preuve se trouvent déjà dans le séquent à démontrer.

De plus, une fois que nous avons démontré la redondance de la règle de coupure, nous savons que le calcul des séquents est cohérent, c'est à dire qu'on ne peut pas démontrer n'importe quel séquent (comme par exemple $\vdash$).

Gentzen a prouvé ce résultat dans [20]. Il y définit une méthode pour transformer une démonstration avec coupures en démonstration sans coupure, et prouve la terminaison de celle-ci.

Intuitivement, en effet, à quoi cela sert-il de d'introduire P dans les hypothèses à gauche du séquent, si nous devons de toutes façons le prouver à droite du séquent plus tard ?

Si donc on peut se passer de la règle de coupure, le résultat est cependant difficile à obtenir. De plus, la taille des démonstrations sans coupure peut devenir beaucoup plus grande que celle des démonstrations du même séquent sans la règle de coupure.

1.3 Sémantique

1.3.1 Sémantiques de la logique

Informellement, un modèle est la donnée d'un ensemble d'interprétation dans lequel nous donnons l'interprétation des symboles (de constante, de fonction) et des prédicats. L'interprétation des propositions et des termes composés est ensuite définie par induction sur la structure des termes, car elle doit obéir à certaines règles.

L'ensemble des règles définissant l'ensemble d'interprétation, l'interprétation des symboles et celle des termes et propositions composés permet de définir une classe des modèles : *la sémantique.*

Par exemple, on peut décider de déclarer $A \wedge B$ vraie dans $\mathcal{M}$ si et seulement si A et B sont vraies dans $\mathcal{M}$. De même, on peut déclarer $\forall x P$ vraie dans $\mathcal{M}$ si pour tout élément a de l'ensemble d'interprétation des termes, P est vraie dans $\mathcal{M}$ quand x est interprétée par a.

Une proposition P est alors déclarée vraie si et seulement si elle est vraie dans tous les modèles de la classe considérée.

Les modèles sont souvent utilisés pour démontrer un résultat négatif : une proposition P n'est pas vraie sous les hypothèses $\mathcal{T}$ s'il existe au moins *un* modèle de $\mathcal{T}$ dans lequel elle est fausse. Grâce au théorème de correction (toutes

les règles de déduction sont valides dans le modèle), nous savons qu'il ne peut pas exister de démonstration de P. C'est l'essence de la construction de contre-modèles.

Par exemple, dans les modèles booléens, la proposition suivante n'est pas vraie (et donc, non démontrable en calcul des séquents classique) :

$$A \vee (B \wedge \neg A)$$

Le modèle où A est interprété par vrai valide cette proposition (i.e. A est vraie dans ce modèle). Cependant, le modèle où A est fausse et B fausse aussi rend la proposition ci-dessus fausse.

Dans les deux sections suivantes, nous allons formaliser ces notions et donner deux sémantiques : une pour la logique classique et une pour la logique intuitionniste.

1.3.2 Modèles booléens

La sémantique s'appuie sur les algèbres de Boole, et plus précisément sur la forme la plus simple des algèbres de Boole : $\{0, 1\}$, où les propositions sont interprétées par deux valeurs de vérité complémentaires : Vrai (1) et Faux (0).

Définition 1.10. *Soit $\mathcal{L}$ un langage. Une structure $\mathcal{M}$ est un ensemble formé d'un domaine M non vide, et pour chaque symbole de prédicat P d'arité n et de fonction f d'arité m du langage $\mathcal{L}$:*

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

Cette structure ne nous permet pas pour l'instant d'interpréter les propositions même atomiques, ni tous les termes de notre langage $\mathcal{L}$. Nous avons défini la seule interprétation des symboles de prédicat et des symboles de fonction (donc, les termes non composés). Il faut donc maintenant étendre cette interprétation. Pour ce faire, nous définissions l'interprétation d'un terme (non clos en règle générale), suivant un assignement σ qui à chaque variable associe un terme clos.

Définition 1.11. *Soit $\mathcal{L}$ un langage, $\mathcal{V}$ l'ensemble de ses variables, $\mathcal{M}$ une structure, et σ un assignement. Nous définissons l'interprétation d'un terme selon σ par induction sur la structure du terme :*

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

Ensuite, nous définissions la valuation (ou l'interprétation) d'une proposition selon l'assignement σ par induction sur la structure de la proposition :

- $|P(t_1, ..., t_n)|_\sigma = \widehat{P}(|t_1|_\sigma, ..., |t_n|_\sigma)$
- $|\neg P|_\sigma = 1$ *ssi* $|P|_\sigma = 0$. *Sinon* $|\neg P|_\sigma = 0$
- $|P \vee Q|_\sigma = 1$ *ssi* $|P|_\sigma = 1$ *ou* $|Q|_\sigma = 1$. *Sinon* $|P \vee Q|_\sigma = 0$
- $|P \wedge Q|_\sigma = 1$ *ssi* $|P|_\sigma = 1$ *et* $|Q|_\sigma = 1$. *Sinon* $|P \wedge Q|_\sigma = 0$
- $|P \vee Q|_\sigma = 1$ *ssi* $|P|_\sigma = 0$ *ou* $|Q|_\sigma = 1$. *Sinon* $|P \vee Q|_\sigma = 0$

– $|\exists x P|_\sigma = 1$ *s'il existe* $a \in M$ *tel que* $|P|_{\sigma:\langle x,a\rangle} = 1$. *Sinon* $|\exists x P|_\sigma = 0$
– $|\forall x P|_\sigma = 1$ *si pour tout* $a \in M$, $|P|_{\sigma:\langle x,a\rangle} = 1$. *Sinon* $|\forall x P|_\sigma = 0$

Nous dirons que la structure $\mathcal{M}$ est un modèle d'une théorie Γ si toutes les propositions de Γ sont interprétées par 1 dans $\mathcal{M}$, selon tous les assignements possibles σ. Nous utiliserons pour cela la notation $\mathcal{M} \vDash \Gamma$. Nous dirons que $\mathcal{M}$ est un modèle lorsque nous parlerons de la structure $\mathcal{M}$ équipée de l'interprétation précédente.

Enfin, nous noterons $\Gamma \vDash \Delta$ lorsque les modèles de Γ sont aussi des modèles de $\bigvee \Delta$. Cela correspondra (grâce au théorème de complétude) à la prouvabilité du séquent correspondant.

Un résultat intéressant est que si une proposition P est close, alors son interprétation dans $\mathcal{M}$ ne dépend pas de l'assignement choisi, et donc, nous pouvons nous permettre d'oublier l'annotation d'assignement et nous écrirons indifféremment $|P|$ ou $|P|_\sigma$.

La plupart du temps, nous interpréterons les termes clos du langage par eux-même. Plus précisément, M est l'ensemble des termes clos du langage, et la fonction $\widehat{f}$ se retrouve être la fonction suivante :

$$\begin{array}{rcl} \widehat{f} : M^m & \mapsto & M \\ t_1, ..., t_m & \to & f(t_1, ..., t_m) \end{array}$$

Une telle structure est appelée modèle syntaxique (et se généralise aussi aux modèles non booléens). Lorsque nous aurons affaire à des modèles syntaxiques, alors l'égalité suivante peut être démontrée (par induction sur la structure de P) :

$$|P|_\sigma = |\{\sigma(x_1)/x_1, ...\sigma(x_n)/x_n\}P|$$

Ainsi, nous pouvons totalement oublier la notion d'assignement dans le cas de modèles syntaxiques, et substituer directement par des termes clos.

Toutes ces définitions s'étendent aux langages qui possèdent plusieurs sortes, en considérant un ensemble d'interprétation M_ι pour chaque sorte ι, et en interprétant de façon adéquate les constantes de fonction et les prédicats. Par exemple, si P est un prédicat de rang $\langle \iota \to \iota \rangle$, alors nous devons avoir :

$$\widehat{P} \quad : \mathcal{M}_{\iota \to \iota} \quad \to \{0, 1\}$$

1.3.3 Structures de Kripke

Si en logique classique nous avons une seule notion de modèle, dans la logique intuitionniste, nous en avons plusieurs, dont les deux principales sont :
– les algèbres de Heyting,

– les structures des Kripke.

Dans notre travail, nous utiliserons les structures de Kripke, c'est pourquoi nous les présentons en détail ici. Pour une présentation des Algèbres de Heyting, voir par exemple [38].

La différence entre une structure de Kripke et un modèle booléen est qu'une structure de Kripke est composée de plusieurs mondes, dans lesquels une proposition est soit vraie, soit fausse. Ainsi, un modèle booléen peut être identifié à une structure de Kripke possédant un unique monde.

Les mondes sont ordonnés par une relation d'ordre partiel, de telle manière que si une proposition est vraie dans un certain monde, elle le restera pour tous les monde "successeurs" ou "futurs". Par contre, si elle y est fausse, il se peut très bien qu'elle devienne vraie dans un certain monde futur.

En voici la définition formelle :

Définition 1.12 (Structure de Kripke). *Une structure de Kripke $\mathcal{K}$ est un quadruplet $\langle K, \leq, D, \Vdash \rangle$ tel que :*

- *K un ensemble non vide, l'ensemble des mondes*
- *$\leq$ est une relation d'ordre partiel sur K*
- *D est une fonction monotone, appelée domaine :*

$$\begin{array}{rcl} \alpha & \longmapsto & D_\alpha \\ \alpha \leq \beta & \Rightarrow & D_\alpha \subseteq D_\beta \end{array}$$

  telle que D_α soit un ensemble non vide.
- *Pour chaque monde α, nous avons un langage $\mathcal{L}_\alpha$ des propositions et des termes interprétables dans ce monde, qui est monotone (de la même manière que le domaine). Et pour chaque symbole de prédicat P d'arité n et de fonction f d'arité m du langage $\mathcal{L}$:*
  - *un symbole $\hat{P} : K \mapsto D_\alpha^n \mapsto \{0,1\}$, monotone en sa première variable. Si $\alpha \leq \beta$, alors pour tous $a_1, ..., a_n \in D_\alpha$ nous avons :*

$$\hat{P}(\alpha)(a_1, ..., a_n) = 1 \quad \textit{implique} \quad \hat{P}(\beta)(a_1, ..., a_n) = 1$$

  - *une fonction $\hat{f} : K \mapsto D_\alpha^m \mapsto D_\alpha$, telle que si on a $\alpha \leq \beta$, alors on a $\hat{f}(\alpha)(a_1, ..., a_n) = \hat{f}(\beta)(a_1, ..., a_n)$ (f dans le monde β est une extension de f dans α).*
- *Pour tout monde α, l'interprétation $|t|_\sigma^\alpha$ d'un terme t dans D_α, selon une substitution σ est définie par induction :*
  - *$|x|_\sigma^\alpha = \sigma(x)$,*
  - *$|f(t_1, ..., t_n)|_\sigma^\alpha = \hat{f}(\alpha)(|t_1|_\sigma^\alpha, ..., |t_n|_\sigma^\alpha)$.*
- *$\Vdash$ est une relation entre les mondes α et les propositions définies sur ce monde, modulo une substitution σ associant à chaque variable un terme $a \in D_\alpha$ vérifiant les conditions suivantes :*
  1. *Si $A(x_1, ..., x_n)$ est un symboles de prédicat n-aire, alors, pour n'importe quels mondes $\beta \geq \alpha$ et pour n'importe quels éléments $t_1, ..., t_n \in$*

$\mathcal{L} \cup \mathcal{V}$:
$\alpha \Vdash_\sigma A(t_1, ..., t_n)$ *ssi* $\hat{A}(\alpha)(|t_1|^\alpha_\sigma, ..., |t_n|^\alpha_\sigma) = 1$.

2. $\alpha \Vdash_\sigma A \vee B$ *ssi* $\alpha \Vdash_\sigma A$ *ou* $\alpha \Vdash_\sigma B$.
3. $\alpha \Vdash_\sigma A \wedge B$ *ssi* $\alpha \Vdash_\sigma A$ *et* $\alpha \Vdash_\sigma B$.
4. $\alpha \Vdash_\sigma A \Rightarrow B$ *ssi pour tout* $\beta \geq \alpha$, $\beta \Vdash_\sigma A$ *implique* $\beta \Vdash_\sigma B$.
5. $\alpha \Vdash_\sigma \neg A$ *ssi pour tout* $\beta \geq \alpha$, $\beta \nVdash_\sigma A$.
6. $\alpha \Vdash_\sigma \exists x A$ *ssi il existe un élément* $a \in D(\alpha)$ *tel que* $\alpha \Vdash_{\sigma+\langle a/x\rangle} A$.
7. $\alpha \Vdash_\sigma \forall x A$ *ssi pour tout* $\beta \geq \alpha$, *pour tout élément* $a \in D(\beta)$, $\beta \Vdash_{\sigma+\langle a/x\rangle} A$.

Avec cette définition, nous avons le lemme de substitution :

Lemme 1.1 (Substitution). *Pour tout monde* α *d'une structure de Kripke* $\mathcal{K}$:

$$\begin{array}{rcl} |\{t'/x\}t|^\alpha_\sigma & = & |t|^\alpha_{\sigma+\langle|t'|/x\rangle} \\ \alpha \Vdash_\sigma \{t'/x\}P & ssi & \alpha \Vdash_{\sigma+\langle|t'|_\sigma/x\rangle} P \end{array}$$

Si P *est une formule close, alors* $\alpha \Vdash_\sigma P$ *ne dépend pas de* σ.

Preuve. Par induction sur la structure des termes. ■

Remarque. Nous considérerons la plupart du temps des structures de Kripke syntaxiques, c'est à dire dans lesquelles le domaine est l'ensemble des termes clos. Dans ce cas-là, grâce au lemme précédent, nous pourrons nous passer de la définition avec des substitutions, et substituer directement à l'intérieur des propositions, en assimilant $\hat{P}$ à P.

Nous pourrons aussi supposer la relation d'ordre $\leq$ sur K bien fondée. D'abord car nous ne nous intéresserons toujours qu'aux mondes $\beta \geq \alpha$ pour un certain α, en ensuite parce que les structures de Kripke que nous construirons seront toujours équipées d'un ordre bien fondé.

Remarque. Cette définition 1.12 des structures de Kripke se restreint à la définition des modèles classiques, si nous prenons pour ensemble K de mondes un singleton.

La condition de monotonicité de $\hat{P}$ se traduit par la monotonicité de la relation de forcing pour toutes les propositions (même non atomiques). Si un monde β est situé après un monde α, alors il force toutes les propositions forcées par α (et, bien sûr, éventuellement d'autres propositions) :

Lemme 1.2. *Soit* $\mathcal{K}$ *une structure de Kripke, et soient* $\alpha \leq \beta$ *deux mondes de* K. *Soit* P *une proposition. Alors :*

$$\alpha \Vdash P \quad \Rightarrow \quad \beta \Vdash P$$

Preuve. Par induction sur la structure de la proposition P. Voyons les cas les plus significatifs :

– Si P est un atome, alors par définition $\alpha \Vdash_\sigma P(t_1, ..., t_n)$ est équivalent à $\hat{P}(\alpha)(|t_1|^\alpha_\sigma, ..., |t_n|^\alpha_\sigma) = 1$. Or,$|t_1|^\alpha_\sigma = |t_1|^\beta_\sigma$, d'après la définition des éléments de D_α (σ associe à toutes les variables des éléments de D_α).
Par monotonie de $\hat{P}$ nous avons donc : $\hat{P}(\beta)(|t_1|^\alpha_\sigma, ..., |t_n|^\alpha_\sigma) = 1$ puis, par l'argument précédent $\hat{P}(\beta)(|t_1|^\beta_\sigma, ..., |t_n|^\beta_\sigma) = 1$ ce qui est équivalent à $\beta \Vdash_\sigma P(t_1, ..., t_n)$.
Nous avons donc $\alpha \Vdash_\sigma P(t_1, ..., t_n)$ implique $\beta \Vdash_\sigma P(t_1, ..., t_n)$. La relation de forcing est monotone pour les atomes.
Remarque. Dans les présentations usuelles des structures de Kripke (par exemple dans [45]), c'est un des axiomes de la relation de forcing. Nous avons fait un autre choix, car les présentations habituelles ne sont pas assez formelles.

– Si $P = A \Rightarrow B$. Alors, soit $\gamma \geq \beta$, tel que $\gamma \Vdash A$. Par transitivité de $\geq$, nous savons que $\gamma \geq \alpha$. Ainsi, nous devons avoir $\gamma \Vdash B$, puisque $\alpha \Vdash P$. Donc $\beta \Vdash A \Rightarrow B$. Notons qu'ici, nous n'avons pas utilisé l'hypothèse d'induction.
– Si $P = A \vee B$. Alors, par définition $\alpha \Vdash A$ ou bien $A \Vdash B$. Par hypothèse d'induction, $\beta \Vdash A$ (dans le premier cas), et $\beta \Vdash B$ (dans le second cas). Donc $\beta \Vdash A \vee B$.
– Tous les autres cas se démontrent de la même manière que les deux précédents.

■

Définition 1.13 (Modèle de Kripke). *Soit Γ une théorie et P une proposition, soit $\mathcal{K}$ une structure de Kripke. Un monde α est un modèle de Γ si et seulement si pour toute proposition $P \in \Gamma$, $\alpha \Vdash P$. Par abus de notation, nous notons $\alpha \Vdash \Gamma$ et nous dirons que α* valide *Γ. Par abus de langage, si $\alpha \Vdash \Gamma$ pour tout $\alpha \in K$, nous dirons que la structure de Kripke $\mathcal{K}$ est un modèle de Γ.*

Si dans toute structure $\mathcal{K}$, tout monde qui est modèle de Γ est aussi un modèle de P, nous noterons $\Gamma \vDash P$.

Remarque. Notons qu'étant donné une structure de Kripke $\mathcal{K}$ et un monde $\alpha \in K$, nous pouvons restreindre $\mathcal{K}$ en $\mathcal{K}_\alpha$ de telle sorte que α soit le plus petit noeud de cette nouvelle structure de Kripke. Il suffit de prendre $K_\alpha = \{\beta \geq \alpha\}$, toutes les autres définition restant inchangées.

1.3.4 Le théorème de complétude de Gödel

Dans aucune de ces sémantiques, il n'y a, a priori, de notion de preuve. Or, nous aimerions bien savoir que si P est vraie dans telle sémantique, alors il existe une démonstration de P dans tel ou tel système de déduction. Inversement, si on a une preuve de P, on voudrait pouvoir conclure que P est vraie dans telle sémantique.

En d'autres mots, puisque nous avons deux moyens de définir la vérité d'une proposition (l'existence d'une preuve de P et l'interprétation de P), nous avons

besoin d'un théorème de correspondance entre les deux.

La première partie du travail est de prouver le théorème de correction : Si on a une preuve de $\Gamma \vdash \Delta$, alors tous les modèles de Γ sont des modèles de Δ (pour une certaine sémantique).

Prouver la réciproque, est beaucoup plus difficile.

Cette tâche à été achevée par Gödel dans le cadre de la logique des prédicats classique, lorsqu'il a prouvé le théorème de complétude [23] (voir par exemple [8] – à ne pas confondre avec le théorème d'incomplétude) des modèles $\{0, 1\}$ par rapport à la logique classique.

Ainsi, l'approche sémantique devient le dual de l'approche syntaxique, et nous pouvons passer de l'une à l'autre selon nos besoins. C'est un résultat de cohérence très fort qui connecte deux approches de la logique qui au départ étaient distinctes.

D'autres théorèmes de complétude ont depuis été prouvés, pour différentes sémantiques, telles que celles de la logique intuitionniste, de la logique linéaire, de la logique d'ordre supérieure, etc.

L'idée de départ de notre travail est de renforcer le théorème de complétude de la façon suivante : si une proposition est vraie dans une certaine sémantique, alors elle est démontrable *sans la règle de coupure* dans un certain système de déduction. Le corollaire de ce résultat est que la règle de coupure est redondante (pour peu que l'on ait le théorème de correction). Cette approche a déjà été utilisée par Beth (voir [45]) pour le calcul des séquents classique, et par de Marco et Lipton [10] et Okada [35], dont reparlerons au chapitre 6.

L'originalité de ce travail, par rapport à ceux de Beth, Tait, Takahashi, et al. est que nous nous plaçons dans le cadre général de la déduction modulo, présenté ci-après.

Chapitre 2

La Déduction Modulo

2.1 Les règles de réécriture

Nous avons déjà expliqué pourquoi il était intéressant d'introduire des règles de réécriture dans un système de déduction. Voyons maintenant quelles sont les règles que nous nous autorisons à introduire.

Définition 2.1. *Une règle de réécriture de terme est une paire de termes $l \to r$ telle que les variables de r apparaissent dans l.*
Une règle de réécriture propositionnelle est une paire de propositions $L \to R$ telle que L soit atomique et que les variables libres de R apparaissent dans L.

Par exemple, des règles de réécriture sur des termes :

$$x * 0 \to 0$$

Et voici un exemple de règle de réécriture sur une proposition atomique :

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

Un système de réécriture, noté $\mathcal{R}$ est composé de deux ensembles :
– un ensemble de règles de réécritures propositionnelles.
– un ensemble de règles de réécritures de terme.

Nous allons maintenant définir sous quelles conditions une proposition P peut se récrire en une autre propositions Q :

Définition 2.2. *Soit un système de réécriture propositionnel $\mathcal{R}$, la proposition P se récrit en P' dans $\mathcal{R}$ si :*
$P_{|\omega} = \sigma(l)$ et $P' = P[\sigma(r)]_\omega$, pour une règle $l \to r \in \mathcal{R}$, une certaine occurrence ω dans P et une certaine substitution σ. Rappelons que σ dénote la substitution évitant la capture de la définition 1.6
On adoptera la notation $P \to_{\mathcal{R}} P'$.

Définition (Notations). *On note $\rightarrow_{\mathcal{R}}^{+}$ la fermeture transitive de $\rightarrow_{\mathcal{R}}$, $\rightarrow_{\mathcal{R}}^{*}$ sa fermeture transitive et réflexive et enfin et $\equiv_{\mathcal{R}}$ la fermeture transitive, réflexive et symétrique (parfois notée aussi $\leftrightarrow_{\mathcal{R}}$).*

Lorsqu'il n'y aura pas d'ambiguïté, nous omettrons l'indice $\mathcal{R}$.

Lorsque $A_1 \rightarrow^* B_1, ..., A_n \rightarrow^* B_n$, on note :

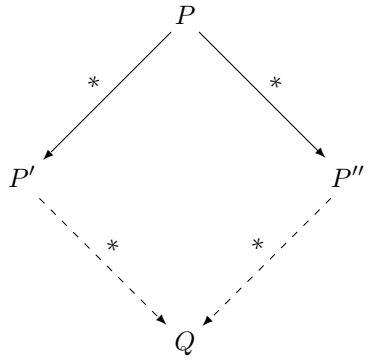
$$\{A_1, ..., A_n\} = \Gamma \quad \rightarrow^* \quad \Delta = \{B_1, ..., B_n\}$$

De même pour la notation $\Gamma \equiv_{\mathcal{R}} \Delta$

Notons que nous ne considérons pas d'axiome équationnel dans notre travail.

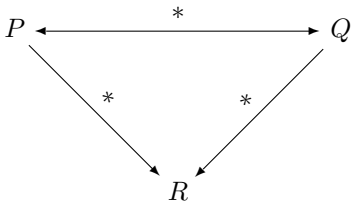
Les propriétés fondamentales que nous utiliserons sont la confluence et la terminaison d'un système de réécriture :

Définition 2.3 (Confluence). *Un système de réécriture $\mathcal{R}$ est dit confluent si pour tout P, P', P'' vérifiant $P \rightarrow^* P'$ et $P \rightarrow^* P''$, il existe Q telle que :*



Cette définition est suffisante, mais la plupart du temps, lorsque nous utiliserons la confluence d'un système de réécriture, nous ferons référence au lemme suivant, qui en découle immédiatement :

Lemme 2.1 (Church-Rosser). *Soit $\mathcal{R}$ un système de réécriture confluent. Soient deux propositions $P \equiv_{\mathcal{R}} Q$. Alors il existe une proposition R telle que :*



Preuve. Par induction sur la dérivation de $P \equiv_{\mathcal{R}} Q$. ■

Définition 2.4 (Terminaison). *Un système de réécriture $\mathcal{R}$ termine si et seulement si toute séquence $P_0 \rightarrow P_1 \ldots \rightarrow P_n$ est finie.*

$$\frac{\Gamma \vdash_{\mathcal{R}} A}{\Gamma \vdash_{\mathcal{R}} B} \quad \text{conv-d si } A \equiv_{\mathcal{R}} B$$

$$\frac{\Gamma, A \vdash_{\mathcal{R}} \Delta}{\Gamma, B \vdash_{\mathcal{R}} \Delta} \quad \text{conv-g si } A \equiv_{\mathcal{R}} B$$

FIG. 2.1 – règles de conversion du calcul des séquents intuitionniste modulo

$$\frac{\Gamma \vdash_{\mathcal{R}} A, \Delta}{\Gamma \vdash_{\mathcal{R}} B, \Delta} \quad \text{conv-d si } A \equiv_{\mathcal{R}} B$$

$$\frac{\Gamma, A \vdash_{\mathcal{R}} \Delta}{\Gamma, B \vdash_{\mathcal{R}} \Delta} \quad \text{conv-g si } A \equiv_{\mathcal{R}} B$$

FIG. 2.2 – règles de conversion du calcul des séquents classique modulo

2.2 Le calcul des séquents modulo

Nous considérons un ensemble de règles propositionnelles et sur les termes $\mathcal{R}$.

Nous voulons maintenant les ajouter au système de déduction, de telle sorte que si on a une démonstration du séquent $\Gamma \vdash P$, alors on a une démonstration du séquent $\Gamma' \vdash P'$ si $\Gamma \equiv_{\mathcal{R}} \Gamma'$ et $P \equiv_{\mathcal{R}} P'$.

La première méthode consiste à ajouter deux règles de conversion aux règles de déduction de la figure 1.1. Ces deux règles supplémentaires sont définies figure 2.1.

De même, pour avoir un calcul des séquents classique avec des règles de réécriture, nous pouvons rajouter les deux règles de conversion de la figure 2.2 au calcul des séquents de la figure 1.2.

Ceci donne des calculs des séquents avec règles de conversion.

Une deuxième méthode est de modifier les règles d'inférence de la figure 1.1, de façon à intégrer les règles de réécriture dans les règles d'inférence. Cette présentation a l'avantage d'être plus conforme à la philosophie de la déduction modulo, qui est d'intégrer calcul et déduction. C'est cette formulation, qui est présentée dans la figure 2.3, et c'est celle que nous utiliserons. Nous effectuons la même modification pour les règles d'inférence de la figure 1.2 et obtenons les règles de la figure 2.4.

Par abus de langage, nous utiliserons déduction modulo à la place de calcul

des séquents modulo, bien que la déduction modulo ne soit pas liée à un système d'inférence particulier (et est donc synonyme de logique des prédicats modulo).

Les présentations avec règles de conversion et sans règle de conversion sont équivalentes, comme l'atteste les proposition 2.2 et corollaire 2.3 ci-dessous.

Nous développerons les preuves et les énoncés dans le cas du calcul des séquents classique, le cas du calcul des séquents intuitionniste étant obtenu en n'autorisant qu'au plus une proposition à droite du séquent (c'est à dire Δ vide ou bien singleton.

Proposition 2.2 (Équivalence). *Soit $\mathcal{R}$ un ensemble de règles de réécriture. Soient $\Gamma \equiv_{\mathcal{R}} \Gamma'$ et $\Delta \equiv_{\mathcal{R}} \Delta'$ des ensembles de proposition équivalentes point à point.*
Alors, nous avons une dérivation du séquent :

$$\Gamma \vdash_{\mathcal{R}} \Delta$$

dans le système présenté figure 2.2 si et seulement si nous avons une dérivation du séquent :

$$\Gamma' \vdash_{\mathcal{R}} \Delta'$$

dans le système présenté figure 2.4

Preuve. Par induction sur la hauteur des preuves, en considérant la dernière règle appliquée, dans un sens comme dans l'autre. Le point délicat réside dans le fait qu'il nous faut absolument considérer des ensembles de propositions *équivalents* modulo $\mathcal{R}$. Voyons rapidement en quoi cela est nécessaire :

– Sens direct : si nous avons une preuve dans le calcul avec règles de conversions de la figure 2.2, et que la dernière règle est une règle de conversion gauche :

$$\dfrac{\dfrac{\pi}{\Gamma'' \vdash_{\mathcal{R}} \Delta}}{\Gamma \vdash_{\mathcal{R}} \Delta}$$

Alors nous pouvons appliquer l'hypothèse de récurrence sur la preuve π, puisque $\Gamma' \equiv_{\mathcal{R}} \Gamma \equiv_{\mathcal{R}} \Gamma''$.

Si c'est une règle du calcul des séquents habituel, par exemple $\wedge$-g :

$$\dfrac{\dfrac{\pi}{\Gamma, A, B \vdash_{\mathcal{R}} \Delta}}{\Gamma, A \wedge B \vdash_{\mathcal{R}} \Delta}$$

Alors, nous devons trouver une preuve du séquent : $\Gamma', P' \vdash_{\mathcal{R}} \Delta'$, avec $P' \equiv_{\mathcal{R}} A \wedge B$, $\Gamma \equiv_{\mathcal{R}} \Gamma'$ et $\Delta \equiv_{\mathcal{R}} \Delta'$.
Comme nous avons $\Gamma, A, B \equiv_{\mathcal{R}} \Gamma', A, B$ nous pouvons appliquer l'hypothèse de récurrence, et nous obtenons une preuve du séquent $\Gamma', A, B \vdash_{\mathcal{R}} \Delta'$, à laquelle nous pouvons appliquer la règle $\wedge$-g, ce qui nous donne la preuve cherchée.

$$\frac{}{P \vdash_{\mathcal{R}} Q}\text{axiome si } P \equiv_{\mathcal{R}} Q$$

$$\frac{\Gamma, P \vdash_{\mathcal{R}} S \quad \Gamma \vdash_{\mathcal{R}} Q}{\Gamma \vdash_{\mathcal{R}} S}\text{coupure si } P \equiv_{\mathcal{R}} Q$$

$$\frac{\Gamma, Q_1, Q_2 \vdash_{\mathcal{R}} S}{\Gamma, P \vdash_{\mathcal{R}} S}\text{contr-g si } P \equiv_{\mathcal{R}} Q_1 \equiv_{\mathcal{R}} Q_2$$

$$\frac{\Gamma \vdash_{\mathcal{R}} S}{\Gamma, P \vdash_{\mathcal{R}} S}\text{affaiblissement-g}$$

$$\frac{\Gamma \vdash_{\mathcal{R}}}{\Gamma \vdash_{\mathcal{R}} S}\text{affaiblissement-d}$$

$$\frac{\Gamma, P, Q \vdash_{\mathcal{R}} S}{\Gamma, R \vdash_{\mathcal{R}} S} \wedge\text{-g si } R \equiv_{\mathcal{R}} (P \wedge Q)$$

$$\frac{\Gamma \vdash_{\mathcal{R}} P \quad \Gamma \vdash_{\mathcal{R}} Q}{\Gamma \vdash_{\mathcal{R}} R} \wedge\text{-d si } R \equiv_{\mathcal{R}} (P \wedge Q)$$

$$\frac{\Gamma, P \vdash_{\mathcal{R}} S \quad \Gamma, Q \vdash_{\mathcal{R}} S}{\Gamma, R \vdash_{\mathcal{R}} S} \vee\text{-g si } R \equiv_{\mathcal{R}} (P \vee Q)$$

$$\frac{\Gamma \vdash_{\mathcal{R}} P}{\Gamma \vdash_{\mathcal{R}} R} \vee\text{-d si } R \equiv_{\mathcal{R}} (P \vee Q) \qquad \frac{\Gamma \vdash_{\mathcal{R}} Q}{\Gamma \vdash_{\mathcal{R}} R} \vee\text{-d si } R \equiv_{\mathcal{R}} (P \vee Q)$$

$$\frac{\Gamma \vdash_{\mathcal{R}} P \quad \Gamma, Q \vdash_{\mathcal{R}} S}{\Gamma, R \vdash_{\mathcal{R}} S} \Rightarrow\text{-g si } R \equiv_{\mathcal{R}} (P \Rightarrow Q)$$

$$\frac{\Gamma, P \vdash_{\mathcal{R}} Q}{\Gamma \vdash_{\mathcal{R}} R} \Rightarrow\text{-d si } R \equiv_{\mathcal{R}} (P \Rightarrow Q)$$

$$\frac{\Gamma \vdash_{\mathcal{R}} P}{\Gamma, R \vdash_{\mathcal{R}} Q}\neg\text{-g si } R \equiv_{\mathcal{R}} \neg P$$

$$\frac{\Gamma, P \vdash_{\mathcal{R}}}{\Gamma \vdash_{\mathcal{R}} R}\neg\text{-d si } R \equiv_{\mathcal{R}} \neg P$$

$$\frac{}{\Gamma, P \vdash_{\mathcal{R}} S}\bot\text{-g si } P \equiv_{\mathcal{R}} \bot$$

$$\frac{\Gamma, \{t/x\}P \vdash_{\mathcal{R}} S}{\Gamma, Q \vdash_{\mathcal{R}} S}\forall\text{-g si } Q \equiv_{\mathcal{R}} \forall xP, t \text{ clos}$$

$$\frac{\Gamma \vdash_{\mathcal{R}} \{c/x\}P}{\Gamma \vdash_{\mathcal{R}} Q}\forall\text{-d si } c \text{ constante fraîche et si } Q \equiv_{\mathcal{R}} \forall xP$$

$$\frac{\Gamma, \{c/x\}P \vdash_{\mathcal{R}} S}{\Gamma, Q \vdash_{\mathcal{R}} S}\exists\text{-g si } c \text{ constante fraîche et si } Q \equiv_{\mathcal{R}} \exists xP$$

$$\frac{\Gamma \vdash_{\mathcal{R}} \{t/x\}P}{\Gamma \vdash_{\mathcal{R}} Q}\exists\text{-d si } Q \equiv_{\mathcal{R}} \exists xP, t \text{ clos}$$

FIG. 2.3 – Règles d'inférence du calcul des séquents intuitionniste modulo

$$\frac{}{P \vdash_{\mathcal{R}} Q}\text{axiome si } P \equiv_{\mathcal{R}} Q$$

$$\frac{\Gamma, P \vdash_{\mathcal{R}} \Delta \quad \Gamma \vdash_{\mathcal{R}} Q, \Delta}{\Gamma \vdash_{\mathcal{R}} \Delta}\text{coupure si } P \equiv_{\mathcal{R}} Q$$

$$\frac{\Gamma, Q_1, Q_2 \vdash_{\mathcal{R}} \Delta}{\Gamma, P \vdash_{\mathcal{R}} \Delta}\text{contr-g si } P \equiv_{\mathcal{R}} Q_1 \equiv_{\mathcal{R}} Q_2$$

$$\frac{\Gamma \vdash_{\mathcal{R}} Q_1, Q_2, \Delta}{\Gamma \vdash_{\mathcal{R}} P, \Delta}\text{contr-d si } P \equiv_{\mathcal{R}} Q_1 \equiv_{\mathcal{R}} Q_2$$

$$\frac{\Gamma \vdash_{\mathcal{R}} \Delta}{\Gamma, P \vdash_{\mathcal{R}} \Delta}\text{affaiblissement-g}$$

$$\frac{\Gamma \vdash_{\mathcal{R}} \Delta}{\Gamma \vdash_{\mathcal{R}} P, \Delta}\text{affaiblissement-d}$$

$$\frac{\Gamma, P, Q \vdash_{\mathcal{R}} \Delta}{\Gamma, R \vdash_{\mathcal{R}} \Delta} \wedge\text{-g si } R \equiv_{\mathcal{R}} (P \wedge Q)$$

$$\frac{\Gamma \vdash_{\mathcal{R}} P, \Delta \quad \Gamma \vdash_{\mathcal{R}} Q, \Delta}{\Gamma \vdash_{\mathcal{R}} R, \Delta} \wedge\text{-d si } R \equiv_{\mathcal{R}} (P \wedge Q)$$

$$\frac{\Gamma, P \vdash_{\mathcal{R}} \Delta \quad \Gamma, Q \vdash_{\mathcal{R}} \Delta}{\Gamma, R \vdash_{\mathcal{R}} \Delta} \vee\text{-g si } R \equiv_{\mathcal{R}} (P \vee Q)$$

$$\frac{\Gamma \vdash_{\mathcal{R}} P, Q, \Delta}{\Gamma \vdash_{\mathcal{R}} R, \Delta} \vee\text{-d si } R \equiv_{\mathcal{R}} (P \vee Q)$$

$$\frac{\Gamma \vdash_{\mathcal{R}} P, \Delta \quad \Gamma, Q \vdash_{\mathcal{R}} \Delta}{\Gamma, R \vdash_{\mathcal{R}} \Delta} \Rightarrow\text{-g si } R \equiv_{\mathcal{R}} (P \Rightarrow Q)$$

$$\frac{\Gamma, P \vdash_{\mathcal{R}} Q, \Delta}{\Gamma \vdash_{\mathcal{R}} R, \Delta} \Rightarrow\text{-d si } R \equiv_{\mathcal{R}} (P \Rightarrow Q)$$

$$\frac{\Gamma \vdash_{\mathcal{R}} P, \Delta}{\Gamma, R \vdash_{\mathcal{R}} \Delta}\neg\text{-g si } R \equiv_{\mathcal{R}} \neg P$$

$$\frac{\Gamma, P \vdash_{\mathcal{R}} \Delta}{\Gamma \vdash_{\mathcal{R}} R, \Delta}\neg\text{-d si } R \equiv_{\mathcal{R}} \neg P$$

$$\frac{}{\Gamma, P \vdash_{\mathcal{R}} \Delta}\bot\text{-g si } P \equiv_{\mathcal{R}} \bot$$

$$\frac{\Gamma, \{t/x\}P \vdash_{\mathcal{R}} \Delta}{\Gamma, Q \vdash_{\mathcal{R}} \Delta}\forall\text{-g si } Q \equiv_{\mathcal{R}} \forall xP, t \text{ clos}$$

$$\frac{\Gamma \vdash_{\mathcal{R}} \{c/x\}P, \Delta}{\Gamma \vdash_{\mathcal{R}} Q, \Delta}\forall\text{-d si } c \text{ constante fraîche et si } Q \equiv_{\mathcal{R}} \forall xP$$

$$\frac{\Gamma, \{c/x\}P \vdash_{\mathcal{R}} \Delta}{\Gamma, Q \vdash_{\mathcal{R}} \Delta}\exists\text{-g si } c \text{ constante fraîche et si } Q \equiv_{\mathcal{R}} \exists xP$$

$$\frac{\Gamma \vdash_{\mathcal{R}} \{t/x\}P, \Delta}{\Gamma \vdash_{\mathcal{R}} Q, \Delta}\exists\text{-d si } Q \equiv_{\mathcal{R}} \exists xP, t \text{ clos}$$

FIG. 2.4 – Règles d'inférence du calcul des séquents classique modulo

– Réciproque : Si nous avons une preuve dans le calcul des séquents de la figure 2.4, et que la dernière règle appliquée est $\wedge$ à gauche :

$$\dfrac{\dfrac{\pi}{\Gamma', A', B' \vdash_{\mathcal{R}} \Delta'}}{\Gamma', P' \vdash_{\mathcal{R}} \Delta'} \; P' \equiv_{\mathcal{R}} A' \wedge B'$$

Nous disposons des égalités $\Delta \equiv_{\mathcal{R}} \Delta'$, $\Gamma \equiv_{\mathcal{R}} \Gamma'$ ainsi que de $P \equiv_{\mathcal{R}} P'$ et nous devons trouver une preuve du séquent $\Gamma, P \vdash_{\mathcal{R}} \Delta$.Par hypothèse de récurrence nous savons trouver une preuve de $\Gamma, A', B' \vdash_{\mathcal{R}} \Delta$ dans le système avec conversion de la figure 2.2. Donc, en appliquant la règle $\wedge$-gauche de la figure 1.2 *puis* une règle de conversion, nous obtenons la preuve suivante :

$$\dfrac{\dfrac{\dfrac{\pi'}{\Gamma, A', B' \vdash_{\mathcal{R}} \Delta}}{\Gamma, A' \wedge B' \vdash_{\mathcal{R}} \Delta} \wedge - \text{g}}{\Gamma, P \vdash_{\mathcal{R}} \Delta} \text{ conv-g } P \equiv_{\mathcal{R}} P' \equiv_{\mathcal{R}} A' \wedge B'$$

qui est ce que nous cherchions.

– Tous les autres cas, dans un sens comme dans l'autre, se résolvent de la même manière.

■

Remarque. Dans toute la transformation précédemment définie, nous pouvons noter qu'une preuve sans coupures dans un système est remplacée par une preuve sans coupures dans l'autre système.

Le corollaire immédiat est celui d'équiprouvabilité :

Corollaire 2.3 (Équivalence). *Soit $\mathcal{R}$ un système de règles de réécriture. Soient Γ et Δ des ensembles de proposition. Alors le séquent :*

$$\Gamma \vdash_{\mathcal{R}} \Delta$$

a une preuve dans le calcul des séquents modulo avec règles de conversion de la figure 2.2, si et seulement si il a une preuve dans le calcul des séquents modulo de la figure 2.4.

Preuve. D'après la proposition 2.2, appliquée avec $\Gamma' = \Gamma$ et $\Delta' = \Delta$. ■

Le calcul des séquents modulo est en adéquation avec $\mathcal{R}$. Autrement dit, deux séquents équivalents modulo $\mathcal{R}$ sont équivalemment prouvables. Ce résultat, bien qu'allant de soi, nécessite d'être démontré et découle presque immédiatement de la proposition précédente :

Corollaire 2.4. *Soit des ensembles de propositions $\Gamma' \equiv_{\mathcal{R}} \Gamma$ et $\Delta' \equiv_{\mathcal{R}} \Delta$.*

$$\Gamma \vdash_{\mathcal{R}} \Delta \quad \textit{ssi} \quad \Gamma' \vdash_{\mathcal{R}} \Delta'$$

dans le même système de déduction.

Preuve. D'après la proposition 2.2. Soit une preuve de $\Gamma \vdash_{\mathcal{R}} \Delta$ en calcul des séquents modulo de la figure 2.4. Nous avons donc une preuve de $\Gamma' \vdash_{\mathcal{R}} \Delta'$ en calcul des séquents avec règles de conversion. Et d'après le corollaire 2.3 nous avons aussi une preuve de $\Gamma \vdash_{\mathcal{R}} \Delta$ en calcul des séquents modulo de la figure 2.4. ■

2.3 Restriction sur les règles d'inférence

Dans toute cette partie, nous étudions l'impact de la confluence sur différents systèmes de déduction modulo. Si rien n'est précisé, alors nous considérons un système de réécriture éventuellement non confluent.

Nous pouvons restreindre, de la même manière qu'à la section 1.2.4 les règles axiome, affaiblissement et $\bot$-gauches à ne s'appliquer qu'à des atomes. Par exemple, avec la règle $A \rightarrow B \wedge C$, nous avons une preuve du séquent $A \vdash_{\mathcal{R}} B \wedge C$:

$$\dfrac{\dfrac{\overline{B, C \vdash_{\mathcal{R}} B} \quad \overline{B, C \vdash_{\mathcal{R}} C}}{B, C \vdash_{\mathcal{R}} B \wedge C}}{A \vdash_{\mathcal{R}} B \wedge C}$$

Ici, ce ne sont pas ces restrictions qui nous intéressent mais les restrictions sur les conditions de bord des règles de déduction (les règles de réécriture).

Une preuve en calcul des séquents est moralement orientée du bas vers le haut. Du moins, dans la vision d'une recherche de preuve : on cherche une preuve du séquent du bas, en essayant certaines règles. Lorsqu'on arrive au bout (les règles axiome), la preuve est complète.

Si l'on veut mélanger déduction et calcul, ne serait-il pas judicieux d'orienter le calcul du haut vers le bas ? Or, une règle de réécriture, vue comme règle de calcul est toujours orientée de la gauche vers la droite, et peut être vue comme une règle de réduction :

$$0 + x \rightarrow x$$

Ainsi, au lieu de conditions d'équivalence dans les règles de déduction :

$$\dfrac{\Gamma \vdash_{\mathcal{R}} P, Q, \Delta}{\Gamma \vdash_{\mathcal{R}} R, \Delta} \vee\text{-d si } R \equiv_{\mathcal{R}} (P \vee Q)$$

nous pourrions avoir envie de briser la symétrie. Nous tirerions un profit maximum de la notion de règle de calcul. La règle précédente serait remplacée par celle-ci :

$$\dfrac{\Gamma \vdash_{\mathcal{R}} P, Q, \Delta}{\Gamma \vdash_{\mathcal{R}} R, \Delta} \vee\text{-d si } R \rightarrow^{*} (P \vee Q)$$

En remplaçant de cette manière toutes les règles du calcul des séquents modulo de la figure 2.4 par des règles asymétriques, nous obtenons le calcul des séquents asymétrique classique de [13], auquel nous avons ajouté des règles de réécriture propositionnelles.

Il est présenté figure 2.5. Il est aussi possible de définir de manière identique un calcul de séquents modulo asymétrique intuitionniste (et surtout, de prouver les mêmes propositions d'équivalence), mais nous n'en aurons pas besoin dans la suite de nos travaux.

Il est aussi possible (sous l'hypothèse confluence de $\mathcal{R}$), de restreindre les règles axiome, $\bot$-g et affaiblissement à des propositions atomiques.

$$\frac{}{\Gamma, P \vdash_{\mathcal{R}} Q}\text{axiome}, P \to^* R^* \leftarrow Q \qquad \frac{\Gamma, P \vdash_{\mathcal{R}} \Delta \quad \Gamma \vdash_{\mathcal{R}} Q, \Delta}{\Gamma \vdash_{\mathcal{R}} \Delta}\text{coupure}, P^* \leftarrow R \to^* Q$$

$$\frac{\Gamma, Q, R \vdash_{\mathcal{R}} \Delta}{\Gamma, P \vdash_{\mathcal{R}} \Delta}\text{contr-g}, Q^* \leftarrow P \to^* R \qquad \frac{}{\Gamma, P \vdash_{\mathcal{R}} \Delta}\bot\text{-g}, P \to^* \bot$$

$$\frac{\Gamma \vdash_{\mathcal{R}} \Delta}{\Gamma, P \vdash_{\mathcal{R}} \Delta}\text{affaiblissement-g} \qquad \frac{\Gamma \vdash_{\mathcal{R}} \Delta}{\Gamma \vdash_{\mathcal{R}} P, \Delta}\text{affaiblissement-d}$$

$$\frac{\Gamma, Q, R \vdash_{\mathcal{R}} \Delta}{\Gamma, P \vdash_{\mathcal{R}} \Delta} \wedge\text{-g}, P \to^* Q \wedge R \qquad \frac{\Gamma \vdash_{\mathcal{R}} Q, \Delta \quad \Gamma \vdash_{\mathcal{R}} R, \Delta}{\Gamma \vdash_{\mathcal{R}} P, \Delta} \wedge\text{-d}, P \to^* Q \wedge R$$

$$\frac{\Gamma, Q \vdash_{\mathcal{R}} \Delta \quad \Gamma, R \vdash_{\mathcal{R}} \Delta}{\Gamma, P \vdash_{\mathcal{R}} \Delta} \vee\text{-g}, P \to^* Q \vee R \qquad \frac{\Gamma \vdash_{\mathcal{R}} Q, R, \Delta}{\Gamma \vdash_{\mathcal{R}} P, \Delta} \vee\text{-d}, P \to^* Q \vee R$$

$$\frac{\Gamma \vdash_{\mathcal{R}} Q, \Delta \quad \Gamma, R \vdash_{\mathcal{R}} \Delta}{\Gamma, P \vdash_{\mathcal{R}} \Delta} \Rightarrow\text{-g}, P \to^* Q \Rightarrow R \qquad \frac{\Gamma, Q \vdash_{\mathcal{R}} R, \Delta}{\Gamma \vdash_{\mathcal{R}} P, \Delta} \Rightarrow\text{-d}, P \to^* Q \Rightarrow R$$

$$\frac{\Gamma \vdash_{\mathcal{R}} Q, \Delta}{\Gamma, P \vdash_{\mathcal{R}} \Delta}\neg\text{-g}, P \to^* \neg Q \qquad \frac{\Gamma, Q \vdash_{\mathcal{R}} \Delta}{\Gamma \vdash_{\mathcal{R}} P, \Delta}\neg\text{-d}, P \to^* \neg Q$$

$$\frac{\Gamma, \{t/x\}Q \vdash_{\mathcal{R}} \Delta}{\Gamma, P \vdash_{\mathcal{R}} \Delta}\forall\text{-g}, P \to^* \forall x Q \qquad \frac{\Gamma \vdash_{\mathcal{R}} \{c/x\}Q, \Delta}{\Gamma \vdash_{\mathcal{R}} P, \Delta}\forall\text{-d}, P \to^* \forall x Q, c \text{ fraîche}$$

$$\frac{\Gamma, \{c/x\}Q \vdash_{\mathcal{R}} \Delta}{\Gamma, P \vdash_{\mathcal{R}} \Delta}\exists\text{-g}, P \to^* \exists x Q, c \text{ fraîche} \qquad \frac{\Gamma \vdash_{\mathcal{R}} \{t/x\}Q, \Delta}{\Gamma \vdash_{\mathcal{R}} P, \Delta}\exists\text{-d}, P \to^* \exists x Q$$

FIG. 2.5 – Calcul des séquents modulo asymétrique classique

Malheureusement, dans sa version sans coupure, le calcul des séquents modulo asymétrique ainsi obtenu n'est pas forcément équivalent au calcul des séquents modulo, comme le montre l'exemple suivant. Nous avons deux règles de réécriture :

$$\begin{aligned} A &\to B \\ A &\to C \end{aligned}$$

Et nous avons la preuve suivante (en déduction modulo) :

$$\frac{}{B \vdash_{\mathcal{R}} C}\ \text{axiome}\ B \equiv_{\mathcal{R}} C$$

Mais nous n'avons pas $B \to A \leftarrow C$, et donc pas de preuve sans coupure de ce séquent en déduction modulo asymétrique. En autorisant la règle de coupure, on a de nouveau l'équivalence (dans le cas général, par induction sur la longueur dérivation de $B \equiv_{\mathcal{R}} C$). Ainsi on n'a plus le théorème d'élimination des coupures pour le calcul asymétrique !

Le système de réécriture précédent n'est pas confluent. Si nous supposons la confluence du système de réécriture $\mathcal{R}$, alors "orienter" le calcul des séquents modulo devient possible. En voici la preuve :

Proposition 2.5. *Soit $\mathcal{R}$ un système de réécriture confluent.*
Soient $\Gamma \to^* \Gamma'$ et $\Delta \to^* \Delta'$ des ensembles de propositions.

Si nous avons une preuve sans coupure du séquent :

$$\Gamma \vdash_{\mathcal{R}} \Delta$$

en déduction modulo, alors nous avons une preuve sans coupure du séquent :

$$\Gamma' \vdash_{\mathcal{R}} \Delta'$$

en déduction modulo asymétrique.

Preuve. Par récurrence sur la hauteur de la preuve du séquent $\Gamma \vdash_{\mathcal{R}} \Delta$. Voyons le cas de la règle $\vee$-d (tous les autres cas se traitent exactement de la même manière). Nous avons la preuve suivante :

$$\frac{\begin{array}{c}\vdots\\ \Gamma \vdash_{\mathcal{R}} P, Q, \Delta\end{array}}{\Gamma \vdash_{\mathcal{R}} R, \Delta}\ \vee\text{-d si}\ R \equiv_{\mathcal{R}} (P \vee Q)$$

Nous devons trouver une preuve en déduction modulo asymétrique du séquent $\Gamma' \vdash_{\mathcal{R}} R', \Delta'$ (avec $R \to^* R'$). Or, $R'^* \leftarrow R \equiv_{\mathcal{R}} P \vee Q$, et par confluence, nous savons que :

$$\begin{array}{ccccc} R' & & \equiv_{\mathcal{R}} & & P \vee Q \\ & \searrow & & \swarrow & \\ & & P' \vee Q' & & \end{array}$$

pour une certaine proposition $P' \vee Q'$. De plus, par hypothèse de récurrence, nous avons une preuve en déduction modulo asymétrique :

$$\begin{array}{c}\vdots\\ \Gamma' \vdash_{\mathcal{R}} P', Q', \Delta'\end{array}$$

car $P \to^* P'$ et $Q \to^* Q'$, d'après le lemme 3.1. Nous pouvons ajouter à la fin de cette preuve la règle $\vee$-d :

$$\dfrac{\dfrac{\vdots}{\Gamma' \vdash_{\mathcal{R}} P', Q', \Delta'}}{\Gamma' \vdash_{\mathcal{R}} R', \Delta'} \vee\text{-d si } R \equiv_{\mathcal{R}} (P \vee Q)$$

Ce qui est la preuve que nous cherchions. ■

Suit le corollaire immédiat :

Corollaire 2.6 (Équivalence). *Soir $\mathcal{R}$ un système de réécriture confluent. $\Gamma \vdash_{\mathcal{R}} \Delta$ a une preuve sans coupure en déduction modulo si et seulement si il a une preuve sans coupure en déduction modulo asymétrique.*

Preuve. La réciproque est immédiate, puisque si l'on a $P \to^* Q$; alors on a aussi $P \equiv_{\mathcal{R}} Q$, et donc une preuve en déduction modulo asymétrique est aussi une preuve en déduction modulo tout court.
Le sens direct s'obtient d'après la proposition précédente. ■

Ceci est un résultat très important du point de vue d'un programme de recherche de preuve. Il affirme que, sous l'hypothèse d'un ensemble de règles de réécriture confluent (hypothèse qui sera toujours vérifiée par la suite) nous pouvons nous contenter d'appliquer les règles de réécriture de la gauche vers la droite.

Dans [11], il est prouvé que si $\mathcal{R}$ est confluent, alors $\equiv_{\mathcal{R}}$ est décidable. Mais rien ne dit comment trouver la proposition Q telle que $P \equiv_{\mathcal{R}} Q$. Notre résultat fournit au contraire un moyen : il faut réécrire P. La recherche de preuve ne se double donc pas d'une recherche de propositions équivalentes, il suffit de réécrire (par exemple, de normaliser si le système est normalisant).

