Systèmes Canoniques Abstraits : Application à la Déduction Naturelle et à la Complétion

Guillaume Burel

Mastère Parisien de Recherche en Informatique
Université Denis Diderot – Paris 7

LORIA
Nancy
Équipe PROTHEO

Rapport de Stage de Mastère 2e année

Systèmes Canoniques Abstraits : Application à la Déduction Naturelle et à la Complétion

Guillaume Burel

mars – août 2005

Stage encadré par Claude Kirchner

Remerciements

Je tiens tout d'abord à remercier Hélène Kirchner, directrice du LORIA, de m'avoir donné l'opportunité d'effectuer un stage au sein de l'équipe PROTHEO.

Je souhaite remercier Claude Kirchner qui m'a encadré durant ce stage en sachant me donner toutes les indications dont j'avais besoin et en étant toujours disponible, tout en me laissant une grande liberté. Je remercie également Nachum Dershowitz, qui m'a aidé pour la preuve de l'application des systèmes canoniques abstraits à la complétion close.

Je remercie enfin tous ceux qui m'ont aidé dans la rédaction de ce rapport.

Table des matières

Première partie

Rapport de Stage de Mastère 2e année

Chapitre 1

Introduction

1.1 Représentation de Preuves en Démonstration Automatique

La démonstration automatique couvre aujourd'hui un grand nombre de domaines. La notion de preuve qui y est intrinsèque a été déclinée par le biais de différents formalismes. D'un côté, on a les systèmes de séquents qui ont été introduits par Gentzen [Gentzen, 1934]. Du fait de l'isomorphisme de Curry-Howard, un certain nombre d'extensions de ces systèmes ont été proposées, comme la théorie des types de Martin-Löf [Martin-Löf, 1984] qui a été la base du calcul des constructions [Coquand et Huet, 1988]. Plus récemment, d'autres extensions ont vu le jour, comme le calcul des constructions algébriques [Blanqui et al., 1999] ou le calcul des structures [Guglielmi, 2002, Brünnler, 2003, http://alessio.guglielmi.name/res/cos/index.html]. De tels formalismes ont permis l'implémentation d'outils de démonstration interactive comme Coq [Dowek et al., 1991, http://coq.inria.fr/].

D'un autre côté, les outils de démonstration automatique utilisent des procédures standards, comme la complétion [Knuth et Bendix, 1970] et la résolution [Robinson, 1965]. Celles-ci utilisent diverses représentations des formules ou des preuves. Ces deux procédures ont été raffinées pour deux raisons : pour avoir un algorithme plus spécifique, et donc plus efficace dans des cas particuliers d'application, ou alors pour augmenter l'efficacité bien qu'en restant dans le cas général. Pour le premier cas, on peut citer les algorithmes de complétion pour des structures algébriques spécifiques (groupes, anneaux, ...) qui sont recensés dans [Le Chenadec, 1986], et la paramodulation qui un raffinement de la résolution dans le cas où on a un prédicat d'égalité [Robinson et Wos, 1969]. Pour le second cas, la complétion a été étendue à la complétion équationnelle [Huet, 1980b, Peterson et Stickel, 1981, Jouannaud et Kirchner, 1986], l'induction sans induction [Kapur et Musser, 1987], ou la complétion ordonnée [Lankford, 1975, Hsiang et Rusinowitch, 1991], tandis que la résolution a été par exemple raffinée pour donner la *lock resolution* [Boyer, 1971] ou la résolution ordonnée avec sélection [Bachmair et Ganzinger, 2001].

1.2 Bonnes Preuves

Bien qu'utilisant des représentations de formules et de preuves différentes, ces diverses formalismes ont un point commun : certaines preuves sont meilleures que les autres, et on peut se contenter de ces preuves pour démontrer l'ensemble de la théorie. Par exemple, pour le calcul des séquents, les preuves sans coupures sont souvent considérées comme meilleures que les autres, puisqu'on peut restreindre l'espace de recherche de preuves à celles-ci grâce au théorème d'élimi-

nation des coupures. On retrouve la même idée derrière la résolution ordonnée : certaines preuves, en l'occurrence les preuves qui applique la règle de résolution uniquement sur les atomes maximaux, sont meilleures que les autres, et on peut restreindre la recherche d'une contradiction à celles-ci puisque la résolution ordonnée reste complète. Enfin, pour la logique équationnelle, les preuves par réécriture (preuve « en vallée ») sont meilleures d'un point de vue calculatoire, et on peut obtenir grâce à la procédure de complétion un ensemble d'axiomes équationnels équivalent à celui donné en entrée mais qui permet de se restreindre aux preuves par réécriture.

Plutôt que de séparer l'ensemble des preuves en deux, les bonnes et les moins bonnes, il peut être intéressant de munir l'ensemble des preuves d'un ordre qui permet de les comparer. Kirchner et Dershowitz ont donc proposés dans [Dershowitz et Kirchner, 2004] un cadre général, les systèmes canoniques abstraits, pour donner une unité à l'ensemble des formalismes cités précédemment. Les bonnes preuves sont alors les preuves minimales pour l'ordre donné. L'idée d'utiliser des ordres sur les preuves a été introduite dans [Bachmair et Dershowitz, 1994] pour prouver la complétude de la complétion standard.

1.3 Bonnes Inférences

Une fois la notion de bonne preuve définie à l'aide d'un ordre, il peut être intéressant d'étudier les mécanismes qui permettent d'obtenir l'ensemble de formules nécessaires pour obtenir les meilleures preuves. C'est ce que fait par exemple l'algorithme de complétion. Il ne suffit pas de construire les formules nécessaires aux meilleures preuves, sinon l'ensemble de la théorie conviendrait, il faut aussi que l'ensemble retourné ne contiennent pas de redondances, c'est-à-dire qu'il ne contienne pas plus que ce dont on a besoin.

Pour formaliser ceci, la notion de bonne inférence a été introduite dans le cadre des systèmes canoniques abstraits [Bonacina et Dershowitz, 2005]. Étant donnée une théorie, sa présentation canonique correspond à l'ensemble exact des formules nécessaires pour former les bonnes preuves. Il est suffisamment grand pour pouvoir prouver toute la théorie à partir des bonnes preuves, d'où une notion de *complétude*, et même pour produire toutes les bonnes preuves, d'où une notion de *saturation*. Néanmoins, il ne contient rien de redondant, d'où une notion de *contraction*. Les présentations, c'est-à-dire les ensembles de formules, sont transformées à l'aide de mécanismes de déduction qui permettent d'obtenir la présentation canonique.

Cette formalisation des mécanismes de déduction a été introduite pour couvrir l'ensemble des complétions existantes, pour lesquelles il existait des preuves de complétude très similaires, mais pas de généralisation formelle à ce jour. De plus, il existe également d'autres algorithmes très similaires, comme l'algorithme pour trouver les bases de Gröbner dans des idéaux polynômiaux proposé par Buchberger [Buchberger, 1965, Buchberger, 1983], et qui rentreraient donc aussi dans ce cadre.

1.4 Application des Systèmes Canoniques Abstraits

Mon travail lors de ce stage a été de vérifier que la cadre des systèmes canoniques abstraits pouvait s'appliquer à des cas concrets. En effet, cette théorie a été développée de façon la plus générale possible, et il est indispensable de s'assurer qu'elle peut bien être appliquée à l'ensemble des formalismes qu'elle devait unifier. Deux systèmes ont été étudiés : d'un premier côté, les systèmes de séquents comme par exemple la déduction naturelle, de l'autre la complétion, qui était à l'origine du développement de ce cadre.

Le chapitre suivant présentera tout d'abord le cadre des systèmes canoniques abstraits telle qu'il a été proposée dans [Dershowitz et Kirchner, 2004, Bonacina et Dershowitz, 2005]. Pour l'appliquer à des systèmes de séquents comme la déduction naturelle, il s'est avéré que ce cadre devait être généralisé. J'ai donc proposé une généralisation qui permette de traiter de tels systèmes tout en restant compatible avec le cadre initial. Cette généralisation sera ensuite appliquée à la déduction naturelle, et je présenterais un ordre sur les preuves tel que les bonnes preuves correspondent aux preuves sans coupures.

Dans un deuxième temps, je me suis intéressé aux diverses complétions, notamment la complétion close [Gallier et al., 1993, Snyder, 1989] et la complétion standard [Knuth et Bendix, 1970]. Il avait déjà été démontré dans [Dershowitz, 2003] que la complétion close est bien une instance du cadre des systèmes canoniques abstraits. Toutefois, la preuve présente surtout les points essentiels, et est par conséquent plutôt elliptique. On trouvera dans la seconde partie, au chapitre 8 une preuve détaillée et originale. Je me suis ensuite intéressé à la complétion standard, ce qui m'a conduit à comparer plusieurs types de représentation des preuves en logique équationnelle, à savoir des termes de preuves comme dans [Meseguer, 1992] ou des preuves par remplacement d'égal par égal [Bachmair et Dershowitz, 1994]. La question intéressante est de savoir si ces deux représentations conduisaient aux mêmes présentations canoniques ou non. Le chapitre 3 présentera donc une comparaison de ces deux représentations, puis j'utiliserai la plus adaptée pour démontrer que la complétion standard rentre bien dans le cadre des systèmes canoniques abstraits.

On trouvera dans la deuxième partie de ce rapport une version plus détaillée, rédigée en anglais. En particulier, le chapitre 6 présente quelques notions mathématiques utiles, ainsi que les notations utilisées dans ce rapport.

Chapitre 2

Systèmes Canoniques Abstraits

Dans ce chapitre, je présente tout d'abord le cadre des systèmes canoniques abstraits. Ensuite, si on essaie de l'appliquer à des systèmes de séquents comme la déduction naturelle, on s'aperçoit qu'il faut le généraliser de façon à ce qu'il puisse traiter des formalisme logiques dans lesquels les hypothèses des sous-preuves peuvent être différentes de celles de la preuve initiale. Je propose une telle généralisation, et je l'ai ensuite appliquée au cas de la déduction naturelle.

2.1 Systèmes de Preuves qui préservent les Hypothèses

Je présente dans cette section le cadre des systèmes canoniques abstraits, telle qu'elle a été définie dans [Dershowitz et Kirchner, 2004, Bonacina et Dershowitz, 2005], que l'on consultera pour les démonstrations. Les démonstrations présentées ici sont originales, à moins qu'il en soit indiqué autrement par une référence.

2.1.1 Définitions et Postulats

On considère deux ensembles : l'ensemble des formules $\mathbb{A}$ sur un vocabulaire fixé, et l'ensemble des preuves $\mathbb{P}$. Ces deux ensembles sont reliés par deux fonctions : $[\cdot]^{Pm} : \mathbb{P} \to 2^{\mathbb{A}}$ donne les hypothèses d'une preuve, tandis que $[\cdot]_{Cl} : \mathbb{P} \to \mathbb{A}$ donne sa conclusion. Ces deux fonctions sont étendues à un ensemble de preuve de façon usuelle. L'ensemble des preuves construites à partir d'un ensemble d'hypothèses $A \subseteq \mathbb{A}$ est noté

$$Pf(A) \quad \stackrel{!}{=} \quad \left\{p \in \mathbb{P} : [p]^{Pm} \subseteq A\right\}$$

À ceci s'ajoute deux ordres *nœthériens* sur les preuves : l'ordre $>$ permet de comparer les preuves, tandis que $\triangleright$ est une relation de sous-preuve. Ces deux ordres sont mis en relation grâce au postulat E présenté dans la section 2.1.3. On suppose que ne sont comparées que les preuves qui ont la même conclusion ($p > q \Rightarrow [p]_{Cl} = [q]_{Cl}$).

On utilise le terme *présentation* pour désigner un ensemble de formules, et *justification* pour un ensemble de preuves. Le terme *théorie* est réservé aux présentations déductivement fermée :

Définition 2.1 (Théorie)**.** *ThA désigne la* théorie *associée a une présentation A, c'est-à-dire l'ensemble des conclusions des preuves construites à l'aide de formules de A :*

$$ThA \quad \stackrel{!}{=} \quad [Pf(A)]_{Cl} \quad = \quad \{[p]_{Cl} : p \in \mathbb{P},\ [p]^{Pm} \subseteq A\}$$

Les théories sont monotones :

Proposition 2.1 (Monotonie)**.** *Pour toutes présentations A et B :*

$$A \subseteq B \Rightarrow ThA \subseteq ThB$$

En plus de ceci, on suppose les deux postulats suivants :

POSTULAT A (Réflexivité)**.**
Pour toute présentation A :

$$A \subseteq ThA$$

POSTULAT B (Fermeture)**.**
Pour toute présentation A :

$$ThThA \subseteq ThA$$

Des présentations A et B sont *équivalentes* ($A \equiv B$) si et seulement si $ThA = ThB$

Définition 2.2 (Preuves Minimales)**.** *L'ensemble des* preuves minimales *d'une présentation A est défini comme l'ensemble des preuves minimales pour $>$ de $Pf(A)$*

$$\mu Pf(A) \stackrel{!}{=} \{p \in Pf(A) : \neg\exists q \in Pf(A).\ p > q\}$$

Définition 2.3 (Présentation Canonique)**.** *L'ensemble des preuves en forme normale d'une présentation A est l'ensemble des preuves minimales de la théorie ThA.*

$$Nf(A) \stackrel{!}{=} \mu Pf(ThA)$$

La présentation canonique *contient les formules qui apparaissent comme hypothèses dans les preuves en forme normale.*

$$A^\sharp \stackrel{!}{=} [Nf(A)]^{Pm}$$

On dira que A est canonique *si $A = A^\sharp$.*

On peut étendre l'ordre sur les preuves aux justifications :

Définition 2.4 (Meilleures Preuves)**.** *La justification Q est* meilleure *que la justification P si*

$$P \sqsupseteq Q \stackrel{!}{\equiv} \forall p \in P\ \exists q \in Q.\ p \geq q$$

Elle est bien meilleure *si*

$$P \sqsupset Q \stackrel{!}{\equiv} \forall p \in P\ \exists q \in Q.\ p > q$$

Les justifications sont similaires *si :*

$$P \simeq Q \stackrel{!}{\equiv} P \sqsupseteq Q \sqsupseteq P$$

Ces relations sont compatibles : $(\sqsupseteq \circ \sqsupset) \subseteq \sqsupset$, $(\sqsupseteq \circ \simeq) \subseteq \sqsupseteq$, etc.
On a alors :

Proposition 2.2. *Pour toutes présentations A, B :*

$$Pf(A) \sqsupseteq Pf(A \cup B)$$

Pour toute justification P :

$$P \sqsupseteq \mu P$$

On peut ensuite étendre ceci aux présentations :

Définition 2.5 (Présentations plus simples)**.** *La présentation B est dite* plus simple *qu'une présentation équivalente A si elle permet de construire des preuves meilleures :*

$$A \gtrsim B \stackrel{!}{\equiv} ThA = ThB \wedge Pf(A) \sqsupseteq Pf(B)$$

Les présentations sont similaires *si leurs preuves le sont elles aussi :*

$$A \approx B \stackrel{!}{\equiv} Pf(A) \simeq Pf(B)$$

On peut ainsi caractériser la présentation canonique en terme d'ordre :

THÉORÈME 2.3.
La présentation canonique est la plus simple :

$$A \equiv B \Rightarrow B \gtrsim A^\sharp$$

2.1.2 Complétude, Saturation et Redondance

Définition 2.6 (Saturation)**.** *Une présentation A est* saturé *si elle permet de produire toutes les preuves en forme normale :*

$$Pf(A) \supseteq Nf(A)$$

Définition 2.7 (Complétude)**.** *Une présentation A est* complète *si on peut obtenir une preuve en forme normale pour tout théorème à partir de A :*

$$ThA = [Pf(A) \cap Nf(A)]_{Cl}$$

Proposition 2.4. *Une présentation est complète si elle est saturée.*

Le théorème suivant relie la canonicité et la saturation. Tout d'abord, on a :

Lemme 2.5. *Une présentation est saturée si et seulement si*

$$\mu Pf(A) = Nf(A)$$

THÉORÈME 2.6.
Une présentation est saturée si et seulement si elle contient sa propre présentation : $A \supseteq A^\sharp$. En particulier, $A^\sharp$ est saturée.

De plus, la présentation canonique $A^\sharp$ est le plus petit ensemble saturé : aucun sous-ensemble strict de $A^\sharp$ est saturé.

Enfin, si A est saturé, tout sur-ensemble équivalent l'est aussi.

La définition qui suit permet de donner une quatrième caractérisation des présentations canoniques, comme lemmes non-redondants. Les formules qui peuvent être retirées d'une présentation sans rendre les preuves plus mauvaises sont « redondantes » :

Définition 2.8 (Redondance)**.** *Une formule r est* redondante *par rapport à une présentation A si :*

$$A \gtrsim A \setminus \{r\}$$

L'ensemble des formules redondantes *d'une présentation A sera noté de la façon suivante :*

$$Red\,A \quad \stackrel{!}{=} \quad \{r \in A : A \gtrsim A \setminus \{r\}\}$$

Une présentation A est contractée *si $Red\,A = \emptyset$*

L'ensemble des formules redondantes est *globalement* redondant :

Proposition 2.7. *Pour toute présentation A :*

$$A \approx A \setminus Red\,A$$

THÉORÈME 2.8.
Une présentation est canonique si et seulement si elle est saturée et contractée.

2.1.3 Sous-preuves et Inférence

On introduit maintenant la notion de sous-preuve, c'est-à-dire qu'on muni $\mathbb{P}$ d'un ordre nœthérien $\rhd$. On dit qu'une preuve est *triviale* quand elle prouve son unique hypothèse et qu'elle ne contient pas de sous-preuve stricte, c'est-à-dire $[p]^{Pm} = \{[p]_{Cl}\}$ et $p \trianglerighteq q \Rightarrow p = q$. On note $\widehat{a}$ la preuve triviale d'une hypothèse $a \in A$, et $\widehat{A}$ l'ensemble des preuves triviales pour toutes les formules de A.

On suppose que les preuves utilisent leurs hypothèses (postulat C), que les sous-preuves n'utilisent pas d'hypothèses nouvelles (postulat D) et que l'ordre sur les preuves est monotone vis-à-vis de la relation de sous-preuve (postulat E) :

POSTULAT C (Trivia)**.**
Pour toute preuve p et toute formule a :

$$a \in [p]^{Pm} \Rightarrow p \trianglerighteq \widehat{a}$$

POSTULAT D (Monotonie des Hypothèses des Sous-Preuves)**.**
Pour toutes preuves p et q :

$$p \trianglerighteq q \Rightarrow [p]^{Pm} \supseteq [q]^{Pm}$$

POSTULAT E (Remplacement)**.**
Pour toutes preuves p, q et r :

$$p \rhd q > r \Rightarrow \exists v \in Pf([p]^{Pm} \cup [r]^{Pm}).\ p > v \rhd r$$

On a alors une nouvelle caractérisation des présentations canoniques comme ensemble des conclusions des preuves triviales minimales.

Lemme 2.9. *Pour toute présentation,* $[\mu Pf(A)]^{Pm} = [\mu Pf(A) \cap \widehat{A}]_{Cl}$

THÉORÈME 2.10.
Pour toute présentation A,

$$A^\sharp = [Nf(A) \cap \widehat{ThA}]_{Cl}$$
$$\widehat{A^\sharp} = Nf(A) \cap \widehat{ThA}$$

La proposition suivante est une conséquence du postulat E :

Proposition 2.11 (Minimalité des Sous-Preuves)**.** *Pour toute présentation A, pour toutes preuves* p, q*,*

$$p \trianglerighteq q \ \wedge \ p \in \mu Pf(A) \Rightarrow q \in \mu Pf(A)$$

On s'intéresse maintenant aux mécanismes de déduction :

Définition 2.9 (Mécanisme de Déduction)**.** *Un* mécanisme de déduction $\rightsquigarrow$ *est une fonction qui associe une présentation à chaque présentation.*

Une suite de présentations $A_0 \rightsquigarrow A_1 \rightsquigarrow \cdots$ *est appelée une* dérivation*.*

Le résultat d'un mécanisme de déduction est l'ensemble des formules persistantes *:*

$$A_\infty \ \stackrel{!}{=} \ \liminf_{j\to\infty} A_j \ = \ \bigcup_{j>0} \bigcap_{i>j} A_i$$

On définit aussi l'ensemble des formules générées :

$$A_* = \bigcup_{i>0} A_i$$

Définition 2.10 (Correction et adéquation)**.**

- *Un mécanisme de déduction* $\rightsquigarrow$ *est* sain *si* $A \rightsquigarrow B$ *implique* $ThB \subseteq ThA$*.*
- *Il est* adéquat *si* $A \rightsquigarrow B$ *implique* $ThA \subseteq ThB$*.*
- *Il est les deux si* $A \equiv B$*.*

Définition 2.11 (Bonté)**.** *Un mécanisme de déduction* $\rightsquigarrow$ *est* bon *si les preuves deviennent meilleures :*

$$\rightsquigarrow \subseteq \succsim$$

En d'autres termes, $Pf(A) \sqsupseteq Pf(B)$ *quand* $A \rightsquigarrow B$*.*

Une dérivation $A_0 \rightsquigarrow A_1 \rightsquigarrow \cdots$ *est* bonne *si* $A_i \succsim A_{i+1}$ *pour tout* i*.*

Proposition 2.12. *Si une dérivation* $\{A_i\}_i$ *est bonne, alors sa limite permet les meilleures preuves :*

$$A_* \approx A_\infty$$

On peut ensuite étendre les notions de complétude, de saturation et de redondance aux dérivations :

Définition 2.12 (Dérivation Canonique)**.**

- *Une dérivation* $\{A_i\}_i$ *est* complétante *si* A_∞ *est complète.*
- *Elle est* saturante *si* A_∞ *est saturée.*

– *Elle est* contractante *si* A_∞ *est contractée.*
– *Elle est* canonique *si elle est à la fois saturante et contractante.*

THÉORÈME 2.13.
Une bonne dérivation est canonique si et seulement si

$$A_\infty = A_0^\sharp$$

On introduit aussi une notion d'équité uniforme, qui correspond à la notion de saturation :

Définition 2.13 (Équité uniforme)**.** *Une bonne dérivation est* uniformément équitable *si*

$$\widehat{A_\infty} \setminus \widehat{A_0^\sharp} \sqsupset Pf(A_*)$$

Proposition 2.14. *Si une bonne dérivation est uniformément équitable, alors sa limite est saturée.*

2.2 Généralisation pour l'Application à des Systèmes de Séquents

2.2.1 La Déduction Naturelle

La déduction naturelle a été introduite par Gentzen comme une alternative plus « naturelle » au calcul des séquents qu'il a également défini dans [Gentzen, 1934].

On trouvera dans la section 7.2.1 la définition des formules et des preuves en déduction naturelle intuitioniste. Il est important de noter que les preuves sont représentées par des λ-termes, et que la notion de sous-preuve correspond quasiment à la notion de sous-arbre, mais est étendue de la manière suivante pour satisfaire le postulat C :

Définition 2.14 (Sous-Preuve en Déduction Naturelle)**.** *On définit la relation de* sous-preuve $\trianglerighteq$ *en déduction naturelle comme la plus petite relation réflexive et transitive telle que :*
– *si* q *est un sous-arbre de* p*, alors* $p \trianglerighteq q$ *;*
– *pour toutes formules* A, B *et ensemble de formules* Γ*,* $\dfrac{}{\Gamma, A \vdash B}\ Ax \trianglerighteq \dfrac{}{A \vdash A}\ Ax$

2.2.2 Modification du Cadre des Systèmes Canoniques Abstraits

On veut appliquer le cadre des systèmes canoniques abstraits comme défini dans la section précédente à des systèmes de séquents comme la déduction naturelle.

Les postulats A et B sont des conséquences bien connue des règles d'inférence données dans la figure 7.1 page 59.

La vérification du postulat C provient de la définition 2.14.

Le postulat D, par contre, ne convient pas à ces systèmes de preuves, à cause de la règle d'inférence d'introduction d'une implication

$$\frac{\Gamma, A \vdash B}{\Gamma \vdash A \to B}\ Abs$$

Dans cette section je généralise le cadre des systèmes canoniques abstraits de façon à ce qu'il soit applicable aux systèmes de séquents. Pour cela, on supprime totalement le postulat D. Il faut alors modifier le postulat E de la manière suivante :

POSTULAT E_{gen} (Remplacement Généralisé)**.**
Pour toutes preuves p, q et r :

$$p \rhd q > r \Rightarrow \exists v \in Pf([p]^{Pm} \cup ([r]^{Pm} \setminus [q]^{Pm})).\ p > v \rhd r$$

L'idée derrière ce postulat est que les hypothèses de q sont de deux sortes : les premières sont celles de p, les autres proviennent de la construction de la preuve. Il faut donc supprimer ces dernières dans la preuve résultant du remplacement de la sous-preuve q par une preuve meilleure r dans p. On obtient donc une preuve dans $Pf([p]^{Pm} \cup ([r]^{Pm} \setminus ([q]^{Pm} \setminus [p]^{Pm}))) = Pf([p]^{Pm} \cup ([r]^{Pm} \setminus [q]^{Pm}))$. Pour mieux comprendre, le mieux est de se reporter à l'exemple 2.1.

Remarque: On a bien une généralisation conservative du cadre, car $[p]^{Pm} \cup ([r]^{Pm} \setminus [q]^{Pm} \subseteq [p]^{Pm} \cup [r]^{Pm}$, et si on suppose en plus que $[p]^{Pm} \supseteq [q]^{Pm}$, on a l'autre inclusion : $[p]^{Pm} \cup ([r]^{Pm} \setminus [q]^{Pm}) \supseteq [p]^{Pm} \cup ([r]^{Pm} \setminus [p]^{Pm}) = [p]^{Pm} \cup [r]^{Pm}$

Exemple 2.1*:* Si on considère la preuve suivante en déduction naturelle :

$$p = \dfrac{\dfrac{\dfrac{}{A, B \vdash A}\,Ax}{A \vdash B \to A}\,Abs}{\vdash A \to B \to A}\,Abs$$

La sous-preuve

$$q = \dfrac{\dfrac{}{A, B \vdash A}\,Ax}{A \vdash B \to A}\,Abs$$

peut être remplacée par la preuve « meilleure »

$$r = \dfrac{}{A, B \to A \vdash B \to A}\,Ax$$

ce qui donne la preuve

$$v = \dfrac{\dfrac{}{A, B \to A \vdash B \to A}\,Ax}{B \to A \vdash A \to B \to A}\,Abs$$

On peut voir que $v \in Pf([p]^{Pm} \cup ([r]^{Pm} \setminus [q]^{Pm})) = Pf(\emptyset \cup (\{A, B \to A\} \setminus \{A\})) = Pf(\{B \to A\})$. La preuve obtenue par remplacement v satisfait les hypothèses du postulat E_{gen}, comme attendu.

Il faut aussi généraliser la proposition 2.11, car on n'est plus assuré que quand p est dans $Pf(A)$, ses sous-preuves s'y trouvent aussi. On peut par exemple utiliser la proposition suivante :

Proposition 2.15 (Minimalité des Sous-Preuves Étendue)**.** *Pour toute présentation A,*

$$p \trianglerighteq q \wedge p \in \mu Pf(A) \Rightarrow q \in \mu Pf(A \cup [q]^{Pm})$$

Démonstration. Si $p = q$, c'est trivial.

Sinon, on suppose $p \rhd q$ et $p \in \mu Pf(A)$. Par l'absurde, supposons qu'il existe une preuve r dans $Pf(A \cup [q]^{Pm})$ telle que $q > r$. On a alors $p \rhd q > r$, donc d'après le postulat de remplacement généralisé E_{gen}, il existe $v \in Pf([p]^{Pm} \cup ([r]^{Pm} \setminus [q]^{Pm}))$ tel que $p > v \rhd r$. Par hypothèse $[r]^{Pm} \subseteq A \cup [q]^{Pm}$, donc $[p]^{Pm} \cup ([r]^{Pm} \setminus [q]^{Pm}) \subseteq A$ et par conséquent $v \in Pf(A)$, ce qui entre en contradiction avec la minimalité de p dans A. □

Remarque: C'est bien une généralisation de la proposition 2.11 : si on suppose le postulat D, et si $p \trianglerighteq q$ et $p \in \mu Pf(A)$, alors $A \cup [q]^{Pm} = A$.

