

Théorie de la démonstration

Olivier Laurent
Olivier.Laurent@ens-lyon.fr

14 octobre 2011

Première partie

Une introduction

On va étudier des systèmes de preuves formelles donnant des objets plus riches et plus manipulables que les preuves obtenues dans le système de Hilbert.

Les règles de dérivation sont similaires à celles rencontrées par exemple dans les systèmes d'aide à la preuve comme **Coq** ou **Phox**.

On insistera sur l'interprétation calculatoire de ces preuves formelles.

Présentation de la notion de séquent

On cherche à définir un système de preuve formelle pour des formules. Il apparaît cependant que l'utilisation de structures plus riches simplifie le travail : les séquents.

Un *séquent* est une paire de listes de formules notée $A_1, \dots, A_n \vdash B_1, \dots, B_k$ qui sert à représenter l'état d'une preuve : à partir des hypothèses A_1, \dots, A_n , on a prouvé les conclusions B_1, \dots, B_k mais la virgule à gauche du signe \vdash est interprétée comme une conjonction et la virgule à droite comme une disjonction.

Chercher à prouver une formule A revient alors à prouver le séquent $\vdash A$.

Quelques preuves formalisées dans une théorie avec axiomes

Cette section constitue une petite introduction *pratique*. On considère le calcul des prédicats avec l'égalité $=$ et le langage de l'arithmétique de Presburger $\{0, S, +\}$.

On se donne un ensemble de règles de base. Pour l'égalité :

$$\frac{}{\vdash t = t} \textit{ refl} \qquad \frac{\vdash t = u}{\vdash u = t} \textit{ sym} \qquad \frac{\vdash t = u \quad \vdash u = v}{\vdash t = v} \textit{ trans}$$

pour les axiomes de l'arithmétique :

$$\frac{}{\vdash \forall x \neg (Sx = 0)} \qquad \frac{}{\vdash \forall x (x = 0 \vee \exists y (x = Sy))} \qquad \frac{\vdash t = u}{\vdash St = Su} \qquad \frac{\vdash St = Su}{\vdash t = u}$$

$$\frac{}{\vdash t + 0 = t} \qquad \frac{}{\vdash t + Su = S(t + u)}$$

Remarque : Si on veut être plus rigoureux, on peut donner comme règles de l'égalité :

$$\frac{}{\vdash t = t} \qquad \frac{\Gamma[t/x] \vdash \Delta[t/x]}{\Gamma[u/x], t = u \vdash \Delta[u/x]}$$

L'objectif est désormais de prouver des résultats élémentaires (mais de plus en plus complexes) à partir des règles ci-dessus et en introduisant de nouvelles règles (essentiellement pour les connecteurs logiques) quand le besoin se fait sentir.

Exercice 1

Montrer $x + SSy = SS(x + y)$.

CORRECTION : Avec les règles que l'on a données :

$$\frac{\frac{}{\vdash x + Sy = S(x + y)}}{\vdash x + SSy = S(x + Sy)} \quad \frac{}{\vdash S(x + Sy) = SS(x + y)}}{\vdash x + SSy = SS(x + y)}$$

Exercice 2

Montrer $\forall x (x + S0 = Sx)$.

CORRECTION : Avec l'introduction du \forall :

$$\frac{\frac{\frac{}{\vdash x + S0 = S(x+0)}}{\vdash x + S0 = Sx}}{\vdash \forall x(x + S0 = Sx)} \quad \frac{\frac{}{\vdash x + 0 = x}}{\vdash S(x+0) = Sx}}$$

Exercice 3

Montrer $\forall x \forall y ((x = 0 \wedge y = 0) \rightarrow x + y = 0)$.

CORRECTION : En calcul des séquents, avec une nouvelle règle pour = :

$$\frac{\frac{\frac{\frac{\frac{}{\vdash 0 + 0 = 0}}{x = 0 \vdash x + 0 = 0}}{x = 0, y = 0 \vdash x + y = 0}}{x = 0 \wedge y = 0 \vdash x + y = 0}}{\vdash (x = 0 \wedge y = 0) \rightarrow x + y = 0}}{\vdash \forall y ((x = 0 \wedge y = 0) \rightarrow x + y = 0)}}{\vdash \forall x \forall y ((x = 0 \wedge y = 0) \rightarrow x + y = 0)}$$

Exercice 4

Montrer $\forall x (\neg(x = 0) \rightarrow \exists y (x = Sy))$.

CORRECTION : Avec un mélange de calcul des séquents et déduction naturelle classique :

$$\frac{\frac{\frac{\frac{\frac{}{\vdash \forall x(x = 0 \vee \exists y(x = Sy))}}{\vdash x = 0 \vee \exists y(x = Sy)}}{\vdash x = 0, \exists y(x = Sy)}}{\neg(x = 0) \vdash \exists y(x = Sy)}}{\vdash \neg(x = 0) \rightarrow \exists y(x = Sy)}}{\vdash \forall x(\neg(x = 0) \rightarrow \exists y(x = Sy))}$$

Exercice 5

Montrer $\forall x \forall y (\neg(y = 0) \rightarrow \exists z (x + y = Sz))$.

CORRECTION : Avec un mélange de calcul des séquents et déduction naturelle :

$$\frac{\frac{\frac{\frac{\frac{}{\vdash \forall y(\neg(y = 0) \rightarrow \exists y'(y = Sy'))}}{\vdash \neg(y = 0) \rightarrow \exists y'(y = Sy')}}{\neg(y = 0) \vdash \neg(y = 0)}}{\neg(y = 0) \vdash \exists y'(y = Sy')}}{\frac{\frac{\frac{\frac{\frac{}{\vdash x + Sy' = S(x + y')}}{\vdash \exists z(x + Sy' = Sz)}}{y = Sy' \vdash \exists z(x + y = Sz)}}{\exists y'(y = Sy') \vdash \exists z(x + y = Sz)}}{\neg(y = 0) \vdash \exists z(x + y = Sz)}}{\vdash \neg(y = 0) \rightarrow \exists z(x + y = Sz)}}{\vdash \forall y(\neg(y = 0) \rightarrow \exists z(x + y = Sz))}}{\vdash \forall x \forall y (\neg(y = 0) \rightarrow \exists z(x + y = Sz))}$$

Exercice 6

Montrer $\forall x \forall y (x + y = 0 \rightarrow y = 0)$.