Nous pouvons de même transformer le calcul des séquents présenté avec des règles de conversion, de la figure 2.2. Nous aurons alors un calcul des séquents modulo avec règles de conversion asymétriques. Il y a équivalence entre les deux présentations :

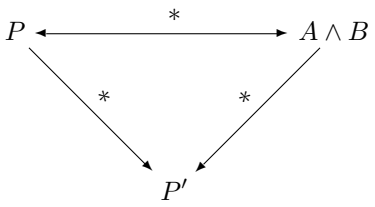
Proposition 2.7 (Équivalence). *Soit $\mathcal{R}$ un ensemble de règles de réécriture confluent. Le calcul des séquents avec règles de conversion asymétriques de la figure 2.2 est équivalent au calcul des séquents asymétrique de la figure 2.5*

Preuve. Exactement la même que celle de la proposition 2.2.
Dans le sens direct, si la dernière règle est une règle $\wedge$-gauche :

$$\dfrac{\dfrac{\pi}{\Gamma, A, B \vdash_{\mathcal{R}} \Delta}}{\Gamma, A \wedge B \vdash_{\mathcal{R}} \Delta}$$

Nous devons trouver une preuve de $\Gamma', P \vdash_{\mathcal{R}} \Delta'$ avec $P \equiv_{\mathcal{R}} A \wedge B$. Par

confluence, nous connaissons l'existence de P' telle que le schéma suivant existe :



Encore une fois par confluence (lemme 3.1), nous savons que P' est de la forme $A' \wedge B'$ avec $A \rightarrow^* A'$ et $B \rightarrow B'$.

Alors nous pouvons appliquer l'hypothèse de récurrence pour avoir une preuve de $\Gamma', A', B' \vdash_{\mathcal{R}} \Delta'$, que nous pouvons combiner avec la règle $\wedge$-g car $P \rightarrow A' \wedge B'$. ■

De l'utilité des règles de réécriture

Sous l'hypothèse de la convergence (confluence et terminaison), nous pouvons nous contenter d'appliquer des règles logiques à des propositions en forme normale. Il pourrait être suffisant de normaliser les séquents au début de la preuve, et d'appliquer la recette suivante, pour trouver une preuve de $\Gamma' \vdash_{\mathcal{R}} \Delta'$:

1. Mettre toutes les propositions en forme normale :

$$\begin{array}{lll} \Gamma' & \triangleright^* & \Gamma \\ \Delta' & \triangleright^* & \Delta \end{array}$$

2. Chercher une preuve de $\Gamma \vdash_{\mathcal{R}} \Delta$ dans le calcul des séquents habituel.

Si une telle méthode était possible, alors l'introduction de règles de réécriture n'aurait pas beaucoup de sens.

Ceci n'est pas possible, et c'est justement une des forces de la déduction modulo. En effet, nous autorisons des règles du type :

$$0 = S(x) \rightarrow \bot$$

Et si l'on veut prouver le séquent $\forall x \exists y (x = S(y)) \vdash_{\mathcal{R}}$, dont toutes les propositions sont en forme normale, on ne peut pas se contenter d'appliquer les règles du calcul des séquents, il faut appliquer celles de la déduction modulo :

$$\dfrac{\dfrac{\dfrac{}{0 = S(c) \vdash_{\mathcal{R}}}\,\bot\text{-g}}{\exists y(0 = S(y)) \vdash_{\mathcal{R}}}}{\forall x \exists y (x = S(y)) \vdash_{\mathcal{R}}}$$

Le calcul des séquents sans coupure

En déduction modulo aussi, il est très important de montrer que la règle de coupure :

$$\dfrac{\Gamma, P \vdash_{\mathcal{R}} \Delta \quad \Gamma \vdash_{\mathcal{R}} Q, \Delta}{\Gamma \vdash_{\mathcal{R}} \Delta}\text{coupure, } P \equiv_{\mathcal{R}} Q$$

est redondante. C'est à dire que si l'on peut trouver une preuve du séquent $\Gamma \vdash_{\mathcal{R}} \Delta$, alors nous pouvons trouver une preuve de ce même séquent *sans utiliser la règle de coupure*. L'élimination de cette règle implique de nombreux résultats fondamentaux, comme la cohérence du calcul des séquents associé, ou son analyticité. Ainsi, en calcul des séquents modulo intuitionniste, nous aurons la propriété de disjonction et de témoin existentiel qui sont les suivantes.

Si on a une preuve des séquents :

$$\vdash_{\mathcal{R}} A \vee B \qquad \vdash_{\mathcal{R}} \exists x P$$

alors on a soit une preuve de $\vdash_{\mathcal{R}} A$, soit une preuve de $\vdash_{\mathcal{R}} B$ et un terme clos t tel qu'on a une preuve de $\vdash_{\mathcal{R}} \{t/x\}P$.

Ces propriétés sont prouvées dans le calcul des séquents sans coupure.

Remarque. Nous perdons cette propriété dès lors que nous avons des hypothèses. Par exemple, on a la preuve suivante :

$$\frac{}{A \vee B \vdash A \vee B}$$

mais on n'a ni $A \vee B \vdash A$, ni $A \vee B \vdash B$. (on peut le prouver en construisant des contre-modèles : un ou B est faux, A vrai, et un autre où A est faux et B vrai).

Dans le chapitre suivant, il sera prouvé que, pour des hypothèses vérifiant une certaine condition, on retrouve cette propriété.

Nos résultats s'appuient principalement sur le théorème de complétude du calcul des séquents sans la règle de coupure. Pour distinguer ce calcul du calcul des séquents avec coupure, et de manière à éviter de longues périphrases, nous adopterons la notation suivante pour un séquent du calcul des séquents sans coupure :

Définition 2.5 (Calcul des séquents modulo sans coupures).

$$\Gamma \vdash_{\mathcal{R}}^{cf} \Delta$$

2.4 Sémantiques de la déduction modulo

Lorsque nous définissons une sémantique, nous devons être capables de prouver les théorèmes de correction et de complétude de cette sémantique par rapport à la logique des prédicats.

C'est pour cette raison que nous devons raffiner les notions de modèles dans le cadre de la déduction modulo, car nous avons introduit dans la syntaxe des règles de réécriture $\mathcal{R}$. Ainsi, les modèles en déduction modulo seront les modèles vus précédemment avec la condition supplémentaire que ceux-ci vérifient $\mathcal{R}$.

Ainsi, la notion de sémantique pour la déduction modulo varie non seulement selon le fait que nous sommes en déduction modulo classique ou intuitionniste, mais aussi selon le système $\mathcal{R}$ de règles de réécriture utilisé, comme nous pouvons le vérifier dans les deux définitions ci-dessous.

Modèles booléens pour la déduction modulo

Définition 2.6 (Modèle pour un système de réécriture). *Soit $\mathcal{M}$ une structure et $\mathcal{R}$ un ensemble de règles de réécriture. Nous dirons que $\mathcal{M}$ est un modèle de $\mathcal{R}$ si et seulement si :*

$$P \equiv_{\mathcal{R}} Q \quad \Leftrightarrow |P|_\sigma = |Q|_\sigma$$

pour tout assignement σ. Lorsque $\mathcal{M}$ est un modèle de $\mathcal{R}$, nous notons la relation $\models$ comme ceci : $\models_{\mathcal{R}}$.

Structures de Kripke pour la déduction modulo

Définition 2.7 (Structure de Kripke pour un système de réécriture). *Soit $\mathcal{K}$ une structure de Kripke, et $\mathcal{R}$ un ensemble de règles de réécriture. Nous dirons que $\mathcal{K}$ est un modèle de $\mathcal{R}$ si et seulement si pour tout monde $\alpha \in K$, pour toutes propositions $P \equiv_{\mathcal{R}} Q$, nous avons :*

$$\alpha \Vdash P \quad \Leftrightarrow \quad \alpha \Vdash Q$$

Nous modifions en conséquence les symboles de modélisation $\models_{\mathcal{R}}$ et de forcing $\Vdash_{\mathcal{R}}$.

Deuxième partie

Propriétés élémentaires de la Déduction Modulo

Chapitre 3

Définitions et premiers résultats

Nous établissons ici certains résultats en déduction modulo, qui sont valables pour tous les systèmes de réécriture (a condition parfois de supposer la confluence). Leur preuve est purement syntaxique et ne requiert aucune introduction de sémantique.

Dans toute la suite de ce chapitre, nous supposerons la confluence du système de réécriture $\mathcal{R}$ étudié, et nous supposerons uniquement celle-ci.

3.1 Connecteur principal

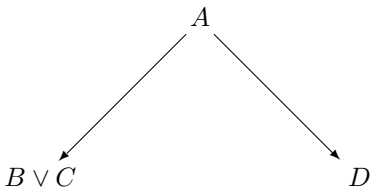
En dehors de tout système de déduction, nous pouvons prouver un résultat qui paraît aller de soi : des propositions équivalentes ont le même connecteur principal (c'est à dire, formellement, celui qui est à la racine de l'arbre de formation de la proposition).

Ce lemme joue un rôle fondamental dans nombre de démonstrations syntaxiques, car elles font pour la plupart d'entre elles appel à une induction sur la structure des propositions, et si $P \equiv_{\mathcal{R}} A \wedge B$ est non atomique alors nous devons être certains que P a aussi pour connecteur principal $\wedge$.

Lemme 3.1 (Connecteurs). *Soient deux propositions non atomiques $P \equiv_{\mathcal{R}} Q$. Alors P et Q ont le même connecteur principal, et leurs sous-formules immédiates sont équivalentes modulo $\mathcal{R}$.*

Remarque. Avant de prouver ce lemme, remarquons que certains systèmes de réécriture, bien que n'étant pas confluents possèdent quand-même la propriété

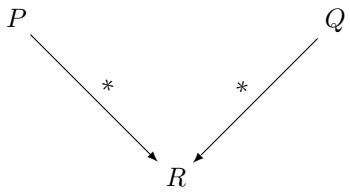
du lemme. Par exemple, le système suivant.



En effet, il est suffisant qu'un atome se réécrive soit sur une proposition complexe, soit sur un autre atome.

Dans la suite, nous aurons besoin non pas de la confluence, mais du résultat du lemme 3.1. Cependant, la confluence est un résultat seulement légèrement plus fort que ce lemme, et dans la pratique nous supposerons avoir des systèmes de réécriture confluents.

Preuve. Par confluence nous avons :



Nous allons prouver par récurrence sur le nombre de dérivations de $P \to^* R$ que P et R ont le même connecteur principal.

- Si $P = R$, alors ils ont le même connecteur principal.
- Si $P \to R' \to^* R$, alors la réécriture de P en R' a lieu dans un atome qui occure dans une sous-formule immédiate de P. Le connecteur principal de P ne peut donc pas changer, et les sous-formules immédiates de P et R' sont soit égales, soit trivialement équivalentes. L'hypothèse de récurrence nous permet de conclure la même chose pour R' et R, ce qui nous permet de conclure par transitivité.

Le même résultat s'applique pour Q et R.

Ainsi, P, R et Q ont le même connecteur principal.

■

3.2 Déduction Modulo Classique

Au chapitre précédent, nous avons commencé par présenter le calcul des séquents intuitionniste, puis sommes passés au cas classique. C'est l'ordre de présentation habituel lorsqu'on veut présenter la syntaxe, car il est plus simple de comprendre des séquents ayant une seule conclusion.

De manière complètement duale, il sera plus compréhensible de présenter d'abord la sémantique classique, puis la sémantique intuitionniste. Comme notre

approche est plutôt basée sur la sémantique que sur la syntaxe, nous utiliserons cette approche dorénavant. C'est pourquoi nous commençons par un chapitre portant sur la déduction modulo classique.

3.2.1 Cohérence et complétude sans coupures : définitions

Soit un ensemble de propositions (éventuellement infini) $\mathcal{T}$, que nous appellerons théorie. Notre point de départ sera que nous supposerons qu'elle ne prouve pas toutes les propositions, c'est à dire qu'elle est cohérente. On ne voudrait pas ceci, par exemple :

$$\mathcal{T} \vdash_{\mathcal{R}} P \qquad \mathcal{T} \vdash_{\mathcal{R}} \neg P$$

En effet, cela implique, par la règle de coupure, que $\mathcal{T} \vdash_{\mathcal{R}}$, c'est à dire que $\mathcal{T}$ peut démontrer n'importe quelle proposition Q :

$$\dfrac{\dfrac{\mathcal{T} \vdash_{\mathcal{R}} P}{\mathcal{T}, \neg P \vdash_{\mathcal{R}}} \qquad \dfrac{}{\mathcal{T} \vdash_{\mathcal{R}} \neg P}}{\dfrac{\mathcal{T} \vdash_{\mathcal{R}}}{\mathcal{T} \vdash_{\mathcal{R}} Q}}\ \textbf{coupure}$$

C'est une des définitions possibles de *l'incohérence* de la théorie $\mathcal{T}$. Cependant, comme lorsque nous plaçons en calcul des séquents sans coupures, il se pourrait que certaines théories ne possèdent plus cette propriété, tout en restant cohérentes. Car à partir de :

$$\begin{array}{lll} \mathcal{T} & \vdash^{cf}_{\mathcal{R}} & P \\ \mathcal{T} & \vdash^{cf}_{\mathcal{R}} & \neg P \end{array}$$

nous n'avons aucun moyen de montrer que $\mathcal{T}$ prouve n'importe quelle proposition, car nous nous interdisons l'application de la règle de coupure.

Ainsi, il faut prendre beaucoup de soin lors de la définition de la cohérence, car toutes ne sont pas égales. Voici donc la définition :

Définition 3.1 (Cohérence sans coupures). *Une théorie $\mathcal{T}$ est cohérente si et seulement si $\mathcal{T} \nvdash^{cf}_{\mathcal{R}}$*

Cette définition est équivalente à la définition standard *dans le calcul avec coupure*, mais, répétons le, nous considérons ici un calcul sans coupures, ce qui rend ces deux définitions distinctes. Pour prouver leur égalité, il faut prouver le théorème d'élimination des coupures. Cette version de la cohérence est plus forte et c'est elle qui nous permettra de démontrer le théorème d'élimination des coupures.

Ayant une théorie cohérente, nous aimerions définir la valeur de vérité des propositions comme suit : si $\mathcal{T} \vdash^{cf}_{\mathcal{R}} P$ alors $|P| = 1$, sinon $|P| = 0$.

Ceci n'est malheureusement pas possible pour toutes les théories. En effet, si nous choisissons la théorie vide, alors, pour un atome A quelconque, nous

n'avons ni $\vdash^{cf}_{\mathcal{R}} A$, ni $\vdash^{cf}_{\mathcal{R}} \neg A$, et donc $|A| = |\neg A| = 0$, ce qui n'est pas du tout ce que nous voulons.

L'idée est de considérer des théories maximales dans le sens suivant :

Définition 3.2 (Théorie Complète). *Une théorie (cohérente) $\mathcal{T}$ est dite complète si pour toute proposition P :*

$$\mathcal{T}, P \vdash^{cf}_{\mathcal{R}} \quad ou \quad P \in \mathcal{T}$$

Enfin, pour des raisons qui apparaîtront plus tard, nous aurons besoin d'avoir des "témoins de Henkin", c'est à dire, à chaque fois que nous aurons une proposition existentielle $\exists x P$, nous devrons pouvoir lui trouver un *témoin* qui réalise la proposition P, c'est à dire un terme clos t tel que $\{t/x\}P$:

Définition 3.3 (Témoins de Henkin). *Soit $\mathcal{T}$ une théorie cohérente, on dit qu'elle admet des témoins de Henkin si pour toute proposition existentielle $\exists x P$ il existe un certain terme t tel que :*

$$\mathcal{T}, \exists x P \nvdash^{cf}_{\mathcal{R}} \quad implique \quad \{t/x\}P \in \mathcal{T}$$

Henkin a introduit cette notion d'une manière légèrement différente :

$$\mathcal{T} \vdash \exists x P \quad \text{implique} \quad \mathcal{T} \vdash \{t/x\}P$$

La version que nous présentons ici est en fait une version modifiée, de deux manières successives. D'abord comme nous travaillons en calcul des séquents sans coupures, nous devons considérer $\vdash^{cf}_{\mathcal{R}}$ ete non $\vdash$. Et pour cette raison, nous devons considérer, de manière identique aux définitions 3.1 et 3.2) une version "doublement niée", plus forte :

$$\mathcal{T}, \exists x P \nvdash^{cf}_{\mathcal{R}} \quad \text{implique} \quad \mathcal{T}, \{t/x\}P \nvdash^{cf}_{\mathcal{R}}$$

En second lieu, nous forçons les témoins à appartenir à $\mathcal{T}$ (de la même manière qu'une théorie complète).

Ces deux définitions ne sont pas si éloignées l'une de l'autre, en apparence (et sont équivalentes en présence de la règle de coupure). Cependant, la définition 3.3, que nous pourrions appeler "Témoins de Henkin sans coupure", permet de prouver le théorème d'élimination des coupures en utilisant la méthode même de Henkin (voir par exemple [8]). Tout ce dont nous avons besoin (dans le cadre de la logique des prédicats), est donc de ces trois définitions 3.1,3.2 et 3.3 modifiées, ainsi que du lemme de Kleene 3.2.

Le but de la section 3.4 est de définir, pour toute théorie $\mathcal{T}$ cohérente, une théorie Γ qui soit complète, cohérente et qui admette des témoins de Henkin. Ce sera notre base pour construire des modèles ensuite.

3.2.2 Lemme de Kleene et inclusion

Commençons par un résultat fondamental, qui a été prouvé pour la première fois par Kleene [27]. Nous l'étendons ici au calcul des séquents modulo un système de réécriture $\mathcal{R}$ confluent. L'intuition est la suivante : si on a une preuve π du séquent :

$$\frac{\pi}{\Gamma \vdash_{\mathcal{R}} A \vee B, \Delta}$$

alors on en a une preuve π' qui commence par une règle $\vee$-d sur la proposition $A \vee B$. Cela veut dire deux choses :

- si la règle $\vee$-d apparaît quelque part dans π (ce qui est le cas si les règles axiome, $\bot$-g et affaiblissement sont atomiques), alors on peut la permuter avec toutes les autres, et la faire migrer vers le bas. C'est le sens initial donné par Kleene à son "lemme de permutation des règles",
- on a une preuve π'' du séquent $\Gamma \vdash_{\mathcal{R}} A, B, \Delta$.

C'est plutôt la seconde approche que nous allons privilégier. Notons que dans le chapitre 9 nous aurons besoin, en plus de ce lemme de Kleene, d'informations sur la hauteur de la preuve π' (et π''). Pour l'instant, nous ne pouvons pas les avoir, car il faudrait restreindre les règles axiome, $\bot$-g et affaiblissement à être atomiques. En effet, si on a une preuve de :

$$\frac{}{A \vee B \vdash_{\mathcal{R}} A \vee B}\ \text{axiome}$$

on construira la preuve suivante :

$$\frac{\dfrac{}{A \vdash_{\mathcal{R}} A, B} \quad \dfrac{}{B \vdash_{\mathcal{R}} A, B}}{A \vee B \vdash_{\mathcal{R}} A, B}\ \vee\text{-g}$$

qui est plus grosse.

L'énoncé du lemme est compliqué par le fait que nous devons tenir compte de règles de contraction et de $\mathcal{R}$.

Lemme 3.2 (Kleene). *Soient $A_1 \equiv_{\mathcal{R}} ... \equiv_{\mathcal{R}} A_n \equiv_{\mathcal{R}} A$ des propositions.*
Si le séquent :

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

a une preuve, alors nous pouvons construire une preuve des séquents suivants :

- *dans le cas où $A = \neg P$: une preuve de $\Gamma \vdash^{cf}_{\mathcal{R}} P, \Delta$,*
- *si $A = P \vee Q$: une preuve de $\Gamma, P \vdash^{cf}_{\mathcal{R}} \Delta$ et de $\Gamma, Q \vdash^{cf}_{\mathcal{R}} \Delta$,*
- *si $A = P \wedge Q$: $\Gamma, P, Q \vdash^{cf}_{\mathcal{R}} \Delta$,*
- *si $A = P \Rightarrow Q$: des preuves de $\Gamma, Q \vdash^{cf}_{\mathcal{R}} \Delta$ et $\Gamma \vdash^{cf}_{\mathcal{R}} P, \Delta$,*
- *si $A = \exists x P$: un preuve de $\Gamma, \{c/x\}P \vdash^{cf}_{\mathcal{R}} \Delta$, avec c constante fraîche.*

Si le séquent :

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

a une preuve, alors nous pouvons construire des preuves des séquents suivants :

- *si* $A = \neg P$ *: de* $\Gamma, P \vdash^{cf}_{\mathcal{R}} \Delta$,
- *si* $A = P \wedge Q$ *: de* $\Gamma \vdash^{cf}_{\mathcal{R}} P, \Delta$ *et de* $\Gamma \vdash^{cf}_{\mathcal{R}} Q, \Delta$,
- *si* $A = P \vee Q$ *: de* $\Gamma \vdash^{cf}_{\mathcal{R}} P, Q, \Delta$,
- *si* $A = P \Rightarrow Q$ *: de* $\Gamma, P \vdash^{cf}_{\mathcal{R}} Q, \Delta$,
- *si* $A = \forall x P$ *: de* $\Gamma \vdash^{cf}_{\mathcal{R}} \{c/x\}P, \Delta$, *avec* c *constante fraîche.*

Preuve. Par induction sur la preuve π du séquent $\Gamma, A_1, ..., A_n \vdash^{cf}_{\mathcal{R}} \Delta$, en considérant la dernière règle appliquée.

Si la dernière règle appliquée a pour proposition(s) active(s) des propositions de Γ, Δ alors, nous pouvons :

1. Appliquer récursivement le lemme 3.2 à la (resp. aux) prémisse(s), et obtenir une (resp. deux) preuves sur lesquelles :
2. nous appliquons cette même règle.

Illustrons cette méthode sur un cas qui fait partie des plus difficiles, à cause de la présence de quantificateurs : si $A_1 \equiv_{\mathcal{R}} ... \equiv_{\mathcal{R}} A_n \equiv_{\mathcal{R}} \exists x P$:

- si la dernière règle est $\vee$ à gauche (sur une proposition de Γ), alors nous avons la preuve suivante :

$$\dfrac{\dfrac{\pi_1}{\Gamma, B, A_1, ..., A_n \vdash^{cf}_{\mathcal{R}} \Delta} \quad \dfrac{\pi_2}{\Gamma, C, A_1, ..., A_n \vdash^{cf}_{\mathcal{R}} \Delta}}{\Gamma, B \vee C, A_1, ..., A_n \vdash^{cf}_{\mathcal{R}} \Delta}$$

  Nous appliquons donc l'hypothèse d'induction sur les prémisses, et obtenons les deux preuves suivantes :

$$\dfrac{\pi'_1}{\Gamma, B, \{c/x\}P \vdash^{cf}_{\mathcal{R}} \Delta} \qquad \dfrac{\pi'_2}{\Gamma, C, \{c'/x\}P \vdash^{cf}_{\mathcal{R}} \Delta}$$

  Remarquons que c est fraîche dans le séquent $\Gamma, B, \{c/x\}P \vdash^{cf}_{\mathcal{R}} \Delta$, et que c' l'est dans le séquent $\Gamma, C, \{c'/x\}P \vdash^{cf}_{\mathcal{R}} \Delta$. Nous pouvons donc choisir une constante d fraîche pour les deux preuves π'_1 et π'_2 et remplacer c par d partout dans π'_1, de même remplacer c' par d partout dans π'_2.
  Ainsi nous obtenons deux preuves des séquents $\Gamma, B, \{d/x\}P \vdash^{cf}_{\mathcal{R}} \Delta$ et $\Gamma, C, \{d/x\}P \vdash^{cf}_{\mathcal{R}} \Delta$. Nous pouvons les combiner avec la même règle $\vee$ à gauche, et finalement, nous avons une preuve de ce que nous cherchions :

$$\dfrac{\dfrac{\{d/c\}\pi_1}{\Gamma, B, \{d/x\}P \vdash^{cf}_{\mathcal{R}} \Delta} \quad \dfrac{\{d/c'\}\pi_2}{\Gamma, C, \{d/x\}P \vdash^{cf}_{\mathcal{R}} \Delta}}{\Gamma, B \vee C, \{d/x\}P \vdash^{cf}_{\mathcal{R}} \Delta}$$

- Si la première règle est $\forall$-gauche sur $\forall y B \in \Gamma$, alors par hypothèse d'induction, nous avons une preuve du séquent $\Gamma, \{t/y\}B, \{c/x\}P \vdash^{cf}_{\mathcal{R}} \Delta$. c est une constante fraîche, et n'apparaît donc pas dans le terme t. Nous pouvons donc appliquer la règle $\forall$-gauche sur $\{t/x\}B$, et obtenir une preuve de $\Gamma \forall y B, \{c/x\}P \vdash^{cf}_{\mathcal{R}} \Delta$.

– Si la première règle est $\exists$-gauche si $\exists y B \in \Gamma$, toujours par hypothèse d'induction nous avons une preuve de $\Gamma, \{c/y\}B, \{d/x\}P \vdash^{cf}_{\mathcal{R}} \Delta$. c et d sont fraîches et distincte l'une de l'autre. Donc nous pouvons appliquer la règle $\exists$ à gauche sur $\{c/y\}B$.

Intéressons nous maintenant au cas où une des propositions actives est A_i pour un certain i, que nous supposerons sans perdre de généralité être 1. Distinguons selon la règle appliquée :

– Tout d'abord, si c'est une contraction, alors il nous suffit d'appliquer l'hypothèse d'induction sur la prémisse.
– Si c'est maintenant une règle d'affaiblissement à gauche, alors, soit $n = 1$ et dans ce cas, il ne reste plus aucune proposition de type $A_1, ..., A_n$, et donc nous pouvons affaiblir non pas sur la propositions A_1, mais sur la sous-formule de P désirée.
  Soit $n > 1$, et dans ce cas nous avons une preuve de $\Gamma, A_2, ..., A_n \vdash^{cf}_{\mathcal{R}} \Delta$, sur laquelle nous pouvons appliquer l'hypothèse d'induction.
– Si c'est un axiome, alors il existe une proposition $Q \equiv_{\mathcal{R}} A_1 \equiv_{\mathcal{R}} P$ appartenant à Δ. Nous pouvons "décomposer" la règle axiome, de façon à la rendre atomique, de la même manière que dans la section 1.2.4. Supposons par exemple que $P = \exists x R$, alors, nous avons la preuve suivante :

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

  Nous pouvons la modifier ainsi :

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

  ce qui nous donne la preuve voulue. Remarquons que la condition de fraîcheur des variables est vérifiée.
  Nous faisons de même pour tous les autres types de propositions. Notons que nous ne pouvons pas faire cela si la proposition P est quantifiée universellement, et se trouve à gauche du séquent, car nous aurions alors une condition de fraîcheur des variables violée. C'est la raison pour laquelle ce combinateur est absent dans l'énoncé du lemme 3.2, de même que le combinateur $\exists$ à gauche.
– Si c'est une autre règle. Supposons que A soit de la forme $B \vee C$. Alors la règle doit être $\vee$-g, car par confluence et le lemme 3.1, $P \equiv_{\mathcal{R}} A_1 \equiv_{\mathcal{R}} A$ (sur laquelle la règle de connecteur s'applique) ne peut être que de la forme $B' \vee C'$, avec $B' \equiv_{\mathcal{R}} B$ et $C' \equiv_{\mathcal{R}} C$.

  Alors nous avons des preuves des deux prémisses suivantes :

$$\Gamma, B', A_2, ..., A_n \vdash^{cf}_{\mathcal{R}} \Delta \qquad\qquad \Gamma, C', A_2, ..., A_n \vdash^{cf}_{\mathcal{R}} \Delta$$

Nous pouvons appliquer l'hypothèse d'induction, et nous obtenons ainsi des preuves des quatre séquents suivants :

$$\begin{array}{ll} \Gamma, B', C \vdash^{cf}_{\mathcal{R}} \Delta & \Gamma, C', C \vdash^{cf}_{\mathcal{R}} \Delta \\ \Gamma, B', B \vdash^{cf}_{\mathcal{R}} \Delta & \Gamma, C', B \vdash^{cf}_{\mathcal{R}} \Delta \end{array}$$

Il suffit maintenant d'appliquer la règle de contraction sur le deuxième et le troisième séquent, et nous obtenons des preuves de ce que nous désirions. Il est ici absolument fondamental de supposer la confluence, de manière à pouvoir utiliser le lemme 3.1.

- Si A est de la forme $\exists x Q$, alors, pour la même raison que précédemment, la règle est $\exists$ à gauche, avec $P \equiv_{\mathcal{R}} A_1 \equiv_{\mathcal{R}} \exists x Q$, et $P = \exists Q'$ d'après le lemme 3.1. L'application de l'hypothèse d'induction sur les prémisses nous donne une preuve du séquent $\Gamma, \{c/x\}Q', \{d/x\}Q \vdash^{cf}_{\mathcal{R}} \Delta$. c et d sont deux constantes fraîches distinctes. Ainsi, nous pouvons les remplacer toutes les deux par une même troisième constante fraîche e, et obtenir une preuve du séquent $\Gamma, \{e/x\}Q', \{e/x\}Q \vdash^{cf}_{\mathcal{R}} \Delta$, auquel nous pouvons appliquer l'hypothèse de contraction.
- Toutes les autres règles sont traitées de la même manière.

■

Remarque. Nous avons considéré tous les cas, sauf deux : ceux du quantificateur existentiel à droite, et universel à gauche. En effet, ce lemme n'est pas valide pour ces règles-ci. La preuve suivante :

$$\dfrac{\dfrac{\dfrac{}{P(c) \vdash^{cf}_{\mathcal{R}} P(c)}}{\forall x P(x) \vdash^{cf}_{\mathcal{R}} P(c)}}{\forall x P(x) \vdash^{cf}_{\mathcal{R}} \forall x P(x)}$$

ne peut en effet pas être transformée de façon à avoir une première règle $\forall$-gauche, car nous ne respecterions pas la condition de fraîcheur des variables pour la règle $\forall$-droite.

Il est intéressant de noter que cela arrive sur la règle $\forall$-g, et non pas comme on pourrait s'y attendre d'un premier abord sur la règle $\forall$-d.

Remarque. L'hypothèse de confluence est ici *absolument fondamentale*. En effet, nous nous en servons pour affirmer que les seules règles de connecteurs pouvant s'appliquer à $A_1, ..., A_n$ sont des règles concernant le connecteur principal de A.

Ainsi, dès nous aurons besoin du lemme de Kleene, nous serons dans l'obligation de supposer la confluence du système de réécriture.

Un contre-exemple au lemme de Kleene faisant intervenir un système de réécriture non confluent est le suivant. Nous considérons les deux règles de réécriture suivantes :

$$\begin{aligned} A &\rightarrow B \wedge C \\ A &\rightarrow D \vee E \end{aligned}$$

Alors la preuve suivante :

$$\frac{\overline{B, C \vdash^{cf}_{\mathcal{R}} B} \quad \overline{B, C \vdash^{cf}_{\mathcal{R}} C}}{B, C \vdash^{cf}_{\mathcal{R}} D \vee E} \wedge\text{-d}$$

ne peut pas commencer par une règle $\vee$-d.

Le lemme 3.2 est valable aussi pour le calcul des séquents avec coupures (nous ne nous en servirons pas). En effet, il suffit de tenir compte en plus du cas de la règle de coupure dans la preuve du lemme 3.2. Il en existe des preuves faisant intervenir la règle de coupure. Cependant, la preuve du lemme 3.2 a l'avantage de ne pas augmenter la hauteur des preuves (dans le cas d'un calcul des séquents avec des règles axiome, affaiblissement et $\bot$-gauche atomiques que nous appellerons par la suite calcul des séquents atomique) :

Lemme 3.3 (Kleene). *Soient $A_1 \equiv_{\mathcal{R}} ... \equiv_{\mathcal{R}} A_n \equiv_{\mathcal{R}} A$ des propositions.*

Si le séquent :

$$\Gamma, A_1, ..., A_n \vdash_{\mathcal{R}} \Delta$$

a une preuve en déduction modulo atomique, alors nous pouvons construire une preuve des séquents suivants :

- *si $A = \neg P$: une preuve de $\Gamma \vdash_{\mathcal{R}} P, \Delta$,*
- *si $A = P \vee Q$: des preuves de $\Gamma, P \vdash_{\mathcal{R}} \Delta$ et de $\Gamma, Q \vdash_{\mathcal{R}} \Delta$,*
- *si $A = P \wedge Q$: une preuve de $\Gamma, P, Q \vdash_{\mathcal{R}} \Delta$,*
- *si $A = P \Rightarrow Q$: des preuves de $\Gamma, Q \vdash_{\mathcal{R}} \Delta$ et de $\Gamma \vdash_{\mathcal{R}} P, \Delta$,*
- *si $A = \exists x P$: un preuve de $\Gamma, \{c/x\}P \vdash_{\mathcal{R}} \Delta$, avec c constante fraîche.*

Si le séquent :

$$\Gamma \vdash_{\mathcal{R}} A_1, ..., A_n, \Delta$$

a une preuve, alors nous pouvons construire une preuve des séquents suivants :

- *si $A = \neg P$: une preuve de $\Gamma, P \vdash_{\mathcal{R}} \Delta$,*
- *si $A = P \wedge Q$: des preuves de $\Gamma \vdash_{\mathcal{R}} P, \Delta$ et de $\Gamma \vdash_{\mathcal{R}} Q, \Delta$,*
- *si $A = P \vee Q$: une preuve de $\Gamma \vdash_{\mathcal{R}} P, Q, \Delta$,*
- *si $A = P \Rightarrow Q$: une preuve de $\Gamma, P \vdash_{\mathcal{R}} Q, \Delta$,*
- *si $A = \forall x P$: une preuve de $\Gamma \vdash_{\mathcal{R}} \{c/x\}P, \Delta$, avec c constante fraîche.*

De plus, si chaque A_i n'est pas atomique, la taille des preuves construites est strictement inférieure à celle de la preuve originale.

Preuve. Identique à celle du lemme 3.2. Considérons le cas supplémentaire de la règle de coupure :

– Si la première règle est la règle de coupure :

$$\dfrac{\dfrac{\vdots}{\Gamma, A_1, ..., A_n, C \vdash_{\mathcal{R}} \Delta} \quad \dfrac{\vdots}{\Gamma, A_1, ..., A_n \vdash_{\mathcal{R}} D, \Delta}\ \text{coupure}, C \equiv_{\mathcal{R}} D}{\Gamma, A_1, ..., A_n \vdash_{\mathcal{R}} \Delta}$$

nous appliquons l'hypothèse d'induction sur les prémisses, et recombinons le résultat à l'aide de la règle de coupure.

Si par hasard $C \equiv_{\mathcal{R}} P$, alors nous appliquons l'hypothèse d'induction à la preuve de la prémisse $\Gamma, A_1, ..., A_n, C \vdash_{\mathcal{R}} \Delta$, et nous obtenons directement la preuve voulue.

Et si chaque A_i n'est pas atomique, alors nous ne pouvons pas avoir ni règle d'affaiblissement sur A_i, ni axiome, ni $\bot$-gauche, car nous sommes en déduction modulo atomique. Ce qui explique que la taille de la preuve, dans ce cas, n'augmente pas. ■

Remarque. Cette dernière propriété est aussi valide dans le cas du lemme de Kleene sans coupure 3.2. Nous nous en servirons dans le chapitre 9 qui concerne la résolution modulo. Cette propriété s'avérera importante car nous ferons des preuves par induction sur la hauteur des démonstrations π, et que l'on aura besoin d'appliquer le lemme de Kleene, puis l'hypothèse d'induction.

Enfin, un lemme de saturation d'une théorie complète :

Lemme 3.4. *Soit Γ une théorie complète, cohérente, admettant des témoins de Henkin. Alors :*

– *si $A \equiv_{\mathcal{R}} B$ et $A \in \Gamma$, alors $B \in \Gamma$,*
– *si $A \vee B \in \Gamma$, $A \in \Gamma$ ou $B \in \Gamma$,*
– *si $A \wedge B \in \Gamma$, $A \in \Gamma$ et $B \in \Gamma$,*
– *si $\exists x P \in \Gamma$, il existe un terme clos t tel que $\{t/x\}P \in \Gamma$,*
– *si $\forall x P \in \Gamma$, pour tout terme clos t, $\{t/x\}P \in \Gamma$,*
– *si $P \Rightarrow Q \in \Gamma$ alors soit Q inΓ, soit $\Gamma \nvdash^{cf}_{\mathcal{R}} P$,*
– *si $\neg P \in \Gamma$ alors $\Gamma \nvdash^{cf}_{\mathcal{R}} P$,*
– *si $A \equiv_{\mathcal{R}} B$ et $\Gamma \nvdash_{\mathcal{R}} A$ alors $\Gamma \nvdash_{\mathcal{R}} B$,*
– *si $\Gamma \nvdash^{cf}_{\mathcal{R}} P \wedge Q$ alors $\Gamma \nvdash^{cf}_{\mathcal{R}} P$ ou $\Gamma \nvdash^{cf}_{\mathcal{R}} Q$,*
– *si $\Gamma \nvdash^{cf}_{\mathcal{R}} P \vee Q$ alors $\Gamma \nvdash^{cf}_{\mathcal{R}} P$ et $\Gamma \nvdash^{cf}_{\mathcal{R}} Q$,*
– *si $\Gamma \nvdash^{cf}_{\mathcal{R}} P \Rightarrow Q$ alors $\Gamma, P \nvdash^{cf}_{\mathcal{R}} Q$ et $P \in \Gamma$,*
– *si $\Gamma \nvdash^{cf}_{\mathcal{R}} \neg P$ alors $\Gamma, P \nvdash^{cf}_{\mathcal{R}}$,*
– *si $\Gamma \nvdash^{cf}_{\mathcal{R}} \exists x P$ alors pour tout terme clos t, $\Gamma \nvdash^{cf}_{\mathcal{R}} \{t/x\}P$,*
– *si $\Gamma \nvdash^{cf}_{\mathcal{R}} \forall x P$ alors il existe un terme clos t tel que $\Gamma \nvdash^{cf}_{\mathcal{R}} \{t/x\}P$.*

Preuve. Elle suit toujours le même schéma. Supposons par exemple que $\Gamma, P \Rightarrow Q \nvdash^{cf}_{\mathcal{R}} A$. Alors, nous ne pouvons pas avoir en même temps $\Gamma, Q \vdash^{cf}_{\mathcal{R}} A$ et $\Gamma \vdash^{cf}_{\mathcal{R}} P$, sinon nous pourrions appliquer la règle $\Rightarrow$-gauche et obtenir une contradiction. Finalement, en appliquant la définition d'une théorie complète,

nous obtenons $Q \in \Gamma$ ou $\Gamma \not\vdash^{cf}_{\mathcal{R}} P$.

Pour les propositions commençant par $\exists$ à gauche, nous utilisons la définition des témoins de Henkin.

Le cas le plus intéressant est celui des proposition de la forme par $\forall x P$ à droite. Nous allons aussi utiliser les témoins de Henkin.

Si pour tous les termes t on a $\Gamma \vdash^{cf}_{\mathcal{R}} \{t/x\}P$, alors on a aussi : $\Gamma, \neg\{t/x\}P \vdash^{cf}_{\mathcal{R}}$. Et donc, $\Gamma, \exists x \neg P \vdash^{cf}_{\mathcal{R}}$, car sinon, nous aurions un témoin Henkin t pour lequel $\Gamma, \neg\{t/x\}P \not\vdash^{cf}_{\mathcal{R}}$.

D'après le lemme de Kleene, appliqué deux fois, nous avons une preuve de $\Gamma \vdash^{cf}_{\mathcal{R}} \{c/x\}P$, avec c constante fraîche. C'est à dire que nous pouvons appliquer la règle $\forall$-d, qui conduit à une preuve du séquent :

$$\Gamma \vdash^{cf}_{\mathcal{R}} \forall x P$$

C'est une contradiction. ■

Remarque. Nous pouvons rapprocher les résultats de ce lemme de la propriété d'Abstract Consistency Property (parfois dite d'Analytic Consistency Property) de Smullyan [40].

À ce sujet, il est intéressant de rappeler la définition d'une semi-valuation, due à Schütte, et étendue ici à la déduction modulo :

Définition 3.4 (Semi-valuation). *Une interprétation partielle quelconque V des propositions P dans l'ensemble $\{0,1\}$ est dite* semi-valuation *lorsque :*

- *si* $P \equiv_{\mathcal{R}} Q$ *alors* $V(P) = V(Q)$
- *si* $V(\neg P) = 0$ *alors* $V(P) = 1$
- *si* $V(\neg P) = 1$ *alors* $V(P) = 0$
- *si* $V(P \vee Q) = 0$ *alors* $V(P) = V(Q) = 0$
- *si* $V(P \vee Q) = 1$ *alors* $V(P) = 1$ *ou* $V(Q) = 1$
- *si* $V(P \wedge Q) = 0$ *alors* $V(P) = 0$ *ou* $V(Q) = 0$
- *si* $V(P \wedge Q) = 1$ *alors* $V(P) = V(Q) = 1$
- *si* $V(P \Rightarrow Q) = 0$ *alors* $V(P) = 1$ *et* $V(Q) = 0$
- *si* $V(P \Rightarrow Q) = 1$ *alors* $V(P) = 0$ *ou* $V(Q) = 1$
- *si* $V(\forall x P) = 0$ *alors il existe un terme clos* t *tel que* $V\{t/x\}P = 0$
- *si* $V(\forall x P) = 1$ *alors pour tout terme clos* t, $V(\{t/x\}P) = 1$
- *si* $V(\exists x P) = 0$ *alors pour tout terme clos* t, $V(\{t/x\}P) = 0$
- *si* $V(\exists x P) = 1$ *alors il existe un terme clos* t *tel que* $V\{t/x\}P = 1$

La correspondance est frappante avec le lemme 3.4. Le lemme 3.4 nous prouve qu'une théorie Γ cohérente, complète et admettant des témoins de Henkin définit une semi-valuation :

1. si $P \in \Gamma$ alors $V(P) = 1$
2. si $\Gamma \not\vdash^{cf}_{\mathcal{R}} P$ alors $V(P) = 0$

3. rien sinon (indéterminé).

Le troisième cas est à envisager car nous considérons le calcul des séquents sans coupure, comme il est dit dans la section 3.2.1.

Nous renvoyons à la section 5.1.3 pour plus de détails sur les liens entre semi-valuation et élimination des coupures.

3.3 Déduction Modulo Intuitionniste

3.3.1 Cohérence et complétude : définitions

Dans le cas intuitionniste, il faut raffiner les notions de cohérence, complétude et celle des témoins de Henkin que nous avons vus section 3.2.

La notion de cohérence en calcul des séquents intuitionniste devient :

Définition 3.5 (A - Cohérence). *Soit A une proposition. Une théorie $\mathcal{T}$ est A-cohérente si et seulement si $\mathcal{T} \nvdash^{cf}_{\mathcal{R}} A$*

La définition 3.1 de complétude dans le cas classique est juste un cas particulier de cette définition 3.5 avec $A = \bot$, de la même manière que la A-translation de Friedman est un raffinement de la $\neg\neg$-translation.

Définition 3.6 (Théorie A-Complète). *Soit A une proposition. Une théorie (cohérente) $\mathcal{T}$ est dite A-complète si pour toute proposition P, nous avons soit :*

$$\mathcal{T}, P \vdash^{cf}_{\mathcal{R}} A \quad \textit{soit} \quad P \in \mathcal{T}$$

Nous raffinons de même la définition des témoins de Henkin :

Définition 3.7 (A-Témoins de Henkin). *Soit $\mathcal{T}$ une théorie A-cohérente, on dit qu'elle admet des A-témoins de Henkin si pour toute proposition existentielle $\exists x P$ il existe une certaine constante c telle que :*

$$\mathcal{T}, \exists x P \nvdash^{cf}_{\mathcal{R}} A \quad \textit{implique} \quad \{c/x\}P \in \mathcal{T}$$

3.3.2 Lemme de Kleene et inclusion

Nous prouvons de la même manière que dans la section classique 3.2 le lemme de Kleene, sous l'hypothèse que le système de réécriture $\mathcal{R}$ est confluent :

Lemme 3.5 (Kleene). *Soient $A_1 \equiv_{\mathcal{R}} ... \equiv_{\mathcal{R}} A_n \equiv_{\mathcal{R}} P$ des propositions. Si l'on a une preuve du séquent :*

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

alors on peut construire une preuve de :

- *si $A = P \vee Q$: $\Gamma, P \vdash^{cf}_{\mathcal{R}} R$ and $\Gamma, Q \vdash^{cf}_{\mathcal{R}} R$,*
- *si $A = P \wedge Q$: $\Gamma, P, Q \vdash^{cf}_{\mathcal{R}} R$,*

– *si* $A = \exists x P : \Gamma, \{c/x\}P \vdash^{cf}_{\mathcal{R}} R$, *avec* c *constante fraîche.*

De même, si l'on a une preuve du séquent :

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

alors on peut construire une preuve de :

– *si* $A = \neg P : \Gamma, P \vdash^{cf}_{\mathcal{R}}$,
– *si* $A = P \wedge Q : \Gamma \vdash^{cf}_{\mathcal{R}} P$ *et* $\Gamma \vdash^{cf}_{\mathcal{R}} Q$,
– *si* $A = P \Rightarrow Q : \Gamma, P \vdash^{cf}_{\mathcal{R}} Q$,
– *si* $A = \forall x P : \Gamma \vdash^{cf}_{\mathcal{R}} \{c/x\}P$, *avec* c *constante fraîche.*

Preuve. Par la même induction que dans la preuve du lemme de Kleene 3.3, en utilisant le lemme 3.1. ■

Remarque. En logique intuitionniste, le lemme de Kleene n'est plus valable pour une nombre plus important de connecteurs. Par exemple, si nous avons une preuve de $A \Rightarrow B \vdash^{cf}_{\mathcal{R}} P$, nous ne pouvons plus forcément la transformer en preuves de $\vdash^{cf}_{\mathcal{R}} B$ et de $A \vdash^{cf}_{\mathcal{R}} P$ (par exemple, si $P = A \Rightarrow B$.)

Remarque. Le lemme 3.5 précédent est de même valable pour le calcul des séquents avec coupures.

Nous avons aussi une version intuitionniste du lemme d'inclusion, qui dit que les sous-formules de formules d'une théorie A-complète sont encore dans cette théorie.

Lemme 3.6 (Inclusion). *Soit* Γ *une théorie* A*-complète,* A*-cohérente, admettant des* A*-témoins de Henkin. Alors :*

– *si* $A \vee B \in \Gamma$, *soit* $A \in \Gamma$, *soit* $B \in \Gamma$,
– *si* $A \wedge B \in \Gamma$, $A \in \Gamma$ *et* $B \in \Gamma$,
– *si* $\exists x P \in \Gamma$, *il existe un terme* t *tel que* $\{t/x\}P \in \Gamma$,
– *si* $\forall x P \in \Gamma$, *pour tout terme* t, $\{t/x\}P \in \Gamma$,
– *si* $P \Rightarrow Q \in \Gamma$ *alors soit* Q *in*Γ, *soit* $\Gamma \nvdash^{cf}_{\mathcal{R}} P$,
– *si* $\neg P \in \Gamma$ *alors* $\Gamma \nvdash^{cf}_{\mathcal{R}} P$,
– *si* $\Gamma \nvdash^{cf}_{\mathcal{R}} P \wedge Q$ *alors* $\Gamma \nvdash^{cf}_{\mathcal{R}} P$ *ou* $\Gamma \nvdash^{cf}_{\mathcal{R}} Q$,
– *si* $\Gamma \nvdash^{cf}_{\mathcal{R}} P \vee Q$ *alors* $\Gamma \nvdash^{cf}_{\mathcal{R}} P$ *et* $\Gamma \nvdash^{cf}_{\mathcal{R}} Q$,
– *si* $\Gamma \nvdash^{cf}_{\mathcal{R}} P \Rightarrow Q$ *alors* $\Gamma, P \nvdash^{cf}_{\mathcal{R}} Q$,
– *si* $\Gamma \nvdash^{cf}_{\mathcal{R}} \neg P$ *alors* $\Gamma, P \nvdash^{cf}_{\mathcal{R}}$,
– *si* $\Gamma \nvdash^{cf}_{\mathcal{R}} \exists x P$ *alors pour tout terme* t, $\Gamma \nvdash^{cf}_{\mathcal{R}} \{t/x\}P$.

Preuve. La preuve suit toujours le même schéma. Supposons par exemple que $\Gamma, P \Rightarrow Q \nvdash^{cf}_{\mathcal{R}} A$. Alors, nous ne pouvons pas avoir en même temps $\Gamma, Q \vdash^{cf}_{\mathcal{R}} A$ et $\Gamma \vdash^{cf}_{\mathcal{R}} P$, sinon nous pourrions appliquer la règle $\Rightarrow$-gauche et obtenir une contradiction. Finalement, en appliquant la définition d'une théorie A-complète, nous obtenons $Q \in \Gamma$ ou $\Gamma \nvdash^{cf}_{\mathcal{R}} P$.

Notons que pour les propositions commençant par $\exists$ à gauche, nous utilisons la définition des témoins de Henkin. ■

Toujours au sujet des théories complètes, nous avons en plus une propriété très intéressante : les théories A-cohérentes, A-complètes et admettant des A-témoins de Henkin ont les propriétés de la disjonction et du témoin existentiel (ce qui n'est pas forcément le cas quand Γ n'est pas vide) :

Lemme 3.7. *Soit A une propositions et Γ une théorie A-complète, A-cohérente, admettant des A-témoins de Henkin. Alors :*

$$\begin{aligned} \Gamma \vdash^{cf}_{\mathcal{R}} P \vee Q &\Rightarrow \Gamma \vdash^{cf}_{\mathcal{R}} P \text{ ou } \Gamma \vdash^{cf}_{\mathcal{R}} Q \\ \Gamma \vdash^{cf}_{\mathcal{R}} \exists x P &\Rightarrow \text{il existe } t \text{ clos tel que } \Gamma \vdash^{cf}_{\mathcal{R}} \{t/x\}P \end{aligned}$$

Preuve. Comme d'habitude, par induction sur la structure de la preuve, et en se servant du fait que Γ est A-complète.

- Si la dernière règle est une règle sur $P \vee Q$ ou sur $\exists x P$, alors la prémisse est ce que nous cherchions.
- Si la dernière règle est sur une proposition appartenant à Γ, qui n'est ni $\Rightarrow$-gauche ni $\neg$-gauche alors nous nous servons du lemme 3.6, et la prémisse est encore une preuve de $\Gamma \vdash^{cf}_{\mathcal{R}} P \vee Q$ (resp. de $\Gamma \vdash^{cf}_{\mathcal{R}} \exists x P$), de taille inférieure. Nous appliquons alors l'hypothèse d'induction.
- Si la dernière règle est une règle $\Rightarrow$-gauche sur une proposition $S \equiv_{\mathcal{R}} S_1 \Rightarrow S_2 \in \Gamma$, alors, nous avons la preuve suivante :

$$\dfrac{\dfrac{\pi}{\Gamma \vdash^{cf}_{\mathcal{R}} S_1} \quad \dfrac{\pi'}{\Gamma, S_2 \vdash^{cf}_{\mathcal{R}} P \vee Q}}{\Gamma \vdash^{cf}_{\mathcal{R}} P \vee Q}$$

  D'après le lemme 3.6, soit $\Gamma \nvdash^{cf}_{\mathcal{R}} S_1$ – ce qui est en contradiction avec π – soit $S_2 \in \Gamma$, et dans ce cas π' doit être vue comme une preuve de $\Gamma \vdash^{cf}_{\mathcal{R}} P \vee Q$ à laquelle nous pouvons appliquer l'hypothèse d'induction. Soit $\Gamma \nvdash^{cf}_{\mathcal{R}} S_1$, ce qui est en contradiction avec π.
- Si la dernière règle est une règle $\neg$-gauche sur une proposition $S \in \Gamma$, alors nous appliquons le même raisonnement.

■

3.4 Complétion d'une théorie

À partir d'une théorie $\mathcal{T}$ cohérente, nous allons définir une théorie $\Gamma \supset \mathcal{T}$ qui soit complète, cohérente, et admette des témoins de Henkin. Nous verrons aussi que cette procédure marche de la même manière pour les cas classiques et intuitionnistes, à condition bien sûr de considérer les définitions raffinées dans le cas intuitionniste.

Dans les chapitres suivants, il sera très important de savoir effectuer cette opération pour toute théorie $\mathcal{T}$.

Soit donc une théorie dénombrable $\mathcal{T}$ qui soit cohérente (resp. A-cohérente pour une certaine proposition A fixée tout au long de la procédure).

Considérons le langage $\mathcal{L}$ dans lequel $\mathcal{T}$ est exprimée. Il est dénombrable, au même titre que $\mathcal{T}$.

Nous rajoutons à ce langage un ensemble infini dénombrable $\mathcal{C}$ de constantes fraîches, c'est à dire des constantes qui n'appartiennent pas déjà à $\mathcal{L}$. Les constantes de $\mathcal{C}$ seront les constantes qui serviront à introduire les témoins de Henkin, comme nous allons le voir.

Soit le langage suivant : $\mathcal{L}' = \mathcal{L} \cup \mathcal{C}$. Énumérons donc de façon exhaustive les propositions de $\mathcal{L}'$:

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

Nous allons construire la théorie Γ pas à pas, en décidant au fur et à mesure si la proposition P_n doit être incluse dans Γ ou pas.

Pour ce faire, définissons une suite de théories Γ_n de la façon suivante :

- $\Gamma_0 = \mathcal{T}$
- Si Γ_n, P_n est cohérente : $\Gamma_n, P_n \nvdash^{cf}_{\mathcal{R}}$ (resp. A-cohérente : $\Gamma_n, P_n \nvdash^{cf}_{\mathcal{R}} A$), alors :
  - Si P_n n'est pas de la forme $\exists x Q$, nous posons $\Gamma_{n+1} = \Gamma_n \cup \{P_n\}$
  - Si P_n est de la forme $\exists x Q$, soit $c \in \mathcal{C}$ une constante qui n'apparaît pas dans $P_1, ..., P_n$. Par hypothèse elle n'apparaît pas non plus dans $\mathcal{T}$ (resp. ni dans $\mathcal{T}$, ni dans A). Elle est donc fraîche, et nous avons donc : $\Gamma, P_n, \{c/x\}Q \nvdash^{cf}_{\mathcal{R}}$ (resp. $\Gamma, P_n, \{c/x\}Q \nvdash^{cf}_{\mathcal{R}} A$). Car si tel n'était pas le cas, du fait de la fraîcheur de c par rapport au séquent précédent, nous pourrions appliquer la règle $\exists$-gauche, et nous aurions une preuve de l'incohérence (resp. de l'A-incohérence) de Γ, P_n) ce qui est une contradiction.

    Nous posons donc $\Gamma_{n+1} = \Gamma_n \cup \{P_n, \{c/x\}Q\}$
- Sinon, $\Gamma_n, P_n \vdash^{cf}_{\mathcal{R}}$ (resp. $\Gamma_n, P_n \vdash^{cf}_{\mathcal{R}} A$). Nous posons donc $\Gamma_{n+1} = \Gamma_n$.

