Théorème de réduction des coupures

Victor ARRIAL

25 juin 2019

Table des matières

1 Introduction **2**
1.1 Présentation et remerciements . . . 2
1.2 Motivation . . . 2

2 Quelques outils **2**
2.1 Deux définitions importantes . . . 2
2.2 Un exemple : la logique propositionnelle . . . 3

3 La déduction naturelle et le calcul des séquents **4**
3.1 Point historique : la démonstration à la Hilbert . . . 4
3.2 Quelques propriétés importantes . . . 4
3.3 Démonstration par déduction naturelle (NJ) . . . 5
3.3.1 Idée et mise en place . . . 5
3.3.2 Une autre sémantique : les algèbres de Heyting . . . 6
3.3.3 Entre intuitionnistes et classiques . . . 7
3.3.4 Propriétés importantes et isomorphisme de Curry-Howard . . . 8
3.4 Démonstration par le calcul des séquents (SJ) . . . 8
3.4.1 Motivation . . . 8
3.4.2 Syntaxe . . . 9
3.4.3 Propriétés importantes et théorème de réduction des coupures . . . 10

4 Logique Linéaire (LJ) **10**
4.1 Motivations . . . 10
4.2 Connecteurs additifs et mutliplicatifs dans LL . . . 11
4.2.1 Plus ou moins de connecteurs . . . 11
4.2.2 Syntaxe . . . 11
4.3 LL en tant que calcul des séquents . . . 11
4.3.1 Syntaxe . . . 11
4.3.2 Conséquences et propriétés principales . . . 12

5 Réseaux de preuves **14**
5.1 Idée générale . . . 14
5.2 Structure de preuves . . . 14
5.3 Critère de correction dans MLL . . . 15
5.4 Réduction des coupures . . . 16
5.5 λ-calcul et réseaux de preuves . . . 16

Annexe A : Axiomes de la logique booléenne **17**

Annexe B : Syntaxe du calcul propositionnel intuitionniste **17**

Annexe C : Sémantique intuitionniste et algèbres de Heyting **17**

Annexe D : Duplication de preuve **18**

Annexe E : Réseaux de preuves **18**

1 Introduction

1.1 Présentation et remerciements

Ce mémoire a été réalisé sous la direction de Jules Chouquet et Léo Stéfanesco, doctorants au sein de l'équipe Preuves, Programmes et Système de l'IRIF, dans le cadre de la troisième année de licence du Cycle Pluridisciplinaire d'Études Supérieures (CPES). J'ai consulté de nombreux documents au cours de mes recherches, les plus importants sont certainement :
- Lectures on the Curry-Howard Isomorphism [So06]
- Proofs and Types [GTL89]
- From Proof-Nets to Interaction Nets [La94]

Je les remercie du temps qu'ils ont bien voulu m'accorder, et de leur grande disponibilité, et tout particulièrement pris le soin m'expliquer cette discipline nouvelle pour moi.

1.2 Motivation

Au long du stage, nous avons cherché à construire des *structures* et des *outils de représentation* des formes de raisonnement mathématique, pour ensuite les étudier et les caractériser afin de mieux les distinguer et de mieux les comprendre. Au cours de l'étude de ces structures, deux résultats importants sont apparus. Le premier résultat fut l'apparition d'un processus de réduction des preuves. Le second fut l'existence d'un parallèle entre certaines formes de programmation informatique et certaines formes de démonstration mathématique.

Motivés par ces résultats, nous avons peu à peu cherché à les améliorer, tant pour caractériser avec plus de finesse le fonctionnement de ces systèmes de démonstration que pour obtenir des propriétés nous garantissant l'implémentabilité informatique des processus d'écriture et de réduction des preuves. L'étude de la structure du langage mathématique mais aussi de la structure de langage du langage de la démonstration nous a amené à étudier différentes formes de système de démonstration.

J'ai choisi de ne pas présenter directement de démonstration des résultats figurant dans ce rapport. J'ai cependant, dans la mesure du possible, donné une idée générale de la démonstration à effectuer.

2 Quelques outils

La construction des structures dont nous avons fait mention dans l'introduction s'appuie sur deux concepts essentiels : la syntaxe et la sémantique. Prenons quelques instants pour les présenter et donner un premier exemple de leur mise en application.

2.1 Deux définitions importantes

Les concepts de syntaxe et de sémantique ont été emprunté à la linguistique et ont l'avantage de permettre des structures à la fois compatible avec un raisonnement mathématique et une interprétation linguistique. En voici une courte définition :

Définition : (Syntaxe)
Ensemble des règles de construction des expressions bien formées [1].

Définition : (Sémantique)
Ensemble des aspects du système logique relatifs aux notions de satisfaction et de vérité [2] des éléments syntaxiques.

On peut donc voir la syntaxe comme un ensemble de règles qui régissent la forme des objets. La sémantique correspond quant à elle au sens qu'on donne à ces objets.

1. Issue des dictionnaires du site CNRTL
2. Issue des dictionnaires du site CNRTL

Il est important de noter que suivant le contexte dans lequel on se place, les expressions biens formées peuvent-être —dans le contexte du langage mathématique— l'ensemble des formules ou —dans le contexte des méthodes de raisonnement— l'ensemble des règles déductives .

2.2 Un exemple : la logique propositionnelle

Pour illustrer ces définitions prenons l'exemple de la *logique propositionnelle*. On travaille alors sur le langage mathématique composé des formules construites sur un ensemble de variables –dites *variables propositionnelles*– et un jeu de connecteurs –unaires et binaires– composé de la conjonction ($\wedge$), la disjonction ($\vee$) et la négation ($\neg$). En posant l'implication ($A \to B$) comme représentant ($\neg A \vee B$) et la double implication ($A \leftrightarrow B$) comme représentant de $(A \to B) \wedge (B \to A)$, il devient alors équivalent d'écrire sur le jeu de connecteurs : $\{\wedge, \vee, \neg, \Rightarrow, \Leftrightarrow\}$.

On peut alors décrire la syntaxe de la logique propositionnelle ($\mathbb{F}$) à l'aide de la forme de Backus-Naur (BNF), prenons $\mathbb{V} = \{p_1, p_2, p_3, ...\}$ l'ensemble des variables propositionnelles, on a :

$$\mathbb{F} ::= \mathbb{V} \,|\, \neg\mathbb{F} \,|\, (\mathbb{F} \vee \mathbb{F}) \,|\, (\mathbb{F} \wedge \mathbb{F}) \,|\, (\mathbb{F} \to \mathbb{F}) \,|\, (\mathbb{F} \leftrightarrow \mathbb{F})$$ [3]

Par exemple, si $p, q \in \mathbb{V}$, alors $(\neg p \vee p), (p \to (q \to p)) \in \mathbb{F}$

Ces formules n'ont pas encore de sens, nous n'avons fait que décrire un ensemble admissible. On peut alors construire une sémantique sur $\mathbb{F}$ en utilisant un anneau de Boole $(\mathbb{B}, +, \cdot, 0, 1)$. Dans un premier temps, on associe à chaque variable propositionnelle une valeur de l'anneau à l'aide d'une première valuation v . Puis on l'étend à $\mathbb{F}$ –l'extension est notée $[\![\cdot]\!]_v$– à l'aide d'un ensemble de relations faisant le lien entre connecteurs et sémantique. On pose généralement :

$$\begin{array}{ll} & \forall\, p \in \mathbb{V},\ [\![p]\!]_v = v(p) \\ \text{si } F = \neg G, & \text{alors } [\![F]\!]_v = 1 \text{ ssi } [\![G]\!]_v = 0 \\ \text{si } F = G \wedge H, & \text{alors } [\![F]\!]_v = 1 \text{ ssi } [\![G]\!]_v = 1 \text{ et } [\![H]\!]_v = 1 \\ \text{si } F = G \vee H, & \text{alors } [\![F]\!]_v = 1 \text{ ssi } [\![G]\!]_v = 1 \text{ ou } [\![H]\!]_v = 1 \\ \text{si } F = G \to H, & \text{alors } [\![F]\!]_v = 1 \text{ ssi } [\![H]\!]_v = 1 \text{ ou } [\![G]\!]_v = 0 \\ \text{si } F = G \leftrightarrow H, & \text{alors } [\![F]\!]_v = 1 \text{ ssi } [\![G]\!]_v = [\![H]\!]_v \end{array}$$

Lorsque l'on observe $[\![F]\!]_v = 1$, on note $v \vDash F$ et on dit que la valuation v *satisfait* la formule F. Ainsi, on définit l'ensemble des *tautologies* de la logique propositionnelle (relativement à cette forme de sémantique) comme l'ensemble des formules qui sont vérifiées pour toutes les valuations, on note alors $\vDash F$. Lorsque toutes les valuations satisfaisant un ensemble de formules Γ satisfont aussi une formule F, on dit que F est une *conséquence* de Γ et on note $\Gamma \vDash F$.