Le lemme 2.9 nécessite quant à lui une démonstration différente de celle donnée avec la théorie originale.

Lemme 2.9. *Pour toute présentation A,* $[\mu Pf(A)]^{Pm} = [\mu Pf(A) \cap \widehat{A}]_{Cl}$

Démonstration. Pour le sens $\supseteq$, c'est trivial car $[\mu Pf(A) \cap \widehat{A}]_{Cl} = [\mu Pf(A) \cap \widehat{A}]^{Pm}$ et par monotonie de $[\cdot]^{Pm}$.

Pour $\subseteq$, on montre tout d'abord que

$$\widehat{[\mu Pf(A)]^{Pm}} \subseteq \mu Pf(A) \tag{2.1}$$

c'est-à-dire que pour tout $a \in [\mu Pf(A)]^{Pm}$ on a $\widehat{a} \in \mu Pf(A)$: soit $a \in [\mu Pf(A)]^{Pm}$, alors par définition il existe $p \in \mu Pf(A)$ qui utilise a comme hypothèse ($a \in [p]^{Pm}$). En utilisant le postulat C on obtient $p \trianglerighteq \widehat{a}$. D'après la proposition 2.15, $\widehat{a} \in \mu Pf(A \cup \{a\}) = \mu Pf(A)$. ($a \in [\mu Pf(A)]^{Pm}$ implique $a \in A$.)

Clairement, on a aussi

$$\widehat{[\mu Pf(A)]^{Pm}} \subseteq \widehat{A} \tag{2.2}$$

car $[\mu Pf(A)]^{Pm} \subseteq A$ et par monotonie de $\widehat{\cdot}$.

De (2.1) et (2.2) on obtient $\widehat{[\mu Pf(A)]^{Pm}} \subseteq \mu Pf(A) \cap \widehat{A}$.

De plus, pour toute présentation B on a $B = [\widehat{B}]_{Cl}$ par définition des preuves triviales, donc on peut conclure avec $[\mu Pf(A)]^{Pm} = [\widehat{[\mu Pf(A)]^{Pm}}]_{Cl} \subseteq [\mu Pf(A) \cap \widehat{A}]_{Cl}$ par monotonie de $[\cdot]_{Cl}$.

□

D'autres démonstrations ont besoin d'être modifiées, aussi que certaines définitions. L'ensemble des modifications nécessaires pour adapter le cadre est détaillé dans la section 7.2.2. On y trouvera en particulier les démonstrations qu'il est nécessaire de changer.

2.2.3 Bonnes Preuves et Preuves sans Coupure

Dans la déduction naturelle il n'y a pas de règle de coupure explicite. La règle de coupure du calcul des séquents est la suivante :

$$\frac{\Gamma \vdash A \quad \Gamma, A \vdash B}{\Gamma \vdash B}\ Coup$$

Elle représente l'utilisation d'un lemme A utilisé pour prouver la conclusion B.

On peut simuler cette règle dans la déduction naturelle en utilisant le schéma suivant :

$$\frac{\dfrac{\Gamma, A \vdash B}{\Gamma \vdash A \to B}\ Abs \qquad \Gamma \vdash A}{\Gamma \vdash B}\ App$$

Le λ-terme associé à une preuve de cette forme est du type $(\lambda x.t_1)t_2$, autrement dit, on peut y appliquer la règle de β-réduction. C'est la raison pour laquelle les preuves qui sont représentées par des λ-termes pour lesquels la β-réduction ne s'applique pas sont appelées des preuves sans coupure.

L'idée est donc de prendre comme ordre sur les preuves la fermeture transitive de la β-réduction $\xrightarrow{+}_{\beta}$. Cet ordre est nœthérien à cause de la normalisation forte du λ-calcul simplement typé. Il satisfait également le postulat E_{gen}. On obtient donc le théorème suivant :

THÉORÈME 2.16 (Preuves sans Coupure Minimales)**.**
Les preuves minimales en déduction naturelle avec l'ordre sur les preuves indiqué précédemment sont les preuves sans coupure.

Démonstration. Les preuves minimales sont celles qui ne peuvent pas se β-réduire, donc par définition ce sont les preuves sans coupure. □

Un tel théorème montre comment le cadre des systèmes canoniques abstraits peut s'appliquer dans un cas concret, bien qu'on ait dû le généraliser un peu. Les preuves minimales correspondent aux preuves sans coupure, qui sont d'un point de vue calculatoire bien meilleures, car on a pas à deviner les différents lemmes utilisés. C'est une première étape pour montrer que le cadre des systèmes canoniques abstraits couvre un large domaine de formalismes logiques dans lesquels il existe une notion intuitive de bonne preuve.

Chapitre 3

Application à la Complétion Standard

Je m'intéresse ici à la complétion standard, telle qu'introduite par Knuth et Bendix [Knuth et Bendix, 1970]. On trouvera également dans la seconde partie une application du cadre des systèmes canoniques abstraits à la complétion close (chapitre 8).

3.1 Présentation

La procédure de complétion standard a été introduit par Knuth et Bendix [Knuth et Bendix, 1970], d'où son appellation courante. Sa correction a été prouvée pour la première fois par Huet [Huet, 1980a], en supposant une hypothèse d'équité. Nous utilisons ici une présentation de la procédure comme règles d'inférence (voir figure 3.1), comme on peut le trouver dans [Bachmair, 1987, Bachmair et Dershowitz, 1994].

Cet algorithme consiste en six règles qui s'appliquent à un couple E, R formé d'un ensemble d'axiomes équationnels et d'un ensemble de règles de réécriture. Il utilise un ordre de réduction sur les termes $\gg$ comme argument. Les règles sont présentées dans la figure 3.1.

Depuis [Huet, 1980a], la complétion standard est associée à une hypothèse d'équité (voir [Bachmair et Dershowitz, 1994, lemme 2.8]) : à la limite, toutes les équations sont orientées ($E_\infty = \emptyset$), et toutes les paires critiques persistantes formées à partir de R_∞ ont été traitées par **Déduit** au moins une fois.

Comme on travaille sur des termes avec variable, l'ordre $\gg$ ne peut être total, de telle sorte que **Oriente** peut échouer. Par conséquent, l'algorithme de complétion standard peut soit :

- terminer par un succès et renvoyer un ensemble de règles de réécriture confluent et terminant ;
- terminer par un échec ; ou
- ne pas terminer.

La complétude de la complétion est démontrée ici uniquement dans le premier cas.

3.2 Représentation des Preuves Équationnelles

On s'intéresse maintenant à la façon de représenter les preuves pour pouvoir appliquer le cadre des systèmes canoniques abstraits. Je compare deux candidats : le premier possède une structure d'arbre, et est donc convient bien pour introduire une relation de sous-preuve, tandis que le second

[1] CP représente l'ensemble des paires critiques, voir la définition 6.19 page 48.

[2] $\blacktriangleright$ représente l'ordre d'inclusion totale, voir la définition 6.10 page 46.

Déduit[1] :
Si $s = t \in CP(R)$

$$E, R \rightsquigarrow E \cup \{s = t\}, R$$

Oriente :
Si $s \gg t$

$$E \cup \{s = t\}, R \rightsquigarrow E, R \cup \{s \to t\}$$

Supprime :

$$E \cup \{s = s\}, R \rightsquigarrow E, R$$

Simplifie :
Si $s \underset{R}{\longrightarrow} u$

$$E \cup \{s = t\}, R \rightsquigarrow E \cup \{u = t\}, R$$

Compose :
Si $t \underset{R}{\longrightarrow} u$

$$E, R \cup \{s \to t\} \rightsquigarrow E, R \cup \{s \to u\}$$

Combine[2] :
Si $s \underset{v \to w \in R}{\longrightarrow} u$, et $s \blacktriangleright v$,

$$E, R \cup \{s \to t\} \rightsquigarrow E \cup \{u = t\}, R$$

FIG. 3.1 – Règles d'Inférence de la Complétion Standard.

provient d'une preuve de la complétude de la complétion standard, avec un ordre sur les preuves bien adapté à ce problème.

3.2.1 Termes de Preuves

Cette représentation provient de la logique de réécriture (voir [Meseguer, 1992], elle est utilisée par exemple dans [Kirchner et al., 1995]). Soit Σ une signature, E un ensemble d'axiomes équationnels et R un ensemble de règles de réécriture basés sur cette signature. On considère l'ensemble des règles de la logique équationnelle donnée en figure 3.2. Ces règles définissent le *terme de preuve* associé à une preuve. La notation $\pi : t \longrightarrow t'$ signifie que π est un terme de preuve qui montre que le terme t est équationnellement équivalent au terme t'.

On remarque que les termes basés sur la signature Σ sont plongé dans l'ensemble des termes de preuves en étant formés des règles **Réflexivité** et **Congruence**. La règle **Réflexivité** pour $t \longrightarrow t$ n'est d'ailleurs pas indispensable, étant donné qu'elle peut être remplacée par un arbre de

Réflexivité :

$$\frac{}{t : t \longrightarrow t}$$

Congruence :

$$\frac{\pi_1 : t_1 \longrightarrow t'_1 \quad \ldots \quad \pi_n : t_n \longrightarrow t'_n}{f(\pi_1, \ldots, \pi_n) : f(t_1, \ldots, t_n) \longrightarrow f(t'_1, \ldots, t'_n)}$$

Remplacement :
Pour toute règle ou axiome équationnel $\ell = (g(x_1, \ldots, x_n), d(x_1, \ldots, x_n)) \in E \cup R$,

$$\frac{\pi_1 : t_1 \longrightarrow t'_1 \quad \ldots \quad \pi_n : t_n \longrightarrow t'_n}{\ell(\pi_1, \ldots, \pi_n) : g(t_1, \ldots, t_n) \longrightarrow d(t'_1, \ldots, t'_n)}$$

Transitivité :

$$\frac{\pi_1 : t_1 \longrightarrow t_2 \quad \pi_2 : t_2 \longrightarrow t_3}{\pi_1 ; \pi_2 : t_1 \longrightarrow t_3}$$

Symétrie :

$$\frac{\pi : t_1 \longrightarrow t_2}{\pi^{-1} : t_2 \longrightarrow t_1}$$

FIG. 3.2 – Règle d'Inférence de la Logique Équationnelle

Congruence isomorphe à t. Les deux termes de preuves formés dans ces deux cas sont d'ailleurs les mêmes : t.

Certains termes de preuves définis ici sont « essentiellement les mêmes ». Par exemple, l'opérateur de transitivité ; devrait être considéré comme associatif, de façon à ce que les termes de preuves $(\pi_1;\pi_2);\pi_3$ et $\pi_1;(\pi_2;\pi_3)$ soient égaux. Ceci peut être obtenu en quotientant l'ensemble des termes de preuves par les règles de la figure 3.3.

Les règles **Associativité**, **Identités** et **Inverse** donne à l'algèbre des termes de preuve une structure de groupe. On peut par exemple montrer que $(\pi_1;\pi_2)^{-1}$ et $\pi_2^{-1};\pi_1^{-1}$ sont équivalents. On peut également montrer que $f(\pi_1, \ldots, \pi_n)^{-1}$ est équivalent à $f(\pi_1^{-1}, \ldots, \pi_n^{-1})$ — car

$$\begin{aligned}
f(\pi_1^{-1}, \ldots, \pi_n^{-1}) &\equiv f(\pi_1^{-1}, \ldots, \pi_n^{-1}); t' \\
&\equiv f(\pi_1^{-1}, \ldots, \pi_n^{-1}); (f(\pi_1, \ldots, \pi_n); f(\pi_1, \ldots, \pi_n)^{-1}) \\
&\equiv (f(\pi_1^{-1}, \ldots, \pi_n^{-1}); f(\pi_1, \ldots, \pi_n)); f(\pi_1, \ldots, \pi_n)^{-1} \\
&\equiv f(\pi_1^{-1}; \pi_1, \ldots, \pi_n^{-1}; \pi_n); f(\pi_1, \ldots, \pi_n)^{-1} \\
&\equiv f(t_1, \ldots, t_n); f(\pi_1, \ldots, \pi_n)^{-1} \\
&\equiv f(\pi_1, \ldots, \pi_n)^{-1}
\end{aligned} \quad .$$

Associativité :
Pour tous termes de preuve π_1, π_2, π_3,

$$\pi_1;(\pi_2;\pi_3) \equiv (\pi_1;\pi_2);\pi_3$$

Identités :
Pour tous termes de preuve $\pi : t \longrightarrow t'$,

$$\pi;t' \equiv t;\pi \equiv \pi$$

Préservation de la composition :
Pour tous termes de preuve $\pi_1, \ldots, \pi_n, \pi'_1, \ldots, \pi'_n$, pour tout symbole de fonction f,

$$f(\pi_1;\pi'_1, \ldots, \pi_n;\pi'_n) \equiv f(\pi_1, \ldots, \pi_n); f(\pi'_1, \ldots, \pi'_n)$$

Lemme des Mouvements Parallèles :
Pour toute règle de réécriture ou axiome équationnel $\ell = (g(x_1, \ldots, x_n), d(x_1, \ldots, x_n)) \in E \cup R$, pour tous termes de preuve $\pi_1 : t_1 \longrightarrow t'_1, \ldots, \pi_n : t_n \longrightarrow t'_n$,

$$\begin{aligned} \ell(\pi_1, \ldots, \pi_n) &\equiv \ell(t_1, \ldots, t_n); d(\pi_1, \ldots, \pi_n) \\ &\equiv g(\pi_1, \ldots, \pi_n); \ell(t'_1, \ldots, t'_n) \end{aligned}$$

Inverse :
Pour tout terme de preuve $\pi : t \longrightarrow t'$,

$$\begin{aligned} \pi;\pi^{-1} &\equiv t \\ \pi^{-1};\pi &\equiv t' \end{aligned}$$

FIG. 3.3 – Équivalence des Termes de Preuve

3.2.2 Preuve par Remplacement d'Égal par Égal

Cette représentation des preuves a été introduite par [Bachmair et Dershowitz, 1994, Bachmair, 1987] pour montrer la complétude de l'algorithme de complétion standard, en utilisant un ordre sur les preuves tel qu'elles décroissent à chaque étape de l'algorithme.

Une *étape de preuve équationnelle* est une expression $s \xleftarrow[e]{p} t$ où s et t sont des termes, ℓ est un axiome équationnel $u = v$, et p est une position de $\mathfrak{p}(s)$ tels que $s_{|p} = \sigma(u)$ et $t = s[\sigma(v)]_p$ pour une certaine substitution σ.

Une *preuve équationnelle* de $s_0 = t_n$ est une suite finie d'étapes de preuve équationnelle

$\left(s_i \xleftarrow[e_i]{p_i} t_i\right)_{i\in\{0,\dots,n\}}$ telle que $t_i = s_{i+1}$ pour tout $i \in \{0,\dots,n-1\}$. On la note

$$s_0 \xleftarrow[e_0]{p_0} s_1 \xleftarrow[e_1]{p_1} s_2 \cdots s_n \xleftarrow[e_n]{p_n} t_n$$

Une *étape de preuve de réécriture* est une expression $s \xrightarrow[\ell]{p} t$ ou $t \xleftarrow[\ell]{p} s$ où s et t sont des termes, ℓ est une règle de réécriture $u \to v$, et p est une position de $\mathfrak{p}(s)$ tels que $s_{|p} = \sigma(u)$ et $t = s[\sigma(v)]_p$ pour une certaine substitution σ.

Une *preuve par remplacement (d'égal par égal)* de $s_0 = t_n$ est une suite finie d'étapes de preuve équationnelle et d'étapes de preuve de réécriture $\left(s_i \overset{p_i}{\underset{\ell_i}{\leftrightarrows_i}} t_i\right)_{i\in\{0,\dots,n\}}$ où $\leftrightarrows_i \in \{\longleftrightarrow, \longrightarrow, \longleftarrow\}$ pour $i \in \{0,\dots,n\}$ et telle que $t_i = s_{i+1}$ pour tout $i \in \{0,\dots,n-1\}$. On la note

$$s_0 \overset{p_0}{\underset{\ell_0}{\leftrightarrows_0}} s_1 \overset{p_1}{\underset{\ell_1}{\leftrightarrows_1}} s_2 \cdots s_n \overset{p_n}{\underset{\ell_n}{\leftrightarrows_n}} t_n$$

3.2.3 Des Termes de Preuve aux Preuves par Remplacement

Pour avoir une correspondance entre ces deux représentations de preuve, on a besoin des règles d'équivalence sur les termes de preuve définies sur la figure 3.3. Celles-ci peuvent être raffinée pour donner le système de réécriture sur les termes de preuve $\rightsquigarrow$ donné sur la figure 3.4, de telle façon que les termes de preuve en forme normale pour ce système correspondent exactement aux preuves par remplacement.

L'associativité est toujours considérée comme une congruence, de telle sorte que le système de réécriture doit être considéré modulo l'associativité de ; qui sera notée $\sim$. Le système de réécriture de classes que l'on considère sera donc noté $\rightsquigarrow / \sim$. Comme ce système est linéaire au sens de la proposition 6.9, on peut utiliser le travail de [Huet, 1980b].

On démontre tout d'abord l'inclusion du système de réécriture dans la relation d'équivalence sur les termes de preuve de la figure 3.3.

Proposition 3.1 (Correction)**.** *Pour tous termes de preuve* π_1, π_2*, si* $\pi_1 \underset{\rightsquigarrow}{\longrightarrow} \pi_2$ *alors* $\pi_1 \equiv \pi_2$.

Démonstration. Comme $\equiv$ est une relation monotone et stable, il suffit en fait de montrer que $\pi_1 \rightsquigarrow \pi_2$ implique $\pi_1 \equiv \pi_2$, ce que peut être fait au cas par cas. □

La réciproque est fausse : par exemple $f(\ell_1,\ell_2) \equiv f(t_1,\ell_2);f(\ell_1,t_2')$ mais on n'a pas $f(\ell_1,\ell_2) \overset{*}{\underset{\rightsquigarrow}{\leftrightarrow}} f(t_1,\ell_2);f(\ell_1,t_2')$.

Pour montrer la terminaison de $\rightsquigarrow / \sim$, conformément à la proposition 6.7 on a besoin d'un ordre de réduction compatible avec l'associativité de ;. La plupart des travaux existant définissent des ordres de réduction compatibles avec l'associativité et la commutativité, donc comme on n'utilise ici que l'associativité on a besoin du lemme suivant :

Lemme 3.2. *Si* $A \subseteq B$ *alors* $>$ *est* B*-compatible implique* $>$ *est* A*-compatible.*

Démonstration. Il suffit de remarquer que $s' \xleftarrow[A]{*} s > t \xleftarrow[A]{*} t'$ implique $s' \xleftarrow[B]{*} s > t \xleftarrow[B]{*} t'$. □

Suppression des Identités Inutiles :
Pour tout terme de preuve $\pi : t \longrightarrow t'$,

$$\left.\begin{array}{l}\pi; t' \\ t; \pi\end{array}\right\} \rightsquigarrow \pi$$

Séquençage :
Pour tout symbole de fonction f, pour tous termes de preuve $\pi_1 : t_1 \longrightarrow t'_1, \ldots, \pi_n : t_n \longrightarrow t'_n$, s'il existe $i \neq j \in \{1, \ldots, n\}$ tel que $\pi_i \neq t_i$ et $\pi_j \neq t_j$,

$$f(\pi_1, \ldots, \pi_n) \rightsquigarrow f(\pi_1, t_2, \ldots, t_n); f(t'_1, \pi_2, \ldots, t_n); \ldots; f(t'_1, t'_2, \ldots, \pi_n)$$

Remontée de la Composition :
Pour tout $i \in \{1, \ldots, n\}$, pour tous Σ-termes $t_1, \ldots, t_n$, pour tout terme de preuve $\pi_i : t_i \longrightarrow t'_i, \pi'_i : t'_i \longrightarrow t''_i$, pour tout symbole de fonction f,

$$f(t_1, \ldots, \pi_i; \pi'_i, \ldots, t_n) \rightsquigarrow f(t_1, \ldots, \pi_i, \ldots, t_n); f(t_1, \ldots, \pi'_i, \ldots, t_n)$$

Mouvements Parallèles :
Pour toute règle de réécriture ou axiome équationnel $\ell = (g(x_1, \ldots, x_n), d(x_1, \ldots, x_n)) \in E \cup R$, pour tous termes de preuves $\pi_1 : t_1 \longrightarrow t'_1, \ldots, \pi_n : t_n \longrightarrow t'_n$, s'il existe $i \in \{1, \ldots, n\}$ tel que $\pi_i \neq t_i$,

$$\ell(\pi_1, \ldots, \pi_n) \rightsquigarrow \ell(t_1, \ldots, t_n); d(\pi_1, \ldots, \pi_n)$$

Suppression des Inverses Inutiles :
Pour tout Σ-terme t,

$$t^{-1} \rightsquigarrow t$$

Inversion de la Congruence :
Pour tous termes $t_1, \ldots, t_n$, pour tout $i \in \{1, \ldots, n\}$, pour tout terme de preuve $\pi_i : t_i \longrightarrow t'_i$, pour tout symbole de fonction f,

$$f(t_1, \ldots, \pi_i^{-1}, \ldots, t_n) \rightsquigarrow f(t_1, \ldots, \pi_i, \ldots, t_n)^{-1}$$

Inversion de la Composition :
Pour tous termes de preuve π_1, π_2,

$$(\pi_1; \pi_2)^{-1} \rightsquigarrow \pi_2^{-1}; \pi_1^{-1}$$

FIG. 3.4 – Système de Réécriture pour les Termes de Preuve

On peut par conséquent utiliser l'ordre *AC*-RPO de [Rubio et Nieuwenhuis, 1995] (voir la définition 6.24 page 50). On utilise une précédence telle que pour tout symbole de fonction f et pour toute étiquette de règle ℓ on ait $\ell > f > \cdot^{-1} >$;. L'ordre *AC*-RPO obtenu sera alors noté $\succ$.

On a alors besoin du lemme suivant :

Lemme 3.3. *Pour tout terme de preuve $\pi : t \longrightarrow t'$ on a $\pi \succeq t$ et $\pi \succeq t'$*

Démonstration. Par induction sur la structure du terme de preuve π.

Pour **Réflexivité**, $\pi = t = t'$.

Pour **Congruence**, $\pi = f(\pi_1,\ldots,\pi_n)$, $t = f(t_1,\ldots,t_n)$ et $t' = f(t'_1,\ldots,t'_n)$. Par hypothèse d'induction, pour tout $i \in \{1,\ldots,n\}$, on a $\pi_i \succeq t_i, t'_i$. De plus, π ne peut pas être réduit en tête en utilisant les règles (6.1), donc $snf(\pi) = \{f(\pi'_1,\ldots,\pi'_n) \ : \ \forall i,\ \pi'_i \in snf(\pi_i)\}$, tandis que t et t' ne sont pas réductible. Par conséquence, par définition d'un AC-RPO, $\pi \succeq t, t'$.

Pour **Remplacement**, $\pi = \ell(\pi_1,\ldots,\pi_n)$, $t = g(t_1,\ldots,t_n)$ et $t' = d(t'_1,\ldots,t'_n)$ où $\ell = (g,d) \in E \cup R$. Avec les mêmes arguments que pour **Congruence**, on peut conclure que $\pi \succeq t, t'$ (je rappelle que $\ell > g, d$).

Pour **Transitivité**, $\pi = \pi_1;\pi_2$ où $\pi_1 : t \longrightarrow t''$ et $\pi_2 : t'' \longrightarrow t'$. Par hypothèse d'induction, $\pi_1 \succeq t$ et $\pi_2 \succeq t'$. Comme $\succ$ est un ordre de simplification, $\pi \succ \pi_1, \pi_2 \succeq t, t'$.

Pour **Symétrie**, $\pi = \pi'^{-1}$ où $\pi' : t' \longrightarrow t$. Par hypothèse d'induction et comme $\succ$ est un ordre de simplification, $\pi \succ \pi' \succeq t', t$. □

Proposition 3.4 (Terminaison)**.** *Le système de réécriture $\rightsquigarrow$ de la figure 3.4 modulo $\sim$ termine pour les termes de preuves clos.*

Démonstration. On cherche à montrer que $\rightsquigarrow \subseteq \succ$, ce qui implique la terminaison de $\rightsquigarrow / \sim$:

Pour **Suppression des Identités Inutiles**, cela provient du fait que $\succ$ est un ordre de simplification.

Pour **Séquençage**, les règles (6.1) ne sont pas appliquables sur le côté gauche, tandis qu'elle mène avec le côté droit à $;(f(\pi_1,t_2,\ldots,t_n), f(t'_1,\pi_2,\ldots,t_n),\ldots,f(t'_1,t'_2,\ldots,\pi_n))$. On a $f >$; donc par définition d'un RPO on doit montrer que pour tout $i \in \{1,\ldots,n\}$ on a $f(\pi_1,\ldots,\pi_n) >_{rpo} f(t'_1,\ldots,t'_{i-1},\pi_i,t_{i+1},\ldots,t_n)$, c'est-à-dire $(\pi_1,\ldots,\pi_n) >^{lex}_{rpo} (t'_1,\ldots,t'_{i-1},\pi_i,t_{i+1},\ldots,t_n)$. Par hypothèse il existe au moins un $j \in \{1,\ldots,n\} \setminus \{i\}$ tel que $\pi_j \neq t_j$, ce qui permet de conclure avec le lemme précédent.

Pour **Remontée de la Composition**, aucun des deux côtés n'est réductible en utilisant les règles (6.1). On a $f >$; donc on doit montrer $f(t_1,\ldots,\pi_i;\pi'_i,\ldots,t_n) >_{rpo} f(t_1,\ldots,\pi_i,\ldots,t_n)$ et $f(t_1,\ldots,\pi_i;\pi'_i,\ldots,t_n) >_{rpo} f(t_1,\ldots,\pi'_i,\ldots,t_n)$. Les deux comparaisons sont une conséquence de la définition d'un RPO.

Pour **Mouvements Parallèles**, aucun des deux côtés n'est réductible en utilisant les règles (6.1). On a $\ell >$; donc on doit montrer $\ell(\pi_1,\ldots,\pi_n) >_{rpo} \ell(t_1,\ldots,t_n)$ et $\ell(\pi_1,\ldots,\pi_n) >_{rpo} d(\pi_1,\ldots,\pi_n)$. La première comparaison provient du lemme précédent et du fait qu'il existe $i \in \{1,\ldots,n\}$ tel que $\pi_i \neq t_i$; la deuxième tient au fait que $\ell > d$.

Pour **Suppression des Inverses Inutiles**, c'est une conséquence du fait que $\succ$ est un ordre de simplification.

Pour **Inversion de la Congruence**, aucun des deux côtés n'est réductible en utilisant les règles (6.1), donc c'est une conséquence de $f > \cdot^{-1}$.

For **Inversion de la Composition**, aucun des deux côtés n'est réductible en utilisant les règles (6.1), donc c'est une conséquence de $\cdot^{-1} >$;. □

On peut également montrer la confluence :

Proposition 3.5 (Confluence)**.** *Le système de réécriture $\rightsquigarrow$ est confluent modulo $\sim$ sur les termes de preuve clos.*

Démonstration. Comme $\rightsquigarrow / \sim$ est linéaire et termine, il suffit que les paires critiques sont confluentes (voir la proposition 6.9 page 50).

Pour $\underset{R}{\longleftarrow} \circ \underset{R}{\longrightarrow}$, il est facile de montrer pour la plupart des paires critiques qu'elles sont bien confluentes. Je détaille ici la plus problématique. Pour deux applications imbriquées de **Séquençage**, on a par exemple pour $f(g(\nu_1,\ldots,\nu_m),\pi_1,\ldots,\pi_n)$ qui peut être réécrit en $f(g(\nu_1,\ldots,\nu_m),t_1,\ldots,t_n);f(g(s_1,\ldots,s_m),\pi_1,\ldots,t_n);\ldots;f(g(s_1,\ldots,s_m),t'_1,\ldots,\pi_n)$ et en $f(g(\nu_1,\ldots,s_m);\ldots;g(s'_1,\ldots,\nu_m),\pi_1,\ldots,\pi_n)$. Tous les deux se réécrivent en $f(g(\nu_1,\ldots,s_m);\ldots;g(s'_1,\ldots,\nu_m),t_1,\ldots,t_n);f(g(s_1,\ldots,s_m),\pi_1,\ldots,t_n);\ldots;f(g(s_1,\ldots,s_m),t'_1,\ldots,\pi_n)$.