CORRECTION : Avec un mélange de calcul des séquents et déduction naturelle, et même plus :

Catalogue de règles de dérivation avec séquents

Voici une liste de règles de dérivation possibles :

$$\begin{array}{c}
 \frac{\Gamma \vdash A}{\Gamma \vdash A \vee B} \qquad \frac{\Gamma \vdash A \rightarrow B \quad \Gamma \vdash A}{\Gamma \vdash B} \qquad \frac{\Gamma, B \vdash \Delta}{\Gamma, A \wedge B \vdash \Delta} \\
 \\
 \frac{\Gamma \vdash A \quad \Gamma, A \vdash \Delta}{\Gamma \vdash \Delta} \qquad \frac{\Gamma \vdash \mathbf{F}}{\Gamma \vdash \Delta} \qquad \frac{\Gamma \vdash A}{\Gamma, B \vdash A} \qquad \frac{\Gamma, A, A \vdash B}{\Gamma, A \vdash B} \\
 \\
 \frac{}{\Gamma, A \vdash A, \Delta} \qquad \frac{\Gamma, A \vee B \vdash \Delta \quad \Gamma \vdash A}{\Gamma \vdash \Delta} \qquad \frac{\Gamma, A[t/x] \vdash \Delta}{\Gamma, \forall x A \vdash \Delta} \qquad \frac{\Gamma \vdash A, \Delta}{\Gamma, \neg A \vdash \Delta}
 \end{array}$$

Les règles sont les briques élémentaires qui permettent de construire les dérivations. Les preuves que l'on va considérer sont des arbres dont les règles constituent les nœuds, elles sont donc de la forme :

$$\frac{\Gamma_1 \vdash \Delta_1 \cdots \Gamma_n \vdash \Delta_n}{\Gamma \vdash \Delta}$$

i.e. on a $n \geq 0$ prémisses et une unique conclusion.

De nombreuses occurrences de formules sont présentes dans une instance d'une règle. Attention, dans le séquent $\vdash A, A$ il y a deux occurrences différentes d'une même formule A . Cependant, par abus de langage, on dira souvent formule à la place d'occurrence de formule. Afin de faire un peu de tri entre les différentes occurrences de formules (et de séquents), on introduit les notions suivantes :

- Une formule est *active* si elle est "concernée par la règle" (c'est-à-dire en particulier que sa présence est requise pour que la règle soit correctement appliquée).
- Une formule est *principale* dans une règle qui agit sur un connecteur particulier si elle contient le connecteur en question.
- Les *contextes* sont les formules qui ne sont pas actives dans la règle (ce sont celles que l'on note Γ ou Δ dans la description de la règle).
- Les *prémisses* d'une règle sont les séquents situés au-dessus de la règle.
- La *conclusion* d'une règle est le séquent situé au-dessous de la règle.
- Une règle *zéroaire* est une règle sans prémisses, une règle *unaire* est une règle avec une prémisses, une règle *binnaire* est une règle avec deux prémisses, ...

Correction des règles

Afin de ne pas engendrer d'aberrations logiques, on peut vérifier que les règles que l'on écrit sont valides pour la logique classique. Pour cela, on interprète un séquent $A_1, \dots, A_n \vdash B_1, \dots, B_k$ par la formule $A_1 \wedge \dots \wedge A_n \rightarrow B_1 \vee \dots \vee B_k$ et une règle $\frac{\Gamma_1 \vdash \Delta_1 \cdots \Gamma_n \vdash \Delta_n}{\Gamma \vdash \Delta}$ par $(\Gamma_1 \rightarrow \Delta_1) \wedge \dots \wedge (\Gamma_n \rightarrow \Delta_n) \rightarrow (\Gamma \rightarrow \Delta)$ et on vérifie que l'interprétation de toute règle est une tautologie.

Exemple 1

La règle :

$$\frac{A_1, \dots, A_n \vdash A, B_1, \dots, B_k \quad A_1, \dots, A_n \vdash B, B_1, \dots, B_k}{A_1, \dots, A_n \vdash A \wedge B, B_1, \dots, B_k} \wedge^{\text{addR}}$$

est interprétée par :

$$(A_1 \wedge \dots \wedge A_n \rightarrow A \vee B_1 \vee \dots \vee B_k) \wedge (A_1 \wedge \dots \wedge A_n \rightarrow B \vee B_1 \vee \dots \vee B_k) \rightarrow (A_1 \wedge \dots \wedge A_n \rightarrow (A \wedge B) \vee B_1 \vee \dots \vee B_k)$$

dont on peut vérifier que la valeur de vérité est 1 pour toutes valeurs des A_i , des B_j , de A et de B .

Il en découle que si toutes les règles d'une dérivation sont ainsi valides, le séquent conclusion de la preuve correspond à une formule vraie de la logique classique.

Zoologie des règles

On cherche à y voir un peu plus clair dans les différentes règles que l'on a rencontrées et pour cela, on les classe selon un certain nombre de critères. Si on considère les règles suivantes qui concernent toutes le connecteur \wedge :

$$\begin{array}{c} \frac{\Gamma \vdash A, \Delta \quad \Gamma \vdash B, \Delta}{\Gamma \vdash A \wedge B, \Delta} \wedge_{\text{intro}}^{\text{add}} \text{R} \qquad \frac{\Gamma \vdash A, \Delta \quad \Gamma' \vdash B, \Delta'}{\Gamma, \Gamma' \vdash A \wedge B, \Delta, \Delta'} \wedge_{\text{intro}}^{\text{mul}} \text{R} \\ \\ \frac{\Gamma, A \vdash \Delta}{\Gamma, A \wedge B \vdash \Delta} \wedge_{\text{intro}}^{\text{add}} \text{L}_1 \qquad \frac{\Gamma, B \vdash \Delta}{\Gamma, A \wedge B \vdash \Delta} \wedge_{\text{intro}}^{\text{add}} \text{L}_2 \qquad \frac{\Gamma, A, B \vdash \Delta}{\Gamma, A \wedge B \vdash \Delta} \wedge_{\text{intro}}^{\text{mul}} \text{L} \\ \\ \frac{\Gamma \vdash A \wedge B, \Delta}{\Gamma \vdash A, \Delta} \wedge_{\text{elim}}^{\text{add}} \text{R}_1 \qquad \frac{\Gamma \vdash A \wedge B, \Delta}{\Gamma \vdash B, \Delta} \wedge_{\text{elim}}^{\text{add}} \text{R}_2 \\ \\ \frac{\Gamma \vdash A \wedge B, \Delta \quad \Gamma', A, B \vdash \Delta'}{\Gamma, \Gamma' \vdash \Delta, \Delta'} \wedge_{\text{elim}}^{\text{mul}} \text{R} \\ \\ \frac{\Gamma, A \wedge B \vdash \Delta \quad \Gamma \vdash A, \Delta \quad \Gamma \vdash B, \Delta}{\Gamma \vdash \Delta} \wedge_{\text{elim}}^{\text{add}} \text{L} \qquad \frac{\Gamma, A \wedge B \vdash \Delta}{\Gamma, A, B \vdash \Delta} \wedge_{\text{elim}}^{\text{mul}} \text{L} \end{array}$$

on peut faire les observations suivantes :