Regardons par exemple les tables de valuations des formules $(\neg p \vee p)$ et $(p \to (q \to p))$ pour montrer qu'il s'agit de tautologie pour cette forme de sémantique :

	p	$\neg p$	$\neg p \vee p$
v_0	1	0	1
v_1	0	1	1

	p	q	$(q \to p)$	$(p \to (q \to p))$
v_0	1	1	1	1
v_1	1	0	1	1
v_2	0	1	0	1
v_3	0	0	1	1

On a généralement besoin de moins de connecteurs. On peut par exemple montrer que $\{\neg, \vee\}$ forme un système complet de connecteurs qui nous garantit la même capacité d'expression. Il est aussi possible de construire une forme dite normale qui permet de simplifier le travail d'évaluation syntaxique. Nous ne traitons donc dans ce rapport qu'une partie minimale de l'étude de la syntaxe et de la sémantique de la logique propositionnelle.

3. On peut aussi construire $\neg A$ comme $A \to \bot$, où $\bot$ est la formule fausse

3 La déduction naturelle et le calcul des séquents

Maintenant que nous avons la syntaxe et la sémantique d'un langage mathématique, construisons une seconde structure linguistique qui permettra de faire des liens entre les formules.

3.1 Point historique : la démonstration à la Hilbert

Au début du XX^{eme} siècle, Hilbert propose un des premiers systèmes de preuve (aussi appelé *calcul*) construit sur la logique propositionnelle. Il s'agit d'ajouter un fonctionnement déductif qui fasse un lien entre ces formules. Pour cela, il utilise deux éléments en particulier :

Il choisit un mode de raisonnement, en l'occurence le principe du *modus ponens* aussi appelé détachement. Ce mode de raisonnement simple se présente sous la forme suivante :

« De A et $A \to B$ on déduit B. »

Il choisit aussi un ensemble de propositions qu'il considère comme vrai, la base axiomatique, et s'appuie ainsi sur les travaux de son prédécesseur Frege.

La démonstration consiste alors à alterner régulièrement l'utilisation d'axiomes, d'hypothèses et de la règle de déduction (modus ponens). La dernière proposition de cette suite de formules est celle à démontrer et le fonctionnement est ainsi séquentiel. Si à partir d'un ensemble d'hypothèses Γ on arrive à construire une démonstration d'une formule A, alors on note $\Gamma \vdash A$. On peut même utiliser la notation $\vdash_H$ pour rappeler qu'il s'agit d'une démonstration dite à la Hilbert.

Les axiomes peuvent-être utilisés directement dans leur forme première, ou sous la forme d'une instance. On dit qu'une formule F est une instance d'une formule G si F s'obtient en substituant certaines variables propositionnelles de G par des formules F_i. Par exemple, la formule $((R \to R) \to Q)$ est une instance de la formule $(P \to Q)$.

Voici quelques-uns des axiomes de la démonstration à la Hilbert [4] :

$(P \to (Q \to P))$	(Axiome 1 pour l'implication)
$((P \to (Q \to R)) \to ((P \to Q) \to (P \to R)))$	(Axiome 2 pour l'implication)
$((P \wedge Q) \to P)$	(Axiome 2 pour la conjonction)
$(P \to (P \vee Q))$	(Axiome 1 pour la disjonction)

Nous venons de décrire un premier système de démonstration, plus précisément, sa syntaxe, c'est à dire l'ensemble des démonstrations qu'on s'autorise à écrire. Nous n'avons cependant pas parlé de sa sémantique, et nous n'en parlerons pas.

3.2 Quelques propriétés importantes

Nous cherchons certaines propriétés dans ces systèmes de démonstration. En particulier, la démonstration à la Hilbert vérifie déjà celle de correction et de complétude.

Définition : (Correction)
On dit qu'un système de démonstration est *correct* si pour tout ensemble de formules Γ et pour toute formule A, lorsque $\Gamma \vdash A$ est prouvable, alors on a $\Gamma \vDash A$, autrement dit, A est une conséquence de Γ. On peut écrire cela plus formellement :

$$(\Gamma \vdash A) \Rightarrow (\Gamma \vDash A)$$

Définition : (Complétude)
On dit qu'un système logique est *complet* si, pour tout ensemble de formules Γ et pour toute conséquence A de cet ensemble de formules, il existe une preuve de A avec pour hypothèses Γ ($\Gamma \vdash A$). On peut écrire cela plus formellement :

$$(\Gamma \vDash A) \Rightarrow (\Gamma \vdash A)$$

4. La liste complète des axiomes dans l'annexe A

Ces propriétés permettent de faire le lien entre la sémantique des formules et la syntaxe du système de démonstration. Plus précisément, elles font le lien entre le fait qu'une formule soit vraie –relativement à la sémantique– et le fait qu'elle soit prouvable –relativement au système de démonstration. La propriété de correction peut alors s'interpréter comme l'assurance que toute formule prouvable est vraie, et la propriété de complétude comme l'assurance que toute formule vraie est prouvable.

Ce lien fort permet par exemple d'assurer la calculabilité du problème de l'existence d'une démonstration dans le cas de la démonstration à la Hilbert. En effet, le problème de la véracité d'une formule est trivialement calculable. Or, la conjonction des propriétés de correction et de complétude permet de rendre équivalent véracité et prouvabilité d'une formule, et assure ainsi la calculabilité de la prouvabilité [5]. Cela n'assure par contre pas la calculabilité de la démonstration puisque qu'il ne s'agit pas d'une bijection entre démonstration et véracité.

3.3 Démonstration par déduction naturelle (NJ)

La déduction naturelle est un système formel développé par Gentzen[Ge69][Pr65] pour rendre plus intuitif le système de démonstration de Hilbert, tout en essayant de garder les propriétés essentielles que nous venons d'exhiber.

3.3.1 Idée et mise en place

L'un des problèmes importants de la démonstration à la Hilbert est qu'à chaque étape il est difficile de déterminer ce qu'il faut faire. De plus, la démonstration à la Hilbert est très sensible au choix initial des axiomes. Pour finir, le travail sous hypothèses n'est pas particulièrement pratique : celles-ci doivent-être choisies au début de la démonstration et ne pourront pas facilement être modifiées.

L'observation de Gentzen est la suivante. L'ensemble des formules est décrit à l'aide d'un ensemble de connecteurs. On devrait donc avoir une règle pour pouvoir facilement introduire un connecteur dans la démonstration d'une formule. L'hypothèse de l'utilisation des règles a deux conséquences sur la syntaxe :

La première vient de l'asymétrie du nombre de propositions qui sont mises en relation dans l'utilisation d'une règle. A chaque étape de démonstration, on utilise un certain nombre d'hypothèses pour obtenir une seule conclusion. Une règle est donc la donnée d'une paire formée par une liste d'hypothèses et par une conclusion et doit donc s'écrire comme telle.

La seconde est la nécessaire symétrie des règles. En effet, pour réaliser l'ensemble des démonstrations, on s'imagine devoir utiliser les règles qui introduisent les connecteurs dans les formules, mais aussi utiliser d'autres règles pour les supprimer. Ainsi, pour chaque connecteur, on doit disposer d'une *règle d'introduction* –notée I– mais aussi d'une *règle d'élimination* –notée E.

On construit alors une représentation formelle des règles : on place une barre horizontale pour séparer les hypothèses de la conclusion. La règle du modus ponens [6] correspond alors à la règle d'élimination de la flèche. On peut alors l'écrire, avec la règle d'introduction associée comme suit :

$$\frac{\text{hypothèses}}{\text{conclusion}}\ (\text{règle}) \qquad \frac{\Gamma \vdash \varphi \qquad \Gamma \vdash \varphi \to \psi}{\Gamma \vdash \psi}\ (\to_E) \qquad \frac{\Gamma, \varphi \vdash \psi}{\Gamma \vdash \varphi \to \psi}\ (\to_I)$$

Une démonstration correspond à un enchainement de ces règles ce qui dessine un arbre. On trouve donc à la racine la proposition qu'on devait démontrer et les hypothèses se retrouvent sur les feuilles de l'arbre.

Donnons par exemple la démonstration de $(\varphi \to (\psi \to \vartheta)) \vdash ((\varphi \to \psi) \to (\varphi \to \vartheta))$. Pour simplifier les notations, posons $\Gamma := \{(\varphi \to (\psi \to \vartheta)), (\varphi \to \psi), \varphi\}$.

5. La démonstration n'est par contre pas constructive
6. L'ensemble des règles sont dans l'annexe B

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{}{\Gamma \vdash \varphi \to (\psi \to \vartheta)}\,(\text{ax}) \quad \dfrac{}{\Gamma \vdash \varphi}\,(\text{ax})}{\Gamma \vdash \psi \to \vartheta}\,(\to_E) \quad \dfrac{\dfrac{}{\Gamma \vdash \varphi \to \psi}\,(\text{ax}) \quad \dfrac{}{\Gamma \vdash \varphi}\,(\text{ax})}{\Gamma \vdash \psi}\,(\to_E)}{\Gamma \vdash \vartheta}\,(\to_E)}{(\varphi \to (\psi \to \vartheta)), (\varphi \to \psi) \vdash (\varphi \to \vartheta)}\,(\to_I)}{(\varphi \to (\psi \to \vartheta)) \vdash ((\varphi \to \psi) \to (\varphi \to \vartheta))}\,(\to_I)$$

On se rend alors compte que la règle d'introduction de la flèche correspond au déchargement d'une hypothèse dans notre raisonnement ce qui signifie qu'une formule passe de la place des hypothèses à la place de la conclusion.