Pour $\underset{R}{\longleftarrow} \circ \underset{A}{\longleftrightarrow}$, les seules règles qui interfèrent avec $\sim$ sont **Suppression des Identités Inutiles**, **Remontée de la Composition** et **Inversion de la Composition**. On peut montrer que les paires critiques résultant de ces règles sont confluentes. □

Le système de réécriture de termes de preuve $\rightsquigarrow$ nous donne une correspondance entre les termes de preuve et les preuves par remplacement : les formes normales des termes de preuve pour ce système correspondent en effet exactement aux preuves par remplacement. Ceci est exprimé dans le théorème suivant, qui est par conséquent une généralisation du lemme 3.6 de [Meseguer, 1992] pour la logique équationnelle, pour laquelle on a opérationnalisé la façon de construire la chaîne de « réécriture séquentielle par étape ».

THÉORÈME 3.6 (Correspondance entre les Représentation de Preuves)**.**
La forme normale pour le système de réécriture de classe $\rightsquigarrow$ / $\sim$, notée $nf(\pi)$, d'un terme de preuve π a la forme suivante :
il existe $n \in \mathbb{N}$, des contextes $w_1[],\ldots,w_n[]$, des indices $i_1,\ldots,i_n \in \{-1,1\}$, des étiquettes de règles $\ell_1,\ldots,\ell_n$ et des termes $t^1_1,\ldots,t^1_{m_1},\ldots,t^n_1,\ldots,t^n_{m_n}$ tels que

$$nf(\pi) = (w_1[\ell_1(t^1_1,\ldots,t^1_{m_1})])^{i_1};\ldots;(w_n[\ell_n(t^n_1,\ldots,t^n_{m_n})])^{i_n}$$

où ν^1 est une notation pour ν.

Un tel terme de preuve correspond à la preuve par remplacement suivante :

$$w_1[g_1(t^1_1,\ldots,t^1_{m_1})] \underset{\ell_1}{\overset{p_1}{\leftrightarrows_1}} w_1[d_1(t^1_1,\ldots,t^1_{m_1})] \underset{\ell_2}{\overset{p_2}{\leftrightarrows_2}} \cdots w_n[g_n(t^n_1,\ldots,t^n_{m_n})] \underset{\ell_n}{\overset{p_n}{\leftrightarrows_n}} w_n[d_n(t^n_1,\ldots,t^n_{m_n})]$$

où pour tout $j \in \{1,\ldots,n\}$ on a :
- *$\ell_j = (g_j, d_j)$,*
- *p_j est la position de $[]$ dans $w_j[]$,*
- *$\leftrightarrows_j = \begin{cases} \longrightarrow & \text{si } i_j = 1 \text{ et } \ell_j \in R, \\ \longleftarrow & \text{si } i_j = -1 \text{ et } \ell_j \in R, \\ \longleftrightarrow & \text{si } \ell_j \in E. \end{cases}$*
- *si $j \neq n$, $w_j[d_j(t^j_1,\ldots,t^j_{m_j})] = w_{j+1}[g_{j+1}(t^{j+1}_1,\ldots,t^{j+1}_{m_{j+1}})]$.*

Démonstration. Il faut d'abord vérifier que les termes de preuve de la forme proposée sont bien irréductibles, ce qui est laissé au lecteur.

Considérons maintenant un terme de preuve irréductible. Comme on ne peut pas appliquer **Séquençage**, il y a au plus un ; sous chaque symbole de fonction. Comme on ne peut pas appliquer **Remontée de la Composition**, il n'y en a en fait aucun. Comme **Inversion de la Composition** et **Inversion de la Congruence** ne peuvent pas être appliquée, les $^{-1}$ sont appliqués entre ; et les symboles de fonction. Les termes de preuve irréductibles sont donc des applications de ; sur éventuellement $^{-1}$ sur des termes de base formés à partir de symboles de fonction et d'étiquettes de règle.

Comme on ne peut pas appliquer **Suppression des Identités Inutiles** ni **Suppression des Inverses Inutiles**, il y a au moins une étiquette de règle dans chacun de ces termes de base. Comme on ne peut pas appliquer **Séquençage**, il y en a au plus un. Comme on ne peut pas appliquer **Mouvements Parallèles**, les étiquettes de règle sont appliquées à des Σ-termes. Par conséquent, chaque terme de base contient une et une seule étiquette de règle appliquée à des Σ-termes.

On obtient bien la forme voulue. □

Exemple 3.1*:* Si $\pi = f(\ell_1(\ell_2),(\ell_3;r)^{-1})$ où $\ell_1 : g(x) \longrightarrow d(x)$, $\ell_2 : s = t$, $\ell_3 : l \longrightarrow r$, on a :

$$\begin{aligned}
\pi &\underset{\rightsquigarrow,\sim}{\longrightarrow} f(\ell_1(s);d(\ell_2),(\ell_3;r)^{-1}) && \textbf{(Mouvements Parallèles)}\\
&\underset{\rightsquigarrow,\sim}{\longrightarrow} f(\ell_1(s);d(\ell_2),r);f(d(t),(\ell_3;r)^{-1}) && \textbf{(Séquençage)}\\
&\underset{\rightsquigarrow,\sim}{\longrightarrow} f(\ell_1(s);d(\ell_2),r);f(d(t),r^{-1};\ell_3^{-1}) && \textbf{(Inversion de la Composition)}\\
&\underset{\rightsquigarrow,\sim}{\longrightarrow} f(\ell_1(s);d(\ell_2),r);f(d(t),r;\ell_3^{-1}) && \textbf{(Suppression des Inverses Inutiles)}\\
&\underset{\rightsquigarrow,\sim}{\longrightarrow} f(\ell_1(s);d(\ell_2),r);f(d(t),\ell_3^{-1}) && \textbf{(Suppression des Identités Inutiles)}\\
&\underset{\rightsquigarrow,\sim}{\longrightarrow} f(\ell_1(s),r);f(d(\ell_2),r);f(d(t),\ell_3^{-1}) && \textbf{(Remontée de la Composition)}\\
&\underset{\rightsquigarrow,\sim}{\longrightarrow} f(\ell_1(s),r);f(d(\ell_2),r);f(d(t),\ell_3)^{-1} && \textbf{(Inversion de la Congruence)}
\end{aligned}$$

On obtient ainsi la forme normale, qui correspond à la preuve par remplacement $f(g(s),r) \xrightarrow[\ell_1]{1} f(d(s),r) \xleftrightarrow[\ell_2]{11} f(d(t),r) \xleftarrow[\ell_3]{2} f(d(t),l)$.

Grâce à ce théorème, les formes normales des termes de preuve seront considérées dans la suite indifféremment comme des termes de preuve ou comme des preuves par remplacement.

3.2.4 Représentation de Preuve Utilisée

Pour appliquer la théorie des systèmes canoniques abstraits, on utilisera la représentation par *termes de preuve*, et la relation de sous-preuve sera alors celle de *sous-terme*.

3.3 Ordre sur les Preuves

La représentation des preuves par remplacement a été défini par Bachmair [Bachmair et Dershowitz, 1994] pour introduire un ordre sur les preuves : étant donné un ordre de réduction $\gg$, à chaque étape de preuve $s \underset{\ell}{\overset{p}{\leftrightarrow}} t$ est associé un *coût*. Le coût d'une étape de preuve équationnelle $s \underset{u=v}{\overset{p}{\longleftrightarrow}} t$ est le triplet $(\{\!\{s,t\}\!\},u,t)$. Le coût d'une étape de preuve de réécriture $s \underset{u\to v}{\overset{p}{\longrightarrow}} t$ est $(\{\!\{s\}\!\},u,t)$. Les étapes de preuve sont comparées les unes aux autres d'après leur coût, en utilisant la combinaison lexicographique de l'extension multi-ensemble $\gg_{mult}$ de l'ordre de réduction sur les termes sur la première composante, l'ordre d'inclusion totale $\blacktriangleright$ sur la deuxième, et l'ordre de réduction sur les termes $\gg$ sur la dernière. Les preuves par remplacement sont comparées comme le multi-ensemble de leurs étapes de preuves. Pour deux preuves par remplacement p et q, on notera $p >_{remp} q$ si p est plus grand que q pour cet ordre.

En utilisant le théorème 3.6, on peut traduire l'ordre que l'on vient de définir aux termes de preuves :

Définition 3.1 (Ordre de Bachmair pour les Termes de Preuves)**.** *Pour tous termes de preuves* π_1, π_2 *on dira que* $\pi_1 >_B \pi_2$ *si*

$$nf(\pi_1) >_{remp} nf(\pi_2)$$

Exemple 3.2*:* Soient $\pi_1 = f(\ell_1^{-1}; \ell_2)$ et $\pi_2 = f(\ell_3)$ où $\ell_1 = a \longrightarrow b$, $\ell_2 = a \longrightarrow c$ et $\ell_3 = b = c$, et supposons $a > b > c$.

On a $nf(\pi_1) = f(b) \xleftarrow[\ell_1]{1} f(a) \xrightarrow[\ell_2]{1} f(c)$ et $nf(\pi_2) = f(b) \xrightarrow[\ell_3]{1} f(c)$. Le coût de $nf(\pi_1)$ est $\{\!\{(\{\!\{f(a)\}\!\}, a, f(b)), (\{\!\{f(a)\}\!\}, a, f(c))\}\!\}$, celui de $nf(\pi_2)$ est $\{\!\{(\{\!\{f(b), f(c)\}\!\}, b, f(c))\}\!\}$, donc $nf(\pi_1) >_{remp} nf(\pi_2)$ et $\pi_1 >_B \pi_2$.

Néanmoins, on ne peut pas espérer étendre un ordre RPO sur les Σ-termes vers un RPO[3] $>_{rpo}$ sur les termes de preuve de telle façon que $>_B$ et $>_{rpo}$ coïncident sur les formes normales des termes de preuves :

Contre-exemple 3.3*:* Soit la signature $\Sigma = \{f^1, a^0, b^0, c^0\}$ où les exposants des symboles de fonction dénotent leur arité. Soit une précédence $f > a > b > c$, on s'intéresse à l'ordre RPO construit sur cette précédence.

Soit $\ell_f = f(a) \longrightarrow c$ et $\ell_b = b \longrightarrow c$.

On cherche maintenant à étendre la précédence à ℓ_f et ℓ_b de façon à obtenir un RPO sur les termes de preuve qui coïncide avec $>_B$. Si $\ell_f < \ell_b$, $f(a) \xrightarrow[\ell_f]{\varepsilon} c >_{remp} b \xrightarrow[\ell_b]{\varepsilon} c$ mais $\ell_f <_{rpo} \ell_b$.

Si on suppose $f > \ell_f > \ell_b$ on a $f(a) \xrightarrow[\ell_f]{\varepsilon} c >_{remp} f(b) \xrightarrow[\ell_b]{1} f(c)$ mais $\ell_f <_{rpo} f(\ell_b)$.

Si on suppose $\ell_f > \ell_b$ et $\ell_f > f$, alors $f(f(b)) \xrightarrow[\ell_b]{11} f(f(c)) >_{remp} f(a) \xrightarrow[\ell_f]{\varepsilon} c$ mais $f(f(\ell_b)) <_{rpo} \ell_f$.

Cette extension est donc impossible, il n'existe pas d'extension de $>_{rpo}$ sur les termes de preuve de telle sorte que pour tout termes de preuve π_1, π_2 on ait $nf(\pi_1) >_{rpo} nf(\pi_2)$ si et seulement si $nf(\pi_1) >_B nf(\pi_2)$.

Pour appliquer la théorie des systèmes canoniques abstraits, on prendra comme ordre sur les preuves l'ordre $>_B$ restreint aux termes de preuve de même conclusion.

3.4 Vérification des Postulats

Les postulats A, B, C et D sont trivialement vérifiés. Seul le postulat E demande un certain effort.

On montre tout d'abord le lemme suivant :

Lemme 3.7. *Pour tout symbole de fonction* f *d'arité* $n+1$*, pour tous termes de preuves* $\pi_1, \ldots, \pi_n$*,* q *et* r*,*

$$q > r \text{ implique } f(\pi_1, \ldots, q, \ldots, \pi_n) > f(\pi_1, \ldots, r, \ldots, \pi_n)$$

Démonstration. Supposons $q > r$, par définition $nf(q) >_{remp} nf(r)$. Pour comparer $f(\pi_1, \ldots, q, \ldots, \pi_n)$ et $f(\pi_1, \ldots, r, \ldots, \pi_n)$, on doit les transformer en preuves par remplacement

[3] ou mieux un *AC*-RPO

On a

$$\begin{array}{rcl} f(\pi_1,\ldots,q,\ldots,\pi_n) & \xrightarrow[\rightsquigarrow]{}{}^{*} & f(\pi_1,t_2,\ldots,t_n);\ldots;f(t'_1,\ldots,q,\ldots,t_n);\ldots;f(t'_1,\ldots,\pi_n) \\ & \xrightarrow[\rightsquigarrow]{}{}^{*} & f(\pi_1,t_2,\ldots,t_n);\ldots;\underline{f(t'_1,\ldots,nf(q),\ldots,t_n)};\ldots;f(t'_1,\ldots,\pi_n) \end{array}$$

Ensuite, si $nf(q)$ contient ; le terme souligné sera décomposé par **Remontée de la Composition**. S'il contient $^{-1}$ la règle **Inversion de la Congruence** sera appliquée. Des termes en dehors du terme souligné seront éliminé par **Suppression des Identités Inutiles**, et la forme normale ressemblera à

$$f(\pi_1,t_2,\ldots,t_n);\ldots;\underline{f(t'_1,\ldots,q_1,\ldots,t_n)^{i_1};\ldots;f(t'_1,\ldots,q_m,\ldots,t_n)^{i_m}};\ldots;f(t'_1,\ldots,\pi_n)$$

avec $nf(q) = q_1^{i_1};\ldots;q_m^{i_m}$.

La même chose va se passer pour r, et par conséquent, pour comparer les preuves initiales, il suffit de comparer les termes soulignés.

Le coût de $nf(q)$ est de la forme $\{\!\{(\{\!\{s_1\}\!\},u_1,h_1),\ldots,(\{\!\{s_m\}\!\},u_m,h_m)\}\!\}$. Celui de $f(t'_1,\ldots,q_1,\ldots,t_n)^{i_1};\ldots;f(t'_1,\ldots,q_m,\ldots,t_n)^{i_m}$ sera alors $\{\!\{(\{\!\{f(t'_1,\ldots,s_1,\ldots,t_n)\}\!\},u_1,f(t'_1,\ldots,h_1,\ldots,t_n)),\ldots,(\{\!\{f(t'_1,\ldots,s_m,\ldots,t_n)\}\!\},u_m,f(t'_1,\ldots,h,m,\ldots,t_n))\}\!\}$. Pour $nf(r)$ il seront respectivement $\{\!\{(\{\!\{g_1\}\!\},v_1,d_1),\ldots,(\{\!\{g_p\}\!\},v_p,d_p)\}\!\}$ et $\{\!\{(\{\!\{f(t'_1,\ldots,g_1,\ldots,t_n)\}\!\},v_1,f(t'_1,\ldots,d_1,\ldots,t_n)),\ldots,(\{\!\{f(t'_1,\ldots,g_p,\ldots,t_n)\}\!\},v_p,f(t'_1,\ldots,d_p,\ldots,t_n))\}\!\}$.

$\gg$, qui est utilisé pour comparer les composantes des coûts qui sont modifiées par l'application de f, est un ordre de réduction, donc $nf(q) >_{remp} nf(r)$ implique $f(t'_1,\ldots,q_1,\ldots,t_n)^{i_1};\ldots;f(t'_1,\ldots,q_m,\ldots,t_n)^{i_m} >_{remp} f(t'_1,\ldots,r_1,\ldots,t_n)^{i_1};\ldots;f(t'_1,\ldots,r_p,\ldots,t_n)^{i_p}$. □

On peut montrer la même chose pour les étiquettes des règles :

Lemme 3.8. *Pour toute étiquette de règle ℓ, pour tous termes de preuve $\pi_1,\ldots,\pi_n$, q et r,*

$$q > r \text{ implique } \ell(\pi_1,\ldots,q,\ldots,\pi_n) > \ell(\pi_1,\ldots,r,\ldots,\pi_n)$$

Démonstration. $\ell(\pi_1,\ldots,q,\ldots,\pi_n)$ et $\ell(\pi_1,\ldots,r,\ldots,\pi_n)$ peuvent être réduits par **Mouvements Parallèles** en $\ell(t_1,\ldots,t_n);d(\pi_1,\ldots,q,\ldots,\pi_n)$ et $\ell(t_1,\ldots,t_n);d(\pi_1,\ldots,r,\ldots,\pi_n)$. On peut conclure en utilisant le lemme précédent.

□

On peut alors montrer

THÉORÈME 3.9 (Postulat E pour les Preuves Équationnelles)**.**
Pour toute position i, pour tous termes de preuves p,r tels que $i \in \mathfrak{p}(p)$,

$$p_{|i} > r \text{ implique } p > p[r]_i$$

Démonstration. On peut prouver ceci par induction sur i. Pour $i = \varepsilon$ c'est trivial. Pour $i \neq \varepsilon$, par hypothèse d'induction le résultat est vrai pour tous les sous-preuves de p. Considérons la tête de p :

- pour **Symétrie**, c'est trivial ;
- pour **Transitivité**, ceci provient du fait que les preuves équationnelles sont comparées comme le multi-ensemble de leurs étapes ;
- pour **Congruence**, c'est un corollaire du lemme 3.7 ;
- pour **Remplacement**, c'est un corollaire du lemme 3.8.

□

3.5 Complétude de la Complétion Standard

3.5.1 La Complétion Standard est Saine et Adéquate

Ceci est montré dans [Bachmair, 1987, lemme 2.1] : si $E,R \rightsquigarrow E',R'$, alors $\overset{*}{\underset{E\cup R}{\longleftrightarrow}}$ et $\overset{*}{\underset{E'\cup R'}{\longleftrightarrow}}$ sont les mêmes relations. Pour démontrer ceci, il faut le vérifier pour chaque règle d'inférence de la complétion standard (figure 3.1), ce qui est laissé au lecteur.

3.5.2 La Complétion Standard est Bonne

Ceci est montré dans [Bachmair, 1987, lemmes 2.5, 2.6] : si $E,R \rightsquigarrow E',R'$, alors les preuves dans E,R peuvent être transformée en preuves dans E',R' en utilisant les règles suivantes :

$$
\begin{array}{rcl}
s \underset{E}{\longleftrightarrow} t & \twoheadrightarrow & s \underset{R'}{\longrightarrow} t \\
s \underset{E}{\longleftrightarrow} t & \twoheadrightarrow & s \underset{R'}{\longrightarrow} u \underset{E'}{\longleftrightarrow} t \\
s \underset{E}{\longleftrightarrow} s & \twoheadrightarrow & s \\
s \underset{R}{\longleftarrow} u \underset{R}{\longrightarrow} t & \twoheadrightarrow & s \underset{E'}{\longleftrightarrow} t \\
s \underset{R}{\longleftarrow} u \underset{R}{\longrightarrow} t & \twoheadrightarrow & s \overset{*}{\underset{R'}{\longrightarrow}} v \overset{*}{\underset{R'}{\longleftarrow}} t \\
s \underset{R}{\longrightarrow} t & \twoheadrightarrow & s \underset{R'}{\longrightarrow} v \underset{R'}{\longleftarrow} t \\
s \underset{R}{\longrightarrow} t & \twoheadrightarrow & s \underset{R'}{\longrightarrow} v \underset{E'}{\longleftrightarrow} t
\end{array}
$$

Comme $\underset{\twoheadrightarrow}{\longrightarrow} \subseteq >$, les preuves deviennent effectivement meilleures.

3.5.3 La Complétion Standard est Canonique

Je rappelle que par hypothèse d'équité, $E_\infty = \emptyset$.

Lemme 3.10. *Pour toute dérivation $(E_i,R_i)_i$ de la complétion standard,*

$$E_0^\sharp \subseteq R_\infty$$

Démonstration. Par contradiction, supposons qu'il existe $(a,b) \in E_0^\sharp \setminus R_\infty$, étiquetée par ℓ. Comme la complétion standard est adéquate, il existe $p \in \mu Pf(R_\infty)$ prouvant $a = b$. Comme $a = b \in E_0^\sharp$, $\ell(x_1,\ldots,x_n) \in Nf(E_0) = Nf(R_\infty)$ où $(x_i)_i$ de telle sorte que

$$p > \ell(x_1,\ldots,x_n)$$

- S'il n'y a pas de pic dans $nf(p)$, alors $nf(p)$ est une preuve en vallée, et il est facile de montrer qu'elle est plus petite que $\ell(x_1,\ldots,x_n)$, ce qui entre en contradiction avec ce que l'on vient de dire.
- S'il y a un pic parallèle (c'est-à-dire s'il y a un terme qui se réécrit dans deux sous-termes distincts), par exemple $s[c,e] \underset{\ell_1}{\overset{i}{\longleftarrow}} s[d,e] \underset{\ell_2}{\overset{j}{\longrightarrow}} s[d,f]$, alors la preuve par remplacement où ce pic est remplacé par $s[c,e] \underset{\ell_2}{\overset{j}{\longrightarrow}} s[c,f] \underset{\ell_1}{\overset{i}{\longleftarrow}} s[d,f]$ est plus petite, ce qui entre en contradiction avec la minimalité de p dans $Pf(R_\infty)$.

– S'il y a un pic critique, alors par hypothèse d'équité il existe une étape k où la paire critique résultante est générée par **Déduit**. La preuve de la conclusion du pic critique à l'étape $k+1$ est donc plus petite. Comme la complétion standard est bonne, on peut toujours trouver une preuve plus petite ou égale à celle-ci aux étapes suivantes. À la limite, on peut remplacer le pic critique par cette dernière dans p pour obtenir une preuve plus petite, ce qui entre en contradiction avec la minimalité de p dans $Pf(R_\infty)$.

□

Lemme 3.11. *Pour toute dérivation $(E_i,R_i)_i$ de la complétion standard qui* termine sans échec*,*

$$R_\infty \subseteq E_0^\sharp$$

Démonstration. Par l'absurde, supposons qu'il existe $(a,b) \in R_\infty \setminus E_0^\sharp$, étiquetée ℓ. Alors il existe une preuve $p \in \mu Pf(E_0^\sharp)$ telle que $\ell(x_1,\ldots,x_n) > p$ où $x_1,\ldots,x_n$ sont les variables libres de ℓ.

Les règles de R_∞ proviennent de l'orientation d'axiomes équationnels par **Oriente**, donc $a \gg b$. Le coût de $\ell(x_1,\ldots,x_n)$ est alors $\{\!\{(\{\!\{a\}\!\},a,b)\}\!\}$. Considérons l'étape la plus à gauche de $nf(p)$. Elle est de la forme $a \overset{i}{\underset{(c,d)}{\leftrightarrows}} a[d]_i$ où $c = a_{|i}$. Si c'est $a \overset{i}{\underset{d\to c}{\longleftarrow}} a[d]_i$ alors le coût de cette étape de preuve est $\{\!\{(\{\!\{a[d]_i\}\!\},d,a)\}\!\}$, ce qui est plus grand que $\{\!\{(\{\!\{a\}\!\},a,b)\}\!\}$, ce qui entre en contradiction avec le fait que $\ell(x_1,\ldots,x_n) > p$. Si c'est $a \overset{i}{\underset{c=d}{\longleftrightarrow}} a[d]_i$ alors le coût de cette étape de preuve est $\{\!\{(\{\!\{a,a[d]_i\}\!\},c,a[d]_i)\}\!\}$, ce qui est plus grand que $\{\!\{(\{\!\{a\}\!\},a,b)\}\!\}$, ce qui entre en contradiction avec le fait que $\ell(x_1,\ldots,x_n) > p$. Si c'est $a \overset{i}{\underset{c\to d}{\longrightarrow}} a[d]_i$ alors il y a une paire critique $(b,a[d]_i)$ dans R_∞ (on vient juste de montrer que $E_0^\sharp \subseteq R_\infty$, donc $c \to d \in R_\infty$). L'hypothèse d'équité peut donc s'appliquer, et la règle **Deduce** va produire l'axiome équationnel $b = a[d]_i$, qui sera ensuite orienté puisqu'il n'y a pas d'échec, et $a \longrightarrow b \in R_\infty$ sera simplifié par **Compose** ou **Collapse**. Comme $a \longrightarrow b$ est persistante, elle doit être générée une nouvelle fois, ce qui entre en contradiction avec la terminaison de la complétion. □

THÉORÈME 3.12.
La complétion standard produit — quand elle termine sans échec — la base canonique.

Démonstration. Il n'y a rien de plus à prouver, car on a $R_\infty = E_0^\sharp$, et la complétion standard est bonne donc on peut utiliser le théorème 2.13.

On peut remarquer que dans ce cas, la complétion standard est uniformément équitable car $R_\infty \setminus E_0^\sharp = \emptyset$. □

Remarque: Quand la complétion standard termine, l'ensemble de règles résultant R_∞ est *saturé*, car $E_0^\sharp = R_\infty^\sharp \subseteq R_\infty$ (théorème 2.6), mais il n'est pas forcément *contracté*.

On a donc montré que le cadre des systèmes canoniques abstraits s'applique au cas de la complétion standard. Ce n'est pas surprenant, car il a été formé autour de telles procédures. Néanmoins il était nécessaire d'en avoir une preuve formelle, et cette preuve détaillée est loin d'être triviale.

Chapitre 4

Conclusion

Au cours de ce stage, deux axes principaux ont été explorés : d'une part l'étude de formalismes logiques pour lesquels les sous-preuves peuvent utiliser des hypothèses différentes de la preuve initiale, comme par exemple pour les systèmes de séquents ; d'autre part l'application à la complétion du cadre des systèmes canoniques abstraits.

Pour pouvoir l'appliquer aux formalismes mentionés ci-dessus, le cadre des systèmes canoniques abstraits a du être généralisé. Ceci a été fait en supprimant le postulat D et en transformant le postulat E en E_{gen}. J'ai obtenu ainsi une généralisation conservative, dans le sens où on peut l'appliquer aux formalismes pour lesquels on pouvait appliquer le cadre original, et j'ai pu redémontrer dans ce nouveau cadre l'ensemble des résultats obtenu avec l'original, en modifiant certaines définitions et certains lemmes quand cela s'averait nécessaire (voir la section 7.2.2 pour voir l'ensemble des démonstrations, lemmes et définitions modifiés). Une autre solution, si on avait voulu appliquer le cadre original à tout prix, aurait été d'utiliser une représentation des preuves différente, par exemple une représentation où les hypothèses apparaissent comme les feuilles de la preuve vue comme un arbre. C'est par exemple le cas pour certaines représentation de la logique linéaire.

J'ai montré que si l'on utilise comme ordre sur les preuves en déduction naturelle propositionnelle la fermeture transitive de la β-réduction, les preuves minimales correspondent exactement aux preuves sans coupures. Cette approche peut être généralisée à des systèmes de séquents plus riches. En effet, on a uniquement besoin pour cela d'un système qui possède une réduction associée fortement normalisante et qui correspond à un processus d'élimination des coupures. Par exemple, on pourrait a priori appliquer ceci au calcul des séquents grâce au travail de Herbelin sur le $\bar{\lambda}$-calcul et ses réductions associées [Herbelin, 1995] et à la logique linéaire avec les réductions des réseaux de preuve [Cosmo et Guerrini, 1999]. Il serait intéressant de voir comment cette méthode pourrait être adaptée à la théorie des types de Martin-Löf [Martin-Löf, 1984] ou une de ses extensions, ou bien au calcul des séquents modulo [Dowek et al., 2003] avec le ρ-calcul associé [Wack, 2005].

En ce qui concerne la complétion, ce rapport montre que le cadre des systèmes canoniques abstraits peut être appliqué pour la complétion close et la complétion standard. Les deux preuves qui sont données ici sont complètement détaillée (voir les chapitres 3, 8, et 9). L'étude de la complétion standard nous a amené à comparer deux représentations de preuves. La première, qui consiste en des termes de preuves comme dans [Meseguer, 1992], est utile quand on a besoin de sous-preuve et de remplacement. La seconde, comme présentée dans [Bachmair et Dershowitz, 1994], est complètement adaptée si on veut montrer la complétude de la complétion standard. J'ai donc proposé un moyen de passer de l'une vers l'autre grâce au système de réécriture de termes de preuve présenté en figure 3.4, ce qui m'a permis d'utiliser l'ordre défini par Bachmair et Dershowitz sur les termes de preuves. Une fois les postulats des systèmes canonique abstraits vé-

rifiés, la démonstration de la complétude de la complétion standard est alors la même que dans [Bachmair et Dershowitz, 1994].