- Il y a des *règles d'introduction*, *i.e.* pour lesquelles la formule principale (celle qui contient le \wedge) est dans la conclusion de la règle. Il y a des *règles d'élimination*, *i.e.* pour lesquelles la formule principale est dans une prémisse de la règle.
- Il y a des *règles gauches*, *i.e.* pour lesquelles la formule principale se trouve dans la partie gauche d'un séquent. Il y a des *règles droites*, *i.e.* pour lesquelles la formule principale se trouve dans la partie droite d'un séquent.
- Enfin si on s'intéresse aux contextes dans les règles binaires, certaines règles requièrent des contextes identiques dans les deux prémisses et les superposent dans la conclusion, on les appelle *règles additives*. D'autres règles binaires au contraire juxtaposent les différents contextes issus des différentes prémisses, ce sont les *règles multiplicatives*. Cette terminologie additive/multiplicative s'étend également aux règles 0-aires, unaires, ... comme indiqué dans le nom des règles ci-dessus, mais il faudra attendre l'élimination des coupures ([section 1.2](#)) pour une justification.

À partir de ces différentes notions, on peut définir plusieurs systèmes de dérivation :

- Le *calcul des séquents* est obtenu en choisissant uniquement des règles d'introduction.
- La *déduction naturelle* est obtenue en choisissant uniquement des règles droites.
- La *déduction libre* est obtenue en choisissant uniquement des règles d'élimination.

Ces différents systèmes sont complets (prouvent toutes les formules vraies en logique classique) ce qui montre que certaines formulations de règles sont redondantes, par exemple élimination droite et introduction gauche (le premier choix donne la déduction naturelle et le second donne le calcul des séquents).

Remarque : En déduction libre, on utilise les règles d'élimination à gauche et à droite sans formule active en conclusion :

$$\frac{\Gamma, A \rightarrow B \vdash \Delta \quad \Gamma, A \vdash \Delta}{\Gamma \vdash \Delta} \rightarrow_{\text{elim}}^{\text{add}} \mathbf{L}_1 \qquad \frac{\Gamma \vdash A \rightarrow B, \Delta \quad \Gamma \vdash A, \Delta \quad \Gamma, B \vdash \Delta}{\Gamma \vdash \Delta} \rightarrow_{\text{elim}}^{\text{add}} \mathbf{R}$$

$$\frac{\Gamma, A \wedge B \vdash \Delta \quad \Gamma' \vdash A, \Delta' \quad \Gamma'' \vdash B, \Delta''}{\Gamma, \Gamma', \Gamma'' \vdash \Delta, \Delta', \Delta''} \wedge_{\text{elim}}^{\text{mul}} \mathbf{L}$$

Deuxième partie

Logiques classique et intuitionniste

Chapitre 1

Calcul des séquents

1.1 Calcul des séquents classique (LK)

Calcul des séquents propositionnel

Les formules de la logique classique propositionnelle que l'on considère sont :

$$A ::= X \mid \neg A \mid A \wedge A \mid A \vee A \mid A \rightarrow A \mid \mathbf{T} \mid \mathbf{F}$$

et les séquents sont de la forme $\Gamma \vdash \Delta$ où Γ et Δ sont des suites de formules (possiblement vides).

La *taille d'une formule* est donnée par $|X| = 1$, $|\neg A| = |A| + 1$, $|A \circ B| = |A| + |B| + 1$ (pour tout connecteur binaire \circ), $|\mathbf{T}| = 1$ et $|\mathbf{F}| = 1$.

Les règles du calcul des séquents sont classées en trois principaux groupes : le *groupe identité*, le *groupe structurel* et le *groupe logique*. On distingue également les versions multiplicatives et additives des règles.

Groupe identité multiplicatif.

$$\frac{}{A \vdash A} \text{ax}^{\text{mul}} \qquad \frac{\Gamma \vdash A, \Delta \quad \Gamma', A \vdash \Delta'}{\Gamma, \Gamma' \vdash \Delta, \Delta'} \text{cut}^{\text{mul}}$$

Groupe identité additif.

$$\frac{}{\Gamma, A \vdash A, \Delta} \text{ax}^{\text{add}} \qquad \frac{\Gamma \vdash A, \Delta \quad \Gamma, A \vdash \Delta}{\Gamma \vdash \Delta} \text{cut}^{\text{add}}$$

Groupe structurel.

$$\frac{\Gamma \vdash \Delta}{\sigma(\Gamma) \vdash \tau(\Delta)} \text{ech}$$
$$\frac{\Gamma, A, A \vdash \Delta}{\Gamma, A \vdash \Delta} \text{ctrL} \qquad \frac{\Gamma \vdash A, A, \Delta}{\Gamma \vdash A, \Delta} \text{ctrR}$$
$$\frac{\Gamma \vdash \Delta}{\Gamma, A \vdash \Delta} \text{wkL} \qquad \frac{\Gamma \vdash \Delta}{\Gamma \vdash A, \Delta} \text{wkR}$$

Groupe logique multiplicatif.

$$\begin{array}{c}
\frac{\Gamma \vdash A, \Delta \quad \Gamma' \vdash B, \Delta'}{\Gamma, \Gamma' \vdash A \wedge B, \Delta, \Delta'} \wedge^{\text{mulR}} \qquad \frac{\Gamma, A, B \vdash \Delta}{\Gamma, A \wedge B \vdash \Delta} \wedge^{\text{mulL}} \\
\\
\frac{\Gamma \vdash A, B, \Delta}{\Gamma \vdash A \vee B, \Delta} \vee^{\text{mulR}} \qquad \frac{\Gamma, A \vdash \Delta \quad \Gamma', B \vdash \Delta'}{\Gamma, \Gamma', A \vee B \vdash \Delta, \Delta'} \vee^{\text{mulL}} \\
\\
\frac{}{\vdash \top} \top^{\text{mulR}} \qquad \frac{\Gamma \vdash \Delta}{\Gamma, \top \vdash \Delta} \top^{\text{mulL}} \\
\\
\frac{\Gamma \vdash \Delta}{\Gamma \vdash \mathbf{F}, \Delta} \mathbf{F}^{\text{mulR}} \qquad \frac{}{\mathbf{F} \vdash} \mathbf{F}^{\text{mulL}} \\
\\
\frac{\Gamma, A \vdash \Delta}{\Gamma \vdash \neg A, \Delta} \neg\text{R} \qquad \frac{\Gamma \vdash A, \Delta}{\Gamma, \neg A \vdash \Delta} \neg\text{L} \\
\\
\frac{\Gamma, A \vdash B, \Delta}{\Gamma \vdash A \rightarrow B, \Delta} \rightarrow^{\text{mulR}} \qquad \frac{\Gamma, B \vdash \Delta \quad \Gamma' \vdash A, \Delta'}{\Gamma, \Gamma', A \rightarrow B \vdash \Delta, \Delta'} \rightarrow^{\text{mulL}}
\end{array}$$