Enfin, nous définissons la théorie Γ :

$$\Gamma = \bigcup_{n \in \mathbb{N}} \Gamma_n$$

Nous devons maintenant prouver que Γ a bien les propriétés attendues :

- Γ est cohérente (resp. A-cohérente). En effet, chaque Γ_n est cohérente par construction. Si donc nous avions une preuve de $\Gamma \vdash^{cf}_{\mathcal{R}}$ (resp. $\Gamma \vdash^{cf}_{\mathcal{R}} A$), alors comme nous l'avons déjà indiqué, cette notation veut dire qu'un sous-ensemble fini $\Gamma' \subset \Gamma$ est tel que $\Gamma' \vdash^{cf}_{\mathcal{R}}$ (resp. $\Gamma' \vdash^{cf}_{\mathcal{R}} A$). Puisqu'il est fini, il existe un n tel que $\Gamma' \subset \Gamma_n$. Ainsi, nous aurions $\Gamma_n \vdash^{cf}_{\mathcal{R}}$ (resp. $\Gamma_n \vdash^{cf}_{\mathcal{R}} A$), ce qui est absurde. ■
- Γ est complète (resp. A-complète). Soit P, proposition telle que $\Gamma, P \nvdash^{cf}_{\mathcal{R}}$ (resp. $\Gamma, P \nvdash^{cf}_{\mathcal{R}} A$). Par l'énumération exhaustive ci-dessus nous savons qu'il existe un indice n tel que $P = P_n$. Comme $\Gamma_n \subset \Gamma$, nous avons donc $\Gamma_n, P \nvdash^{cf}_{\mathcal{R}}$ (resp. $\Gamma_n, P \nvdash^{cf}_{\mathcal{R}} A$), et par construction : $P_n \in \Gamma_{n+1} \subset \Gamma$. ■
- Γ admet des témoins de Henkin (resp. des A-témoins de Henkin). Nous faisons le même raisonnement que pour la propriété de complétude qui précède. ■

Enfin, il est trivial que $\mathcal{T} = \Gamma_0 \subset \Gamma$. Nous avons donc construit ce que nous voulions, et c'est de ce genre de théories dont nous allons nous occuper dans les chapitres suivants. En effet, nous allons définir des modèles pour des théories complètes, cohérentes, et admettant des témoins de Henkin.

La dernière remarque est que nous avons équivalence entre $P \in \Gamma$ et Γ, P cohérent (respectivement A-cohérent) pour toutes les théories complètes, d'après les définition 3.2 et 3.6.

Chapitre 4

Théorèmes de Skolem

Ce chapitre est indépendant des autres. Sa compréhension ne nécessite que le chapitre 1, de même que sa lecture n'est pas nécessaire pour la compréhension des chapitres suivants. Il peut donc être ignoré dans un premier temps, bien qu'il familiarise le lecteur avec les méthodes sémantiques utilisées ensuite.

Le théorème de Skolem est un résultat central en théorie de la démonstration, et cependant, extrêmement difficile à démontrer rigoureusement de manière syntaxique. De ce fait, il en existe peu de preuves justes, en logique des prédicats classique ou intuitionniste [15, 32].
Cependant, si l'on essaie de démontrer ce théorème de manière sémantique, alors la preuve devient beaucoup plus simple.
Cela va nous donner une occasion de mettre en oeuvre une première fois des méthodes sémantiques pour prouver des résultats syntaxiques, avant de commencer la partie suivante.

En voici un énoncé possible (dans sa version intuitionniste, Δ est réduit à une proposition au maximum) :

Théorème 4.1 (Skolem). *Soient Γ, Δ des multi-ensembles de propositions, $\forall x \exists y P$ une proposition, et f un symbole de fonction n'ayant pas d'occurrence dans $\Gamma, \Delta, \forall x \exists y P$. Il existe une preuve du séquent :*

$$\Gamma, \forall x \exists y P \vdash \Delta$$

si et seulement si il existe une preuve du séquent :

$$\Gamma, \forall x (\{f(x)/y\}P) \vdash \Delta$$

Ce chapitre est l'occasion d'utiliser les différentes sémantiques introduites aux chapitres 5, 6 pour démontrer d'autres propriétés que la complétude ou l'élimination des coupures.

4.1 Théorème de Skolem classique

Nous survolerons cette partie, qui peut être vue comme une introduction aux méthodes utilisées dans la partie suivante.

4.1.1 Sens direct

Le sens direct est quasiment immédiat et ne requiert aucune technicité. Supposons avoir une démonstration du séquent :

$$\frac{\pi}{\Gamma, \forall x \exists y P \vdash \Delta}$$

alors nous pouvons construire la preuve suivante :

$$\dfrac{\dfrac{\dfrac{\pi}{\Gamma, \forall x \exists y P \vdash \Delta}}{\Gamma, \forall x(\{f(x)/y\}P), \forall x \exists y P \vdash \Delta} \quad \dfrac{\dfrac{\dfrac{\dfrac{}{\Gamma, \{c/x\}\{f(x)/y\}P \vdash \{f(c)/y\}\{c/x\}P, \Delta}}{\Gamma, \{c/x\}\{f(x)/y\}P \vdash \exists y\{c/x\}P, \Delta}}{\Gamma, \forall x(\{f(x)/y\}P) \vdash \exists y\{c/x\}P, \Delta}}{\Gamma, \forall x(\{f(x)/y\}P) \vdash \forall x \exists y P, \Delta}}{\Gamma, \forall x(\{f(x)/y\}P) \vdash \Delta}\ \text{coupure}$$

Pour avoir cette démonstration, nous sommes cependant obligés d'introduire une règle de coupure. Si nous ne voulons pas nous en servir, il faudrait définir une transformation syntaxique plus compliquée, mais néanmoins plus simple que celle de la réciproque (en supposant que les propositions du type $\{t/x\}\exists y P$ ne sont pas contractées, ce que nous pourrions supposer – puisque les contractions ne sont utiles que pour les propositions quantifiées universellement à gauche et existentiellement à droite).

4.1.2 Réciproque

La réciproque n'est pas aussi simple. Comme annoncé plus haut, au lieu de prouver :

$$\Gamma, \forall x(\{f(x)/y\}P) \vdash \Delta \quad \text{implique} \quad \Gamma, \forall x \exists y P \vdash \Delta$$

nous allons prouver :

$$\Gamma, \forall x(\{f(x)/y\}P) \vDash \Delta \quad \text{implique} \quad \Gamma, \forall x \exists y P \vDash \Delta$$

C'est à dire que nous allons travailler dans l'espace sémantique plutôt que syntaxique. Ensuite, grâce aux théorèmes de correction 5.1 et de complétude 5.2 du calcul des séquents (sans règle de réécriture), nous aurons la démonstration suivante du théorème 4.1 :

$$\begin{array}{lcl} \Gamma, \forall x(\{f(x)/y\}P) \vdash \Delta & \Rightarrow & \Gamma, \forall x(\{f(x)/y\}P) \vDash \Delta \\ & \Rightarrow & \Gamma, \forall x \exists y P \vDash \Delta \\ & \Rightarrow & \Gamma, \forall x \exists y P \vdash \Delta \end{array}$$

Passons donc à la preuve du théorème de Skolem dans sa version sémantique.
Preuve. Considérons un modèle booléen $\mathcal{M}$ du langage $\mathcal{L}$ dans lequel toutes les propositions de Γ et $\forall x \exists y P$ sont valides (interprétées par 1).

Sans changer le domaine de $\mathcal{M}$, mais en étendant la fonction $\widehat{\cdot}$ pour prendre en compte un nouveau symbole, nous allons transformer $\mathcal{M}$ en modèle de toutes les propositions de $\Gamma, \forall x(\{f(x)/y\}P)$.

Tout ce que nous avons donc à faire est étendre la fonction $\widehat{\cdot}$ pour interpréter le nouveau symbole f. Nous posons :

$$\begin{array}{rcl} \widehat{f} := M & \rightarrow & M \\ a & \mapsto & b \text{ tel que } |P|_{\{a/x, b/y\}} = 1 \end{array}$$

Alors, il est trivial que $|\{f(x)/y\}P|_{\{a/x\}} = 1$. De plus, comme nous ne modifions pas la fonction $\widehat{\cdot}$ pour les autres symboles (de prédicat et de fonction), toutes les propositions de Γ restent vraies. Ainsi, $\mathcal{M}$ est un modèle de $\Gamma, \forall x(\{f(x)/y\}P)$ et puisque nous avions supposé $\Gamma, \forall x(\{f(x)/y\}P) \vDash \Delta$, c'est donc un modèle de $\bigvee \Delta$.

Nous avons donc prouvé $\Gamma, \forall x \exists y P \vDash \Delta$. ■

4.2 Théorème de Skolem intuitionniste

La démonstration du théorème de Skolem pour le calcul des séquents intuitionniste est plus difficile, d'un point de vue sémantique comme d'un point de vue syntaxique. Nous allons nous intéresser à la preuve du point de vue de la sémantique, c'est à dire prouver :

$$\Gamma, \forall x(\{f(x)/y\}P) \vDash Q \quad \text{implique} \quad \Gamma, \forall x \exists y P \vDash Q$$

puis conclure en utilisant les théorèmes 6.1 et 6.2, comme dans la section précédente.

Cependant, la tâche n'est pas aussi aisée que dans le cadre des modèles booléens. D'abord, quelle sémantique choisir ? Nous avons deux sémantiques principales à notre disposition :

- Les algèbres de Heyting,
- Les Structures de Kripke.

Et ni l'une ni l'autre ne sont adaptées à la preuve du théorème de Skolem. Nous allons le voir pour les structures de Kripke.

4.2.1 Inadaptation des Structures de Kripke

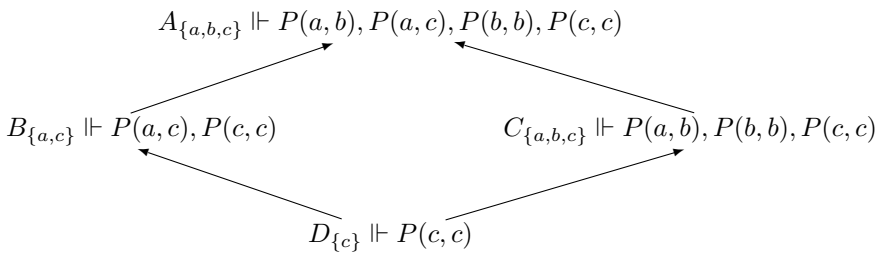
Nous pouvons essayer de copier la preuve classique de la section précédente. Soit donc une Structure de Kripke $\mathcal{K}$ et un noeud α tels que :

$$\alpha \Vdash \Gamma, \forall x \exists y P$$

Essayons de prouver que :

$$\alpha \Vdash \forall x(\{f(x)/y\}P)$$

avec les même domaines, mais une fonction $\widehat{\cdot}$ étendue. Ceci n'est pas possible, d'après le contre-exemple suivant :



Le domaine des mondes A, B, C, D est noté en indice. La flèche représente la relation $>$, et nous avons indiqué tous les atomes forcés. Alors, nous avons :

$$D \Vdash \forall x \exists y P$$

Si nous essayons de définir $\widehat{f}$, nous devons avoir :

$$\begin{aligned}
\widehat{f}(D)(c) &:= c \\
\widehat{f}(B)(a) &:= c \\
\widehat{f}(B)(c) &:= c \\
\widehat{f}(C)(a) &:= b \\
\widehat{f}(C)(b) &:= b \\
\widehat{f}(C)(c) &:= c
\end{aligned}$$

de manière à pouvoir forcer aux mondes D, B, C les atomes du type $P(x, f(x))$. Une difficulté insurmontable arrive au monde A. Compte tenu de l'obligation de monotonie de $\widehat{\cdot}$, nous devons avoir à la fois $\widehat{f}(A)(a) := a$ et $\widehat{f}(A)(a) := b$. Nous devons donc choisir l'interprétation de $f(a)$, ce que nous sommes incapables de faire.

Le problème vient du fait que dans B et C nous avons choisi deux fois la même constante, et que nous avons réunis ces deux mondes par dessus.

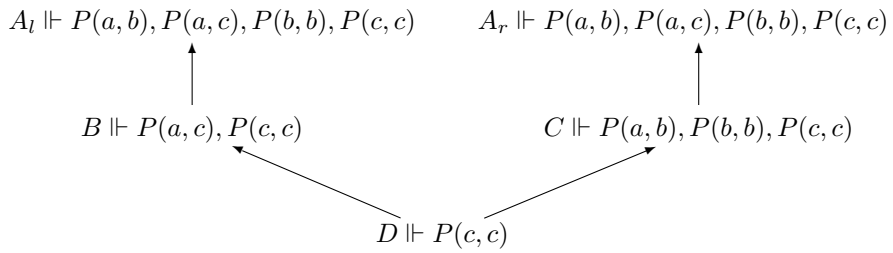
Il a donc deux sources, en voici les remèdes (chacun d'entre eux est suffisant) :

- interdire l'utilisation d'une même nouvelle constante dans deux mondes différents : mettre une condition sur les domaines.
- interdire une telle structure de mondes (le fait de les réunir alors que nous venions de les séparer) : mettre une condition sur la relation d'ordre.

Nous choisissons cette deuxième voie. Premièrement, elle est plus facile à définir, et donc beaucoup plus compréhensible. Deuxièmement, elle met en avant

le besoin d'ordonner les Structures de Kripke. Il s'agit d'introduire une structure d'arbre.

Pour introduire cette structure d'arbres, l'idée est que la réunion des deux mondes est totalement artificielle, et que nous devons considérer le monde A comme deux mondes distincts A à gauche et A à droite :



le lecteur intéressé peut vérifier que maintenant, $\widehat{f}$ est définissable sans problème.

Une chose reste cependant à prouver. Si nous utilisons la sémantique des arbres de Kripke, nous devons nous assurer que les théorèmes de correction et de complétude vis à vis du calcul des séquents intuitionniste est encore valable. Faute de quoi nous ne pourrions rien prouver du tout.

Remarque. L'échec de notre tentative de preuve de :

$$\Gamma, \forall x(\{f(x)/y\}P) \vDash Q \quad \text{implique} \quad \Gamma, \forall x \exists y P \vDash Q$$

en utilisant les structures de Kripke comme sémantique *ne signifie pas* que le résultat précédent est faux pour cette sémantique. En effet, s'il est vrai dans le calcul des séquents, alors il est vrai dans *toute* sémantique correcte et complète.

Cela veut simplement dire que la preuve "naïve" ne marche pas.

4.2.2 Les arbres de Kripke

Définition 4.1 (Arbres de Kripke). *Une Structure de Kripke $\langle K, \leq, D, \Vdash \rangle$ est un arbre si et seulement si l'ordre $\leq$ est bien fondé et si pour tous les mondes α, β, γ, lorsque $\gamma \leq \alpha$ et $\beta \leq \alpha$, nous pouvons comparer γ et β, i.e. :*

$$\beta \leq \gamma \quad ou \quad \gamma \leq \beta$$

La correction des arbres de Kripke par rapport au calcul des séquents est une conséquence immédiate du théorème de correction 6.1, puisque les arbres de Kripke sont une spécialisation des structures de Kripke. Le théorème de complétude, par contre, ne découle pas du théorème de complétude 6.2 du calcul des séquents. Nous devons le redémontrer. Au lieu de refaire la démonstration dans le cas des arbres de Kripke, nous allons prouver l'équivalence entre les deux sémantiques, en définissant une transformation conservative des Structures de Kripke vers les arbres de Kripke (dont l'idée générale a été exposée à la section précédente) :

Proposition 4.2. *$\Gamma \vDash P$ pour la sémantique des arbres de Kripke ssi $\Gamma \vDash P$ pour la sémantique des Structures de Kripke.*

Preuve. Sens direct : Soit $\langle K, \leq, D, \Vdash \rangle$ une Structure de Kripke et α tel que $\alpha \Vdash \Gamma$. Nous devons prouver $\alpha \Vdash P$. Pour cela, nous définissons l'arbre de Kripke $\langle K', \preceq, D', \Vdash \rangle$ par peignage (*unravelling* en anglais).

- K' est défini comme l'ensemble des séquences finies strictement croissantes de K : $(a_1...a_j a_{j+1}...a_n) \in K'$ ssi $a_j < a_{j+1}$ et $a_j \in K$ pour tout j.
- L'ordre $\preceq$ est : $(a_1...a_n) \preceq (a'_1...a'_m)$ ssi $n \leq m$ et $\forall i \leq n, a_i = a'_i$. ($(a_1...a_n)$ est une séquence initiale de $(a'_1...a'_m)$).
- $D'_{(a_1...a_n)} = D_{a_n}$.
- La relation de forcing est : $(a_1...a_n) \Vdash' P$ ssi $a_n \Vdash P$ et ce, pour toutes les propositions, y compris non atomiques.

Montrer que c'est un arbre est une preuve standard, notons que l'ordre $\preceq$ défini est bien fondé même si $\leq$ ne l'est pas. Il reste à vérifier les conditions sur le forcing d'une structure de Kripke (définition 1.12). Ceci est vrai grâce à notre définition de $\Vdash'$, et au fait que $\mathcal{K}$ est elle-même une structure de Kripke.

De plus, la définition de $\Vdash'$ est telle que nous avons défini un arbre de Kripke conservatif par rapport à la structure préçédente, c'est à dire que $(a_1...a_n) \Vdash' Q$ si et seulement si $a_n \Vdash Q$.

Dans cet arbre de Kripke, nous avons $(\alpha) \Vdash' \Gamma$, et donc, par hypothèse de la proposition, nous avons $(\alpha) \Vdash' P$ (où (α) représente la séquence composée du seul noeud α). Par définition de $\Vdash'$, nous avons donc $\alpha \Vdash P$. ■

Réciproque : immédiate, car les arbres de Kripke sont des Structures de Kripke. ■

Ainsi, les deux sémantiques sont équivalentes, et tous les théorèmes valables pour l'une sont valables pour l'autre. Cela signifie que dès le départ, les Structures de Kripke auraient pu être définies comme ayant une structure d'arbre.

4.2.3 Preuve du théorème de Skolem

Maintenant que nous savons que le théorème de complétude 6.2 est valable pour les arbres de Kripke, nous pouvons terminer la démonstration du théorème de Skolem de la même manière que dans le cas classique :

$$\Gamma, \forall x(\{f(x)/y\}P) \vDash Q \quad \text{implique} \quad \Gamma, \forall x \exists y P \vDash Q$$

Preuve. Soit donc un arbre de Kripke $\mathcal{K}$ et un noeud $\alpha \in K$ tels que :

$$\alpha \Vdash \Gamma, \forall x \exists y P$$

Nous devons montrer que $\alpha \Vdash Q$.

Sans changer D_β ni la relation $\Vdash$, nous allons montrer $\alpha \Vdash \forall x(\{f(x)/y\}P)$.

Il faut tenir compte d'un nouveau symbole de fonction f, et définir $\widehat{f}$ dans tous les mondes. Notons que l'interprétation de $\widehat{f}$ nous intéresse uniquement pour les mondes $\beta \geq \alpha$, donc nous considérons uniquement ces mondes, et définissons $\widehat{f}(\beta)$ par induction sur l'ordre bien fondé $\geq$.

Pour tout $a \in D_\beta$, nous définissons $\widehat{f}(\beta)(a)$:

– si a est une constante n'apparaissant dans aucun des domaines des mondes $\gamma \leq \beta$, alors :

$$\widehat{f}(\beta)(a) \quad := \quad b \text{ tel que } \beta \Vdash_{\{a/x, b/y\}} P$$

– sinon, alors parce que $\mathcal{K}$ a une structure d'arbre, nous considérons un monde $\gamma < \beta$ tel que $a \in D_\gamma$. Nous posons :

$$\widehat{f}(\beta)(a) \quad := \quad \widehat{f}(\gamma)(a)$$

Il faut vérifier que l'extension de $\widehat{\cdot}$ est bien monotone sur K. Cela se fait par induction sur $\geq$. Soient donc $\beta \geq \delta$ deux mondes, et $a \in D_\delta$.

– Soit a apparaît dans D_β et dans aucun monde en dessous. Dans ce cas, $\delta = \beta$, et nous pouvons conclure directement.
– Sinon, soit γ tel que $\widehat{f}(\beta)(a)$ ait été défini égal à $\widehat{f}(\gamma)(a)$. Si $\gamma = \delta$ le résultat est immédiat. Supposons donc en plus que $\delta < \beta$.
  Comme nous avons une structure d'arbre, soit nous avons $\delta \leq \gamma$ – dans ce cas là, nous concluons par hypothèse d'induction (sur γ) que $\widehat{f}(\gamma)(a) = \widehat{f}(\delta)(a)$ –, soit $\gamma \leq \delta$ – nous concluons aussi par hypothèse d'induction (cette fois-ci, sur δ).

Nous vérifions maintenant que pour tout $\beta \succ \alpha$, tout terme $a \in D_\beta$, $\beta \Vdash P(a, f(a))$, encore une fois par induction sur $\geq$ (en se servant de la monotonie de la relation de forcing $\Vdash$). Donc, $\alpha \Vdash \Gamma, \forall x P(x, f(x))$.

Par l'hypothèse, $\alpha \Vdash Q$, ce qui clôt la démonstration du théorème de Skolem.
□ ■

4.3 Théorème de Skolem en Déduction Modulo

Un des avantages de cette méthode est qu'elle est facilement extensible à d'autres formalismes, du moment qu'on a une sémantique qui ressemble à celle de Kripke. Par exemple, si l'on prend la déduction modulo, en supposant qu'on ait correction et complétude (pas forcément complétude forte) donc dans tous les cas des chapitres 5 et 6 en particulier, le théorème est démontré :

Théorème 4.3 (Skolem en déduction modulo). *Soit $\mathcal{R}$ un système de réécriture complet et correct pour la sémantique des structures de Kripke. Soient Γ, Δ des ensembles de propositions, $\forall x \exists y P$ une proposition, et f un symbole de fonction n'ayant aucune occurrence dans $\Gamma, \Delta, \forall x \exists y P$, ni dans $\mathcal{R}$. Il existe une preuve du séquent :*

$$\Gamma, \forall x \exists y P \vdash_{\mathcal{R}} \Delta$$

si et seulement si il existe une preuve du séquent :

$$\Gamma, \forall x(\{f(x)/y\}P) \vdash_{\mathcal{R}} \Delta$$

Preuve. Au lieu de considérer les modèles booléens et les Structures de Kripke, il suffit de considérer les modèles de $\mathcal{R}$. La démonstration ne change pas. ■

Remarque. Il est très important dans ce cas-là que f n'apparaisse pas non plus dans les règles de réécriture $\mathcal{R}$. De cette manière, nous avons libre choix pour définir $\widehat{f}$.

Théorème de Skolem pour la complétude de ENAR

Malheureusement, ce résultat n'est pas suffisant pour démontrer l'axiome de Skolem 9.1 dont nous aurons besoin au chapitre 9 suivant. En effet, nous aurons besoin du théorème dans sa version sans coupures :

Théorème 4.4 (Skolem). *Soient Γ, Δ des multi-ensembles de propositions, $\forall x \exists y P$ une proposition, et f un symbole de fonction n'ayant aucune occurrence dans $\Gamma, \Delta, \forall x \exists y P$. Le séquent :*

$$\Gamma, \forall x \exists y P \vdash^{cf}_{\mathcal{R}} \Delta$$

a une preuve si et seulement si il existe une preuve du séquent :

$$\Gamma, \forall x(\{f(x)/y\}P) \vdash^{cf}_{\mathcal{R}} \Delta$$

Sémantiquement, nous sommes incapables de prouver ce résultat sans faire appel (au moins implicitement, par le théorème de complétude forte 6.3) au théorème d'élimination des coupures. Il semblerait qu'une preuve syntaxique soit nécessaire. Cependant, une telle méthode n'est pas encore connue pour la déduction modulo.

Troisième partie

Complétude et Élimination des Coupures

Chapitre 5

Complétude du Calcul des Séquents sans coupure

Dans ce chapitre, nous nous intéressons au calcul des séquents modulo classique, tel qu'il est présenté figure 2.4 de la section 2.2.

Quand nous travaillons dans le calcul des séquents classiques, nous avons à notre disposition plusieurs méthodes de recherche de preuve, en particulier la résolution des formes clausales. Cette méthode a été étendue à la déduction modulo par G. Dowek, T. Hardin et C. Kirchner dans [16], et la résolution modulo associée est appelée ENAR (pour "Extended Narrowing And Resolution").

Or, dans le chapitre 9, il est prouvé que si l'on a une dérivation de la clause vide dans ENAR à partir de $\Gamma, \neg\Delta$, alors on a une preuve sans coupure du séquent associé $\Gamma \vdash^{cf}_{\mathcal{R}} \Delta$.

Supposons qu'on arrive à prouver que pour toute preuve de $\Gamma \vdash_{\mathcal{R}} \Delta$ on a une dérivation de la clause vide à partir de $\Gamma, \neg\Delta$ (théorème de complétude de ENAR). On obtient alors indirectement un théorème d'élimination des coupures, en passant par la résolution des formes clausales.

J. Stuber, dans [41], a prouvé la complétude de ENAR pour une certaine classe de systèmes de réécriture $\mathcal{R}$. Plus précisément, il introduit une condition d'ordre sur les règles de réécriture, et prouve la complétude de ENAR en construisant des modèles.

Nous reprenons cette idée de Stuber dans une première partie, mais cette fois-ci, sans passer par le détour ENAR, et en prouvant la complétude forte du calcul des séquents. Nous l'étendrons ensuite à d'autres conditions sur le système de réécriture $\mathcal{R}$.

5.1 Correction, Complétude, Coupure

Au chapitre 2 nous avons défini une syntaxe – le calcul des séquents modulo – et une sémantique – les modèles booléens vérifiant $\mathcal{R}$.

Nous devons maintenant relier ces deux approches de la logique modulo. C'est à dire que nous devons prouver la proposition suivante :
Les propositions vraies dans tous les modèles sont prouvables en déduction modulo. Inversement, les propositions prouvables en déduction modulo sont vraies dans tous les modèles.
Ces deux propositions représentent respectivement la complétude et la correction du calcul des séquents par rapport aux modèles booléens de $\mathcal{R}$.

5.1.1 Théorème de correction

Commençons donc par le théorème de correction :

Théorème 5.1 (Correction). *Soit $\mathcal{R}$ un ensemble de règles de réécriture confluent. Si $\Gamma \vdash_{\mathcal{R}} \Delta$ alors $\Gamma \vDash_{\mathcal{R}} \Delta$*

Remarque. Ce théorème est énoncé pour le calcul des séquents modulo avec coupures. Le même théorème s'applique aussi au calcul des séquents modulo sans coupures $\vdash^{cf}_{\mathcal{R}}$, puisque une preuve du séquent $\Gamma \vdash^{cf}_{\mathcal{R}} \Delta$ est aussi une preuve du séquent $\Gamma \vdash_{\mathcal{R}} \Delta$.

Preuve.
La démonstration s'effectue par induction sur la structure de la preuve du séquent $\Gamma \vdash_{\mathcal{R}} \Delta$, en fonction de la dernière règle utilisée. En fait, nous allons démontrer que chaque règle du calcul des séquents est admissible dans nos modèles booléens. Et donc, si la première règle est :

– axiome. La preuve est donc :

$$\frac{}{\Gamma, A \vdash_{\mathcal{R}} B, \Delta}$$

avec $A \equiv_{\mathcal{R}} B$. Comme tout modèle $\mathcal{M}$ de Γ, A doit être un modèle de $\mathcal{R}$, $\mathcal{M} \vDash_{\mathcal{R}} B$, et ainsi $\mathcal{M} \vDash_{\mathcal{R}} B \vee \bigvee \Delta$

– $\vee$ à gauche. Dans ce cas, la preuve a la forme suivante :

$$\frac{\dfrac{\pi}{\Gamma, A \vdash_{\mathcal{R}} \Delta} \quad \dfrac{\pi'}{\Gamma, B \vdash_{\mathcal{R}} \Delta}}{\Gamma, C \vdash_{\mathcal{R}} \Delta}$$

Par hypothèse d'induction, $\Gamma, A \vDash_{\mathcal{R}} \Delta$ et $\Gamma, B \vDash_{\mathcal{R}} \Delta$. Considérons un modèle $\mathcal{M} \vDash_{\mathcal{R}} \Gamma, A \vee B$. Puisqu'il valide $C \equiv A \vee B$, il doit valider soit A, soit B. Supposons que nous soyons dans le premier cas. Alors, nous utilisons la première hypothèse d'induction, pour montrer que $\mathcal{M} \vDash_{\mathcal{R}} \bigvee \Delta$. De même si nous sommes dans le deuxième cas.

– $\vee$ à droite. La preuve a la forme suivante :

$$\dfrac{\dfrac{\pi}{\Gamma \vdash_{\mathcal{R}} A, B, \Delta}}{\Gamma \vdash_{\mathcal{R}} C, \Delta}$$

Par hypothèse d'induction, tout modèle $\mathcal{M} \models_{\mathcal{R}} \Gamma$ est un modèle soit de A, soit de B, soit de $\bigvee \Delta$, ce qui nous permet de conclure.

– $\wedge$ à gauche. La preuve a donc la forme suivante :

$$\dfrac{\dfrac{\pi}{\Gamma, A, B \vdash_{\mathcal{R}} \Delta}}{\Gamma, C \vdash_{\mathcal{R}} \Delta}$$

Considérons un modèle $\mathcal{M} \models_{\mathcal{R}} \Delta, C$. Il valide donc aussi $A \wedge B$ donc A et B. Donc, par hypothèse d'induction, $\mathcal{M} \models_{\mathcal{R}} \bigvee \Delta$

– $\wedge$ à droite :

$$\dfrac{\dfrac{\pi}{\Gamma \vdash_{\mathcal{R}} A, \Delta} \quad \dfrac{\pi'}{\Gamma \vdash_{\mathcal{R}} B, \Delta}}{\Gamma \vdash_{\mathcal{R}} C, \Delta}$$

Par hypothèse d'induction, tout modèle $\mathcal{M}$ de Γ valide $A \vee \bigvee \Delta$ et $B \vee \bigvee \Delta$. Soit il valide une proposition de Δ, soit il doit valider A et B en même temps, donc $A \wedge B \equiv C$. Donc il valide $C \vee \bigvee \Delta$

– $\Rightarrow$ à droite :

$$\dfrac{\dfrac{\pi}{\Gamma, A \vdash_{\mathcal{R}} B, \Delta}}{\Gamma, \vdash_{\mathcal{R}} C, \Delta}$$

Soit $\mathcal{M}$ un modèle de Γ. Si $\mathcal{M} \not\models_{\mathcal{R}} A$, alors $\mathcal{M} \models_{\mathcal{R}} A \Rightarrow B$ et donc c'est un modèle de C.
Sinon, c'est un modèle de Γ, A et donc par hypothèse d'induction, c'est un modèle d'une des propositions de B, Δ. Si $\mathcal{M} \models B$, alors $\mathcal{M} \models_{\mathcal{R}} A \Rightarrow B$ et donc c'est un modèle de C. Sinon, c'est un modèle d'une des propositions de Δ.

Dans tous les cas, on a $\mathcal{M} \models_{\mathcal{R}} C \vee \bigvee \Delta$.

– $\Rightarrow$ à gauche :

$$\dfrac{\dfrac{\pi}{\Gamma \vdash_{\mathcal{R}} A, \Delta} \quad \dfrac{\pi'}{\Gamma, B \vdash_{\mathcal{R}} \Delta}}{\Gamma, C \vdash_{\mathcal{R}} \Delta}$$

Soit donc un modèle $\mathcal{M}$ de Γ, C. C'est aussi un modèle de Γ. Par hypothèse de récurrence sur la prémisse gauche, c'est un modèle d'au moins une des propositions parmi A, Δ. Si ce n'est pas A, alors $\mathcal{M} \models_{\mathcal{R}} \bigvee \Delta$ et nous pouvons conclure.
Si $\mathcal{M} \models_{\mathcal{R}} A$, alors puisque $\mathcal{M} \models_{\mathcal{R}} C$, nous devons avoir $\mathcal{M} \models_{\mathcal{R}} B$ (car c'est un modèle de $\mathcal{R}$). Donc, par hypothèse de récurrence sur la deuxième prémisse, nous avons $\mathcal{M} \models \bigvee \Delta$.

– $\forall$ à gauche :

$$\frac{\frac{\pi}{\Gamma, \{t/x\}P \vdash_{\mathcal{R}} \Delta}}{\Gamma, Q \vdash_{\mathcal{R}} \Delta}$$

Soit $\mathcal{M}$ un modèle de Γ, Q. Comme c'est un modèle de $\mathcal{R}$, $|\forall x P| = |Q| = 1$. Nous avons donc $|P|_{a/x} = 1$ pour tout $a \in M$. Ceci est en particulier vrai pour $a = |t|$ (t étant un terme clos), donc $\mathcal{M}$ est un modèle de $\Gamma, \{t/x\}P$. C'est donc par hypothèse d'induction un modèle de $\bigvee \Delta$.

– $\exists$ à gauche :

$$\frac{\frac{\pi}{\Gamma, \{c/x\}P \vdash_{\mathcal{R}} \Delta}}{\Gamma, Q \vdash_{\mathcal{R}} \Delta}$$

où c est une constante fraîche. Rappelons que sommes en train de prouver par récurrence sur $\Gamma \vdash_{\mathcal{R}} \Delta$ que pour tout langage $\mathcal{L}$ dans lequel Γ, Δ sont des ensembles de propositions valides, pour tout modèle $\mathcal{M}$ de ce langage, si $\mathcal{M}$ est un modèle de toutes les propositions de Γ, alors $\mathcal{M}$ est un modèle d'au moins une des propositions de Δ.

Considérons un modèle de $\mathcal{R}$ tel que $\mathcal{M} \vDash \Gamma, Q$. Par définition, il existe $a \in M$ tel que $|P|_{a/x} = 1$. Le problème est que nous ne sommes pas certains que a soit l'interprétation de quoi que ça soit dans notre langage $\mathcal{L}$, car le modèle peut contenir des valeurs non atteintes.

Il nous faut donc augmenter $\mathcal{L}$ d'un ensemble de nouvelles constantes $\mathcal{C} = \{c_b | b \in M\}$, et obtenir un langage $\mathcal{L}_M$.
Reste à définir l'interprétation de toutes ces constantes dans $\mathcal{M}$, ou plus exactement, dans une extension conservative de $\mathcal{M}$, en ce sens que les propositions déjà interprétées dans $\mathcal{M}$ ne changent pas de valeur de vérité. Nous appelons cette extension $\mathcal{M}'$. Tous les symboles de $\mathcal{L}$ sont interprétés de la même manière que dans $\mathcal{M}$, et de plus, nous posons, pour les nouvelles constantes :

$$\widehat{c_a} = a$$

c'est l'interprétation naturelle.

Premièrement, $\mathcal{M}' \vDash_{\mathcal{R}} \Gamma, \{c_a/x\}P$. Deuxièmement, c_a est une constante fraîche par rapport au séquent $\Gamma, \exists x P \vdash_{\mathcal{R}} \Delta$. Donc nous pouvons remplacer c par c_a dans la preuve du séquent $\Gamma, \{c/x\}P \vdash_{\mathcal{R}} \Delta$. Nous avons une preuve de $\Gamma, \{c_a/x\}P \vdash_{\mathcal{R}} \Delta$ et donc, par hypothèse d'induction $\mathcal{M}' \vDash_{\mathcal{R}} \bigvee \Delta$. Puisqu'aucune des nouvelles constantes n'apparaît dans Δ, et que $\mathcal{M}$ est une extension conservative de $\mathcal{M}'$, nous avons $\mathcal{M} \vDash_{\mathcal{R}} \bigvee \Delta$

– $\forall$ à droite :

$$\frac{\frac{\pi}{\Gamma \vdash_{\mathcal{R}} \{c/x\}P, \Delta}}{\Gamma \vdash_{\mathcal{R}} Q, \Delta}$$

avec c constante fraîche. Un modèle de Γ est un modèle de $\{c/x\}P \vee \bigvee \Delta$ par hypothèse d'induction. L'idée est que l'interprétation de c n'a aucune espèce d'importance, car c n'apparaît ni dans Γ, ni dans Δ.
Considérons donc tous les modèles $\mathcal{M}_a$ avec $a \in M$, qui sont définis de la façon suivante : tous les symboles sont interprétés de la même manière que dans $\mathcal{M}$ sauf c, qui est interprété par a. Puisque c est fraîche par rapport à Γ, Δ, nous pouvons affirmer que les valeurs de vérité des propositions de Γ et de Δ ne sont pas affectées, et qu'elles sont donc les mêmes que celles dans $\mathcal{M}$.

Donc, soit $\mathcal{M} \vDash_{\mathcal{R}} \bigvee \Delta$, et nous pouvons directement conclure. Soit, pour tout $a \in M$, $\mathcal{M}_a \vDash_{\mathcal{R}} \{c/x\}P$, autrement dit $|P|_{a/x} = 1$ pour tout a, *dans* $\mathcal{M}$ (car dans ce cas précis, l'interprétation dans $\mathcal{M}$ et dans $\mathcal{M}_a$ est la même, P ne comportant pas de constante c), ce qui veut dire : $\mathcal{M} \vDash_{\mathcal{R}} \forall x P$, et qui nous permet de conclure.

Ceci représente une preuve alternative du cas précédent (qui fonctionne de la même manière, de par la symétrie gauche-droite des règles du calcul des séquents classique).

– $\exists$ à droite.

$$\frac{\dfrac{\pi}{\Gamma \vdash_{\mathcal{R}} \{t/x\}P, \Delta}}{\Gamma \vdash_{\mathcal{R}} \exists x P, \Delta}$$

Soit $\mathcal{M}$ un modèle de Γ. Par hypothèse d'induction, c'est soit un modèle de Δ, soit un modèle de $\{t/x\}P$. Dans le deuxième cas nous avons $|P|_{|t|/x} = 1$, et donc $|\exists x P| = 1$. Cela nous permet de conclure.

– la règle de coupure :

$$\frac{\dfrac{\pi}{\Gamma \vdash_{\mathcal{R}} A, \Delta} \quad \dfrac{\pi'}{\Gamma, B \vdash_{\mathcal{R}} \Delta}}{\Gamma \vdash_{\mathcal{R}} \Delta}$$

avec $A \equiv_{\mathcal{R}} B$. Considérons donc un modèle $\mathcal{M}$ de Γ. Par hypothèse d'induction, c'est un modèle de $A \vee \bigvee \Delta$. Supposons que ça soit un modèle de A (l'autre cas a déjà été traité plusieurs fois). C'est donc aussi un modèle de B, et finalement, c'est un modèle de Γ, B. Par hypothèse d'induction (sur π' cette fois), c'est donc un modèle de $\bigvee \Delta$.

– contraction : pour la contraction à gauche, tout modèle de Γ, P est aussi un modèle de Γ, P, P. Nous concluons donc par hypothèse d'induction. Pour la contraction à droite, tout modèle de P, Δ est aussi un modèle de P, P, Δ.

– affaiblissement : pour l'affaiblissement à gauche, tout modèle de Γ, P est aussi un modèle de Γ. Nous concluons donc par hypothèse de récurrence. Pour l'affaiblissement à droite, si $\mathcal{M}$ est un modèle de $\bigvee \Delta$ (hypothèse de récurrence), alors c'est aussi un modèle de $P \vee \bigvee \Delta$.

– Les cas $\neg$ à gauche et à droite se traitent de la même manière que $\Rightarrow$ à gauche et à droite.

■

5.1.2 Complétude et élimination des coupures

Une fois ce théorème prouvé, nous pouvons nous atteler à la preuve du théorème inverse, le théorème de complétude :

Théorème 5.2 (Complétude). *Si* $\Gamma \vDash_{\mathcal{R}} \Delta$ *alors* $\Gamma \vdash_{\mathcal{R}} \Delta$.

La première preuve de ce théorème a été donnée par Gödel, voir par exemple [8], pour le calcul des séquents classique (sans règles de réécriture, bien sûr). Au lieu de cela, et dans l'optique d'éliminer les coupures, nous allons prouver la version forte de ce théorème, qui est la complétude du calcul des séquents sans coupures par rapport aux modèles booléens :

Théorème 5.3 (Complétude forte). *Si* $\Gamma \vDash_{\mathcal{R}} \Delta$ *alors* $\Gamma \vdash^{cf}_{\mathcal{R}} \Delta$.

Prouver ce théorème demande plus d'efforts que de prouver le précédent. Cependant, si nous faisons très attention aux définitions utilisées, alors nous pouvons suivre les lignes de la preuve du théorème 5.2.

Une difficulté supplémentaire provient du fait que nous nous plaçons en déduction modulo, et nous devrons donc tenir compte des règles de réécriture. Néanmoins, cela n'altère pas l'essence de la preuve, qui reste la même que celle qu'on peut trouver dans [8].

L'idée pour prouver ce théorème est de passer par la contraposée. Il paraît en effet plus naturel d'essayer de construire un contre-modèle à partir d'une assertion du type $\Gamma \nvdash^{cf}_{\mathcal{R}} \Delta$. Nous nous efforcerons donc de prouver le théorème suivant :

Théorème 5.4. *Si* $\Gamma \nvdash^{cf}_{\mathcal{R}} \Delta$*, alors il existe un modèle* $\mathcal{M}$ *tel que :* $\Gamma, \neg\Delta$ *soient valides.*

Le point essentiel de la démonstration est que nous nous appuyons sur des définitions légèrement différentes. Car les définitions habituelles ne sont pas adaptées au calcul des séquents sans coupures.

Si nous faisons tant d'effort pour prouver ce théorème, c'est parce qu'il induit le théorème d'élimination des coupures. En effet, il suffit maintenant d'associer le théorème de correction 5.1 à celui de complétude forte :

Théorème 5.5 (Élimination des coupures). *Si* $\Gamma \vdash_{\mathcal{R}} \Delta$ *alors* $\Gamma \vdash^{cf}_{\mathcal{R}} \Delta$

Preuve. Par le théorème de correction (théorème 5.1), nous savons que $\Gamma \vDash_{\mathcal{R}} \Delta$. Par celui de complétude forte, nous avons donc $\Gamma \vdash^{cf}_{\mathcal{R}} \Delta$. ■

Jusqu'à maintenant, nous n'avons fait aucune hypothèse sur les règles de réécriture. Cependant ici, nous devrons supposer plus. Il est en effet connu que certains systèmes, même confluents et terminant ne possèdent pas la propriété

d'élimination des coupures [17].

Ainsi, le théorème 5.3 de complétude forte est faux dans le cas général, ce qui justifie le fait de prouver indépendamment le théorème 5.2 de complétude.

De plus, les constructions de contre-modèle dans la preuve du théorème 5.3 seront différentes selon les conditions mises sur l'ensemble $\mathcal{R}$ des règles de réécriture. Nous allons donc détailler ci-dessous plusieurs cas.

5.1.3 Semi-valuations

Rappelons brièvement la définition d'une semi-valuation :

Définition (Semi-valuation). *Une interprétation partielle quelconque V des propositions P dans l'ensemble $\{0,1\}$ est dite* semi-valuation *lorsque :*

- *si $P \equiv_{\mathcal{R}} Q$ alors $V(P) = V(Q)$*
- *si $V(\neg P) = 0$ alors $V(P) = 1$*
- *si $V(\neg P) = 1$ alors $V(P) = 0$*
- *si $V(P \vee Q) = 0$ alors $V(P) = V(Q) = 0$*
- *si $V(P \vee Q) = 1$ alors $V(P) = 1$ ou $V(Q) = 1$*
- *si $V(\forall x P) = 0$ alors il existe un terme clos t tel que $V\{t/x\}P = 0$*
- *si $V(\forall x P) = 1$ alors pour tout terme clos t, $V(\{t/x\}P) = 1$*
- *idem pour les autres connecteurs.*

Comme nous le savons déjà (section 3.2.2), une théorie complète, cohérente et admettant des témoins de Henkin définit une semi-valuation.

Comme chez Schütte, la différence avec une interprétation normale (valuation totale) est que nous avons une approche partielle (certaines propositions peuvent ne pas avoir d'interprétation). Nous devons seulement nous assurer que si nous donnons à $A \vee B$ la valeur de vérité vrai, alors soit A est vraie, soit B est vraie. On peut faire le rapprochement entre les semi-valuations et la logique tri-valuée, où les propositions sont interprétées par trois valeurs : vrai, faux, indéterminé. Nous pourrions d'ailleurs définir une tri-valuation comme suit :

1. si $P \in \Gamma$ alors $V(P) = 1$
2. si $\Gamma \not\vdash^{cf}_{\mathcal{R}} P$ alors $V(P) = 0$
3. sinon, $V(P) = 2$ (indéterminé).

Il serait relativement facile, mais pénible de vérifier que cette interprétation correspond bien à une tri-valuation à la manière de Girard. Cela se fait par induction sur la structure de P et par distinction de cas, d'une manière similaire aux démonstrations des lemmes 5.9 pour les cas 1,2 et 5.10 pour le troisième cas.

Pour continuer la comparaison avec Schütte, nous devons maintenant étendre notre théorie complète (notre semi-valuation) en un modèle (une valuation totale), de manière à avoir le théorème de complétude forte (la réciproque du théorème de correction 5.1).

Cette extension est nécessaire. On pourrait par exemple avoir l'idée de définir une sémantique à base de semi-valuations (ou de théories complètes). Cette sémantique serait bien complète (puisque, étant donné une théorie cohérente, on peut, par la complétion de la section 3.4 définir une théorie complète/une semi-valuation). Mais ce qui manquerait, c'est le théorème de correction.
Car les semi-valuation *n'admettent pas certaines règles* du calcul des séquents, et le théorème 5.1 de correction n'est plus valable. Supposons par exemple avoir une démonstration :

$$\dfrac{\dfrac{\vdots}{\Gamma, C \vdash_{\mathcal{R}} \Delta}}{\Gamma \vdash_{\mathcal{R}} \neg C, \Delta}$$

Considérons une semi-valuation, ou même une valuation partielle, qui valide Γ (de manière équivalente, une théorie complète contenant Γ). Si elle valide C, alors nous pouvons conclure par hypothèse de récurrence. Si elle ne valide pas C, alors cela ne veut pas dire pour autant que $V(\neg C) = 1$ car nous pouvons très bien avoir $V(\neg C)$ non définie.

C'est pour cette raison que nous avons besoin d'étendre une semi-valuation (une théorie complète) en un modèle des règles de réécriture qui soit en accord avec la semi-valuation (avec la théorie complète). Nous pouvons pousser plus loin l'analogie avec les semi-valuations de Schütte : tous les résultats des sections suivantes sont valables si l'on remplace la notion de "Γ, théorie complète, cohérente et admettant des témoins de Henkin" par la notion de semi-valuation V. Il faut alors aussi remplacer

$$\begin{array}{lll} P \in \Gamma & \text{par} & V(P) = 1 \\ P \notin \Gamma & \text{par} & V(P) = 0 \end{array}$$

Remarquons que l'étape difficile n'est pas la définition de la semi-valuation, c'est son extension à un modèle de $\mathcal{R}$, car nous avons des règles de réécriture. Toutes les démonstrations du théorème de complétude forte (pour différentes conditions) seront basées sur ce principe :
définir un modèle, prouver que c'est un modèle des règles de réécriture et que c'est une extension de la semi-valuation définie par l'appartenance à Γ (lemmes 5.6 et 5.9).

Nous retrouverons les semi-valuations dans le chapitre 7, où nous les utiliserons explicitement.

5.2 Conditions pour la complétude forte

5.2.1 Une condition d'ordre

Nous considérons un système de réécriture $\mathcal{R}$ vérifiant les conditions suivantes :

- il est confluent
- il est compatible avec une relation d'ordre bien fondée et possédant la propriété de la sous-formule, c'est à dire que :
  - B est une sous-formule de A, alors $A \succ B$
  - si $A \to B$ est une règle de réécriture, alors $A \succ B$

Par exemple, le système suivant vérifie cette condition :

$$\begin{aligned} A &\to \forall x B(x) \\ B(0) &\to C \wedge \neg D \\ B(S(x)) &\to C \end{aligned}$$

Les systèmes sans quantificateurs, confluents et terminant de [17] sont eux-aussi compatibles avec un tel ordre. Notre condition est donc une généralisation de celle qu'on peut trouver dans [17].

Tout d'abord, remarquons que grâce au fait que $\succ$ possède la propriété de la sous-formule, pour toutes propositions $P \to^+ Q$, nous avons $P \succ Q$. Cela est vrai pour les atomes, et se propage par induction structurelle sur P aux propositions composées, car les étapes de réécriture ne s'effectuent que sur des atomes.

Puisque $\succ$ est bien-fondé, $\mathcal{R}$ est donc un système qui termine.

Nous allons maintenant définir notre modèle, pour une théorie complète, cohérente, et admettant des témoins de Henkin.

Définition 5.1. *Soit une théorie Γ, complète, cohérente, admettant des témoins de Henkin, dans un langage $\mathcal{L}$. Nous définissons la structure $\mathcal{M}$ par*

- *$M = \{t \mid t$ terme clos de $\mathcal{L}\}$*
- *Pour tout prédicat atomique normal n-aire A :*

  Si $A(t_1, ..., t_n)$ est en forme normale, nous définissons :

$$\begin{aligned} \widehat{A}(t_1, ..., t_n) &= 1 \text{ si } A(t_1, ..., t_n) \in \Gamma \\ \widehat{A}(t_1, ..., t_n) &= 0 \text{ sinon} \end{aligned}$$

  Si $A(t_1, ..., t_n)$ n'est pas en forme normale, nous définissons :

$$\widehat{A}(t_1, ..., t_n) = |A(t_1, ..., t_n)\downarrow|$$

  où $A\downarrow$ dénote la forme normale de A.
- *si P n'est pas atomique, $|P|$ est définie comme à la définition 1.11.*

Cette définition est bien-fondée, grâce aux propriétés de sous formule et de bonne fondation de $\succ$, et grâce à la compatibilité des règles de réécriture avec un tel ordre.

Notons que comme nous n'interdisons nulle part, pour un atome (ou même une proposition quelconque) le fait de vérifier à la fois :

$$\begin{array}{rl} \Gamma, A & \vdash^{cf}_{\mathcal{R}} \\ \Gamma & \vdash^{cf}_{\mathcal{R}} \quad A \end{array}$$

nous ne pouvons plus définir $|P| = 1$ si $\Gamma \vdash^{cf}_{\mathcal{R}} A$ et 0 si $\Gamma, A \vdash^{cf}_{\mathcal{R}}$ (voir section 3.2.1)

Montrons premièrement que $\mathcal{M}$ est un modèle des règles de réécriture. Nous allons prouver le fait suivant : pour toute proposition P (y compris non atomique), nous avons $|P| = |P \downarrow|$. Nous procédons par induction sur l'ordre $\succ$.

- Si P est une proposition atomique, alors par définition, $|P| = |P \downarrow|$.
- Si P est $A \vee B$, alors nous appliquons l'hypothèse de récurrence sur A et B, et nous obtenons la suite d'égalités suivantes :

  $$|P| = |A \vee B| = |A| \tilde{\vee} |B| = |A \downarrow| \tilde{\vee} |B \downarrow| = |(A \downarrow) \vee (B \downarrow)| = |(A \vee B) \downarrow|$$

  où $\tilde{\vee}$ est l'opérateur booléen de disjonction. ($x \tilde{\vee} y = 0$ ssi $x = y = 0$). La suite d'égalités est justifiée par les arguments suivants :

  1. identité
  2. définition de $|A \vee B|$
  3. hypothèse de récurrence
  4. définition de $|A' \vee B'|$
  5. Parce que $(A \downarrow) \vee (B \downarrow) = (A \vee B) \downarrow$ (les règles de réécriture sont atomiques).
- Si P est $\exists x Q$, alors nous appliquons l'hypothèse de récurrence sur $\{t/x\}Q$, et nous obtenons la suite d'égalités suivantes :

  $$\begin{array}{rcl} |P| & = & |\exists x Q| = \tilde{\bigvee_{t \in M}} |\{t/x\}Q| = \bigvee |(\{t/x\}Q) \downarrow| = \tilde{\bigvee_{t \in M}} |(\{t/x\}(Q \downarrow)) \downarrow| \\ & = & \tilde{\bigvee_{t \in M}} |\{t/x\}(Q \downarrow)| = |\exists x (Q \downarrow)| = |(\exists x Q) \downarrow| \end{array}$$

  Avec les justifications suivantes :

  1. identité
  2. définition de $|\exists x Q|$
  3. hypothèse de récurrence ($\exists x Q \succ \{t/x\}Q$)
  4. car $\{t/x\}Q \downarrow = (\{t/x\}(Q \downarrow)) \downarrow$. Ce sont deux formes normales de la même proposition.
  5. hypothèse de récurrence (car $Q \succ Q \downarrow$).
  6. définition de $|\exists x Q'|$

7. $\exists x Q \downarrow = \exists x Q \downarrow$ (les règles de réécriture sont atomiques).

– Tous les autres cas sont identiques.

Pour terminer, comme nous avons supposé la confluence et la terminaison de notre système de réécriture, si $P \equiv_{\mathcal{R}} Q$, alors $P \downarrow = R = Q \downarrow$. Ainsi $|P| = |R| = |Q|$.

Il nous reste maintenant à prouver que $\mathcal{M}$ est un modèle de Γ, et que si Γ est P-cohérente, alors $|P| = 0$.

Ceci est simple pour les atomes normaux : c'est quasiment la définition de $\mathcal{M}$. Si $A \in \Gamma$, c'est la définition, et si $\Gamma \nvdash^{cf}_{\mathcal{R}} A$, alors $A \notin \Gamma$, et $|A| = 0$.

Il faut maintenant montrer que ce résultat s'étend à toutes les propositions. Nous devons donc montrer le résultat suivant :

Lemme 5.6.

$$Si \;\; \Gamma, P \nvdash^{cf}_{\mathcal{R}} \quad alors \quad \mathcal{M} \vDash P \tag{5.1}$$

$$Si \;\; \Gamma \quad \nvdash^{cf}_{\mathcal{R}} P \quad alors \quad \mathcal{M} \nvDash P \tag{5.2}$$

Preuve. La preuve procède par induction sur l'ordre $\succ$, qui est bien fondé.

– Si P est un atome normal, c'est la définition du modèle, comme nous l'avons vu. (Γ étant complète, si l'on a $\Gamma, A \nvdash^{cf}_{\mathcal{R}}$, alors on doit avoir $A \in \Gamma$)

– Si $P = A \vee B$, dans le cas 5.1 $\Gamma, A \vee B \nvdash^{cf}_{\mathcal{R}}$ implique :

$$\begin{cases} \Gamma, A & \nvdash^{cf}_{\mathcal{R}} \\ \quad \text{ou} & \\ \Gamma, B & \nvdash^{cf}_{\mathcal{R}} \end{cases}$$

En appliquant l'hypothèse d'induction, nous obtenons donc $|A| = 1$ ou $|B| = 1$, ce qui nous permet de conclure que $|A \vee B| = 1$.

Si au contraire nous sommes dans le cas 5.2, cela implique que :

$$\begin{cases} \Gamma & \nvdash^{cf}_{\mathcal{R}} \quad A \\ \text{et} & \\ \Gamma & \nvdash^{cf}_{\mathcal{R}} \quad B \end{cases}$$

Donc, en appliquant l'hypothèse d'induction, nous avons $|A| = |B| = |A \vee B| = 0$.

– Si P est de la forme $\neg Q$, dans le cas 5.1, nous avons $\Gamma \nvdash^{cf}_{\mathcal{R}} Q$, et nous appliquons l'hypothèse d'induction, nous obtenons $|Q| = 0$, ce qui donne $|P| = 1$.