Le cadre des systèmes canoniques abstraits a été introduit pour unifier l'ensemble des procédures de complétion. Ce travail fournit donc un premier élément pour dire qu'il correspond bien à son objectif. Il faut maintenant vérifier qu'il convient également pour d'autres procédures de complétion. Un ordre sur les preuves est également défini dans [Bachmair, 1987] pour la complétion modulo, ce qui laisse penser que cette dernière rentre également dans le cadre des systèmes canoniques abstraits. Il faudra aussi regarder comment ce cadre s'adapte à d'autres mécanismes de déduction, comme l'algorithme de Buchberger [Buchberger, 1965] et la résolution [Robinson, 1965].

Perspectives

Si on revient sur les systèmes de séquent, il serait également intéressant d'utiliser d'autres ordres sur les preuves. Comme les preuves en déduction naturelle sont représentées par des λ-termes, on peut ainsi penser utiliser l'ordre récursif sur les chemins d'ordre supérieur (Higher Order RPO) [Jouannaud et Rubio, 1996].

De même, si les preuves sans coupures sont pratiques d'un point calculatoire, ce qui les rend bien adaptée à la démonstration automatique, elles ne correspondent pas à l'idée qu'un mathématicien se fait d'une « bonne » preuve. Les lemmes qui sont mis à plat dans les preuves sans coupure sont utiles pour la compréhension d'une preuve par un être humain. Il serait intéressant de voir comment cette autre notion de bonne preuve peut être traduite dans le formalisme des systèmes canoniques abstraits. L'utilisation d'un nombre correct de lemme (pas trop peu pour des raisons de compréhension, pas trop pour ne pas introduire des lemmes inutiles) semble être lié à la β-réduction optimale, grâce à l'isomorphisme de Curry-Howard : un lemme doit être introduit s'il servira à plusieurs reprise dans la preuve, ce qui correspond à un λ-terme de la forme $(\lambda x.w[x,x])l$, mais il ne doit pas être introduit s'il n'est jamais utilisé, ce qui correpond à un λ-terme de la forme $(\lambda x.t)l$ où x n'apparaît pas librement dans t.

En ce qui concerne les termes de preuve introduits par [Meseguer, 1992], ils constituent une des bases du ρ-calcul [Cirstea et al., 2003, `http://rho.loria.fr/`]. La relation entre les procédures de complétion et les systèmes de séquents mentionnés ci-dessus peut donc probablement être trouvé ici. Un tel lien a déjà été relevé par Dowek dans un papier où il montre que les systèmes de réécriture confluents peuvent être mis en relation avec des preuves sans coupures d'un certain système de séquents [Dowek, 2003].

Par ailleurs, le fait d'avoir rendu le plus formel possible le cadre des systèmes canoniques abstraits laisse entrevoir la possibilité d'une utilisation dans un outil de démonstration interactive de théorème comme Coq [`http://coq.inria.fr/`]. On pourrait ainsi obtenir des preuves formelles de la complétude des différentes procédures de complétion, ce qui ne semble pas encore exister à ce jour.

Enfin, il existe d'autres cadres pour décrire des systèmes logiques, comme par exemple la logique générale introduite par [Meseguer, 1989, Martí-Oliet et Meseguer, 1994]. Il est surement intéressant de voir comment ce cadre interagit avec celui des systèmes canoniques abstraits.

Index des Définitions

Part II

Master's Thesis
Natural Deduction and Completion as Instances of Abstract Canonical Systems

Chapter 5

Introduction

5.1 Proof Representation in Automated Theorem Proving

Automated theorem proving covers now a wide range of domains. The inherent notion of proof has been declined through different formalisms. On the one hand, there are sequent systems which were first introduced by Gentzen [Gentzen, 1934]. The isomorphism of Curry-Howard contributed to the development of a certain number of extensions of this, such as the Martin-Löf type theory [Martin-Löf, 1984] and the calculus of constructions [Coquand et Huet, 1988], or more recently with the calculus of algebraic constructions [Blanqui et al., 1999] or the calculus of structures [Guglielmi, 2002, Brünnler, 2003, http://alessio.guglielmi.name/res/cos/index.html]. Such works resulted in the implementation of interactive theorem provers such as Coq [Dowek et al., 1991, http://coq.inria.fr/].

On the other hand, most of the automated theorem provers use standard procedures such as completion [Knuth et Bendix, 1970] and resolution [Robinson, 1965], which leads to other proofs representations. Both procedures were refined for two purposes: to have a more specific and thus more efficient algorithm when dealing with particular cases, or to increase the efficiency although remaining general. For the first case, a revue of specific completion procedures for specific algebraic structures can be found in [Le Chenadec, 1986], and one can also speak of the paramodulation for the resolution in presence of an equality predicate [Robinson et Wos, 1969]. For the second case, completion has been extended to equational completion [Huet, 1980b, Peterson et Stickel, 1981, Jouannaud et Kirchner, 1986], inductionless induction (initiated by Musser; see [Kapur et Musser, 1987]), ordered completion [Lankford, 1975, Hsiang et Rusinowitch, 1991], to mention a few, whereas resolution was refined for instance to lock resolution [Boyer, 1971] and ordered resolution with selection [Bachmair et Ganzinger, 2001].

5.2 Good Proofs

All these domains have something in common: some proofs are better than the other, and to find efficient algorithms, we can restrict ourselves to these proofs. For instance, for sequent systems, **Cut**-free proofs are often considered as better than other proofs, and the **Cut**-elimination theorem give the possibility to restrict the space of search to **Cut**-free proofs. This is also the idea behind ordered resolution: some proofs, namely the one resolving greater atoms first, are better, and the resolution is still complete when restricted to such proofs. For equational logic, rewrite ("valley") proofs are better, and the completion procedure give us the best set of equational axiom, i.e. a set

from which everything can be proved using rewrite proofs.

Kirchner and Dershowitz proposed in [Dershowitz et Kirchner, 2004] a general framework to unify this notion of good proof. The main idea is to provide to the set of proofs an ordering. The best proofs are therefore the minimal one. *Proof orderings* were first introduced in [Bachmair et Dershowitz, 1994] to prove the completeness of the standard completion.

5.3 Good Inferences

Once one has defined what are the best proofs by the mean of a proof ordering, the next step is to obtain the best presentation of a theory, i.e. the set of axioms necessary for obtaining the best proofs for all the theory, but not containing anything useless. This is exactly what the completion procedure do: from a set of equational axioms, it produces a set of rewrite rules with the same congruence relation such that every equality can be proved using rewrite proofs.

To formalize this, the notion of *good inference* was introduced [Bonacina et Dershowitz, 2005]. Given a theory, its canonical presentation is defined as the set of the axioms needed to obtain the minimal proofs. It is wide enough to produce all best proofs, leading to a notion of *saturation*, but is does not contain any redundant informations, hence the notion of *contraction*. Presentations, i.e. sets of axioms, are then transformed using deduction mechanisms to produce this canonical presentation.

Such deduction mechanisms were introduced to cover the different completions. Indeed, such procedures have very similar properties, but until now, no formal generalization was proposed. Furthermore, other algorithms, such as Buchberger's Gröbner basis algorithm for polynomial ideals works similarly [Buchberger, 1965, Buchberger, 1983].

5.4 Overview

The object of this work was to show some instances where the framework of abstract canonical systems can be applied. This theory was indeed developed as general as possible, in order to cover a wide range of formalisms, and this is important to show that it can be used for some concrete cases. Two directions were explored: sequent systems through natural deduction, and completion, which was the original basis for the development of the theory.

The next chapter will present some basic mathematical notions and some notations used in the rest of the report.

Then, the first approach we had was to apply the abstract canonical systems to sequent systems such as natural deduction or sequent calculus. Nevertheless, this could not be done immediately, so we had to generalize the framework. Chapter 7 will first present the theory of the abstract canonical systems as introduced in [Dershowitz et Kirchner, 2004, Bonacina et Dershowitz, 2005], and then the generalization we propose in order to deal with logical formalisms where assumptions of subproofs can differ from the ones of their initial proof. As expected, we will present an ordering such that **Cut**-free proofs will be interpreted as good proofs.

The second approach was to provide formal proofs that ground and standard completions are instances of abstract canonical systems. The adequacy of ground completion was already shown in [Dershowitz, 2003], but this report present a less elliptical proof. The proof of the adequacy of standard completion is nevertheless completely original: we first ask ourselves what proof representation could be the best to use, and this has make us wonder if we could obtain different canonical presentation using these different representations. Chapter 8 will present an original

proof of the completeness of ground completion using abstract canonical systems. In chapter 9, we will first compare two proof representations and choose the most adapted to our case, and we will then prove the completeness of standard completion using abstract canonical systems.

Chapter 6

Mathematical notions

In this chapter are presented notions and notations which are used in the rest of this report. For a more complete survey on term rewriting and orderings, see [Baader et Nipkow, 1998], [Rusinowitch, 1987] or [Kirchner et Kirchner,].

The notation $\stackrel{!}{=}$ is used for definitions.

6.1 Terms, Algebras

Definition 6.1 (Alphabet, Language)**.** *An* alphabet *is a denumerable set* Σ*.*

A language *built over* Σ *is a subset of* Σ^**, the set of finite sequences of elements of* Σ*. A sequence* $(a_i)_{i\in\{1,\ldots,n\}}$ *is noted* $a_1a_2\ldots a_n$*.* Σ *is embedded in* Σ^* *in the usual way.*

Definition 6.2 (Signature, Terms)**.** *A* signature *is a couple* (Σ,α) *where* Σ *is an alphabet whose elements are called* function symbols*, and* α *is a function associating to each function symbol a natural number called its* arity*. A function symbol* a *such that* $\alpha(a)=0$ *is called a* constant*. A signature* (Σ,α) *is usually abbreviated as* Σ*.*

Let V *be a denumerable set called the set of* variables*. The set of* terms *built over* Σ *and* V*, noted* $\mathcal{T}(\Sigma,V)$*, is the smallest language built over* Σ *such that:*

- $V\subseteq\mathcal{T}(\Sigma,V)$*;*
- *for all function symbols* $f\in\Sigma$*, for all terms* $t_1,\ldots,t_{\alpha(f)}\in\mathcal{T}(\Sigma,V)$*, we have* $ft_1t_2\ldots t_{\alpha(f)}\in\mathcal{T}(\Sigma,V)$*.*

For commodity, because arities are not always specified, terms will be parenthesized like $f(t_1,\ldots,t_{\alpha(f)})$*.* f *is called the* head *of the term* $f(t_1,\ldots,t_{\alpha(f)})$*.*

The set $\mathcal{T}(\Sigma,\emptyset)$ *is the set of* ground terms*. It is non-empty if and only if* Σ *contains at least one constant.*

Definition 6.3 (Position, Subterm)**.** *Let* t *be a term in* $\mathcal{T}(\Sigma,V)$*. The set* $\mathfrak{p}(t)$ *of* positions *in* t *is the smallest language over* $\mathbb{N}\setminus\{0\}$ *such that:*

- *the empty sequence, noted* ε*, is an element of* $\mathfrak{p}(t)$*;*
- *if there exists a function symbol* f*, an integer* n *and some terms* $t_1,\ldots,t_n$ *such that* $t=f(t_1,\ldots,t_n)$*, then for all* $i\in\{1,\ldots,n\}$*,* $\{ip\ ;\ p\in\mathfrak{p}(t_i)\}\subseteq\mathfrak{p}(t)$*.*

The subterm *of t at the position $p \in \mathfrak{p}(t)$, noted $t_{|p}$ is recursively defined by:*

- $t_{|\varepsilon} \stackrel{!}{=} t$;
- $f(t_1,\ldots,t_n)_{|ip} \stackrel{!}{=} t_{i|p}$.

The replacement *of $t_{|p}$ by u in t, noted $t[u]_p$, is recursively defined by:*

- $t[u]_\varepsilon \stackrel{!}{=} u$;
- $f(t_1,\ldots,t_n)[u]_{ip} \stackrel{!}{=} f(t_1,\ldots,t_i[u]_p,\ldots,t_n)$.

Definition 6.4 (Context)**.** *A* context *over $\mathcal{T}(\Sigma,V))$ is a term of $\mathcal{T}(\Sigma,V\cup\{[]\})$ such that [] appears exactly one time.*

If $w[]$ is a context over $\mathcal{T}(\Sigma,V)$, and p is the position of $w[]$ where [] appears, then for all terms $u \in \mathcal{T}(\Sigma,V)$ we define $w[u] \stackrel{!}{=} w[][u]_p$. This is by definition a term of $\mathcal{T}(\Sigma,V)$.

Definition 6.5 (Substitution)**.** *A* substitution σ *over $\mathcal{T}(\Sigma,V)$ is an application from the set of variable V to the set of terms $\mathcal{T}(\Sigma,V)$, with a finite domain, i.e. a finite set of elements x such that $\sigma(x) \neq x$.*

The application of a substitution σ to a term t is the replacement of all variables occurring in t by their images through σ.

6.2 Orderings

6.2.1 Definitions

Definition 6.6 (Binary relation)**.** *A* binary relation *(shortly relation in the following) over a set S is a subset of the Cartesian product $S \times S$.*

The identity relation ι_S *over the set S is defined as*

$$\iota_S \stackrel{!}{=} \{(x,x)\ ;\ x \in S\}$$

The inverse ρ^{-1} *of a relation* ρ *is defined as*

$$\rho^{-1} \stackrel{!}{=} \{(y,x)\ ;\ (x,y) \in \rho\}$$

The composition *of two relations is defined as*

$$\rho_1 \circ \rho_2 \stackrel{!}{=} \{(x,z)\ ;\ \exists y \in S,\ (x,y) \in \rho_1 \wedge (y,z) \in \rho_2\}$$

The relation ρ *over S is said:*

(i) reflexive *if* $\iota_S \subseteq \rho$

(ii) irreflexive *if* $\iota_S \subseteq S^2 \setminus \rho$

(iii) symmetric *if* $\rho = \rho^{-1}$

(iv) antisymmetric *if* $\rho \cap \rho^{-1} \subseteq \iota_S$

(v) transitive *if* $\rho \circ \rho \subseteq \rho$

(vi) total *if* $\rho \cup \rho^{-1} = S^2$

For an antisymmetric relation ρ, ρ^{-1} will be noted $\mathfrak{q}$.

Definition 6.7 (Closures)**.** *For a relation* ρ*,*

- ρ^+ *is defined as its transitive closure, i.e. the least relation containing* ρ *and satisfying transitivity ((v));*
- ρ^* *is defined as its transitive reflexive closure, i.e. the least relation containing* ρ *and satisfying reflexivity and transitivity ((i) and (v));*
- $\mathfrak{q}\rho$ *is defined as its symmetric closure, i.e. the least relation containing* ρ *and satisfying symmetry ((iii)).*

Definition 6.8 (Partial ordering, partial order)**.** *A* quasi-order *over a set* S *is a relation verifying reflexivity and transitivity ((i) and (v)).*

A partial ordering *over a set* S *is a relation verifying irreflexivity and transitivity ((ii) and (v)).*

A partial order *over a set* S *is a relation verifying reflexivity, antisymmetry and transitivity ((i), (iv) and (v)).*

Proposition 6.1 (Relation between partial orderings and partial order)**.** *If* $>$ *is a partial ordering over a set* S*, then*

$$\geq \quad \stackrel{!}{=} \quad > \cup \iota_S$$

is a partial order.

Conversely, if $\geq$ *is a partial order, then*

$$> \quad \stackrel{!}{=} \quad \geq \setminus \iota_S$$

is a partial ordering.

As usual, for a relation ρ, we will write $x\rho y$ for $(x,y) \in \rho$. We will speak shortly of *ordering* (resp. *order*) for partial orderings (resp. partial order), even if they are *not* total ((vi)). According to proposition 6.1, $\geq$ will represent the order associated with the ordering $>$, and vice versa.

Definition 6.9 (Well-foundedness)**.** *A relation* ρ *is said* well-founded *iff there exists no infinite sequence* $(x_i)_{i\in\mathbb{N}}$ *such that for all* $i \in \mathbb{N}$*,* $x_i \rho x_{i+1}$*.*

6.2.2 Orderings over Terms

Definition 6.10 (Encompassment Ordering)**.** *Two terms* s *and* t *are comparable using the* encompassment ordering *(*$s \blacktriangleright t$*) if and only if a subterm of* s *in an instance of* t

$$\exists p \in \mathfrak{p}(s), \exists \sigma,\ \sigma(s_{|p}) = t$$

but not vice versa.

Definition 6.11 (Reduction ordering)**.** *A relation* ρ *over* $\mathcal{T}(\Sigma,V)$ *is said* monotonic *if and only if for all contexts* $w[]$*, for all terms* s,t*,*

$$s\rho t \Rightarrow w[s]\rho w[t]$$

It is stable *if and only if for all substitutions* σ*, for all terms* s,t*,*

$$s\rho t \Rightarrow \sigma(s)\rho\sigma(t)$$

An ordering $\gg$ *is called a* reduction ordering *if it is well-founded, monotonic and stable.*

Definition 6.12 (Simplification ordering)**.** *A reduction ordering is called a* simplification ordering *if and only if it verify the* subterm property*: for all terms* s*, for all positions* $p \in \mathfrak{p}(s)$*,*

$$s \gtrdot s_{|p}$$

6.2.3 Extensions of Orderings

Definition 6.13 (Ordering Functional)**.** *An* ordering functional *is an application which maps every ordering over* S *to an ordering over* S*.*

Definition 6.14 (Multiset)**.** *A* multiset M *over a set* S *is a function from* S *to* $\mathbb{N}$*.*

For $x \in S$*,* $M(x)$ *represents the number of occurrences of* x *in* M*, so that multisets can be viewed as sets where elements can occurs multiple times. For finite multisets, the notation* $\{\!\{a,a,b,\ldots,c\}\!\}$ *will be used.*

Definition 6.15 (Multiset ordering)**.** *The* multiset extension $>_{mult}$ *of an ordering* $>$ *over a set* S *is defined as follow:*

$$M >_{mult} N \text{ iff } M \neq N \wedge \forall t \in S,\ N(t) >_{\mathbb{N}} M(t) \Rightarrow \exists t' \in S,\ t' > t \wedge M(t') >_{\mathbb{N}} N(t')$$

where $>_{\mathbb{N}}$ *represented the standard ordering over natural numbers.*

Proposition 6.2 (Lernean Hydra)**.** *If* $>$ *is well-founded (resp. total),* $>_{mult}$ *is well-founded (resp. total) too.*

Definition 6.16 (Lexicographic ordering)**.** *The* lexicographic extension $>_{lex}$ *of an ordering* $>$ *over a set* S *is defined as follow:*
$\forall x_1,\ldots,x_n,y_1,\ldots,y_n \in S,\ (x_1,\ldots,x_n) >_{lex} (y_1,\ldots,y_n)$ *iff*

$$\exists i \in \{1,\ldots,n\},\ x_i > y_i \wedge (\forall j \in \{1,\ldots,i-1\},\ x_j = y_j)$$

Proposition 6.3. *If* $>$ *is well-founded (resp. total),* $>_{lex}$ *is well-founded (resp. total) too.*

Definition 6.17 (Recursive Path Ordering [Dershowitz, 1982, Kamin et Lévy, 1982, Rusinowitch, 1987])**.** *Let* Σ *be a signature, and* $>$ *be a ordering called* precedence *over function symbols in* Σ*.*

Let Δ *be a function which maps every function symbols to an ordering functional.*

The Recursive Path Ordering *(short RPO) with precedence* $>$ *and* status Δ *over* $\mathcal{T}(\Sigma,V)$ *is defined as follow:*
$\forall s = f(s_1,\ldots,s_n), t = g(t_1,\ldots,t_m) \in \mathcal{T}(\Sigma,V),\ s >_{rpo} t$ *iff*

- $f = g$ *and* $s\Delta(f)(>_{rpo})t$ *or*
- $f > g$ *and* $\forall j \in \{1,\ldots,m\},\ f >_{rpo} t_j$ *or*
- $\exists i \in \{1,\ldots,n\},\ s_i >_{rpo} t$

Note: The two ordering functionals generally used are the following ones:

- lexicographic functional: for all orderings $>$,

$$f(s_1,\ldots,s_n)\Delta(f)(>)f(t_1,\ldots,t_n) \text{ iff } (s_1,\ldots,s_n) >_{lex} (t_1,\ldots,t_n)$$

- multiset functional: for all orderings $>$,

$$f(s_1,\ldots,s_n)\Delta(f)(>)f(t_1,\ldots,t_n) \text{ iff } \{\!\{s_1,\ldots,s_n\}\!\} >_{mult} \{\!\{t_1,\ldots,t_n\}\!\}$$

For the next propositions, we consider that these functionals are used.

Proposition 6.4. *A RPO is a simplification ordering.*

Proposition 6.5. *If the precedence is total, the RPO is total on ground terms.*

6.3 Rewriting

6.3.1 Generalities

Definition 6.18 (Rewrite relation)**.** *A couple* $(l,r) \in \mathcal{T}(\Sigma,V)^2$ *is called a* rewrite rule *if and only if* $l \notin V$ *and the set of variables appearing in* t *is included in the one of* s*. Rewrite rules are usually noted as* $l \to r$*.*

A set of rewrite rules $R \subseteq \mathcal{T}(\Sigma,V)^2$ *is called a* rewrite system*.*

The rewrite relation $\underset{R}{\longrightarrow}$ *associated with a rewrite system* R *is defined as the least relation such that for all rewrite rules* $l \to r \in R$*, for all contexts* $w[]$*, for all substitution* σ*,*

$$w[\sigma(l)] \underset{R}{\longrightarrow} w[\sigma(r)]$$

i.e. this is the least monotonic and stable relation containing R*.*

R *is said* terminating *if* $\underset{R}{\longrightarrow}$ *is well-founded.*

Proposition 6.6 (Termination of rewrite system [Lankford, 1977])**.** *A rewrite system* R *is terminating if and only if there exists a reduction ordering* $\gg$ *such that* $\underset{R}{\longrightarrow} \subseteq \gg$*.*

Definition 6.19 (Critical Pairs)**.** *Given a rewrite system* R*, a* critical pair *is a couple* (r,t) *such that there exists two rules* $l \longrightarrow r$ *and* $g \longrightarrow d$ *such that* $l \underset{\{g \to d\}}{\longrightarrow} t$*. The set of critical pairs is noted* $CP(R)$*.*

6.3.2 Rewriting Modulo

Rewrite relations can be generalized so they can be applied modulo a set of equational axioms.

Definition 6.20 (Equational axiom)**.** *An* equational axiom *is a multiset* $\{\!\{l, r\}\!\}$ *of two terms* $l, r \in \mathcal{T}(\Sigma, V)$*. Equational axioms are usually noted* $l = r$*.*

Given a set A *of equational axioms, the congruence generated by* A *is* $\xleftrightarrow[A]{*}$*, the smallest reflexive, symmetric, transitive, monotonic and stable relation containing* A *(where the mapping from the set of 2-elements multisets of terms to the product* $\mathcal{T}(\Sigma, V)^2$ *is obvious).*

Example 6.1*:* The equational axiom of the associativity of a function symbol f is

$$f(f(x,y),z) = f(x,f(y,z))$$

where $x, y, z \in V$.

With a parenthesized infix notation for the function symbol $\cdot$ it is $(x \cdot y) \cdot z = x \cdot (y \cdot z)$.

The set of equational axioms AC for the associativity and commutativity of an operator $\cdot$ is

$$\{(x \cdot y) \cdot z = x \cdot (y \cdot z), x \cdot y = y \cdot x\}$$

Definition 6.21 (Class rewrite system)**.** *A* class rewrite system R/A *consists in a set of equational axioms* A *and a rewrite system* R*.*

The class rewrite relation $\xrightarrow[R/A]{}$ *associated with class rewrite system is defined by*

$$\xrightarrow[R/A]{} \quad \stackrel{!}{=} \quad \xleftrightarrow[A]{*} \xrightarrow[R]{} \xleftrightarrow[A]{*}$$

.

This relation can be viewed as the rewrite relation $\xrightarrow[R]{}$ applied to the set of terms quotiented by the equivalence relation $\xleftrightarrow[A]{*}$.

The proposition 6.6 can also be generalized:

Definition 6.22 (Termination of a class rewrite system)**.** *The class rewrite system* R/A *is* terminating *if* $\xrightarrow[R/A]{}$ *is well fonded.*

Definition 6.23 (Compatible ordering)**.** *A reduction ordering* $>$ *is* compatible *with a set of axioms* A *if for any terms* s, s', t, t'*,*

$$s' \xleftrightarrow[A]{*} s > t \xleftrightarrow[A]{*} t' \text{ implies } s' > t'$$

Proposition 6.7. *A class rewrite system* R/A *is terminating if and only if* R *is contained in some reduction ordering compatible with* A*.*

A total AC-compatible simplification ordering on ground terms is defined in [Rubio et Nieuwenhuis, 1995], as an extension of the RPO. To compare terms, they are interpreted using flattening and interpretation rules. As we consider in this report that the associative commutative symbols have the lowest precedence, we do not need the interpretation rules, and we will only present the flattening rules: terms are reduced using a set of rules

$$f(x_1, \ldots, x_n, f(y_1, \ldots, y_r), z_1, \ldots, z_m) \to f(x_1, \ldots, x_n, y_1, \ldots, y_r, z_1, \ldots, z_m) \tag{6.1}$$

for all AC-symbols f with $n+m \geq 1$ and $r \geq 2$. Such a rewrite system is terminating as shown in [Rubio et Nieuwenhuis, 1995].

For all terms t, let $snf(t)$ denote the *set of normal forms* of t using rules (6.1).

Given a precedence $>$ on function symbols, let $>_{rpo}$ denote the recursive path ordering with precedence $>$ where AC function symbols have multiset status and other symbols have lexicographic status.

If $f(s_1,\ldots,s_n)$ is the normal form of a term s rewriting by (6.1) only at topmost position, then $tf(s) \stackrel{!}{=} (s_1,\ldots,s_n)$.

Definition 6.24 (AC-RPO)**.** *For all terms s,t, $s >_{AC-rpo} t$ if:*

- $\forall t' \in snf(t)\ \exists s' \in snf(s),\ s' >_{AC-rpo} t'$ ***or***
- $\forall t' \in snf(t)\ \exists s' \in snf(s),\ s' \geq_{rpo} t'$ ***and*** $tf(s) = f(s_1,\ldots,s_m)$ *and* $tf(t) = (t_1,\ldots,t_n)$ ***and***
  - *if the head of s is AC then* $\{\!\{s_1,\ldots,s_m\}\!\} >_{AC-rpo_{mult}} \{\!\{t_1,\ldots,t_n\}\!\}$ ***or***
  - *if the head of s is not AC then* $(s_1,\ldots,s_m) >_{AC-rpo_{lex}} (t_1,\ldots,t_n)$.

Proposition 6.8 ([Rubio et Nieuwenhuis, 1995])**.** *The AC-RPO is an AC-compatible simplification ordering which is total for non AC-equivalent ground terms.*

Notions of confluence are also defined:

Definition 6.25. *We say that a $\xrightarrow[R]{}$ is* confluent modulo A *if*

$$\xleftarrow[R]{*} \circ \xleftrightarrow[A]{*} \circ \xrightarrow[R]{*} \subseteq \xrightarrow[R]{*} \circ \xleftrightarrow[A]{*} \circ \xleftarrow[R]{*}$$

The following theorem holds for linear class rewrite systems (in the sense of its two first assumptions):

Proposition 6.9 ([Huet, 1980b, Theorem 3.3])**.** *A class rewrite system R/A is confluent if and only if:*

- *for all rules $u \to v \in R$, u is linear, i.e. its variables appears only one time in it;*
- *for all equational axiom $u = v \in A$, the variables appearing in u and v are the same;*
- *R/A is terminating;*
- *for all critical pairs (s,t) formed by $\xleftarrow[R]{} \circ \xrightarrow[R]{}$ and by $\xleftarrow[R]{} \circ \xleftrightarrow[A]{}$,*

$$s \xrightarrow[R]{*} \circ \xleftrightarrow[A]{*} \circ \xleftarrow[R]{*} t$$

Chapter 7

Abstract Canonical Systems

In this chapter we will first present the framework of the abstract canonical systems. As we wanted to apply it to sequent systems such as the natural deduction, it appears that it could not be used with logical systems where assumption of subproofs are different from the one of the proof itself. We therefore have to generalize the framework, as it is done in the second part. We proved that this generalization is conservative, and that all results proved for the original framework does still hold with minor modifications. It is then applied to the natural deduction to see an instance of sequent systems.