Groupe logique additif.

$$\begin{array}{c}
\frac{\Gamma \vdash A, \Delta \quad \Gamma \vdash B, \Delta}{\Gamma \vdash A \wedge B, \Delta} \wedge^{\text{addR}} \qquad \frac{\Gamma, A \vdash \Delta}{\Gamma, A \wedge B \vdash \Delta} \wedge^{\text{addL}_1} \qquad \frac{\Gamma, B \vdash \Delta}{\Gamma, A \wedge B \vdash \Delta} \wedge^{\text{addL}_2} \\
\\
\frac{\Gamma \vdash A, \Delta}{\Gamma \vdash A \vee B, \Delta} \vee^{\text{addR}_1} \qquad \frac{\Gamma \vdash B, \Delta}{\Gamma \vdash A \vee B, \Delta} \vee^{\text{addR}_2} \qquad \frac{\Gamma, A \vdash \Delta \quad \Gamma, B \vdash \Delta}{\Gamma, A \vee B \vdash \Delta} \vee^{\text{addL}} \\
\\
\frac{}{\Gamma \vdash \top, \Delta} \top^{\text{addR}} \qquad \frac{}{\Gamma, \mathbf{F} \vdash \Delta} \mathbf{F}^{\text{addL}} \\
\\
\frac{\Gamma, A \vdash \Delta}{\Gamma \vdash \neg A, \Delta} \neg\text{R} \qquad \frac{\Gamma \vdash A, \Delta}{\Gamma, \neg A \vdash \Delta} \neg\text{L} \\
\\
\frac{\Gamma, A \vdash \Delta}{\Gamma \vdash A \rightarrow B, \Delta} \rightarrow^{\text{addR}_1} \qquad \frac{\Gamma \vdash B, \Delta}{\Gamma \vdash A \rightarrow B, \Delta} \rightarrow^{\text{addR}_2} \qquad \frac{\Gamma \vdash A, \Delta \quad \Gamma, B \vdash \Delta}{\Gamma, A \rightarrow B \vdash \Delta} \rightarrow^{\text{addL}}
\end{array}$$

On a choisi de représenter les séquents par deux suites de formules ce qui induit la présence de la règle d'échange. C'est la manière la plus propre de présenter les choses (en particulier en ce qui concerne la notion d'occurrence de formule), mais dans la pratique on considérera plutôt une représentation des séquents par deux multi-ensembles (ce qui transforme la règle d'échange en une égalité). En cas de doute c'est la représentation avec échange explicite qui fera foi.

Proposition 1 (Correction et Complétude)

Le calcul des séquents pour la logique minimale (i.e. avec pour seul connecteur \rightarrow) est correct et complet par rapport au système de Hilbert.

DÉMONSTRATION : On prouve tout d'abord la correction à l'aide du théorème de complétude de la logique classique : si $\vdash A$ est prouvable dans LK, on vérifie, par induction sur la taille de la preuve, que A est vraie (à la manière décrite [page 8](#)) donc A est prouvable dans le système de Hilbert.

Pour la complétude, on prouve par récurrence sur la longueur n de la preuve $A_1 \dots A_n$ de A_n dans le système de Hilbert que pour tout $1 \leq i \leq n$, $\vdash A_i$ est prouvable dans LK.

Si A_n est une instance de l'axiome $A \rightarrow (B \rightarrow A)$, par récurrence $\vdash A_1, \dots, \vdash A_{n-1}$ sont prouvables dans LK, et il suffit d'instancier la preuve :

$$\frac{\frac{\frac{\overline{A \vdash A} \text{ ax}}{A, B \vdash A} \text{ wkL}}{A \vdash B \rightarrow A} \rightarrow^{\text{mul}} \text{R}}{\vdash A \rightarrow (B \rightarrow A)} \rightarrow^{\text{mul}} \text{R}}$$

pour prouver $\vdash A_n$.

De même dans le cas de l'application d'une instance de $(A \rightarrow (B \rightarrow C)) \rightarrow ((A \rightarrow B) \rightarrow (A \rightarrow C))$:

$$\frac{\frac{\frac{\frac{\overline{C \vdash C} \text{ ax}}{B \rightarrow C, A \rightarrow B, A \vdash C} \rightarrow^{\text{mul}} \text{L}}{\frac{\frac{\frac{\overline{B \vdash B} \text{ ax}}{A \rightarrow B, A \vdash B} \rightarrow^{\text{mul}} \text{L}}{A \rightarrow (B \rightarrow C), A \rightarrow B, A, A \vdash C} \rightarrow^{\text{mul}} \text{L}}{A \rightarrow (B \rightarrow C), A \rightarrow B, A \vdash C} \text{ ctrL}}{A \rightarrow (B \rightarrow C), A \rightarrow B \vdash A \rightarrow C} \rightarrow^{\text{mul}} \text{R}}{A \rightarrow (B \rightarrow C) \vdash (A \rightarrow B) \rightarrow (A \rightarrow C)} \rightarrow^{\text{mul}} \text{R}}{\vdash (A \rightarrow (B \rightarrow C)) \rightarrow ((A \rightarrow B) \rightarrow (A \rightarrow C))} \rightarrow^{\text{mul}} \text{R}}{\frac{\overline{A \vdash A} \text{ ax}}{A \rightarrow (B \rightarrow C), A \rightarrow B, A, A \vdash C} \rightarrow^{\text{mul}} \text{L}}$$

Et encore idem pour $((A \rightarrow B) \rightarrow A) \rightarrow A$:

$$\frac{\frac{\frac{\frac{\overline{A \vdash A} \text{ ax}}{A \vdash B, A} \text{ wkR}}{A \vdash A} \text{ ax}}{\vdash A \rightarrow B, A} \rightarrow^{\text{mul}} \text{R}}{\frac{(A \rightarrow B) \rightarrow A \vdash A, A}{(A \rightarrow B) \rightarrow A \vdash A} \text{ ctrR}}{\vdash ((A \rightarrow B) \rightarrow A) \rightarrow A} \rightarrow^{\text{mul}} \text{R}}$$

Enfin si A_n est obtenue par application de la règle de *modus ponens* entre la formule A_i et la formule A_j , alors $A_i = A_j \rightarrow A_n$ et par hypothèse de récurrence $\vdash A_i$ et $\vdash A_j$ sont prouvables dans LK, il reste à montrer $\vdash A_n$:

$$\frac{\frac{\frac{\overline{A_n \vdash A_n} \text{ ax}}{A_j \rightarrow A_n \vdash A_n} \rightarrow^{\text{mul}} \text{L}}{\vdash A_j \rightarrow A_n} \rightarrow^{\text{mul}} \text{L}}{\vdash A_n} \text{ cut}$$

□

Remarque : La preuve précédente utilise *toutes* les règles du calcul des séquents pour le connecteur \rightarrow ainsi que toutes celles des groupes identité (multiplicatif par exemple ici) et structurel.