3.3.2 Une autre sémantique : les algèbres de Heyting

Regardons un autre style de sémantique, un peu plus complexe, qui donne donc plus d'informations sur les formules et qui permet par ailleurs de garantir les propriétés de complétude et de correction. La sémantique que nous avions présenté pour la logique propositionnelle appartenait à la famille des sémantiques algébriques qui s'appuie sur la notion d'algèbres de Boole. La sémantique que nous allons maintenant présenter appartient à la famille des algèbres de Heyting. Posons les premières définitions pour ensuite pouvoir la construire :

La sémantique se fait à l'aide d'un ensemble H sur lequel nous allons interpréter nos formules.

Définition : ($\sim$ et $\leqslant$)
Soit $\Gamma \subset \mathbb{F}$ un contexte, posons $\sim$ une relation d'équivalence sur $\mathbb{F}$ définie par :

$$\forall\, \varphi, \psi \in \mathbb{F},\ \ \varphi \sim \psi \ \ \Leftrightarrow\ \ (\Gamma \vdash \varphi \to \psi \ \text{ et } \ \Gamma \vdash \psi \to \varphi)$$

Définissons sur $\mathbb{F}/_\sim$ un ordre partiel[7] $\leqslant$ tel que :

$$\forall\, \varphi, \psi \in \mathbb{F},\ \ [\varphi]_\sim \leqslant [\psi]_\sim \ \ \Leftrightarrow\ \ \Gamma \vdash \varphi \to \psi$$

On peut construire les opérations suivantes :

$$\begin{array}{rcl} [\neg\varphi]_\sim & = & -[\varphi]_\sim \\ [\varphi \vee \psi]_\sim & = & [\varphi]_\sim \cup [\psi]_\sim \\ [\varphi \wedge \psi]_\sim & = & [\varphi]_\sim \cap [\psi]_\sim \end{array}$$

Dont la cohérence avec les classes d'équivalence est justifiée par la prouvabilité des formules :

$$\begin{array}{c} \vdash (\varphi \to \varphi') \to (\neg\varphi' \to \neg\varphi) \\ \vdash (\varphi \to \varphi') \to ((\psi \to \psi') \to ((\varphi \vee \psi) \to (\varphi' \vee \psi'))) \\ \vdash (\varphi \to \varphi') \to ((\psi \to \psi') \to ((\varphi \wedge \psi) \to (\varphi' \wedge \psi'))) \end{array}$$

On peut aussi constater d'autres propriétés importantes de cette structure. En notant $\top = \bot \to \bot$, on a que $[\bot]_\sim$ est le plus petit élément, et $[\top]_\sim$ le plus grand, pour l'ordre $\leqslant$ dans $\mathbb{F}/_\sim$. On a aussi $[\top]_\sim = \{\varphi \mid \Gamma \vdash \varphi\}$[8]. Démontrons rapidement ces propriétés :

$$\dfrac{\dfrac{\dfrac{}{\Gamma, \varphi, \bot \vdash \bot}\,(ax)}{\Gamma, \varphi \vdash \bot \to \bot}\,(\to_I)}{\Gamma \vdash \varphi \to (\bot \to \bot)}\,(\to_I) \qquad \dfrac{\dfrac{\dfrac{}{\Gamma, \bot \vdash \bot}\,(ax)}{\Gamma, \bot \vdash \varphi}\,(\bot_E)}{\Gamma \vdash \bot \to \varphi}\,(\to_I)$$

Et pour finir, on observe aussi que $\cap$ et $\cup$ sont distributifs l'un sur l'autre, $[\bot]_\sim$ est le neutre de $\cup$, $[\top]_\sim$ est le neutre de $\cap$.

Définition : (Pseudo-complement relatif)
Soit $A, B \in H$. On nomme *pseudo-complément* de A relativement à B le plus grand élément $C \in H$ tel que $A \cap C \leqslant B$, et on le note $A \Rightarrow B$.

Dans ces conditions, on se retrouve avec une structure d'algèbre de Heyting[9] pour $\mathcal{H} = \langle H, \cup, \cap, 0, 1, \Rightarrow \rangle$ ce qui va constituer notre sémantique. Nous pouvons construire une valuation qui représente l'interprétation des formules :

7. Cet ordre est bien transitif grâce à la prouvabilité de $(\varphi \to \psi) \to ((\psi \to \vartheta) \to (\varphi \to \vartheta))$
8. Démonstration dans l'annexe C
9. La définition exacte est donné dans l'annexe C

Définition : (Sémantique intuitionniste par une algèbre de Heyting)
Soit $\mathcal{H} = \langle H, \cup, \cap, \Rightarrow, -, 0, 1\rangle$ une algèbre de Heyting. Une sémantique construite sur cette algèbre permet d'interpréter les formules à l'aide d'une valuation initiale $v : \mathbb{V} \mapsto H$, qu'on étend sur $\mathbb{F}$ à l'aide des relations :

$$\begin{array}{rcll} [\![\varphi]\!]_v & := & v(\varphi) & \text{si } \varphi \in \mathbb{V} \\ [\![\bot]\!]_v & := & 0 & \\ [\![\varphi \vee \psi]\!]_v & := & [\![\varphi]\!]_v \cup [\![\psi]\!]_v & \\ [\![\varphi \wedge \psi]\!]_v & := & [\![\varphi]\!]_v \cap [\![\psi]\!]_v & \\ [\![\varphi \to \psi]\!]_v & := & [\![\varphi]\!]_v \Rightarrow [\![\psi]\!]_v & \end{array}$$

Notons que toutes nos relations ont été construites relativement à un contexte Γ. L'interprétation sémantique est donc elle aussi relative à ce contexte Γ. Le cas de sémantique qui nous intéresse particulièrement est en fait celui du le contexte vide $\Gamma = \emptyset$ pour pouvoir interpréter nos formules sans hypothèse. L'identification des formules équivalentes –par démonstration– sous un contexte par la relation d'équivalence nous permet de les interpréter de la même façon. Les espaces topologiques permettent de mettre en place facilement ce genre de sémantique.

3.3.3 Entre intuitionnistes et classiques

Cette seconde sémantique est plus complexe mais elle nous permet d'avoir un plus large spectre d'interprétation des formules. En effet, la première donnait une première approche de la notion de vérité qui était rapidement limitée par la faible taille de l'espace $\mathbb{B}$. L'espace H de la seconde, de plus grande taille, nous permet ainsi de donner plus de nuances dans l'interprétation des formules. Les propositions y sont vues comme des sous-ensembles de l'espace, et ainsi, la conjonction (resp. disjonction) de propositions correspond sémantiquement à l'union (resp. l'intersection) des espaces associés.

Nous pouvons observer une seconde différence importante entre ces deux sémantiques. La première sémantique, sur $\mathbb{B}$ et notée ici $[\![\cdot]\!]_v^{(1)}$, vérifie les propriétés :

$$\begin{array}{rcll} \forall\, F \in \mathbb{F},\ [\![\neg F \wedge F]\!]_v^{(1)} & = & 0 & \text{(Principe de non-contradiction)} \\ \forall\, F \in \mathbb{F},\ [\![\neg F \vee F]\!]_v^{(1)} & = & 1 & \text{(Principe du tiers exclu)} \end{array}$$

Tandis qu'avec la seconde sémantique, sur H et notée $[\![\cdot]\!]_v^{(2)}$, on a :

$$\begin{array}{rcl} \forall\, F \in \mathbb{F},\ [\![\neg F \wedge F]\!]_v^{(2)} & = & 0 \\ \exists\, F \in \mathbb{F},\ [\![\neg F \vee F]\!]_v^{(2)} & \neq & 1 \end{array}$$

Démontrons les résultats pour la seconde sémantique. On a, par le fait que $\bot$ soit le plus petit élément, $[\bot]_v \leqslant [\neg F \wedge F]_v$. Montrons maintenant $[\neg F \wedge F]_v \leqslant [\bot]_v$ ce qui nous permettra de conclure. On a :

$$\dfrac{\dfrac{\dfrac{\dfrac{}{\Gamma, (\neg F \wedge F) \vdash \neg F \wedge F}\,(ax)}{\Gamma, (\neg F \wedge F) \vdash F}\,(\wedge_E) \quad \dfrac{\dfrac{}{\Gamma, (\neg F \wedge F) \vdash (\neg F \wedge F)}\,(ax)}{\Gamma, (\neg F \wedge F) \vdash \neg F}\,(\wedge_E)}{\Gamma, (\neg F \wedge F) \vdash \bot}\,(\to_E)}{\Gamma \vdash (\neg F \wedge F) \to \bot}\,(\to_I)$$

Etant donné qu'on a $[\![\bot]\!]_v = 0$, on obtient bien l'équation souhaitée : $[\![\neg F \wedge F]\!]_v^{(2)} = 0$ [10].

Nous ne travaillons donc plus dans un système qui accepte le principe du tiers-exclu. Les formules considérées comme des tautologies ne sont plus les même que celles de la première sémantique. En particulier, nous dirons que les sémantiques construites à l'aide d'algèbres de Heyting sont des *sémantiques intuitionnistes* alors que celles construites à l'aide d'algèbre de Boole sont des *sémantiques classiques*. Une caractéristique des systèmes de démonstration intuitionnistes est de refuser les démonstrations qui ne construisent pas le résultat.