7.1 Preserving Assumption Proof Systems

The results in this section are extracted from [Dershowitz et Kirchner, 2004, Bonacina et Dershowitz, 2005], which should be consulted for proofs. The proofs mentioned here, unless otherwise specified by a reference, are corrections from the original ones.

7.1.1 Definitions and Postulates

Let $\mathbb{A}$ be the set of all formulæ over some fixed vocabulary. Let $\mathbb{P}$ be the set of all proofs. These sets are linked by two functions: $[\cdot]^{Pm} : \mathbb{P} \to 2^{\mathbb{A}}$ gives the *premises* in a proof, and $[\cdot]_{Cl} : \mathbb{P} \to \mathbb{A}$ gives its *conclusion*. Both are extended to sets of proofs in the usual fashion. The set of proofs built using assumptions in $A \subseteq \mathbb{A}$ is noted by

$$Pf(A) \stackrel{!}{=} \left\{p \in \mathbb{P} : [p]^{Pm} \subseteq A\right\}$$

The framework proposed here is predicated on two *well-founded* partial orderings over $\mathbb{P}$: a *proof ordering* $>$ and a *subproof relation* $\rhd$. They are related by a monotonicity requirement given in section 7.1.3 (postulate E). We assume for convenience that the proof ordering only compares proofs with the same conclusion ($p > q \Rightarrow [p]_{Cl} = [q]_{Cl}$), rather than mention this condition each time we have cause to compare proofs.

We will use the term *presentation* to mean a set of formulæ, and *justification* to mean a set of proofs. We reserve the term *theory* for deductively closed presentations.

Definition 7.1 (Theory)**.** *Let ThA denote the* theory *of presentation A, that is, the set of conclusions of all proofs with assumptions included in A:*

$$ThA \stackrel{!}{=} [Pf(A)]_{Cl} = \{[p]_{Cl} : p \in \mathbb{P},\ [p]^{Pm} \subseteq A\}$$

Theories are monotonic:

Proposition 7.1 (Monotonicity)**.** *For all presentations A and B:*

$$A \subseteq B \Rightarrow ThA \subseteq ThB$$

In addition to this, we assume the two following postulates:

POSTULATE A (Reflexivity)**.**
For all presentations A:

$$A \subseteq ThA$$

POSTULATE B (Closure)**.**
For all presentations A:

$$ThThA \subseteq ThA$$

Proposition 7.1 and postulates A and B forms three standard properties of Tarskian consequence relations and are related to Scott's axioms for a consequence relation (see [Scott, 1974]). Thus, Th is a closure operator.

We say that presentation A is a *basis* for theory C if $ThA = C$. Presentations A and B are *equivalent* ($A \equiv B$) if their theories are identical: $ThA = ThB$.

We want to define what a "normal-form proof" is, i.e. the minimal proofs of $Pf(ThA)$:

Definition 7.2 (Minimal proofs)**.** *The set of* minimal proofs *of a presentation A is the set of minimal proofs in $Pf(A)$ for $>$:*

$$\mu Pf(A) \stackrel{!}{=} \{p \in Pf(A) : \neg\exists q \in Pf(A).\ p > q\}$$

Definition 7.3 (Canonical Presentation)**.** *The set of* normal-form proofs *for a presentation A is the set of minimal proofs of the theory ThA:*

$$Nf(A) \stackrel{!}{=} \mu Pf(ThA)$$

The canonical presentation *contains those formulæ that appear as assumptions of normal-form proofs:*

$$A^\sharp \stackrel{!}{=} [Nf(A)]^{Pm}$$

So, we will say that A is canonical *if $A = A^\sharp$.*

THEOREM 7.2.
The function $\cdot^\sharp$ is "canonical" with respect to the equivalence of presentations. That is:

1. $A^\sharp \equiv A$ *(consistency)*
2. $A \equiv B \Leftrightarrow A^\sharp = B^\sharp$ *(monotonicity)*
3. $A^{\sharp\sharp} = A^\sharp$ *(idempotence)*

By lifting proof orderings to justifications and presentations, the canonical presentation can be characterized in terms of the ordering directly. First, proof orderings are lifted to sets of proofs, as follows:

Definition 7.4 (Better proofs)**.** *Justification Q is* better *than justification P if:*

$$P \sqsupseteq Q \quad \stackrel{!}{\equiv} \quad \forall p \in P\ \exists q \in Q.\ p \geq q$$

It is much better[1] *if:*

$$P \sqsupset Q \quad \stackrel{!}{\equiv} \quad \forall p \in P\ \exists q \in Q.\ \ p > q$$

Justifications are similar *if:*

$$P \simeq Q \quad \stackrel{!}{\equiv} \quad P \sqsupseteq Q \sqsupseteq P$$

This relation are compatible: $(\sqsupseteq \circ \sqsupset) \subseteq \sqsupset$, $(\sqsupset \circ \simeq) \subseteq \sqsupseteq$, etc.
Then we have:

Proposition 7.3. *For all presentations A, B:*

$$Pf(A) \sqsupseteq Pf(A \cup B)$$

For all justifications P:

$$P \quad \sqsupseteq \quad \mu P$$

This "better than" quasi-order on proofs is lifted to a "simpler than" quasi-order on (equivalent) sets of formulæ, as follows:

Definition 7.5 (Simpler presentation)**.** *Presentation B is said to be* simpler *than an equivalent presentation A when B provides better proofs than does A:*

$$A \gtrsim B \quad \stackrel{!}{\equiv} \quad Th A = Th B \wedge Pf(A) \sqsupseteq Pf(B)$$

Presentations are similar *if their proofs are:*

$$A \approx B \quad \stackrel{!}{\equiv} \quad Pf(A) \simeq Pf(B)$$

$\approx$ is the equivalence relation associated to $\gtrsim$.

Then, we have the characterization of canonicity in terms of the ordering:

THEOREM 7.4.
The canonical presentation is the simplest:

$$A \equiv B \Rightarrow B \gtrsim A^\sharp$$

7.1.2 Completeness, Saturation and Redundancy

We now define what it means for a presentation to be saturated or complete:

Definition 7.6 (Saturation)**.** *A presentation A is* saturated *if it supports all possible normal form proofs:*

$$Pf(A) \supseteq Nf(A)$$

[1] This doesn't correspond to the strict version of $\sqsupseteq$, see [Bonacina et Dershowitz, 2005] for more details.

Definition 7.7 (Completeness)**.** *A presentation A is* complete *if every theorem has a normal form proof:*

$$ThA = [Pf(A) \cap Nf(A)]_{Cl}$$

A presentation is complete if it is saturated, but for the converse, we need a further hypothesis: *minimal proofs are unique* if for all theorems $c \in [Pf(A)]_{Cl}$, there is exactly one minimal proof in $Nf(A)$ with conclusion c. In particular, this holds for proof orderings that are total (on proofs of the same theorem).

Proposition 7.5. *A presentation is complete if it is saturated. If minimal proofs are unique, then a presentation is saturated iff it is complete.*

The next theorem relates canonicity and saturation. First, we have

Lemma 7.6. *A presentation is saturated if and only if*

$$\mu Pf(A) = Nf(A)$$

THEOREM 7.7.
A presentation A is saturated if and only if it contains its own canonical presentation: $A \supseteq A^\sharp$. In particular, $A^\sharp$ is saturated.

Moreover, the canonical presentation $A^\sharp$ is the smallest saturated set: no equivalent proper subset of $A^\sharp$ is saturated; if A is saturated, then every equivalent superset also is.

Proposition 7.8.

- *Presentation A is saturated iff $ThA \approx A$.*
- *Similar presentations are either both saturated or neither is.*
- *Similar presentations are either both complete or neither is.*

The following definition sets the stage for the forth characterization of canonical presentation, as non-redundant lemmata. Formulæ that can be removed from a presentation —without making proofs worse— are "redundant":

Definition 7.8 (Redundancy)**.** *A formula r is* redundant *with respect to a presentation A when:*

$$A \gtrsim A \setminus \{r\}$$

The set of all redundant formulæ *of a given presentation A will be denoted as follows:*

$$RedA \quad \stackrel{!}{=} \quad \{r \in A : A \gtrsim A \setminus \{r\}\}$$

A presentation A is contracted *if*

$$RedA = \emptyset$$

The set of redundant formulæ is *globally* redundant:

Proposition 7.9. *For all presentations A:*

$$A \;\approx\; A \setminus RedA$$

We then have the following result:

THEOREM 7.10.
A presentation is canonical iff it is saturated and contracted.

7.1.3 Subproofs and Inference

We now introduce the notion of *subproof*: We call a proof *trivial* when it proves only its unique assumption and has no subproofs other than itself, that is, if $[p]^{Pm} = \{[p]_{Cl}\}$ and $p \trianglerighteq q \Rightarrow p = q$. We denote by $\widehat{a}$ such a trivial proof of $a \in \mathbb{A}$ and by $\widehat{A}$ the set of trivial proofs of each $a \in A$.

We assume that proofs use their assumptions (postulate C), that subproofs don't use non-existent assumptions (postulate D), and that proof orderings are monotonic with respect to subproofs (postulate E):

POSTULATE C (Trivia)**.**
For all proofs p and formulæ a:

$$a \in [p]^{Pm} \Rightarrow p \trianglerighteq \widehat{a}$$

POSTULATE D (Subproofs Premises Monotonicity)**.**
For all proofs p and q:

$$p \trianglerighteq q \Rightarrow [p]^{Pm} \supseteq [q]^{Pm}$$

POSTULATE E (Replacement)**.**
For all proofs p, q and r:

$$p \triangleright q > r \Rightarrow \exists v \in Pf([p]^{Pm} \cup [r]^{Pm}).\ p > v \triangleright r$$

We make no other assumptions regarding proofs or their structure.

Every formula a admits a trivial proof $\widehat{a}$ by postulates A and C.

It may be convenient to think of a proof-tree "leaf" as a subproof with only itself as a subproof; other subproofs are the "internal nodes". There are two kinds of leaves: trivial proofs $\widehat{a}$, and vacuous proofs $\bar{a}$ with $[\bar{a}]^{Pm} = \emptyset$ and $[\bar{a}]_{Cl} = a$. By well-foundedness of $\trianglerighteq$, there are no infinite "paths" in proof trees. It follows from postulate E that the transitive closure of $> \cup \triangleright$ is also well-founded.

Now that all basic definitions over presentation are given, we can show the following useful lemma:

Lemma 7.11. *The following functions over justifications or presentations are monotonic with regard to $\subseteq$: for all justifications P, Q, if $P \subseteq Q$ then*

$$[P]^{Pm} \subseteq [Q]^{Pm}$$

$$[P]_{Cl} \subseteq [Q]_{Cl}$$

For all presentations A, B, if $A \subseteq B$ then

$$Pf(A) \subseteq Pf(B)$$

$$\widehat{A} \subseteq \widehat{B}$$

Proof. All these functions f are defined as an extension over presentations of functions over proofs or formulæ: $f(X) \stackrel{!}{=} \bigcup_{x \in X} f(x)$, and are therefore monotonic. □

Counter-example 7.1*:* This is not the case for μ. Indeed, if we have $p > q$ then $P = \{p\} \subseteq Q = \{p, q\}$ but $\mu P = \{p\} \not\subseteq \mu Q = \{q\}$. For this reason, Nf and $\cdot^\sharp$ are not monotonic too.

Lemma 7.12. *For all presentation A,* $[\mu Pf(A)]^{Pm} = [\mu Pf(A) \cap \widehat{A}]_{Cl}$

A corollary of this lemma gives equivalent characterizations of canonical presentations as minimal trivial theorems.

THEOREM 7.13.
For all presentations A,

$$A^\sharp = [Nf(A) \cap \widehat{ThA}]_{Cl}$$

$$\widehat{A^\sharp} = Nf(A) \cap \widehat{ThA}$$

The next proposition says that the subproofs of minimal proofs are minimal. It follows from postulate E:

Proposition 7.14 (Subproofs Minimality)**.** *For all presentations A, for all proofs* p, q*,*

$$p \trianglerighteq q \ \wedge \ p \in \mu Pf(A) \Rightarrow q \in \mu Pf(A)$$

We now consider inference and deduction mechanisms.

Definition 7.9 (Deduction Mechanisms)**.** *A* deduction mechanism $\rightsquigarrow$ *is a function from presentations to presentations and we call the relation* $A \rightsquigarrow B$ *a* deduction step*.*

A sequence of presentations $A_0 \rightsquigarrow A_1 \rightsquigarrow \cdots$ *is called a* derivation*.*

The result *of the derivation is, as usual, its* persisting *formulæ:*

$$A_\infty \stackrel{!}{=} \liminf_{j\to\infty} A_j = \bigcup_{j>0} \bigcap_{i>j} A_i$$

We also define the set of all generated formulæ:

$$A_* = \bigcup_{i>0} A_i$$

We say that a proof p *persists* when $[p]^{Pm} \subseteq A_\infty$. Thus, if a proof persists, so do its subproofs (by postulate D). By the first statement of proposition 7.3), we have $Pf(A_i) \sqsupseteq Pf(A_*)$ for all i.

Definition 7.10 (Soundness and adequacy)**.**

- *A deduction mechanism* $\rightsquigarrow$ *is* sound *if* $A \rightsquigarrow B$ *implies* $ThB \subseteq ThA$*.*
- *It is* adequate *if* $A \rightsquigarrow B$ *implies* $ThA \subseteq ThB$*.*
- *It is both if* $A \equiv B$*.*

Definition 7.11 (Goodness)**.** *A deduction mechanism* $\rightsquigarrow$ *is* good *if proofs only get better:*

$$\rightsquigarrow \subseteq \succsim$$

That is, $Pf(A) \sqsupseteq Pf(B)$ *whenever* $A \rightsquigarrow B$*.*

A derivation $A_0 \rightsquigarrow A_1 \rightsquigarrow \cdots$ *is* good *if* $A_i \succsim A_{i+1}$ *for all* i*.*

Lemma 7.15. *If a deduction mechanism is good then*

$$Pf(A_i) \sqsupseteq Pf(A_\infty) \text{ and therefore } ThA_i \subseteq ThA_\infty$$

for all i in a derivation $\{A_i\}_i$.

Lemma 7.16. *For all presentation A and B:*

$$Pf(A) \sqsupseteq Pf(B) \Rightarrow B \cap RedA \subseteq RedB$$

Proposition 7.17. *If a derivation* $\{A_i\}_i$ *is good, then its limit supports the best proofs:*

$$A_* \approx A_\infty$$

We now extend the notion of completeness, saturation and contraction to derivation:

Definition 7.12 (Canonical Derivation)**.**

- *A derivation* $\{A_i\}_i$ *is* completing *if* A_∞ *is complete.*
- *It is* saturating *if* A_∞ *is saturated.*
- *It is* contracting *if* A_∞ *is contracted.*
- *It is* canonical *if both saturating and contracting.*

A canonical derivation can be used to build the canonical presentation of the initial presentation:

Lemma 7.18. *A good derivation is canonical if and only if*

$$A_\infty = A_0^\sharp$$

.

We now introduce critical proofs:

Definition 7.13 (Critical Proofs)**.** *A minimal proof* $p \in \mu Pf(A)$ *is* critical *if it is not in normal form, but all its proper subproofs in A are:*

$$p \in \mu Pf(A) \setminus Nf(A)$$
$$\forall q. p \rhd q \Rightarrow q \in Nf(A)$$

The set of critical proofs of a presentation A is denoted $Crit(A)$.

Definition 7.14 (Fairness)**.**

- *A good derivation* $\{A_i\}_i$ *is* fair *if*
$$Crit(A_\infty) \sqsupset Pf(A_*)$$
- *It is* uniformly fair *if*
$$\widehat{A_\infty} \setminus \widehat{A_0^\sharp} \sqsupset Pf(A_*)$$

These two notions of fairness correspond to completeness and saturation.

Lemma 7.19. *For all presentation A, $Crit(A) \sqsupset Pf(A) \Leftrightarrow Crit(A) = \emptyset$.*

Proof. $\Leftarrow$: We have to show $\forall p \in \emptyset\ \exists q \in Pf(A).\ p > q$, which is trivially true.

$\Rightarrow$: By contradiction, suppose there exists $p \in Crit(A)$. Then by definition $p \in \mu Pf(A)$. But, using the hypothesis, there exists $q \in Pf(A)$ such that $p > q$ which leads to a contradiction with the minimality of p. □

THEOREM 7.20.
If a good derivation is fair, then its limit is complete

Proof. If a good derivation is fair, then by definition of fairness we have $Crit(A_\infty) \sqsupset Pf(A_*)$. Using goodness, by proposition 7.17 we have $Pf(A_*) \simeq Pf(A_\infty)$, so that $Crit(A_\infty) \sqsupset Pf(A_\infty)$. With the precedent lemma, we have $Crit(A_\infty) = \emptyset$.

Consequently, $\mu Pf(A_\infty) \cap Nf(A_\infty) = \mu Pf(A_\infty)$ and $[Pf(A_\infty) \cap Nf(A_\infty)]_{Cl} \supseteq [\mu Pf(A_\infty) \cap Nf(A_\infty)]_{Cl} = [\mu Pf(A_\infty)]_{Cl} = [Pf(A_\infty)]_{Cl} = ThA_\infty$. The presentation A_∞ is complete. □

THEOREM 7.21.
If a good derivation is uniformly fair, then its limit is saturated.

7.2 Generalization towards the Application to Sequent Systems

7.2.1 Propositional Natural Deduction

The natural deduction was first introduced by Gentzen as a more "natural" alternative of the sequent calculus he also defined in [Gentzen, 1934].

Let A, B range over formulæ, where a *formula* is either an atomic formula X or an implication $A \to B$:

$$\mathbb{A} \stackrel{!}{=} X \mid \mathbb{A} \to \mathbb{A}$$

Let Γ be a set of formulæ. The notation Γ, A must be understood as $\Gamma \cup \{A\}$. An intuitionistic *sequent* for the intuitionistic propositional natural deduction is a couple $\Gamma \vdash A$ of a set of formulæ Γ and a formula A.

The inference rules for the natural deduction are given in figure 7.1.

A *proof* of a formula A under the set of premises Γ is a tree build with this inference rules, whose root is the sequent $\Gamma \vdash A$ and whose leaves are all Axiom rules.

Example 7.2*:* Here is a proof of $(A \to B) \to B$ under the premise A:

$$\dfrac{\dfrac{\dfrac{}{A, A \to B \vdash A \to B}\ Ax \qquad \dfrac{}{A, A \to B \vdash A}\ Ax}{A, A \to B \vdash B}\ App}{A \vdash (A \to B) \to B}\ Abs$$

We now check that the postulates are verified:

The postulate A and B are direct consequences of the inference rules in figure 7.1.

The intuition behind *subproofs* is subtrees. Nevertheless, the postulate C does not hold with this. Trivial proofs are particular cases of Axiom proofs: the trivial proof of A is indeed $\widehat{A} = \dfrac{}{A \vdash A}\ Ax$. But for instance the Axiom proof $\dfrac{}{A, B \vdash B}\ Ax$ does not have the trivial proofs of its premises $\widehat{A}$ and $\widehat{B}$ as subtrees. We therefore extend the relation $\triangleright$ by having all trivial proofs of premises of Axiom proofs as subproofs of these:

Axiom:

$$\frac{}{\Gamma, A \vdash A}\ Ax$$

Abstraction (→Introduction):

$$\frac{\Gamma, A \vdash B}{\Gamma \vdash A \to B}\ Abs$$

Application (→Elimination):

$$\frac{\Gamma \vdash A \to B \qquad \Gamma \vdash A}{\Gamma \vdash B}\ App$$

Figure 7.1: Inference Rules for Intuitionistic Propositional Natural Deduction

Definition 7.15 (Subproofs in Natural Deduction)**.** *We define the* subproof *relation* $\trianglerighteq$ *over proofs in Natural Deduction as the smallest reflexive and transitive relation verifying:*

- *if* q *is a subtree of* p*, then* $p \trianglerighteq q$*;*
- *if* A *is a premise of an axiom proof* p*, then* $p \trianglerighteq \widehat{A}$*.*

It is quite clear that $\triangleright$ is well-founded.

It is now trivial to show that the postulate C holds: for all inference rules in figure 7.1, the set of premises grows up in the subtrees. The original premises of a proof are then included in the one of its leaves, which are by definition Axiom rules. Thus, by transitivity, the trivial proofs of these premises are indeed subproofs of the whole proof.

Proofs can be represented using so-called *(simply) typed* λ*-terms* (see [Barendregt, 1984]). λ-terms are built using the following syntax:

$$t \stackrel{!}{=} x \mid \lambda x.t \mid tt$$

where x ranges over a set of variables.

An occurrence of the variable x in t is said *free* if it is not guarded by a λx. More formally, the set $\mathcal{F}(t)$ of free variables in t can be defined by induction:

$$\begin{aligned} \mathcal{F}(x) &\stackrel{!}{=} \{x\} \\ \mathcal{F}(\lambda x.t) &\stackrel{!}{=} \mathcal{F}(t) \setminus \{x\} \\ \mathcal{F}(t_1 t_2) &\stackrel{!}{=} \mathcal{F}(t_1) \cup \mathcal{F}(t_2) \end{aligned}$$

λ-terms are related using the so-called β*-reduction*. Basically, we have $w[(\lambda x.t_1)t_2] \to_\beta w[\{t_2/x\}t_1]$ with $w[]$ some context, and the term $\{t_2/x\}t_1$ defined as the term t_1 where all free occurrences of x have been replaced by t_2.

Typed λ-terms are the subset of λ-terms that can be derived by the rules of figure 7.2. Note the correspondence with the rules of figure 7.1.

Axiom:

$$\frac{}{\Gamma, x : A \vdash x : A}\ Ax$$

Abstraction (→Introduction):

$$\frac{\Gamma, x : A \vdash t : B}{\Gamma \vdash \lambda x.t : A \to B}\ Abs$$

Application (→Elimination):

$$\frac{\Gamma \vdash t_1 : A \to B \qquad \Gamma \vdash t_2 : A}{\Gamma \vdash t_1 t_2 : B}\ App$$

Figure 7.2: Inference Rules for the Simply Typed λ-Calculus

7.2.2 Extended Postulates Framework

We want to apply the abstract canonical systems framework [Dershowitz et Kirchner, 2004, Bonacina et Dershowitz, 2005] to deduction systems such as natural deduction or sequent calculus [Gentzen, 1934].

The postulate D does not hold for these proofs systems, due to the inference rule for the introduction of an implication :

$$\frac{\Gamma, A \vdash B}{\Gamma \vdash A \to B}\ Abs$$

In this section we generalize the abstract canonical systems theory in order to be able to apply it to these systems. Thus, we remove the premises monotonicity postulate D. The replacement postulate E must then be modified in order to be applied in the following way :

POSTULATE E_{gen} (Generalized Replacement)**.**
For all proofs p, q and r:

$$p \rhd q > r \Rightarrow \exists v \in Pf([p]^{Pm} \cup ([r]^{Pm} \setminus [q]^{Pm})).\ p > v \rhd r$$

The idea behind this postulate is that the premises of q are of two kind: the first ones are premises of p whereas the other ones comes from the construction of the proof. These last premises must be removed in the resulting proof when we replace the subproof q by a better proof r in p. This proof v is thus an element of $Pf([p]^{Pm} \cup ([r]^{Pm} \setminus ([q]^{Pm} \setminus [p]^{Pm}))) = Pf([p]^{Pm} \cup ([r]^{Pm} \setminus [q]^{Pm}))$.

Note: This is indeed a generalization of postulate E: $[p]^{Pm} \cup ([r]^{Pm} \setminus [q]^{Pm}) \subseteq [p]^{Pm} \cup [r]^{Pm}$, and if we suppose the postulate D, we have $[p]^{Pm} \supseteq [q]^{Pm}$ and therefore $[p]^{Pm} \cup ([r]^{Pm} \setminus [q]^{Pm}) \supseteq [p]^{Pm} \cup ([r]^{Pm} \setminus [p]^{Pm}) = [p]^{Pm} \cup [r]^{Pm}$, so that $[p]^{Pm} \cup ([r]^{Pm} \setminus [q]^{Pm}) = [p]^{Pm} \cup [r]^{Pm}$.

The following example enlights why the postulate E_{gen} does hold for intuitionistic propositional natural deduction:

Example 7.3*:* Consider the following proofs in Natural Deduction:

$$p = \dfrac{\dfrac{\dfrac{\dfrac{\dfrac{}{A,B\vdash A}\,Ax}{A\vdash B\to A}\,Abs}{A\vdash A\to B\to A}\,Abs \qquad \dfrac{}{A\vdash A}\,Ax}{A\vdash B\to A}\,App}{\vdash A\to B\to A}\,Abs$$

It's quite clear that the subproof

$$q = \dfrac{\dfrac{\dfrac{\dfrac{\dfrac{}{A,B\vdash A}\,Ax}{A\vdash B\to A}\,Abs}{A\vdash A\to B\to A}\,Abs \qquad \dfrac{}{A\vdash A}\,Ax}{A\vdash B\to A}\,App$$

can be replaced by the "better" proof

$$r = \dfrac{\dfrac{}{A,B\vdash A}\,Ax}{A\vdash B\to A}\,Abs$$

thus resulting in the proof

$$v = \dfrac{\dfrac{\dfrac{}{A,B\vdash A}\,Ax}{A\vdash B\to A}\,Abs}{\vdash A\to B\to A}\,Abs$$

We can see that $v \in Pf([p]^{Pm} \cup ([r]^{Pm} \setminus [q]^{Pm})) = Pf(\emptyset \cup (\{A\} \setminus \{A\})) = Pf(\emptyset)$. The replacement proof v satisfies the hypothesis of postulate E_{gen}, as expected.

7.2.3 Revisiting the Abstract Canonical Systems Framework

In this section, we go through the complete abstract canonical systems framework, and we check that the modifications that we propose do not make it incoherent or useless.

Some results must be modified. First, we have to modify the minimality of subproofs of minimal proofs, using the following lemma instead of the proposition 7.14:

Proposition 7.22 (Subproofs Extended Minimality)**.** *For all presentation A,*

$$p \trianglerighteq q \wedge p \in \mu Pf(A) \Rightarrow q \in \mu Pf(A \cup [q]^{Pm})$$

Proof. If $p = q$, this is trivial.

Otherwise, suppose $p \rhd q$ and $p \in \mu Pf(A)$. By contradiction, suppose there is a proof $r \in Pf(A \cup [q]^{Pm})$ such that $q > r$. We then have $p \rhd q > r$, hence by the replacement postulate E_{gen} there exists $v \in Pf([p]^{Pm} \cup ([r]^{Pm} \setminus [q]^{Pm}))$ such that $p > v \rhd r$. By hypothesis, we have $[r]^{Pm} \subseteq A \cup [q]^{Pm}$, thus $[p]^{Pm} \cup ([r]^{Pm} \setminus [q]^{Pm}) \subseteq A$ and therefore $v \in Pf(A)$, leading to a contradiction with the minimality of p in A. □

Note: This is indeed a generalization of proposition 7.14: if we suppose the postulate D, and if $p \trianglerighteq q$ and $p \in Pf(A)$, then $A \cup [q]^{Pm} = A$.

Other results, such as lemma 7.12, have different proofs.

Lemma 7.12. *For all presentation A,* $[\mu Pf(A)]^{Pm} = [\mu Pf(A) \cap \widehat{A}]_{Cl}$

Proof. The $\supseteq$ part is trivial, because $[\mu Pf(A) \cap \widehat{A}]_{Cl} = [\mu Pf(A) \cap \widehat{A}]^{Pm}$ and by monotonicity of $[\cdot]^{Pm}$.