Dans le cas 5.2, nous obtenons $\Gamma, Q \nvdash^{cf}_{\mathcal{R}}$, soit, après application de l'hypothèse d'induction $|Q| = 1$, donc $|P| = 0$.

– Si P est de la forme $\exists x Q$, et que nous sommes dans le cas 5.1, alors nous devons avoir $\{c/x\}Q \in \Gamma$ car Γ admet des témoins de Henkin. Ainsi, par hypothèse d'induction, $\mathcal{M} \vDash \{c/x\}Q$, ce qui implique que $\mathcal{M} \vDash P$.

Si nous sommes dans le cas 5.2, alors nous savons que $\Gamma \nvdash^{cf}_{\mathcal{R}} \exists x Q$. Pour un terme t quelconque, nous devons donc avoir $\Gamma \nvdash^{cf}_{\mathcal{R}} \{t/x\}Q$. Ainsi, par hypothèse d'induction $|\{t/x\}Q| = 0$ pour tout t, et $|P| = 0$.

– Si P est de la forme $\forall x Q$, et que nous sommes dans le cas 5.1, alors nous devons avoir $\Gamma, \{t/x\}Q \nvdash^{cf}_{\mathcal{R}}$ pour tout terme t (sinon, nous pourrions appliquer la règle $\forall$ à gauche et obtenir une preuve de l'incohérence de $\Gamma, \forall x Q$). Ainsi, par hypothèse d'induction, $\mathcal{M} \vDash \{t/x\}Q$ pour tout t, ce qui implique que $\mathcal{M} \vDash P$.
Si nous sommes dans le cas 5.2, alors nous savons que $\Gamma \nvdash^{cf}_{\mathcal{R}} \forall x Q$. Nous allons nous servir des témoins de Henkin. En effet, nous avons :

$$\Gamma, \exists x \neg Q \nvdash^{cf}_{\mathcal{R}} \tag{5.3}$$

Nous montrons cela par l'absurde : si $\Gamma, \exists x \neg Q \vdash^{cf}_{\mathcal{R}}$, alors par le lemme de Kleene 3.2, nous avons une preuve de $\Gamma, \neg\{c/x\}Q \vdash^{cf}_{\mathcal{R}}$ avec c constante fraîche. En appliquant encore une fois le lemme de Kleene 3.2, nous obtenons une preuve de $\Gamma \vdash^{cf}_{\mathcal{R}} \{c/x\}Q$, et nous pouvons y appliquer la règle $\forall$ à droite.
À partir de 5.3, et puisque Γ admet des témoins de Henkin, il existe c telle que $\neg\{c/x\}Q \in \Gamma$. Ainsi, $\Gamma, \neg\{c/x\}Q \nvdash^{cf}_{\mathcal{R}}$. Ce qui implique (sans lemme de Kleene cette fois-ci) :

$$\Gamma \nvdash^{cf}_{\mathcal{R}} \{c/x\}Q$$

Nous pouvons maintenant appliquer l'hypothèse d'induction, et obtenons que $|P| = |\{c/x\}Q| = 0$.
– Si P est un atome qui n'est pas normal, alors, nous en prenons la forme normale et appliquons l'hypothèse d'induction. En effet, si l'on a $\Gamma, P \nvdash^{cf}_{\mathcal{R}}$, alors on aura $\Gamma, P' \nvdash^{cf}_{\mathcal{R}}$ quand $P \equiv_{\mathcal{R}} P'$. De même, les interprétations de P et P' dans $\mathcal{M}$ seront les mêmes, puisque $\mathcal{M}$ est un modèle des règles de réécriture.
– Les autres cas se traitent de la même manière que ceux précédemment traités.$A \Rightarrow B$ peut par exemple être vu comme $\neg A \vee B$, et $A \wedge B$ est traité de la manière duale de $A \vee B$.

■

Nous pouvons maintenant prouver le théorème 5.3 pour notre condition :

Théorème 5.7. *Soit $\mathcal{R}$ un système de réécriture confluent, compatible avec un ordre bien fondé ayant la propriété de la sous-formule. Si $\Gamma \vDash_{\mathcal{R}} \Delta$ alors $\Gamma \vdash^{cf}_{\mathcal{R}} \Delta$*

Preuve. Nous faisons la preuve de la contraposée : si $\Gamma \nvdash^{cf}_{\mathcal{R}} \Delta$, alors $\Gamma, \neg\Delta \nvdash^{cf}_{\mathcal{R}}$ par le lemme de Kleene 3.2. Nous construisons donc un modèle de la façon précédente de $\Gamma, \neg\Delta$ (en complétant si besoin est cette théorie) qui est un modèle qui valide Γ et qui ne valide aucune des propositions de Δ. ■

Remarque. Une autre preuve, plus constructive, pourrait être celle-ci : soit Γ une théorie complète, cohérente et admettant des témoins de Henkin, telle que $\Gamma \vDash \Delta$. Alors c'est en particulier vrai pour le modèle de Γ que nous venons de construire. Or, le lemme 5.6, nous dit que $|P| = 1$ implique $\Gamma \vdash^{cf}_{\mathcal{R}} P$ (c'est la contraposée du cas 5.2). Ainsi, dans notre modèle universel, puisque $|\bigvee \Delta| = 1$, on a $\Gamma \vdash^{cf}_{\mathcal{R}} \bigvee \Delta$ puis $\Gamma \vdash^{cf}_{\mathcal{R}} \Delta$ (après application du lemme de Kleene).
Cette preuve n'est cependant pas constructive dans le sens où elle n'est valable

que pour des théories complètes, et le procédé de complétion n'est lui-même pas constructif.

Et enfin, nous avons le corollaire d'élimination des coupures :

Corollaire 5.8. *Soit $\mathcal{R}$ un système de réécriture compatible avec un ordre bien fondé possédant la propriété de la sous-formule.*
S'il existe une preuve du séquent :

$$\Gamma \vdash_{\mathcal{R}} \Delta$$

alors il en existe une preuve sans coupure :

$$\Gamma \vdash_{\mathcal{R}}^{cf} \Delta$$

Nous ne détaillons pas la preuve, c'est celle du théorème 5.5.

5.2.2 Une condition de positivité

Nous allons maintenant imposer une nouvelle condition portant sur les règles de réécriture. Nous supposons, outre le fait qu'il est confluent et qu'il termine, que notre système $\mathcal{R}$ vérifie la condition de positivité :

Définition 5.2. *Une règle de réécriture propositionnelle $l \to r$ est positive ssi toutes les occurrences d'atomes dans r sont positives.*

Un système de réécriture $\mathcal{R}$ est positif quand toutes ses règles propositionnelles le sont.

Par exemple, la règle :

$$A \to (B \Rightarrow C)$$

n'est pas positive, alors que les suivantes le sont :

$$\begin{array}{rcl} A & \to & (\forall x B[x]) \vee C \\ A' & \to & (\neg B') \Rightarrow C' \\ A'' & \to & B \vee C' \end{array}$$

La méthode est la même : étant donné une théorie Γ complète, cohérente, admettant des témoins de Henkin, nous allons en construire un modèle.

Définition 5.3. *Soit une théorie Γ, complète, cohérente, admettant des témoins de Henkin, dans un langage $\mathcal{L}$. Nous définissions la structure $\mathcal{M}$ par*
- *$M = \{t \mid t$ terme clos de $\mathcal{L}\}$*
- *Pour tout prédicat atomique n-aire P :*

$$\begin{array}{rcl} \widehat{P}(t_1, ..., t_n) & = & 1 \text{ si } P(t_1, ..., t_n) \in \Gamma \\ \widehat{P}(t_1, ..., t_n) & = & 0 \text{ sinon} \end{array}$$

Cette fois-ci, nous fixons aussi l'interprétation des propositions atomiques non normales : en effet, le système est positif. Nous devrions donc avoir plus de difficultés à prouver que $\mathcal{M}$ est un modèle des règles de réécriture.

Par contre, nous pouvons d'ores et déjà tenter de prouver que $\mathcal{M}$ est un modèle de Γ, de la même manière que précédemment :

Lemme 5.9.

$$Si\ \Gamma, P \nvdash^{cf}_{\mathcal{R}} \quad alors \quad \mathcal{M} \vDash P \tag{5.4}$$

$$Si\ \Gamma \nvdash^{cf}_{\mathcal{R}} P \quad alors \quad \mathcal{M} \nvDash P \tag{5.5}$$

Preuve. Nous procédons de manière absolument identique à la preuve du lemme 5.6. Nous ne détaillerons donc pas les différents cas de l'induction. Nous nous bornerons à remarquer que cette fois-ci, n'ayant plus d'ordre bien-fondé, l'induction se fait sur la structure de la proposition P, et que les cas de base comprennent les atomes non-normaux, puisque c'est ainsi que nous avons défini $\mathcal{M}$. ■

Comme déjà souligné, le point crucial est de prouver que notre modèle est un modèle des règles de réécriture. Nous en avons déjà prouvé une partie. Supposons en effet que $P \equiv_{\mathcal{R}} Q$ et que $\Gamma, P \nvdash^{cf}_{\mathcal{R}}$. Dans ce cas-là, $\Gamma, Q \nvdash^{cf}_{\mathcal{R}}$ aussi (car le système de déduction, lui, correspond bien au système de réécriture $\mathcal{R}$). Ainsi, par le lemme 5.9 précédent, dans le cas 5.4 nous obtenons $|P| = |Q| = 1$. De même, si nous sommes dans le cas 5.5, nous aurons $|P| = |Q| = 0$.

Que reste-t-il a prouver, alors ? Souvenons nous qu'il peut exister des propositions telles qu'on ait des preuves des séquents :

$$\begin{array}{ll} \Gamma, P & \vdash^{cf}_{\mathcal{R}} \\ \Gamma & \vdash^{cf}_{\mathcal{R}} \quad P \end{array}$$

et ce, même si Γ est cohérente (voir 3.2.1).

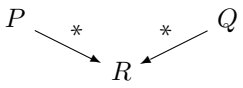
En fait, il n'existe pas de telles propositions. Mais nous ne le saurons qu'après avoir démontré le théorème d'élimination des coupures. Il est intéressant de remarquer qu'on retrouve ce problème dans *toutes* les démonstrations sémantiques d'élimination des coupures, qu'elles soient classiques ou intuitionnistes ([10, 35]), ainsi que dans les démonstrations de normalisation à base de réductibilité, où l'on ne peut pas prouver l'équivalence entre la notion de réductibilité et de normalisation forte, (voir [22]) avant d'avoir prouvé le théorème d'élimination des coupures.

Nous devons donc prouver que si P (et donc $Q \equiv_{\mathcal{R}} P$ aussi) est tel que nous avons des démonstrations de :

$$\begin{array}{ll} \Gamma, P & \vdash^{cf}_{\mathcal{R}} \\ \Gamma & \vdash^{cf}_{\mathcal{R}} \quad P \end{array}$$

alors $|P| = |Q|$.

Remarquons tout d'abord que nous pouvons nous contenter de traiter le cas où P est un atome. En effet, les règles de réécriture propositionnelles ont un membre gauche atomique, et nous avons supposé notre système de réécriture confluent. Ainsi, lorsque $P \equiv_{\mathcal{R}} Q$, nous pouvons trouver R telle que :



Nous pouvons donc nous limiter uniquement aux règles de réécriture sur les atomes de P (ou de Q).

En conclusion, le seul cas qui nous reste à considérer est le cas des atomes vérifiant :

$$\begin{array}{lll} \Gamma, A & \vdash^{cf}_{\mathcal{R}} & \\ \Gamma & \vdash^{cf}_{\mathcal{R}} & A \end{array}$$

Pour ces atomes, il reste donc à prouver que si $A \to P$, $|P| = 0$ (car $|A| = 0$ par définition).

Notons plusieurs faits. D'abord, nous ne nous sommes pas pour l'instant servis de la propriété de positivité de $\mathcal{R}$, et donc du fait que les atomes se récrivent sur des propositions positives. Et enfin, nous avons interprété tous les atomes vérifiant les conditions précédentes par la même valeur de vérité, d'après la définition 5.3.

Ceci nous amène assez naturellement au lemme suivant :

Lemme 5.10. *Si* $\Gamma, P^+ \vdash^{cf}_{\mathcal{R}}$ *et* $\Gamma \vdash^{cf}_{\mathcal{R}} P^+$ *alors* $|P^+| = 0$.
Si $\Gamma, P^- \vdash^{cf}_{\mathcal{R}}$ *et* $\Gamma \vdash^{cf}_{\mathcal{R}} P^-$ *alors* $|P^-| = 1$.

Ici, P^+ dénote une proposition ayant tout ses atomes occurant positivement, et P^- tout ses atomes occurant négativement.

La formulation de ce lemme peut sembler d'un premier abord étrange, car intuitivement, une formule positive devrait être interprétée par 1 et non pas par 0. En fait, nous aurions très bien pu prendre ce choix, dans la définition 5.3. Il aurait tout simplement fallu fixer la condition de la manière suivante, pour P, atome quelconque (donc, pas forcément en forme normale) :

$$|P| = 1 \quad \text{ssi} \quad \Gamma \vdash^{cf}_{\mathcal{R}} P$$

Ceci nous aurait donné un autre modèle, en fait un plus grand point fixe, par rapport au plus petit point fixe que nous construisons ici (voir [17]).

La preuve de ce lemme se fera par induction sur la structure de P, le cas atomique étant déjà défini grâce à notre définition de modèles. Elle fait appel très fortement au lemme de Kleene 3.2, et donc à la confluence du système de réécriture.

Le lemme de Kleene n'est pas valable pour des propositions de la forme $\forall x Q$ à gauche et $\exists x Q$ à droite, et cela posera problème dans la démonstration. Dans ces deux cas, nous le remplacerons par les lemmes 5.11 et 5.12 suivants, valables uniquement pour les théories complètes :

Lemme 5.11. *Soit Γ une théorie complète, cohérente, admettant des témoins de Henkin. Soient Γ_1, Δ_1 des ensembles quelconques de propositions.*

En posant $\Delta = \{P | \neg P \in \Gamma\}$, si nous avons une preuve π du séquent :

$$\Gamma, \Gamma_1 \vdash_{\mathcal{R}}^{cf} \Delta_1, \Delta$$

alors, nous pouvons en trouver une preuve π' qui commence par une règle portant sur une proposition de Γ_1, Δ_1. La taille de π' est inférieure ou égale à celle de π.

Remarque. Ce lemme est un lemme de Kleene "généralisé", car qu'il s'applique à tous les ensembles de propositions Γ_1, Δ_1, y compris Δ_1 vide, et Γ_1 réduit à la proposition $\forall x P$. En ce sens, il est plus fort, mais d'un autre côté il est plus faible : la première règle peut très bien être une règle de contraction, et non pas une règle $\forall$-d, comme nous l'attendrions dans un vrai lemme d'inversion de Kleene comme le lemme 3.2.

De plus, rappelons que puisque Γ est un ensemble infini de propositions, lorsque nous l'écrivons dans un séquent $\Gamma \vdash_{\mathcal{R}}^{cf} P$, nous voulons dire par là un sous-ensemble fini de propositions de Γ. En particulier, il est toujours possible d'introduire des constantes fraîches par rapport au séquent $\Gamma \vdash_{\mathcal{R}}^{cf} \Delta$.

Preuve. Par induction sur la taille de la preuve π. Considérons la dernière règle appliquée.

Si la proposition active appartient à Γ_1, Δ_1, alors il nous suffit de prendre $\pi' = \pi$.

Une règle axiome a forcément comme proposition active au moins une proposition de Γ_1, Δ_1. Si ce n'est pas le cas, alors $A \in \Gamma$ et $B \in \Delta$, avec $A \equiv_{\mathcal{R}} B$. $B \in \Delta$ veut dire que $\neg B \in \Gamma$. Ainsi, nous pourrions avoir une preuve d'incohérence de Γ :

$$\dfrac{\overline{\Gamma \vdash_{\mathcal{R}}^{cf} B}}{\Gamma, \neg B \vdash_{\mathcal{R}}^{cf}}$$

Supposons maintenant que dans la première règle de π, la proposition active appartienne à Γ ou à Δ. La règle ne peut pas être un axiome. Examinons alors les différents cas :

- Si c'est une règle structurelle (contraction ou affaiblissement), alors nous l'ignorons, car nous continuons à avoir Γ, Δ (plus exactement, comme souligné ci-dessus, des sous-ensembles finis), et nous pouvons appliquer l'hypothèse d'induction sur les prémisses.

- Si c'est une règle logique, par exemple $\vee$ à gauche sur une proposition de Γ, alors nous avons deux preuves de séquents $\Gamma, A, \Gamma_1 \vdash^{cf}_{\mathcal{R}} \Delta_1, \Delta$ et $\Gamma, B, \Gamma_1 \vdash^{cf}_{\mathcal{R}} \Delta_1, \Delta$. Mais par le lemme 3.4, nous savons que soit A, soit B appartiennent à Γ. Donc, l'une de ces deux preuves est en réalité une preuve de $\Gamma, \Gamma_1 \vdash^{cf}_{\mathcal{R}} \Delta_1, \Delta$, sur laquelle nous pouvons appliquer l'hypothèse d'induction, puisque la taille de cette preuve est plus petite.
  Si, c'est une règle $\vee$ à droite, donc sur une proposition appartenant à Δ, nous avons une preuve du séquent suivant : $\Gamma, \Gamma_1 \vdash^{cf}_{\mathcal{R}} \Delta_1, A, B, \Delta$. Nous allons maintenant montrer que Δ contient A et B. Tout d'abord, nous savons que $\neg(A \vee B) \in \Gamma$, par définition de Δ.
  D'après le lemme 3.4, nous savons donc que $\Gamma \nvdash^{cf}_{\mathcal{R}} A \vee B$, puis, que $\Gamma \nvdash^{cf}_{\mathcal{R}} A$ et $\Gamma \nvdash^{cf}_{\mathcal{R}} B$. En appliquant le lemme de Kleene 3.2, nous obtenons $\Gamma, \neg A \nvdash^{cf}_{\mathcal{R}}$, et la même chose pour $\neg B$. Ainsi, $\neg A \in \Gamma$ et $\neg B \in \Gamma$. En reprenant la définition de Δ, nous obtenons ce que nous voulions. Ainsi, nous avons en fait une preuve de $\Gamma, \Gamma_1 \vdash^{cf}_{\mathcal{R}} \Delta_1, \Delta$, qui est de hauteur inférieure. Nous pouvons lui appliquer l'hypothèse d'induction, et obtenir le résultat désiré.
- Toutes les autres règles se traitent de la même façon, y compris les règles $\exists$ à gauche et $\forall$ à droite, qui utilisent le fait que Γ admet des témoins de Henkin.

■

Remarque. Une propriété supplémentaire nous sera utile : toutes les règles de π comportant comme proposition active des propositions appartenant à Γ_1, Δ_1 sont conservées à l'identique dans π'. En particulier, le nombre de ces règles ne change pas.
La deuxième remarque est que $\neg\Delta \subset \Gamma$ par construction.

Ce lemme 5.11 se sert du calcul des séquents sans coupures. En effet, nous ne pourrions pas le prouver pour le calcul des séquents classiques, car nous ne pouvons pas analyser le cas avec des coupures comme les autres.

Dans une autre version, sans l'ensemble Δ, le lemme 5.11 prend la forme suivante :

Lemme 5.12. *Soit Γ une théorie complète, cohérente, admettant des témoins de Henkin. Si nous avons une preuve π du séquent*

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

alors nous pouvons trouver une preuve π' de ce même séquent telle que la première règle soit :

- *Soit une règle dont la propositions active appartient à Γ_1, Δ_1.*
- *Soit une règle $\neg$ à gauche sur une proposition de Γ, puis une règle axiome sur une proposition de Γ_1.*

Preuve. En appliquant le lemme précédent, nous avons une preuve π' de $\Gamma, \Gamma_1 \vdash^{cf}_{\mathcal{R}} \Delta_1, \Delta$, avec une première règle sur une des propositions de Γ_1, Δ_1. Nous prouvons le lemme en faisant une analyse par cas sur cette règle :

– C'est un axiome impliquant une proposition de Γ et de Δ_1. Nous pouvons ainsi prendre Δ égal à l'ensemble vide.
– C'est un axiome avec une proposition $B \in \Delta$ et $A \in \Gamma_1$. Alors, comme $\neg B \in \Gamma$, nous pouvons transformer π' en la preuve suivante :

$$\dfrac{\dfrac{}{\Gamma, \Gamma_1 \vdash^{cf}_{\mathcal{R}} \Delta_1, B}\ \text{axiome}}{\Gamma, \neg B, \Gamma_1 \vdash^{cf}_{\mathcal{R}} \Delta_1}\ \neg - \text{gauche}$$

C'est ce que nous voulions.
– Sinon, c'est que la proposition active ne fait pas partie de Γ, Δ. Si c'est une règle axiome, alors nous pouvons prendre des sous-ensembles vides de Γ et Δ, et nous avons une preuve de $\Gamma_1 \vdash^{cf}_{\mathcal{R}} \Delta_1$. Sinon, supposons par exemple que la règle soit $\Rightarrow$ à droite :

$$\dfrac{\dfrac{\pi}{\Gamma, \Gamma_1, A \vdash^{cf}_{\mathcal{R}} B, \Delta_1, \Delta}}{\Gamma, \Gamma_1 \vdash^{cf}_{\mathcal{R}} A \Rightarrow B, \Delta_1, \Delta}$$

Alors, nous pouvons (en rajoutant des règles $\neg$ à gauche en bas de π) obtenir une preuve de :

$$\dfrac{\dfrac{\dfrac{\pi}{\vdots}}{\Gamma, \neg\Delta, \Gamma_1, A \vdash^{cf}_{\mathcal{R}} B, \Delta_1}}{\Gamma, \Gamma_1 \vdash^{cf}_{\mathcal{R}} A \Rightarrow B, \Delta_1}$$

puisque, comme nous l'avons déjà vu, $\neg\Delta \subset \Gamma$. De plus, comme nous insérons uniquement des règles $\neg$ à gauche, aucune condition de fraîcheur des variables n'est transgressée. Donc, nous pouvons appliquer ce raisonnement à toutes les règles d'inférence, y compris $\forall$-d et $\exists$-g.

■

Remarque. Dans la preuve de lemme précédent 5.12, la taille de la preuve π' peut être plus grand que celle de π du fait de l'introduction de règles $\neg$-gauche. Par contre, le nombre de règles ayant comme proposition active des propositions issues de Γ_1, Δ_1 ne change pas.

Enfin, rappelons encore une fois que nous considérons uniquement des sous-ensembles finis $\Gamma' \subset \Gamma$, d'après la définition 1.9 et que ce ne sont pas les mêmes Γ'' dans π' et Γ' dans π. (Et c'est pour cela que nous avons besoin d'une théorie complète, cohérente, et admettant des témoins de Henkin).

Nous pouvons maintenant passer à la preuve du lemme 5.10 :

Lemme. *Si* $\Gamma, P^+ \vdash^{cf}_{\mathcal{R}}$ *et* $\Gamma \vdash^{cf}_{\mathcal{R}} P^+$ *alors* $|P^+| = 0$.
Si $\Gamma, P^- \vdash^{cf}_{\mathcal{R}}$ *et* $\Gamma \vdash^{cf}_{\mathcal{R}} P^-$ *alors* $|P^-| = 1$.

Preuve. La preuve se fait par induction sur la structure de P.

– Si P est un atome, c'est la définition du modèle (définition 5.3).
– Si $P = A \vee B$. Alors, d'après le lemme de Kleene 3.2, nous avons des preuves des séquents :

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

Plaçons nous dans le cas positif. Si $\Gamma \nvdash^{cf}_{\mathcal{R}} A^+$, alors $|A| = 0$ par le lemme 5.6. Si au contraire $\Gamma \vdash^{cf}_{\mathcal{R}} A^+$, alors par hypothèse d'induction $|A| = 0$. Nous appliquons le même raisonnement à B, et nous obtenons $|A| = |B| = |A \vee B| = 0$.
Dans le cas négatif, nous devons montrer que $|A \vee B| = 1$. Supposons donc que $|A^-| = 0$. Cela veut dire que $\Gamma \nvdash^{cf}_{\mathcal{R}} A$, sinon nous pourrions appliquer l'hypothèse d'induction sur A et obtenir $|A| = 1$. Par le lemme de Kleene 3.2, nous avons $\Gamma, \neg A \nvdash^{cf}_{\mathcal{R}}$, donc $\neg A \in \Gamma$. Ainsi, nous pouvons rajouter une règle $\neg$-gauche à la preuve de $\Gamma \vdash^{cf}_{\mathcal{R}} A, B$, et obtenir une preuve de $\Gamma \vdash^{cf}_{\mathcal{R}} B$. Nous appliquons maintenant l'hypothèse d'induction, et obtenons $|B| = 1$. Ce qui implique $|P^-| = 1$.
– Si $P = \forall x Q$, alors d'après le lemme de Kleene 3.2, pour tout terme t, nous avons une preuve π de $\Gamma \vdash^{cf}_{\mathcal{R}} \{c/x\}Q$, avec c une constante fraîche.
Dans π, nous pouvons remplacer c par n'importe quel terme t du langage (à condition parfois de renommer certaines variables fraîches). Ainsi, nous avons des preuves de séquents suivants, pour tout terme t :

$$\Gamma, \forall x Q \vdash^{cf}_{\mathcal{R}}$$
$$\Gamma \vdash^{cf}_{\mathcal{R}} \{t/x\}Q$$

Dans le cas où P est une proposition négative, il nous faut prouver que pour tous les termes clos t du langage, $|\{t/x\}Q| = 1$. Soit donc un terme t quelconque. Il y a deux choix. Soit $\Gamma, \{t/x\}Q \vdash^{cf}_{\mathcal{R}}$, dans ce cas, $|\{t/x\}Q^-| = 1$ par hypothèse d'induction. Soit $\Gamma, \{t/x\}Q \nvdash^{cf}_{\mathcal{R}}$, et nous obtenons la même conclusion grâce au lemme 5.9. Nous en déduisons donc que $|P| = 1$.

Dans le cas où P est une proposition positive, alors il nous faut prouver qu'il existe au moins un terme clos t tel que $|\{t/x\}Q| = 0$. Nous savons déjà que :

$$\Gamma \vdash^{cf}_{\mathcal{R}} \{t/x\}Q$$

pour tout terme t. Nous allons trouver par récurrence sur la preuve de $\Gamma, P \vdash^{cf}_{\mathcal{R}}$ un terme t_0 tel que $\Gamma, \{t_0/x\}Q \vdash^{cf}_{\mathcal{R}}$. Ainsi, par hypothèse d'induction, nous saurons que $|\{t_0/x\}Q| = 0$.
Nous allons raisonner sur la preuve de $\Gamma, P \vdash^{cf}_{\mathcal{R}}$, et plus précisément sur le nombre de règles appliquées à une proposition issue de P. En effet, ce nombre est limité (la preuve elle-même étant finie), disons N, et supposons en plus qu'il s'agisse du plus petit nombre N possible.

Pour les besoins de la démonstration, nous généralisons légèrement, et nous supposons avoir, un nombre N minimal et le nombre n correspondant, tels que nous ayons une preuve π du séquent $\Gamma, P_1, ..., P_n \vdash^{cf}_{\mathcal{R}}$ où apparaissent N règles sur des propositions actives issues de $P_1, ..., P_n$, avec $P_i \equiv_{\mathcal{R}} P$ pour n'importe quel i. (Une telle démonstration existe, puisque nous avons une démonstration de $\Gamma, P \vdash^{cf}_{\mathcal{R}}$).

Nous pouvons appliquer le lemme 5.12 à π.
Si la preuve transformée π' est une règle $\neg$-gauche et un axiome, alors P_i est proposition active, et cela veut dire que $\neg P \equiv_{\mathcal{R}} \neg P_i \in \Gamma$. Étant donné que $\Gamma \vdash^{cf}_{\mathcal{R}} P$, ceci n'est pas possible (on obtiendrait une preuve de l'incohérence de Γ).
Donc, la première règle est sur P. Cela peut-être une règle de contraction :

$$\dfrac{\dfrac{\pi''}{\Gamma, P_1, ..., P_{n+1} \vdash^{cf}_{\mathcal{R}}}}{\Gamma, P_1, ..., P_n \vdash^{cf}_{\mathcal{R}}}$$

Et nous avons trouvé une preuve de $\Gamma, P_1, ..., P_{n+1} \vdash^{cf}_{\mathcal{R}}$ avec $N-1$ règles sur des propositions issues de $P_1, ..., P_{n+1}$, ce qui contredit l'hypothèse.
De même, pour une règle d'affaiblissement :

$$\dfrac{\dfrac{\pi''}{\Gamma, P_1, ..., P_{n-1} \vdash^{cf}_{\mathcal{R}}}}{\Gamma, P_1, ..., P_n \vdash^{cf}_{\mathcal{R}}}$$

nous avons aussi trouvé une preuve de $\Gamma, P_1, ..., P_{n-1} \vdash^{cf}_{\mathcal{R}}$ avec $N-1$ règles sur des propositions issues de $P_1, ..., P_{n-1}$, ce qui contredit l'hypothèse.
Dans le cas où $n = 1$, alors nous avons trouvé une preuve de l'incohérence de Γ, ce qui n'est pas mieux.
La dernière possibilité (et la seule restante) est la règle $\forall$-gauche. En effet, grâce au lemme 3.1, seule cette règle peut s'appliquer :

$$\dfrac{\dfrac{\pi''}{\Gamma, P_1, ..., P_{i-1}, \{t_0/x\}Q', P_{i+1}, ..., P_n \vdash^{cf}_{\mathcal{R}}}}{\Gamma, P_1, ..., P_n \vdash^{cf}_{\mathcal{R}}}$$

avec $Q' \equiv_{\mathcal{R}} Q$.
Alors, de deux choses l'une :
- Soit $\Gamma, \{t_0/x\}Q' \nvdash^{cf}_{\mathcal{R}}$ et dans ce cas $\{t_0/x\}Q \equiv_{\mathcal{R}} \{t_0/x\}Q' \in \Gamma$, donc nous avons une preuve de $\Gamma, P_1, ..., P_{i-1}, P_{i+1}, ..., P_n \vdash^{cf}_{\mathcal{R}}$ où apparaissent $N-1$ règles sur les propositions issues de $P_1, ..., P_{i-1}, P_{i+1}, ..., P_n$, ce qui est en contradiction avec l'hypothèse que N est minimal.
- Soit $\Gamma, \{t_0/x\}Q' \vdash^{cf}_{\mathcal{R}}$, et dans ce cas $\Gamma, \{t_0/x\}Q \vdash^{cf}_{\mathcal{R}}$. Et nous avons trouvé le terme t_0 cherché.

Finalement, seul le dernier cas est possible. Nous avons forcé Γ à nous donner un témoin. Il existe donc bien t_0 tel que :

$$\begin{array}{rl} \Gamma, \{t_0/x\}Q & \vdash^{cf}_{\mathcal{R}} \\ \Gamma & \vdash^{cf}_{\mathcal{R}} \quad \{t_0/x\}Q \end{array}$$

Et nous pouvons conclure par hypothèse d'induction que $|\{t_0/x\}Q|_\sigma = 0$ et donc $|P^+|_\sigma = 0$.

– Les autres cas sont traités d'une manière identique.

■

Nous pouvons finalement prouver le résultat final :

Proposition 5.13. *$\mathcal{M}$ est un modèle des règles de réécriture.*

Preuve. Comme déjà évoqué précédemment, il nous suffit de regarder le cas atomique. Soit donc un atome $A \to P$. Nous avons trois cas de figure possible :

$$\begin{array}{rcl} \Gamma, A & \nvdash^{cf}_{\mathcal{R}} & \\ \Gamma & \nvdash^{cf}_{\mathcal{R}} & A \\ \Gamma, A \vdash^{cf}_{\mathcal{R}} & \text{et} & \Gamma \vdash^{cf}_{\mathcal{R}} A \end{array}$$

Dans le deux premiers cas, le lemme 5.9 permet de conclure que, respectivement $|A| = |P| = 1$ et $|A| = |P| = 0$. Dans le dernier cas, puisque P est positive, nous pouvons appliquer le lemme 5.10, et nous obtenons que $|P| = 0 = |A|$.

Ainsi, nous venons de prouver le théorème de complétude forte. ■

Comme d'habitude, nous avons le corollaire d'élimination des coupures :

Corollaire 5.14. *Soit $\mathcal{R}$ un ensemble de règles de réécriture positives. S'il existe une preuve du séquent :*

$$\Gamma \vdash_{\mathcal{R}} \Delta$$

alors il existe une preuve de ce même séquent sans coupure :

$$\Gamma \vdash^{cf}_{\mathcal{R}} \Delta$$

Relaxation de la condition de terminaison

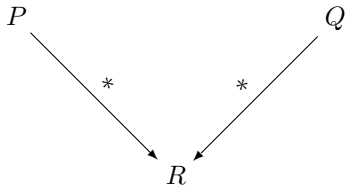
Nous avons supposé dans la preuve précédente que $\mathcal{R}$ était confluent et terminait. Le critère de terminaison n'est pas essentiel à la preuve, et le lecteur intéressé peut vérifier que nous ne nous en servons nulle part (à aucun moment nous ne parlons de forme normale, par exemple).

En revanche, le critère de confluence est indispensable. En effet, si nous considérons des systèmes de réécriture non-confluents, alors nous ne pouvons plus nous servir du lemme de Kleene 3.2, et le lemme d'inclusion 3.4 doit être revu lui aussi.

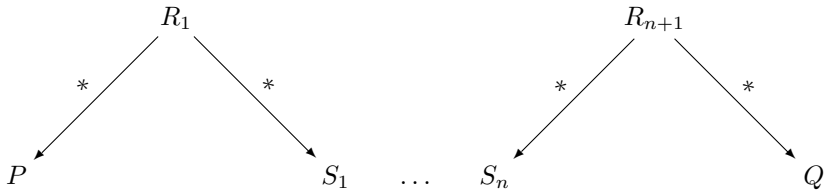
Le seul point où nous pouvons nous passer de la confluence est dans la justification du fait que lorsque l'on veut prouver que $P \equiv_{\mathcal{R}} Q$ implique $|P| = |Q|$, nous portons notre attention uniquement sur les atomes tels que :

$$\begin{array}{rl} \Gamma, A & \vdash^{cf}_{\mathcal{R}} \\ \Gamma & \vdash^{cf}_{\mathcal{R}} \quad A \end{array}$$

Car les réductions ont lieu seulement sur des atomes, et par confluence :



Or, nous pouvons nous contenter de faire une récurrence sur le nombre de "pics" de la conversion de $P \equiv_{\mathcal{R}} Q$:



L'exemple suivant montre qu'il est vital d'avoir un système de réécriture $\mathcal{R}$ positif confluent, c'est à dire qu'on ne peut pas se passer partout du lemme de Kleene. Soit $\mathcal{R}$ l'ensemble de règles de réécritures suivant :

$$\begin{array}{rcl} A & \rightarrow & B \wedge C \\ A & \rightarrow & \forall x D(x) \end{array}$$

Alors, nous ne pouvons pas prouver le séquent suivant sans la règle de coupure :

$$\frac{B, C \vdash^{cf}_{\mathcal{R}} B \wedge C, D(0) \qquad B, C, B \wedge C \vdash^{cf}_{\mathcal{R}} D(0)}{B, C \vdash_{\mathcal{R}} D(0)} \text{ coupure}$$

Ici, la règle de coupure est indispensable pour "reconstruire" la proposition $B \wedge C$, que nous pouvons réécrire seulement après. Ce contre-exemple fonctionne aussi en logique intuitionniste.

5.2.3 Réunir les deux conditions précédentes

Dans cette partie, nous allons voir comment il est possible de mélanger les deux conditions précédentes l'une à l'autre. En effet, la preuve de la section 5.2.2 semble être valide pour tous les modèles syntaxiques : il suffirait donc de rajouter des règles positives à des règles compatibles avec un ordre bien fondé,

pour obtenir un système de réécriture qui vérifie le théorème de complétude forte.

Le schéma de la preuve du théorème est un mélange des preuves des sections 5.2.1 et 5.2.2 : tout d'abord nous construisons, comme dans le section 5.2.1 un modèle des règles compatibles avec l'ordre, et deuxièmement nous prouvons, comme dans la section 5.2.2 que ce modèle est aussi un modèle des règles de réécriture positives.

Les résultats de cette section sont entièrement nouveaux, et ne figurent pas, même sous une forme simplifiée dans [17]. À l'heure actuelle, nous ne sommes pas en mesure de démontrer la normalisation de ce genre de systèmes de réécriture.

Si on peut mélanger des règles positives aux règles compatibles avec un ordre, nous ne pouvons cependant pas faire n'importe quoi. En effet, le système composé des deux règles suivantes a la propriété d'ordre pour la première règle, et celle de positivité pour la seconde. Il est même confluent :

$$\begin{aligned} A &\rightarrow \neg B \\ B &\rightarrow A \end{aligned}$$

Même si nous supposons la terminaison du système de réécriture, cela n'est plus suffisant. En effet, il est possible décomposer l'exemple que donnent Dowek et Werner [17] :

$$\begin{aligned} R \in R &\rightarrow \forall y A(y) \\ A(y) &\rightarrow (\forall x(y \in x \Rightarrow y \in R)) \Rightarrow \neg y \in R \end{aligned}$$

La condition que nous introduisons ici est une condition de normalité à droite pour les règles de réécriture positives. L'idée est que les atomes introduits par une règle de réécriture positive sont irréductibles par les autres règles (celles qui sont compatibles avec l'ordre).

Autrement dit, les règles positives viennent s'ajouter "par dessus" les autres, sans les déranger. Elles ont le droit d'interférer dans les règles qui sont compatibles avec l'ordre, à condition, bien sûr de respecter la confluence. Par contre, les règles compatibles avec l'ordre ne peuvent pas interférer dans les règles positives. Nous formalisons cela dans la définition suivante :

Définition 5.4. *Soient deux systèmes de réécriture $\mathcal{R}$ et $\mathcal{R}'$. $\mathcal{R}'$ est normal à droite pour $\mathcal{R}$ ($\mathcal{R}$-normal à droite) si, pour toute règle propositionnelle $l \rightarrow r \in \mathcal{R}'$, toutes les instances des atomes de r par des substitutions σ R-normales sont normales pour $\mathcal{R}$.*

Dans cette section, nous supposerons donc avoir un système de réécriture confluent, qui termine, et se décomposant en deux parties complémentaires et confluentes $\mathcal{R}_>$ et $\mathcal{R}_+$, telles que $\mathcal{R}_+$ soit positif et normal à droite pour $\mathcal{R}_>$. Nous utiliserons les abréviations +-normal au lieu de normal pour le système de réécriture $\mathcal{R}_+$ et >-normal au lieu de normal pour le système de réécriture $\mathcal{R}_>$

Alors, soit Γ une théorie complète, cohérente, admettant des témoins de Henkin, construisons-en un modèle qui soit un modèle des règles de réécriture.

Comme indiqué ci-dessus, nous reprenons la construction de modèle de la section 5.2.1.

Définition 5.5. *Soit une théorie Γ, complète, cohérente, admettant des témoins de Henkin, dans un langage $\mathcal{L}$. Nous définissons la structure $\mathcal{M}$ par*

- *$M = \{t | t$ terme clos de $\mathcal{L}\}$*
- *Pour tout prédicat atomique normal n-aire P.*
  Si $P(t_1, ..., t_n)$ est en forme normale pour $\mathcal{R}_>$:

$$\begin{aligned} \widehat{P}(t_1, ..., t_n) &= 1 \text{ si } P(t_1, ..., t_n) \in \Gamma \\ \widehat{P}(t_1, ..., t_n) &= 0 \text{ sinon} \end{aligned}$$

Si $P(t_1, ..., t_n)$ n'est pas en forme normale pour $\mathcal{R}_>$:

$$\widehat{P}(t_1, ..., t_n) = |P(t_1, ..., t_n) \downarrow_> |$$

où $P \downarrow_>$ représente la forme normale de P pour les règles de $\mathcal{R}_>$.

Notons que comme dans la section 5.2.2, nous définissons notre modèle sans tenir compte des règles de écriture positives $\mathcal{R}_+$, et fixons arbitrairement une valeur de vérité aux atomes non $\mathcal{R}_+$ normaux, mais $\mathcal{R}_>$ normaux. Enfin, la définition est bien fondée grâce à la bonne fondation de l'ordre $>$, et au fait qu'il possède la propriété de la sous-formule.

Nous avons effectivement construit un modèle. Reste à vérifier deux choses. Premièrement, nous devons démontrer que le modèle est un modèle de Γ. C'est l'objet du lemme suivant.

Lemme 5.15.

$$\begin{aligned} \text{Si } P \in \Gamma \quad & \text{alors} \quad |P| = 1 \\ \text{Si } \Gamma \nvdash^{cf}_{\mathcal{R}} P \quad & \text{alors} \quad |P| = 0 \end{aligned}$$

Preuve. La preuve se fait par induction sur l'ordre $>$. Voyons rapidement quelques cas, qui sont exactement les mêmes que dans la démonstration du lemme 5.6.

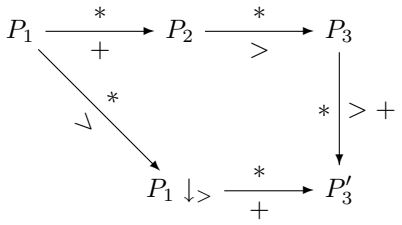
- Si P est un atome $>$-normal, alors c'est la définition 5.5.
- Si P est un atome non normal, alors $P \rightarrow_> Q$, et nous appliquons l'hypothèse d'induction à Q.
- Si $P = A \vee B$, alors, dans le premier cas, le lemme 3.4 nous dit que $A \in \Gamma$ ou $B \in \Gamma$. En appliquant l'hypothèse d'induction, nous obtenons $|A \vee B| = 1$.
- Si $P = A \vee B$ dans le deuxième cas, alors le lemme 3.4 nous dit que $\Gamma \nvdash^{cf}_{\mathcal{R}} A$ et $\Gamma \nvdash^{cf}_{\mathcal{R}} B$. Nous appliquons alors l'hypothèse d'induction.

■

Maintenant, il nous faut prouver que le modèle est un modèle des règles de réécriture. Montrons le d'abord sur les règles compatibles avec l'ordre bien fondé $>$. Cela se fait par induction sur $>$, et l'hypothèse est si $P \to_>^* Q$, alors $|P| = |Q|$:

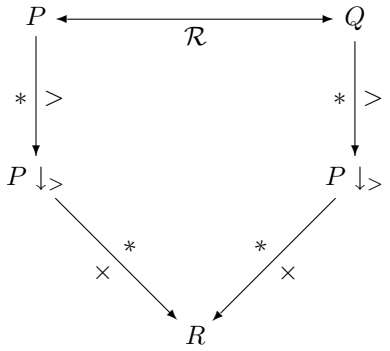
- Si la dérivation a une longueur nulle, alors c'est trivial.
- Si P est un atome non normal, alors $P \to^+ Q \to^* P\downarrow$. Nous appliquons l'hypothèse d'induction sur Q, et obtenons $|Q| = |P\downarrow|$.
- Si P n'est pas atomique, alors nous la décomposons en fonction de son connecteur principal. Par exemple, si $P = A \wedge B$, alors, puisque le système de réécriture $\mathcal{R}$ est confluent, nous avons par le lemme 3.1 $Q = A' \wedge B'$, et $A \to^* A'$, $B \to^* B'$. Nous pouvons donc appliquer l'hypothèse d'induction sur A et B.

Il nous faut ensuite le montrer pour tout l'ensemble des règles. Puisque $\mathcal{R}_+$ est normal à droite pour $\mathcal{R}_>$, si nous avons une dérivation $P_1 \to_+ P_2 \to_> P_3$, nous pouvons presque inverser ces règles et commencer par des réécritures avec des règles de $\mathcal{R}_>$ (ce n'est cependant pas la déférabilité de Soloviev). En fait, il faut se servir de la confluence. Nous avons le schéma suivant :



En effet, par confluence $P_1\downarrow_>$ et P_3 ont un réduit commun P_3', et tous les réduits de $P_1\downarrow_>$ sont normaux pour les règles de $\mathcal{R}_>$ (par normalité à droite des règles de $\mathcal{R}_+$), donc seules des règles de $\mathcal{R}_+$ sont applicables.

Ainsi, si $P \equiv_\mathcal{R} Q$, il existe R tel que :



Et nous savons déjà que :

$$\begin{aligned} |P| &= |P\downarrow_>| \\ |Q| &= |Q\downarrow_>| \end{aligned}$$

Donc, ce qu'il nous reste à montrer est que pour tout P et Q, si $P \rightarrow_+^* Q$, nous avons $|P| = |Q|$. Cela se fait exactement de la même manière que dans la section 5.2.2, nous le montrons d'abord sur les atomes. Pour cela il nous faut montrer le lemme :

Lemme 5.16. *Soit P une proposition, soit négative soit positive, et $>$-normale.*
Si $\Gamma, P^+ \vdash_{\mathcal{R}}^{cf}$ et $\Gamma \vdash_{\mathcal{R}}^{cf} P^+$ alors $|P^+| = 0$.
Si $\Gamma, P^- \vdash_{\mathcal{R}}^{cf}$ et $\Gamma \vdash_{\mathcal{R}}^{cf} P^-$ alors $|P^-| = 1$.

Preuve. Elle se fait exactement de la même manière que dans la section 5.2.2, par induction sur la taille de la preuve.

- Si P est un atome, alors c'est la définition du modèle. Et ce, parce que P est $>$-normal.
- Les autres cas se traitent de la même manière que dans la section 5.2.2. En effet, le lemme 5.12 est toujours valide (et les lemmes de Kleene aussi), même si $\mathcal{R}_+$ en soi n'est pas confluent (ce qui est important, c'est que $\mathcal{R}$ le soit.

■

Dans la preuve précédente, nous voyons qu'il est extrêmement important de supposer que $\mathcal{R}_+$ est normal à droite pour $\mathcal{R}_>$. Sinon nous ne pourrions pas conclure dans le cas atomique, ni prouver que dans le cas positif, l'on peut considérer des dérivations du type $P \rightarrow *_> R \rightarrow_+^* Q$.

Donc, si $A \rightarrow_+ P$, comme les deux systèmes de réécriture vérifient la condition 5.4, nous avons P positive et $>$-normale. Ainsi, $|A| = |P| = 1$ si $A \in \Gamma$ (par le lemme 5.15), et 0 dans le cas contraire (soit par le lemme 5.16, soit par le lemme 5.15). Nous étendons ensuite ce résultat à toutes les propositions $P \rightarrow_+ Q$, par induction sur la structure de P.

Soit maintenant $P \rightarrow^* Q$, alors, puisqu'il existe R telle que $P \rightarrow_> R \rightarrow_+ Q$, nous avons $|P| = |R|$ parce que $\mathcal{M}$ est un modèle de $\mathcal{R}_>$, et $|R| = |Q|$ par le lemme 5.16 précédent. Donc $\mathcal{M}$ est un modèle des règles de réécriture.

Nous avons donc le théorème suivant :

Théorème 5.17. *Soit $\mathcal{R}$ un système de réécriture compatible avec un ordre bien-fondé.*
Soit $\mathcal{R}_+$ un système de réécriture positif qui soit normal à droite pour $\mathcal{R}$, et tel que $\mathcal{R} \cup \mathcal{R}_+$ soit confluent.
Si $\Gamma \vDash_{\mathcal{R} \cup \mathcal{R}_+} \Delta$ alors on a une preuve (sans coupure) du séquent :

$$\Gamma \vdash_{\mathcal{R} \cup \mathcal{R}_+}^{cf} \Delta$$

La preuve est donnée ci-dessus.

Nous avons donc le théorème d'élimination des coupures :

Corollaire 5.18. *Soit $\mathcal{R}$ un système de réécriture compatible avec un ordre bien-fondé.*
Soit $\mathcal{R}_+$ un système de réécriture positif qui soit normal à droite pour $\mathcal{R}$, et tel que $\mathcal{R} \cup \mathcal{R}_+$ soit confluent.
Alors la règle de coupure est redondante dans le calcul des séquents modulo $\mathcal{R} \cup \mathcal{R}_+$.

Remarque. Notre méthode semble applicable à tous les systèmes de réécriture pour lesquels il est possible de construire un modèle syntaxique d'élimination des coupures, avec la même condition que les règles positives soient normales à droite pour le système de réécriture initial. Cependant, nous ne sommes pas en mesure de démontrer le résultat suivant :

Soit $\mathcal{R}$ un système de réécriture pour lequel on peut prouver le théorème de complétude forte vis à vis des modèles syntaxiques. Soit $\mathcal{R}_+$ un système de réécriture qui soit normal à droite pour $\mathcal{R}$, et tel que $\mathcal{R} \cup \mathcal{R}_+$ soit confluent. Si $\Gamma \vDash_{\mathcal{R}\cup\mathcal{R}_+} \Delta$ alors on a une preuve (sans coupure) du séquent :

$$\Gamma \vdash^{cf}_{\mathcal{R}\cup\mathcal{R}_+} \Delta$$

Supposons Γ complète, cohérente et admettant des témoins de Henkin pour $\mathcal{R} \cup \mathcal{R}_+$. Pour en construire un modèle $\mathcal{M}$ de $\mathcal{R}$, il faudrait le compléter vis à vis du calcul de séquents pour $\mathcal{R}$ seulement, et nous n'obtenons plus forcément une théorie cohérente pour $\mathcal{R} \cup \mathcal{R}_+$. La solution serait de considérer la semi-valuation définie par Γ et de montrer que nous pouvons l'étendre en un modèle dont le domaine *soit les mêmes termes que ceux de* Γ. Ceci semble plus fort que l'hypothèse que nous avions faite sur $\mathcal{R}$ (qui est celle de l'existence d'un modèle syntaxique).

Ensuite, le deuxième problème arrive avec les propositions atomiques A qui sont $\mathcal{R}$-normales et telles que :

$$\begin{array}{lll} \Gamma, A & \vdash^{cf}_{\mathcal{R}} & \\ \Gamma & \vdash^{cf}_{\mathcal{R}} & A \end{array}$$

Rien ne nous dit que dans le modèle $\mathcal{M}$ précédemment défini, elles sont toutes interprétées par la même valeur de vérité, ce dont nous avons besoin pour pouvoir appliquer le lemme 5.16. On peut cependant raisonnablement penser que c'est le cas, car leur interprétation ne change en rien le fait que le modèle $\mathcal{M}$ soit un modèle de $\mathcal{R}$ et soit un modèle de Γ.

Notons que ces deux conditions sont réunies pour les systèmes $\mathcal{R}$ compatibles avec un ordre bien fondé.

Il faudrait donc par exemple la condition supplémentaire suivante : la possibilité d'extension d'une semi-valuation (compatible avec $\mathcal{R}$) en un modèle de $\mathcal{R}$, dont le domaine est consittué des termes présents dans la semi-valuation et seulement ceux-ci. De plus, le modèle doit être cohérent par rapport aux atomes A dont nous avons parlé plus haut.

Remarque. L'ajout de règles positives peut être vue comme l'ajout de types inductifs. Notre résultat démontre que l'on peut rajouter des types inductifs,

sans pour autant casser les bonnes propriétés du système.

Chapitre 6

Complétude du Calcul des Séquents intuitionniste sans coupure

Nous abordons maintenant l'élimination des coupures dans le calcul des séquents intuitionniste modulo, tel qu'il est présenté dans la figure 2.3 du chapitre 3.

Comme nous allons le voir, les structures de Kripke se prêtent très bien aux preuves sémantiques d'élimination des coupures. En particulier, nous pouvons étendre relativement facilement les méthodes classiques vues dans le chapitre 5, le seul coût supplémentaire étant de considérer non pas les définitions de la section 3.2, mais celles de la section 3.3.

6.1 Théorème de correction et réciproque

6.1.1 Le théorème de correction

De même qu'au chapitre précédent, nous devons relier la syntaxe et la sémantique de la logique des prédicats. Nous commençons par le théorème de correction ci-dessous.

Théorème 6.1 (Correction). *Si* $\Gamma \vdash_{\mathcal{R}} P$ *alors* $\Gamma \vDash_{\mathcal{R}} P$

Preuve. Par induction sur la dérivation du séquent $\Gamma \vdash_{\mathcal{R}} P$, selon la dernière règle appliquée :

- Si la règle est un axiome, alors, il est clair que $Q \vDash_{\mathcal{R}} P$ quand $Q \equiv_{\mathcal{R}} P$, grâce à la définition 2.7.
- Si la règle est une règle de coupure, alors par hypothèse d'induction :

$$\Gamma \vDash_{\mathcal{R}} C \quad \text{et} \quad \Gamma, D \vDash_{\mathcal{R}} P$$

avec $C \equiv_{\mathcal{R}} D$ Ainsi, soit $\mathcal{K}$ et $\alpha \in K$ un monde qui valide Γ. Il valide aussi C par hypothèse d'induction, et D parce que $\mathcal{K}$ est un modèle de $\mathcal{R}$. Ainsi, hypothèse d'induction encore une fois, nous avons $\alpha \Vdash_{\mathcal{R}} P$.

– Si la règle est $\vee$-droite :

$$\frac{\Gamma \vdash_{\mathcal{R}} A}{\Gamma \vdash_{\mathcal{R}} P}$$

Soit $\alpha \in K$ un monde d'une structure de Kripke $\mathcal{K}$ telle que $\alpha \Vdash_{\mathcal{R}} \Gamma$. Par hypothèse d'induction, $\alpha \Vdash_{\mathcal{R}} A$, et donc $\alpha \Vdash_{\mathcal{R}} A \vee B$, par définition d'une structure de Kripke 1.12. De plus, c'est un modèle des règles de réécriture, et donc $\alpha \Vdash_{\mathcal{R}} P$.

– Si la règle est $\vee$-gauche :

$$\frac{\dfrac{\pi}{\Gamma, A \vdash_{\mathcal{R}} P} \quad \dfrac{\pi'}{\Gamma, B \vdash_{\mathcal{R}} P}}{\Gamma, Q \vdash_{\mathcal{R}} P}$$

Soit donc une structure $\mathcal{K}$ et un monde α validant Γ, Q. $\mathcal{K}$ est un modèle de $\mathcal{R}$, donc, $\alpha \Vdash_{\mathcal{R}} A \vee B$. Par définition 1.12, nous avons donc $\alpha \Vdash_{\mathcal{R}} A$ ou $\alpha \Vdash_{\mathcal{R}} B$. Dans les deux cas, nous pouvons appliquer l'hypothèse d'induction sur la prémisse de droite (resp. de gauche), et nous obtenons que $\alpha \Vdash_{\mathcal{R}} P$, ce qui est ce que nous voulions.