Calcul des séquents du 1^{er} ordre

Pour obtenir la logique du premier ordre, on étend les formules à partir d'un langage de termes du premier ordre par :

$$A ::= Xt_1 \dots t_n \mid \dots \mid \forall xA \mid \exists xA$$

La taille d'une formule est $|Xt_1 \dots t_n| = 1$, ..., $|\forall xA| = |A| + 1$ et $|\exists xA| = |A| + 1$ (ainsi $|A[t/x]| = |A|$).

$$\frac{\Gamma \vdash A, \Delta}{\Gamma \vdash \forall xA, \Delta} \forall \text{R} \qquad \frac{\Gamma, A[t/x] \vdash \Delta}{\Gamma, \forall xA \vdash \Delta} \forall \text{L}$$

$$\frac{\Gamma \vdash A[t/x], \Delta}{\Gamma \vdash \exists xA, \Delta} \exists \text{R} \qquad \frac{\Gamma, A \vdash \Delta}{\Gamma, \exists xA \vdash \Delta} \exists \text{L}$$

avec la contrainte que x ne doit pas être libre dans Γ ni Δ pour les règles $\forall R$ et $\exists L$.

Exemple 2

Une preuve en calcul des prédicats classique :

$$\begin{array}{c}
\frac{}{Py \vdash Py} ax \\
\frac{}{Px_0, Py \vdash Py} wkL \\
\frac{}{Px_0, Py \vdash Py, Py'} wkR \\
\frac{}{Px_0 \vdash Py, Py \rightarrow Py'} \rightarrow^{mul} R \\
\frac{}{\vdash Px_0 \rightarrow Py, Py \rightarrow Py'} \rightarrow^{mul} R \\
\frac{}{\vdash Px_0 \rightarrow Py, \forall y' Py \rightarrow Py'} \forall R \\
\frac{}{\vdash Px_0 \rightarrow Py, \exists x \forall y Px \rightarrow Py} \exists R \\
\frac{}{\vdash \forall y Px_0 \rightarrow Py, \exists x \forall y Px \rightarrow Py} \forall R \\
\frac{}{\vdash \exists x \forall y Px \rightarrow Py, \exists x \forall y Px \rightarrow Py} \exists R \\
\frac{}{\vdash \exists x \forall y Px \rightarrow Py} ctrR
\end{array}$$

Exercice 9

Donner toutes les contraintes sur les variables pour que cette preuve soit correcte.

CORRECTION : Il faut $x_0 \neq y$, $x_0 \neq y'$ et $y \neq y'$.

Symétries, équivalences de connecteurs, ...

Il existe plusieurs manières d'enrichir un système logique avec de nouvelles règles sans en changer l'expressivité. On distinguera principalement règles *dérivables* (c'est le cas qui nous intéressera principalement) et *admissibles*.

Définition 1 (Règles dérivables et admissibles)

Une règle $\frac{\Gamma_1 \vdash \Delta_1 \cdots \Gamma_n \vdash \Delta_n}{\Gamma \vdash \Delta}$ est *dérivable* si il existe une preuve qui, partant des prémisses $\Gamma_i \vdash \Delta_i$, permet de dériver $\Gamma \vdash \Delta$.

Une règle $\frac{\Gamma_1 \vdash \Delta_1 \cdots \Gamma_n \vdash \Delta_n}{\Gamma \vdash \Delta}$ est *admissible* si dès que les prémisses $\Gamma_i \vdash \Delta_i$ sont prouvables, la conclusion $\Gamma \vdash \Delta$ est également prouvable.

Remarque : Ainsi toute règle dérivable est admissible, mais la réciproque n'est pas toujours vraie, notamment si on quitte la logique classique (par exemple $\frac{A \rightarrow C \vdash A \vee B}{\vdash ((A \rightarrow C) \rightarrow A) \vee ((A \rightarrow C) \rightarrow B)}$)

en logique intuitionniste ou $\frac{\vdash A \& B}{\vdash A \otimes B}$ en logique linéaire).

Le calcul des séquents possède les propriétés importantes suivantes :

- Il existe une symétrie (presque) parfaite entre les règles gauches et les règles droites. Étant donnée une règle gauche, si on fait passer les formules actives de l'autre côté du signe \vdash et si on modifie comme il faut le connecteur principal, on obtient une règle droite (et réciproquement).

La symétrie est encore plus simple dans le cas du groupe identité et du groupe structurel.

- La symétrie précédente permet d'associer une *dualité* entre connecteurs de la manière suivante (les règles gauches de l'un correspondent aux règles droites de l'autre et réciproquement) :

$$\begin{array}{ccc}
\wedge & \leftrightarrow & \vee \\
\top & \leftrightarrow & \text{F} \\
\neg & \leftrightarrow & \neg \\
\forall & \leftrightarrow & \exists
\end{array}$$

À cette dualité correspondent les *lois de De Morgan* qui permettent de faire commuter la négation et les autres connecteurs :

$$\begin{aligned}
\neg(A \vee B) &\dashv\vdash \neg A \wedge \neg B \\
\neg(A \wedge B) &\dashv\vdash \neg A \vee \neg B \\
\neg \mathbf{T} &\dashv\vdash \mathbf{F} \\
\neg \mathbf{F} &\dashv\vdash \mathbf{T} \\
\neg(\forall x A) &\dashv\vdash \exists x \neg A \\
\neg(\exists x A) &\dashv\vdash \forall x \neg A
\end{aligned}$$

ainsi également que le cas trivial $\neg(\neg A) \dashv\vdash \neg\neg A$ (puisque \neg est auto-dual).