For $\subseteq$, we first want to show that

$$\widehat{[\mu Pf(A)]^{Pm}} \subseteq \mu Pf(A) \tag{7.1}$$

i.e. for all $a \in [\mu Pf(A)]^{Pm}$, we have $\widehat{a} \in \mu Pf(A)$: suppose $a \in [\mu Pf(A)]^{Pm}$, then by definition there exists $p \in \mu Pf(A)$ such that $a \in [p]^{Pm}$. Using the postulate C, we have $p \trianglerighteq \widehat{a}$. By proposition 7.22, $\widehat{a} \in \mu Pf(A \cup \{a\}) = \mu Pf(A)$ ($a \in [\mu Pf(A)]^{Pm}$ implies $a \in A$).

Clearly

$$\widehat{[\mu Pf(A)]^{Pm}} \subseteq \widehat{A} \tag{7.2}$$

because $[\mu Pf(A)]^{Pm} \subseteq A$ and by monotonicity of $\widehat{\cdot}$.

With (7.1) and (7.2) we have $\widehat{[\mu Pf(A)]^{Pm}} \subseteq \mu Pf(A) \cap \widehat{A}$.

Furthermore, for all presentation B we trivially have $B = [\widehat{B}]_{Cl}$ by definition of trivial proofs, and therefore we can conclude with $[\mu Pf(A)]^{Pm} = [\widehat{[\mu Pf(A)]^{Pm}}]_{Cl} \subseteq [\mu Pf(A) \cap \widehat{A}]_{Cl}$ by monotonicity of $[\cdot]_{Cl}$. □

This proof shows how some other proofs, like the one of the proposition 7.17, need to be modified with our new postulate: somehow, the proof needs the assumption that for a premise a of a proof $p \in \mu Pf(A)$, we have $\widehat{a} \in \mu Pf(A)$. This comes from proposition 7.22 and postulate C, by noting that $A \cup [\widehat{a}]^{Pm} = A$ because $a \in [p]^{Pm} \subseteq A$.

We need to modify the proof of lemma 7.16 in the following way:

Lemma 7.16. *For all presentation A and B:*

$$Pf(A) \sqsupseteq Pf(B) \Rightarrow B \cap Red\,A \subseteq Red\,B$$

Proof. Consider $a \in B \cap Red\,A$. We have to show that for all proofs in $Pf(B)$ there exist a better proof in $Pf(B \setminus \{a\})$.

Suppose $p \in Pf(B)$ such that $a \in [p]^{Pm}$. By postulate C we have $p \trianglerighteq \widehat{a}$. As $a \in Red\,A$, by definition of redundancy there exists $q \in Pf(A \setminus \{a\})$ such that $\widehat{a} \geq q$. Because $a \notin [q]^{Pm}$, $a \neq q$ so $a > q$. By assumption, $Pf(A) \sqsupseteq Pf(B)$, so that there exists $r \in Pf(B)$ such that $q \geq r$. If $p = \widehat{a}$, let $p' = r$ so that $p' \in Pf(B)$ and $p > p'$. Otherwise, by the postulate E_{gen}, $p \triangleright \widehat{a} > r$ implies the existence of a $p' \in Pf(B \cup (B \setminus \{a\})) = Pf(B)$ such that $p > p'$. If $a \notin [p']^{Pm}$, we found a better proof for p in $Pf(B \setminus \{a\})$. Else we can continue this process with p'. We can't continue forever because of the well-foundedness of $>$. □

We also have to refine the definition 7.13 of critical proofs:

Definition 7.16 (Generalized Critical Proofs)**.** *A minimal proof $p \in \mu Pf(A)$ is* critical *if it is not in normal form, but all its proper subproofs in A are:*

$$p \in \mu Pf(A) \setminus Nf(A)$$

$$\forall q.\, p \triangleright q \Rightarrow q \in \mu Pf(A) \Rightarrow q \in Nf(A)$$

The set of critical proofs of a presentation A is denoted $Crit(A)$.

Note: Once again, this is indeed a generalization: suppose the postulate D, then using proposition 7.14, $p \trianglerighteq q$ and $p \in \mu Pf(A)$ implies $q \in \mu Pf(A)$ as expected.

The lemma 7.19 is still valid, thus allowing us to prove the theorem 7.20:

THEOREM 7.20.
If a good derivation is fair, then its limit is complete

Proof. By definition of fairness we have $Crit(A_\infty) \sqsupset Pf(A_*)$. By proposition 7.17, $Pf(A_*) \approx Pf(A_\infty)$, so that $Crit(A_\infty) \sqsupset Pf(A_\infty)$. Using the lemma 7.19, we therefore have $Crit(A_\infty) = \emptyset$.

By contradiction, suppose there is $c \in ThA_\infty$ such that $c \notin [Pf(A_\infty) \cap Nf(A_\infty)]_{Cl}$. Then there is a proof p of c in $\mu Pf(A_\infty) \setminus Nf(A_\infty)$. As $Crit(A_\infty) = \emptyset$, $p \notin Crit(A_\infty)$, i.e. by definition $\exists q.\ p \rhd q \wedge q \in \mu Pf(A_\infty) \wedge q \notin Nf(A_\infty)$. Hence $q \in \mu Pf(A_\infty) \setminus Nf(A_\infty)$, we can reproduce this process with q forever. The contradiction comes from the wellfoundedness of $\rhd$. □

7.2.4 Good Proofs as Cut-Free Proofs

In natural deduction, there is no **Cut** rule, as in sequent calculus. The ***Cut*** *rule* in the intuitionistic sequent calculus is the following:

$$\frac{\Gamma \vdash A \quad \Gamma, A \vdash B}{\Gamma \vdash B}\ Cut$$

It represent the use of a lemma A to prove B.

It can be simulated in natural deduction by

$$\frac{\dfrac{\Gamma, A \vdash B}{\Gamma \vdash A \to B}\ Abs \qquad \Gamma \vdash A}{\Gamma \vdash B}\ App$$

If we look at the λ-term representation of the proof, this corresponds to $(\lambda x.t_1)t_2$. The term of a proof containing a **Cut** is therefore a term where the β-reduction can be applied. This is why proof terms with no β-redex are called **Cut**-free.

This idea here is to take as an ordering for the proofs in Natural Deduction the transitive closure of the β-reduction $\xrightarrow{+}_\beta$. It is well-founded because of the strong normalization of the simply typed λ-calculus. It also satisfies the postulate E_{gen}, because the β-reduction is a monotonic relation. We therefore have the following theorem :

THEOREM 7.23.
Minimal proofs in natural deduction with the ordering define above are ***Cut****-free proofs.*

Proof. Trivial. □

Such a theorem show us how the framework of abstract canonical systems can be instantiated to give a notion of good proofs corresponding to **Cut**-free proofs. One has to generalized this framework, but it can be done in a conservative way. This is a first step in showing that it can cover a wide range of logical formalisms.

Chapter 8

Application to Ground Completion

In this chapter, we apply the framework of the abstract canonical systems to the ground completion [Snyder, 1989]. It was already done in [Dershowitz, 2003, Bonacina et Dershowitz, 2005], but the proofs presented here are fully detailled, and the section 8.5.4 is totaly original.

8.1 Presentation

The ground completion, as presented in [Gallier et al., 1993, Snyder, 1989], takes a reduction ordering on ground terms $\gg$ and a set of ground equational axioms E (i.e. equational axioms over $\mathcal{T}(\Sigma,\emptyset)$) and transforms it using the rules presented on figure 8.1 to produce a confluent set of equational axioms of the same theory. It is a particular case of the standard completion (see next chapter 9) for ground terms based equational axioms. The rule **Deduce** of the ground completion correspond to the rules **Deduce**, **Simplify**, **Compose** and **Collapse** of the standard completion.

Deduce:
If $u = v \in E$ and $u \gg v$,

$$E \cup \{w = t[u]\} \rightsquigarrow E \cup \{w = t[v]\}$$

Delete:

$$E \cup \{t = t\} \rightsquigarrow E$$

Figure 8.1: Rules for the Ground Completion

Ground completion characteristics compared to standard completion are its termination (see section 8.5.3) and the possibility to have a total ordering over ground terms (see section 6.2.3). It can be efficiently implemented: it is shown in [Snyder, 1989] to run in $O(n \log n)$ where n is the occurrences of symbols in the original set of ground equational axioms E.

The completeness of the ground completion as an instance of the abstract canonical systems was already shown in [Bonacina et Dershowitz, 2005]. We will present here a more detailed proof.

8.2 Proofs Representation

The set of formula $\mathbb{A}$ consists here in the set of all ground equational axioms.

The proofs in $\mathbb{P}$ are built using the inference rules presented on the figure 8.2. The boxed representation for **Introduction** is used to emphase the assumptions occurring in a proof.

Congruence:
For all functions symbol f of arity n, for all terms $t_1,\ldots,t_n,t'_1,\ldots,t'_n$,

$$\frac{t_1 = t'_1 \quad \cdots \quad t_n = t'_n}{f(t_1,\ldots,t_n) = f(t'_1,\ldots,t'_n)}\ C$$

Transitivity:
For all terms r,s,t,

$$\frac{r = s \quad s = t}{r = t}\ T$$

Introduction:
For all equational axioms $s = t$,

$$\frac{\boxed{s = t}}{s = t}\ I_{s=t}$$

Figure 8.2: Inference Rules for Ground Proofs

8.3 Proofs Ordering

Proofs are compared using a RPO (see section 6.2.3) with the following precedence $\succ$: for all equational axioms $s = t$ and $u = v$, $I_{s=t} \succ I_{u=v}$ iff $\{\!\{s,t\}\!\} \gg_{mult} \{\!\{u,v\}\!\}$, and $I_{s=t} \succ T \succ C$.

Example 8.1*:* A critical peak is greater than the introduction of its conclusion: for all terms r,s,t such that $s \gg r,t$,

$$\frac{\dfrac{\boxed{r = s}}{r = s}\ I_{r=s} \quad \dfrac{\boxed{s = t}}{s = t}\ I_{s=t}}{r = t}\ T \quad > \quad \frac{\boxed{r = t}}{r = t}\ I_{r=t}$$

8.4 Adequacy to the Postulates

We suppose here that E is a set of ground equational axioms.

8.4.1 Postulate A

We want to show that for all $u = v \in E$ there exist a proof of $u = v$ in $Pf(E)$. This proof is $I_{u=v}$.

8.4.2 Postulate B

Let $u = v$ be in $ThThE$. By definition, there exists a proof p of $u = v$ in $Pf(ThE)$. Consider $s = t$ introduced in p. Thus $s = t \in ThE$, and there exists a proof q of $s = t$ in $Pf(E)$. We can replace all introductions such as $I_{s=t}$ by its corresponding q in p to obtain a proof in $Pf(E)$.

8.4.3 Postulate C and D

These postulates hold because of the tree structure of proofs: the assumptions of a proof are the equational axioms introduced in it, so they are by definition its subproofs, and the assumptions of its subproofs are also its assumptions.

8.4.4 Postulate E

This postulate holds because a RPO is monotonic: if $p \rhd p_{|i} > r$ then $v \stackrel{!}{=} p[r]_i \in Pf([p]^{Pm} \cup [r]^{Pm})$ and $p > v$.

8.5 Completeness of the Ground Completion

We suppose here that $\gg$ is a total simplification ordering. Such an ordering exists (see propositions 6.4 and 6.5).

8.5.1 Ground Completion is Sound and Adequate

The ground completion mechanism of the figure 8.1 corresponds to the definition of a deduction mechanism. It is both sound and adequate: we have to show that for all presentations E, E' such that $E \rightsquigarrow E'$ we have $ThE = ThE'$.

- If the deduction step is **Delete** where $E = E' \cup \{t = t\}$, we have $E' \subseteq E$, so that $ThE' \subseteq ThE$. Furthermore, the assumption $t = t$ in a proof of $Pf(E)$ can be replaced by a proof $\bar{t}$ using only **Congruence** and whose tree structure is isomorph to the one of t — for instance, if $t = f(a, g(b))$, $\bar{t}$ will be

$$\dfrac{\dfrac{}{a=a}\,C \qquad \dfrac{\dfrac{}{b=b}\,C}{g(b)=g(b)}\,C}{f(a,g(b))=f(a,g(b))}\,C$$

  — so that every proof in $Pf(E)$ can be transformed to a proof in $Pf(E')$.

- If the deduction step is **Deduce** where $E \setminus E' = \{w = t[u]\}$ and $E' \setminus E = \{w = t[v]\}$, the assumption $w = t[u]$ in a proof of $Pf(E)$ can be replaced by the proof

$$\dfrac{\dfrac{\boxed{w=t[v]}}{w=t[v]}\,I_{w=t[v]} \qquad \begin{array}{c}\dfrac{\boxed{v=u}}{v=u}\,I_{v=u}\\ \vdots\\ C^*\end{array}}{t[v]=t[u]}\,T$$
$$w = t[u]$$

  where the right subtree consists only in **Congruence** and **Introduction** of $v = u$, so that every proof in $Pf(E)$ can be transformed to a proof of $Pf(E')$, and $ThE \subseteq ThE'$. The other inclusion is exactly symmetrical.

8.5.2 Ground Completion is Good

We want to show that $\rightsquigarrow \subseteq \succsim$. Let E, E' be presentations such that $E \rightsquigarrow E'$.

- If the deduction step is **Delete**, we first note that $I_{t=t} > \bar{t}$. Using the replacement postulate E, we can therefore transform proofs in $Pf(E)$ to smaller proofs in $Pf(E') = Pf(E \setminus \{t = t\})$.
- If the deduction step is **Deduce**, we first note that if $u \gg v$,

$$\dfrac{\dfrac{}{w = t[u]}\, I_{w=t[u]}}{w = t[u]} > \dfrac{\dfrac{\dfrac{}{w = t[v]}\, I_{w=t[v]} \qquad \dfrac{\dfrac{}{v = u}\, I_{v=u}}{\vdots\, C^*}}{t[v] = t[u]}\, T}{w = t[u]}$$

  clearly $I_{w=t[u]} > I_{w=t[v]}$ and $I_{w=t[u]} > I_{v=u}$ because $\gg$ is a simplification ordering so that $u \gg v$ implies $t[u] \gg t[v]$ and $t[u] \gg u \gg v$.

8.5.3 Ground Completion terminates

To show this, consider $\gg_{mult\,mult}$ the multiset extension of the multiset extension of the ordering over terms, which is well-founded because $\gg$ is. It is easy to show that $\rightsquigarrow \subseteq \gg_{mult\,mult}$:

- if the deduction step is **Delete**, it is trivial;
- if the deduction step is **Deduce** with $E \cup \{w = t[u]\} \rightsquigarrow E \cup \{w = t[v]\}$ and $u \gg v$, then $t[u] \gg t[v]$ because $\gg$ is a reduction ordering, so that $w = t[u] \gg_{mult} w = t[v]$ and $E \cup \{w = t[u]\} \gg_{mult\,mult} E \cup \{w = t[v]\}$.

Let n denotes the step when the ground completion terminates.

8.5.4 Ground Completion is Canonical

To show this, we need another proof representation, as presented in section 9.2. The rules to obtain a proof by replacement are here a little different, as presented in figure 8.3.

Lemma 8.1. *For all ground completion derivations* $(E_i)_i$,

$$E_0^\sharp \subseteq E_n$$

Proof. By contradiction, suppose there exists $a = b \in E_0^\sharp \setminus E_n$. Because for all terms t, $I_{t=t} > \bar{t}$ and $I_{a=b} \in Nf(E_0)$ (see theorem 7.13), we have $a \neq b$. Suppose for instance that $a \gg b$.

Because ground completion is adequate, there exists a proof of $a = b$ in $Pf(E_n)$ and a fortiori in $\mu Pf(E_n)$. Let p denotes this proof. Because $a = b \in E_0^\sharp$, $I_{a=b} \in Nf(E_0) = Nf(E_n)$ so that

$$p > I_{a=b} \tag{8.1}$$

p consists in **Transitivity**, **Congruence** and **Introduction**. Because of the definition of the precedence, (8.1) is possible if and only if there exists an introduction of some equational axiom $c = d$ in p such that

$$c = d \gg_{mult} a = b \tag{8.2}$$

Delete Useless Identities:
For all proof terms $\pi : t = t'$,

$$\left.\begin{array}{l} T(\pi, \bar{t'}) \\ T(\bar{t}, \pi) \end{array}\right\} \rightsquigarrow_g \pi$$

Sequentialization:
For all proof terms $\pi_1 : t_1 = t'_1, \ldots, \pi_n : t_n = t'_n$, if there exists $i \neq j \in \{1, \ldots, n\}$ such that $\pi_i \neq t_i$ and $\pi_j \neq t_j$, and if σ is a permutation in $\{1, \ldots, n\}$ such that there exists $i \in \{1, \ldots, n\}$ such that for all $j \in \{1, \ldots, i\}$, $t_{\sigma(j)} \gtrdot t'_{\sigma(j)}$ and for all $j \in \{i+1, \ldots, n\}$, $t'_{\sigma(j)} \gg t_{\sigma(j)}$

$$C(\pi_1, \ldots, \pi_n) \rightsquigarrow_g$$
$$T(C(\bar{t_1}, \ldots, \pi_{\sigma(1)}, \ldots, \bar{t_n}), T(\ldots, C(\bar{t'_1}, \ldots, \pi_{\sigma(n)}, \ldots, \bar{t'_n})))$$

Composition Shallowing:
For all $i \in \{1, \ldots, n\}$, for all Σ-terms $t_1, \ldots, t_n$, for all proof terms $\pi_i : t_i = t'_i, \pi'_i : t'_i = t''_i$,

$$C(\bar{t_1}, \ldots, T(\pi_i, \pi'_i), \ldots, \bar{t_n}) \rightsquigarrow_g T(C(\bar{t_1}, \ldots, \pi_i, \ldots, \bar{t_n}), C(\bar{t_1}, \ldots, \pi'_i, \ldots, \bar{t_n}))$$

Figure 8.3: Rewrite System for Proof Terms in the Ground Case

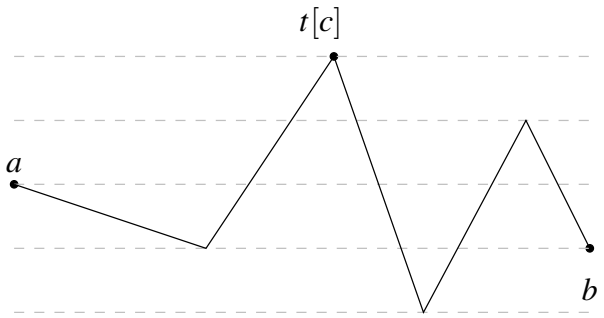
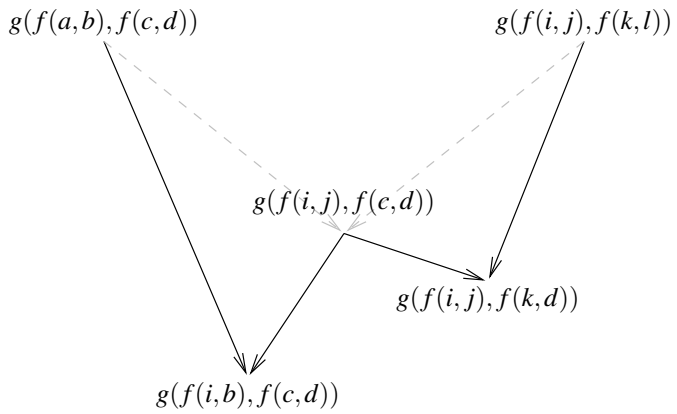


Figure 8.4: Shape of a Non-Canonical Proof

Suppose for instance that $c \gtrdot d$. (8.2) means that $c \gtrdot a$ and $c \gg b$.

Consider the proof by replacement $\vec{p}$ obtained from p with the rules of figure 8.3. The equational axiom $c = d$ rewrites a term $t[c]$ in a term $t[d]$ in that proof. Because $\gg$ has the subterm property, $t[c] \gtrdot a, b$. The proof by replacement has the shape represented in figure 8.4.

- If $t[c] \gg a, b$, then there must be some peak in the proof $\vec{p}$. Consider the maximal peak in $\vec{p}$. Due to the way we rewrote p into $\vec{p}$, this can not be a parallel peak, i.e. when the rewriting in both sides occurs in different subterms of $t[c]$, as shown in figure 8.5. Then we have here an instance of **Deduce** between equational axioms of E_n, which leads to a contradiction with the termination of the ground completion at the step n.



$$\dfrac{\dfrac{\dfrac{\boxed{a=i}}{a=i}\,I_{a=i} \quad \dfrac{\boxed{b=j}}{b=j}\,I_{b=j}}{f(a,b)=f(i,j)}\,C \quad \dfrac{\dfrac{\boxed{c=k}}{c=k}\,I_{c=k} \quad \dfrac{\boxed{d=l}}{d=l}\,I_{d=l}}{f(c,d)=f(k,l)}\,C}{g(f(a,b),f(c,d))=g(f(i,j),f(k,l))}\,C$$

with $a > i, j > b$ and $d > k, l > c$

Figure 8.5: Example of *non-maximal* parallel peak in the proof by replacement of $g(f(a,b),f(c,d)) = g(f(i,j),f(k,l))$. Because we impose the subproofs to be ordered in a valley way, parallel peaks do not appear above the side terms.

- If $t[c] = a$, then because $c \geq a$, we have $c = a$. Because $c = d \gg_{mult} a = b$, we have then $d \gg b$. Consider $e = f$ the equational axiom introduced after $c = d$ in $\vec{p}$. If $e \gg f$, then we have an instance of **Deduce** because d can be rewritten by $e = f$. Otherwise, because $d \gg b$, there must be a peak somewhere in $\vec{p}$, and we can conclude with the same arguments as above.

□

The converse can also be shown:

Lemma 8.2. *For all ground completion derivations* $(E_i)_i$,

$$E_n \subseteq E_0^\sharp$$

Proof. By contradiction, suppose there exists $a = b \in E_n \setminus E_0^\sharp$. Because ground completion terminates at step n, we can not have an instance of **Delete**, thus $a \neq b$. Suppose for instance $a \gg b$.

Because $a = b \notin E_0^\sharp$, there exist $p \in Pf(E_0^\sharp)$ such that $I_{a=b} > p$. Consider $c = d$ the leftmost **Introduction** in p. We must have $a = t[c]$ for some context $t[]$. If $d \gg c$, then $t[d] \gg b$, there must be a peak appearing in p. With the same argument than in the preceding proof, there must be an instance of **Deduce** in $E_0^\sharp$, and because we just proved that $E_0^\sharp \subseteq E_n$, this leads to a contradiction with the termination of the ground completion at the step n. Otherwise, there is an instance of **Deduce** between $a = b$ and $c = d$, which also leads to a contradiction with the termination of the ground completion at the step n. □

THEOREM 8.3 (Completeness of Completion[Bonacina et Dershowitz, 2005])**.**
Ground completion results — at the limit — in the canonical, Church-Rosser basis.

Proof. There is nothing more to prove, because we have $E_n = E_\infty = E_0^\sharp$, and ground completion is good so we can use lemma 7.18.

Notice that because $E_\infty \setminus E_0^\sharp = \emptyset$, ground completion is in fact uniformly fair, as expected. □

We have therefore shown that the framework of the abstract canonical systems can be applied to the ground completion. This is not surprising, because this framework was built around this kind of completion procedures. Nevertheless, we had to give a formal proof, and the fully detailed proof was not so trivial.

Chapter 9

Application to Standard Completion

We now want to see if the work presented in the precedent chapter can be applied to the standard completion [Knuth et Bendix, 1970]. It appears that the proof representation as proof tree with a RPO as ordering is not well adapted to this case. We therefore had to think about two different representations, as presented in section 9.2. A fully detailed proof that the standard completion is an instance of the framework of the abstract canonical systems is then given.

9.1 Presentation

The standard completion algorithm was first introduced by Knuth and Bendix in [Knuth et Bendix, 1970], hence the name it is often called. Its correctness was first shown by Huet in [Huet, 1980a], using a fairness hypothesis. We use here a presentation of this algorithm as inference rules (see figure 9.1), as can be found in [Bachmair, 1987, Bachmair et Dershowitz, 1994].

The Knuth-Bendix algorithm consists in 6 rules which apply to a couple E, R of a set of equational axioms and a set of rewriting rules. It takes a reduction ordering $\gg$ over terms as argument. The rules are presented in figure 9.1.

Since [Huet, 1980a], standard completion is associated with a fairness assumption (see [Bachmair, 1987, lemma 2.8]): at the limit, all equations are oriented ($E_\infty = \emptyset$) and all persistent critical pairs coming from R_∞ are treated by **Deduce** at least once.

Because we work with terms with variables, the reduction ordering $\gg$ can not be total, so that **Orient** may fail. Therefore, the standard completion algorithm may either:

- terminate with success and yield a terminating, confluent set of rules;
- terminate with failure; or
- not terminate.

The completeness of the standard completion will only be shown for the first case.

[1] CP design the set of critical pairs, see definition 6.19 page 48.
[2] $\blacktriangleright$ design the encompassment ordering, see definition 6.10 page 46.

Deduce[1]**:**
If $s = t \in CP(R)$

$$E, R \rightsquigarrow E \cup \{s = t\}, R$$

Orient:
If $s \gg t$

$$E \cup \{s = t\}, R \rightsquigarrow E, R \cup \{s \to t\}$$

Delete:

$$E \cup \{s = s\}, R \rightsquigarrow E, R$$

Simplify:
If $s \underset{R}{\longrightarrow} u$

$$E \cup \{s = t\}, R \rightsquigarrow E \cup \{u = t\}, R$$

Compose:
If $t \underset{R}{\longrightarrow} u$

$$E, R \cup \{s \to t\} \rightsquigarrow E, R \cup \{s \to u\}$$

Collapse[2]**:**
If $s \underset{v \to w \in R}{\longrightarrow} u$, and $s \blacktriangleright v$,

$$E, R \cup \{s \to t\} \rightsquigarrow E \cup \{u = t\}, R$$

Figure 9.1: Standard Completion Inference Rules.

9.2 Equational Proofs Representation

9.2.1 Proof Terms

This proof representation comes from the rewriting logic (introduced by [Meseguer, 1992], it is for instance used in [Kirchner et al., 1995]). Consider a signature Σ, and a set of equational axioms E and a set of rewrite rules R based on this signature. We consider the rules of the equational logic given in the figure 9.2. These inference rules define the *proof term* associated with a proof. The notation $\pi : t \longrightarrow t'$ means that π is a proof term showing that the term t can be rewritten to the term t'.

Notice that the terms based on the signature Σ are plunged into the proof terms when they are formed with the rules **Reflexivity** and **Congruence**. Notice also that **Reflexivity** for $t \longrightarrow t$ is not essential because it can be replaced by a tree of **Congruence** isomorph to t. The proof terms associated are furthermore the same in both case: t.

Reflexivity:

$$\frac{}{t : t \longrightarrow t}$$

Congruence:

$$\frac{\pi_1 : t_1 \longrightarrow t'_1 \quad \ldots \quad \pi_n : t_n \longrightarrow t'_n}{f(\pi_1,\ldots,\pi_n) : f(t_1,\ldots,t_n) \longrightarrow f(t'_1,\ldots,t'_n)}$$

Replacement:
For all rules or equational axiom $\ell = (g(x_1,\ldots,x_n), d(x_1,\ldots,x_n)) \in E \cup R$,

$$\frac{\pi_1 : t_1 \longrightarrow t'_1 \quad \ldots \quad \pi_n : t_n \longrightarrow t'_n}{\ell(\pi_1,\ldots,\pi_n) : g(t_1,\ldots,t_n) \longrightarrow d(t'_1,\ldots,t'_n)}$$

Transitivity:

$$\frac{\pi_1 : t_1 \longrightarrow t_2 \quad \pi_2 : t_2 \longrightarrow t_3}{\pi_1;\pi_2 : t_1 \longrightarrow t_3}$$

Symmetry:

$$\frac{\pi : t_1 \longrightarrow t_2}{\pi^{-1} : t_2 \longrightarrow t_1}$$

Figure 9.2: Inference Rules for Equational Logic

Some proof terms defined here are "essentially the same". For instance, the transitivity operator should be considered as associative, so that the proofs $(\pi_1;\pi_2);\pi_3$ and $\pi_1;(\pi_2;\pi_3)$ are equal. This can be done by quotienting the proof terms algebra by the congruence rules of figure 9.3.