– Si la règle est $\Rightarrow$-droite, alors, nous avons la preuve suivante :

$$\frac{\dfrac{\pi}{\Gamma, R \vdash_{\mathcal{R}} Q}}{\Gamma \vdash_{\mathcal{R}} P}$$

Soit donc $\mathcal{K}$ un modèle de Γ, $\alpha \in K$ le monde tel que $\alpha \Vdash_{\mathcal{R}} \Gamma$. Soit $\beta \geq \alpha$ un monde tel que $\beta \Vdash_{\mathcal{R}} R$ (s'il existe). Par monotonicité de la relation de forcing (lemme 1.2), nous avons aussi $\beta \Vdash_{\mathcal{R}} \Gamma$. Ainsi, nous pouvons appliquer l'hypothèse d'induction sur π et nous obtenons $\beta \Vdash_{\mathcal{R}} Q$. Au final, nous avons bien prouvé que $\alpha \Vdash_{\mathcal{R}} R \Rightarrow Q$,

– Si la règle est $\Rightarrow$-gauche, alors, nous avons la preuve suivante :

$$\frac{\dfrac{\pi}{\Gamma, A \vdash_{\mathcal{R}} P} \quad \dfrac{\pi'}{\Gamma \vdash_{\mathcal{R}} B}}{\Gamma, Q \vdash_{\mathcal{R}} P}$$

Soit donc $\mathcal{K}$ une structure de Kripke, et $\alpha \Vdash_{\mathcal{R}} \Gamma, Q$ un noeud de K. Par hypothèse d'induction (sur π'), nous avons $\alpha \Vdash_{\mathcal{R}} B$. Ainsi, par définition d'une structure de Kripke 2.7 et 1.12, et puisque $\alpha \Vdash_{\mathcal{R}} B$, nous devons avoir $\alpha \Vdash_{\mathcal{R}} A$. Maintenant, par hypothèse d'induction sur π, nous avons donc $\alpha \Vdash_{\mathcal{R}} P$.

– Si la règle est $\forall$-droite, alors nous avons la preuve suivante :

$$\frac{\dfrac{\pi}{\Gamma \vdash_{\mathcal{R}} \{c/x\}Q}}{\Gamma \vdash_{\mathcal{R}} P}$$

avec c constante fraîche. Soit $\beta \geq \alpha$. Puisque c est fraîche, nous pouvons la remplacer par n'importe quel terme, y compris par un terme "fantôme" (intuitivement : une variable), qui s'interprète successivement par tous les éléments de D_β, et nous pouvons utiliser le lemme 1.1[1].

Par hypothèse d'induction sur π, nous avons, pour tout élément $a \in D_\beta$: $\alpha \Vdash_{\mathcal{R}\sigma} \{c_a/x\}Q$, et donc, pour tout élément $a \in D_\beta$, $\beta \Vdash_{\mathcal{R}\sigma+\langle a/x\rangle} Q$ par le lemme 1.1. Ce qui nous donne bien $\alpha \Vdash_{\mathcal{R}\sigma} P$.
Remarquons que dans la preuve précédente, nous n'avons changé ni les domaines ni l'ensemble K de la structure de Kripke $\mathcal{K}$, mais nous avons seulement changé le langage formel associé.

– Si la règle est $\forall$-gauche, alors nous avons la preuve suivante :

$$\dfrac{\dfrac{\pi}{\Gamma, \{t/x\}Q \vdash_{\mathcal{R}} R}}{\Gamma, P \vdash_{\mathcal{R}} R}$$

Soit un monde α d'une structure de Kripke quelconque, tel que $\alpha \Vdash_{\mathcal{R}\sigma} \Gamma, P$. Alors, par définition, nous savons que $\alpha \Vdash_{\mathcal{R}\sigma+\langle\sigma(t)/x\rangle} Q$, et par le lemme 1.1, $\alpha \Vdash_{\mathcal{R}\sigma} \{t/x\}Q$. Ainsi, nous pouvons appliquer l'hypothèse de récurrence pour prouver $\alpha \Vdash_{\mathcal{R}} R$

– Les autres cas se traitent de la même manière.

■

Rappelons que les résultats précédents sont valides pour tous les systèmes de réécriture, y compris non confluents.

6.1.2 La complétude forte

Comme au chapitre précédent, le théorème de correction a une réciproque, qui est le théorème de complétude :

Théorème 6.2 (Complétude). *Si $\mathcal{T} \models_{\mathcal{R}} P$, alors $\mathcal{T} \vdash_{\mathcal{R}} P$.*

Au lieu de prouver ce théorème, nous allons, pour certaines classes de règles de réécriture prouver le théorème de complétude forte :

Théorème 6.3 (Complétude forte). *Si $\mathcal{T} \models_{\mathcal{R}} P$, alors $\mathcal{T} \vdash^{cf}_{\mathcal{R}} P$.*

dont le corollaire est le théorème d'élimination des coupures. De plus, les constructions que nous verrons sont très proches de celles que nous avons vues au chapitre 5.

[1] Formellement, il faudrait procéder de la même manière que dans la preuve du théorème de correction 5.1 du chapitre 5, en rajoutant pour chaque élément $a \in D_\beta$ des constantes c_a dans un nouveau langage, de manière à atteindre tous les termes de D_β, et considérer la structure de Kripke $\mathcal{K}_\beta$ définie par $K_\beta = \{\alpha \in K | \alpha \geq \beta\}$, c'est à dire la structure de Kripke $\mathcal{K}$ tronquée. Ce problème est lié à la définition du système d'inférence avec des constantes fraîches lors de la règle $\exists$ à gauche et $\forall$ à droite. De ce que nous avons gagné en évitant l'α-conversion, nous en perdons un peu ici.

6.1.3 Les semi-structures de Kripke

Nous avons défini la notion de semi-valuation à la définition 3.4, puis nous avons vu qu'une théorie complète définissait une semi-valuation. Nous allons à présent introduire une nouvelle définition, celle des semi-structures de Kripke, qui en est l'équivalent dans le cadre intuitionniste. Nous verrons ensuite plus loin que les théories complètes forment une semi-structure de Kripke, et pousserons l'analogie avec le cas classique.

Ce qui change fondamentalement par rapport à la définition d'une structure de Kripke est que nous définissons mutuellement deux relations, $\Vdash$ et $\check{\Vdash}$, *partielles*, par induction sur les formules :

1. si $\alpha \Vdash_\sigma A \vee B$ alors $\alpha \Vdash_\sigma A$ ou $\alpha \Vdash_\sigma B$.
2. si $\alpha \check{\Vdash}_\sigma A \vee B$ alors $\alpha \check{\Vdash}_\sigma A$ et $\alpha \check{\Vdash}_\sigma B$.
3. si $\alpha \Vdash_\sigma A \wedge B$ alors $\alpha \Vdash_\sigma A$ et $\alpha \Vdash_\sigma B$.
4. si $\alpha \check{\Vdash}_\sigma A \wedge B$ alors $\alpha \check{\Vdash}_\sigma A$ ou $\alpha \check{\Vdash}_\sigma B$.
5. si $\alpha \Vdash_\sigma A \Rightarrow B$ alors pour tout $\beta \geq \alpha$, $\beta \Vdash_\sigma A$ implique $\beta \Vdash_\sigma B$.
6. si $\alpha \check{\Vdash}_\sigma A \Rightarrow B$ alors il existe $\beta \geq \alpha$, $\beta \check{\Vdash}_\sigma A$ implique $\beta \check{\Vdash}_\sigma B$.
7. si $\alpha \Vdash_\sigma \neg A$ alors pour tout $\beta \geq \alpha$, $\beta \check{\Vdash}_\sigma A$.
8. si $\alpha \check{\Vdash}_\sigma \neg A$ alors il existe $\beta \geq \alpha$, $\beta \Vdash_\sigma A$.
9. si $\alpha \Vdash_\sigma \exists x A$ alors il existe un élément $a \in D(\alpha)$ tel que $\alpha \Vdash_{\sigma+\langle a/x\rangle} A$.
10. si $\alpha \check{\Vdash}_\sigma \exists x A$ alors pour tout élément $a \in D(\alpha)$, $\alpha \check{\Vdash}_{\sigma+\langle a/x\rangle} A$.
11. si $\alpha \Vdash_\sigma \forall x A$ alors pour tout $\beta \geq \alpha$, pour tout élément $a \in D(\beta)$, $\beta \Vdash_{\sigma+\langle a/x\rangle} A$.
12. si $\alpha \Vdash_\sigma \forall x A$ alors il existe $\beta \geq \alpha$, $a \in D(\beta)$, tels que $\beta \check{\Vdash}_{\sigma+\langle a/x\rangle} A$.

$\Vdash$ est monotone, alors que $\check{\Vdash}$ est anti-monotone (sur les atomes, et par extension, pour toutes les propositions).

Grâce au lemme 3.6, nous pouvons définir de manière simple une semi-structure de Kripke :

- L'ensemble des mondes est formé par les mondes A-complets, A-cohérents et admettant des A-témoins de Henkin.
- les relations $\Vdash$ et $\check{\Vdash}$ sont définies par :

$$\begin{array}{rll} P \in \Gamma & \text{implique} & \Gamma \Vdash P \\ \Gamma \nvdash^{cf}_{\mathcal{R}} P & \text{implique} & \Gamma \check{\Vdash} P \end{array}$$

Ici il faut faire attention au fait que $\check{\Vdash}$ est aussi une relation, qui correspond moralement à $\nvdash$, mais, contrairement à celle-ci, $\check{\Vdash}$ n'est *plus* le complémentaire de $\Vdash$ (sinon ce seraient des relations totales) Si on n'a pas $\alpha \Vdash P$, alors on a $\alpha \nVdash P$, mais on n'a pas $\alpha \check{\Vdash} P$. Et ici, comme la semi-structure est une relation partielle, c'est exactement ce que nous voulons.

Comme au chapitre précédent, section 5.1.3, nous n'avons pas de théorème de correction pour les semi-structures de Kripke. Tout l'important dans les

démonstrations du théorème de complétude forte est donc d'étendre cette semi-structure de Kripke en une structure de Kripke qui soit conservative (et, dans notre cas, qui soit en plus un modèle des règles de réécriture). C'est le schéma qui sera suivi dans les sections suivantes.

6.2 Complétude forte

Nous montrons maintenant le théorème de complétude forte (et ainsi, le théorème d'élimination des coupures) pour différentes classes de système de réécriture, que nous avons déjà rencontrés auparavant. Nous reprendrons les conditions vues au chapitre 5.

6.2.1 Une condition d'ordre

Dans cette section, nous supposerons le système de réécriture compatible avec un ordre bien fondé possédant la propriété de la sous-formule, comme nous l'avons vu dans la section 5.2.1 du chapitre précédent. Cette condition étend celle que l'on peut trouver dans [17] pour les systèmes de réécriture sans quantificateurs.

La construction de notre structure de Kripke est la suivante :

Définition 6.1. *Soit $\mathcal{K}$ la structure de Kripke définie comme suit :*
- *K est l'ensemble des théories A-complètes, A-cohérentes et admettant des A-témoins de Henkin.*
- *l'ordre partiel sur K est l'inclusion*
- *D_α est l'ensemble des termes du langage. Nous avons donc une structure syntaxique.*
- *la relation de forcing est définie de la façon suivante :*
  1. *Si A est un atome normal, alors $\Gamma \Vdash_{\mathcal{R}} A$ ssi $A \in \Gamma$.*
  2. *Si A n'est pas un atome normal, alors soit $A\downarrow$ son unique forme normale ($\mathcal{R}$ est confluent et termine, grâce à l'ordre, donc la forme normale existe). Nous posons $\alpha \Vdash_{\mathcal{R}} A$ ssi $\alpha \Vdash_{\mathcal{R}} A\downarrow$.*
  3. *La relation $\Vdash_{\mathcal{R}}$ entre les mondes et les propositions composées sont définis de la même manière que dans la définition 1.12.*

Tout d'abord, remarquons que la définition est bien fondée car l'ordre lui-même est bien fondé (en effet, on ne fixe la valeur de vérité que des atomes normaux, en définissant en fait celle d'une proposition P par induction sur l'ordre).

Il nous faut montrer deux choses. D'abord, que la structure définie est une structure de Kripke, puis que c'est un modèle de $\mathcal{R}$. Vérifier les conditions de la définition 1.12 est immédiat, sauf pour le cas d'une proposition P atomique. Nous allons montrer par induction sur l'ordre $\geq$ le lemme suivant :

Lemme 6.4. *Pour toute proposition P, si $\alpha \leq \beta$ alors $\alpha \Vdash_{\mathcal{R}} P$ implique $\beta \Vdash_{\mathcal{R}} P$*

Preuve. Nous procédons comme dans la preuve du lemme 1.2, à la différence que l'induction s'effectuera sur l'ordre bien-fondé dont est muni l'ensemble des règles de réécriture $\mathcal{R}$. Voyons les deux cas qui diffèrent de ceux explicités dans la preuve de 1.2 :

- Le cas de base : il s'agit maintenant des atomes normaux A. Il est tout aussi immédiat, car c'est la définition que nous avons donnée de $\mathcal{K}$.
- Un cas supplémentaire, celui des atomes non normaux : si A n'est pas un atome normal, alors nous appliquons l'hypothèse d'induction sur $A\downarrow$. Ceci est justifié car nous faisons décroître strictement l'ordre bien fondé.
- Tous les autres cas sont exactement identiques.

■

Corollaire 6.5. *La structure $\mathcal{K}$ est une structure de Kripke.*

Ce corollaire nous amène à la deuxième propriété que nous devons montrer : $\mathcal{K}$ doit être une structure de Kripke pour les règles de réécriture $\mathcal{R}$.

Lemme 6.6. *Soit $\mathcal{K}$ la structure de Kripke précédemment définie, $\alpha \in K$ et P une proposition.*
$\alpha \Vdash_{\mathcal{R}} P$ ssi $\alpha \Vdash_{\mathcal{R}} P\downarrow$.

Preuve. Par induction sur l'ordre bien fondé $\succ$. Nous distinguons des cas suivant le connecteur principal de la proposition P :

- Si P est un atome A, normal ou non, d'après la définition 6.1, A et $A\downarrow$ ont la même interprétation.
- Si $P = \exists x Q$, alors puisque la réécriture ne peut se faire que sur des prédicats, $P\downarrow = \exists x(Q\downarrow)$. Nous utilisons ensuite la définition des structures de Kripke 1.12 pour conclure, par hypothèse d'induction (car $\{c/x\}(Q\downarrow)\downarrow = (\{c/x\}Q)\downarrow$ et nous pouvons appliquer l'hypothèse d'induction à ces deux propositions.
- Si $P = A \vee B$, alors $P\downarrow = (A\downarrow) \vee (B\downarrow)$, et nous pouvons appliquer l'hypothèse d'induction sur A et B, en se servant de la règle pour $\vee$ dans la définition de la structure de Kripke.
- Tous les autres cas sont traités de manière similaire.

. ■

Corollaire 6.7. *Soit $\mathcal{K}$ la structure de Kripke définie précédemment, $\alpha \in K$ et $P \equiv_{\mathcal{R}} Q$ deux propositions. Alors $\alpha \Vdash_{\mathcal{R}} P$ ssi $\alpha \Vdash_{\mathcal{R}} Q$.*

Preuve. Par confluence, $P\downarrow = Q\downarrow$. ■

Il nous reste à prouver que $\mathcal{K}$ est un contre-modèle de $\mathcal{T} \vDash A$, avec $\mathcal{T}$ A-cohérente. C'est à dire qu'il existe un noeud α tel que $\alpha \Vdash_{\mathcal{R}} \mathcal{T}$ et $\alpha \nVdash_{\mathcal{R}} A$. Nous allons plutôt prouver le lemme suivant, qui en est une généralisation :

Lemme 6.8. *Soit $\mathcal{K}$ la structure de Kripke ci-dessus définie, soit $\Gamma \in K$ un de ses mondes, et soit P une proposition de $\mathcal{L}_\Gamma$, alors :*

$$P \in \Gamma \quad \textit{implique} \quad \Gamma \Vdash_{\mathcal{R}} P$$
$$\Gamma \nvdash^{cf}_{\mathcal{R}} P \quad \textit{implique} \quad \Gamma \nVdash_{\mathcal{R}} P$$

Notons que nous avons équivalence entre $P \in \Gamma$ et $\Gamma, P \nvdash_{\mathcal{R}} A$, d'après la construction de la section 3.4.

Preuve. Par induction sur l'ordre $\succ$, en distinguant suivant le connecteur principal de la proposition P.

- A est un atome normal. C'est la définition de $\Vdash_{\mathcal{R}}$
- A n'est pas un atome normal. Nous appliquons l'hypothèse d'induction à $A\downarrow$
- $Q \vee R$. Si $Q \vee R \in \Gamma$, alors prouvons que $Q \in \Gamma$ ou bien $R \in \Gamma$. Si ce n'était pas le cas, nous aurions $\Gamma, R \vdash^{cf}_{\mathcal{R}} A$ et $\Gamma, Q \vdash^{cf}_{\mathcal{R}} A$. Par la règle $\vee$ gauche nous aurions alors $\Gamma, R \vee Q \vdash^{cf}_{\mathcal{R}} A$, ce qui est une contradiction.
  Si $\Gamma \nvdash^{cf}_{\mathcal{R}} Q \vee R$, alors $\Gamma \nvdash^{cf}_{\mathcal{R}} Q$ et donc $\Gamma \nVdash_{\mathcal{R}} Q$ par hypothèse de récurrence. Nous procédons de même pour R. Ainsi $\Gamma \nVdash_{\mathcal{R}} P$.
- $Q \Rightarrow R$. Si $Q \Rightarrow R \in \Gamma$, alors soit un monde $\Delta \supseteq \Gamma$ tel que $\Delta \Vdash_{\mathcal{R}} Q$. Comme $Q \Rightarrow R \in \Delta$, nous avons $\Delta, Q \Rightarrow R \nvdash^{cf}_{\mathcal{R}} B(1)$ (Avec Δ B-cohérente). De même, nous avons $\Delta \vdash^{cf}_{\mathcal{R}} Q(2)$ car $\Delta \Vdash_{\mathcal{R}} Q$, et nous pouvons appliquer l'hypothèse d'induction.
  Il faut maintenant prouver que $\Delta \Vdash_{\mathcal{R}} R$. D'après (1), nous pouvons conclure que soit $\Delta \nvdash^{cf}_{\mathcal{R}} Q$, soit $\Delta, R \nvdash^{cf}_{\mathcal{R}} B$. La première possibilité est interdite par (2). Nous devons donc avoir la deuxième, ce qui implique que $R \in \Delta$ et donc par hypothèse d'induction par $\Delta \Vdash_{\mathcal{R}} R$.

  Si $\Gamma \nvdash^{cf}_{\mathcal{R}} Q \Rightarrow R$, alors nous devons avoir $\Gamma, Q \nvdash^{cf}_{\mathcal{R}} R$. Dans un langage plus riche, nous pouvons compléter Γ en Δ, Q-cohérent, etc. Mais si Δ est Q-cohérent, etc. il représente donc un monde de $\mathcal{K}$. De plus, nous avons $Q \in \Delta$ et $\Delta \nvdash^{cf}_{\mathcal{R}} R$. Par hypothèse d'induction $\Delta \Vdash_{\mathcal{R}} Q$ mais $\Delta \nVdash_{\mathcal{R}} R$.
- $\forall x Q$. Si $P \in \Gamma$, alors soit $\Delta \supseteq \Gamma$ et $t \in D_\Delta$. Puisque $P \in \Delta$, nous devons avoir $\Delta, \forall x P \nvdash^{cf}_{\mathcal{R}} B$, avec Δ B-cohérente. Ainsi, nous devons avoir $\Delta, \{t/x\}P \nvdash^{cf}_{\mathcal{R}} B$. Par hypothèse d'induction, nous avons donc $\Delta \Vdash_{\mathcal{R}} \{t/x\}Q$. Et ce, pour tout Δ et pour tout terme t.

  Si $\Gamma \nvdash^{cf}_{\mathcal{R}} P$, alors soit c une constante fraîche (d'un langage plus riche, donc) par rapport à Γ. Nous devons avoir $\Gamma \nvdash^{cf}_{\mathcal{R}} \{c/x\}Q$. Dans ce nouveau langage plus riche, nous pouvons compléter Γ en Δ, qui soit $\{c/x\}Q$-cohérente, $\{c/x\}Q$-complète et qui admette des $\{c/x\}Q$-témoins de Henkin. Cette théorie Δ représente un monde de K, ainsi, par hypothèse de récurrence, $\Delta \nVdash_{\mathcal{R}} \{c/x\}Q$.
- $\exists x Q$. Nous faisons intervenir les témoins de Henkin dans le cas $P \in \Gamma$. Dans le cas contraire, nous procédons comme dans le cas précédent.
- Tous les autres cas se traitent d'une manière similaire.

■

De ce lemme, nous pouvons enfin déduire le théorème de complétude forte :

Théorème 6.9 (Complétude forte). *Si $\mathcal{T} \vDash_{\mathcal{R}} P$, alors $\mathcal{T} \vdash^{cf}_{\mathcal{R}} P$.*

Preuve. Prouvons la contraposée. Si $\mathcal{T} \nvdash^{cf}_{\mathcal{R}} P$, alors dans la structure de Kripke précédemment définie, soit Γ un monde qui contient $\mathcal{T}$ (nous avons vu

qu'ils existaient). Par le lemme 6.8, nous avons $\Gamma \Vdash_{\mathcal{R}} \mathcal{T}$ et $\Gamma \nVdash_{\mathcal{R}} P$. ■

Et le corollaire d'élimination des coupures :

Corollaire 6.10. *Si* $\mathcal{T} \vdash_{\mathcal{R}} P$ *alors* $\mathcal{T} \vdash_{\mathcal{R}}^{cf} P$.

6.2.2 Une condition de positivité

Nous changeons maintenant la condition sur le système de réécriture. Nous allons supposer maintenant que le système $\mathcal{R}$, outre le fait qu'il soit confluent possède la propriété de positivité, c'est à dire que pour toute règle $A \to P \in \mathcal{R}$, nous avons P positive, dans le sens de la définition 1.8.

Sous cette hypothèse, d'une manière relativement similaire à celle de la section 5.2.2 nous allons prouver le théorème d'élimination de complétude forte pour le calcul des séquents modulo intuitionniste associé.

La construction du modèle mime celle du chapitre 5. Étant donné une théorie $\mathcal{T}$ qui est A-cohérente, nous commençons par définir une structure de Kripke, telle que pour un certain monde $\alpha \Vdash_{\mathcal{R}} \mathcal{T}$ et $\alpha \nVdash_{\mathcal{R}} A$. Ensuite, et seulement ensuite, nous prouvons que la structure définie est un modèle des règles de réécriture $\mathcal{R}$, et ce, grâce à la condition de positivité introduite.

Définition 6.2. *Nous considérerons la structure de Kripke* $\mathcal{K} = \langle K, \leq, D, \Vdash \rangle$ *suivante :*

- K *est l'ensemble des théories* A*-complètes,* A*-cohérentes et admettant des* A*-témoins de Henkin, pour une certaine proposition* A*,*
- $\leq$ *est la relation d'inclusion,*
- D_Γ *est l'ensemble des termes du langage dans lequel* Γ *est* A*-complète,*
- *La relation de forcing est définie de la façon suivante :*
  - *Si* B *est un atome (normal ou non pour* $\mathcal{R}$*), nous posons* $\Gamma \Vdash B$ *ssi* $B \in \Gamma$.
  - *Pour toutes les formules non-atomiques, nous définissons la relation de forcing en adéquation avec sa définition dans une structure de Kripke 1.12.*

Il est ainsi immédiat de constater que la structure précédemment définie est bien une structure de Kripke. Ce qui l'est moins est de prouver qu'elle est modèle de $\mathcal{R}$. En effet, nous n'utilisons nulle part dans la définition précédente les règles de réécriture.

Avant de nous intéresser à ce problème, intéressons nous au problème suivant :

Lemme 6.11. *Dans la structure de Kripke précédemment définie, nous avons, pour tout monde* $\Gamma \in K$ *:*

$$\begin{aligned} P \in \Gamma &\Rightarrow \Gamma \Vdash P \\ \Gamma \nvdash_{\mathcal{R}}^{cf} P &\Rightarrow \Gamma \nVdash P \end{aligned}$$

Preuve. Par induction sur la structure des propositions. Nous noterons dans toute la suite C_Γ la proposition A telle que Γ soit A-cohérente, A-complète

et admette des A-témoins de Henkin. Insistons sur le fait que ce n'est qu'une abréviation, et que C_Γ n'est en particulier pas une proposition atomique que l'on vient rajouter *a posteriori* au langage dans lequel est exprimé Γ.

Voyons quelques cas significatifs :

- Si P est une proposition atomique (normale ou non), c'est la définition.
- Si $P = A \Rightarrow B$. Considérons le cas $P \in \Gamma$. Soit $\Delta \supseteq \Gamma$. Nous avons donc $P \in \Delta$. Ainsi, $\Delta, B \nvdash^{cf}_{\mathcal{R}} C_\Delta$ ou $\Delta \nvdash^{cf}_{\mathcal{R}} A$. Dans le cas contraire, nous pourrions invoquer la règle $\Rightarrow$-gauche, et aurions une preuve de $\Delta, P \vdash^{cf}_{\mathcal{R}} C_\Delta$. Ainsi, par hypothèse d'induction, nous devons avoir soit $\Delta \Vdash B$ (car $B \in \Delta$, d'après une remarque de la section 3.4), soit $\Delta \nVdash A$. Dans tous les cas, si $\Delta \Vdash A$ alors $\Delta \Vdash B$, donc nous avons prouvé $\Gamma \Vdash P$.
  Concernant le cas $\Gamma \nvdash^{cf}_{\mathcal{R}} P$, nous devons avoir $\Gamma, A \nvdash^{cf}_{\mathcal{R}} B$. Dans un langage plus riche, nous pouvons compléter Γ, A en Δ telle que $C_\Delta = B$. Ainsi, en considérant Δ comme un monde de K, nous avons $\Gamma \leq \Delta$, $\Delta \Vdash A$ (Hypothèse de Récurrence) et $\Delta \nVdash B$, ce qui implique bien que $\Gamma \nVdash P$.
- Si $P = \exists x Q$. Dans le cas où $P \in \Gamma$, nous faisons intervenir la définition des C_Γ témoins de Henkin.
  Dans le cas où $\Gamma \nvdash^{cf}_{\mathcal{R}} P$, nous avons, pour n'importe quel terme $t \in D_\Gamma$: $\Gamma \nvdash^{cf}_{\mathcal{R}} \{t/x\}Q$, sinon nous pourrions prouver le séquent d'origine. Ainsi, par hypothèse de récurrence, nous avons $\Gamma \nVdash \{t/x\}Q$ pour tout terme t, donc $\Gamma \nVdash P$.
- Si $P = \forall x Q$. Dans le cas où $P \in \Gamma$, soit $\Delta \supseteq \Gamma$, nous faisons la même analyse que dans le cas précédent, et obtenons que pour tout terme $t \in D_\Delta$, $\Delta \Vdash \{t/x\}Q$. Donc $\Gamma \Vdash P$.
  Dans le cas contraire, soit c une constante fraîche par rapport au langage dans lequel est exprimé Γ. Alors, nous devons avoir $\Gamma \nvdash^{cf}_{\mathcal{R}} \{c/x\}Q$, car c est fraîche. Nous pouvons compléter (dans un langage plus riche) Γ en Δ, en forçant le fait que $C_\Delta = \{c/x\}Q$. Nous obtenons alors $\Delta \nVdash \{c/x\}Q$ par hypothèse de récurrence. Ce qui nous permet de conclure que $\Gamma \nVdash P$.

■

Reste maintenant à prouver le résultat annoncé plus haut : $\mathcal{K}$ est une structure de Kripke pour les règles de réécriture $\mathcal{R}$. D'un premier abord, on pourrait penser qu'il suffit d'utiliser le lemme 6.11 précédent de la façon suivante :

- Si $P \equiv_{\mathcal{R}} Q$ et $P \in \Gamma$, alors $\Gamma, P \nvdash^{cf}_{\mathcal{R}} C_\Gamma$, donc $\Gamma, Q \nvdash^{cf}_{\mathcal{R}} C_\Gamma$, et donc $Q \in \Gamma$
- Si $P \equiv_{\mathcal{R}} Q$ et $\Gamma \nvdash^{cf}_{\mathcal{R}} P$, alors $\Gamma \nvdash^{cf}_{\mathcal{R}} Q$ et nous avons $\Gamma \nVdash P$ et $\Gamma \nVdash Q$.

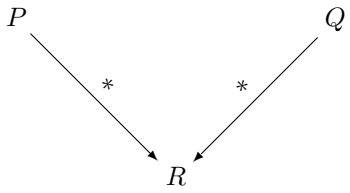
Cela fonctionne. Le problème est que ces deux cas ne sont pas exhaustifs. Il y en a un troisième :

$$\Gamma, P \vdash^{cf}_{\mathcal{R}} C_\Gamma$$
$$\Gamma \vdash^{cf}_{\mathcal{R}} P$$

voir les remarques correspondantes aux sections 5.2.2 et 3.2.1.

Nous restreignons tout d'abord notre problème, en utilisant le fait que les réécritures ont lieu sur des termes atomiques, et le fait que notre système de réécriture est supposé confluent.

Étant donné $P \equiv_{\mathcal{R}} Q$, si l'on veut prouver $\alpha \Vdash P \Leftrightarrow \alpha \Vdash Q$, comme le système de réécriture $\mathcal{R}$ est supposé confluent, il existe R tel que :



Ainsi, il suffit de prouver $\alpha \Vdash P \Leftrightarrow \alpha \Vdash R$. De plus, comme les réécritures dans P ne s'effectuent que sur des atomes, nous pouvons nous limiter au cas atomique (le reste s'obtient par une classique induction structurelle sur P).

Le résultat à prouver se simplifie donc en :

$$\text{Si } A \to P, \text{ nous avons } \alpha \Vdash A \Leftrightarrow \alpha \Vdash P$$

Pour cela, nous devons nous servir du fait que P est une propositions positive. En effet, nous avons supposé que $\mathcal{R}$ était un système de réécriture positif. Nous allons en fait prouver le lemme suivant par induction mutuelle :

Lemme 6.12. *Soit Γ un monde de la structure de Kripke définie précédemment (définition 6.2) et soit A la proposition telle que Γ est A-cohérente. Soient P, Q des propositions telles que :*

$$\begin{array}{cccc} \Gamma, P^+ \vdash^{cf}_{\mathcal{R}} A & & \Gamma, Q^- \vdash^{cf}_{\mathcal{R}} A & \\ \Gamma \quad \vdash^{cf}_{\mathcal{R}} P^+ & & \Gamma \quad \vdash^{cf}_{\mathcal{R}} Q^- & \end{array}$$

alors nous avons $\Gamma \Vdash P^+$ et $\Gamma \nVdash Q^-$.

Preuve.

La preuve se fait par induction mutuelle sur la structure de P et de Q. Distinguons les cas suivant le connecteur principal :

- il n'y en a pas. P est un atome : c'est la définition 6.2 de notre modèle. Q ne peut pas être un atome, car Q est négative.
- C'est $\wedge$. $P = R^+ \wedge S^+$. D'après de lemme de Kleene 3.5, nous avons des preuves des séquents suivantes :

$$\begin{array}{rcl} \Gamma, R, S & \vdash^{cf}_{\mathcal{R}} & A \\ \Gamma & \vdash^{cf}_{\mathcal{R}} & R \\ \Gamma & \vdash^{cf}_{\mathcal{R}} & S \end{array}$$

  Considérons R. Si $\Gamma, R^+ \vdash^{cf}_{\mathcal{R}} A$, alors par hypothèse de récurrence, nous avons $\Gamma \Vdash R$. Sinon, nous avons $\Gamma, R \nvdash^{cf}_{\mathcal{R}} A$, c'est à dire, par A-complétude de Γ, $R \in \Gamma$. Donc $\Gamma \Vdash R$ aussi, d'après le lemme 6.11. Même raisonnement pour S^+. Ce qui nous amène à la conclusion que $\Gamma \Vdash R \wedge S$.

$Q = R^- \wedge S^-$. Alors, toujours par le même lemme de Kleene 3.5, nous avons des preuves des mêmes séquents que précédemment. Considérons R. Si $\Gamma, R^- \vdash^{cf}_{\mathcal{R}} A$, alors par hypothèse de récurrence, nous avons $\Gamma \nVdash R$. Ainsi, $\Gamma \nVdash R \wedge S$.
Si $\Gamma, R^- \nvdash^{cf}_{\mathcal{R}} A$, alors $R \in \Gamma$. Alors, nous pouvons conclure que la preuve de $\Gamma, R, S \vdash^{cf}_{\mathcal{R}} A$ est en fait une preuve de $\Gamma, S \vdash^{cf}_{\mathcal{R}} A$. Et par hypothèse de récurrence (sur S^-, cette fois), nous obtenons $\Gamma \nVdash S$, ainsi, $\Gamma \nVdash R \wedge S$.

– C'est $\vee$. $P^+ = R^+ \vee S^+$. Alors nous utilisons la propriété de disjonction de Γ (lemme 3.7) et le lemme de Kleene, qui nous donnent des preuves des séquents suivants :

$$\begin{array}{rcl} \Gamma, R^+ & \vdash^{cf}_{\mathcal{R}} & A \\ \Gamma, S^+ & \vdash^{cf}_{\mathcal{R}} & A \\ \Gamma \vdash^{cf}_{\mathcal{R}} R^+ & \text{ou} & \Gamma \vdash^{cf}_{\mathcal{R}} S^+ \end{array}$$

Supposons que $\Gamma \vdash^{cf}_{\mathcal{R}} R^+$. Alors l'hypothèse de récurrence nous permet de conclure que $\Gamma \Vdash R^+$ et donc $\Gamma \Vdash P$.
$Q^- = R^- \vee S^-$. Nous avons encore des preuves des séquents ci-dessus. Peu importe que $\Gamma \vdash^{cf}_{\mathcal{R}} R^-$ ou que $\Gamma \nvdash^{cf}_{\mathcal{R}} R^-$, car la conclusion est la même (soit par hypothèse de récurrence, soit par le lemme 6.11), $\Gamma \nVdash R$. De même, $\Gamma \nVdash S$, et donc $\Gamma \nVdash P^-$.

– C'est $\Rightarrow$. $P = R^- \Rightarrow S^+$. Le lemme de Kleene nous fournir une preuve du séquent suivant :

$$\Gamma, R^- \quad \vdash^{cf}_{\mathcal{R}} \quad S^+$$

Supposons que dans un monde $\Delta \supseteq \Gamma$, nous ayons $\Delta \Vdash R$. D'après le lemme 6.11, nous avons donc $\Delta \vdash^{cf}_{\mathcal{R}} R$. De plus, par hypothèse de récurrence, et parce que R est une proposition négative, nous devons avoir aussi $\Delta, R \nvdash^{cf}_{\mathcal{R}} B$, avec Δ B-cohérente, B-complète. Ainsi, $R \in \Delta$, et donc, nous avons en fait une preuve de $\Delta \vdash^{cf}_{\mathcal{R}} S^+$. Si $S \in \Delta$, alors le lemme 6.11 permet de conclure, et sinon, c'est l'hypothèse d'induction qui permet de dire que $\Delta \Vdash S$. Ce qui prouve que $\Gamma \Vdash R \Rightarrow S$.

$Q = R^+ \Rightarrow S^-$. Le lemme de Kleene nous fournit la preuve du même séquent que précédemment. Cependant, ici il nous faut construire un monde $\Delta \supseteq \Gamma$ tel que $\Delta \Vdash R$ et $\Delta \nVdash S$. Comme nous allons le construire par induction sur la structure de la preuve du séquent $\Gamma, R \Rightarrow S \vdash^{cf}_{\mathcal{R}} A$, il nous faut un lemme intermédiaire plus général :

Lemme 6.13. *Soient $P_1 \equiv_{\mathcal{R}} ... \equiv_{\mathcal{R}} P_n \equiv_{\mathcal{R}} R \Rightarrow S$ des propositions. Soit Δ un monde (B-cohérent, B-complet et admettant des B-témoins de Henkin) qui vérifie :*

$$\Delta, P_1, ..., P_n \vdash^{cf}_{\mathcal{R}} B \tag{6.1}$$

$$\Delta \vdash^{cf}_{\mathcal{R}} R \Rightarrow S \tag{6.2}$$

alors il existe un monde $\Delta' \supset \Delta$ *tel que* $\Delta' \Vdash R^+$ *et* $\Delta' \nVdash S^-$*, et qui vérifie les équations 6.1 et 6.2.*
Preuve. La répétition des propositions P_i est nécessaire uniquement pour tenir compte des règles de contraction.

La preuve de ce lemme 6.13 se fait en deux temps. Nous allons d'abord trouver un monde Δ' tel que $\Delta' \Vdash R^+$. Cela se fait par récurrence sur la taille de la preuve du séquent 6.1. Puis nous prouverons que $\Delta' \nVdash Q^-$. Passons à la première étape.

Tout d'abord, si Δ est telle que le séquent suivant a une preuve :

$$\Delta \vdash^{cf}_{\mathcal{R}} R^+$$

alors nous pouvons choisir $\Delta' = \Delta$ car soit par hypothèse de récurrence (si $\Delta, R \vdash^{cf}_{\mathcal{R}} B$), soit par le lemme 6.11 (si $R \in \Delta$), nous avons $\Delta \Vdash R$.
Donc, dans toute la suite (de cette première étape), nous supposerons que :

$$\Delta \vdash^{cf}_{\mathcal{R}} R^+ \tag{6.3}$$

Faisons une distinction suivant la dernière règle appliquée dans la preuve de 6.1 :
- si la dernière règle de 6.1 est la règle axiome, alors cela ne peut être que parce que $B \equiv_{\mathcal{R}} R \Rightarrow S$ Ainsi, nous avons $\Delta \nvdash^{cf}_{\mathcal{R}} B$ et $\Delta \vdash^{cf}_{\mathcal{R}} R \Rightarrow S$. C'est une contradiction.
- Si c'est une règle sur Δ qui n'est ni $\neg$-gauche, ni $\Rightarrow$-gauche, alors nous utilisons la propriété d'inclusion de Δ du lemme 3.6, pour enfin appliquer l'hypothèse de récurrence. Par exemple, si la preuve est de la forme suivante :

$$\frac{\overline{\Delta, A, P_1, ..., P_n \vdash^{cf}_{\mathcal{R}} B} \quad \overline{\Delta, A', P_1, ..., P_n \vdash^{cf}_{\mathcal{R}} B}}{\Delta, P_1, ..., P_n \vdash^{cf}_{\mathcal{R}} B} \vee -\text{gauche}$$

  alors, puisque $A \vee A' \in \Delta$, nous pouvons utiliser le lemme 3.6. Supposons que $A \in \Delta$. Alors nous gardons la prémisse gauche, et avons une preuve de $\Delta, P_1, ..., P_n \vdash^{cf}_{\mathcal{R}} B$, à laquelle nous pouvons appliquer l'hypothèse de récurrence, puisque la hauteur de cette preuve est strictement plus petite.
- Si c'est $\Rightarrow$-gauche sur une proposition $A \Rightarrow A' \in \Delta$. Alors nous nous retrouvons avec deux preuves des séquents suivants :

$$\begin{aligned} \Delta, A', P_1, ..., P_n &\vdash^{cf}_{\mathcal{R}} B \\ \Delta, P_1, ..., P_n &\vdash^{cf}_{\mathcal{R}} A \end{aligned}$$

  Nous pouvons encore utiliser le lemme 3.6. Supposons dans un premier temps qu'on ait $A' \in \Delta$. Dans ce cas-là, nous pouvons, comme précédemment appliquer l'hypothèse d'induction. Dans le cas contraire,

$\Delta \nvdash^{cf}_{\mathcal{R}} A$ et nous pouvons compléter Δ en Δ', A-cohérente, A-complète et qui admet des A-témoins de Henkin. Δ' vérifie clairement 6.1, 6.2 car c'est une extension de Δ (dans un langage plus riche).
Nous appliquons l'hypothèse de récurrence sur Δ', car la preuve du séquent $\Delta, A', P_1, ..., P_n \vdash^{cf}_{\mathcal{R}} B$ est aussi une preuve de $\Delta', P_1, ..., P_n \vdash^{cf}_{\mathcal{R}} B$, mais de taille strictement inférieure.

- Si c'est $\neg$-gauche sur une proposition $\neg A \in \Delta$, nous faisons la même chose que dans le cas précédent.
- Si la règle est une règle de contraction/affaiblissement à gauche sur $P_i \equiv_{\mathcal{R}} R \Rightarrow S$, alors nous appliquons l'hypothèse de récurrence. Dans le cas de l'affaiblissement, il est impossible d'avoir $n = 1$ car nous aurions $\Delta \vdash^{cf}_{\mathcal{R}} B$ par B-cohérence.
- Si la règle est une règle sur la proposition B qui n'est pas $\forall$-droit, nous faisons la même chose que dans le cas précédent. Nous construisons une super-théorie Δ', qui est A-cohérente et A-complète pour une certaine sous-formule A de B (choisie grâce au lemme 3.6). Par exemple, si $B \equiv_{\mathcal{R}} A \Rightarrow A'$, alors nous avons une preuve du séquent $\Delta, A, P_1, ..., P_n \vdash^{cf}_{\mathcal{R}} A'$. Par le lemme 3.6, nous savons que $\Delta, A \nvdash^{cf}_{\mathcal{R}} A'$ et nous pouvons construire une super-théorie Δ' contenant A et A'-cohérente. ensuite, nous appliquons l'hypothèse de récurrence à la preuve de $\Delta', P_1, ..., P_n \vdash^{cf}_{\mathcal{R}} A'$
- Si la règle est une règle sur B qui est $\forall$-droite, alors nous avons une preuve de $\Delta, P_1, ..., P_n \vdash^{cf}_{\mathcal{R}} \{c/x\}A$ avec c qui est fraîche par rapport à la preuve. En particulier, nous pouvons la remplacer par n'importe quel terme dans toute la preuve (à un renommage des constantes fraîches près). En particulier, puisque $\Delta \nvdash^{cf}_{\mathcal{R}} B$, nous avons, pour une constante fraîche, dans une langage étendu :

$$\Delta \nvdash^{cf}_{\mathcal{R}} \{d/x\}A$$

Ceci implique que nous pouvons compléter, Δ en Δ' qui soit $\{d/x\}A$-cohérente, $\{d/x\}A$-complète et admette des $\{d/x\}A$-témoins de Henkin. Ainsi, la preuve de $\Delta, P_1, ..., P_n \vdash^{cf}_{\mathcal{R}} \{c/x\}A$ se transforme en une preuve de $\Delta, P_1, ..., P_n \vdash^{cf}_{\mathcal{R}} \{d/x\}A$, par substitution de c par d, puis en une preuve de $\Delta', P_1, ..., P_n \vdash^{cf}_{\mathcal{R}} \{d/x\}A$. Comme plus haut, si Δ' n'est pas le monde cherché, alors nous pouvons lui appliquer l'hypothèse de récurrence.

- Si la règle est une règle de connecteur sur P_i, cela ne peut être, par le lemme 3.1 que $\Rightarrow$-gauche (supposons $i = 1$ par simplicité. Alors nous avons deux preuves des séquents suivants $\Delta, S'^{-}, P_2, ..., P_n \vdash^{cf}_{\mathcal{R}} B$ et $\Delta, P_2, ..., P_n \vdash^{cf}_{\mathcal{R}} R'^{+}$ avec $S' \equiv_{\mathcal{R}} S$ t $R' \equiv_{\mathcal{R}} R$, ce qui nous donne immédiatement d'après le lemme 2.4 des preuves de :

$$\begin{aligned} \Delta, S^{-}, P_2, ..., P_n &\vdash^{cf}_{\mathcal{R}} B \\ \Delta, P_2, ..., P_n &\vdash^{cf}_{\mathcal{R}} R^{+} \end{aligned}$$

Puisque le séquent 6.3 n'a pas de preuve, nous pouvons compléter Δ en $\Delta' \supset \Delta$ R-cohérente, R-complète et qui admet des R-témoins de Henkin. Δ' vérifie 6.2 car c'est une théorie contenant Δ, et 6.1 car nous avons une preuve de $\Delta, P_2, ..., P_n \vdash^{cf}_{\mathcal{R}} R^+$, ce qui se transforme immédiatement en preuve du séquent $\Delta', P_2, ..., P_n \vdash^{cf}_{\mathcal{R}} R^+$.
Nous pouvons donc appliquer l'hypothèse de récurrence à Δ'.

– Tous les autres cas se traitent de la même manière.

Nous avons donc par récurrence trouvé une théorie $\Delta' \Vdash R^+$. Reste à prouver que $\Delta' \nVdash S^-$.
Nous remarquons que dans la preuve du séquent 6.1, avec Δ' comme théorie, nous pouvons remplacer les propositions $P_1, ..., P_n$ par la proposition S^-. En effet, si dans la démonstration de $\Delta', P_1, ..., P_n \vdash^{cf}_{\mathcal{R}} B$ on utilise la règle $\Rightarrow$-gauche, alors il suffit d'ignorer cette règle et de ne garder que la preuve de la prémisse droite (qui est $\Delta, P_1, ..., P_{n-1}, S' \vdash^{cf}_{\mathcal{R}} B$).
De même, si la règle est une règle axiome sur $T \equiv_{\mathcal{R}} R \Rightarrow S$, alors nous pouvons la remplacer par la démonstration suivante :

$$\dfrac{\dfrac{}{S, R \vdash^{cf}_{\mathcal{R}} S}\text{ axiome}}{S \vdash^{cf}_{\mathcal{R}} T}\Rightarrow\text{-droit}$$

Ainsi, en appliquant n fois la règle de contraction, nous avons trouvé que $\Delta', S^- \vdash^{cf}_{\mathcal{R}} B$. Soit par hypothèse de récurrence (du lemme 6.12 englobant ce lemme), soit par le lemme 6.11, nous pouvons conclure que $\Delta' \nVdash S^-$, et Δ' est le monde cherché. ■
Nous appliquons maintenant ce lemme à Γ. Γ vérifie les deux premières équations par hypothèse (par l'hypothèse du lemme 6.12). Nous pouvons donc lui appliquer le lemme 6.13 et nous obtenons l'existence d'un monde $\Delta \supset \Gamma$ tel que $\Delta \Vdash R$ et $\Delta \nVdash S$, ce qui amène à la même conclusion :

$$\Gamma \nVdash R^+ \Rightarrow S^-$$

– C'est $\exists$. $P^+ = \exists x R^+$. Alors, le lemme de Kleene 3.5 nous donne une preuve du séquent :

$$\dfrac{\pi}{\Gamma, \{c/x\}R \vdash^{cf}_{\mathcal{R}} A}$$

avec c constante fraîche (par rapport à la preuve π). Dans π, nous pouvons remplacer c par n'importe quel terme t (quitte à renommer certaines constantes fraîches). Cela implique que nous avons des preuves des séquents $\Gamma, \{t/x\}R \vdash^{cf}_{\mathcal{R}} A$.
De plus, par la propriété existentielle des théories A-complètes 3.7, nous avons une preuve de $\Gamma \vdash^{cf}_{\mathcal{R}} \{t/x\}P$ pour un certain terme t. Ainsi, par hypothèse d'induction $\Gamma \Vdash \{t/x\}P$ et donc $\Gamma \Vdash \exists x R$.
$Q^- = \exists x R^-$. Alors, comme ci-dessus, nous avons des preuves de tous les séquents de la forme $\Gamma, \{t/x\}R \vdash^{cf}_{\mathcal{R}} A$. Soit par hypothèse d'induction, soit par le lemme 6.11, nous avons $\Gamma \nVdash \{t/x\}R$, et ainsi $\Gamma \nVdash \exists x R$.

– C'est $\forall$. $P^+ = \forall x R^+$. Alors pour n'importe quel monde $\Delta \supseteq \Gamma$, le lemme de Kleene 3.5 nous donne la preuve suivante :

$$\frac{\pi}{\Delta \vdash^{cf}_{\mathcal{R}} \{c/x\}R}$$

Soit t un terme. Nous savons que $\Delta \vdash^{cf}_{\mathcal{R}} \{t/x\}R$, en remplaçant c par t dans π (et en renommant certaines constantes fraîches). Si $\Delta, \{t/x\}R \nvdash^{cf}_{\mathcal{R}} A$, alors $\Delta \Vdash \{t/x\}R$ par le lemme 6.11. De même, si $\Delta, \{t/x\}R^+ \vdash^{cf}_{\mathcal{R}} A$ alors par hypothèse d'induction $\Delta \Vdash \{t/x\}R^+$ aussi. Donc, pour tout $t \in D_\Delta$, $\Delta \Vdash \{t/x\}R$, c'est à dire $\Gamma \Vdash P^+$.

$Q^- = \forall x R^-$. Le but de l'étude de ce cas est de trouver un monde $\Delta \supseteq \Gamma$ tel qu'il existe un terme $t \in D_\Gamma$ tel que $\Delta \nVdash \{t/x\}R$. Ce n'est pas si simple que cela, en particulier parce que Δ peut très bien être différente de Γ. En fait, il nous faut procéder de manière similaire à ce que nous faisons dans le lemme 6.13. Plus exactement, nous devons prouver le lemme suivant :

Lemme 6.14. *Soit Δ une théorie B-complète, B-consistante, admettant des B-témoins de Henkin, des propositions $P_1 \equiv_{\mathcal{R}} ... \equiv_{\mathcal{R}} P_n \equiv_{\mathcal{R}} \forall x R^-$ telles que les séquents suivants aient des preuves :*

$$\Delta, P_1, ..., P_n \quad \vdash^{cf}_{\mathcal{R}} \quad B \tag{6.4}$$

$$\Delta \quad \vdash^{cf}_{\mathcal{R}} \quad \forall x R^- \tag{6.5}$$

alors nous pouvons trouver $\Delta' \supseteq \Delta$ et un terme $t \in D_{\Delta'}$ tel que $\Delta' \nVdash \{t/x\}R$

Preuve. Par récurrence sur la hauteur de la preuve du séquent 6.4. Remarquons tout d'abord que nous avons $\Delta \vdash^{cf}_{\mathcal{R}} \{t/x\}R^-$ pour tout terme t du langage d'après le lemme de Kleene et par substitution de la variable fraîche introduite (comme ci-dessus, dans le cas positif).

En distinguant selon la dernière règle appliquée :

– c'est une règle sur une proposition de Δ. Nous utilisons le lemme 3.6, dans le cas où ce n'est ni la règle $\Rightarrow$-gauche ni la règle $\neg$-gauche : nous pouvons ignorer cette règle car elle transforme une proposition de Δ en une proposition de Δ.
  Si c'est une de ces deux règles, nous agissons de la même manière que dans la démonstration du lemme 6.13 : nous construisons un monde $\Delta' \supset \Delta$ qui vérifie encore les hypothèses du lemme, mais avec une preuve de 6.4 plus petite, et nous pouvons appliquer l'hypothèse de récurrence.
– C'est une règle sur la proposition B : même manière que précédemment. Nous construisons $\Delta' \supset \Delta$ A-complète pour une certaine sous-formule A de B, et qui vérifie les hypothèses du lemme 6.14, de telle manière que la preuve de 6.4 soit plus petite et que nous puissions appliquer l'hypothèse de récurrence.
– C'est une règle de contraction ou d'affaiblissement sur P_i. Nous appliquons l'hypothèse de récurrence. L'affaiblissement avec $n = 1$ ne peut

pas avoir lieu (car Δ est B- cohérente).
– C'est une règle de connecteur sur P_i (P_1 par simplicité). Ça ne peut être que $\forall$-gauche d'après le lemme 3.1. Alors nous avons pour un certain terme t_0 une preuve du séquent suivant :

$$\Delta, \{t_0/x\}R'^{-}, P_2, ..., P_n \vdash^{cf}_{\mathcal{R}} B$$

Deux cas sont envisageables. Soit $\Delta, \{t_0/x\}R^- \vdash^{cf}_{\mathcal{R}} B$, et dans ce cas, par l'hypothèse de récurrence du lemme 6.12, nous obtenons $\Delta \nVdash \{t_0/x\}R^-$. Sinon, c'est que $\{t_0/x\}R^- \in \Delta$ et alors nous avons en fait une preuve de $\Delta, P_2, ..., P_n \vdash^{cf}_{\mathcal{R}} B$ de taille inférieure, à laquelle nous pouvons appliquer l'hypothèse de récurrence.

■

Ainsi, comme Γ vérifie les conditions du lemme 6.14, nous avons prouvé que $\Gamma \nvdash^{cf}_{\mathcal{R}} Q^-$.

■

Nous sommes maintenant prêts à démontrer le lemme qui conclut notre construction :

Lemme 6.15. *La structure de Kripke $\mathcal{K}$ précédemment construite est une structure de Kripke pour les règles de réécriture $\mathcal{R}$.*

Preuve. Comme déjà dit, nous pouvons nous focaliser sur les atomes, car les règles de réécriture interviennent sur les atomes. Soit donc un monde Γ A-complet, un atome B et une proposition P telle que :

$$A \to P$$

Alors, soit $B \in \Gamma$, et dans ce cas, $P \in \Gamma$ aussi et d'après le lemme 6.11, nous avons $\Gamma \Vdash B$ et $\Gamma \Vdash P$.

Si $B \notin \Gamma$, mais si $\Gamma \nvdash^{cf}_{\mathcal{R}} B$, nous utilisons le même raisonnement pour dire que $\Gamma \nVdash B$ et $\Gamma \nVdash P$.

Enfin, si ce n'est pas le cas, c'est parce que :

$$\begin{array}{rcl} \Gamma, B & \vdash^{cf}_{\mathcal{R}} & A \\ \Gamma & \vdash^{cf}_{\mathcal{R}} & B \end{array}$$

Ceci est vrai aussi pour P. Comme P est positive, nous avons d'après le lemme 6.12 $\Gamma \Vdash P$. Et nous avons par définition $\Gamma \Vdash B$.

Ainsi, $\Gamma \Vdash B \Leftrightarrow \Gamma \Vdash P$. Nous étendons sans difficulté cette équivalence à la réécriture en général ($B \to^* P$), puis aux propositions non atomiques ($P \to^* Q$) par induction sur la structure de P, et enfin à l'équivalence modulo $\mathcal{R}$. ■

$\mathcal{K}$ est donc un modèle des règles de réécriture. De plus, $\Gamma \Vdash_{\mathcal{R}} \Gamma$ et $\Gamma \nVdash_{\mathcal{R}} A$ par le lemme 6.11. Ceci termine la démonstration du théorème de complétude forte pour les systèmes de réécriture positifs :

Théorème 6.16 (Complétude forte). *Soit $\mathcal{R}$ un système de réécriture positif, $\mathcal{T}$ une théorie A-cohérente. Alors il existe un noeud α d'une certaine structure de Kripke (pour $\mathcal{R}$) tel que $\alpha \Vdash \mathcal{T}$ et $\alpha \nVdash A$.*

Preuve. Complétons $\mathcal{T}$ en Γ A-complète, et construisons la structure de Kripke $\mathcal{K}$ telle que précédemment, ayant pour racine Γ. D'après tout ce qui précède, Γ et $\mathcal{K}$ ont toutes les propriétés voulues. ■

Il s'ensuit le corollaire d'élimination des coupures :

Corollaire 6.17 (Élimination des coupures). *Soit un système de réécriture positif $\mathcal{R}^+$. Alors le calcul des séquents associé possède l'élimination des coupures.*

Preuve. Par correction puis complétude forte. ■

6.2.3 Réunir les deux conditions précédentes

Nous reprenons les résultats de la section 5.2.3 et les prouvons pour le calcul des séquents modulo intuitionniste.