10. On montre que le tiers exclu n'est pas vérifié avec un exemple dans l'annexe C

3.3.4 Propriétés importantes et isomorphisme de Curry-Howard

En utilisant la sémantique intuitionniste construite à l'aide d'une algèbre de Heyting, on montre que la déduction naturelle vérifie les propriétés de complétude et de correction. La preuve s'effectue par induction sur l'ensemble des règles de construction des preuves par déduction naturelle.

Ce nouveau système de démonstration, en plus de vérifier ces propriétés, permet de réaliser plus facilement les démonstrations. Cependant, nous nous rendons rapidement compte, qu'il est possible de construire plusieurs preuves de la même formule, certaines plus longues que d'autres. En particulier, reprenons notre exemple de preuve par déduction naturelle :

Notons A_P l'arbre de preuve suivant :

$$\dfrac{\dfrac{\dfrac{}{\Gamma, \varphi \vdash \varphi \to (\psi \to \vartheta)}\,(\text{ax}) \quad \dfrac{}{\Gamma, \varphi \vdash \varphi}\,(\text{ax})}{\Gamma, \varphi \vdash \psi \to \vartheta}\,(\to_E) \quad \dfrac{\dfrac{}{\Gamma, \varphi \vdash \varphi \to \psi}\,(\text{ax}) \quad \dfrac{}{\Gamma, \varphi \vdash \varphi}\,(\text{ax})}{\Gamma, \varphi \vdash \psi}\,(\to_E)}{\Gamma, \varphi \vdash \vartheta}\,(\to_E)$$

Cela nous permet de construire une autre preuve de $(\varphi \to (\psi \to \vartheta)) \vdash ((\varphi \to \psi) \to (\varphi \to \vartheta))$:

$$\dfrac{\dfrac{A_P}{\Gamma, \varphi \vdash \vartheta} \quad \dfrac{\dfrac{\dfrac{}{\Gamma, \psi \vdash \varphi}\,(ax) \quad \dfrac{}{\Gamma, \psi \vdash \varphi \to (\psi \to \vartheta)}\,(ax)}{\Gamma, \psi \vdash \psi \to \vartheta}\,(\to_E) \quad \dfrac{}{\Gamma, \psi \vdash \psi}\,(ax)}{\Gamma, \psi \vdash \vartheta}\,(\to_E) \quad \dfrac{\dfrac{}{\Gamma \vdash \varphi}\,(ax)}{\Gamma \vdash \varphi \vee \psi}\,(\vee_I)_{(*)}}{\Gamma \vdash \vartheta}\,(\vee_E)_{(*)}$$

$$\vdots$$

La seconde preuve est beaucoup plus longue que la première et certaines étapes ne semblent pas nécessaires. La dernière ligne consiste en l'élimination de la disjonction introduite à la ligne précédente $(*)$. Nous pourrions donc facilement, à partir de cette preuve, construire une autre de taille inférieure. Ce qui donnerait par exemple :

$$\dfrac{\dfrac{\dfrac{A_P}{\Gamma \vdash \varphi \to \vartheta}\,(\to_I) \quad \dfrac{}{\Gamma \vdash \varphi}\,(ax)}{\Gamma \vdash \vartheta}\,(\to_E)}{\vdots}$$

Etant donné la forme de l'arbre de preuves A_P, on pourrait continuer à itérer ce processus, cette fois sur l'introduction de la flèche. Ce processus de réduction semble nous permettre de déduire des preuves de petites tailles.

Un autre élément remarquable de ce système de démonstration est la ressemblance entre les règles de construction des démonstrations et les règles de construction des termes du lambda-calcul simplement typé à la Church. En l'occurence, en apportant une extension à ce dernier, on peut construire un isomorphisme avec la déduction naturelle. Cette isomorphisme mis en lumière par Curry[Cu58] en 1959 et par Howard[Ho80] en 1969 nous permet de faire un lien entre une preuve mathématique et un programme informatique. En particulier, nous pouvons remarquer que le processus de réduction que nous venons de mettre en lumière s'identifie à la β-réduction du λ-calcul, son système d'évaluation des fonctions. Réduire une preuve s'apparente donc à effectuer un calcul.

Bien que plus intuitif, ce système de démonstration demande toujours d'avoir de l'intuition pour arriver à réaliser une démonstrations. Rien ne nous permet de borner le domaine de recherche des formules intermédiaires. Il est donc difficile d'imaginer pouvoir réaliser une implémentation informatique de la recherche d'une preuve d'une formule.

3.4 Démonstration par le calcul des séquents (SJ)

3.4.1 Motivation

La force de la déduction naturelle vient des conjectures sur sa syntaxe. La difficulté à surmonter était alors un changement de sémantique, qui nous a finalement apporté un résultat supplémentaire : la correspondance preuve-programme. Essayons d'améliorer ces conjectures pour construire

un système de démonstration qui garde les mêmes propriétés et où la réalisation de la démonstration d'une formule se rapprocherait d'un problème décidable. C'est ce qu'à fait Gentzen[Ge69] en construisant le calcul des séquents.

On peut remettre en question la restriction de l'unique conclusion des règles. De plus, la possibilité d'introduire des connecteurs dans les hypothèses nous permettrait aussi de réaliser plus simplement les démonstrations. Avant d'essayer de regarder les conséquences que cela peut avoir dans le calcul, nous devons adapter nos notations. Pour cela, nous utilisons un nouvel objet : le séquent.

3.4.2 Syntaxe

Le séquent est une paire de listes finies de formules séparée par un *taquet* ($\vdash$) que l'on note alors $A_1, \ldots, A_n \vdash B_1, \ldots, B_m$. La partie à gauche correspond comme avant aux hypothèses, la partie droite, aux conclusions. Appuyons-nous sur les règles de la déduction naturelle pour essayer de déduire une première interprétation de cette notation. Quatre d'entre-elles permettent de compléter la conclusion :

$$\frac{\Gamma \vdash \varphi}{\Gamma \vdash \varphi \vee \psi}\ (\vee_I) \qquad \frac{\Gamma, \varphi \vdash \psi}{\Gamma \vdash \varphi \to \psi}\ (\to_I)$$

$$\frac{\Gamma \vdash \psi}{\Gamma \vdash \varphi \vee \psi}\ (\vee_I) \qquad \frac{\Gamma \vdash \varphi \qquad \Gamma \vdash \psi}{\Gamma \vdash \varphi \wedge \psi}\ (\wedge_I)$$

A l'exception de l'introduction de la conjonction dont le fonctionnement est particulier –elle assemble deux preuves– toutes les autres semblent lier les deux propositions par une disjonction. Ainsi, on s'appuie sur le fait que si une des formules d'une disjonction est une conséquence alors cette disjonction est une conséquence, il semble cohérent d'interpréter le séquent comme suit :

$$A_1 \wedge \ldots \wedge A_n \vdash B_1 \vee \ldots \vee B_m \qquad \text{ou encore} \qquad \vdash (A_1 \wedge \ldots \wedge A_n) \to B_1 \vee \ldots \vee B_m$$

Ou encore : la conjonction des hypothèses donne au moins une des conclusions.

Regardons maintenant plus en détail les règles syntaxiques. De part la symétrie qu'on a créé entre les deux cotés du taquet, on se limite aux règles d'introduction. On obtient alors le jeu de règles suivant [11] :

$$\frac{\Gamma, \varphi \vdash \vartheta}{\Gamma, \varphi \wedge \psi \vdash \vartheta}\ (\wedge_L) \qquad \frac{\Gamma, \psi \vdash \vartheta}{\Gamma, \varphi \wedge \psi \vdash \vartheta}\ (\wedge_L) \qquad \frac{\Gamma \vdash \varphi \qquad \Gamma \vdash \psi}{\Gamma \vdash \varphi \wedge \psi}\ (\wedge_R)$$

$$\frac{\Gamma, \varphi \vdash \vartheta \qquad \Gamma, \psi \vdash \vartheta}{\Gamma, \varphi \vee \psi \vdash \vartheta}\ (\vee_L) \qquad \frac{\Gamma \vdash \varphi}{\Gamma \vdash \varphi \vee \psi}\ (\vee_R) \qquad \frac{\Gamma \vdash \psi}{\Gamma \vdash \varphi \vee \psi}\ (\vee_R)$$

$$\frac{\Gamma \vdash \varphi, \vartheta \qquad \Gamma, \psi \vdash \vartheta}{\Gamma, \varphi \to \psi \vdash \vartheta}\ (\to_L) \qquad \frac{\Gamma, \varphi \vdash \psi}{\Gamma \vdash \varphi \to \psi}\ (\to_R) \qquad \frac{}{\Gamma, A \vdash A}\ (ax)$$

$$\frac{\Gamma \vdash \vartheta}{\Gamma, \varphi \vdash \vartheta}\ (w_L) \qquad \frac{\Gamma \vdash}{\Gamma \vdash \vartheta}\ (w_R)$$

$$\frac{\Gamma, \varphi, \varphi \vdash \vartheta}{\Gamma, \varphi \vdash \vartheta}\ (c) \qquad \frac{\Gamma \vdash \varphi \qquad \Sigma, \varphi \vdash \vartheta}{\Gamma, \Sigma \vdash \vartheta}\ (Cut)$$

Il est alors possible de réécrire la déduction naturelle (N) par le calcul des séquents intuitionniste (SJ). Les règles d'introduction de N correspondent aux règles d'introduction à droite de SJ et les règles d'élimination de N se réécrive à l'aide de la composition des règles d'introduction à gauche, de l'axiome et de la coupure de SJ. La limitation aux règles d'introduction ne restreint

11. J'ai fait le choix de ne présenter que le calcul des séquents intuitionniste, ce qui gomme un peu l'impact de l'hypothèse de Gentzen puisqu'on limite le nombre de formules à droite du taquet à un. La syntaxe classique est donnée dans l'annexe ...

donc pas la capacité d'expression du système.