The rules **Associativity**, **Identities** and **Inverse** give a group structure to the proof terms algebra. We can therefore deduce for instance that the proofs $(\pi_1;\pi_2)^{-1}$ and $\pi_2^{-1};\pi_1^{-1}$ are equivalent. We similarly have $f(\pi_1,\ldots,\pi_n)^{-1}$ equivalent to $f(\pi_1^{-1},\ldots,\pi_n^{-1})$ — because

$$\begin{aligned}
f(\pi_1^{-1},\ldots,\pi_n^{-1}) &\equiv f(\pi_1^{-1},\ldots,\pi_n^{-1});t' \\
&\equiv f(\pi_1^{-1},\ldots,\pi_n^{-1});(f(\pi_1,\ldots,\pi_n);f(\pi_1,\ldots,\pi_n)^{-1}) \\
&\equiv (f(\pi_1^{-1},\ldots,\pi_n^{-1});f(\pi_1,\ldots,\pi_n));f(\pi_1,\ldots,\pi_n)^{-1} \\
&\equiv f(\pi_1^{-1};\pi_1,\ldots,\pi_n^{-1};\pi_n);f(\pi_1,\ldots,\pi_n)^{-1} \\
&\equiv f(t_1,\ldots,t_n);f(\pi_1,\ldots,\pi_n)^{-1} \\
&\equiv f(\pi_1,\ldots,\pi_n)^{-1}
\end{aligned} \quad .$$

9.2.2 Proofs by Replacement of Equal by Equal

This proof representation was introduced by [Bachmair et Dershowitz, 1994, Bachmair, 1987] to prove the completeness of the Knuth-Bendix completion algorithm, using an ordering over such proofs that decreases for every completion step.

Associativity:
For all proof terms π_1, π_2, π_3,

$$\pi_1;(\pi_2;\pi_3) \equiv (\pi_1;\pi_2);\pi_3$$

Identities:
For all proof terms $\pi : t \longrightarrow t'$,

$$\pi;t' \equiv t;\pi \equiv \pi$$

Preservation of composition:
For all proof terms $\pi_1, \ldots, \pi_n, \pi'_1, \ldots, \pi'_n$, for all function symbols f,

$$f(\pi_1;\pi'_1, \ldots, \pi_n;\pi'_n) \equiv f(\pi_1, \ldots, \pi_n);f(\pi'_1, \ldots, \pi'_n)$$

Parallel Move Lemma:
For all rewrite rules or equational axiom $\ell = (g(x_1, \ldots, x_n), d(x_1, \ldots, x_n)) \in E \cup R$, for all proof terms $\pi_1 : t_1 \longrightarrow t'_1, \ldots, \pi_n : t_n \longrightarrow t'_n$,

$$\begin{aligned} \ell(\pi_1, \ldots, \pi_n) &\equiv \ell(t_1, \ldots, t_n);d(\pi_1, \ldots, \pi_n) \\ &\equiv g(\pi_1, \ldots, \pi_n);\ell(t'_1, \ldots, t'_n) \end{aligned}$$

Inverse:
For all proof terms $\pi : t \longrightarrow t'$,

$$\begin{aligned} \pi;\pi^{-1} &\equiv t \\ \pi^{-1};\pi &\equiv t' \end{aligned}$$

Figure 9.3: Equivalence of Proof Terms

An *equational proof step* is an expression $s \underset{e}{\overset{p}{\longleftrightarrow}} t$ where s and t are terms, e is an equational axiom $u = v$, and p is a position in $\mathfrak{p}(s)$ such that $s_{|p} = \sigma(u)$ and $t = s[\sigma(v)]_p$ for some substitution σ.

An *equational proof* of $s_0 = t_n$ is any finite sequence of equational proof steps $\left(s_i \underset{e_i}{\overset{p_i}{\longleftrightarrow}} t_i\right)_{i \in \{0,\ldots,n\}}$ such that $t_i = s_{i+1}$ for all $i \in \{0, \ldots, n-1\}$. It is noted

$$s_0 \underset{e_0}{\overset{p_0}{\longleftrightarrow}} s_1 \underset{e_1}{\overset{p_1}{\longleftrightarrow}} s_2 \cdots s_n \underset{e_n}{\overset{p_n}{\longleftrightarrow}} t_n$$

A *rewrite proof step* is an expression $s \underset{\ell}{\overset{p}{\longrightarrow}} t$ or $t \underset{\ell}{\overset{p}{\longleftarrow}} s$ where s and t are terms, ℓ is a rewrite rule $u \to v$, and p is a position in $\mathfrak{p}(s)$ such that $s_{|p} = \sigma(u)$ and $t = s[\sigma(v)]_p$ for some substitution σ.

An *proof by replacement (of equal by equal)* of $s_0 = t_n$ is any finite sequence of equational proof

steps and rewrite proof step $\left(s_i \overset{p_i}{\underset{\ell_i}{\leftrightarrows}} t_i\right)_{i\in\{0,\dots,n\}}$ where $\leftrightarrows_i \in \{\longleftrightarrow, \longrightarrow, \longleftarrow\}$ for $i \in \{0,\dots,n\}$ and such that $t_i = s_{i+1}$ for all $i \in \{0,\dots,n-1\}$. It is noted

$$s_0 \overset{p_0}{\underset{\ell_0}{\leftrightarrows}}_0 s_1 \overset{p_1}{\underset{\ell_1}{\leftrightarrows}}_1 s_2 \cdots s_n \overset{p_n}{\underset{\ell_n}{\leftrightarrows}}_n t_n$$

9.2.3 From Proof Terms to Proofs by Replacement

In order to have a one to one correspondence between proof representations, we need to use the equivalence of proof terms defined in figure 9.3. We can refine them to the proof term rewrite system $\rightsquigarrow$ given in the figure 9.4, so that the proofs terms in normal form correspond exactly to proof by replacement.

The associativity is still considered as a congruence, so that all proof terms rewrite rules must be considered modulo the associativity of ; which will be noted $\sim$. The class rewrite system that we consider will be therefore noted $\rightsquigarrow / \sim$. As it is linear, we can use the work of [Huet, 1980b].

We first prove that this rewrite system is included in the equivalence relation of figure 9.3.

Proposition 9.1 (Correctness)**.** *For all proof terms π_1, π_2, if $\pi_1 \rightsquigarrow \pi_2$ then $\pi_1 \equiv \pi_2$.*

Proof. By case study. □

The converse is false: for instance $f(\ell_1,\ell_2) \equiv f(t_1,\ell_2);f(\ell_1,t_2')$ but we do not have $f(\ell_1,\ell_2) \overset{*}{\underset{\rightsquigarrow}{\leftrightarrow}} f(t_1,\ell_2);f(\ell_1,t_2')$.

To prove the termination of $\rightsquigarrow / \sim$, according to proposition 6.7, we need a reduction ordering compatible with the associativity. We consider only associativity here, although most of the existing works use associativity and commutativity. Therefore, we need the following lemma.

Lemma 9.2. *If $A \subseteq B$ then $>$ is B-compatible implies $>$ is A-compatible.*

Proof. Just notice that $s' \overset{*}{\underset{A}{\longleftrightarrow}} s > t \overset{*}{\underset{A}{\longleftrightarrow}} t'$ implies $s' \overset{*}{\underset{B}{\longleftrightarrow}} s > t \overset{*}{\underset{B}{\longleftrightarrow}} t'$. □

We can therefore use the *AC*-RPO ordering of [Rubio et Nieuwenhuis, 1995] (see definition 6.24 page 50). We define a precedence $>$ such that for all function symbols f and for all rule labels ℓ we have $\ell > f > \cdot^{-1} >$;. The *AC*-RPO built with this precedence will be noted $\succ$.

To show termination, we also need the following lemma:

Lemma 9.3. *For all proof terms $\pi : t \longrightarrow t'$, we have $\pi \succeq t$ and $\pi \succeq t'$.*

Proof. By induction on the structure of the proof term π.

For **Reflexivity**, $\pi = t = t'$.

For **Congruence**, $\pi = f(\pi_1,\dots,\pi_n)$, $t = f(t_1,\dots,t_n)$ and $t' = f(t_1',\dots,t_n')$. By induction hypothesis, for all $i \in \{1,\dots,n\}$, we have $\pi_i \succeq t_i, t_i'$. Furthermore, π is not reducible on the top position using rules (6.1), so that $snf(\pi) = \{f(\pi_1',\dots,\pi_n') \,:\, \forall i,\ \pi_i' \in snf(\pi_i)\}$, whereas t and t' are not reducible. Consequently, by definition of an *AC*-RPO, $\pi \succeq t, t'$.

For **Replacement**, $\pi = \ell(\pi_1,\dots,\pi_n)$, $t = g(t_1,\dots,t_n)$ and $t' = d(t_1',\dots,t_n')$ where $\ell = (g,d) \in E \cup R$. With the same arguments than for **Congruence**, we can conclude that $\pi \succeq t, t'$ (recall that $\ell > g, d$).

Delete Useless Identities:
For all proof terms $\pi : t \longrightarrow t'$,

$$\left.\begin{array}{l}\pi; t' \\ t; \pi\end{array}\right\} \rightsquigarrow \pi$$

Sequentialization:
For all function symbols f, for all proof terms $\pi_1 : t_1 \longrightarrow t'_1, \ldots, \pi_n : t_n \longrightarrow t'_n$, if there exists $i \neq j \in \{1, \ldots, n\}$ such that $\pi_i \neq t_i$ and $\pi_j \neq t_j$,

$$f(\pi_1, \ldots, \pi_n) \rightsquigarrow f(\pi_1, t_2, \ldots, t_n); f(t'_1, \pi_2, \ldots, t_n); \ldots; f(t'_1, t'_2, \ldots, \pi_n)$$

Composition Shallowing:
For all $i \in \{1, \ldots, n\}$, for all Σ-terms $t_1, \ldots, t_n$, for all proof terms $\pi_i : t_i \longrightarrow t'_i, \pi'_i : t'_i \longrightarrow t''_i$, for all function symbols f,

$$f(t_1, \ldots, \pi_i; \pi'_i, \ldots, t_n) \rightsquigarrow f(t_1, \ldots, \pi_i, \ldots, t_n); f(t_1, \ldots, \pi'_i, \ldots, t_n)$$

Parallel Moves:
For all rewrite rules or equational axiom $\ell = (g(x_1, \ldots, x_n), d(x_1, \ldots, x_n)) \in E \cup R$, for all proof terms $\pi_1 : t_1 \longrightarrow t'_1, \ldots, \pi_n : t_n \longrightarrow t'_n$, if there exists $i \in \{1, \ldots, n\}$ such that $\pi_i \neq t_i$,

$$\ell(\pi_1, \ldots, \pi_n) \rightsquigarrow \ell(t_1, \ldots, t_n); d(\pi_1, \ldots, \pi_n)$$

Delete Useless Inverses:
For all Σ-term t,

$$t^{-1} \rightsquigarrow t$$

Inverse Congruence:
For all terms $t_1, \ldots, t_n$, for all i in $\{1, \ldots, n\}$, for all proof terms $\pi_i : t_i \longrightarrow t'_i$, for all function symbols f,

$$f(t_1, \ldots, \pi_i^{-1}, \ldots, t_n) \rightsquigarrow f(t_1, \ldots, \pi_i, \ldots, t_n)^{-1}$$

Inverse Composition:
For all proof terms π_1, π_2,

$$(\pi_1; \pi_2)^{-1} \rightsquigarrow \pi_2^{-1}; \pi_1^{-1}$$

Figure 9.4: Rewrite System for Proof Terms

For **Transitivity**, $\pi = \pi_1; \pi_2$ where $\pi_1 : t \longrightarrow t''$ and $\pi_2 : t'' \longrightarrow t'$. By induction hypothesis, $\pi_1 \succeq t$ and $\pi_2 \succeq t'$. As $\succ$ is a simplification ordering, $\pi \succ \pi_1, \pi_2 \succeq t, t'$.

For **Symmetry**, $\pi = \pi'^{-1}$ where $\pi' : t' \longrightarrow t$. By induction hypothesis and because $\succ$ is a simplification ordering, $\pi \succ \pi' \succeq t', t$.

□

Proposition 9.4 (Termination)**.** *The rewrite system $\rightsquigarrow$ of figure 9.4 modulo $\sim$ is terminating for ground proof terms.*

Proof. We can show that $\rightsquigarrow \subseteq \succ$, thus proving the termination of $\rightsquigarrow / \sim$:

For **Delete Useless Identities**, it comes from the fact that $\succ$ is a simplification ordering.

For **Sequentialization**, rules (6.1) are not applicable on the left side whereas they lead on the right side to $;(f(\pi_1,t_2,\ldots,t_n),f(t'_1,\pi_2,\ldots,t_n),\ldots,f(t'_1,t'_2,\ldots,\pi_n))$. We have $f >;$, thus by definition of a RPO, we must then prove that for all $i \in \{1,\ldots,n\}$ we have $f(\pi_1,\ldots,\pi_n) \succ_{RPO} f(t'_1,\ldots,t'_{i-1},\pi_i,t_{i+1},\ldots,t_n)$, i.e. $(\pi_1,\ldots,\pi_n) \succ^{lex}_{RPO} (t'_1,\ldots,t'_{i-1},\pi_i,t_{i+1},\ldots,t_n)$. By hypothesis there exists at least a $j \in \{1,\ldots,n\} \setminus \{i\}$ such that $\pi_j \neq t_j$, so we can conclude with the preceding lemma.

For **Composition Shallowing**, both sides are not reducible using rules (6.1). We have $f >;$, thus we have to show: $f(t_1,\ldots,\pi_i;\pi'_i,\ldots,t_n) \succ_{RPO} f(t_1,\ldots,\pi_i,\ldots,t_n)$ and $f(t_1,\ldots,\pi_i;\pi'_i,\ldots,t_n) \succ_{RPO} f(t_1,\ldots,\pi'_i,\ldots,t_n)$. Both comparisons hold by definition of a RPO.

For **Parallel Moves**, both sides are not reducible using rules (6.1). We have $\ell >;$, thus we have to prove that $\ell(\pi_1,\ldots,\pi_n) \succ_{RPO} \ell(t_1,\ldots,t_n)$ and $\ell(\pi_1,\ldots,\pi_n) \succ_{RPO} d(\pi_1,\ldots,\pi_n)$. The first comparison holds because of the lemma and because there exists a $i \in \{1,\ldots,n\}$ such that $\pi_i \neq t_i$; the second one holds because $\ell > d$.

For **Delete Useless Inverses**, this comes from the fact that $\succ$ is a simplification ordering.

For **Inverse Congruence**, both sides are not reducible using rules (6.1), therefore this is a consequence of $f > \cdot^{-1}$.

For **Inverse Composition**, both sides are not reducible using rules (6.1), therefore this is a consequence of $\cdot^{-1} >;$. □

We can also prove confluence:

Proposition 9.5 (Confluence)**.** *The rewrite system $\rightsquigarrow$ is confluent modulo $\sim$ on ground proof terms.*

Proof. The class rewrite system is linear and terminating, so we just have to check that the critical pairs are confluent.

For $\underset{R}{\longleftarrow} \circ \underset{R}{\longrightarrow}$, it is easy to check for most of the critical pairs that they are confluent. We only detail the most problematic one. For two possible applications of **Sequentialization**, we have for instance $f(g(\nu_1,\ldots,\nu_m),\pi_1,\ldots,\pi_n)$ that can be rewritten to $f(g(\nu_1,\ldots,\nu_m),t_1,\ldots,t_n);f(g(s_1,\ldots,s_m),\pi_1,\ldots,t_n);\ldots;f(g(s_1,\ldots,s_m),t'_1,\ldots,\pi_n)$ and to $f(g(\nu_1,\ldots,s_m);\ldots;g(s'_1,\ldots,\nu_m),\pi_1,\ldots,\pi_n)$. Both of them reduce to $f(g(\nu_1,\ldots,s_m);\ldots;g(s'_1,\ldots,\nu_m),t_1,\ldots,t_n);f(g(s_1,\ldots,s_m),\pi_1,\ldots,t_n);\ldots;f(g(s_1,\ldots,s_m),t'_1,\ldots,\pi_n)$.

For $\underset{R}{\longleftarrow} \circ \underset{A}{\longleftrightarrow}$, the only rules that can interfere with $\sim$ are **Delete Useless Identities**, **Composition Shallowing** and **Inverse Composition**. We can check that all critical pairs are confluent.

□

The proof terms rewrite system $\rightsquigarrow$ allow us to give a correspondence between proof terms and proofs by replacement of equal by equal: normal forms of proof terms correspond exactly to proofs by replacement. This fact is expressed in the following theorem, which is indeed a generalization of Lemma 3.6 in [Meseguer, 1992] for equational logic. We also have operationalized the way to construct the chain of "one-step sequential rewrites".

THEOREM 9.6 (Correspondence between Proof Representations)**.**
The normal form of a proof term π for the rewrite system $\rightsquigarrow$, noted $nf(\pi)$, has the following form: there exists $n \in \mathbb{N}$, some contexts $w_1[],\ldots,w_n[]$, some indices $i_1,\ldots,i_n \in \{-1,1\}$, some rule labels $\ell_1,\ldots,\ell_n$ and some terms $t^1_1,\ldots,t^1_{m_1},\ldots,t^n_1,\ldots,t^n_{m_n}$ such that

$$nf(\pi) = (w_1[\ell_1(t^1_1,\ldots,t^1_{m_1})])^{i_1};\ldots;(w_n[\ell_n(t^n_1,\ldots,t^n_{m_n})])^{i_n}$$

where ν^1 *is a notation for* ν.

We will denote by $nf(\pi)$ *the normal form of a proof term* π.

Such a proof term correspond with the following proof by replacement of equal by equal:

$$w_1[g_1(t_1^1,\dots,t_{m_1}^1)] \underset{\ell_1}{\overset{p_1}{\leftrightarrows}}_1 w_1[d_1(t_1^1,\dots,t_{m_1}^1)] \underset{\ell_2}{\overset{p_2}{\leftrightarrows}}_2 \cdots w_n[g_n(t_1^n,\dots,t_{m_n}^n)] \underset{\ell_n}{\overset{p_n}{\leftrightarrows}}_n w_n[d_n(t_1^n,\dots,t_{m_n}^n)]$$

where for all $j \in \{1,\dots,n\}$ *we have:*

- $\ell_j = (g_j, d_j)$,
- p_j *is the position of* $[]$ *in* $w_j[]$,
- $\leftrightarrows_j = \begin{array}{ll} \longrightarrow & \text{if } i_j = 1 \text{ and } \ell_j \in R, \\ \longleftarrow & \text{if } i_j = -1 \text{ and } \ell_j \in R, \\ \longleftrightarrow & \text{if } \ell_j \in E. \end{array}$
- *if* $j \neq n$, $w_j[d_j(t_1^j,\dots,t_{m_j}^j)] = w_{j+1}[g_{j+1}(t_1^{j+1},\dots,t_{m_{j+1}}^{j+1})]$.

Proof. We first have to check that proof terms in that form are indeed irreducible by $\rightsquigarrow$, what is left to the reader.

Then, suppose that we have an irreducible proof term. Because **Sequentialization** can not be applied, there is at most one ; under all function symbols. Because **Composition Shallowing** can not be applied, there are no ; under all function symbols. Because **Inverse Congruence** and **Inverse Composition** can not be applied, $\cdot^{-1}$ is applied between ; and function symbols. Irreducible proof term are therefore application of ; over eventually $\cdot^{-1}$ over base terms composed of function symbols and rule labels.

Because **Delete Useless Identities** and **Delete Useless Inverse** can not be applied, there is a least one non-trivial proof (i.e a proof with a label in it) in each of these base terms. Because **Sequentialization** can not be applied, there is at most one non-trivial proof in each of them. Because **Parallel Moves** can not be applied, the subterms of the labels are Σ-terms. Consequently, each base term contains one and only one rule label, applied to Σ-terms. □

Example 9.1*:* Consider $\pi = f(\ell_1(\ell_2),(\ell_3;r)^{-1})$ where $\ell_1 : g(x) \longrightarrow d(x)$, $\ell_2 : s = t$, $\ell_3 : l \longrightarrow r$, we have:

$$\begin{array}{ll}
\pi \underset{\rightsquigarrow}{\longrightarrow} f(\ell_1(s);d(\ell_2),(\ell_3;r)^{-1}) & \textbf{(Parallel Moves)} \\
\underset{\rightsquigarrow}{\longrightarrow} f(\ell_1(s);d(\ell_2),r);f(d(t),(\ell_3;r)^{-1}) & \textbf{(Sequentialization)} \\
\underset{\rightsquigarrow}{\longrightarrow} f(\ell_1(s);d(\ell_2),r);f(d(t),r^{-1};\ell_3^{-1}) & \textbf{(Inverse Composition)} \\
\underset{\rightsquigarrow}{\longrightarrow} f(\ell_1(s);d(\ell_2),r);f(d(t),r;\ell_3^{-1}) & \textbf{(Delete Useless Inverses)} \\
\underset{\rightsquigarrow}{\longrightarrow} f(\ell_1(s);d(\ell_2),r);f(d(t),\ell_3^{-1}) & \textbf{(Delete Useless Identities)} \\
\underset{\rightsquigarrow}{\longrightarrow} f(\ell_1(s),r);f(d(\ell_2),r);f(d(t),\ell_3^{-1}) & \textbf{(Composition Shallowing)} \\
\underset{\rightsquigarrow}{\longrightarrow} f(\ell_1(s),r);f(d(\ell_2),r);f(d(t),\ell_3)^{-1} & \textbf{(Inverse Congruence)}
\end{array}$$

This last term is the normal form proof term, and it is equivalent to the proof by replacement $f(g(s),r) \underset{\ell_1}{\overset{1}{\longrightarrow}} f(d(s),r) \underset{\ell_2}{\overset{11}{\longleftrightarrow}} f(d(t),r) \underset{\ell_3}{\overset{2}{\longleftarrow}} f(d(t),l)$.

Due to this theorem, normal forms of proof terms can be considered in the following indifferently as proof terms or as proofs by replacement.

9.2.4 Proof Representation used

In the following, the *proof terms* representation will be used, and the subproof relation $\triangleright$ will therefore be the *subterm relation*.

9.3 Proofs Ordering

The representation of Bachmair by the mean of proof by replacement was defined to introduce an order on proofs [Bachmair, 1987]: given a reduction ordering $\gg$, to each single proof steps $s \overset{p}{\underset{\ell}{\leftrightarrows}} t$ is associated a *cost*. The cost of an equational proof step $s \overset{p}{\underset{u=v}{\longleftrightarrow}} t$ is the triple $(\{\!\{s,t\}\!\},u,t)$. The cost of a rewrite proof step $s \overset{p}{\underset{u\to v}{\longrightarrow}} t$ is $(\{\!\{s\}\!\},u,t)$. Proof steps are compared with each other according to their cost, using the lexicographic combination of the multiset $\gg_{mult}$ extension of the reduction ordering over terms in the first component, the encompassment ordering $\blacktriangleright$ on the second component, and the reduction ordering $\gg$ on the last component. Proofs are compared as multisets of their proof steps. For two proofs by replacement p,q, we will write $p >_{rep} q$ if p is greater than q for such an ordering.

Using theorem 9.6, we can translate Bachmair's proof ordering to proof terms:

Definition 9.1 (Bachmair's Ordering on Proof Terms)**.** *For all proof terms π_1,π_2, we say that $\pi_1 >_B \pi_2$ iff*

$$nf(\pi_1) >_{rep} nf(\pi_2)$$

Example 9.2*:* Consider $\pi_1 = f(\ell_1^{-1};\ell_2)$ and $\pi_2 = f(\ell_3)$ where $\ell_1 = a \longrightarrow b$, $\ell_2 = a \longrightarrow c$ and $\ell_3 = b = c$, and suppose $a > b > c$.

We have $nf(\pi_1) = f(b) \overset{1}{\underset{\ell_1}{\longleftarrow}} f(a) \overset{1}{\underset{\ell_2}{\longrightarrow}} f(c)$ and $nf(\pi_2) = f(b) \overset{1}{\underset{\ell_3}{\longrightarrow}} f(c)$. The cost of $nf(\pi_1)$ is $\{\!\{(\{\!\{f(a)\}\!\},a,f(b)),(\{\!\{f(a)\}\!\},a,f(c))\}\!\}$, the cost of $nf(\pi_2)$ is $\{\!\{(\{\!\{f(b),f(c)\}\!\},b,f(c))\}\!\}$, so $nf(\pi_1) >_{rep} nf(\pi_2)$ and $\pi_1 >_B \pi_2$.

Nevertheless, we cannot hope to extend an RPO on Σ-terms to an RPO[3] $>_{rpo}$ on proof terms so that $>_B$ and $>_{rpo}$ coincide for the normal forms of proof terms:

Counter-example 9.3*:* Suppose we have $\Sigma = \{f^1,a^0,b^0,c^0\}$ where the exponents of function symbols denote their arity, and a precedence $f > a > b > c$. We consider the RPO based on such a precedence.

Let $\ell_f = f(a) \longrightarrow c$ and $\ell_b = b \longrightarrow c$.

We now want to extend the precedence to ℓ_f and ℓ_b in order to extend the RPO to proof terms. If we have $\ell_f < \ell_b$, $f(a) \overset{\varepsilon}{\underset{\ell_f}{\longrightarrow}} c >_{rep} b \overset{\varepsilon}{\underset{\ell_b}{\longrightarrow}} c$ but $\ell_f <_{rpo} \ell_b$.

If we suppose $f > \ell_f > \ell_b$ we have $f(a) \overset{\varepsilon}{\underset{\ell_f}{\longrightarrow}} c >_{rep} f(b) \overset{1}{\underset{\ell_b}{\longrightarrow}} f(c)$ but $\ell_f <_{rpo} f(\ell_b)$.

If we suppose $\ell_f > \ell_b$ and $\ell_f > f$, then $f(f(b)) \overset{11}{\underset{\ell_b}{\longrightarrow}} f(f(c)) >_{rep} f(a) \overset{\varepsilon}{\underset{\ell_f}{\longrightarrow}} c$ but $f(f(\ell_b)) <_{rpo} \ell_f$.

Such an extension is therefore impossible, there is no extension of $>_{rpo}$ on proof terms so that for all proof terms π_1,π_2, we have $nf(\pi_1) >_{rpo} nf(\pi_2)$ if and only if $nf(\pi_1) >_B nf(\pi_2)$.

[3] or better an *AC*-RPO

In the following, the proof ordering $>$ between proof terms will be the ordering $>_B$ restricted to proofs with the same conclusion.

9.4 Adequacy to the Postulates

9.4.1 Postulate A

The proof of $(u,v) \in E \cup R$ labelled by ℓ is $\ell(x_1,\ldots,x_n)$ where $x_1,\ldots,x_n$ are the free variables of (u,v).

9.4.2 Postulate B

We can replace the assumption $\ell(\pi_1,\ldots,\pi_n)$ of something proved by its proof where the free variables are replaced by the proofs $\pi_1,\ldots,\pi_n$.

9.4.3 Postulate C and D

These postulates hold because of the tree structure of proofs.

9.4.4 Postulate E

This one does not trivially hold.

We first show the following lemma:

Lemma 9.7. *For all function symbols f of arity $n+1$, for all proof terms $\pi_1,\ldots,\pi_n$, q and r,*

$$q > r \text{ implies } f(\pi_1,\ldots,q,\ldots,\pi_n) > f(\pi_1,\ldots,r,\ldots,\pi_n)$$

Proof. Suppose $q > r$, thus by definition $nf(q) >_{rep} nf(r)$. To compare $f(\pi_1,\ldots,q,\ldots,\pi_n)$ and $f(\pi_1,\ldots,r,\ldots,\pi_n)$, we have to transform them to proof by replacement. As $\underset{\rightsquigarrow/\sim}{\longrightarrow}$ is Church-Rosser, the way it is applied does not matter.