Les résultats de cette section sont de même nouveaux.

Rappelons la définition centrale :

Définition. *Soient deux systèmes de réécriture $\mathcal{R}$ et $\mathcal{R}'$. $\mathcal{R}'$ est normal à droite pour $\mathcal{R}$ si, pour toute règle propositionnelle $l \to r \in \mathcal{R}'$, toutes les instances des atomes de r par des substitutions σ R-normales sont normales pour $\mathcal{R}$.*

Nous supposerons donc avoir un système de réécriture confluent, qui termine, et se décomposant en deux parties complémentaires et confluentes $\mathcal{R}$ et $\mathcal{R}_+$, telles que $\mathcal{R}_+$ soit positif et normal à droite pour $\mathcal{R}_>$.

Définition 6.3. *Soit une théorie Γ, complète, cohérente, admettant des témoins de Henkin, dans un langage $\mathcal{L}$. Nous définissions la Structure de Kripke $\mathcal{K}$ comme à la définition 6.1, en considérant les règles de réécriture $\mathcal{R}_>$ uniquement.*

Notons que comme dans la section 6.2.2, nous définissons notre modèle sans tenir compte des règles de écriture positives $\mathcal{R}_+$, et fixons arbitrairement à chaque monde une valeur de vérité aux atomes non $\mathcal{R}_+$ normaux, mais $\mathcal{R}_>$ normaux. (nous avons décidé que $\alpha \nVdash A$).

Lemme 6.18.

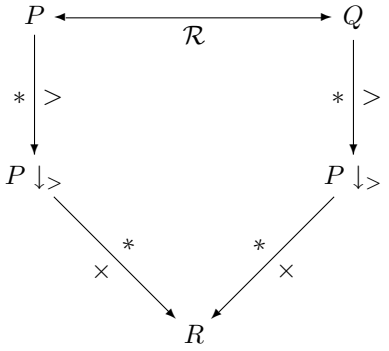
$$\begin{array}{rcl} \textit{Si } P \in \Gamma & \textit{alors} & \Gamma \Vdash P \\ \textit{Si } \Gamma \nvdash^{cf}_{\mathcal{R}} P & \textit{alors} & \Gamma \nVdash P \end{array}$$

Preuve. Par induction sur l'ordre $>$. ■

Pour prouver que le modèle est un modèle des règles de réécriture, nous commençons par le prouver sur les règles de $\mathcal{R}_>$, par induction sur l'ordre $>$. L'hypothèse est si $P \to^*_> Q$, alors pour tout monde Γ, $\Gamma \Vdash P$ ssi $\Gamma \Vdash Q$.

– Si P est un atome normal, alors $P = Q$.
– Si P est un atome non normal, alors $P \rightarrow^+ Q \rightarrow^* P\downarrow$. Nous appliquons l'hypothèse d'induction sur Q, et obtenons $\Gamma \Vdash Q$ ssi $\Gamma \Vdash P\downarrow$, ssi $\Gamma \Vdash P$ (la dernière équivalence étant par définition).
– Si P n'est pas atomique, alors nous la décomposons en fonction de son connecteur principal.

Il nous faut ensuite le montrer pour les règles positives, et nous pourrons conclure par le même argument de quasi-commutativité des règles de réécriture de $\mathcal{R}_>$ et $\mathcal{R}_+$: si $P \equiv_{\mathcal{R}} Q$, il existe R tel que :



Lemme 6.19. *Soit P une proposition, soit négative soit positive, et $>$-normale.*
Si $\Gamma, P^+ \vdash^{cf}_{\mathcal{R}}$ et $\Gamma \vdash^{cf}_{\mathcal{R}} P^+$ alors $\Gamma \nVdash P$.
Si $\Gamma, P^- \vdash^{cf}_{\mathcal{R}}$ et $\Gamma \vdash^{cf}_{\mathcal{R}} P^-$ alors $\Gamma \Vdash$.

Preuve. Elle se fait exactement de la même manière que dans la section 6.2.2, par induction sur la structure de la proposition, et en utilisant le fait que P et toutes ses instances sont $>$-normale dans le cas atomique. ■

$\mathcal{K}$ est un donc modèle des règles de réécriture.

Nous avons donc le théorème suivant :

Théorème 6.20. *Soit $\mathcal{R}$ un système de réécriture compatible avec un ordre bien-fondé.*
Soit $\mathcal{R}_+$ un système de réécriture qui soit normal à droite pour $\mathcal{R}$, et tel que $\mathcal{R} \cup \mathcal{R}_+$ soit confluent.
Si $\Gamma \vDash_{\mathcal{R}\cup\mathcal{R}_+} P$ alors on a une preuve (sans coupure) du séquent :

$$\Gamma \vdash^{cf}_{\mathcal{R}\cup\mathcal{R}_+} P$$

Nous avons donc le théorème d'élimination des coupures :

Corollaire 6.21. *Soit $\mathcal{R}$ un système de réécriture compatible avec un ordre bien-fondé.*
Soit $\mathcal{R}_+$ un système de réécriture qui soit normal à droite pour $\mathcal{R}$, et tel que $\mathcal{R} \cup \mathcal{R}_+$ soit confluent.
Alors la règle de coupure est redondante dans le calcul des séquents modulo intuitionniste $\mathcal{R} \cup \mathcal{R}_+$.

6.3 Autres méthodes sémantiques

Lipton et de Marco ([10]), ainsi que Okada ([35]) ont introduit une méthode d'élimination des coupures à base d'algèbres de Heyting très intéressante qui pourrait sans doute être mise en relation avec la nôtre (Okada introduit ces techniques dans le cadre de la logique linéaire). Plusieurs questions méritent d'être posées à ce sujet : peut-on étendre sa méthode dans le cadre de la déduction modulo ? Existe-t-il une correspondance entre ces deux méthodes ? Et plus généralement, quel lien y-a-t-il entre les algèbres de Heyting et les structures de Kripke "pour l'élimination des coupures" ? Nous laissons ces questions pour un travail futur.

Il est possible que la condition d'ordre de la section 6.2.1 soit suffisante pour démontrer *à la* Gentzen le théorème d'élimination des coupures, mais ne serait pas généralisable à la condition de positivité. C'est là un des atouts de la méthode que nous définissons, elle s'étend facilement à différentes conditions.

Chapitre 7

La Logique d'Ordre Supérieur

Dans ce chapitre, nous présentons une formulation au premier ordre de la logique d'ordre supérieur, en abrégé HOL. Ceci est rendu possible grâce aux règles de réécriture et aux combinateurs.

7.1 Expressions de HOL

7.1.1 HOL avec des lieurs

L'idée qui sous-tend HOL est de pouvoir quantifier sur des propositions. En effet, pourquoi n'aurait-on pas le droit de parler de la proposition $\forall P(P \Rightarrow P)$? Ceci n'est pas possible dans la logique du premier ordre, où nous avons une séparation claire entre les termes et les propositions. Ici, les propositions seront des termes auxquels nous réserverons un traitement un peu particulier.

Nous commençons par définir les types possibles des termes que nous rencontrerons :

Définition 7.1 (Types Simples).

o est un type de base (atomique), c'est le type des propositions.

ι est le deuxième type de base. Il sert à dénoter les termes non propositionnels.

Nous pouvons combiner deux types entre eux avec la flèche. Si T et U sont des types, alors $T \to U$ est un type. C'est le type des fonctions qui à tout terme de type T associe un terme de type U.

Au niveau des termes eux-mêmes, pour chaque type T nous supposerons avoir un nombre au plus dénombrable de constantes de type T, et un nombre toujours infini dénombrable de variables $x_T : T$.

En particulier, les combinateurs logiques $\Rightarrow$, $\wedge$, $\vee$ ont pour type $o \to o \to o$, le combinateur $\neg$ a pour type $o \to o$. Ce sont des constantes "distinguées" ou "logiques" de ce type, qui existent toujours.

$$\frac{\Gamma, Pt\downarrow}{\Gamma, \forall_T P \vdash \Delta}\forall\text{-gauche, } t:T \qquad \frac{\Gamma \vdash Px_T\downarrow}{\Gamma \vdash \forall_T P, \Delta}\forall^*\text{-droite,} x_T : T$$

FIG. 7.1 – Deux règles du calcul des séquents en Logique d'Ordre Supérieur

Quand nous avons un symbole de prédicat $P : \iota \to o$ par exemple, nous pouvons quantifier universellement ou existentiellement, et former la proposition $\forall_\iota P$ qui est de type o. Ici, nous n'avons pas besoin de dire quelle est le nom de la variable liée, car il est clair d'après le type de P. Si l'on veut instancier cette proposition pour un certain terme $t : \iota$ il suffit de prendre Pt. Ainsi, pour chaque type T, nous avons deux symboles de constante, $\forall_T$ et $\exists_T$ qui ont le type $(T \to o) \to o$.

Maintenant, supposons que nous ayons un symbole de proposition $P : o$. Pour n'importe quel type T, nous pouvons former un prédicat de type $T \to o$ de la manière suivante :

$$\lambda x_T.P \ : T \to o$$

Nous pouvons faire ceci pour absolument n'importe quel type et n'importe quel nom de variable associé à ce type. Bien sûr, si x_T n'apparaît pas dans P, la fonction sera une fonction constante qui à tout terme $t : T$ associe P. Les cas intéressants sont ceux où x_T apparaît dans P.

Le système de déduction associé a des règles quasiment identiques à celles du calcul des séquents, à l'exception des règles régissant les quantificateurs. Dans le cas classique, elles sont exprimées par la figure 7.1.1 et de manière symétrique pour le quantificateur existentiel. Notons qu'ici, nous avons utilisé la présentation avec une instanciation par des variables fraîches à la place de constantes fraîches.

Notons que nous β réduisons $(Pt\downarrow)$, car nous avons une forme de λ-calcul typé (le λ-calcul simplement typé). De plus, pour l'instant, nous ne pouvons pas éviter les problèmes d'α-conversion, et nous devons identifier les termes $\lambda x_T.(\ Px_T)$ et $\lambda y_T.(\ Py_T)$. Ce problème est temporaire, car nous allons définir une version de HOL avec des combinateurs, qui ne possède pas le lieur λ, et qui donc n'a pas besoin de variable.

Si nous avons un symbole de prédicat $P : \iota \to (\iota \to o)$ par exemple, alors l'équivalent de la proposition $\forall x \forall y P(x, y)$ s'écrit :

$$\forall_\iota \lambda x.(\forall_\iota \lambda y.(P\ x\ y)\ )$$

La force théorique de ce système de déduction vient du fait que nous pouvons définir des termes de la forme $o \to \iota$ par exemple, mais surtout, des termes dits "imprédicatifs". Ce sont des termes qui sont construits en quantifiant sur un ensemble auquel ils finissent par appartenir.

Par exemple, si nous disposons d'une proposition $Q = \forall P(P \Rightarrow P)$, rien ne nous empêche d'instancier P par Q elle-même et d'obtenir l'instance $(\forall P(P \Rightarrow P)) \Rightarrow (\forall P(P \Rightarrow P))$.

Cette possibilité supplémentaire est très importante, et complique beaucoup notre tâche. En effet, il devient impossible de définir comme dans le chapitre 5 des modèles syntaxiques, car les termes se “mordent la queue”.

7.1.2 HOL avec des combinateurs

Au lieu de travailler avec le lieur λ, qui amène des problèmes d'α-conversion, il existe une présentation de HOL avec des combinateurs, qui évitent l'utilisation du lieur λ. Cette présentation peut être prouvée équivalente (voir par exemple [14]), c'est à dire qu'on peut simuler l'une par l'autre et inversement, à condition d'avoir l'extensionnalité.

Elle est basée sur l'introduction de constantes S et K pour chaque types, et par la définition de règles de réduction associées (qui simulent la β-réduction).

Définition 7.2 (langage de HOL avec des combinateurs). *Le langage est formé des éléments suivants :*

- *Pour tout type T, un ensemble dénombrable de constantes.*
- *Pour tous types T, U une constante $K_{T,U} : T \to U \to T$.*
- *Pour tous types T, U, V une constante $S_{T,U,V} : (T \to U \to V) \to (T \to U) \to T \to V$*
- *des constantes $\bot, \top$ de type o*
- *une constante $\neg$ de type $o \to o$*
- *des constantes $\Rightarrow, \wedge, \vee$ de type $o \to o \to o$*
- *pour tout type T des constantes $\forall_T, \exists_T$ de type $(T \to o) \to o$*

Nous avons les mêmes règles de déduction que précédemment, avec les règles de β-réduction suivantes :

$$\begin{aligned} S_{T,U,V}xyz &\to (xz)(yz) \\ K_{T,U}xy &\to x \end{aligned}$$

Donnons seulement un exemple : la fonction $o \to o$ qui à tout P associe P s'écrit :

$$S_{o,o\to o,o}K_{o,(o\to o)}K_{o,o}$$

La β-réduction correspond déjà à une forme de réécriture, sur les termes commençant par S ou K. Dowek et Werner dans [17] ont montré qu'il était possible de plonger tout ce calcul dans le calcul des séquents du premier ordre, avec la déduction modulo.

7.1.3 HOL en déduction modulo

Le problème de HOL est qu'il n'y a plus de distinction entre les termes et les propositions, ces dernières étant simplement des “termes distingués” de type o. La distinction se fait simplement au niveau des règles de déduction. La déduction modulo, en ce sens, clarifie la situation en introduisant de nouveau une séparation entre les propositions et les termes.

L'idée principale est que toute la syntaxe que nous venons de voir est en fait la syntaxe des *termes*, et que les termes de type o, et seulement ceux-ci représentent de manière cachée des propositions. Pour achever la transformation des termes de type o en propositions, il faut inventer un déguisement. Pour ce faire, nous introduisons le symbole ε, de rang $\langle o \rangle$, qui joue un rôle d'encapsulement : puisque les termes de type o sont des termes spéciaux, il faut les faire ressortir, et ce, à travers l'encapsulateur ε.

Pour distinguer les connecteurs de termes $\wedge : o \to o \to o$, des connecteurs de propositions (qui n'ont pas de type), nous allons maintenant noter les connecteurs de terme avec un point, c'est la convention retenue dans la définition 7.3.

Le travail se poursuit de la manière suivante : un terme de type o de la forme $\dot{\wedge}\, PQ$ représente moralement une proposition $P \wedge Q$. Cela se traduira donc par la règle de réécriture suivante :

$$\varepsilon(\dot{\wedge}\, PQ) \to \varepsilon(P) \wedge \varepsilon(Q)$$

Nous ferons un travail identique pour tous les autres connecteurs. De plus, pour formaliser l'application d'un terme à un autre (comme SKK par exemple), nous introduirons le symbole α, de rang $\langle T \to U, T, U \rangle$.

Finalement, voici la définition de HOL exprimée au premier ordre avec des combinateurs, avec T, U, V des types simples de la définition 7.1 :

Définition 7.3. *Le langage de la logique d'ordre supérieur est constitué, pour chaque type simple d'un ensemble dénombrable de constantes et de variables, ainsi que des symboles suivants, étant donné des types simples T, U, V quelconques :*

- $S_{T,U,V} : (T \to U \to V) \to (T \to U) \to T \to V$
- $K_{T,U} : T \to U \to T$
- $\dot{\Rightarrow}, \dot{\vee}, \dot{\wedge}$: $o \to o \to o$
- $\dot{\neg}$: $o \to o$
- $\dot{\exists}_T, \dot{\forall}_T$: $T \to o$ *symboles de quantificateurs.*
- $\alpha_{T,U}$ *symbole d'application, de rang* $\langle T \to U, T, U \rangle$.

Et enfin, nous définissons un unique symbole de prédicat ε de rang $\langle o \rangle$.

Les constantes de la définition précédente ne sont pas des constantes très importantes. Elles servent seulement à fournir des constantes fraîches lorsque nous en aurons besoin.

Nous utiliserons couramment ft au lieu de $\alpha(f, t)$, et de même, $\alpha(f, t)$ au lieu de $\alpha_{T,U}(f, t)$ où T est le type de f et U celui de t. De manière plus générale, lorsque le type des termes n'est pas important, ou lorsqu'il sera clair d'après le contexte, nous ne le noterons pas.

Enfin, nous écrivons les connecteurs logiques surmontés d'un point $\dot{\wedge}$ tout simplement parce que ce sont des *termes*, et non pas des symboles logiques. En effet, ils connectent maintenant les termes entre eux, car nous n'avons qu'un seul symbole de proposition, qui est ε, qui encapsule tout le reste.

Nous donnons maintenant les règles de réécriture associées au calcul :

Définition 7.4. *Soit $\mathcal{R}$ le système de réécriture suivant :*

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

Moralement, $\varepsilon(p_o)$ et p_o représentent la même chose. C'est à dire que p est l'objet, et $\varepsilon(p)$ est son encapsulation, qui en fait une proposition. p représente le contenu de la proposition $\varepsilon(p)$. Nous pourrions poursuivre la comparaison pour les connecteurs $\Rightarrow$ et $\dot{\Rightarrow}$ par exemple.

Dans [14], il est démontré que ce système de réécriture est confluent et termine, ce que nous supposerons acquis.

Intéressons nous maintenant à la propriété d'élimination des coupures de ce système.

7.2 L'élimination des coupures

Takahashi [43] et Prawitz [37] ont démontré la propriété d'élimination des coupures du système HOL classique, par des méthodes sémantiques. Elles ont été modernisées par Andrews [2], qui l'a formalisé dans l'expression de HOL avec le lieur λ.

Nous montrons ici que la preuve d'Andrews s'applique à la présentation de HOL en déduction modulo, c'est à dire exprimée avec des combinateurs S, K plutôt qu'avec un lieur λ. De plus, la preuve que nous développons ici suit exactement le même schéma que les preuves précédentes.

Notre problème est un peu le même que dans le cas des systèmes de réécriture positifs de la section 5.2.2 , car là aussi nous pouvons avoir une sorte de circularité, par exemple avec la règle de réécriture $P(0) \to \forall x P(x)$, ce qui ressemble à de l'imprédicativité. Seulement, nous avons ici des règles de réécriture qui ne sont pas positives : celles associées aux symboles $\dot{\neg}$ et $\dot{\Rightarrow}$. Remarquons cependant que celle-ci pourraient très bien être compatibles avec un ordre bien-fondé, et nous pourrions être tentés d'appliquer la condition trouvée à la section 5.2.3 du chapitre 5. Nous ne pouvons pas faire cela, car les règles positives ne sont pas normales à droite pour les règles compatibles avec un ordre.

L'idée est, ayant une théorie Γ complète, cohérente et admettant des témoins de Henkin, de considérer trois types de propositions (comme dans le cas positif) :

1. les propositions de Γ, qui doivent être interprétées par 1.
2. les propositions telles que $\Gamma \not\vdash^{cf}_{\mathcal{R}} P$ qui doivent être interprétées par 0.
3. les propositions qui ne sont ni l'une, ni l'autre, que nous ne savons pas interpréter.

La troisième catégorie n'est pas forcément vide, comme nous en avons déjà fait la remarque section 5.2.2, car nous pouvons tout à fait avoir $\Gamma, P \vdash^{cf}_{\mathcal{R}}$ et $\Gamma \vdash^{cf}_{\mathcal{R}} P$ sans que Γ ne soit incohérente à moins d'avoir déjà démontré le théorème d'élimination des coupures.

Pour les propositions de la troisième catégorie, nous avons fait le choix, dans la section 5.2.2 du chapitre 5, d'interpréter tout d'abord les atomes, et d'étendre cette interprétation à toutes les propositions.

Malheureusement, il n'est pas possible de procéder ainsi ici, car les règles de réécriture ne sont plus positives. Au lieu d'interpréter les propositions de la troisième catégorie de cette manière par trop impérative, nous allons prendre les deux interprétations possibles, et différer la résolution de ce problème jusqu'à la construction du modèle.

L'astuce technique, puisque dans un modèle les propositions doivent être interprétées par 0 ou par 1 quoi qu'il arrive, est de se placer au niveau du contenu propositionnel de ces propositions (c'est à dire des termes de type o), et d'associer à tout terme de type o non seulement lui-même (comme dans un modèle syntaxique), mais aussi ses interprétations possibles :

$$\widehat{p_o} \quad := \quad \langle p_o, v \rangle$$

avec $v = V(p_o)$ si $V(p_o)$ est définie, et soit 0, soit 1 sinon.

Ainsi, notre modèle ne sera plus un modèle à base de termes, mais un modèle plus complexe, où nous tenons compte à la fois du fait que p est un terme, mais aussi une proposition.

Remarque. La formulation de HOL en déduction modulo permet de manière très simple de résoudre le problème de l'intentionnalité de HOL. Pour mémoire, même si dans HOL nous pouvons prouver :

$$p_o \mathrel{\dot\wedge} p_o \quad \Leftrightarrow \quad p_o$$

pour un prédicat $q_{o \to o}$ nous ne pouvons pas prouver :

$$q(p \mathrel{\dot\wedge} p) \quad \Leftrightarrow \quad q(p)$$

Ce qui veut dire que q est capable de discriminer finement. Elle ne voit pas p comme une *proposition* (une valeur de vérité), mais comme un *terme* (une suite de caractères). Cela veut dire aussi que dans nos modèles, nous ne devrons pas interpréter les termes de type o par $0, 1$, sous peine de ne pouvoir distinguer les deux propositions précédentes.

Ce problème est quasi inexistant en déduction modulo, car nous faisons une distinction très nette entre p_o et $\varepsilon(p)$. Alors, de manière assez naturelle, nous interpréterons $\varepsilon(p)$ (proposition) par $0, 1$, et p_o (terme propositionnel) sera interprété de manière plus syntaxique.

En effet, $\varepsilon(p)$ n'est pas un terme, et ne pourra jamais se retrouver en argument d'un prédicat.

7.2.1 Les semi-valuations sur les termes

Puisque nous avons des termes propositionnels (de type o), nous étendons la notion de semi-valuation 3.4 à ces termes.

Définition 7.5 (Semi-valuation). *Une* semi-valuation V *sur les termes propositionnels (de type o) est une fonction partielle de o vers* $\{0,1\}$ *telle que :*

- *si* $p \equiv_{\mathcal{R}} q$ *alors* $\| p \| = \| q \|$
- *si* $\| \alpha(\dot{\neg}, p) \| = 0$ *alors* $\| p \| = 1$
- *si* $\| \alpha(\dot{\neg}, p) \| = 1$ *alors* $\| p \| = 0$
- *si* $\| \alpha(\alpha(\dot{\vee}, p), q) \| = 0$ *alors* $\| p \| = \| q \| = 0$
- *si* $\| \alpha(\alpha(\dot{\vee}, p), q) \| = 1$ *alors* $\| p \| = 1$ *ou* $\| q \| = 1$
- *si* $\| \alpha(\dot{\forall}_{,} p_{T \to o}) \| = 0$ *alors il existe un terme* t_T *tel que* $\| \alpha(p, t) \| = 0$
- *si* $\| \alpha(\dot{\forall}_{,} p_{T \to o}) \| = 1$ *alors pour chaque terme* t_T, $\| \alpha(p, t) \| = 1$

De même pour les autres quantificateurs.

Ici, notre semi-valuation est toute trouvée : étant donné une théorie complète, cohérente et admettant des témoins de Henkin, nous savons déjà qu'elle définit une semi-valuation sur les propositions. Nous l'étendons aux termes de type o de la façon la plus simple :

$$V(p_o) = V(\varepsilon(p_o))$$

Il nous faut vérifier que nous avons bien une semi-valuation pour les termes de type o, selon la définition 7.5. Ceci est vrai car la semi-valuation sur les propositions V est compatible avec les règles de réécriture par la définition 3.4. Par exemple, si $p = \dot{\wedge}\ q\ r$, et $V(p) = 1$, vérifions que $V(q) = V(r) = 1$:

$$1 = V(p) = V(\varepsilon(\dot{\wedge}\ qr)) = V(\varepsilon(q) \wedge \varepsilon(r)) = V(\varepsilon(q)) = V(\varepsilon(r)) = V(q) = V(r)$$

Le traitement est identique pour les autres quantificateurs, et si $p \equiv_{\mathcal{R}} q$, alors puisque $\varepsilon(p) \equiv_{\mathcal{R}} \varepsilon(q)$ aussi, nous avons forcément $V(p) = V(q)$.

7.2.2 Le domaine du modèle : les V-complexes

L'idée de prendre comme ensemble d'interprétation des termes de type o un couple composé du terme et de sa valeur de vérité possible doit être étendue à tous les termes, de manière à pouvoir gérer les types de prédicats tels que $\iota \to o$.

Cette construction n'est pas toujours très utile, en particulier dans le cas des termes de type ι. Nous conjecturons le fait que les V-complexes sont nécessaires uniquement dans le cas de termes dont le dernier type est o, par exemple $\iota \to \iota \to o$ ou bien encore $(o \to (\iota \to o)) \to (o \to o)$, mais pas $o \to \iota$. En effet, les seuls termes vraiment imprédicatifs sont ceux dont le type final est o, car seuls les termes de type o se réécrivent en propositions.

Cependant, pour des raisons d'uniformité de présentation, il est bien mieux de tout présenter comme une liste de couples.

Voici donc la définition du modèle des termes :

Définition 7.6 (V-complexes). *Soit $\mathcal{L}$ le langage d'une théorie de HOL. À chaque type simple T nous associons un ensemble, appelé V-complexe de type T :*

- *ι : l'ensemble $D_\iota = \{\langle t, \iota\rangle | t : \iota \in \mathcal{L}, t$ en forme normale$\}$*
- *o : l'ensemble $D_o = \{\langle t, b\rangle | t : o \in \mathcal{L}, b = 0$ ou $1, t$ en forme normale$\}$. Avec la condition suivante sur le booléen b : si $\varepsilon(t) \in \Gamma$ alors $b = 1$, si $\Gamma \not\vdash^{cf}_{\mathcal{R}} \varepsilon(t)$ alors $b = 0$ et sinon $b = 0$ ou $b = 1$.*
- *$T \to U$: l'ensemble $D_{T\to U} = \{\langle t, f\rangle | t : (T \to U) \in \mathcal{L}, f : D_T \to D_U\}$ tel que $f(\langle t, g\rangle) = \langle ft\downarrow, h\rangle$ pour un certain h.*

Nous nous placerons dans toute la suite dans le modèle $\mathcal{M}$ dont les ensembles de base sont les V-complexes. Nous allons tout d'abord définir l'interprétation des termes dans ce modèle, puis l'interprétation des propositions.

La première chose à vérifier est qu'à tout terme $t : T$ nous sommes capables d'associer un V-complexe de la forme $\langle t, f\rangle \in D_T$ (chaque t est habité) :

Lemme 7.1 (Forme canonique). *à tout terme $t : T$ nous pouvons associer une terme $can(t) = \langle \beta t, f_t \in D_T\rangle$*

Preuve. Par induction sur le type T :

- Si le type de t est ι, alors $can(t) = \langle \beta(t), \iota\rangle$ est un V-complexe par définition.
- Si le type de t est o, alors $can(t) = \langle \beta(t), v\rangle$ avec $v = V(t)$ si $V(t)$ est définie, et 1 sinon (0 est aussi possible et conduit à un autre modèle). Par définition, c'est aussi un V-complexe.
- Si le type de t est $U \to V$, alors $can(t) = \langle \beta(t), f_t\rangle$ avec

$$\begin{array}{rcl} f_t : D_U & \to & D_V \\ \langle u, g\rangle & \mapsto & \langle \beta(\alpha(t, u)), h_{\beta(\alpha(t,u))}\rangle \end{array}$$

  Il est immédiat de vérifier que $can(t)$ est un V-complexe (la partie fonctionnelle vérifie bien la définition 7.6).

■

Nous allons maintenant définir l'interprétation d'un terme t de type T dans le modèle, modulo un assignement σ qui à toute variable de type T associe un V-complexe de type T. Nous l'appellerons $|t|_\sigma$.

Notation. Nous noterons C^1 la première composante du V-complexe C au lieu de $\pi_1(C)$. De même, étant donné un assignement σ, nous noterons σ^1 (resp. σ^2) les assignements qui à toute variable x associent $\sigma(x)^1$ (resp. $\sigma(x)^2$).

Nous commençons par définir $|t|^1_\sigma = \beta(\sigma^1(t))$

La définition de $|t|^2_\sigma$ se fait par induction sur la structure de t :

- $t = x$ est une variable, alors $|t|^2_\sigma = \sigma(x)^2$ de telle manière que $|x|_\sigma = \sigma(x)$
- $t = c$ est une constante qui n'est ni une constante logique, ni K ni S. Alors, nous pouvons poser $|t|^2_\sigma = can(t)^2$ de telle manière que $|t|_\sigma = can(t)$.
- $t = K_{A,B}$. Nous prenons pour $|K_{A,B}|^2_\sigma$ la fonction f suivante :

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

avec h définie ainsi :

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

Montrons que $|K|_\sigma = \langle K, f\rangle$ est un V-complexe de type $A \to B \to A$. $\langle t_A, g\rangle \in \mathcal{D}_A$ par définition. Donc h est réellement une fonction de $\mathcal{D}_B$ dans $\mathcal{D}_A$ (ce que l'on avait affirmé dans sa définition). De plus, nous savons que $\beta\alpha(\alpha(K, t_A), t'_B) = t_A$ car t_A est en forme normale. Ainsi, $\langle \alpha(K, t_A), h\rangle \in \mathcal{D}_{B\to A}$, et f est réellement une fonction de $\mathcal{D}_A$ dans $\mathcal{D}_{A\to B}$. Enfin, $\alpha(K, t_A)$ est en forme β-normale, car t_A l'est. Donc f est la fonction attendue, et $\langle K, f\rangle \in \mathcal{D}_{A\to B\to A}$.

Nous voyons que pour l'instant, la définition de $|K|^2_\sigma$ correspond à la règle de réduction que nous nous étions fixés pour K. Il en est de même pour le symbole suivant.

- $t = S_{T,U,V}$. Nous posons $|S_{T,U,V}|^2_\sigma = f$ telle que :

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

avec h :

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

avec j :

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

avec l :

$$l \quad = \quad \left(g(\langle t''_T, k\rangle)^2 \left(i(\langle t''_T, k\rangle)\right)\right)^2$$

Le lecteur intéressé peut vérifier que, de la même manière qu'à l'étape précédente, $|S|_\sigma$ est bien un V-complexe. Notons encore une fois que la fonction f a été définie en accord avec la règle de réécriture associée au symbole S.

– $t = \dot{\neg}$ connecteur logique. Nous posons $| \dot{\neg} |^2_\sigma = f$:

$$\begin{array}{rcl} \mathcal{D}_o & \longrightarrow & \mathcal{D}_o \\ \langle p, v\rangle & \longrightarrow & \langle \alpha(\dot{\neg}, p), \overline{v}\rangle \end{array}$$

Où $\overline{v}$ représente l'opposée de v (1 si v vaut 0 et réciproquement). Pour vérifier qu'il s'agit bien d'un V-complexe, nous devons vérifier que $\langle \alpha(\dot{\neg}, p), \overline{v}\rangle$ est un V-complexe (de type o). Pour ceci, supposons que $V(\dot{\neg}\ p)$ est définie (le cas contraire est trivial) et égale à 1 (le cas 0 est identique). Puisque V est une semi-valuation (définition 7.5) nous savons que $V(p) = 0$. Donc $v = 0$, $\overline{v} = 1$ et $\langle \alpha(\dot{\neg}, p), \overline{v}\rangle$ est un V-complexe (car $\alpha(\dot{\neg}, p)$ est irréductible et donc en forme β-normale, p l'étant déjà par définition).
Notons que f a été définie (sur le deuxième terme) exactement comme la négation booléenne.

– $t = \dot{\vee}$ Nous procédons d'une manière identique. Soit $| \dot{\vee} |^2_\sigma$ la fonction f telle que :

$$\begin{array}{rcl} \mathcal{D}_o & \longrightarrow & \mathcal{D}_{o\to o} \\ \langle p, v_1\rangle & \longrightarrow & \langle \alpha(\dot{\vee}, p), g\rangle \end{array}$$

avec g :

$$\begin{array}{rcl} \mathcal{D}_o & \longrightarrow & \mathcal{D}_o \\ \langle q, v_2, \ \ \rangle & \longrightarrow & \langle \alpha(\alpha(\dot{\vee}, p), q), v\rangle \end{array}$$

avec $v = 1$ si $v_1 = 1$ ou si $v_2 = 1$ et 0 sinon.
Nous vérifions de même que $\langle \alpha(\alpha(\dot{\vee}, p), q), v\rangle$ est un V-complexe. Car si $V(\dot{\vee}\ p\ q)$ est définie et égale à 1 par exemple, alors, si $V(p) = 1$ et dans ce cas là, $v_1 = 1$ et donc $v = 1 = V(\dot{\vee}\ p\ q)$. L'autre cas se traite de la même manière exactement.

– $t = \dot{\wedge}$ se traite de la même manière que le cas précédent, sauf que nous posons $v = 1$ si $v_1 = 1$ et $v_2 = 1$ et 0 sinon.
Notons que la définition des deuxièmes composantes de $|t|_\sigma$ "collent" toujours très bien avec les définitions booléennes de $\vee$ et $\wedge$.

– $t = \dot{\Rightarrow}$ se traite de la même manière que les deux cas précédents, sauf que nous posons $v = 1$ si $v_1 = 0$ ou si $v_2 = 1$ et 0 sinon.

– $t = \dot{\forall}_T$. Nous posons $| \dot{\forall}_T |^2_\sigma = f$:

$$\begin{array}{rcl} \mathcal{D}_{T\to o} & \longrightarrow & \mathcal{D}_o \\ \langle p, g\rangle & \longmapsto & \langle \alpha(\dot{\forall}_{,}\ p), v\rangle \end{array}$$

avec $v = 1$ ssi pour tout V-complexe $c \in \mathcal{D}_T$, $g(c)^2 = 1$.

De même que précédemment, nous devons vérifier que le terme $|\dot{\forall}_T|_\sigma = \langle \dot{\forall}_T, f\rangle$ est bien un V-complexe. Pour cela, il faut démontrer que $\langle \alpha(\dot{\forall}_T, p), v\rangle$ est un V-complexe. Supposons que $V(\alpha(\dot{\forall}_T, p))$ soit définie et égale à 1. Dans ce cas, d'après la définition 7.5, nous savons que pour tout terme $t : T$, $V(\alpha(p,t)) = 1$. Ainsi, tout V-complexe de la forme $\langle \beta(\alpha(p,t)), b\rangle$ sera tel que $b = 1$. Or $g(c)$ est justement de cette forme-là, d'après la définition de g (définition 7.6). Donc $g(c)^2 = 1$.

De même, si $V((\alpha(\dot{\forall}_T, p)) = 0$, il existe un terme t_0 tel que $V(\alpha(p, t_0)) = 0$. Et donc, $g(can(t_0)) = \langle \beta(\alpha(p, t_0)), 0\rangle$ par définition de g et des V-complexes.

Enfin, si V n'est pas définie en $\alpha(\dot{\forall}_T, p)$, alors n'importe quelle valeur de vérité convient.

– $t = \dot{\exists}_T$ se traite de la même manière que le cas précédent, sauf que $v = 1$ ssi il existe un V-complexe $c \in \mathcal{D}_T$, $g(c) = \langle \_, 1\rangle$.
– Enfin, passons au cas où $t = \alpha(t', t'')$. Nous posons

$$|\alpha(t', t'')|^2_\sigma = |t'|^2_\sigma \left(|t''|_\sigma\right)^2$$

C'est un V-complexe, puisque $|t'|_\sigma$ et $|t''|_\sigma$ le sont. On vérifie sans problème l'égalité suivante :

$$|\alpha(t', t'')|_\sigma = |t'|^2_\sigma \left(|t''|_\sigma\right)$$

Une propriété primordiale de cette interprétation des termes est qu'elle vérifie le lemme de substitution :

Lemme 7.2 (Substitution). *Soit $p : T \to U$ tel que x ne soit pas libre dans p et $c \in \mathcal{D}_T$. Alors :*

$$|p|^2_\sigma c = |\alpha(p, x)|_{\sigma + \langle c/x\rangle}$$

Preuve. La preuve est quasi-immédiate, si l'on remarque que si x n'est pas libre dans t, alors $|t|_{\sigma+\langle c/x\rangle} = |t|_\sigma$. Ceci est assez intuitif mais demanderait une démonstration rigoureuse par induction sur la structure de t.

Nous avons la suite d'égalités :

$$\begin{aligned} |\alpha(p,x)|_{\sigma+\langle c/x\rangle} &= |p|^2_{\sigma+\langle c/x\rangle}(|x|_{\sigma+\langle c/x\rangle}) \\ &= |p|^2_\sigma(|x|_{\sigma+\langle c/x\rangle}) \\ &= |p|^2_\sigma c \end{aligned}$$

La première égalité est la définition de $|.|_\sigma$ sur des termes commençant par α. La deuxième vient de la remarque que nous avons faite plus haut (x n'est pas libre dans p), et la troisième égalité vient de la définition de $|.|_\sigma$ pour les variables. ■

Ayant défini l'interprétation des termes, nous allons maintenant définir l'interprétation des propositions :

Définition 7.7. *Soit $\mathcal{M}$ le modèle à base de V-complexes, défini à partir de la semi-valuation V, soit σ un assignement. Nous définissons l'interprétation d'une proposition de la manière suivante :*

- $|P \wedge Q|_\sigma = |P|_\sigma \wedge |Q|_\sigma$
- $|P \Rightarrow Q|_\sigma = |P|_\sigma \Rightarrow |Q|_\sigma$
- $|P \vee Q|_\sigma = |P|_\sigma \vee |Q|_\sigma$
- $|\neg P|_\sigma = \neg |P|_\sigma$
- $|\forall x_T P|_\sigma = 1$ *si pour tout V-complexe* $C \in \mathcal{D}_T$, $|P|_{\sigma+\langle C/X\rangle} = 1$ *et* 0 *sinon.*
- $|\exists x_T P|_\sigma = 1$ *si il existe un V-complexe* $C \in \mathcal{D}_T$ *tel que* $|P|_{\sigma+\langle C/X\rangle} = 1$ *et* 0 *sinon.*
- $|\varepsilon(p)|_\sigma = |p|^2_\sigma$

Remarque. Nous avons commis un abus de notation, car par exemple $|P|_\sigma \Rightarrow |Q|_\sigma$ n'est pas une valeur de vérité. Nous devrions dire 1 si $|P|_\sigma = 0$ ou $|Q|_\sigma = 1$ et 0 sinon.

Nous venons de définir l'interprétation dans un modèle, mais nous ne savons pas encore que c'est un modèle des règles de réécriture. C'est l'objet du lemme suivant.

Lemme 7.3. $\mathcal{M}$ *est un modèle des règles de réécriture.*

Preuve. Cette preuve se décompose en deux parties. Nous allons tout d'abord nous intéresser aux termes du langage, auxquels on ne peut appliquer que les règles de réécriture qui concernent S ou K. Soient donc deux termes $t \to^1 t'$ (une seule étape de réduction) d'un type T quelconque. Nous allons prouver par induction sur la structure de t que $|t|_\sigma = |t'|_\sigma$.

- t ne peut pas être ni une variable, ni une constante, car on ne pourrait pas appliquer de règle de réécriture. C'est donc une application.
- $t = \alpha(t_1, t_2)$ avec $t_1 \to^* t'_1$ ou $t_2 \to^* t'_2$ (la réduction se fait à l'intérieur des sous-termes, en au plus une étape sur chacun d'eux), nous appliquons l'hypothèse de récurrence. Ainsi :

$$|t|_\sigma = |t_1|^2_\sigma\,(|t_2|_\sigma) = |t'_1|^2_\sigma\,(|t'_2|_\sigma) = |t'|_\sigma$$

- $t = \alpha(\alpha(K, t_1), t_2) \to^1 t_2 = t'$. Grâce à notre définition de $|.|_\sigma$, nous avons les égalités suivantes :

$$|t|_\sigma = |\alpha(K, t_1)|^2_\sigma\,(|t_2|_\sigma) = |t_2|_\sigma$$

- $t = \alpha(\alpha(\alpha(S, t_1), t_2), t_3) \to \alpha(\alpha(t_1, t_3), \alpha(t_2, t_3)) = t'$. Nous avons par définition de $|S|^2_\sigma$:

$$\begin{aligned} |t|_\sigma &= |\alpha(\alpha(\alpha(S, t_1), t_2), t_3)|_\sigma \\ &= ((|S|^2_\sigma |t_1|_\sigma)^2 |t_2|_\sigma)^2 |t_3|_\sigma \\ &= (|t_1|^2_\sigma |t_3|_\sigma)^2 (|t_2|^2_\sigma |t_3|_\sigma) \\ &= |t'|_\sigma \end{aligned}$$

Nous étendons le résultat par récurrence à un nombre arbitraire de règles de réécriture $t \to^* t'$ et enfin à l'équivalence modulo $\mathcal{R}$.

Considérons maintenant deux propositions $P \to Q$. Comme cela a déjà été dit dans les chapitres précédents, nous pouvons nous restreindre aux propositions P atomiques car les règles de réécriture sont atomiques. Nous distinguons des cas suivant la règle de réécriture employée :

- $\varepsilon(p) \to \varepsilon(q)$. Alors $p \to q$ et nous sommes dans le cas d'une réécriture entre termes.
- $\varepsilon(\dot\wedge\, pq) \to \varepsilon(p) \wedge \varepsilon(q)$. Alors $|\varepsilon(p) \wedge \varepsilon(q)|_\sigma = 1$ ssi $|\varepsilon(p)|_\sigma = 1$ et $|\varepsilon(q)|_\sigma = 1$. Or :
$$|\varepsilon(\dot\wedge\, pq)|^2_\sigma = \left(|\, \dot\wedge\, |^2_\sigma (|p|_\sigma)^2 (|q|_\sigma)\right)^2 = b$$
et $b = 1$ ssi $|p|^2_\sigma = 1$ et $|q|^2_\sigma = 1$.
- $\varepsilon(\dot\vee\, pq) \to \varepsilon(p) \vee \varepsilon(q)$, $\varepsilon(\dot\Rightarrow\, pq) \to \varepsilon(p) \Rightarrow \varepsilon(q)$ et $\varepsilon(\dot\neg\, p) \to \neg\varepsilon(p)$ se traitent de la même manière.
- $\varepsilon(\dot\forall_T\, p) \to \forall_T x \varepsilon(px)$.
$|\forall x \varepsilon(px)|_\sigma = 1$ ssi pour tout V-complexe $c \in \mathcal{D}_T$, nous avons :
$$|\varepsilon(px)|_{\sigma + \langle c/x\rangle} = 1$$
ce qui, par la définition 7.7, est vrai ssi :
$$|px|^2_{\sigma + \langle c/x\rangle} = 1$$
or, d'après le lemme de substitution, nous avons :
$$|px|_{\sigma + \langle c/x\rangle} = |p|^2_\sigma c$$
Donc pour tout $c \in \mathcal{D}_T$ nous avons $(|p|^2_\sigma c)^2 = 1$, et ainsi $|\, \dot\forall_T\, p|^1_\sigma = 1$
- $\varepsilon(\dot\exists_T\, p) \to \exists_T x \varepsilon(px)$ se traite de la même manière.

Nous avons traité tous les cas possibles de réduction des propositions. La preuve du lemme est donc terminée. ■

Le modèle est un modèle des règles de réécriture. Mais est-ce un modèle de la théorie Γ de départ (celle qui avait servi à définir la semi-valuation V sur les propositions) ? Pour pouvoir répondre à cette question, nous allons prouver le lemme d'adéquation suivant :

Lemme 7.4. *Si la semi-valuation V est définie en P, alors $|P|_\sigma = V(P)$*

Preuve. Il faut le vérifier sur les termes de type o. Si P est une proposition, nous pouvons sans difficulté construire un terme p_o (par induction sur la structure de P) tel que $P \equiv_{\mathcal{R}} \varepsilon(p)$. Alors, nous avons $V(P) = V(p_o)$ par définition de la semi-valuation sur les termes. Puis, $V(p) = |p|^2_\sigma$ par définition des V-complexes de $\mathcal{D}_o$, et enfin, nous avons $|P|_\sigma = |p|^2_\sigma$ puisque $P \equiv \varepsilon(p)$. ■

Remarque. Nous avons égalité stricte entre V et l'interprétation puisque, comme nous le saurons dans un instant, V est en fait une valuation totale, et toutes les propositions ont déjà reçu une interprétation par V.

De ces deux lemmes 7.3 et 7.4, nous pouvons déduire directement le théorème de complétude forte pour la Logique d'Ordre Supérieur exprimée en déduction modulo :

Théorème 7.5. *Soit $\mathcal{R}$ le système de réécriture HOL. Si $\mathcal{T} \nvdash^{cf}_{\mathcal{R}}$ alors il existe un modèle $\mathcal{M}$ tel que $\mathcal{M} \models_{\mathcal{R}} \mathcal{T}$*

Preuve. Comme d'habitude. Nous complétons $\mathcal{T}$ en Γ, et nous définissons la semi-valuation V comme étant l'appartenance à Γ. Nous construisons le modèle $\mathcal{M}$ à base de V-complexes associé, et les lemmes 7.3 et 7.4 nous permettent de conclure. ■

Le corollaire d'élimination des coupures s'en suit, là aussi comme au chapitre 5.

Chapitre 8

Normalisation et élimination des coupures

Dans ce chapitre, nous étudions les liens entre la normalisation définie dans [17], et l'élimination des coupures sémantique telle que nous la faisons.

La normalisation implique directement l'élimination des coupures en calcul des séquents intuitionniste, puisqu'elle définit une méthode de transformation des preuves. De plus, il est démontré (voir par exemple [17]) que l'élimination des coupures en calcul des séquents modulo intuitionniste implique celle du calcul des séquents modulo classique, par le biais d'une $\neg\neg$-translation.

Dans ce chapitre, nous étudions l'existence d'une réciproque à ce résultat.

8.1 Le contre-exemple de Dowek et Werner

Dans [17], il est introduit le système défini par la règle de réécriture suivante :

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

Ici, $y \simeq z$ est un abréviation pour $\forall x(y \in x \Rightarrow z \in x)$, et $\in$ est un symbole de prédicat à deux variables.

Le système $\mathcal{R}$ défini par cette règle termine et est confluent.

Nous avons une preuve π (sans coupure) des séquents suivants (en calcul des

séquents modulo intuitionniste, donc aussi dans le cas classique) :

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

de même, nous avons une preuve intuitionniste π' du séquent suivant :

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

Les termes de preuve associé étant :

$$\begin{array}{ll} (\pi) & \lambda\alpha(\alpha R(\lambda x \lambda\beta\beta)\alpha) \\ (\pi') & \lambda y \lambda\alpha\lambda\beta(t(\pi)(\alpha R\beta)) \end{array}$$

En combinant les preuves de ces deux séquents avec la règle de coupure, nous obtenons une preuve de l'incohérence de $\mathcal{R}$:

$$\dfrac{\dfrac{\pi}{R \in R \vdash^{cf}_{\mathcal{R}}} \quad \dfrac{\pi'}{\vdash^{cf}_{\mathcal{R}} R \in R}}{\vdash_{\mathcal{R}}}$$

Or, sans la règle de coupure, nous ne pouvons pas démontrer $\vdash_{\mathcal{R}}$, car aucune règle ne peut s'appliquer. Ce système est donc incohérent, mais surtout, il ne possède ni la propriété d'élimination des coupures, ni la propriété de normalisation. Le terme de preuve $(\pi\pi')$ se réduit sur lui-même :

$$(\pi\ \pi') \rhd^* (\pi\ \pi')$$

Nous allons maintenant raffiner ce contre-exemple de manière à avoir une théorie cohérente (sinon nous ne pourrions pas avoir élimination des coupures) qui possède la propriété d'élimination des coupures.

8.2 Un premier raffinement

Un premier raffinement consiste à remplacer toutes les propositions du type $\neg P$ par $P \Rightarrow C$, avec C une proposition atomique quelconque (qui est normale pour les règles de réécriture), de même que la A-traduction est une généralisation de la $\neg$-traduction.

Nous obtenons la règle suivante, et nous définissons le système de réécriture $\mathcal{R}$ composé uniquement de cette règle :

$$R \in R \rightarrow_{\mathcal{R}} \forall y(y \simeq R \Rightarrow ((y \in R) \Rightarrow C))$$

Modulo ce système de réécriture, et de la même manière que dans la section précédente, nous avons une preuve π du séquent $R \in R \vdash^{cf}_{\mathcal{R}} C$ dans le calcul des séquents intuitionnistes modulo :

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

et une preuve intuitionniste π' du séquent suivant :

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

Les termes de preuve sont toujours les mêmes que dans la section précédente.

Nous pouvons toujours combiner π et π' et obtenons une preuve de la proposition C :

$$\dfrac{\pi \;\; \pi'}{\vdash_{\mathcal{R}} C}\ \text{coupure}$$

D'autre part, il n'existe pas de preuve de $\vdash^{cf}_{\mathcal{R}} C$ (c'est à dire sans utiliser la règle de coupure). Si une telle preuve existait, alors la première règle ne pourrait être qu'une contraction sur la proposition C, et ainsi de suite. La preuve ne pourrait donc jamais être close. Notons que C doit être normale pour les règles de réécriture sinon d'autres règles pourraient s'appliquer.

Nous ne pouvons donc toujours pas éliminer les coupures, en particulier nous n'avons pas la normalisation, et la réduction du terme de preuve $(\pi\pi')$ boucle.

Remarque. Cette règle de réécriture définit cependant un calcul des séquents modulo cohérent. Pour montrer cela, il suffirait de définir un modèle de $\mathcal{R}$ qui valide cette règle de réécriture. Cela est réalisable si l'on interprète C par 1. C'est le point de départ de la section suivante.

8.3 Déduction Modulo classique

Observons maintenant ce qui se passe si nous remplaçons C par une tautologie bien connue de la logique des prédicats : $A \vee \neg A$, avec A une proposition atomique quelconque. Nous obtenons la règle de réécriture suivante, qui formera le système de réécriture $\mathcal{R}'$:

$$R \in R \rightarrow_{\mathcal{R}} \forall y(y \simeq R \Rightarrow ((y \in R) \Rightarrow (A \vee \neg A)))$$

En calcul des séquents intuitionniste, il n'existe pas de preuve sans coupures de $\vdash^{cf}_{\mathcal{R}'} A \vee \neg A$, car la première règle s'appliquant doit forcément être $\vee$ droit, et ensuite, on se retrouve à devoir démontrer soit $\vdash^{cf}_{\mathcal{R}'} A$, soit $\vdash^{cf}_{\mathcal{R}'} \neg A$, ce qui est impossible dans les deux cas, car nous avons supposé A quelconque.

Par contre, en calcul des séquents classique, il y a la preuve triviale suivante :

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

L'idée est que le calcul des séquents classique modulo cette règle de réécriture possède la propriété d'élimination des coupures, alors que, comme nous venons de le voir, le calcul des séquents intuitionniste ne la possède pas (et donc, en particulier le processus de normalisation échoue).

Il nous reste à prouver que la règle de coupure est effectivement redondante dans le calcul des séquents modulo $\mathcal{R}'$. Pour cela, nous allons utiliser la méthode habituelle. Étant donné une théorie complète, cohérente et admettant des témoins de Henkin, nous lui construisons un modèle qui est aussi un modèle des règles de réécriture.

La construction se fait de la manière suivante : nous fixons la valeur de vérité de tous les atomes, puis nous étendons cela à toutes les propositions par induction structurelle.

Définition 8.1. *Soit Γ une théorie complète, cohérente, admettant des témoins de Henkin. Nous définissons le modèle syntaxique $\mathcal{M}$ par les valeurs de vérité des prédicats atomiques de la manière suivante :*

- *Si $\Gamma \vdash^{cf}_{\mathcal{R}'} A$, alors $|A| = 1$*
- *Sinon $|A| = 0$*

On étend de la manière habituelle la définition à toutes les propositions.

Remarquons que puisque π' est une preuve de $\vdash^{cf}_{\mathcal{R}'} R \in R$, c'est aussi une preuve de $\Gamma \vdash^{cf}_{\mathcal{R}'} R \in R$. Ainsi $|R \in R| = 1$ par définition.

Tout d'abord, nous prouvons comme dans les sections 5.2.1 et 5.2.2 que $\mathcal{M}$ est un modèle de Γ. Nous renvoyons à ces sections pour de plus amples détails, par exemple à la preuve du lemme 5.6.

Nous devons donc prouver que $\mathcal{M}$ est un modèle de $\mathcal{R}'$. Pour ce faire, nous regardons la seule règle de $\mathcal{R}'$, et puisque nous connaissons déjà l'interprétation de $R \in R$, nous devons prouver que $|\forall y(y \simeq R \Rightarrow ((y \in R) \Rightarrow (A \vee \neg A)))| = 1$.

Or nous savons que $|A \vee \neg A|$ vaut 1, car soit A, soit $\neg A$ valent 1. Donc, pour tout terme clos t, $((t \in R) \Rightarrow (A \vee \neg A))$ est vraie. Ce qui implique que $|(t \simeq R \Rightarrow ((t \in R) \Rightarrow (A \vee \neg A))| = 1$. Ceci prouve ce que nous voulions :

$$|\forall y(y \simeq R \Rightarrow ((y \in R) \Rightarrow (A \vee \neg A)))| = 1$$

Donc, le calcul des séquents classique modulo $\mathcal{R}'$ a la propriété d'élimination des coupures.

Cependant, ce calcul ne peut pas normaliser, car la normalisation implique l'élimination des coupures dans le calcul des séquents intuitionniste, et par la $\neg\neg$-traduction légère de Dowek et Werner [17], l'élimination des coupures intuitionniste implique l'élimination des coupures classique.

Ceci est dû au fait que dans notre preuve d'élimination des coupures, nous avons utilisé fortement le fait que $A \vee \neg A$ est une tautologie classique. Nous avons donc des outils sémantiques à notre disposition que nous n'avons pas lors de la définition du processus de normalisation.

Nous pouvons aussi faire la remarque que la preuve sans coupures de $\vdash^{cf}_{\mathcal{R}'} A \vee \neg A$ n'a rien à voir avec celle avec coupure.

Nous avons donc établi que la normalisation, ainsi que l'élimination des coupures dans le cas intuitionniste était une propriété plus forte que l'élimination des coupures dans le cas classique. Nous allons maintenant comparer normalisation et élimination des coupures dans le cas intuitionniste.

8.4 Déduction Modulo intuitionniste

Remplaçons maintenant C par une tautologie intuitionniste :$A \Rightarrow A$.

Nous obtenons la règle de réécriture suivante :

$$R \in R \rightarrow_{\mathcal{R}} \forall y(y \simeq R \Rightarrow ((y \in R) \Rightarrow (A \Rightarrow A))$$

On a toujours les même termes de preuve π et π' pour prouver les deux séquents suivant :

$$\begin{array}{lll} R \in R & \vdash^{cf}_{\mathcal{R}} & C \\ & \vdash^{cf}_{\mathcal{R}} & R \in R \end{array}$$

Si nous les combinons avec la règle de coupure, nous obtenons une preuve du séquent $\vdash_{\mathcal{R}} A \Rightarrow A$.