Il nous faut maintenant différencier la notion de prouvabilité suivant les différents modes de démonstration. On note $\vdash_N$ pour la déduction naturelle et $\vdash^+_{SJ}$ pour le calcul des séquents intuitionniste. Le $+$ désigne l'utilisation du séquent de coupure. Ainsi, écrire $\Gamma \vdash_{SJ} \varphi$ désigne une preuve de $\Gamma \vdash \varphi$ dans le calcul des séquents intuitionniste et sans l'utilisation de la coupure.

3.4.3 Propriétés importantes et théorème de réduction des coupures

Le lien entre N et SJ est en fait plus fort qu'une simple réécriture du premier dans le deuxième. On a le théorème :

Théorème :
$\forall\, \Gamma \subset \mathbb{F},\ \ \forall\, \varphi \in \Gamma,\ \ \Gamma \vdash^+_{SJ} \varphi \ \ \Leftrightarrow \ \ \Gamma \vdash_N \varphi$

On prouve sans trop de difficulté le théorème par récurrence sur la longueur de la preuve et en disjonction de cas sur l'ensemble des règles de construction des preuves, dans les deux sens de l'équivalence.

Une autre force du calcul des séquents est de simplifier la tâche de l'étude du processus d'élimination des coupures. Grâce à la syntaxe du calcul des séquents, on peut plus facilement exhiber les différents cas classiques de réduction des coupures et montrer qu'ils permettent de recouvrir l'ensemble des cas. Ensuite, en posant un ordre sur les preuves, on montre que dans chaque cas de réduction, soit la taille de la preuve diminue, soit la coupure remonte dans la preuve. Cela nous permet alors d'obtenir le théorème suivant :

Théorème : (Elimination des coupures)
$\forall\, \Gamma \subset \mathbb{F},\ \ \forall\, \varphi \in \mathbb{F},\ \ \Gamma \vdash^+_{SJ} \varphi \ \ \Leftrightarrow \ \ \Gamma \vdash_{SJ} \varphi$

Pour finir une troisième propriété importante se déduit du théorème d'élimination des coupures, et c'est celui-ci qui nous apporte un résultat satisfaisant pour le problème de la rédaction de preuves. Ce théorème permet de borner l'espace de recherche des formules utilisées dans une preuve :

Théorème : (Sous-formule)
Chaque formule qui apparait dans une preuve de $\Gamma \vdash_{SJ} \varphi$ est, soit une sous-formule de Γ, soit une sous-formule de φ

Il se prouve par récurrence sur la longueur de la preuve sans coupure et par disjonction de cas sur la forme de la règle utilisée.

En plus de donner le caractère calculable au problème de la construction de démonstration en calcul des séquents intuitionniste, ce résultat nous permet aussi d'affirmer la stabilité de ses fragments. En effet, les sous-formules préservent les fragments de logique et donc le théorème de la sous-formule nous permet d'étendre cette propriété à la preuve elle-même.

4 Logique Linéaire (LJ)

Les résultats que sont l'isomorphisme de Curry-Howard et le théorème des coupures que nous venons de mettre en lumière dans le calcul des séquents et la déduction naturelle nous permettent de considérer les preuves en tant que termes d'un calcul que l'on cherche à réaliser. On va considérer une nouvelle logique, plus abstraite, pour essayer d'exprimer et de réaliser plus précisément ce calcul et ainsi de mieux rendre compte du fonctionnement des systèmes de démonstration jusque là étudiés. Elle va aussi permettre de capturer les phénomènes de passage par valeur et passage par référence dans les langages de programmation comme le λ-calcul simplement typé.

4.1 Motivations

La réduction des coupures telle qu'elle a été présentée possède un défaut : lors de la réduction de certaines preuves, on se retrouve parfois à en dupliquer d'autres [12]. Nous allons essayer de mieux comprendre ce phénomène et chercher à l'éliminer.

12. Exemple dans l'annexe D

Grâce à la correspondance de Curry-Howard, nous pouvons considérer les preuves comme des termes du λ-calcul simplement typé. En particulier, l'introduction de la flèche s'interprète comme l'abstraction et le processus de réduction des coupures s'interprète comme la β-réduction, la méthode d'évaluation des fonctions de ce langage de programmation théorique. Ainsi, en cherchant à mieux comprendre l'introduction de la flèche –qui semble être un point important dans la duplication des preuves–, nous étudions par isomorphisme les abstractions du λ-calcul et l'utilisation de leurs arguments. En particulier, la duplication d'un terme non encore réduit –qui est isomorphe à la duplication d'une preuve non réduite– multiplie le nombre de calcul à effectuer.

Nous allons donc essayer de décomposer l'implication en éléments plus simples, à la recherche d'une implication élémentaire qui présenterait des propriétés de linéarité, linéarité que l'on retrouve dans les autres cas de réduction. La logique linéaire à été introduire par J-Y. Girard en 1986[Gir87]

4.2 Connecteurs additifs et mutliplicatifs dans LL

4.2.1 Plus ou moins de connecteurs

En observant l'exemple de duplication de preuve [12], on se rend compte que la raison de la duplication est l'identification des contextes lors de l'introduction du connecteur conjonctif ($\wedge$). Ainsi, lorsque l'on fait remonter la coupure, elle s'effectue sur les deux preuves dont les contextes ont été identifiés, ce qui est à l'origine de la duplication de la preuve coupante. Afin de marquer la différence entre les situations qui présentent cette identification et les autres, il nous faut donc introduire de nouveaux connecteurs. Il y a donc deux jeux de connecteurs : les connecteurs *multiplicatifs* –notés $\otimes$ et $\parr$– qui conservent les contextes, et les connecteurs *additifs* –notés $\oplus$ et &– qui les identifient.

Pour garder le même pouvoir d'expression que dans les situations précédentes, on se donne un connecteur qui différencie les formules duplicables –potentiellement un nombre infini de fois comme dans l'utilisation de l'affaiblissement– de celles qui sont uniques.

4.2.2 Syntaxe

Dans les connecteurs multiplicatifs, le *tenseur* ($\otimes$) correspond au connecteur de conjonction et le *par* ($\parr$) au connecteur de disjonction. Dans les connecteurs additif, le *avec* (&) correspond au connecteur conjonctif et le *plus* ($\oplus$) au connecteur disjonctif. On note la négation $^\perp$.

En accord avec ce qu'on vient de dire, on construit l'implication élémentaire à partir des connecteurs multiplicatifs pour obtenir la propriété de linéarité :

$$A \multimap B := A^\perp \parr B$$

Pour finir, il nous faut les connecteurs qui garantissent le même niveau d'expression. Nous utilisons un connecteur unaire appelé *bien sûr* noté à l'aide du point d'exclamation ! pour dénoter les preuves duplicables. Il est conjugué au connecteur unaire nommé *pourquoi pas* et noté à l'aide d'un point d'interrogation ?.

Nous n'écrivons donc plus sur même ensemble de formules.
Nous travaillons maintenant sur : (noté $\mathbb{F}$ en l'absence d'ambiguïté)

$$\mathbb{F} ::= \mathbb{V} \mid \mathbb{F}^\perp \mid (\mathbb{F} \otimes \mathbb{F}) \mid (\mathbb{F} \parr \mathbb{F}) \mid (\mathbb{F} \oplus \mathbb{F}) \mid (\mathbb{F} \,\&\, \mathbb{F}) \mid (\mathbb{F} \multimap \mathbb{F}) \mid (\mathbb{F} \circ\!\!-\!\!\circ \mathbb{F}) \mid !\mathbb{F} \mid ?\mathbb{F}$$