- Certaines règles sont redondantes. Ainsi il est possible de définir certains connecteurs à partir d'autres (et les règles du connecteur défini sont dérivables à partir de celles des connecteurs qui le définissent), par exemple :

$$\begin{aligned}
A \rightarrow B &= \neg A \vee B \\
\neg A &= A \rightarrow \mathbf{F} \\
\mathbf{F} &= A \wedge \neg A
\end{aligned}$$

- Les règles additives sont dérivables à partir des règles multiplicatives et réciproquement (modulo les règles structurelles). C'est en particulier le cas pour le groupe identité et nous ne retiendrons désormais que le groupe identité multiplicatif plus "atomique" que le groupe identité additif. Ainsi :

$$\begin{array}{c}
\frac{\frac{\frac{A \vdash A}{\Gamma, A \vdash A} ax^{mul}}{\Gamma, A \vdash A} wkL}{\Gamma, A \vdash A, \Delta} wkR \qquad \frac{}{A \vdash A} ax^{add} \\
\\
\frac{\frac{\frac{\Gamma \vdash A, \Delta \quad \Gamma, A \vdash \Delta}{\Gamma, \Gamma \vdash \Delta, \Delta} cut^{mul}}{\Gamma \vdash \Delta, \Delta} ctrL}{\Gamma \vdash \Delta} ctrR \qquad \frac{\frac{\frac{\Gamma \vdash A, \Delta}{\Gamma, \Gamma' \vdash A, \Delta} wkL}{\Gamma, \Gamma' \vdash A, \Delta, \Delta'} wkR} \quad \frac{\frac{\frac{\Gamma', A \vdash \Delta'}{\Gamma, \Gamma', A \vdash \Delta'} wkL}{\Gamma, \Gamma', A \vdash \Delta, \Delta'} wkR}}{\Gamma, \Gamma' \vdash \Delta, \Delta'} cut^{add} \\
\\
\frac{\frac{\Gamma \vdash A, \Delta}{\Gamma \vdash A, B, \Delta} wkR}{\Gamma \vdash A \vee B, \Delta} \vee^{mul}R \qquad \frac{\frac{\Gamma \vdash B, \Delta}{\Gamma \vdash A, B, \Delta} wkR}{\Gamma \vdash A \vee B, \Delta} \vee^{mul}R \qquad \frac{\frac{\frac{\Gamma \vdash A, B, \Delta}{\Gamma \vdash A \vee B, B, \Delta} \vee^{add}R_1}{\Gamma \vdash A \vee B, A \vee B, \Delta} \vee^{add}R_2}}{\Gamma \vdash A \vee B, \Delta} ctrR
\end{array}$$

Remarque : Lors de la description de la dualité de De Morgan ci-dessus, on a ignoré le connecteur \rightarrow . Il peut en fait parfaitement rentrer dans ce cadre à condition de définir le connecteur peu usuel $A - B$ dont les règles peuvent être obtenues à partir de la définition $A - B = A \wedge \neg B$.

Exercice 10

Soit A une (occurrence de) sous-formule d'une formule B , on dit que A est en *occurrence positive* (resp. *occurrence négative*) dans B si elle se situe un nombre pair (resp. impair) de fois soit à

gauche d'un connecteur \rightarrow soit sous un connecteur \neg :

$$\begin{array}{ll}
pos(Xt_1 \dots t_n) = \{Xt_1 \dots t_n\} & neg(Xt_1 \dots t_n) = \emptyset \\
pos(\neg A) = neg(A) \cup \{\neg A\} & neg(\neg A) = pos(A) \\
pos(A \wedge B) = pos(A) \cup pos(B) \cup \{A \wedge B\} & neg(A \wedge B) = neg(A) \cup neg(B) \\
pos(A \vee B) = pos(A) \cup pos(B) \cup \{A \vee B\} & neg(A \vee B) = neg(A) \cup neg(B) \\
pos(A \rightarrow B) = neg(A) \cup pos(B) \cup \{A \rightarrow B\} & neg(A \rightarrow B) = pos(A) \cup neg(B) \\
pos(\mathbf{T}) = \{\mathbf{T}\} & neg(\mathbf{T}) = \emptyset \\
pos(\mathbf{F}) = \{\mathbf{F}\} & neg(\mathbf{F}) = \emptyset \\
pos(\forall x A) = pos(A) \cup \{\forall x A\} & neg(\forall x A) = neg(A) \\
pos(\exists x A) = pos(A) \cup \{\exists x A\} & neg(\exists x A) = neg(A)
\end{array}$$

Soit A une (occurrence de) sous-formule d'une formule B d'un séquent s , A est positive dans s si elle est positive dans B et B est à droite dans s ou si elle est négative dans B et B est à gauche dans s (A est négative dans s sinon).

Montrer que A est positive (resp. négative) dans le séquent conclusion d'une preuve si et seulement si elle l'est également dans tous les séquents où elle apparaît (attention il ne s'agit que des apparitions de "ce" A pas d'autres occurrences égales à A "par hasard", distinction qu'il conviendrait de formaliser proprement, on parle parfois de *classe d'identité de formule*).

Calcul des séquents monolatère

On a $\neg\neg A \vdash A$ et $A \vdash \neg\neg A$ et, en s'appuyant sur les symétries gauche / droite pour les règles des connecteurs duaux et les lois de De Morgan, on peut même considérer que $A = \neg\neg A$: il revient au même par exemple d'appliquer la règle droite d'un connecteur \circ pour obtenir $A \circ B$ ou de passer à gauche par négation, appliquer la règle du connecteur dual \diamond pour obtenir $(\neg A) \diamond (\neg B)$ et revenir à droite par négation pour obtenir $\neg(\neg A \diamond \neg B)$ ($= \neg\neg(A \circ B)$ par De Morgan).

Autrement dit, les règles de De Morgan permettent de faire commuter la négation avec tous les autres connecteurs (on va oublier \rightarrow pour se simplifier la vie), on peut donc la faire descendre au plus bas.

Définition 2 (Négation involutive définie)

Au lieu de considérer des formules données par la grammaire :

$$A ::= Xt_1 \dots t_n \mid \neg A \mid A \wedge A \mid A \vee A \mid \mathbf{T} \mid \mathbf{F} \mid \forall x A \mid \exists x A$$

On se restreint à :

$$A ::= Xt_1 \dots t_n \mid \neg Xt_1 \dots t_n \mid A \wedge A \mid A \vee A \mid \mathbf{T} \mid \mathbf{F} \mid \forall x A \mid \exists x A$$

On définit $\neg A$ pour $A \neq Xt_1 \dots t_n$ par :

$$\begin{aligned}
\neg(\neg Xt_1 \dots t_n) &= Xt_1 \dots t_n \\
\neg(A \wedge B) &= \neg A \vee \neg B \\
\neg(A \vee B) &= \neg A \wedge \neg B \\
\neg\mathbf{T} &= \mathbf{F} \\
\neg\mathbf{F} &= \mathbf{T} \\
\neg(\forall x A) &= \exists x \neg A \\
\neg(\exists x A) &= \forall x \neg A
\end{aligned}$$

ainsi $A = \neg\neg A$.