Le procédé de normalisation boucle encore dans cette théorie. Les termes de preuve sont en effet incapables de distinguer la proposition C de la proposition $A \Rightarrow A$, et de savoir, dans ce cas précis, que c'est une tautologie intuitionniste. Encore une fois, nous avons à notre disposition des informations sémantiques inaccessibles aux termes de preuve.

Le théorème de complétude forte reste ainsi valide : pour une théorie Γ B-complète, B-cohérente et admettant des B-témoins de Henkin, nous définissons une structure de Kripke exactement comme dans la définition 6.2 de la section 6.2.2.

Alors, nous avons bien $\Gamma \Vdash \Gamma$ et $\Gamma \nVdash B$, de la même manière que dans la section 6.2.2.

Mais, toujours comme dans cette section, il faut montrer que la structure de Kripke définie est un modèle des règles de réécriture, en l'occurrence, de la règle de réécriture.

Puisque le séquent $\vdash^{cf}_{\mathcal{R}} R \in R$ a une preuve, et de par la définition de notre structure de Kripke ($R \in R$ est une proposition atomique), nous savons que pour tout monde Δ, $\Delta \Vdash R \in R$. Reste à montrer que :

$$\Delta \Vdash \forall y(y \simeq R \Rightarrow (y \in R \Rightarrow (A \Rightarrow A)))$$

Ceci est laissé en exercice au lecteur intéressé, et se démontre quasiment de la même manière qu'à la section précédente.

Ainsi, le théorème d'élimination des coupures est vrai, bien que celui de normalisation soit faux.

Le raffinement du contre-exemple de Dowek et Werner [17] peut être comparé à l'approche de Dowek dans [13], qui montre que, dans le calcul des séquents asymétrique, la normalisation n'est pas équivalente à l'élimination des coupures. Il y raffine une contre-exemple de Newman. Nous obtenons un résultat plus fort puisque nous travaillons dans le calcul de séquents modulo *symétrique avec règles propositionnelles*.

Nous obtenons un résultat négatif : la normalisation est une propriété plus forte que l'élimination des coupures. De plus, nous avons aussi montré que l'élimination des coupures dans un cadre intuitionniste est une propriété elle aussi plus forte que l'élimination des coupures dans le cas classique.

En particulier, les méthodes sémantiques ne sont pas une version affaiblie des méthodes de normalisation, car elles permettent de démontrer la propriété d'élimination des coupures pour un plus grand nombre de systèmes.

Quatrième partie

Démonstration Automatique

Chapitre 9

La Résolution Modulo

9.1 ENAR, un système de résolution

La déduction modulo est un formalisme bien adapté à la recherche de preuve, du fait de l'introduction de règles de réécriture. C'est pourquoi il est intéressant de définir des méthodes efficaces de recherche de preuve, telles que la construction de tableaux ou la résolution. Ces méthodes sont en général plus rapides que la recherche de preuve d'un séquent. Mais il faut prouver leur correction et leur complétude par rapport au calcul des séquents.

ENAR est un système de déduction qui étend la résolution des formes clausales aux théories avec des règles de réécriture.

Dans le chapitre 5, nous introduisons une condition d'ordre (section 5.2.1). Stuber, dans [41], prouve la complétude de ENAR par rapport au calcul des séquents par des méthodes sémantiques, avec cette même condition.

Dowek, Hardin et Kirchner dans [16] ont prouvé la complétude de ENAR par rapport au calcul des séquents sans coupure, et un théorème de correction par rapport au calcul des séquents *avec* coupure. Le but de ce chapitre est de raffiner le résultat et de démontrer la correction forte de ENAR par rapport au calcul des séquents sans coupure.

Les règles de déduction en ENAR s'appliquent sur un ensemble d'ensembles de propositions atomiques ou leur négation, que l'on appelle une clause. Il existe des règles permettant d'écrire une proposition quelconque du calcul des séquents dans sa forme clausale, elles sont présentées dans la figure 9.1.

Notons que dans cette section, nous considérons des règles supplémentaires $\mathcal{E}$ qui ne sont pas des règles de réécriture, mais des règles d'équivalence entre les propositions. Formellement, $\mathcal{E}$ est un ensemble de paires $t = r$, chacune d'entre elles est un axiome équationnel.

Exemple d'axiome équationnel :

$$x + (y + z) = (x + y) + z$$

On note $=_{\mathcal{E}}$ la congruence générée par les égalités de $\mathcal{E}$, telle que si $P =_{\mathcal{E}} Q$ alors P et Q ont les mêmes variables libres.

La définition d'équivalence $\equiv_{\mathcal{RE}}$ est redéfinie en conséquence :

Définition 9.1. *Soit un système de réécriture $\mathcal{RE}$, la proposition P se réécrit en P' dans $\mathcal{RE}$ si :*
$P =_{\mathcal{E}} Q$, $Q_{|\omega} = \sigma(l)$ et $P' =_{\mathcal{E}} Q[\sigma(r)]_\omega$, pour une règle $l \to r \in \mathcal{R}$, une certaine proposition Q, une certaine occurrence ω dans Q et une certaine substitution σ. Quand on applique σ, nous renommons les variables liées pour éviter la capture le cas échéant.

Tous les résultats syntaxiques du chapitre 3 restent valides pour cette formulation de la déduction modulo, et les preuves sont exactement les mêmes. Nous les étendrons légèrement dans la section 9.3.1, pour avoir des résultats plus précis sur la hauteur des preuves.

9.1.1 Les formes clausales

Pour travailler en résolution modulo (l'autre nom de ENAR), nous devons d'abord définir, de la même manière que dans [16] ce qu'est la forme clausale d'une proposition P.

Définition 9.2. *Soit P une proposition et l une liste des variables libres de P, appelée label.*
Une proposition labellée est une paire $\langle P, l\rangle$, notée P^l.

Définition 9.3. *Soit θ une substitution. Quand on applique θ à une proposition labellée, on remplace dans le label chaque variable x par la liste des variables libres de θx.*
Une proposition labellée P^l est $\mathcal{E}$-équivalente à une proposition labellée $Q^{l'}$ si $P =_{\mathcal{E}} Q$ et $l = l'$.

Définition 9.4 (Clause). *Une clause est un ensemble de propositions labellées telles que chacune de ces propositions soit un littéral, c'est à dire un atome, ou bien sa négation.*
On note la clause vide $\Box$.

Donnons les règles qui permettent de calculer la forme clausale d'une proposition. La forme clausale est un ensemble de clauses. Avec les règles de la figure 9.1, nous pouvons calculer la forme clausale de n'importe quelle proposition. Ces règles s'appliquent sur des ensembles d'ensembles de propositions. Nous noterons $cl(P_1, ..., P_n)$ le résultat de la mise en forme clausale de $\{\{P_1\}, ..., \{P_n\}\}$.

Définition 9.5 (proposition associée à une clause sans labels). *Soit $\psi = \{P_1, ..., P_n\}$ un ensemble de propositions. On note $\overline{\psi} = P_1 \vee (P_2 \vee (... \vee P_n))$.*

Définition 9.6 (proposition close associée à une clause). *Soit un ensemble de propositions labellées $\psi = \{P_1^{l_1}, ..., P_n^{l_n}\}$. On suppose avoir un ordre total sur*

$$
\begin{array}{rcl}
\Phi, (\psi, (P \wedge Q)^l) & \longrightarrow & \Phi, (\psi, P^l), (\psi, Q^l) \\
\Phi, (\psi, (P \vee Q)^l) & \longrightarrow & \Phi, (\psi, P^l, Q^l) \\
\Phi, (\psi, (P \Rightarrow Q)^l) & \longrightarrow & \Phi, (\psi, (\neg P)^l, Q^l) \\
\Phi, (\psi, \bot^l) & \longrightarrow & \Phi, \psi \\
\Phi, (\psi, (\forall x P)^{y_1,\ldots,y_n}) & \longrightarrow & \Phi, (\psi, P^{y_1,\ldots,y_n,x}), (**) \\
\Phi, (\psi, (\exists x P)^{y_1,\ldots,y_n}) & \longrightarrow & \Phi, (\psi, (\{f(y_1,...,y_n)/x\}P)^{y_1,\ldots,y_n}), (*) \\
\Phi, (\psi, (\neg(P \vee Q))^l) & \longrightarrow & \Phi, (\psi, (\neg P)^l), (\psi, (\neg Q)^l) \\
\Phi, (\psi, (\neg(P \wedge Q))^l) & \longrightarrow & \Phi, (\psi, (\neg P)^l, (\neg Q)^l) \\
\Phi, (\psi, (\neg(P \Rightarrow Q))^l) & \longrightarrow & \Phi, (\psi, P^l), (\psi, (\neg Q)^l) \\
\Phi, (\psi, (\neg\bot)^l) & \longrightarrow & \Phi \\
\Phi, (\psi, (\neg\exists x P)^{y_1,\ldots,y_n}) & \longrightarrow & \Phi, (\psi, (\neg P)^{y_1,\ldots,y_n,x}), (**) \\
\Phi, (\psi, (\neg\forall x P)^{y_1,\ldots,y_n}) & \longrightarrow & \Phi, (\psi, (\neg\{f(y_1,...,y_n)/x\}P)^{y_1,\ldots,y_n}), (*) \\
\Phi, (\psi, (\neg\neg P)^l) & \longrightarrow & \Phi, (\psi, P^l)
\end{array}
$$

$(*)$: f est un symbole de fonction qui n'apparaît dans aucune clause de Φ, ni dans ψ, ni dans P (symbole de Skolem).
$(**)$: x est une variable fraîche.

FIG. 9.1 – règles de la mise en forme clausale

le nom des variables (par ex. l'ordre alphabétique). Soit $S = l_1 \cup ... \cup l_n$ *l'ensemble des variables apparaissant dans les labels.*

Nous posons :

$$\overline{\forall}\psi \quad := \quad \forall x_1 ... \forall x_n \overline{\psi}$$

où les quantifications se font par ordre croissant.

Remarquons que nous quantifions universellement sur les variables libres (c'est à dire les variables des labels).

9.1.2 Les règles d'inférence ENAR

Définition 9.7. *Soit un système d'équations* $\mathcal{E}$*. Une équation modulo* $\mathcal{E}$ *est une paire de termes ou de propositions atomiques* $t =^?_{\mathcal{E}} t'$*.*
Une clause avec contraintes $U[\mathcal{C}]$ *est une clause* U *et un ensemble d'équations* $\mathcal{C}$*, que l'on appelle* contraintes*.*

Les règles de déduction sont données dans la figure 9.2.

Extended Resolution

$$\frac{\{P_1, ..., P_n, Q_1, ..., Q_m\}[\mathcal{C}_1] \quad \{R_1, ..., R_p, S_1, ..., S_q\}[\mathcal{C}_2]}{\{Q_1, ..., Q_m, S_1, ..., S_q\}[\mathcal{C}_1 \cup \mathcal{C}_2 \cup \{P_1 =^?_{\mathcal{E}} ... =^?_{\mathcal{E}} P_n =^?_{\mathcal{E}} R_1 =^?_{\mathcal{E}} ... =^?_{\mathcal{E}} R_p\}]}$$

Extended Narrowing

$$\frac{U[\mathcal{C}]}{U'[\mathcal{C} \cup \{U_{|\omega} =^?_{\mathcal{E}} l\}]} \text{ si } l \to r \in \mathcal{R}, U_{|\omega} \text{ atomique, et } U' \in cl(\{U[r]_\omega\})$$

FIG. 9.2 – Règles d'inférence de ENAR

9.1.3 Correction et complétude de ENAR

Dowek, Hardin et Kirchner ont prouvé que si un système de réécriture possédait la propriété d'élimination des coupures, alors ENAR était correcte et complète, c'est à dire qu'on a une démonstration de :

$$\Gamma \vdash_{\mathcal{RE}} \Delta$$

si et seulement si on a une dérivation de :

$$cl(\Gamma, \neg\Delta) \hookrightarrow \Box[\mathcal{C}]$$

avec $\mathcal{C}$ un ensemble de contraintes $\mathcal{E}$-unifiable.

Plus précisément, ils ont prouvé que si on avait une preuve sans coupures de :

$$\Gamma \vdash_{\mathcal{RE}} \Delta$$

alors on pouvait trouver une dérivation dans ENAR de :

$$cl(\Gamma, \neg\Delta) \hookrightarrow \Box[\mathcal{C}]$$

avec $\mathcal{C}$ un ensemble de contraintes $\mathcal{E}$-unifiable.
Et inversement, si on a une dérivation dans ENAR de la forme précédente, alors on a une preuve de :

$$\Gamma \vdash_{\mathcal{RE}} \Delta$$

qui peut éventuellement comporter des coupures (mais grâce à la propriété d'élimination des coupures, nous pouvons trouver une démonstration de ce séquent sans coupure).

9.1.4 ENAR et le calcul des séquents sans coupure

Dans ENAR, on ne peut pas trouver de dérivation de

$$\emptyset \hookrightarrow \Box$$

Ce qui revient à dire que pour un certain système de règles de réécriture, si on a le théorème de complétude de ENAR vis à vis de la déduction modulo, alors on ne peut pas trouver de démonstration de :

$$\vdash_{\mathcal{RE}}$$

Donc, la déduction modulo $\mathcal{RE}$ est cohérente.

Malheureusement, dans la preuve de complétude de ENAR, on utilise fortement l'hypothèse que le système de réécriture possède la propriété d'élimination des coupures. Qui plus est, dans la preuve de correction, on transforme une dérivation dans ENAR en une démonstration en calcul des séquents qui en général comporte un grand nombre de coupures.

Nous démontrons ici que les systèmes pour lesquels ENAR (la résolution modulo) est correct sont exactement ceux qui possèdent la propriété d'élimination des coupures :
Si on a une dérivation de :

$$cl(\Gamma, \neg\Delta) \hookrightarrow \Box$$

alors on a une preuve sans coupure de :

$$\Gamma \vdash_{\mathcal{RE}} \Delta$$

Avec le résultat de complétude de [16], nous aurons alors trouvé une caractérisation de ENAR qui sera satisfaisante : ENAR correspond au fragment du calcul des séquents sans coupure (y compris et surtout si le système de réécriture ne possède pas la propriété d'élimination des coupures).

9.1.5 Le système EIR

Le système EIR (Extended Identical Resolution) a été introduit dans la démonstration de la complétude et de la correction du système de déduction ENAR dans [16].
C'est un système intermédiaire et complètement équivalent à ENAR. Il s'applique lui aussi sur des ensembles de clauses, comme ENAR.

Nous travaillerons sur le système EIR, car si nous arrivons à prouver que toute dérivation dans EIR se réécrit en preuve sans coupures en déduction modulo, alors on n'aura plus qu'à étendre le résultat à ENAR.

EIR a les règles d'inférence données dans la figure 9.3.

$$\frac{U}{\{x \mapsto t\}U} \quad \textbf{Instantiation}$$

$$\frac{U}{U'} \quad \textbf{Conversion} \text{ si } U =_{\mathcal{E}} U'$$

$$\frac{U, P^{l_1} \quad U', \neg P^{l_2}}{U \cup U'} \quad \textbf{Identical Resolution}$$

$$\frac{U}{U'} \quad \textbf{Reduction} \text{ si } U \rightarrow_{\mathcal{R}} \psi \text{ et } U' \in cl(\psi)$$

FIG. 9.3 – Règles d'inférence de EIR

Définition 9.8. *Soit un système de règles de réécriture $\mathcal{RE}$ et un ensemble de clauses $\mathcal{K}$. Nous écrirons :*

$$\mathcal{K} \hookrightarrow_{\mathcal{RE}} U$$

si la clause U peut être déduite des clauses de $\mathcal{K}$ en utilisant un nombre fini de fois les règles d'inférence de EIR.
C'est à dire, il existe $U_1, ..., U_n$ telles que si $n = 0$, $U \in \mathcal{K}$, et si $n \geq 1$, pour tout $p \in [1..n]$, U_p est déduit de $\mathcal{K}, U_1, ..., U_{p-1}$ par l'application d'une des règles d'inférence de EIR.

Remarque. Sur les règles d'inférence de EIR :
- dans la règle **Instantiation**, on remplace dans les labels la variable instanciée par les variables libres du terme substitué.
- En ce qui concerne la règle **Conversion**, les labels restent inchangés, grâce à la condition imposée sur la conversion $=_{\mathcal{E}}$ que les variables libres des membres droit et gauche sont les mêmes.
- Dans la règle **Reduction**, les labels sont modifiés par la mise en forme clausale.
- Dans la règle **Identical Resolution**, on peut éliminer deux propositions n'ayant pas le même label.

Nous allons donc démontrer le théorème suivant :

Théorème 9.1. *Soient* Γ, Δ *des ensembles de propositions. Si dans EIR :*

$$cl(\Gamma, \neg\Delta) \hookrightarrow \Box$$

alors on a une dérivation sans coupure de :

$$\Gamma \vdash_{\mathcal{RE}} \Delta$$

Dans la démonstration de ce théorème, il apparaît crucial que les règles de réécriture soient asymétriques, ce qui peut se comprendre intuitivement par le fait que les dérivations de EIR sont elles aussi asymétriques (règle **Reduction**).C'est pourquoi nous utiliserons le calcul des séquents asymétrique sans coupure.

Nous prouverons ce théorème en rajoutant un axiome, l'axiome de Skolem 9.1. Nous conjecturons que cet axiome est démontrable. Il est déjà démontré si on retire la condition "sans coupures".

9.2 Calcul des séquents modulo utilisé

Dans toute cette partie, nous nous placerons dans le calcul des séquents modulo asymétrique sans coupure de la figure 2.5, où nous restreignons les règles axiome, affaiblissement et $\bot$-g à être atomiques et à s'appliquer à un contexte vide, et où nous enlevons la règle de coupure.

De plus, nous n'utiliserons pas la présentation de la figure 2.5, mais plutôt celle avec règles de conversion, de manière à coller au plus près à EIR (figure 9.3), qui possède explicitement une règle de conversion. Cette présentation est résumée figure 9.4. Remarquons encore que ce calcul est présenté directement sans la règle de coupure.

Nous supposerons aussi que $\mathcal{RE}$ est confluent.

La taille se réfère à la hauteur de l'arbre de démonstration.

Rappelons que le système de la figure 2.5, restreint de la manière dont nous l'avons fait est équivalent au calcul des séquents modulo classique usuel, de par la confluence. Nous travaillons dans ce système de manière à prouver certains lemmes par récurrence sur la taille des démonstrations, qui ne seraient pas prouvables dans d'autres systèmes tels que celui que nous utilisions jusqu'alors (figure 2.4).

Rappelons aussi que le lemme de Kleene 3.3 et le lemme 3.1 sont valables.

9.3 Du calcul des séquents vers la résolution

Une clause est un ensemble de littéraux : ils n'ont pas d'ordre. Or, tous les connecteurs sont binaires, et en principe $A \vee (B \vee C)$ n'est pas la même chose que

$$\frac{}{P \vdash^{cf}_{\mathcal{RE}} P}\text{axiome, } P \text{ atomique}$$

$$\frac{\Gamma, P, P \vdash^{cf}_{\mathcal{RE}} \Delta}{\Gamma, P \vdash^{cf}_{\mathcal{RE}} \Delta}\text{contr-g}$$

$$\frac{\Gamma \vdash^{cf}_{\mathcal{RE}} P, P, \Delta}{\Gamma \vdash^{cf}_{\mathcal{RE}} P, \Delta}\text{contr-d}$$

$$\frac{\Gamma \vdash^{cf}_{\mathcal{RE}} \Delta}{\Gamma, P \vdash^{cf}_{\mathcal{RE}} \Delta}\text{affaiblissement-g, } P \text{ atomique}$$

$$\frac{\Gamma \vdash^{cf}_{\mathcal{RE}} \Delta}{\Gamma \vdash^{cf}_{\mathcal{RE}} P, \Delta}\text{affaiblissement-d, } P \text{ atomique}$$

$$\frac{\Gamma, P, Q \vdash^{cf}_{\mathcal{RE}} \Delta}{\Gamma, P \wedge Q \vdash^{cf}_{\mathcal{RE}} \Delta} \wedge\text{-g}$$

$$\frac{\Gamma \vdash^{cf}_{\mathcal{RE}} P, \Delta \quad \Gamma \vdash^{cf}_{\mathcal{RE}} Q, \Delta}{\Gamma \vdash^{cf}_{\mathcal{RE}} P \wedge Q, \Delta} \wedge\text{-d}$$

$$\frac{\Gamma, P \vdash^{cf}_{\mathcal{RE}} \Delta \quad \Gamma, Q \vdash^{cf}_{\mathcal{RE}} \Delta}{\Gamma, P \vee Q \vdash^{cf}_{\mathcal{RE}} \Delta} \vee\text{-g}$$

$$\frac{\Gamma \vdash^{cf}_{\mathcal{RE}} P, Q, \Delta}{\Gamma \vdash^{cf}_{\mathcal{RE}} P \vee Q, \Delta} \vee\text{-d}$$

$$\frac{\Gamma \vdash^{cf}_{\mathcal{RE}} P, \Delta \quad \Gamma, Q \vdash^{cf}_{\mathcal{RE}} \Delta}{\Gamma, P \Rightarrow Q \vdash^{cf}_{\mathcal{RE}} \Delta} \Rightarrow\text{-g}$$

$$\frac{\Gamma, P \vdash^{cf}_{\mathcal{RE}} Q, \Delta}{\Gamma \vdash^{cf}_{\mathcal{RE}} P \Rightarrow Q, \Delta} \Rightarrow\text{-d}$$

$$\frac{\Gamma \vdash^{cf}_{\mathcal{RE}} P, \Delta}{\Gamma, \neg P \vdash^{cf}_{\mathcal{RE}} \Delta}\neg\text{-g}$$

$$\frac{\Gamma, P \vdash^{cf}_{\mathcal{RE}} \Delta}{\Gamma \vdash^{cf}_{\mathcal{RE}} \neg P, \Delta}\neg\text{-d}$$

$$\frac{}{\bot \vdash^{cf}_{\mathcal{RE}} P}\bot\text{-g, } P \text{ atomique}$$

$$\frac{\Gamma, \{t/x\}P \vdash^{cf}_{\mathcal{RE}} \Delta}{\Gamma, \forall x P \vdash^{cf}_{\mathcal{RE}} \Delta}\forall\text{-g}$$

$$\frac{\Gamma \vdash^{cf}_{\mathcal{RE}} \{c/x\}P, \Delta}{\Gamma \vdash^{cf}_{\mathcal{RE}} \forall x P, \Delta}\forall\text{-d, } c \text{ constante fraîche}$$

$$\frac{\Gamma, \{c/x\}P \vdash^{cf}_{\mathcal{RE}} \Delta}{\Gamma, \exists x P \vdash^{cf}_{\mathcal{RE}} \Delta}\exists\text{-g, } c \text{ constante fraîche}$$

$$\frac{\Gamma \vdash^{cf}_{\mathcal{RE}} \{t/x\}P, \Delta}{\Gamma \vdash^{cf}_{\mathcal{RE}} \exists x P, \Delta}\exists\text{-d}$$

$$\frac{\Gamma, P \vdash^{cf}_{\mathcal{RE}} \Delta}{\Gamma, Q \vdash^{cf}_{\mathcal{RE}} \Delta}\text{conversion-g si } Q \rightarrow_{\mathcal{RE}} P$$

$$\frac{\Gamma \vdash^{cf}_{\mathcal{RE}} P, \Delta}{\Gamma \vdash^{cf}_{\mathcal{RE}} Q, \Delta}\text{conversion-d si } Q \rightarrow_{\mathcal{RE}} P$$

FIG. 9.4 – Règles d'inférence du calcul des séquents modulo asymétrique

$(A \vee B) \vee C$ (avoir une preuve de l'un implique-t-il le fait d'avoir une preuve de l'autre ?). C'est ce genre de résultats que nous allons prouver dans cette section.

Tous ces résultats sont très importants dans notre cas, et ont été ignorés dans les travaux de démonstration du théorème de correction précédents, car ils sont immédiats *dès qu'on s'autorise à utiliser la règle de coupure*. Or notre but est justement de ne pas utiliser cette règle.

9.3.1 Disjonction

Conséquences du lemme de Kleene

Nous renforçons dans cette section le lemme de Kleene 3.3 avec des informations sur la hauteur des démonstrations. Comme nous sommes en déduction modulo avec règles axiome, affaiblissement et $\bot$-g atomiques, la hauteur des preuves décroît, ce qui sera important pour la suite (car nous faisons des récurrences sur la hauteur des démonstrations).

Lemme 9.2. *Soit une démonstration de :*

$$\Gamma,\ \exists x_1 P_1,\ ...,\ \exists x_n P_n \vdash^{cf}_{\mathcal{RE}} \Delta$$

alors il existe une démonstration du séquent :

$$\Gamma, \{c_1/x_1\}P_1,\ ..., \{c_n/x_n\}P_n \vdash^{cf}_{\mathcal{RE}} \Delta$$

de taille inférieure de n au moins, $c_1, ...c_n$ étant des constantes fraîches.

Preuve. La même que celle du lemme de Kleene. On vérifie que la hauteur de la démonstration diminue, et ce, grâce au fait que nous avons des règles axiome, affaiblissement et $\bot$-gauche *atomiques* (figure 9.4) : ainsi, la première règle de la démonstration ne peut pas être une de ces trois règles là.

- Si la première règles est $\vee$-g :
  Par hypothèse de récurrence on obtient des démonstrations θ et θ' des séquents :

  $$\Gamma, A, \{c_1/x_1\}P_1, ..., \{c_n/x_n\}P_n \vdash^{cf}_{\mathcal{RE}} \Delta$$
  $$\Gamma, B, \{c'_1/x_1\}P_1, ..., \{c'_n/x_n\}P_n \vdash^{cf}_{\mathcal{RE}} \Delta$$

  de taille inférieure de n au moins.

  Choisissons $d_1, ..., d_n$ des constantes entièrement fraîches par rapport à θ et θ'. Nous substituons dans θ et θ' :
  - $c_1, ..., c_n$ par $d_1, ..., d_n$.
  - $c'_1, ..., c'_n$ par $d_1, ..., d_n$.

  Puis on applique la règle $\vee$-gauche.
- Si la première règle est une contraction sur $\exists x_1 P_1$, alors nous appliquons l'hypothèse de récurrence.

– Si la première règle est ∃-gauche sur $\exists x_1 P_1$, alors nous avons la preuve :

$$\dfrac{\dfrac{\theta}{\Gamma, \{c_1/x_1\}P_1,\ \exists x_2 P_2,\ ...,\ \exists x_n P_n \vdash^{cf}_{\mathcal{RE}} \Delta}}{\Gamma,\ \exists x_1 P_1,\ ...,\ \exists x_n P_n \vdash^{cf}_{\mathcal{RE}} \Delta}$$

Nous appliquons l'hypothèse de récurrence sur θ et obtenons une preuve de taille inférieur à celle de $\Gamma,\ \exists x_1 P_1,\ ...,\ \exists x_n P_n \vdash^{cf}_{\mathcal{RE}} \Delta$ de $(n-1)+1 = n$.

– C'est une règle de conversion sur $\exists x_1 P_1 \rightarrow^* Q_1$. D'après le lemme 3.1, Q_1 est encore une proposition $\exists x_1 P'_1$ avec $P_1 \rightarrow P'_1$. Nous appliquons l'hypothèse de récurrence sur la preuve de :

$$\Gamma,\ \exists x_1 P'_1,\ ...,\ \exists x_n P_n \vdash^{cf}_{\mathcal{RE}} \Delta$$

puis la règle de conversion.

– Si c'est une règle sur une des propositions de Γ, Δ, alors nous pouvons appliquer l'hypothèse de récurrence.

– De même pour les autres règles.

La taille inférieure de n au moins est obtenue grâce au fait que nous n'autorisons que les axiomes et les affaiblissements sur des propositions atomiques, et donc, que nous rencontrons forcément ∃-g sur $\exists x_1 P_1$. ■

De la même manière, si nous appliquons le lemme de Kleene à une preuve du séquent :

$$\Gamma, A \vee B \vdash^{cf}_{\mathcal{RE}} \Delta$$

alors nous obtenons des preuves des séquents :

$$\begin{array}{lll} \Gamma, A & \vdash^{cf}_{\mathcal{RE}} & \Delta \\ \Gamma, B & \vdash^{cf}_{\mathcal{RE}} & \Delta \end{array}$$

de taille strictement inférieure.

Permutation des propositions

Du lemme de Kleene 3.3 sur les propositions ∨ à gauche, on peut déduire le corollaire suivant, qui désambiguïse l'écriture sans parenthèses d'une proposition $P_1 \vee ... \vee P_n$:

Corollaire 9.3. *Si on a une démonstration du séquent :*

$$\Gamma, P_1 \vee (... \vee P_n)...) \vdash^{cf}_{\mathcal{RE}} \Delta$$

alors pour toute permutation σ *de* $[1..n]$ *on a une démonstration de :*

$$\Gamma, P_{\sigma(1)} \vee (... \vee P_{\sigma(n)})...) \vdash^{cf}_{\mathcal{RE}} \Delta$$

Preuve. Par récurrence sur le nombre n de propositions. Le cas initial $n = 2$ vient du lemme de Kleene.

Soient $m = \sigma(1)$ et $l = \sigma^{-1}(1)$. On applique le lemme 3.3 de Kleene et obtient deux démonstrations des séquents :

$$\Gamma, P_1 \vdash^{cf}_{\mathcal{RE}} \Delta$$
$$\Gamma, P_2 \vee (... \vee P_n)...) \vdash^{cf}_{\mathcal{RE}} \Delta$$

Par hypothèse de récurrence la deuxième démonstration est équivalente à :

$$\Gamma, P_{\sigma(1)} \vee (...(P_{\sigma(l-1)} \vee (P_{\sigma(l+1)} \vee (... \vee P_{\sigma(n)})...) \vdash^{cf}_{\mathcal{RE}} \Delta$$

On applique encore une fois le lemme 3.3, et on obtient des démonstrations des trois séquents :

$$\Gamma, P_1 \vdash^{cf}_{\mathcal{RE}} \Delta$$
$$\Gamma, P_{\sigma(1)} \vdash^{cf}_{\mathcal{RE}} \Delta$$
$$\Gamma, P_{\sigma(2)} \vee (...(P_{\sigma(l-1)} \vee (P_{\sigma(l+1)} \vee (... \vee P_{\sigma(n)})...) \vdash^{cf}_{\mathcal{RE}} \Delta$$

On recombine la première et la troisième démonstration, on réutilise encore une fois l'hypothèse de récurrence et on obtient deux démonstrations de :

$$\Gamma, P_{\sigma(1)} \vdash^{cf}_{\mathcal{RE}} \Delta$$
$$\Gamma, P_{\sigma(2)} \vee (...(P_{\sigma(l-1)} \vee (P_{\sigma(l)} \vee (P_{\sigma(l+1)} \vee (... \vee P_{\sigma(n)})...) \vdash^{cf}_{\mathcal{RE}} \Delta$$

Et enfin, on combine ces deux démonstrations et on obtient ce que l'on cherchait. Notons que la taille de la démonstration peut s'en trouver allongée. ■

Remarque. Grâce à ce corollaire, nous pourrons travailler dans toute la suite de cette partie sans nous soucier du parenthésage en ce qui concerne le signe $\vee$ à gauche. Nous pourrons le faire quand le parenthésage réel n'est pas important. Le corollaire assure l'équiprouvabilité de tous les parenthésages possibles.

Nous pourrons travailler de cette manière tant que l'on n'aura pas à tenir compte de la taille de l'arbre de démonstration.

9.3.2 L'axiome de Skolem

Axiome 9.1 (Skolem). *Il existe une démonstration de :*

$$\Gamma, \forall x_1 ... \forall x_n \exists y P \vdash^{cf}_{\mathcal{RE}} \Delta$$

si et seulement si il existe une démonstration de :

$$\Gamma, \forall x_1 ... \forall x_n \{f(x_1, ..., x_n)/y\} P \vdash^{cf}_{\mathcal{RE}} \Delta$$

f symbole de fonction frais, i.e. qui n'apparaît pas dans Γ, P *et* Δ.

Comme déjà remarqué dans le chapitre 4 précédent, il n'existe pas de preuve de ce résultat pour le moment, car nous avons ici besoin du calcul des séquents modulo sans coupure. Prouver le théorème de Skolem par des méthodes syntaxiques est équivalent à avoir le théorème d'élimination des coupures (via le théorème de complétude forte), or nous supposons justement que ce n'est pas forcément le cas. De plus, les méthodes sémantiques actuellement existantes ne permettent pas d'avoir le résultat dans le calcul des séquents modulo sans coupure.

9.3.3 Les quantifications

Nous démontrons des résultats qui seront utiles lorsque nous manipulerons des quantificateurs. De même que dans la partie précédente, nous n'aurions pas besoin de démontrer ces résultats si nous nous autorisions à utiliser la règle de coupure.

C'est la partie la plus fastidieuse de la preuve. Il est normal qu'elle concerne les quantificateurs, étant donné que ce sont eux qui donnent tout son sens à la logique des prédicats, en même temps que toute sa difficulté.

Règles $\forall$-gauche regroupées

L'idée de cette définition 9.9 est que nous allons essayer de différer l'application de ces règles, qui n'obéissent pas au lemme de Kleene 3.3, le plus tard possible. Si l'on veut, on peut considérer que cette section est une sorte d'anti-lemme de Kleene : puisqu'on ne peut pas avoir $\forall$-g comme première règle, alors "poussons" là le plus profond possible.

Nous allons démontrer que dans une preuve, nous pouvons différer l'emploi des règles $\forall$-g jusqu'au tout dernier moment. Ce dernier moment est identifié comme étant celui où on a besoin d'appliquer une règle sur la sous-formule Q de $P = \forall x_1 ... \forall x_n Q$ et qui n'est *pas* $\forall$-g (donc Q n'est pas une formule quantifiée universellement). Nous allons démontrer ceci par la proposition 9.5, qui est la proposition centrale de cette section.

Définition 9.9 (Règles $\forall$-g regroupées). *Nous disons d'une démonstration que c'est une* démonstration avec des règles $\forall$-g regroupées *si et seulement si elle vérifie la condition suivante :*

Lorsqu'on rencontre une règle $\forall$-g sur $\forall x P$, alors la règle suivante sera une règle sur P qui n'est pas la contraction.

Exemples : La démonstration suivante a ses règles ∀-gauche regroupées.

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{}{P(x_1,y_1)\vdash^{cf}_{\mathcal{RE}} P(x_1,y_1)}\text{ axiome}}{\forall xP(x,y_1)\vdash^{cf}_{\mathcal{RE}} P(x_1,y_1)}\forall\text{-g}}{\forall y\forall xP(x,y)\vdash^{cf}_{\mathcal{RE}} P(x_1,y_1)}\forall\text{-g}}{\forall y\forall xP(x,y)\vdash^{cf}_{\mathcal{RE}} \forall xP(x,y_1)}\forall\text{-d}}{\forall y\forall xP(x,y)\vdash^{cf}_{\mathcal{RE}} \forall y\forall xP(x,y)}\forall\text{-d}$$

Mais la démonstration suivante n'a pas ses règles ∀-gauche regroupées :

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{}{P(x_1,y_1)\vdash^{cf}_{\mathcal{RE}} P(x_1,y_1)}\text{ axiome}}{\forall xP(x,y_1)\vdash^{cf}_{\mathcal{RE}} P(x_1,y_1)}\forall\text{-g}}{\forall xP(x,y_1)\vdash^{cf}_{\mathcal{RE}} \forall xP(x,y_1)}\forall\text{-d}}{\forall y\forall xP(x,y)\vdash^{cf}_{\mathcal{RE}} \forall xP(x,y_1)}\forall\text{-g}}{\forall y\forall xP(x,y)\vdash^{cf}_{\mathcal{RE}} \forall y\forall xP(x,y)}\forall\text{-d}$$

en revanche, celle-ci les a :

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\pi}{\Gamma,P(x_1,y_1,z_1),Q(x_1,y_1,z_1)\vdash^{cf}_{\mathcal{RE}}\Delta}}{\Gamma,(P\wedge Q)(x_1,y_1,z_1)\vdash^{cf}_{\mathcal{RE}}\Delta}}{\Gamma,\forall z(P\wedge Q)(x_1,y_1,z)\vdash^{cf}_{\mathcal{RE}}\Delta}}{\Gamma,\exists y\forall z(P\wedge Q)(x_1,y,z)\vdash^{cf}_{\mathcal{RE}}\Delta}}{\Gamma,\forall x\exists y\forall z(P\wedge Q)(x,y,z)\vdash^{cf}_{\mathcal{RE}}\Delta}$$

Lemme 9.4. *Si on a une démonstration avec les règles ∀-g regroupées de :*

$$\Gamma,\{t_1/x_1\}P_1,\ ...,\ \{t_n/x_n\}P_n\vdash^{cf}_{\mathcal{RE}}\Delta$$

alors on peut construire une démonstration avec les règles ∀-gauche regroupées de :

$$\Gamma,\forall x_1P_1,\ ...,\ \forall x_nP_n\vdash^{cf}_{\mathcal{RE}}\Delta$$

dans laquelle la première règle est :

- *soit la même que dans la démonstration de départ*
- *soit ∀-g sur une des propositions considérées, suivi de la même règle que dans la démonstration de départ.*

Preuve. Par récurrence sur la taille de la démonstration :
On considère la première règle appliquée. Si c'est une règle sur Γ ou Δ alors, soit $\Gamma',\{t_1/x_1\}P_1,\ ...,\ \{t_n/x_n\}P_n\vdash^{cf}_{\mathcal{RE}}\Delta'$ la (les) prémisse(s). Par hypothèse de récurrence on a une démonstration de $\Gamma',\forall x_1P_1,\ ...,\ \forall x_nP_n\vdash^{cf}_{\mathcal{RE}}\Delta'$. On peut encore appliquer cette même règle, car la condition de fraîcheur des variables n'est pas transgressée. Par exemple, si on a :

$$\dfrac{\dfrac{\pi}{\{t'/y\}A\ ,\ \{t/x\}P, \Gamma \vdash^{cf}_{\mathcal{RE}} \Delta}}{\exists y A, \{t/x\}P, \Gamma \vdash^{cf}_{\mathcal{RE}} \Delta}$$

avec t' frais dans le séquent considéré, alors on a :

$$\dfrac{\dfrac{\pi'}{\{t'/y\}A\ ,\ \forall x P, \Gamma \vdash^{cf}_{\mathcal{RE}} \Delta}}{\exists y A, \forall x P, \Gamma \vdash^{cf}_{\mathcal{RE}} \Delta}$$

et la condition de fraîcheur des variables n'est pas transgressée, car t' est toujours une variable fraîche.

Si c'est une règle sur P_1 alors :

– C'est axiome ou affaiblissement – pour la règle axiome :

$$\dfrac{}{P_1(t_1) \vdash^{cf}_{\mathcal{RE}} P_1(t_1)}\ \text{axiome}$$

se transforme en :

$$\dfrac{\dfrac{}{P_1(t_1) \vdash^{cf}_{\mathcal{RE}} P_1(t_1)}\ \text{axiome}}{\forall x_1 P_1(x_1) \vdash^{cf}_{\mathcal{RE}} P_1(t_1)}\ \forall\text{-g}$$

De même pour la règle affaiblissement (qui s'applique uniquement sur des atomes).

– C'est contraction sur P_1 - nous appliquons l'hypothèse de récurrence, puis nous contractons sur $\forall x_1 P_1$.

– C'est $\forall$-gauche sur P_1- nous appliquons l'hypothèse de récurrence et nous obtenons une preuve de :

$$\Gamma, \{t_1/x_1\}\{t'/y\}P'_1,\ \forall x_2 P_2,\ ...,\ \forall x_n P_n \vdash^{cf}_{\mathcal{RE}} \Delta \tag{9.1}$$

qui a ses règles $\forall$-g regroupées, et dont la première règle est une règle sur P'_1. En effet, dans la prémisse :

$$\Gamma, \{t_1/x_1\}\{t'/y\}P'_1,\ \{t_2/x_2\}P_2,\ ...,\ \{t_n/x_n\}P_n \vdash^{cf}_{\mathcal{RE}} \Delta$$

la première règle est sur P'_1, puisque les règles $\forall$-g sont regroupées dans la démonstration de départ.

D'après l'hypothèse de récurrence, si dans 9.1 on a une règle $\forall$-g sur P_2 par exemple, les règles $\forall$-g soient regroupées (car la règle suivante serait celle sur P'_1 d'après l'énoncé du lemme).
Donc dans 9.1 la première règle est une règle sur P'_1 qui n'est pas la contraction. Nous rajoutons $\forall$-gauche sur y puis sur x_1 et nous conservons les propriétés voulues.

– C'est une autre règle sur P_1, on applique l'hypothèse de récurrence de façon à avoir une démonstration de :

$$\Gamma, \{t_1/x_1\}P'_1, \forall x_2 P_2, ..., \forall x_n P_n \vdash^{cf}_{\mathcal{RE}} \Delta$$

qui sont la (les) prémisse(s) de la règle. Puis nous appliquons la même règle, et enfin, nous rajoutons $\forall$-gauche sur x_1.

■

Lemme 9.5. *Si on a une démonstration de :*

$$\Gamma \vdash^{cf}_{\mathcal{RE}} \Delta$$

alors on peut construire une démonstration du même séquent dans laquelle toutes les règles $\forall$-g sont regroupées.

Preuve. Par récurrence sur la taille de la démonstration.
– Si la première règle n'est pas $\forall$-gauche sur la proposition considérée alors on applique l'hypothèse de récurrence sur les prémisses.
– Si la première règle est $\forall$-gauche sur P, alors on applique l'hypothèse de récurrence, pour obtenir une démonstration sans coupures de :

$$\{t/x\}P, \Gamma \vdash^{cf}_{\mathcal{RE}} \Delta$$

où toutes les règles $\forall$-gauche seront regroupées.

Grâce au lemme 9.4, à partir de la preuve de $\Gamma, \{t/x\}P \vdash^{cf}_{\mathcal{RE}} \Delta$ obtenue par hypothèse de récurrence, nous pouvons construire une preuve de :

$$\Gamma, \forall x P \vdash^{cf}_{\mathcal{RE}} \Delta$$

qui a toutes ses règles $\forall$-gauche regroupées.

■

L'ordre de quantification n'est pas significatif

Proposition 9.6. *Soient $\sigma_1, ..., \sigma_m$ des permutations de $[1..n_1]$, ..., $[1..n_m]$. Si on a une démonstration de :*

$$\Gamma, \ \forall x_{1,1}...\forall x_{1,n_1} \ P_1, \ ..., \ \forall x_{m,1}...\forall x_{m,n_m} \ P_m \ \vdash^{cf}_{\mathcal{RE}} \Delta$$

alors on a une démonstration de :

$$\Gamma, \ \forall x_{1,\sigma_1(1)}...\forall x_{1,\sigma_1(n_1)} \ P_1, \ ..., \ \forall x_{m,\sigma_m(1)}...\forall x_{m,\sigma_m(n_m)} \ P_m \ \vdash^{cf}_{\mathcal{RE}} \Delta$$

Preuve.

1. On applique le lemme 9.5 pour avoir une démonstration où toutes les règles $\forall$-gauche sont regroupées. Notons que toutes les règles $\forall$-gauche sont présentes grâce à la condition que les règles affaiblissement, axiome

et $\perp$ s'appliquent à des propositions atomiques seulement. Autrement dit, à un moment ou à un autre dans la démonstration, on aura une règle $\forall$-gauche sur $\forall x P$:

$$\frac{\pi}{\Gamma, \forall x P \vdash^{cf}_{\mathcal{RE}} \Delta} \forall\text{-g}$$

2. On construit par récurrence sur la taille de cette démonstration la nouvelle démonstration :
   - Si la règle de déduction r n'est pas $\forall$-gauche sur $P_1, ..., P_m$, on applique l'hypothèse de récurrence, et on obtient π' (éventuellement π''). Ce sont des démonstrations auxquelles on peut appliquer cette même règle r pour construire π.
   - Si la règle est un $\forall$-gauche sur P_1 alors on est certain que tous les autres $\forall$-gauche sur P_1 sont les règles suivantes, de la manière suivante :

$$\dfrac{\dfrac{\dfrac{\theta}{\Gamma, \sigma(P_1),\ ...,\ \forall x_{m,1}...\forall x_{m,n_m}\ P_m\ \vdash^{cf}_{\mathcal{RE}} \Delta}\ \forall\text{-g}}{\vdots}}{\Gamma,\ \forall x_{1,1}...\forall x_{1,n_1}\ P_1,\ ...,\ \forall x_{m,1}...\forall x_{m,n_m}\ P_m\ \vdash_{\mathcal{RE}} \Delta}\ \forall\text{-g}$$

   Nous appliquons l'hypothèse de récurrence sur θ et rajoutons sur la preuve obtenue de $\Gamma, \sigma(P_1),\ ...,\ \forall x_{m,1}...\forall x_{m,n_m}\ P_m\ \vdash^{cf}_{\mathcal{RE}} \Delta$ les règles $\forall$-g, mais dans l'ordre qui nous convient.

■

Proposition 9.7. *Il existe une démonstration du séquent suivant :*

$$\Gamma, (\exists x P) \vee Q \vdash^{cf}_{\mathcal{RE}} \Delta$$

avec x non libre dans Q
si et seulement si il existe une démonstration du séquent :

$$\Gamma, \exists x (P \vee Q) \vdash^{cf}_{\mathcal{RE}} \Delta$$

Preuve. On construit une preuve à partir de l'autre en appliquant le lemme de Kleene 3.3.
Dans un sens, à partir de :

$$\Gamma, (\exists x P) \vee Q \vdash^{cf}_{\mathcal{RE}} \Delta$$

on applique d'abord le lemme 3.3 et on obtient deux démonstrations de :

$$\Gamma, (\exists x P) \vdash^{cf}_{\mathcal{RE}} \Delta$$
$$\Gamma, Q \vdash^{cf}_{\mathcal{RE}} \Delta$$

puis sur la première démonstration, on applique encore une fois le lemme de Kleene 3.3 et on obtient une preuve de :

$$\Gamma, (\{c/x\}P) \vdash^{cf}_{\mathcal{RE}} \Delta$$

avec c constante fraîche. On remplace c par d dans toute cette démonstration, d étant une constante entièrement fraîche, c'est-à-dire qui n'apparaît nulle part dans toutes les démonstrations. Alors on a la démonstration du séquent suivant :

$$\dfrac{\dfrac{\dfrac{\vdots}{\Gamma, (\{d/x\}P) \vdash^{cf}_{\mathcal{RE}} \Delta} \quad \dfrac{\vdots}{\Gamma, Q \vdash^{cf}_{\mathcal{RE}} \Delta}}{\Gamma, \{d/x\}(P \vee Q) \vdash^{cf}_{\mathcal{RE}} \Delta} \vee\text{-g}}{\Gamma, \exists x(P \vee Q) \vdash^{cf}_{\mathcal{RE}} \Delta} \exists\text{-g}$$

Le lecteur intéressé peut essayer de prouver la réciproque, elle fait appel exactement aux mêmes techniques, mais dans l'ordre inverse. ■

Nous allons prouver un résultat similaire, pour les quantificateurs universels.

Proposition 9.8. *Il existe une démonstration du séquent :*

$$\begin{aligned}\Gamma, \quad & \forall x_{1,1} \ ... \ \forall x_{1,n_1} \ \forall y_{1,1} \ ... \ \forall y_{1,m_1} \ (P_1 \vee Q_1), \ ... \\ & \forall x_{p,1} \ ... \ \forall x_{p,n_p} \ \forall y_{p,1} \ ... \ \forall y_{p,m_p} \ (P_p \vee Q_p) \ \vdash^{cf}_{\mathcal{RE}} \Delta\end{aligned}$$

avec $y_{r,1}, ..., y_{r,m_r}$ n'étant pas libres dans P_r si et seulement si il existe une démonstration du séquent :

$$\begin{aligned}\Gamma, \quad & \forall x_{1,1} \ ... \ \forall x_{1,n_1} (P_1 \vee \forall y_{1,1} \ ... \ \forall y_{1,m_1} Q_1), \ ... \\ & \forall x_{p,1} \ ... \ \forall x_{p,n_p} (P_p \vee \forall y_{p,1} \ ... \ \forall y_{p,m_p} Q_p) \ \vdash^{cf}_{\mathcal{RE}} \Delta\end{aligned}$$

Preuve. Dans cette preuve on appellera $\forall \overline{x}$ l'ensemble des règles $\forall$-gauche sur $x_{r,1}, ..., x_{r,n_r}$ lorsqu'elles sont regroupées, et $\forall \overline{y}$ la même chose sur $y_{r,1}, ..., y_{r,m_r}$. On fait la démonstration du sens direct et celle du sens inverse séparément.

Sens direct : nous procédons en deux étapes.

On applique le lemme 9.5 pour regrouper tous les $\forall$-gauche. On obtient une démonstration dans laquelle, puisque les propositions commencent par un quantificateur universel, ces dernières sont décomposées de la manière suivante (où nous oublions la substitution $\sigma = \{t_1/x_1, ..., t_n/x_n, t'_1/y_1, ..., t'_m/y_m\}$) :

$$\dfrac{\dfrac{\dfrac{\dfrac{\pi}{\Gamma, P \vdash^{cf}_{\mathcal{RE}} \Delta} \quad \dfrac{\pi'}{\Gamma, Q \vdash^{cf}_{\mathcal{RE}} \Delta}}{\Gamma, P \vee Q \vdash^{cf}_{\mathcal{RE}} \Delta} \vee\text{-g}}{\Gamma, \forall y_1 ... \forall y_m (P \vee Q) \vdash^{cf}_{\mathcal{RE}} \Delta} \forall \overline{y} - g}{\Gamma, \forall x_1 ... \forall x_n \forall y_1 ... \forall y_m (P \vee Q) \vdash^{cf}_{\mathcal{RE}} \Delta} \forall \overline{x} - l$$

On voit qu'il suffit, lorsqu'on se trouve devant un tel cas, de "pousser" les règles $\forall \overline{y}$-gauches au dessus de la règle $\vee$-gauche. C'est l'objet de l'étape suivante.

Ayant une démonstration ainsi modifiée nous construisons la démonstration du séquent désiré par récurrence sur cette démonstration.

– Si la règle r n'est pas $\forall$-gauche sur une proposition $\forall x_1...\forall x_n\forall y_1...\forall y_m(P\vee Q)$, alors on applique l'hypothèse de récurrence sur la(les) prémisse(s) puis on réapplique la même règle r.
En particulier, si la règle est une règle de conversion (y compris sur $\forall x_1...\forall x_n\forall y_1...\forall y_m(P\vee Q)$), nous nous servons du lemme 3.1 et du fait que la règle de conversion est orientée (ainsi, la proposition considérée reste de la forme voulue). De même, si la règle est une règle de contraction ou d'affaiblissement, nous appliquons l'hypothèse de récurrence.
– Si la règle est $\forall$-gauche sur la proposition $\forall x_1...\forall x_n\forall y_1...\forall y_m(P\vee Q)$ alors nous avons exactement le schéma décrit ci-dessus (en considérant qu'il n'y a qu'une seule proposition $\forall x_1...\forall x_n\forall y_1...\forall y_m(P\vee Q)$).
Nous appliquons alors l'hypothèse de récurrence sur π et π' (nous obtenons deux démonstrations, ν et ν' de la forme que nous désirons), puis on assemble ν et ν' en mettant à la suite de ν' les règles $\forall\overline{y}$. Ensuite, nous appliquons la règle du $\vee$-gauche, et enfin nous accolons les règles $\forall\overline{x}$.

Nous obtenons la démonstration suivante :

$$\dfrac{\dfrac{\dfrac{\nu}{\Gamma, P\vdash^{cf}_{\mathcal{RE}}\Delta}\quad\dfrac{\dfrac{\nu'}{\Gamma, Q\vdash^{cf}_{\mathcal{RE}}\Delta}}{\Gamma,\forall y_1...\forall y_m Q\vdash^{cf}_{\mathcal{RE}}\Delta}\,\forall\overline{y}-l}{\Gamma, P\vee(\,\forall y_1...\forall y_m Q\,)\vdash^{cf}_{\mathcal{RE}}\Delta}\,\vee\text{-g}}{\Gamma,\forall x_1...\forall x_n(P\vee(\,\forall y_1...\forall y_m Q\,))\vdash^{cf}_{\mathcal{RE}}\Delta}\,\forall\overline{x}-l$$

Le fait de remonter $\forall y$-gauche est justifié car les variables $y_{r,1},...,y_{r,m_r}$ ne sont pas libres dans P_r.

Réciproque :

Elle se fait toujours par récurrence sur la taille de la preuve. Notons que nous n'appliquons pas pour l'instant le lemme 9.5 de regroupement des règles $\forall$-g.

– Si la dernière règle s'applique à une proposition qui n'est pas de la forme $\forall x_1...\forall x_m(P\vee(\forall y_1...\forall y_m Q))$, on applique l'hypothèse de récurrence, et à la démonstration obtenue on applique la même règle.
– Si la dernière règle s'applique à une proposition de la forme $\forall x_1...\forall x_n(P\vee(\forall y_1...\forall y_m Q))$, c'est soit :
  – une règle de contraction. Nous appliquons l'hypothèse de récurrence.
  – $\forall$-gauche. Dans ce cas, nous appliquons l'hypothèse de récurrence, à la démonstration de :

$$\begin{aligned}\Gamma,\quad &\forall x_{1,2}\ ...\ \forall x_{1,n_1}(P_1\vee\forall y_{1,1}\ ...\ \forall y_{1,m_1}Q_1),\ ...\\ &\forall x_{p,1}\ ...\ \forall x_{p,n_p}(P_p\vee\forall y_{p,1}\ ...\ \forall y_{p,m_p}Q_p)\ \vdash^{cf}_{\mathcal{RE}}\Delta\end{aligned}$$

et obtenons une démonstration de :

$$\Gamma, \quad \forall x_{1,2} \ ... \ \forall x_{1,n_1} \ \forall y_{1,1} \ ... \ \forall y_{1,m_1} \ (P_1 \vee Q_1), \ ... \\ \forall x_{p,1} \ ... \ \forall x_{p,n_p} \ \forall y_{p,1} \ ... \ \forall y_{p,m_p} \ (P_p \vee Q_p) \ \vdash^{cf}_{\mathcal{RE}} \Delta$$

à laquelle nous rajoutons la règle $\forall$-gauche sur x_1.