4.3 LL en tant que calcul des séquents

4.3.1 Syntaxe

Une première approche peut se faire par le calcul des séquents. On peut reprendre l'idée de Gentzen et construire un calcul des séquents adapté à la logique linéaire. Les démonstrations sont donc sous la forme d'arbres. Nous n'exposerons ici que le calcul des séquents en version unilatère mais le passage à la négation lors du changement de coté permet d'obtenir la version bilatère. On pose les règles suivantes :

$$\frac{}{\vdash A, A^\perp}\ (\text{ax}) \qquad \frac{\vdash \Gamma, A, B}{\vdash \Gamma, A \parr B}\ (\parr) \qquad \frac{\vdash \Gamma, B}{\vdash \Gamma, A \oplus B}\ (\oplus)$$

$$\frac{\vdash \Gamma, A}{\vdash \Gamma, A \oplus B}\ (\oplus) \qquad \frac{\vdash \Gamma, A \qquad \vdash \Gamma, B}{\vdash \Gamma, A \,\&\, B}\ (\&) \qquad \frac{\vdash \Gamma, A \qquad \vdash \Delta, B}{\vdash \Gamma, \Delta, A \otimes B}\ (\otimes)$$

$$\frac{\vdash \Gamma, A \qquad \vdash \Delta, A^\perp}{\vdash \Gamma, \Delta}\ (\text{cut}) \qquad \frac{\vdash \Gamma, A}{\vdash \Gamma, ?A}\ (?\text{d}) \qquad \frac{\vdash ?\Gamma,\ A}{\vdash ?\Gamma, !A}\ (!)$$

$$\frac{\vdash \Gamma}{\vdash \Gamma, ?A}\ (?w) \qquad \frac{\vdash \Gamma, ?A, ?A}{\vdash \Gamma, ?A}\ (?c)$$

Les règles de l'axiome et de la coupure ont un fonctionnement similaire à celles du calcul des séquents de Gentzen. On remarque la différence de fonctionnement des règles associées au connecteurs multiplicatifs et connecteurs additifs. On utilise comme annoncé les connecteurs exponentiels pour former les règles structurelles, mais une attention est portée au statut de duplicabilité des formules. On remarque des relations de dualité entre les connecteurs $\otimes$ et $\parr$, $\oplus$ et $\&$ et pour finir ! et de ?.

D'autres propriétés essentielles se retrouvent aussi par de courtes démonstrations sur ces règles. Nous pouvons par exemple rédiger le sens direct de la démonstration de la distributivité de $\otimes$ sur $\oplus$:

$$\dfrac{\dfrac{\dfrac{\dfrac{}{\vdash \mathrm{A}^\perp, \mathrm{A}} \quad \dfrac{}{\vdash \mathrm{B}^\perp, \mathrm{B}}}{\vdash \mathrm{A}^\perp, \mathrm{A}\otimes\mathrm{B}, \mathrm{B}^\perp}}{\vdash \mathrm{A}^\perp, (\mathrm{A}\otimes\mathrm{B})\oplus(\mathrm{A}\otimes\mathrm{C}), \mathrm{B}^\perp} \qquad \dfrac{\dfrac{\dfrac{}{\vdash \mathrm{A}^\perp, \mathrm{A}} \quad \dfrac{}{\vdash \mathrm{C}^\perp, \mathrm{C}}}{\vdash \mathrm{A}^\perp, \mathrm{A}\otimes\mathrm{C}, \mathrm{C}^\perp}}{\vdash \mathrm{A}^\perp, (\mathrm{A}\otimes\mathrm{B})\oplus(\mathrm{A}\otimes\mathrm{C}), \mathrm{C}^\perp}}{\vdash \mathrm{A}^\perp, (\mathrm{A}\otimes\mathrm{B})\oplus(\mathrm{A}\otimes\mathrm{C}), (\mathrm{B}^\perp \,\&\, \mathrm{C}^\perp)}}{\vdash \mathrm{A}^\perp \,\&\, (\mathrm{B}^\perp \,\&\, \mathrm{C}^\perp) \,\&\, (\mathrm{A}\otimes\mathrm{B})\oplus(\mathrm{A}\otimes\mathrm{C})}$$

En utilisant les formules de dualité entre les connecteurs, on a bien une preuve de la formule :

$$A \otimes (B \oplus C) \multimap (A \oplus B) \otimes (A \oplus C)$$

La présentation en calcul des séquents nous permet de plus facilement construire la preuve d'une formule. En effet, pour construire cette preuve, il suffit de partir du bas de l'arbre et d'appliquer les règles à chaque étape, suivant leurs hypothèses et conclusions, l'ensemble des règles applicables étant généralement de très faible cardinal. En utilisant cette méthode on trouve les nombreuses relations entre connecteurs, ce qui permet ensuite de simplifier le calcul.

Le fragment intéressant à étudier pour ses propriétés de linéarité est celui composé des connecteurs et règles multiplicatives et exponentielles. On l'appelle le fragment multiplicatif-exponentiel noté *MELL*. Il nous permet en effet d'accéder aux propriétés de linéarité des connecteurs multiplicatifs et de garder une certaine expressabilité grâce aux connecteurs exponentiels et à leur règles structurelles. En particulier, une restriction sur les règles d'affaiblissement et de contraction dans une démonstration de MELL nous permettrait de garantir la non-duplication de sous-preuves lors de la réduction des coupures.

4.3.2 Conséquences et propriétés principales

On observe que les différentes coupures et leur réductions par élimination dans MELL semblent être :

$$\dfrac{\dfrac{\begin{array}{c}\Pi_1\\ \vdots\\ \vdash \Gamma, A\end{array} \quad \dfrac{}{\vdash A, A^\perp}}{\vdash \Gamma, A}}{} \quad \overset{\text{elim}}{\rightsquigarrow} \quad \dfrac{\begin{array}{c}\Pi_1\\ \vdots\\ \vdash \Gamma, A\end{array}}{}\ (\text{ax})$$

$$\dfrac{\dfrac{\dfrac{\Pi_1}{\vdots}}{\vdash \Gamma, A} \quad \dfrac{\dfrac{\Pi_2}{\vdots}}{\vdash \Delta, \mathrm{B}} \quad \dfrac{\dfrac{\Pi_3}{\vdots}}{\vdash \Omega, A^{\perp}, B^{\perp}}}{\dfrac{\vdash \Gamma, \Delta, \mathrm{A}\otimes\mathrm{B} \quad \vdash \Omega, A^{\perp} \parr B^{\perp}}{\vdash \Gamma, \Delta, \Omega}} \quad \underset{(\otimes/\parr)}{\overset{\text{elim}}{\rightsquigarrow}} \quad \dfrac{\dfrac{\dfrac{\Pi_1}{\vdots}}{\vdash \Gamma, \mathrm{A}} \quad \dfrac{\dfrac{\Pi_2}{\vdots}}{\vdash \Delta, \mathrm{B}} \quad \dfrac{\dfrac{\Pi_3}{\vdots}}{\vdash \Omega, \mathrm{A}^{\perp}, \mathrm{B}^{\perp}}}{\vdash \Delta, \Omega, \mathrm{A}^{\perp}}}{\vdash \Gamma, \Delta, \Omega}$$

$$\dfrac{\dfrac{\dfrac{\Pi_1}{\vdots}}{\vdash \Gamma, A}}{\vdash \Gamma, ?A} \quad \dfrac{\dfrac{\dfrac{\Pi_2}{\vdots}}{\vdash ?\Delta, A^{\perp}}}{\vdash ?\Delta, !A^{\perp}} \quad \underset{(?d/!)}{\overset{\text{elim}}{\rightsquigarrow}} \quad \dfrac{\dfrac{\Pi_1}{\vdots}}{\vdash \Gamma, A} \quad \dfrac{\dfrac{\Pi_2}{\vdots}}{\vdash ?\Delta, A^{\perp}}}{\vdash \Gamma, ?\Delta}$$

$$\dfrac{\dfrac{\dfrac{\Pi_1}{\vdots}}{\vdash \Gamma}}{\vdash \Gamma, ?A} \quad \dfrac{\dfrac{\dfrac{\Pi_2}{\vdots}}{\vdash ?\Delta, A^{\perp}}}{\vdash ?\Delta, !A^{\perp}} \quad \underset{(?w/!)}{\overset{\text{elim}}{\rightsquigarrow}} \quad \dfrac{\dfrac{\Pi_1}{\vdots}}{\vdash \Gamma}}{\vdash \Gamma, ?\Delta}$$

$$\dfrac{\dfrac{\dfrac{\Pi_1}{\vdots}}{\vdash \Gamma, ?A, ?A}}{\vdash \Gamma, ?A} \quad \dfrac{\dfrac{\dfrac{\Pi_2}{\vdots}}{\vdash ?\Delta, A^{\perp}}}{\vdash ?\Delta, !A^{\perp}} \quad \underset{(?c/!)}{\overset{\text{elim}}{\rightsquigarrow}} \quad \dfrac{\dfrac{\dfrac{\Pi_1}{\vdots}}{\vdash \Gamma, ?A, ?A} \quad \dfrac{\dfrac{\Pi_2}{\vdots}}{\vdash ?\Delta, A^{\perp}}}{\vdash \Gamma, ?\Delta, ?A} \quad \dfrac{\dfrac{\Pi_2}{\vdots}}{\vdash ?\Delta, A^{\perp}}}{\dfrac{\vdash \Gamma, ?\Delta, ?\Delta}{\vdash \Gamma, ?\Delta}}$$