On peut réécrire les règles du calcul des séquents en remplaçant $\Gamma \vdash \Delta$ par $\vdash \neg\Gamma, \Delta$ (on ne garde que le groupe identité multiplicatif car on a vu que le groupe identité additif est alors redondant, on discutera le cas des groupes logiques à la [section 1.2](#) ; on oublie également l'implication qui est définissable et dont les règles sont dérivables). Les règles de la négation deviennent l'identité.

$$\begin{array}{c}
\frac{}{\vdash A, \neg A} \text{ ax} \qquad \frac{\vdash \Gamma, A \quad \vdash \Delta, \neg A}{\vdash \Gamma, \Delta} \text{ cut} \\
\\
\frac{\vdash \Gamma, A, A}{\vdash \Gamma, A} \text{ ctr} \qquad \frac{\vdash \Gamma}{\vdash \Gamma, A} \text{ wk} \\
\\
\frac{\vdash \Gamma, A \quad \vdash \Delta, B}{\vdash \Gamma, \Delta, A \wedge B} \wedge^{\text{mul}} \qquad \frac{\vdash \Gamma, A, B}{\vdash \Gamma, A \vee B} \vee^{\text{mul}} \\
\\
\frac{\vdash \Gamma, A \quad \vdash \Gamma, B}{\vdash \Gamma, A \wedge B} \wedge^{\text{add}} \qquad \frac{\vdash \Gamma, A}{\vdash \Gamma, A \vee B} \vee_1^{\text{add}} \qquad \frac{\vdash \Gamma, B}{\vdash \Gamma, A \vee B} \vee_2^{\text{add}} \\
\\
\frac{}{\vdash \top} \top^{\text{mul}} \qquad \frac{\vdash \Gamma}{\vdash \Gamma, \text{F}} \text{F}^{\text{mul}} \qquad \frac{}{\vdash \Gamma, \text{T}} \text{T}^{\text{add}} \\
\\
\frac{\vdash \Gamma, A}{\vdash \Gamma, \forall x A} \forall \qquad \frac{\vdash \Gamma, A[t/x]}{\vdash \Gamma, \exists x A} \exists
\end{array}$$

avec la contrainte que x ne doit pas être libre dans Γ pour la règle \forall .

Ce système n'est pas forcément plus confortable pour écrire des preuves mais l'est très nettement pour étudier les propriétés de LK puisqu'on a essentiellement divisé le nombre de règles par deux.

Exemple 3 (Distributivité)

$A \wedge (B \vee C) \leftrightarrow (A \wedge B) \vee (A \wedge C)$ et $A \vee (B \wedge C) \leftrightarrow (A \vee B) \wedge (A \vee C)$

$$\frac{\frac{\frac{\frac{}{\vdash \neg A, A} \text{ ax}}{\vdash \neg A, \neg A} \text{ ax}}{\vdash \neg A, \neg A, \neg B \wedge \neg C, A \wedge B, A \wedge C} \wedge^{\text{mul}}}{\vdash \neg A, \neg A, \neg B \wedge \neg C, A \wedge B, A \wedge C} \wedge^{\text{mul}}}{\vdash \neg A, \neg B \wedge \neg C, (A \wedge B) \vee (A \wedge C)} \vee^{\text{mul}}}{\vdash \neg A \vee (\neg B \wedge \neg C), (A \wedge B) \vee (A \wedge C)} \vee^{\text{mul}}$$

Réversibilité / irréversibilité

Lorsque l'on s'intéresse à construire une dérivation en calcul des séquents dont la conclusion est un séquent donné, on utilise les règles de bas en haut et il est important de remarquer que certaines règles peuvent être appliquées de manière automatique.

La définition même d'une règle est basée sur le fait que s'il est possible de dériver les prémisses alors on autorise à dériver la conclusion. Le contraire est en général faux, on peut dériver $\vdash X \vee \neg X$ mais ce n'est pas pour ça que l'on peut dériver $\vdash X$ (ni $\vdash \neg X$) qui est la prémisses correspondante de la règle \vee_1^{add} (ou \vee_2^{add}).

On dit qu'une règle est *réversible* si lorsque sa conclusion est dérivable alors ses prémisses sont dérivables. Autrement dit les règles inverses sont admissibles (en général on utilisera plutôt dérivables). Les autres règles sont dites *irréversibles*.

Ces notions sont surtout intéressantes dans le cas des règles logiques. En effet cela permet de savoir lorsque l'on peut automatiquement détruire un connecteur. Par contre la règle de contraction est réversible mais l'appliquer de manière systématique donnerait lieu à une preuve infinie.

Les règles logiques réversibles sont : \vee^{mul} , \wedge^{add} , \mathbf{F}^{mul} , \mathbf{T}^{mul} et \mathbf{T}^{add} (cas un peu dégénéré voir [section 5.2](#) où l'on parlera de connecteur réversible) et \forall .

$$\frac{\frac{\frac{}{\vdash \neg A, A} ax}{\vdash \Gamma, A \vee B} \quad \frac{\frac{\frac{}{\vdash \neg A, A} ax} \quad \frac{\frac{}{\vdash \neg B, B} ax}}{\vdash \neg A \wedge \neg B, A, B} \wedge^{\text{mul}}}{\vdash \Gamma, A, B} cut}{\vdash \Gamma, A, B} cut$$

$$\frac{\frac{\frac{}{\vdash \neg A, A} ax}{\vdash \Gamma, A \wedge B} \quad \frac{\frac{}{\vdash \neg A \vee \neg B, A} \vee_1^{\text{add}}}{\vdash \Gamma, A} cut}{\vdash \Gamma, A} cut \quad \frac{\frac{\frac{}{\vdash \neg B, B} ax}{\vdash \Gamma, A \wedge B} \quad \frac{\frac{}{\vdash \neg A \vee \neg B, B} \vee_2^{\text{add}}}{\vdash \Gamma, B} cut}{\vdash \Gamma, B} cut$$

$$\frac{\frac{}{\vdash \Gamma, \mathbf{F}} \quad \frac{}{\vdash \mathbf{T}} \mathbf{T}^{\text{mul}}}{\vdash \Gamma} cut$$

$$\frac{\frac{}{\vdash \Gamma, \forall x A} \quad \frac{\frac{}{\vdash \neg A, A} ax}{\vdash \exists x \neg A, A} \exists}{\vdash \Gamma, A} cut$$

Les autres règles logiques sont irréversibles, par exemple $\vdash \neg X \vee \neg Y, X \wedge Y$ est dérivable alors que $\vdash \neg X \vee \neg Y, X$ l'est mais pas $\vdash Y$ donc la règle \wedge^{mul} est irréversible.