– $\vee$-gauche (s'il n'y a pas de quantificateurs $\forall x_i$). Nous commençons par appliquer l'hypothèse de récurrence sur les deux prémisses, et obtenons des démonstrations de :

$$\Gamma', P \ \vdash^{cf}_{\mathcal{RE}} \ \Delta \tag{9.2}$$

$$\Gamma', \forall y_1 ... \forall y_m Q \ \vdash^{cf}_{\mathcal{RE}} \ \Delta \tag{9.3}$$

où l'abréviation suivante est utilisée :

$$\Gamma' \ := \Gamma, \quad \forall x_{2,1} \ ... \ \forall x_{2,n_2} \ \forall y_{2,1} \ ... \ \forall y_{2,m_2} \ (P_2 \vee Q_2), \ ... \\ \forall x_{p,1} \ ... \ \forall x_{p,n_p} \ \forall y_{p,1} \ ... \ \forall y_{p,m_p} \ (P_p \vee Q_p)$$

Nous voulons trouver une démonstration du séquent suivant :

$$\Gamma', \forall y_1 ... \forall y_m (P \vee Q) \vdash^{cf}_{\mathcal{RE}} \Delta$$

L'idée force est de commencer par des règles de contraction sur toutes les propositions de Γ' et Δ de façon à devoir démontrer le séquent :

$$\Gamma'_*, \Gamma', \forall y_1 ... \forall y_m (P \vee Q) \vdash^{cf}_{\mathcal{RE}} \Delta_*, \Delta$$

Nous avons annoté par $*$ toutes les propositions sur lesquelles nous venons de faire une contraction, de manière à garder leur trace, car nous ne voulons pas qu'elles soient modifiées.

Ensuite, nous continuons la construction de la démonstration en faisant une récurrence sur la démonstration du séquent :

$$\Gamma', \forall y_1 ... \forall y_m Q \vdash^{cf}_{\mathcal{RE}} \Delta$$

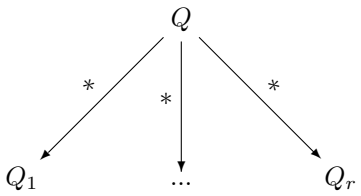
que nous avons obtenue en 9.3.

Nous distinguons les cas selon la première règle :

– Si ce n'est pas $\forall$-gauche sur $\forall y_m Q$. Nous appliquons l'hypothèse de récurrence, et nous rajoutons la même règle (sur les propositions de Γ', Δ, et surtout pas sur celles de Γ'_*, Δ_*).
Nous obtenons alors des démonstrations incomplètes de séquents de la forme suivante :

$$\Gamma'_*, \Gamma'', \forall y_{p_1} ... \forall y_m (P \vee Q_1), \ ..., \forall y_{p_q} ... \forall y_m (P \vee Q_q) \vdash^{cf}_{\mathcal{RE}} \Delta_*, \Delta''$$

avec :



La démonstration sur laquelle nous effectuons la récurrence étant, quant à elle :

$$\Gamma'', \forall y_{p_1} ... \forall y_m Q_1,\ ..., \forall y_{p_q} ... \forall y_m Q_q \vdash^{cf}_{\mathcal{RE}} \Delta''$$

Nous faisons très attention à ne pas appliquer les règles sur les propositions étoilées. Nous les conservons ainsi telles quelles jusqu'à rencontrer la règle $\forall$-g sur $\forall y_m Q_i$.

– Si la première règle est $\forall$-gauche sur $\forall y_m Q_i$ (sans perte de généralité, on peut supposer $i = 1$), alors on rajoute $\forall$-gauche (qui ne transgresse pas la condition de fraîcheur des variables) et $\vee$-gauche à la démonstration qu'on construit et on se retrouve à devoir démontrer les deux séquents suivant :

$$\Gamma'_*, \Gamma'', P, \forall y_{p_2} ... \forall y_m (P \vee Q_2),\ ..., \forall y_{p_q} ... \forall y_m (P \vee Q_q) \vdash^{cf}_{\mathcal{RE}} \Delta_*, \Delta''$$
$$\Gamma'_*, \Gamma'', Q, \forall y_{p_2} ... \forall y_m (P \vee Q_2),\ ..., \forall y_{p_q} ... \forall y_m (P \vee Q_q) \vdash^{cf}_{\mathcal{RE}} \Delta_*, \Delta''$$

En utilisant répétivement l'affaiblissement sur le premier séquent, on en arrive à devoir prouver le séquent :

$$\Gamma'_*, P \vdash^{cf}_{\mathcal{RE}} \Delta_*$$

dont on a une démonstration (c'est exactement la démonstration de 9.2).

Il reste à trouver une démonstration de :

$$\Gamma'_*, \Gamma'', Q_1, \forall y_{p_2} ... \forall y_m (P \vee Q_2),\ ..., \forall y_{p_q} ... \forall y_m (P \vee Q_q) \vdash^{cf}_{\mathcal{RE}} \Delta_*, \Delta''$$

qu'on peut trouver en continuant la récurrence sur la démonstration qui est maintenant :

$$\Gamma'', Q_1, \forall y_{p_2},\ ..., \forall y_m Q_2,\ ...,\ \forall y_{p_q},\ ..., \forall y_m Q_q \vdash^{cf}_{\mathcal{RE}} \Delta''$$

– il n'y a pas d'autres règles qui puissent s'appliquer.

■

Remarque. Cette preuve est la seule où nous avons besoin de construire une démonstration *entièrement*, du bas (séquent d'arrivée) vers le haut.

9.4 Le théorème de correction

9.4.1 Résultats sur la mise en forme clausale

Nous allons prouver des propositions plus en rapport avec le théorème, qui concernent la résolution EIR et la mise en forme clausale.

Lemme 9.9. *Soient $\psi_1, ..., \psi_n$, $\chi_1, ..., \chi_q$ des ensembles de propositions tels que $\{\psi_1, ..., \psi_n\} \rightarrow \{\chi_1, ..., \chi_q\}$ au sens du calcul des formes clausales de la figure 9.1.*
Si on a un démonstration du séquent :

$$\overline{\forall}\chi_1, ..., \overline{\forall}\chi_q \vdash_{\mathcal{RE}}$$

alors on peut construire une démonstration du séquent :

$$\overline{\forall}\psi_1, ..., \overline{\forall}\psi_n \vdash_{\mathcal{RE}}$$

Preuve. Par récurrence sur la longueur de la dérivation de la mise en forme clausale.

Si la dérivation a une longueur nulle, alors nous gardons la même preuve.

Sinon, nous distinguons des cas selon la règle de calcul employée lors de la première étape de la dérivation. Sans perte de généralité, nous pouvons supposer que la règle s'applique sur la clause ψ_1.

– si la règle est :
$$\varphi, P \vee Q \rightarrow \varphi, P, Q$$
Par hypothèse de récurrence on a une démonstration de :
$$\overline{\forall}(\varphi \vee P \vee Q), \overline{\forall}\psi_1, ..., \overline{\forall}\psi_n \vdash^{cf}_{\mathcal{RE}}$$
Ce qui est exactement ce que nous cherchions.

– si la règle est :
$$\varphi, \forall x P^l \rightarrow \varphi, P^{l::x}$$
Nous appliquons l'hypothèse de récurrence sur ce dernier ensemble de propositions, puis nous appliquons la proposition 9.6 de permutation des $\forall$-g.

– si la règle est :
$$\{\varphi, P \wedge Q\} \rightarrow \{\varphi, P\}, \{\varphi, Q\}$$
on a par hypothèse de récurrence une démonstration de :
$$\overline{\forall}(\overline{\varphi} \vee P),\ \overline{\forall}(\overline{\varphi} \vee Q),\ \overline{\forall}\psi_2, ..., \overline{\forall}\psi_n \quad \vdash^{cf}_{\mathcal{RE}} \tag{9.4}$$
que nous pouvons supposer avoir ses règles $\forall$-g regroupées d'après le lemme 9.5.

On va construire une démonstration de

$$\overline{\forall}(\overline{\varphi} \vee (P \wedge Q)), \overline{\forall}\psi_2, ..., \overline{\forall}\psi_n \vdash^{cf}_{\mathcal{RE}}$$

On commence par appliquer la règle de contraction sur la proposition $\overline{\forall}(\overline{\varphi} \vee (P \wedge Q))$. Notons que les variables quantifiées sont les mêmes, et dans le même ordre pour $\overline{\forall}(\overline{\varphi} \vee P)$, $\overline{\forall}(\overline{\varphi} \vee Q)$ et $\overline{\forall}(\overline{\varphi} \vee (P \wedge Q))$ (d'après la définition 9.6). Sinon, on appliquerait la proposition 9.6 sur les deux propositions que nous venons de contracter.
Ensuite, nous construisons par récurrence sur la démonstration de 9.4 la démonstration voulue. La contraction effectuée dès le départ nous permet de faire suivre à l'une des propositions contractées le chemin de $\overline{\forall}\overline{\varphi} \vee P$ et à l'autre, celui de $\overline{\forall}\overline{\varphi} \vee Q$. Le but est de remplacer dans la démonstration d'origine toutes les propositions dérivant de $\overline{\forall}(\overline{\varphi} \vee P)$ et de $\overline{\forall}(\overline{\varphi} \vee Q)$ par $\overline{\forall}(\overline{\varphi} \vee (P \wedge Q))$

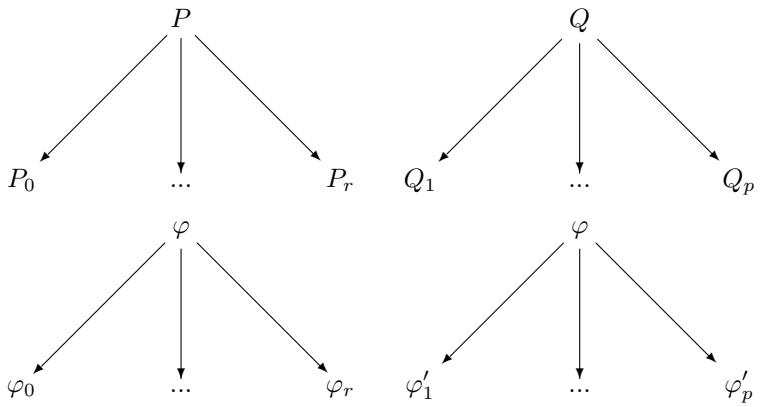
Pour faire proprement la récurrence, il faudrait considérer les différentes règles : règle sur Γ, Δ ou bien contraction/$\forall$-gauche/conversion sur une proposition $\forall x_1 ... \forall x_n(\overline{\varphi_1} \vee P_1)$ avec $P \rightarrow^* P_1$ et $\varphi \rightarrow^* \varphi_1$.

Nous traitons ici seulement le cas le plus significatif, celui de la (première) règle $\forall$-gauche sur $\overline{\varphi} \vee P$ (de manière équivalente sur $\overline{\varphi} \vee Q$). Puisque les règles $\forall$-gauche sont regroupées, nous savons qu'en fait nous avons immédiatement les prémisses suivantes :

$$\begin{array}{ll} \Gamma, \overline{\varphi_0}, & \overline{\forall}(\overline{\varphi_1} \vee P_1),\ ..., \overline{\forall}(\overline{\varphi_r} \vee P_r), \\ & \overline{\forall}(\overline{\varphi'_1} \vee Q_1),\ ..., \overline{\forall}(\overline{\varphi'_p} \vee Q_p) \vdash^{cf}_{\mathcal{RE}} \Delta \end{array}$$

$$\begin{array}{ll} \Gamma, P_0, & \overline{\forall}(\overline{\varphi_1} \vee P_1),\ ..., \overline{\forall}(\overline{\varphi_r} \vee P_r), \\ & \overline{\forall}(\overline{\varphi'_1} \vee Q_1),\ ..., \overline{\forall}(\overline{\varphi'_p} \vee Q_p) \vdash^{cf}_{\mathcal{RE}} \Delta \end{array}$$

les indices sont là pour tenir compte des réécritures et des contractions et nous avons :



Ici, $\overline{\forall}$ est la quantification sur toutes les variables libres de $\varphi \vee (P \wedge Q)$ (car φ_1 peut avoir un nombre strictement inférieur de variables libres). Nous trouvons donc des démonstrations de :

$$\Gamma, \overline{\varphi_0}, \quad \overline{\forall}(\overline{\varphi_1} \vee (P_1 \wedge Q)), \ ..., \overline{\forall}(\overline{\varphi_r} \vee (P_r \wedge Q)), \\ \overline{\forall}(\overline{\varphi'_1} \vee (P \wedge Q_1)), \ ..., \overline{\forall}(\overline{\varphi'_p} \vee (P \wedge Q_p)) \vdash^{cf}_{\mathcal{RE}} \Delta$$

$$\Gamma, P_0, \quad \overline{\forall}(\overline{\varphi_1} \vee (P_1 \wedge Q)), \ ..., \overline{\forall}(\overline{\varphi_r} \vee (P_r \wedge Q)), \\ \overline{\forall}(\overline{\varphi'_1} \vee (P \wedge Q_1)), \ ..., \overline{\forall}(\overline{\varphi'_p} \vee (P \wedge Q_p)) \vdash^{cf}_{\mathcal{RE}} \Delta$$

Sur la démonstration contenant l'instanciation $\{t_1/x_1, ..., t_n/x_n\}P_0$ de P (toutes les substitutions ont été omises pour plus de lisibilité), nous affaiblissons sur Q (en introduisant éventuellement plusieurs règles si Q n'est pas atomique), nous obtenons des démonstrations des séquents suivants :

$$\Gamma, \overline{\varphi_0}, \quad \overline{\forall}(\overline{\varphi_1} \vee (P_1 \wedge Q)), \ ..., \overline{\forall}(\overline{\varphi_r} \vee (P_r \wedge Q)), \\ \overline{\forall}(\overline{\varphi'_1} \vee (P \wedge Q_1)), \ ..., \overline{\forall}(\overline{\varphi'_p} \vee (P \wedge Q_p)) \vdash^{cf}_{\mathcal{RE}} \Delta$$

$$\Gamma, P_0, Q, \quad \overline{\forall}(\overline{\varphi} \vee (P_1 \wedge Q)), \ ..., \overline{\forall}(\overline{\varphi} \vee (P_r \wedge Q)), \\ \overline{\forall}(\overline{\varphi} \vee (P \wedge Q_1)), \ ..., \overline{\forall}(\overline{\varphi} \vee (P \wedge Q_p)) \vdash^{cf}_{\mathcal{RE}} \Delta$$

Les variables libres de Q sont substituées par les termes correspondants (il faut regarder le label $\mathbf{l}$ de $(P \wedge Q)^l$ pour définir cette substitution, pour les autres variables libres, nous sommes libres de les substituer par ce que nous voulons, puisque juste en dessous, nous allons quantifier universellement). Sur cette dernière démonstration, nous appliquons la règle du $\wedge$-gauche. à la suite de quoi nous réunissons ces deux démonstrations avec la règle $\vee$-gauche pour en obtenir une de :

$$\Gamma, \overline{\varphi} \vee (P \wedge Q), \quad \overline{\forall}(\overline{\varphi} \vee (P_1 \wedge Q)), \ ..., \overline{\forall}(\overline{\varphi} \vee (P_r \wedge Q)), \\ \overline{\forall}(\overline{\varphi} \vee (P \wedge Q_1)), \ ..., \overline{\forall}(\overline{\varphi} \vee (P \wedge Q_p)) \vdash^{cf}_{\mathcal{RE}} \Delta$$

et enfin, nous quantifions universellement sur toutes les variables libres de $\overline{\varphi} \vee (P_0 \wedge Q)$ et obtenons une démonstration du séquent :

$$\Gamma, \overline{\forall}(\overline{\varphi} \vee (P \wedge Q)), \quad \overline{\forall}(\overline{\varphi} \vee (P_1 \wedge Q)), \ ..., \overline{\forall}(\overline{\varphi} \vee (P_r \wedge Q)), \\ \overline{\forall}(\overline{\varphi} \vee (P \wedge Q_1)), \ ..., \overline{\forall}(\overline{\varphi} \vee (P \wedge Q_p)) \vdash^{cf}_{\mathcal{RE}} \Delta$$

ce que nous cherchions.

– Enfin, le dernier cas à considérer est le cas du quantificateur existentiel. $\psi_1 = \{\varphi, \exists x P^{y_1,...,y_N}\} \rightarrow \chi_1 = \{\varphi, \{f(y_1, ..., y_N)/x\}P^{y_1,...,y_N}\}$.
Soient $z_1, ..., z_m$ les variables libres de φ n'étant pas parmi $y_1, ..., y_N$.
Ayant une démonstration de :

$$\overline{\forall}\chi_1, \overline{\forall}\psi_2, ..., \overline{\forall}\psi_n \vdash^{cf}_{\mathcal{RE}}$$

on a une démonstration de :

$$\forall y_1 ... \forall y_N, \forall z_1 ... \forall z_m (\{f(y_1, ..., y_N)/x\}P \vee \overline{\varphi}), \quad \overline{\forall}\psi_2, ..., \overline{\forall}\psi_n \vdash^{cf}_{\mathcal{RE}}$$

grâce au lemme 9.6 de permutation des $\forall$ à gauche. On applique alors la proposition 9.8 et on obtient une démonstration de :

$$\forall y_1 ... \forall y_N (\{f(y_1, ..., y_N)/x\}P \vee \forall z_1 ... \forall z_m \overline{\varphi}), \quad \overline{\forall}\psi_2, ..., \overline{\forall}\psi_n \vdash_{\mathcal{RE}}$$

D'après l'axiome de Skolem 9.1, on a aussi une démonstration de :

$$\forall y_1 ... \forall y_N \exists x (P \vee \forall z_1 ... \forall z_m \overline{\varphi}), \quad \overline{\forall}\psi_2, ..., \overline{\forall}\psi_n \vdash_{\mathcal{RE}}$$

avec x variable non libre dans $\forall z_1, ..., \forall z_m \overline{\varphi}$. On applique la proposition 9.7 pour trouver une démonstration de :

$$\forall y_1 ... \forall y_N (\exists x P \vee \forall z_1 ... \forall z_m \overline{\varphi}), \quad \overline{\forall}\psi_2, ..., \overline{\forall}\psi_n \vdash_{\mathcal{RE}}$$

et enfin, on applique une dernière fois la proposition 9.8 pour trouver une démonstration de :

$$\forall y_1 ... \forall y_N \forall z_1 ... \forall z_m (\exists x P \vee \overline{\varphi}), \quad \overline{\forall}\psi_2, ..., \overline{\forall}\psi_n \vdash^{cf}_{\mathcal{RE}}$$

– les autres règles se traitent de la même manière que les règles dont nous venons de traiter les cas.

■

La réciproque est vraie aussi. La seule chose qui change par rapport à cette preuve est le traitement de la dérivation de ψ_1 lorsque $\psi_1 = \{\varphi, P \wedge Q\}$. Mais nous n'en avons pas besoin pour la suite.

Remarque. La partie qui concerne la mise en forme clausale s'arrête ici. Le plus gros du travail a donc été de prouver des lemmes sur le calcul des séquents sans coupure, de manière à rapprocher celui-ci de la résolution.

9.4.2 Résultats concernant EIR

Lemme 9.10 (Introduction de $P, \neg P$). *Soient $P_1, ..., P_m$ des propositions quelconques (possédant des variables libres ou non).*
Si on a une preuve du séquent :

$$\begin{aligned} \Gamma \quad , \quad & \forall x_{1,1} ... \forall x_{1,n_1} A_1 \vee B_1, ..., \\ & \forall x_{m,1} ... \forall x_{m,n_m} A_m \vee B_m \vdash^{cf}_{\mathcal{RE}} \Delta \end{aligned}$$

où toutes les propositions sont closes, alors on a une preuve du séquent :

$$\begin{array}{lll}\Gamma & , & \forall x'_{1,1}...\forall x'_{1,p_1}(A_1 \vee P_1), \forall x''_{1,1}...\forall x''_{1,q_1}(B_1 \vee \neg P_1), \\ & & ..., \\ & & \forall x'_{m,1}...\forall x'_{m,p_m}(A_m \vee P_m), \forall x''_{m,1}...\forall x''_{m,q_m}(B_m \vee \neg P_m), \\ & & \vdash^{cf}_{\mathcal{RE}} \Delta\end{array}$$

où $x'_{1,i}, ..., x'_{1,p_i}$ sont exactement les variables libres de A_i, P_i et $x''_{1,i}, ..., x''_{1,p_i}$ sont exactement les variables libres de B_i, P_i.

Preuve. On construit tout d'abord par récurrence sur la taille de la preuve initiale une preuve de :

$$\begin{array}{lll}\Gamma, & \forall x_{1,1}...\forall x_{1,n_1}(A_1 \vee P_1), \forall x_{1,1}...\forall x_{1,n_1}(B_1 \vee \neg P_1), \\ & ..., ..., \\ & \forall x_{m,1}...\forall x_{m,n_m}(A_m \vee P_m), \forall x_{m,1}...\forall x_{m,n_m}(B_m \vee \neg P_m), \\ & \vdash^{cf}_{\mathcal{RE}} \Delta\end{array}$$

telle que les occurrences des variables libres et des termes de A_i, B_i soient les mêmes que dans la démonstration initiale, et que les occurrences des variables libres et des termes de $P_i, \neg P_i$ soient identiques pair à pair.

- Si la règle est une règle sur Γ ou Δ, on applique l'hypothèse de récurrence.
- Si la règle est une contraction sur $\forall x_{1,1}...\forall x_{1,n_1}(A_1 \vee B_1)$, alors on applique l'hypothèse de récurrence et on contracte deux fois, sur $\forall x_{1,1}...\forall x_{1,n_1}(A_1 \vee P_1)$ et sur $\forall x_{1,1}...\forall x_{1,n_1}(B_1 \vee \neg P_1)$.
- Si la règle est une réécriture, on applique l'hypothèse de récurrence, puis on fait intervenir la règle de réécriture deux fois.
- Si la règle est $\forall$-gauche sur $\forall x_{1,1}...\forall x_{1,n_1}(A_1 \vee B_1)$, alors on applique l'hypothèse de récurrence, et on applique deux fois la règle $\forall$-gauche, en substituant x_1 par le même terme deux fois de suite (qui est aussi le terme substitué dans la preuve initiale).
- Si la règle est $\vee$-gauche, alors on applique l'hypothèse de récurrence et on se retrouve avec des démonstrations de :

$$\begin{array}{lll}\Gamma, A_1 & , & \forall x_{2,1}...\forall x_{2,n_2}(A_2 \vee P_2), \forall x_{2,1}...\forall x_{2,n_2}(B_2 \vee \neg P_2), \\ & & ..., ..., \\ & & \forall x_{m,1}...\forall x_{m,n_m}(A_m \vee P_m), \forall x_{m,1}...\forall x_{m,n_m}(B_m \vee \neg P_m), \vdash^{cf}_{\mathcal{RE}} \Delta\end{array}$$

et de :

$$\begin{array}{lll}\Gamma, B_1 & , & \forall x_{2,1}...\forall x_{2,n_2}(A_2 \vee P_2), \forall x_{2,1}...\forall x_{2,n_2}(B_2 \vee \neg P_2), \\ & & ..., ..., \\ & & \forall x_{m,1}...\forall x_{m,n_m}(A_m \vee P_m), \forall x_{m,1}...\forall x_{m,n_m}(B_m \vee \neg P_m), \vdash^{cf}_{\mathcal{RE}} \Delta\end{array}$$

que l'on simplifie pour la suite en :

$$\Gamma', A_1 \vdash^{cf}_{\mathcal{RE}} \Delta'$$

$$\Gamma', B_1 \vdash^{cf}_{\mathcal{RE}} \Delta'$$

Dans ce cas là, on a une démonstration triviale de :

$$\Gamma', P_1, \neg P_1 \vdash^{cf}_{\mathcal{RE}} \Delta'$$

à condition que toutes les occurrences variables libres et tous les termes de P_1 et de $\neg P_1$ soient identiques.

Donc on peut construire la preuve suivante :

$$\dfrac{\dfrac{\dfrac{\dfrac{\pi}{\Gamma', A_1 \vdash^{cf}_{\mathcal{RE}} \Delta'}}{\Gamma', A_1, \neg P_1, \vdash^{cf}_{\mathcal{RE}} \Delta'} \quad \dfrac{\dfrac{\vdots}{\Gamma', P_1 \vdash^{cf}_{\mathcal{RE}} P_1, \Delta'}}{\Gamma', P_1, \neg P_1 \vdash^{cf}_{\mathcal{RE}} \Delta'}\,\neg\text{-g}}{\Gamma', \neg P_1, A_1 \vee P_1 \vdash^{cf}_{\mathcal{RE}} \Delta'}\,\vee\text{-g} \quad \dfrac{\dfrac{\pi'}{\Gamma', B_1 \vdash^{cf}_{\mathcal{RE}} \Delta'}}{\Gamma', B_1, A_1 \vee P_1 \vdash^{cf}_{\mathcal{RE}} \Delta'}\,\vee\text{-g}}{\Gamma', B_1 \vee \neg P_1, A_1 \vee P_1 \vdash^{cf}_{\mathcal{RE}} \Delta'}$$

Ce qui est ce que nous cherchions.
Nous devons encore transformer cette démonstration de façon à ne quantifier que sur les variables apparaissant des propositions. Nous supprimons par récurrence sur la taille de la démonstration toutes les quantifications inutiles.

Puis nous rajoutons des règles de quantification sur les variables non encore quantifiées. Et enfin, nous appliquons le lemme 9.6 de permutation des quantificateurs universels. ■

Lemme 9.11. *Si on a une preuve du séquent :*

$$\begin{aligned}\Gamma \quad , \quad & \forall z_{1,1}...\forall z_{1,m_1}\, \forall y_{1,1}...\forall y_{1,n_1}\, \{t_1/x_1\}U_1, ..., \\ & \forall z_{p,1}...\forall z_{p,m_p}\, \forall y_{p,1}...\forall y_{p,n_p}\, \{t_p/x_p\}U_p \;\vdash^{cf}_{\mathcal{RE}} \Delta\end{aligned}$$

où $z_{i,1}, ..., z_{i,m_i}$ sont les variables libres qui apparaissent dans t_i, on peut trouver une preuve du séquent :

$$\Gamma, \forall x_1 \forall y_{1,1}...\forall y_{1,n_1} U_1,\ ...,\ \forall x_p \forall y_{p,1}...\forall y_{p,n_p} U_p \;\vdash^{cf}_{\mathcal{RE}} \Delta$$

Preuve. Par récurrence sur la taille de la démonstration :
- Si c'est une règle sur Γ ou Δ, on applique l'hypothèse de récurrence.
- Si c'est une règle $\forall$-gauche sur z_{1,m_1}, alors le terme t_1 est instancié. Donc, on ajoute $\forall$-gauche sur x_1, en substituant x_1 par t_1.
- Si c'est une règle $\forall$-gauche sur $z_{x,1}, ..., z_{x,m_x-1}$, on ne fait rien.
- Si c'est une règle de contraction, on applique l'hypothèse de récurrence.

■

Lemme 9.12. *Soient $U_1, ..., U_n$ des clauses. Si*

$$U_1, ..., U_n \hookrightarrow \square$$

alors

$$\overline{\forall} U_1, ..., \overline{\forall} U_n \vdash^{cf}_{\mathcal{RE}}$$

Preuve. Par récurrence sur la longueur de la dérivation.

- Si nous avons une dérivation de longueur nulle, alors l'une des clauses, U_1 par exemple, est la clause vide, dans ce cas, $\overline{U_1} = \bot$, ce qui nous permet de conclure avec la règle $\bot$-gauche.
- Si la première règle appliquée est **Identical Resolution** sur

  $$U_1 = \{A, P\}, U_2 = \{B, \neg P\}$$

  nous avons une démonstration de :

  $$\overline{\forall}(A \vee B), \overline{\forall} U_1, ..., \overline{\forall} U_n \vdash^{cf}_{\mathcal{RE}}$$

  D'après le lemme 9.10, nous avons alors une démonstration de :

  $$\overline{\forall}(A \vee P), \overline{\forall}(B \vee \neg P), \overline{\forall} U_1, ..., \overline{\forall} U_n \vdash^{cf}_{\mathcal{RE}}$$

  c'est la preuve cherchée.
- si la règle appliquée est **Reduction**. Nous supposons qu'elle s'applique à $U_1 \rightarrow_{\mathcal{RE}} \psi$. Nous possédons une dérivation plus courte de :

  $$U_1, ..., U_n, U' \hookrightarrow \square \text{ avec } U' \in cl(\psi)$$

  et par hypothèse de récurrence une démonstration sans coupures de :

  $$\overline{\forall} U_1, ..., \overline{\forall} U_n, \overline{\forall} U' \vdash^{cf}_{\mathcal{RE}}$$

  En utilisant les règles d'affaiblissement, on peut obtenir :

  $$\overline{\forall} U_1, ..., \overline{\forall} U_n, \ \overline{\forall} U', \overline{\forall} U'_1, ..., \overline{\forall} U'_m \vdash^{cf}_{\mathcal{RE}}$$

  avec $cl(\psi) = \{U', U'_1, ..., U'_m\}$
  D'après le lemme 9.9, puisqu'on a une dérivation de :

  $$\{\psi, U_1, ..., U_n\} \rightarrow \{U', U'_1, ..., U'_m, U_1, ..., U_n\}$$

  au sens des formes clausales, on a une démonstration de :

  $$\overline{\forall} U_1, ..., \overline{\forall} U_n, \overline{\forall} \psi \vdash^{cf}_{\mathcal{RE}}$$

  Nous rajoutons une règle de réécriture de U_1 en ψ.

  $$\dfrac{\dfrac{\pi}{\overline{\forall} U_1, ..., \overline{\forall} U_n, \overline{\forall} \psi \vdash^{cf}_{\mathcal{RE}}}}{\overline{\forall} U_1, ..., \overline{\forall} U_n, \overline{\forall} U_1 \vdash^{cf}_{\mathcal{RE}}} \text{ conversion-g } U_1 \rightarrow^* \psi$$

  Puis, nous utilisons la contraction gauche, et nous obtenons la preuve cherchée.

– Si la règle est **Conversion**, alors on a une preuve de :

$$\overline{\forall}U_1, ..., \overline{\forall}U_n, \overline{\forall}U' \vdash^{cf}_{\mathcal{RE}}$$

avec $U' =_{\mathcal{E}} U_1$. Donc on peut rajouter une règle de conversion et avoir une preuve de :

$$\overline{\forall}U_1, ..., \overline{\forall}U_n, \overline{\forall}U_1 \vdash^{cf}_{\mathcal{RE}}$$

On conclut en appliquant la règle de contraction, car les labels des propositions restent les mêmes (voir la remarque concernant la règle conversion, page 146).

– Si la règle est **Instantiation**, alors on a une preuve de :

$$\overline{\forall}U_1, ..., \overline{\forall}U_n, \overline{\forall}\{t/x\}U_1 \vdash^{cf}_{\mathcal{RE}}$$

Mais on peut avoir de nouvelles variables quantifiées par la clôture $\overline{\forall}$. On construit donc par récurrence sur cette démonstration une démonstration de :

$$\overline{\forall}U_1, ..., \overline{\forall}U_n, \overline{\forall}U_1 \vdash^{cf}_{\mathcal{RE}}$$

Pour cela nous nous servons du lemme 9.11. D'après ce lemme, on possède une démonstration de :

$$\overline{\forall}U_1, ..., \overline{\forall}U_n, \forall x\overline{\forall}U_1 \vdash^{cf}_{\mathcal{RE}}$$

où $\overline{\forall}U_1$ dénote cette fois-ci la clôture par quantification universelle, moins la quantification sur la variable x. Nous appliquons le lemme 9.6 de permutation des quantificateurs universels, et nous obtenons une démonstration sans coupures du séquent :

$$\overline{\forall}U_1, ..., \overline{\forall}U_n, \overline{\forall}U_1 \vdash^{cf}_{\mathcal{RE}}$$

que nous contractons.

■

Nous sommes enfin prêts à démontrer le théorème de correction, ce qui est facile, grâce aux deux lemmes 9.9, 9.12 et au lemme 3.3.

Théorème 9.13 (Correction).
Soient $P_1, ..., P_n, Q_1, ..., Q_m$ des propositions. Si

$$cl(P_1, ..., P_n, \neg Q_1, ..., \neg Q_m) \hookrightarrow \square$$

alors

$$P_1, ..., P_n \vdash^{cf}_{\mathcal{RE}} Q_1, ..., Q_m$$

Preuve. Par le lemme 9.12 , si nous avons $cl(P_1, ..., P_n, \neg Q_1, ..., \neg Q_m) \hookrightarrow \square$, cela veut dire que :

$$\overline{U_1}, ..., \overline{U_p} \vdash^{cf}_{\mathcal{RE}}$$

où $\{U_1, ..., U_p\} = cl(P_1, ..., P_n, \neg Q_1, ..., \neg Q_m)$.

Puisque $P_1, ..., P_n, \neg Q_1, ..., \neg Q_m \rightarrow_{\mathcal{RE}} \{U_1, ..., U_p\}$ au sens du calcul des formes clausales, on a, d'après le lemme 9.9 :

$$P_1, ..., P_n, \neg Q_1, ..., \neg Q_m \vdash^{cf}_{\mathcal{RE}}$$

Nous la transformons en la démonstration cherchée en utilisant le lemme de Kleene 3.2 sur la démonstration de $P_1, ..., P_n, \neg Q_1, ..., \neg Q_m \vdash^{cf}_{\mathcal{RE}}$. Donc on a une démonstration de :

$$P_1, ..., P_n \vdash^{cf}_{\mathcal{RE}} Q_1, ..., Q_m$$

■

9.5 Conclusion

Ce théorème démontré, que pouvons nous en faire ? Tout d'abord, dans [16] il est démontré que :

Théorème 9.14. *Soient $P_1, ..., P_n, Q_1, ..., Q_m$ des propositions. Si le séquent :*

$$P_1, ..., P_n \vdash_{\mathcal{RE}} Q_1, ..., Q_m$$

a une preuve en déduction modulo sans coupure, alors :

$$cl(P_1, ..., P_n, \neg Q_1, ..., \neg Q_m) \hookrightarrow \Box$$

dans EIR.

Nous pouvons en conclure que pour *n'importe quel système de réécriture* $\mathcal{RE}$, EIR équivaut aux preuves sans coupures du système. Autrement dit, on a $cl(\Gamma, \neg\Delta) \hookrightarrow \Box$ si et seulement si on a une démonstration de $\Gamma \vdash^{cf}_{\mathcal{RE}} \Delta$ (donc en déduction modulo sans coupure).

Puisque ENAR est équivalent à EIR, on a obtenu le résultat qu'ENAR était équivalent au fragment sans coupures de la déduction modulo, y compris pour des ensembles de règles de réécriture n'admettant pas la propriété d'élimination des coupures.

Pour revenir au théorème d'élimination des coupures, souvenons nous que le résultat de complétude de ENAR de Stuber [41] nous dit que pour certains systèmes de réécriture, si on a une démonstration de :

$$\Gamma \vdash^{cf}_{\mathcal{RE}} \Delta$$

alors on a :

$$cl(\Gamma, \neg\Delta) \hookrightarrow \Box[\mathcal{C}]$$

avec $\mathcal{C}$ ensemble de contraintes soluble.

Ce qui, mis en relation avec le théorème 9.13 de correction forte ci-dessus redémontre le théorème d'élimination des coupures 5.5 pour les systèmes de réécriture compatibles avec un ordre bien-fondé de la section 5.2.1.

Perspectives

Preuves constructives

Une question très intéressante est celle de la constructivisation des preuves prśentées dans ce travail, et notamment celle du leur contenu calculatoire.

Comme nous le disons dans les section 5.1.2 et 6.1.2, nous avons besoin de construire une semi-valuation (respectivement une semi-structure de Kripke), avant de pouvoir l'étendre en un modèle de notre théorie Γ.

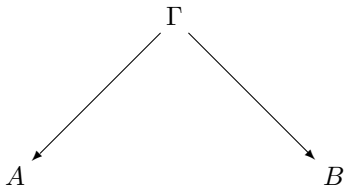
Or, l'étape de complétion de la section 3.4 qui sert ensuite à définir la semi-valuation (respectivement, la semi-structure de Kripke) n'est pas constructive. Ceci, car nous ne savons pas décider si $\Gamma, P \nvdash^{cf}_{\mathcal{R}}$ ou si $\Gamma, P \vdash^{cf}_{\mathcal{R}}$ pour toutes les propositions P.

Or, dans une semi-valuation, nous avons besoin de considérer seulement les sous-formules des propositions de Γ (oublions pour l'instant l'existence des règles de réécriture $\mathcal{R}$). Cela suggère que nous avons une construction trop forte par rapport à ce que nous voulons réellement.

La solution à ce problème passe par la construction de tableaux. Cette méthode a été introduite par Beth, Hintikka et Smullyan dans le cadre de la logique des prédicats classique, puis intuitionniste. Nous discutons ci-dessous le cas de la logique classique.

L'idée des méthodes de tableaux est d'examiner uniquement les sous-formules de Γ, et ce, de manière juste (c'est à dire que toute sous-formule doit être examinée à une certaine étape).

Dans le cas par exemple de l'examen de $A \vee B \in \Gamma$, nous savons classiquement que soit $\Gamma, A \nvdash^{cf}$, soit $\Gamma, B \nvdash^{cf}$. Comme nous ne savons pas lequel des choix est le bon (il se peut que les deux le soient), nous construisons donc *deux* branches différentes, l'une contenant Γ, A, l'autre contenant Γ, B :



Nous devons donc définir un algorithme "juste" qui examine, non seulement toutes les sous-formules de Γ, A, mais aussi explore toutes les branches de l'arbre ainsi créé (voir par exemple [40]).

Notons que certaines branches peuvent être incohérentes, par exemple, si $\Gamma = \{\neg A, A \vee B\}$, alors la branche gauche est incohérente. Nous fermons ce genre de branches (lors d'étapes ultérieures de l'algorithme).

Remarque. Une remarque clé est que les branches "closes par incohérence" ci-dessus formeront ce que Krivine appelle "modèle trivial" (modèle dans lequel toute proposition est valide) dans [30] où il prouve un théorème de complétude constructif.

Ainsi, il semblerait que la méthode de Krivine se rapproche de celle des tableaux que nous discutons ici.

Une fois que nous avons construit un tableau (complet - c'est à dire clos par toutes les règles d'extension de la méthode des tableaux), on remarque qu'une branche non-close (c'est à dire non incohérente) définit exactement *une* semi-valuation. Une branche close, quant à elle, correspond au modèle trivial.

Si $\Gamma \vDash \Delta$, alors le seul modèle de $\Gamma, \neg\Delta$ est le modèle trivial. Le tableau commençant par $\Gamma, \neg\Delta$ a toutes ses branches closes (on ne doit pas pouvoir définir de semi-valuation). Or, un tableau clos correspond à une preuve du calcul des séquents sans coupure, donc nous avons trouvé une preuve du séquent $\Gamma \vdash^{cf} \Delta$. Ceci prouve de manière constructive le théorème de complétude *forte*. Nous passons au théorème d'élimination des coupures par correction, puis complétude forte.

De plus, si Γ est cohérente (sans coupure), on peut prouver (classiquement) qu'il existe au moins une branche non-close, donc, il existe au moins une semi-valuation et donc au moins un modèle (non trivial) de Γ. Nous sommes ici obligés de nous servir de la logique classique, car nous avons supposé avoir une théorie cohérente.

Remarque. La méthode des tableaux essaie de construire *toutes* les semi-valuations existant. Autrement dit, elle essaie de construire tous les modèles possibles de Γ.

De manière à avoir une présentation uniforme, il faudrait reformuler la définition d'une semi-valuation V, sans l'aide valeurs de vérité $0, 1$, et définir un symbole $\vDash$ à la manière de Krivine :

$$\begin{array}{rll} V \vDash \bot & \text{implique} & V \vDash P \text{ (pour tout } P) \\ V \vDash \neg P & \text{implique} & \text{si} V \vDash P \text{ alors } V \vDash \bot \end{array}$$

et ainsi de suite pour les autres connecteurs.

Extension à la déduction modulo et contenu calculatoire

La question de l'extension de ces méthodes à la déduction modulo est un sujet très intéressant. Il existe déjà une notion de tableaux en déduction modulo, par Bonichon [6], ce qui est un grand pas en direction d'une preuve constructive du théorème d'élimination des coupures.

Cependant, la question de savoir si une branche infinie peut s'étendre en une semi-valuation (non triviale) n'est pas encore clairement résolue. Le point qui pose problème est celui de la compatibilité de la semi-valuation avec les règles de réécriture :

$$P \equiv_{\mathcal{R}} Q \quad \text{implique} \quad V(P) = V(Q)$$

car on ne sait pas énumérer toutes les propositions Q telles que $P \equiv_{\mathcal{R}} Q$ dans une méthode de tableaux. Ce problème pourrait par exemple trouver sa résolution en définissant la condition de compatibilité de la manière suivante :

$$\begin{array}{ccc} P \equiv_{\mathcal{R}} Q \quad \text{et } V(P), V(Q) \text{ définis, implique} & & V(P) = V(Q) \\ V(P) \text{ défini} & \text{implique} & V(P\downarrow) \text{ défini} \end{array}$$

Ce thème de recherche demande encore à être approfondi.

Même si on ne connaît pas encore de méthode sémantique constructive d'élimination des coupures, on peut se poser la question de son contenu calculatoire. D'après le chapitre 8, on sait que ça ne peut pas être une méthode de normalisation.

L'emploi de la méthode des tableaux revient finalement, étant donné une preuve de $\Gamma \vdash_{\mathcal{R}} \Delta$ à la construction "à la main" d'une preuve de $\Gamma \vdash_{\mathcal{R}}^{cf} \Delta$. Il est très vraisemblable que nous ne puissions pas faire mieux, notamment à cause des résultats du chapitre 8. Du moins, tant que nous gardons une sémantique à base de modèles booléens.

Extension au cas intuitionniste

Pour étendre tous ces résultats au cadre du calcul des séquents intuitionniste, il faut se servir des tableaux intuitionniste [33], en les étendant à la déduction modulo. Ceci n'a pas encore été effectué, et cette tâche est laissée pour un travail futur.

Comme dans la partie précédente, nous pouvons discuter du contenu calculatoire possible d'une telle méthode. Les résultats du chapitre 8 laissent à penser que nous ne pouvons espérer qu'une méthode d'élimination des coupures triviale : la construction (*via* un théorème constructif de complétude forte) d'une preuve de $\Gamma \vdash_{\mathcal{R}}^{cf} \Delta$ ne s'appuyant aucunement sur celle de $\Gamma \vdash \Delta$.

Ces affirmations sont à relativiser par les résultats de Okada [35, 34]. La sémantique utilisée est la sémantique des phases (qui se réduit aux Algèbres de Heyting dans le cas de la logique intuitionniste) pour prouver un théorème d'élimination des coupures sémantique, puis une sémantique plus raffinée pour prouver la normalisation de manière sémantique. Ainsi, notre contre-exemple en déduction modulo fonctionne toujours, car la sémantique utilisée diffère dans le cadre de la normalisation (mis à part le fait que nous utilisons ici les structures de Kripke, au lieu des Algèbres de Heyting).

L'axe de recherche le plus prometteur dans ce domaine est la formalisation des preuves exposées ici et dans les chapitres précédents à l'aide d'un assistant de preuve tel que Coq. Ainsi, nous pourrons obtenir un algorithme d'élimination des coupures sémantique. Dans ce domaine, il serait très intéressant de se référer aux travaux de Berger et Schwichtenberg [4], C. Coquand [7] ou Altenkirch et al. [1].

Structures de Kripke et Algèbres de Heyting

De manière à jeter des ponts entre l'approche basée sur les Algèbres de Heyting (qui est un cas particulier de [35]) et les structures de Kripke, nous pourrions tenter d'étudier les translations d'une sémantique à l'autre.

Cette question a été étudiée de manière catégorique par López-Escobar dans [31]. La réponse qu'il y donne n'est pas entièrement satisfaisante. En effet, s'il est possible de définir une translation des structures de Kripke vers les Algèbres de Heyting, elle passe par les modèles de Beth, puis par la syntaxe de la déduction naturelle. Dans notre optique, une traduction directe des structures de Kripke vers les Algèbres de Heyting est plus utile.

Dans [46], les deux translations sont définies, et font appel aux Ω-ensembles et à un opérateur d'extension. C'est cette même technique – étendue – qui est utilisée dans [10], à des fins légèrement différentes.

La traduction inverse, non définie dans [31], est plus difficile. Cela tient en partie au fait que dans une structure de Kripke, si $\alpha \Vdash A \vee B$, alors $\alpha \Vdash A$ ou $\alpha \Vdash B$. Or, il est bien connu que cette propriété n'est pas vraie pour toutes les théories Γ. Par exemple, on a une preuve de $A \vee B \vdash A \vee B$, mais on n'a de preuve ni de $A \vee B \vdash A$, ni de $A \vee B \vdash B$.

Cette propriété de disjonction (et de témoin existentiel) des structures de Kripke est la raison essentielle pour laquelle nous devons absolument définir une étape de complétion de Γ en théorie A-complète admettant des A-témoins de Henkin. Ainsi, pour définir une traduction des Algèbres de Heyting vers les structures de Kripke, il faut avoir un procédé ressemblant à la complétion d'une théorie. Dans le cadre propositionnel, cela s'effectue à travers les filtres premiers, qui définissent les mondes de la structure de Kripke.

L'étude de ces translations appliquées à des modèles pour l'élimination des

coupures pourrait s'avérer être un outil puissant dans l'optique d'une définition uniforme de l'élimination des coupures sémantiques.

De la normalisation vers la sémantique

Un des enjeux de la discussion de la partie précédente est la définition d'une projection des pré-modèles de [17] vers des modèles sémantiques. Puisqu'une projection a déjà été définie par Okada [34], il serait sans doute possible de définir une projection du même type dans les Algèbres de Heyting. La définition de la projection des pré-modèles dans les structures de Kripke est de même encore ouverte.

Notons encore une fois que les résultats du chapitre 8 impliquent que la projection se fait obligatoirement avec perte irréversible d'information.

Ainsi, loin d'être un affaiblissement des méthodes syntaxiques d'élimination des coupures, les méthodes sémantiques sont au contraire plus fortes, puisqu'elles permettent de prouver l'élimination des coupures dans un nombre strictement plus grand de cas.

Table des matières

Index

Table des figures

Bibliographie

[1] T. Altenkirch, M. Hofmann, and T. Streicher. Categorical reconstruction of a reduction free normalization proof. In D. Pitt, D. E. Rydeheard, and P. Johnstone, editors, *Category Theory and Computer Science*, LNCS 953, pages 182–199. Springer, 1995.

[2] P. B. Andrews. Resolution in type theory. *The Journal of Symbolic Logic*, 36(3) :414–432, September 1971.

[3] L. Bachmair and H. Ganzinger. *Associative-commutative superposition*, chapter 11, pages 353–397. Kluwer, 1998.

[4] U. Berger and H. Schwichtenberg. An inverse to the evaluation functional for typed λ-calculus. In *Proceedings of the 6th Annual IEEE Symposium on Logic in Computer Science*, pages 202–211, 1991.

[5] E. W. Beth. Semantic entailment and provability in logic. In J. Largeault, editor, *Logique Mathématique, Textes*. Armand Colin, 1972.

[6] R. Bonichon. Tamed : A tableaux method for deduction modulo. *Automated Reasoning : Second International Joint Conference, IJCAR 2004, July 4-8, 2004*, 2004.

[7] C. Coquand. From semantics to rules : A machine-assisted analysis. In *CSL*, LNCS 832, pages 91–105. Springer, 1993.

[8] R. Cori and D. Lascar. *Logique mathématique*. Masson, 1993.

[9] T. Crolard. *Extension de l'isomorphisme de Curry-Howard au traitement des exceptions*. PhD thesis, Université Paris VII, 1996.

[10] M. De Marco and J. Lipton. Cut elimination and completeness in Church's intuitionistic theory of types. *Journal of Logic and Application*, 2005. To appear.

[11] G. Dowek. *La part du calcul*. Mémoire d'habilitation, 1999.

[12] G. Dowek. Introduction to proof theory. *Course notes for the 13th European Summer School in Logic, Language and Information*, 2001.

[13] G. Dowek. Confluence as a cut elimination property. *Rewriting Techniques and Applications*, pages 2–13, 2003.

[14] G. Dowek. *Théorie des Types*. Notes de cours MPRI, 2004.

[15] G. Dowek and W. Benjamin. A constructive proof of skolem theorem for constructive logic. to appear, 2005.

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

[17] G. Dowek and B. Werner. Proof normalization modulo. *The Journal of Symbolic Logic*, 68(4) :1289–1316, December 2003.

[18] G. Dowek and B. Werner. Arithmetic as a theory modulo. *Term rewriting and applications*, pages 423–437, 2005.

[19] S. Feferman and al, editors. *Kurt Gödel : Collected Works*, volume 1. Oxford University Press, New York, 1986.

[20] G. Gentzen. Untersuchungen über das logische Schliessen. *Mathematische Zeitschrift*, 39 :176–210, 405–431, 1934.

[21] G. Gentzen. Über das Verhaltnis zwischen intuitionistischer une klassischer Logik. *Archiv für matematische Logik und Grundlagenforschung*, 16 :119–132, 1974.

[22] J.-Y. Girard. *Logique à Rome*. Notes de cours, Rome, 2004.

[23] K. Gödel. *Über die Vollstandigkeit des Logikkalkuls*. PhD thesis, Vienna, 1929.

[24] O. Hermant. A model-based cut elimination proof. *2nd St-Petersburg Days of Logic and Computability*, 2003.

[25] O. Hermant. Semantic cut elimination in the intuitionistic sequent calculus. *Typed Lambda-Calculi and Applications*, pages 221–233, 2005.

[26] S. Kanger. *Provability in Logic*. Almquist and Wicksell, Stockholm, 1957.

[27] S. C. Kleene. Permutability of inferences in Gentzen's calculi LK and LJ. *Memoirs of the American Mathematical Society*, 10 :1–26, 27–68, 1952.

[28] S. C. Kleene. *Logique mathématique*. Armand Colin, 1967.

[29] S. Kripke. Semantical analysis of intuitionistic logic. In J. N. Crossley and M. A. E. Dummett, editors, *Formal systems and recursive function*, pages 92–130. North-Holland, 1965.

[30] J.-L. Krivine. Une preuve formelle et intuitionniste du théorème de complétude de la logique classique. *The Bulletin of Symbolic Logic*, 2 : 405–421, 1996.

[31] E. G. K. López-Escobar. Equivalence between semantics for intuitionism. *The Journal of Symbolic Logic*, 46(4), 1981.

[32] S. Maehara. The predicate calculus with ε symbol. *Journal of the Mathematical Society of Japan*, 7(4) :323–344, 1955.

[33] A. Nerode and R. Shore. *Logic for Applications*. Springer, 1993.

[34] M. Okada. Phase semantic cut-elimination and normalization proofs of first- and higher-order linear logic. *Theoretical Computer Science*, 227 : 333–396, 1999.

[35] 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.

[36] D. Prawitz. Completeness and hauptsatz for second order logic. *Theoria*, 33 :246–258, 1964.

[37] D. Prawitz. Hauptsatz for higher order logic. *The Journal of Symbolic Logic*, 33(3) :452–457, September 1968.

[38] H. Rasiowa and R. Sikorski. *The mathematics of metamathematics*. PWN, Polish Scientific Publishers, Warszawa, 1963.

[39] K. Schütte. Syntactical and semantical properties of simple type theory. *The Journal of Symbolic Logic*, 25(4) :305–326, December 1960.

[40] R. M. Smullyan. *Frist-Order Logic*. Springer-Verlag, Berlin Heidelberg New York, 1968.

[41] J. Stuber. A model-based completness proof of extended narrowing and resolution. In *First International Joint Conference on Automated Reasoning (IJCAR-2001)*, volume 2083 of *LNCS*, pages 195–210. Springer, June 2001.

[42] M. E. Szabo, editor. *Collected Papers of Gerhard Gentzen*. Studies in Logic and the Foundation of Mathematics. North Holland Publishing Company, 1969.

[43] M.-o. Takahashi. A proof of cut-elimination theorem in simple type-theory. *Journal of the Mathematical Society of Japan*, 19(4) :399–410, 1967.

[44] A. S. Troelstra. *Metamathematical Investigation of Intuitionistic Arithmetic and Analysis*. Springer-Verlag, 1973.

[45] A. S. Troelstra and H. Schwichtenberg. *Basic Proof Theory*. Cambridge University Press, 1996.

[46] A. S. Troelstra and D. van Dalen. *Constructivism in Mathematics, An Introduction*. North-Holland, 1988.

[47] J. L. Underwood. *Aspects of the Computational Content of Proofs*. PhD thesis, Cornell University, 1994.

Résumé :

La Déduction Modulo est un formalisme logique qui intègre des étapes de déduction et des étapes de calcul, sous la forme de règles de réécriture. On obtient ainsi un calcul plus souple, plus adapté à la démonstration automatique, plus lisible pour un être humain. Une conséquence remarquable est qu'il permet d'exprimer beaucoup de théories axiomatiques avec des règles de calcul.
L'une des propriétés étudiée dans cette thèse est l'élimination des coupures. Elle est capitale car elle implique la cohérence du système considéré, et permet l'implantation effective d'algorithmes de recherche de preuve. Or, en Déduction Modulo, cette propriété n'est pas vraie pour tous les systèmes de réécriture, mais seulement dans certains. Ceci amène à rechercher les systèmes vérifiant l'élimination des coupures.
Cette thèse introduit tout d'abord les outils sémantiques permettant de prouver cette propriété. Nous donnons au passage une application des méthodes à la preuve du théorème de Skolem intuitionniste.
Puis nous étendons le théorème de complétude de Gödel, en rajoutant la réécriture et en renforçant l'hypothèse. Cela permet de prouver l'élimination des coupures pour plusieurs classes de systèmes de réécriture, à la fois en Déduction Modulo classique et intuitionniste.
Nous nous intéressons ensuite aux liens existant entre la propriété d'élimination des coupures et la propriété de normalisation. À ce titre, nous fournissons un exemple montrant qu'elles sont distinctes.

Enfin, nous nous intéressons à la démonstration automatique, et au lien entre la résolution modulo et le calcul des séquents modulo sans coupure.

Mots clefs :

Déduction Modulo, coupure, élimination des coupures, calcul des séquents, résolution, ENAR, règles de réécriture, sémantique, modèles booléeens, modèles de Kripke, complétude, normalisation, Skolem, skolémisation, logique.

Abstract :

Deduction Modulo is a logical frame allowing to integrate deduction and computation via rewrite rules. This way we obtain more modular logical framworks, thanks to the wide range of potential rewrite rules, more readable proofs, a system adapted to automatic theorem proving, an we can also express axiomatic theories with the only mean of rewrite rules.
This work is mainly focused on the property of cut elimination of Deduction Modulo. This is a key property, since it implies consistency of the calculus, and allows to have efficient proof search algorithms. In deduction modulo, this property is not always true.
This PhD thesis first introduces the semantical tools we will use to prove the property. We then give an application to the proof of Skolem theorem in an intuitionnistic frame.
In a second part, we extend Gödel's completeness theorem, strengthening it and extending it with rewrite rules. We get the cut elimination property for a wide range of rewrite systems. This work is done in both classical and intuitionistic Deduction Modulo.
We also focus on the link between our method and the proof normalization method. We give an example proving that both methods are distinct.

In a last part, we focus on the resolution modulo method and its link with the cut-free fragment of sequent calculus modulo.

Keywords :

Deduction Modulo, cut, cut elimination, sequent calculus, resolution, ENAR, rewriting rules, semantics, boolean models, Kripke models, completeness, normalization, Skolem, skolemization, logic.