On remarque aussi qu'il est possible de commuter les règles d'introduction des connecteurs avec la coupure, en n'affectant que localement la démonstration. Cela nous permet de faire remonter la coupure au niveau des règles d'introduction des connecteurs concernés. Nous appelons ces règles des *règles de commutation*. Prenons rapidement l'exemple d'une commutation avec le tenseur :

$$\dfrac{\dfrac{\dfrac{\Pi_1}{\vdots}}{\vdash \Gamma, C} \quad \dfrac{\dfrac{\Pi_2}{\vdots}}{\vdash \Delta, A, C^{\perp}} \quad \dfrac{\dfrac{\Pi_3}{\vdots}}{\vdash \Omega, B}}{\dfrac{\vdash \Gamma, C \quad \vdash \Delta, \Omega, A \otimes B, C^{\perp}}{\vdash \Gamma, \Delta, \Omega, A \otimes B}} \quad \leftrightsquigarrow \quad \dfrac{\dfrac{\dfrac{\Pi_1}{\vdots}}{\vdash \Gamma, C} \quad \dfrac{\dfrac{\Pi_2}{\vdots}}{\vdash \Delta, A, C^{\perp}}}{\vdash \Gamma, \Delta, A} \quad \dfrac{\dfrac{\Pi_3}{\vdots}}{\vdash \Omega, B}}{\vdash \Gamma, \Delta, \Omega, A \otimes B}$$

Grâce à ces étapes élémentaires, on arrive à construire l'élimination complète des coupures et on montre :

Théorème : (Elimination des coupures)
Dans le fragment multiplicatif et exponentiel (MELL) de la logique linéaire intuitionniste (LJ), on a :

$$\forall\, \Gamma \subset \mathbb{F},\ \ \forall\, \varphi \in \mathbb{F},\ \ \Gamma \vdash^{+}_{LJ} \varphi \ \ \Leftrightarrow\ \ \Gamma \vdash_{LJ} \varphi$$

Et on montre, avec un démonstration similaire à celle dans SJ :

Théorème : (Sous-formule)
Chaque formule qui apparait dans une preuve de $\Gamma \vdash_{LJ} \varphi$ de MELL est, soit une sous-formule de Γ, soit une sous-formule de φ

Nous avons donc conservé les propriétés importantes du calcul des séquents. On peut même montrer une propriété encore plus forte : la confluence de la réduction des coupures. Autrement dit, quels que soit nos choix de réduction des coupures, on ne peut obtenir au final qu'une seule preuve réduite :

Définition : (Confluence)
On dit qu'une relation $\mathcal{R}$ sur E est confluente si :
$\forall\, A, B, C \in E,\ (A \,\mathcal{R}\, B \text{ et } A \,\mathcal{R}\, C) \Rightarrow \exists\, D \in E,\ (B \,\mathcal{R}\, D \text{ et } C \,\mathcal{R}\, D)$

Théorème : (Normalisation forte)
La réduction des coupures est confluente sur l'ensemble des arbres de preuves de MELL

Pour prouver le théorème, on montre que les cas où deux réductions ne sont pas indépendantes mènent finalement à la même preuve car ils correspondent à des cas triviaux. On montre que dans les autres cas, la réductions est indépendante des autres étapes.

C'était déjà le cas dans le calcul des séquents intuitionniste (SJ) de Gentzen. On peut essayer de s'en convaincre en regardant par isomorphisme le théorème de β-réduction de Church-Rosser.

5 Réseaux de preuves

Lors de la réduction des coupures, nous avons dû ajouter des étapes de commutation pour faire remonter la coupure au niveau de l'introduction des connecteurs concernés. On ne donne pas d'importance à la position d'introduction des connecteurs dans la réduction lorsqu'ils peuvent commuter et c'est pour cela qu'on autorise les commutations dans la réduction. Cependant, cela témoigne du fait que la syntaxe que nous utilisons capture des détails inutiles qui rendent ensuite plus difficile la réduction. Nous cherchons donc maintenant à relaxer la syntaxe pour simplifier le processus d'élimination des coupures.

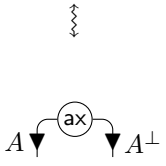
5.1 Idée générale

Les démonstrations de la syntaxe suivant le calcul des séquents prennent la formes d'arbres. C'est cette forme qui semble être à l'origine du caractère profondément séquentiel de nos démonstrations. Nous allons donc pouvoir relaxer cette contrainte en prenant une forme plus libre, celle des graphes.

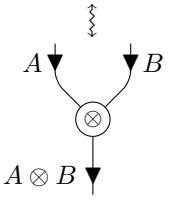
5.2 Structure de preuves

Etant donné qu'une règle est supposée prendre la forme d'une liste d'hypothèses et d'une conclusion, il semble naturel d'utiliser les noeuds du graphes pour les représenter. Les formules se retrouvent représentées par les arêtes. On ajoute à cela une valuation et on oriente les arêtes afin de pouvoir vérifier que le graphe respecte les règles associées aux connecteurs présents sur les noeuds. Prenons un exemple des noeuds associés aux connecteurs de MLL :

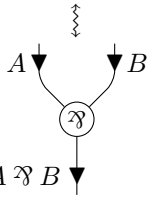
$$\frac{}{\vdash A, A^{\perp}}\ (\text{ax}) \qquad \frac{\vdash \Gamma, A \qquad \vdash \Delta, B}{\vdash \Gamma, \Delta, A \otimes B}\ (\otimes) \qquad \frac{\vdash \Gamma, A, B}{\vdash A \parr B}\ (\parr)$$



Les étiquettes en sortie doivent porter deux formules conjuguées.

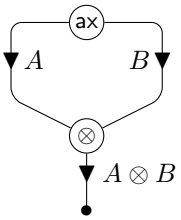


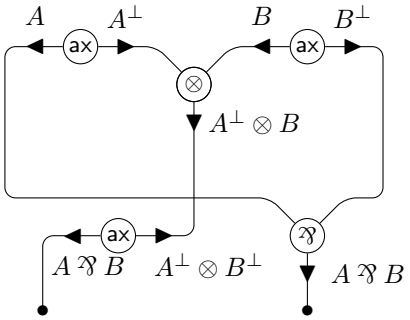
L'étiquette de l'arête en sortie doit porter la formule composée du tenseur des deux formules sur les arêtes entrantes.



L'étiquette de l'arête en sortie doit porter la formule composée du par des deux formules sur les arêtes entrantes.

On peut, par exemple, tracer les graphes suivants :





On remarque alors rapidement que ces règles ne sont pas suffisantes pour assurer qu'il s'agit bien d'une preuve de MELL. En effet, dans les deux exemples que nous venons de donner, le graphe de droite correspond bien à une preuve [13] tandis que le graphe de gauche ne correspond à aucune preuve de MELL. On voit aussi dans l'exemple de droite qu'on a bien une syntaxe qui identifie les preuves qui ne diffèrent que d'une commutation.

5.3 Critère de correction dans MLL

Nous cherchons donc à déterminer une condition nécessaire et suffisante qui nous permette de sélectionner la classe de graphes qui correspondent à des preuves dans MELL. Le problème se pose au niveau du noeud associé à la règle d'introduction du $\parr$. En effet, cette règle ne prend qu'une seule hypothèse alors que le noeud qui y est associé prend deux formules. En particulier, rien n'assure sur le graphe qu'elles appartiennent au même séquent. Il faut donc observer des propriétés de connexité et d'acyclicité particulière lors de la déconnexion de certaines branches des noeud $\parr$.

Introduisons les notions nécessaires à la mise en place d'un tel critère :

Définition : (Graphes de correction)
Soit une structure de preuve P. Un graphe de correction de la structure P est un graphe obtenu à partir de P en enlevant une des deux branches de chaque noeud $\parr$.

Une structure de preuve multiplicative dont tous les graphes de correction sont acycliques et ne possèdent qu'une seule composante connexe est appelée *réseau de preuve multiplicatif*.

On obtient alors le critère de correction (ou *séquentialisation*) suivant :

Théorème : (Critère de correction de Danos-Regnier)
Une structure de preuve est l'image d'une preuve de MLL en calcul des séquents si et seulement si il s'agit d'un réseau de preuve multiplicatif.

La preuve de ce théorème est complexe et je ne l'aborderai donc pas dans ce rapport. On peut cependant regarder la complexité de l'implémentation d'un tel critère. Un graphe avec n noeud $\parr$ permet de former 2^n graphes de corrections différents. Il faut alors vérifier l'acyclicité de chacun d'eux puis tester leur connexité. La complexité est donc élevée. On peut donc essayer de déterminer d'autres critères de correction dont l'implémentation serait moins coûteuse. On se satisfera dans ce rapport du lemme suivant qui permet de diminuer le nombre de test de connexité à effectuer :

Lemme :
Le nombre de composantes connexes de tous les graphes de correction acyclique d'une structure de preuve multiplicative est le même.

Donc, si tous les graphes de correction sont acycliques, il suffit de tester la connexité d'un d'eux pour déterminer s'il s'agit de l'image d'une preuve de MLL. Ce théorème est le cas particulier d'un théorème de théorie des graphes faisant le lien entre le nombre de composantes connexes, et le nombre cyclomatique dans un graphe acyclique.

On peut aussi étendre le critère de correction au structure de preuves sur MELL, mais je ne traiterai pas de cela dans ce rapport.