We have

$$\begin{aligned} f(\pi_1,\ldots,q,\ldots,\pi_n) &\underset{\rightsquigarrow}{\longrightarrow}^* f(\pi_1,t_2,\ldots,t_n);\ldots;f(t'_1,\ldots,q,\ldots,t_n);\ldots;f(t'_1,\ldots,\pi_n) \\ &\underset{\rightsquigarrow}{\longrightarrow}^* f(\pi_1,t_2,\ldots,t_n);\ldots;\underline{f(t'_1,\ldots,nf(q),\ldots,t_n)};\ldots;f(t'_1,\ldots,\pi_n) \end{aligned}$$

Then, if $nf(q)$ contains ; the underlined term will be split by **Composition Shallowing**. If it contains $^{-1}$ the rule **Inverse Congruence** will be applied. Some terms outside the underline corresponding to identity will be removed by **Delete Useless Identities**, and the normal form will look like

$$f(\pi_1,t_2,\ldots,t_n);\ldots;\underline{f(t'_1,\ldots,q_1,\ldots,t_n)^{i_1};\ldots;f(t'_1,\ldots,q_m,\ldots,t_n)^{i_m}};\ldots;f(t'_1,\ldots,\pi_n)$$

with $nf(q) = q_1^{i_1};\ldots;q_m^{i_m}$.

The same will apply with r, and therefore, to compare the initial proofs, we just have to compare the costs of the underlined terms.

The cost of $nf(q)$ will look like $\{\!\{(\{\!\{s_1\}\!\},u_1,h_1),\ldots,(\{\!\{s_m\}\!\},u_m,h_m)\}\!\}$. Then the cost of $f(t'_1,\ldots,q_1,\ldots,t_n)^{i_1};\ldots;f(t'_1,\ldots,q_m,\ldots,t_n)^{i_m}$ will be

$\{\!\{(\{\!\{f(t'_1,\ldots,s_1,\ldots,t_n)\}\!\},u_1,f(t'_1,\ldots,h_1,\ldots,t_n)),\ldots,(\{\!\{f(t'_1,\ldots,s_m,\ldots,t_n)\}\!\},u_m,f(t'_1,\ldots,h,m,\ldots,t_n))\}\!\}$.
For $nf(r)$ they will be respectively $\{\!\{(\{\!\{g_1\}\!\},v_1,d_1),\ldots,(\{\!\{g_p\}\!\},v_p,d_p)\}\!\}$ and $\{\!\{(\{\!\{f(t'_1,\ldots,g_1,\ldots,t_n)\}\!\},v_1,f(t'_1,\ldots,d_1,\ldots,t_n)),\ldots,(\{\!\{f(t'_1,\ldots,g_p,\ldots,t_n)\}\!\},v_p,f(t'_1,\ldots,d_p,\ldots,t_n))\}\!\}$.

$\gg$, which is used to compare the first and the third components of each part of the cost, is a reduction ordering, so that $nf(q) >_{rep} nf(r)$ implies for instance $f(t'_1,\ldots,q_1,\ldots,t_n)^{i_1};\ldots;f(t'_1,\ldots,q_m,\ldots,t_n)^{i_m} >_{rep} f(t'_1,\ldots,r_1,\ldots,t_n)^{i_1};\ldots;f(t'_1,\ldots,r_p,\ldots,t_n)^{i_p}$.

□

The same is true for labels:

Lemma 9.8. *For all rule labels ℓ, for all proof terms $\pi_1,\ldots,\pi_n$, q and r,*

$$q > r \text{ implies } \ell(\pi_1,\ldots,q,\ldots,\pi_n) > \ell(\pi_1,\ldots,r,\ldots,\pi_n)$$

Proof. $\ell(\pi_1,\ldots,q,\ldots,\pi_n)$ and $\ell(\pi_1,\ldots,r,\ldots,\pi_n)$ can be reduced by **Parallel Moves** to $\ell(t_1,\ldots,t_n);d(\pi_1,\ldots,q,\ldots,\pi_n)$ and $\ell(t_1,\ldots,t_n);d(\pi_1,\ldots,r,\ldots,\pi_n)$. We can therefore conclude using the preceding lemma.

□

This allow us to show

THEOREM 9.9 (Postulate E for Equational Proofs)**.**
For all proof terms p,r, for all position $i \in \mathfrak{p}(p)$,

$$p_{|i} > r \text{ implies } p > p[r]_i$$

Proof. This is proved by induction on i. For $i = \varepsilon$ this is trivial. For $i \neq \varepsilon$, by induction hypothesis, the result holds for the subproofs of p. Consider the head of p:

- for **Symmetry**, it is trivial;
- for **Transitivity**, it comes from the fact that equational proofs are compared as the multiset of their equational proof steps;
- for **Congruence**, it comes from lemma 9.7;
- for **Replacement**, it comes from lemma 9.8.

□

9.5 Completeness of the Standard Completion

9.5.1 Standard Completion is Sound and Adequate

This is shown in [Bachmair, 1987, Lemma 2.1]: if $E,R \rightsquigarrow E',R'$, then $\overset{*}{\underset{E\cup R}{\longleftrightarrow}}$ and $\overset{*}{\underset{E'\cup R'}{\longleftrightarrow}}$ are the same. To prove this, one has to verify it for each inference rule of standard completion, what is left to the reader.

9.5.2 Standard Completion is Good

This is shown in [Bachmair, 1987, Lemma 2.5, 2.6]: if $E,R \rightsquigarrow E',R'$, then proofs in E,R can be transformed to proofs in E',R' using following rules:

$$
\begin{array}{rcl}
s \underset{E}{\longleftrightarrow} t & \twoheadrightarrow & s \underset{R'}{\longrightarrow} t \\
s \underset{E}{\longleftrightarrow} t & \twoheadrightarrow & s \underset{R'}{\longrightarrow} u \underset{E'}{\longleftrightarrow} t \\
s \underset{E}{\longleftrightarrow} s & \twoheadrightarrow & s \\
s \underset{R}{\longleftarrow} u \underset{R}{\longrightarrow} t & \twoheadrightarrow & s \underset{E'}{\longleftrightarrow} t \\
s \underset{R}{\longleftarrow} u \underset{R}{\longrightarrow} t & \twoheadrightarrow & s \overset{*}{\underset{R'}{\longrightarrow}} v \overset{*}{\underset{R'}{\longleftarrow}} t \\
s \underset{R}{\longrightarrow} t & \twoheadrightarrow & s \underset{R'}{\longrightarrow} v \underset{R'}{\longleftarrow} t \\
s \underset{R}{\longrightarrow} t & \twoheadrightarrow & s \underset{R'}{\longrightarrow} v \underset{E'}{\longleftrightarrow} t
\end{array}
$$

We have $\underset{\twoheadrightarrow}{\longrightarrow} \subseteq >$, so these proofs become indeed better.

9.5.3 Standard Completion is Canonical

The proof is essentially the same as for ground completion, but the relation with proofs by replacement is more obvious here because of the choice of the ordering over proofs. Remember that by fairness assumption, $E_\infty = \emptyset$.

Lemma 9.10. *For all standard completion derivations* $(E_i,R_i)_i$,

$$E_0^\sharp \subseteq R_\infty$$

Proof. By contradiction, suppose there is $(a,b) \in E_0^\sharp \setminus R_\infty$, labelled ℓ. Because completion is adequate, there exists $p \in \mu Pf(R_\infty)$ proving $a = b$. Because $a = b \in E_0^\sharp$, $\ell(x_1,\ldots,x_n) \in Nf(E_0) = Nf(R_\infty)$ where $(x_i)_i$ are the free variables of ℓ, so that

$$p > \ell(x_1,\ldots,x_n)$$

- If there are no peak in $nf(p)$, then $nf(p)$ is a valley proof, and it is easy to show that it is smaller than $\ell(x_1,\ldots,x_n)$, which is a contradiction with the preceding comparison.
- If there is a parallel peak, for instance $s[c,e] \underset{\ell_1}{\overset{i}{\longleftarrow}} s[d,e] \underset{\ell_2}{\overset{j}{\longrightarrow}} s[d,f]$, then the proof by replacement where this peak is replaced by $s[c,e] \underset{\ell_2}{\overset{j}{\longrightarrow}} s[c,f] \underset{\ell_1}{\overset{i}{\longleftarrow}} s[d,f]$ is smaller, thus leading to a contradiction with the minimality of p in $Pf(R_\infty)$.
- If there is a critical peak, then by fairness assumption there is some step k where this critical peak is treated by **Deduce**. The proof of the conclusion of the critical peak at the step $k+1$ is therefore smaller. Because standard completion is good, it can only go smaller, so that at the limit we can find by replacement of the critical peak by this proof a smaller proof of $a = b$, thus leading to a contradiction with the minimality of p in $Pf(R_\infty)$.

□

Lemma 9.11. *For all standard completion derivations* $(E_i, R_i)_i$ *which* terminate without failure,

$$R_\infty \subseteq E_0^\sharp$$

Proof. By contradiction, suppose there is $(a,b) \in R_\infty \setminus E_0^\sharp$, labelled by ℓ. Then there exists a proof $p \in \mu Pf(E_0^\sharp)$ such that $\ell(x_1,\ldots,x_n) > p$ where $x_1,\ldots,x_n$ are the free variables of ℓ.

Rules comes from orientation of equational axioms through **Orient**, so that $a \gg b$. The cost of $\ell(x_1,\ldots,x_n)$ is then $\{\!\{(\{\!\{a\}\!\},a,b)\}\!\}$. Consider the leftmost step of $nf(p)$. It is of the form $a \overset{i}{\underset{(c,d)}{\leftrightarrows}} a[d]_i$ where $c = a_{|i}$. If it is $a \xleftarrow[d\to c]{i} a[d]_i$ then the cost of this proof step would be $\{\!\{(\{\!\{a[d]_i\}\!\},d,a)\}\!\}$, which is then greater than $\{\!\{(\{\!\{a\}\!\},a,b)\}\!\}$, thus leading to a contradiction with the fact that $\ell(x_1,\ldots,x_n) > p$. If $a \xleftrightarrow[c=d]{i} a[d]_i$ then the cost of this proof step would be $\{\!\{(\{\!\{a,a[d]_i\}\!\},c,a[d]_i)\}\!\}$, which is then greater than $\{\!\{(\{\!\{a\}\!\},a,b)\}\!\}$, thus leading to a contradiction with the fact that $\ell(x_1,\ldots,x_n) > p$. If it is $a \xrightarrow[c\to d]{i} a[d]_i$ then there is a critical pair $(b, a[d]_i)$ in R_∞ (we just proved that $E_0^\sharp \subseteq R_\infty$). The fairness assumption will therefore apply, and therefore **Deduce** will produce the equational axiom $b = a[d]_i$, which will be oriented, and $a \longrightarrow b \in R_\infty$ will be simplified through **Compose** or **Collapse**. Because $a \longrightarrow b$ is persisting, it must be generated once again, thus contradicting the termination of the completion. □

THEOREM 9.12 (Completeness of Standard Completion)**.**
Standard completion results — at the limit, when it terminates without failure — in the canonical, Church-Rosser basis.

Proof. There is nothing more to prove, because we have $R_\infty = E_0^\sharp$, and standard completion is good so we can use lemma 7.18.

Notice that because, when standard completion terminates without failure, $R_\infty \setminus E_0^\sharp = \emptyset$, it is in fact uniformly fair, as expected. □

Note: When standard completion does not terminate, the resulting set R_∞ is *saturated*, because $E_0^\sharp = R_\infty^\sharp \subseteq R_\infty$ (theorem 7.7), but it is not necessarily *reduced*.

This shows that the standard completion is an instance of the framework of the abstract canonical systems, when we choose the convenient proof representation.

Chapter 10

Conclusion

10.1 Abstract Canonical Systems and Natural Deduction

To apply the theory of abstract canonical systems to sequent systems such as natural deduction, we had to generalize it. This has been done by removing the premise monotonicity postulate (postulate D) and by changing the postulate of replacement (postulate E to E_{gen}). This gives us indeed a conservative generalization, so that instances of the original version of the framework of abstract canonical systems are instances of its generalization too. Another solution could have been to use another presentation of the sequent calculus where premises appears as the leafs of the proofs, as in the representation used for ground completion. This is the case for instance for some presentation of the linear logic.

We have shown that when considering the transitive closure of the β-reduction as ordering over proof terms, minimal proofs corresponds to **Cut**-free proofs. This approach can be generalized to richer sequent systems. The only requirement is that the reduction associated with such a system is strongly normalizing, and corresponds to a process of **Cut**-elimination. For instance, this can be applied to sequent calculus thanks to the work of Herbelin about the $\bar{\lambda}$-calculus and its associated reductions [Herbelin, 1995] and to linear logic with the proof-nets reduction [Cosmo et Guerrini, 1999]. It would be interesting to see how this method could be adapted to the Martin-Löf type theory [Martin-Löf, 1984] or one of its extensions, or to the sequent calculus modulo [Dowek et al., 2003] with the associated ρ-calculus [Wack, 2005].

Nevertheless, one should also consider other orderings for such systems. Because proof in natural deduction are naturally represented by λ-terms, it should be interesting to investigate what happens when using the Higher Order Recursive Path Ordering [Jouannaud et Rubio, 1996].

Furthermore, whereas **Cut**-free proofs are well adapted to automated proof search, they do not correspond to the notion of what a "good" proof is for a mathematician. Lemmas that are inlined in **Cut**-free proofs help considerably to the understanding of a proof by a human being. It could be interesting to investigate how this notion of good proof can be translated into the formalism of abstract canonical systems. The use of the "good" number of lemmas introduced seems to have something to do with the optimal β-reduction, thanks to the Curry-Howard isomorphism: a lemma should be introduced if it can be used several times in the proofs, which correspond of a proof term of the form $(\lambda x.w[x,x])l$, but it should not be introduced when it is never used, which correspond to a term of the form $(\lambda x.t)l$ where x does not freely appear in t.

10.2 Completion(s)

We presented in this report full proofs of the adequacy of ground and standard completions to the theory of abstract canonical systems. This conducted us to think about the relations between equational proofs representation. The first one, proof terms as presented in [Meseguer, 1992], is convenient to consider proofs as terms, with subterms relation and substitutions. The other one, presented in [Bachmair et Dershowitz, 1994], is fully adapted to the study of the completeness of the standard completion procedure. We presented a way to pass from one representation to another by the mean of the proof term rewrite rules presented in figure 9.4. Thanks to this, we can extend the ordering introduced with the proof by replacement to the proof terms and thus combine the advantages of both representations. The demonstration of the completeness of standard completion is consequently the same as in [Bachmair et Dershowitz, 1994].

One has now to see how these proofs can be extended to other completion procedure. Bachmair introduced another proof ordering to prove the completeness of the completion modulo [Bachmair, 1987], so that the generalization to this seems possible. One should also look at some other kind of deduction mechanisms, such as Buchberger's algorithm [Buchberger, 1965] or resolution [Robinson, 1965].

Furthermore, proof terms as presented by [Meseguer, 1992] are one of the basis for the ρ-calculus [Cirstea et al., 2003, `http://rho.loria.fr/`]. The link between the completion procedure and the sequent systems mentioned above can probably be found here. Such a relation was already presented by Dowek in a paper where he proves that confluent rewrite rules can be linked with **Cut**-free proofs of some sequent systems [Dowek, 2003].

Moreover, the framework of the abstract canonical systems was developed as formal as possible, so we can think of an utilization in an interactive theorem prover such as Coq [`http://coq.inria.fr/`]. We could therefore obtain a formal proof of the completeness of the different completion procedures, what does not seems to exist yet.

Finally, another formalism to describe logical systems, the theory of general logic, was introduced in [Meseguer, 1989, Martí-Oliet et Meseguer, 1994]. It should certainly be interesting to see how this interacts with the theory of abstract canonical systems.

Index of Definitions

Index of Notations

Table des figures

Bibliographie

[Baader et Nipkow, 1998] BAADER (F.) et NIPKOW (T.), *Term* Re*writing and* all That. Cambridge University Press, 1998. 44

[Bachmair, 1987] BACHMAIR (L.), *Proof methods for equational theories*. Thèse de doctorat, University of Illinois, Urbana-Champaign, (Ill., USA), 1987. Version révisée, août 1988. 23, 26, 34, 37, 71, 73, 79, 81, 82, 85

[Bachmair et Dershowitz, 1994] BACHMAIR (L.) et DERSHOWITZ (N.), « Equational inference, canonical proofs, and proof orderings », *Journal of Association for Computing Machinery*, vol. 41, n° 2, 1994, p. 236–276. 12, 13, 23, 26, 31, 36, 37, 42, 71, 73, 85

[Bachmair et Ganzinger, 2001] BACHMAIR (L.) et GANZINGER (H.), « Resolution theorem proving », dans *Handbook of Automated Reasoning*, p. 19–99. 2001. 11, 41

[Barendregt, 1984] BARENDREGT (H.), *The λ-Calculus, its syntax and semantics*, coll. « Studies in Logic and the Foundation of Mathematics ». Elsevier Science Publishers B. V. (North-Holland), Amsterdam, 2e édition, 1984. 59

[Blanqui et al., 1999] BLANQUI (F.), JOUANNAUD (J.-P.) et OKADA (M.), « The calculus of algebraic constructions », dans NARENDRAN (P.) et RUSINOWITCH (M.), éditeurs, *Proceedings of the 10th International Conference on Rewriting Techniques and Applications (RTA-99)*, p. 301–316, Trento, Italy, juillet 1999. Springer-Verlag LNCS 1631. 11, 41

[Bonacina et Dershowitz, 2005] BONACINA (M. P.) et DERSHOWITZ (N.), « Abstract Canonical Inference », *ACM Transactions on Computational Logic*, 2005. 12, 13, 14, 42, 51, 53, 60, 64, 69

[Boyer, 1971] BOYER (R. S.), *Locking : A Restriction of Resolution*. Thèse de doctorat, The University of Texas at Austin, 1971. 11, 41

[Brünnler, 2003] BRÜNNLER (K.), *Deep Inference and Symmetry in Classical Proofs*. Thèse de doctorat, Technische Universität Dresden, septembre 2003. 11, 41

[Buchberger, 1965] BUCHBERGER (B.), *Ein Algorithmus zum auffinden der Basiselemente des Restklassenringes nach einem nulldimensionalen Polynomideal*. Thèse de doctorat, Univ. Innsbruck, Austria, 1965. 12, 37, 42, 85

[Buchberger, 1983] BUCHBERGER (B.), « A critical-pair/completion algorithm for finitely generated ideals in rings », dans BÖRGER (E.), HASENJAEGER (G.) et RÖDDING (D.), éditeurs, *Proceedings of Logic and Machines : Decision problems and Complexity*, vol. 171 (coll. *Lecture Notes in Computer Science*), p. 137–161. Springer-Verlag, 1983. 12, 42

[Cirstea et al., 2003] CIRSTEA (H.), LIQUORI (L.) et WACK (B.), « Rewriting calculus with fixpoints : Untyped and first-order systems ». Post-proceedings of TYPES, 2003. 37, 85

[Coquand et Huet, 1988] COQUAND (T.) et HUET (G.), « The Calculus of Constructions », *Information and Computation*, vol. 76, 1988. 11, 41

[Cosmo et Guerrini, 1999] COSMO (R. D.) et GUERRINI (S.), « Strong normalization of proof nets modulo structural congruences », dans *RtA '99 : Proceedings of the 10th International Conference on Rewriting Techniques and Applications*, p. 75–89, London, UK, 1999. Springer-Verlag. 36, 84

[Dershowitz, 1982] DERSHOWITZ (N.), « Orderings for term-rewriting systems », *Theoretical Computer Science*, vol. 17, 1982, p. 279–301. 47

[Dershowitz, 2003] DERSHOWITZ (N.), « Canonicity », dans DAHN (I.) et VIGNERON (L.), éditeurs, *Fourth International Workshop on First-Order Theorem Proving (FTP)*, vol. 86. Electronic Notes in Theoretical Computer Science, juin 2003. 13, 42, 64

[Dershowitz et Kirchner, 2004] DERSHOWITZ (N.) et KIRCHNER (C.), « Abstract Canonical Presentations », *Theorical Computer Science*, 2004. Soumis. 12, 13, 14, 42, 51, 60

[Dowek, 2003] DOWEK (G.), « Confluence as a cut elimination property. », dans NIEUWENHUIS (R.), éditeur, *RTA*, vol. 2706 (coll. *Lecture Notes in Computer Science*), p. 2–13. Springer, 2003. 37, 85

[Dowek et al., 1991] DOWEK (G.), FELTY (A.), HERBELIN (H.) *et al.*, « The Coq Proof Assistant ». Guide pour Utilisateur, INRIA-CNRS-ENS, 1991. 11, 41

[Dowek et al., 2003] DOWEK (G.), HARDIN (T.) et KIRCHNER (C.), « Theorem proving modulo, revised version ». Rapport de Recherche n° 4861, Institut National de Recherche en Informatique et en Automatique, juillet 2003. http://www.inria.fr/rrrt/rr-4861.html. 36, 84

[Gallier et al., 1993] GALLIER (J.), NARENDRAN (P.), PLAISTED (D.) *et al.*, « An algorithm for finding canonical sets of ground rewrite rules in polynomial time », *J. ACM*, vol. 40, n° 1, 1993, p. 1–16. 13, 64

[Gentzen, 1934] GENTZEN (G.), « Untersuchungen über das logische Schliessen », *Mathematische Zeitschrift*, vol. 39, 1934, p. 176–210, 405–431. Traduit dans Szabo, éditeur, *The Collected Papers of Gerhard Gentzen* en tant que « Investigations into Logical Deduction ». 11, 19, 41, 58, 60

[Guglielmi, 2002] GUGLIELMI (A.), « A system of interaction and structure ». Rapport technique n° WV-02-10, Technische Universität Dresden, 2002. 11, 41

[Herbelin, 1995] HERBELIN (H.), *Séquents qu'on calcule : de l'interprétation du calcul des séquents comme calcul de λ-termes et comme calcul de stratégies gagnantes*. Thèse d'université, Université Paris 7, janvier 1995. 36, 84

[Hsiang et Rusinowitch, 1991] HSIANG (J.) et RUSINOWITCH (M.), « Proving refutational completeness of theorem proving strategies : The transfinite semantic tree method », *Journal of the ACM*, vol. 38, n° 3, juillet 1991, p. 559–587. 11, 41

[Huet, 1980a] HUET (G.), « A complete proof of correctness of the Knuth-Bendix completion algorithm ». Rapport technique n° 25, INRIA, août 1980. 23, 71

[Huet, 1980b] HUET (G.), « Confluent reductions : Abstract properties and applications to term rewriting systems », *Journal of the ACM*, vol. 27, n° 4, octobre 1980, p. 797–821. Version préliminaire dans 18th Symposium on Foundations of Computer Science, IEEE, 1977. 11, 27, 41, 50, 75

[Jouannaud et Kirchner, 1986] JOUANNAUD (J.-P.) et KIRCHNER (H.), « Completion of a set of rules modulo a set of equations », *SIAM Journal of Computing*, vol. 15, n° 4, 1986, p. 1155–1194. 11, 41

[Jouannaud et Rubio, 1996] JOUANNAUD (J.-P.) et RUBIO (A.), « A Recursive Path Ordering for Higher-Order Terms in η-Long β-Normal Form », dans GANZINGER (H.), éditeur, *Rewriting Techniques and Applications, 7th International Conference, RTA-96*, coll. « LNCS 1103 », p. 108–122, New Brunswick, NJ, USA, juillet 1996. Springer-Verlag. 37, 84

[Kamin et Lévy, 1982] KAMIN (S.) et LÉVY (J.-J.), « Attempts for generalizing the recursive path ordering », *Inria, Rocquencourt*, 1982. 47

[Kapur et Musser, 1987] KAPUR (D.) et MUSSER (D. R.), « Proof by consistency », *Artificial Intelligence*, vol. 13, n° 2, 1987, p. 125–157. 11, 41

[Kirchner et Kirchner,] KIRCHNER (C.) et KIRCHNER (H.), « Rewriting, Solving, Proving ». À paraître. Disponible sur http://www.loria.fr/~ckirchne/rsp.pdf. 44

[Kirchner et al., 1995] KIRCHNER (C.), KIRCHNER (H.) et VITTEK (M.), « Designing constraint logic programming languages using computational systems », dans VAN HENTENRYCK (P.) et SARASWAT (V.), éditeurs, *Principles and Practice of Constraint Programming. The Newport Papers.*, chap. 8, p. 131–158. The MIT press, 1995. 24, 72

[Knuth et Bendix, 1970] KNUTH (D. E.) et BENDIX (P. B.), « Simple word problems in universal algebras », dans LEECH (J.), éditeur, *Computational Problems in Abstract Algebra*, p. 263–297. Pergamon Press, Oxford, 1970. 11, 13, 23, 41, 71

[Lankford, 1975] LANKFORD (D. S.), « Canonical inference ». Rapport technique, Louisiana Tech. University, 1975. 11, 41

[Lankford, 1977] LANKFORD (D. S.), « Some approaches to equality for computational logic : A survey and assessment ». Mémo n° ATP-36, Automatic Theorem Proving Project, University of Texas, Austin (Texas, USA), 1977. 48

[Le Chenadec, 1986] LE CHENADEC (P.), *Canonical Forms in Finitely Presented Algebras*. John Wiley & Sons, 1986. 11, 41

[Martí-Oliet et Meseguer, 1994] MARTÍ-OLIET (N.) et MESEGUER (J.), « General logics and logical frameworks », dans GABBAY (D.) et GUENTHNER (F.), éditeurs, *What is a Logical System ?* Oxford University Press, 1994. 37, 85

[Martin-Löf, 1984] MARTIN-LÖF (P.), *Intuitionistic Type Theory*, coll. « Studies in Proof Theory ». Bibliopolis, 1984. 11, 36, 41, 84

[Meseguer, 1989] MESEGUER (J.), « General logics », dans EBBINGHAUS (H.-D.) *et al.*, éditeurs, *Logic Colloquium'87*, p. 275–329. Elsevier Science Publishers B. V. (North-Holland), 1989. 37, 85

[Meseguer, 1992] MESEGUER (J.), « Conditional rewriting logic as a unified model of concurrency », *Theoretical Computer Science*, vol. 96, n° 1, 1992, p. 73–155. 13, 24, 30, 36, 37, 72, 77, 85

[Peterson et Stickel, 1981] PETERSON (G.) et STICKEL (M. E.), « Complete sets of reductions for some equational theories », *Journal of the ACM*, vol. 28, 1981, p. 233–264. 11, 41

[Robinson et Wos, 1969] ROBINSON (G. A.) et WOS (L. T.), « Paramodulation and first-order theorem proving », dans MELTZER (B.) et MITCHIE (D.), éditeurs, *Machine Intelligence 4*, p. 135–150. Edinburgh University Press, 1969. 11, 41

[Robinson, 1965] ROBINSON (J. A.), « A machine-oriented logic based on the resolution principle », *Journal of the ACM*, vol. 12, 1965, p. 23–41. 11, 37, 41, 85

[Rubio et Nieuwenhuis, 1995] RUBIO (A.) et NIEUWENHUIS (R.), « A total AC-compatible ordering based on RPO », *Theoretical Computer Science*, vol. 142, n° 2, 1995, p. 209–227. 28, 49, 50, 75

[Rusinowitch, 1987] RUSINOWITCH (M.), *Démonstration automatique par des techniques de réécriture*. Thèse de Doctorat d'Etat, Université Henri Poincaré – Nancy 1, 1987. Voir aussi [Rusinowitch, 1989]. 44, 47

[Rusinowitch, 1989] RUSINOWITCH (M.), *Démonstration automatique-Techniques de réécriture*. InterEditions, 1989. 93

[Scott, 1974] SCOTT (D.), « Completeness and axiomatizability in many-valued logic », dans HENKIN (L.) *et al.*, éditeurs, *Proceedings of the Tarski Symposium*, vol. XXV (coll. *Proceedings of Symposia in Pure Mathematics*), p. 71–116, American Mathematical Society, Berkeley, CA, 1974. 52

[Snyder, 1989] SNYDER (W.), « Efficient ground completion : An $O(n\log(n))$ algorithm for generating reduced sets of ground rewrite rules equivalent to a set of ground equations E », dans DERSHOWITZ (N.), éditeur, *Proceedings 3rd Conference on Rewriting Techniques and Applications, Chapel Hill (N.C., USA)*, vol. 355 (coll. *Lecture Notes in Computer Science*), p. 419–433. Springer-Verlag, avril 1989. 13, 64

[Wack, 2005] WACK (B.), *Typage et Déduction dans le Calcul de Réécriture*. Thèse de doctorat, Université Henri Poincaré – Nancy 1, 2005. 36, 84