13. Les preuves qui y sont associées sont présentées dans l'annexe E

Annexe A: Axiomes de la logique booléenne

1.	$(P \to (Q \to P))$	(implication 1)
2.	$((P \to (Q \to R)) \to ((P \to Q) \to (P \to R)))$	(implication 2)
3.	$(P \to \neg\neg P)$	(negation 1)
4.	$(\neg\neg P \to P)$	(negation 2)
5.	$((P \to Q) \to (\neg Q \to \neg P))$	(negation 3)
6.	$(P \to (Q \to (P \wedge Q)))$	(conjonction 1)
7.	$((P \wedge Q) \to P)$	(conjonction 2)
8.	$((P \wedge Q) \to Q)$	(conjonction 3)
9.	$(P \to (P \vee Q))$	(disjonction 1)
10.	$(Q \to (P \vee Q))$	(disjonction 2)
11.	$((((P \vee Q) \wedge (P \to R)) \wedge (Q \to R)) \to R)$	(disjonction 3)

Annexe B: Syntaxe du calcul propositionnel intuitionniste

$$\frac{}{\Gamma, \varphi \vdash \varphi}\,(ax) \qquad \frac{\Gamma \vdash \bot}{\Gamma \vdash \varphi}\,(\bot_E)$$

$$\frac{\Gamma \vdash \varphi \qquad \Gamma \vdash \psi}{\Gamma \vdash \varphi \wedge \psi}\,(\wedge_I) \qquad \frac{\Gamma \vdash \varphi \wedge \psi}{\Gamma \vdash \varphi}\,(\wedge_E) \qquad \frac{\Gamma \vdash \varphi \wedge \psi}{\Gamma \vdash \psi}\,(\wedge_E)$$

$$\frac{\Gamma \vdash \varphi}{\Gamma \vdash \varphi \vee \psi}\,(\vee_I) \qquad \frac{\Gamma \vdash \psi}{\Gamma \vdash \varphi \vee \psi}\,(\vee_I) \qquad \frac{\Gamma, \varphi \vdash \rho \qquad \Gamma, \psi \vdash \rho \qquad \Gamma \vdash \varphi \vee \psi}{\Gamma \vdash \rho}\,(\vee_E)$$

$$\frac{\Gamma, \varphi \vdash \psi}{\Gamma \vdash \varphi \to \psi}\,(\to_I) \qquad \frac{\Gamma \vdash \varphi \to \psi \qquad \Gamma \vdash \varphi}{\Gamma \vdash \psi}\,(\to_E)$$

Annexe C: Sémantique intuitionniste et algèbres de Heyting

Démonstration de $[\top]_\sim = \{\varphi \mid \Gamma \vdash \varphi\}$ **:**
Soit $\varphi \in \{\varphi \mid \Gamma \vdash \varphi\}$, on a $\Gamma \vdash \varphi$ donc :

$$\frac{\dfrac{\dfrac{}{\Gamma, \varphi, \bot \vdash \bot}\,(ax)}{\Gamma, \varphi \vdash \bot \to \bot}\,(\to_I)}{\Gamma \vdash \varphi \to (\bot \to \bot)}\,(\to_I)$$

On a une peuve de : $\Gamma \vdash \varphi \to \top$

$$\frac{\dfrac{}{\Gamma, (\bot \to \bot) \vdash \varphi}\,(ax)}{\Gamma \vdash (\bot \to \bot) \to \varphi}\,(\to_I)$$

On a une peuve de : $\Gamma \vdash \top \to \varphi$

Donc on a : $\varphi \in [\top]_\sim$

Soit $\varphi \in [\top]_\sim$, on a donc $\Gamma \vdash \top \to \varphi$

$$\frac{\dfrac{\dfrac{}{\Gamma, \bot \vdash \bot}\,(ax)}{\Gamma \vdash (\bot \to \bot)}\,(\to_I) \qquad \dfrac{}{\Gamma \vdash (\bot \to \bot) \to \varphi}}{\Gamma \vdash \varphi}\,(\to_E)$$

Donc on a $\Gamma \vdash \varphi$
Ce qui conclut la démonstration de $[\top]_\sim = \{\varphi \mid \Gamma \vdash \varphi\}$

Définition : (Algèbre de Heyting)
$\mathcal{H} = \langle H, \cup, \cap, \Rightarrow, -, 0, 1\rangle$ est une algèbre de Heyting si et seulement si les conditions suivantes sont vérifiées :

- $\cup$ et $\cap$ sont associatives et commutatives

- $(A \cup B) \cap C = (A \cap C) \cup (B \cap C)$ et $(A \cap B) \cup C = (A \cup C) \cap (B \cup C)$
- $A \cup 0 = A$ et $A \cap 1 = A$ (0 neutre de $\cup$ et 1 neutre de $\cap$)
- $A \cup A = A$
- $-A = A \Rightarrow A = 0$
- $A \cap C \leqslant B \Leftrightarrow C \leqslant A \Rightarrow B$ (avec $A \leqslant B \Leftrightarrow A \cup B = B$)

Démonstration d'un contre exemple du tiers-exclu

$A \wedge B$

${}_A\backslash^B$	0	1/2	1
0	0	0	0
1/2	0	1/2	1/2
1	0	1/2	1

$A \vee B$

${}_A\backslash^B$	0	1/2	1
0	0	1/2	1
1/2	1/2	1/2	1
1	1	1	1

$A \to B$

${}_A\backslash^B$	0	1/2	1
0	1	1	1
1/2	0	1	1
1	0	1/2	1

$\neg A$

A	$\neg A$
0	1
1/2	1/2
1	0

On a : $1/2 \vee 1/2 = 1/2 \vee (1/2 \to 0) = 1/2 \vee 0 = 1/2 \neq 1$

Annexe D: Duplication de preuve

Exemple de duplication de preuve par le processus de réduction des coupures :

$$\dfrac{\dfrac{\dfrac{\dfrac{\vdots}{\Gamma, P \vdash Q} \quad \dfrac{\vdots}{\Gamma, P \vdash R}\,(\wedge_I)}{\Gamma, P \vdash Q \wedge R}\,(\to_I)_{(*)}}{\Gamma \vdash P \to (Q \wedge R)} \quad \dfrac{\vdots}{\Gamma \vdash P}\,{}^{(**)}}{\Gamma \vdash Q \wedge R}\,(\to_E)_{(*)}$$

Devient par réduction sur $(*)$:

$$\dfrac{\dfrac{\vdots}{\Gamma \vdash P}\,{}^{(**)} \quad \dfrac{\dfrac{\vdots}{\Gamma, P \vdash Q}}{\Gamma \vdash P \to Q}\,(\to_I)}{\Gamma \vdash Q}\,(\to_E) \quad \dfrac{\dfrac{\dfrac{\vdots}{\Gamma, P \vdash R}}{\Gamma \vdash P \to R}\,(\to_I) \quad \dfrac{\vdots}{\Gamma \vdash P}\,{}^{(**)}}{\Gamma \vdash R}\,(\to_E)}{\Gamma \vdash Q \wedge R}\,(\wedge_I)$$

Ce qui a mené à la duplication de la preuve de $\Gamma \vdash P$ $(**)$.

Annexe E: Réseaux de preuves

Le graphe de gauche correspond à la structure de preuve suivante.

$$\dfrac{\dfrac{}{\vdash A, A^\perp}}{\vdash A \otimes A^\perp}$$

On se rend alors effectivement compte qu'il ne s'agit pas d'une preuve valide dans MELL.
Le graphe de droite correspond aux deux preuves suivantes :

$$\dfrac{\dfrac{}{\vdash A \parr B, A^\perp \otimes B^\perp} \quad \dfrac{\dfrac{\dfrac{}{\vdash A, A^\perp} \quad \dfrac{}{\vdash B, B^\perp}}{\vdash A, B, A^\perp \otimes B^\perp}\,(\parr)}{\vdash A \parr B, A^\perp \otimes B^\perp}\,(cut)}{\vdash A \parr B, A^\perp \otimes B^\perp} \qquad \dfrac{\dfrac{\dfrac{\dfrac{}{\vdash A, A^\perp} \quad \dfrac{}{\vdash B, B^\perp}}{\vdash A, B, A^\perp \otimes B^\perp}\,(cut)}{\vdash A \parr B, A^\perp \otimes B^\perp}\,(\parr)}{\vdash A \parr B, A^\perp \otimes B^\perp}$$

Ces deux graphes ne diffèrent que d'une permutation (cut/$\parr$) mais se retrouvent bien identifiés au même réseau de preuve.

Références

[GTL89] Girard, Jean-Yves and Taylor, Paul and Lafont, Yves, Proofs and Types, Cambridge University Press, 1989

[So06] Sørensen, Morten Heine and Urzyczyn, Pawel, Lectures on the Curry-Howard Isomorphism, Elsevier Science Inc., 2006

[La94] Yves Lafont, From Proof-Nets to Interaction Nets, Cambridge University Press, 1994

[Ge69] Gerhard Gentzen, Untersuchungen über das logische Schliessen, Mathematische Zeitschrift, 1934

[Cu58] H.B. Curry and R. Feys, Combinatory Logic, North-Holland, 1958.

[Ho80] W. Howard, The formulae-as-types notion of construction. In Seldin and Hindley, H.B. Curry : Essays on Combinatory Logic, Lambda Calculus and Formalism, Academic Press Limited, 1980.

[Pr65] D. Prawitz, Natural Deduction : A Proof Theoretical Study, Almquist & Wiksell, 1965

[Gir87] J.-Y. Girard, Linear Logic, Theoretical Computer Science, 1987