Exercice 11

Montrer que les autres règles logiques sont bien irréversibles.

Une manière plus intuitive de comprendre la réversibilité est de voir que la conclusion contient toutes les informations nécessaires pour reconstruire les prémisses (ce n'est pas le cas, par exemple, pour \wedge^{mul} où il faut choisir un partage du contexte ni pour \vee_1^{add} et \vee_2^{add} où il faut choisir quel côté du \vee on efface).

1.2 Élimination des coupures

La propriété centrale, essentielle, fondamentale, cruciale, ... du calcul des séquents est *l'élimination des coupures* qui consiste à transformer une preuve pour faire disparaître la règle de coupure.

Cas clefs

Un cas simple (et central) est celui où les deux formules coupées sont principales dans une règle logique. On transforme localement un morceau de dérivation :

$$\frac{\frac{\frac{}{\vdash \Gamma, A} \quad \frac{}{\vdash \Delta, B}}{\vdash \Gamma, \Delta, A \wedge B} \wedge^{\text{mul}} \quad \frac{\frac{}{\vdash \Xi, \neg A, \neg B}}{\vdash \Xi, \neg A \vee \neg B} \vee^{\text{mul}}}{\vdash \Gamma, \Delta, \Xi} cut \quad \rightsquigarrow \quad \frac{\frac{}{\vdash \Gamma, A} \quad \frac{\frac{}{\vdash \Delta, B} \quad \frac{}{\vdash \Xi, \neg A, \neg B}}{\vdash \Delta, \Xi, \neg A} cut}{\vdash \Gamma, \Delta, \Xi} cut} cut$$

on a en fait deux choix ici.

$$\begin{array}{c}
\frac{\frac{\frac{\vdash \Gamma, A \quad \vdash \Gamma, B}{\vdash \Gamma, A \wedge B} \wedge^{\text{add}} \quad \frac{\vdash \Delta, \neg A}{\vdash \Delta, \neg A \vee \neg B} \vee_1^{\text{add}}}{\vdash \Gamma, \Delta} \text{cut}}{\vdash \Gamma, \Delta} \rightsquigarrow \frac{\vdash \Gamma, A \quad \vdash \Delta, \neg A}{\vdash \Gamma, \Delta} \text{cut} \\
\\
\frac{\frac{\frac{\vdash \Gamma, A \quad \vdash \Gamma, B}{\vdash \Gamma, A \wedge B} \wedge^{\text{add}} \quad \frac{\vdash \Delta, \neg B}{\vdash \Delta, \neg A \vee \neg B} \vee_2^{\text{add}}}{\vdash \Gamma, \Delta} \text{cut}}{\vdash \Gamma, \Delta} \rightsquigarrow \frac{\vdash \Gamma, B \quad \vdash \Delta, \neg B}{\vdash \Gamma, \Delta} \text{cut} \\
\\
\frac{\frac{\frac{\vdash \top}{\vdash \top} \top^{\text{mul}} \quad \frac{\vdash \Gamma}{\vdash \Gamma, \text{F}} \text{F}^{\text{mul}}}{\vdash \Gamma} \text{cut}}{\vdash \Gamma} \rightsquigarrow \vdash \Gamma \\
\\
\frac{\frac{\frac{\vdash \Gamma, A}{\vdash \Gamma, \forall x A} \forall \quad \frac{\vdash \Delta, \neg A[t/x]}{\vdash \Delta, \exists x \neg A} \exists}{\vdash \Gamma, \Delta} \text{cut}}{\vdash \Gamma, \Delta} \rightsquigarrow \frac{[t/x]}{\vdash \Gamma, A[t/x] \quad \vdash \Delta, \neg A[t/x]} \text{cut}
\end{array}$$

la condition $x \notin \Gamma$ est ici cruciale pour que la substitution dans la sous-dérivation de gauche ne modifie pas Γ .

$$\begin{array}{c}
\frac{\frac{\frac{\vdash \Gamma, A \quad \vdash \Delta, B}{\vdash \Gamma, \Delta, A \wedge B} \wedge^{\text{mul}} \quad \frac{\vdash \Xi, \neg A}{\vdash \Xi, \neg A \vee \neg B} \vee_1^{\text{add}}}{\vdash \Gamma, \Delta, \Xi} \text{cut}}{\vdash \Gamma, \Delta, \Xi} \rightsquigarrow \frac{\frac{\vdash \Gamma, A \quad \vdash \Xi, \neg A}{\vdash \Gamma, \Xi} \text{cut}}{\vdash \Gamma, \Delta, \Xi} \text{wk} \\
\\
\frac{\frac{\frac{\vdash \Gamma, A \quad \vdash \Gamma, B}{\vdash \Gamma, A \wedge B} \wedge^{\text{add}} \quad \frac{\vdash \Delta, \neg A, \neg B}{\vdash \Delta, \neg A \vee \neg B} \vee^{\text{mul}}}{\vdash \Gamma, \Delta} \text{cut}}{\vdash \Gamma, \Delta} \rightsquigarrow \frac{\frac{\vdash \Gamma, B \quad \vdash \Delta, \neg A, \neg B}{\vdash \Gamma, \Delta, \neg A} \text{cut}}{\frac{\vdash \Gamma, A \quad \vdash \Gamma, \Delta}{\vdash \Gamma, \Delta} \text{ctr}} \text{cut}
\end{array}$$

On constate que si on mélange règles additives et multiplicatives, il est nécessaire d'introduire des règles structurelles (ceci correspond en fait à repasser par le codage des règles d'un style dans l'autre et à appliquer le cas clef additif/additif ou multiplicatif/multiplicatif).

Exercice 12

Écrire les autres cas possibles.

La possibilité d'écrire ces cas clefs d'élimination des coupures (notamment dans les cas additif/additif ou multiplicatif/multiplicatif) est un signe de la bonne interaction entre les différentes règles des connecteurs duaux (ou entre règles gauches et règles droites de chaque connecteur si on revient en bilatère).

Additif / multiplicatif

Les cas clefs de l'élimination des coupures nous montrent que pour minimiser l'apparition de règles structurelles, il faut grouper les règles logiques entre règles additives et règles multiplicatives ce qui justifie le choix de dénomination pour les règles 0-aires et unaires. On a déjà vu que ces règles sont inter-prouvables, on peut donc se contenter de ne garder que les règles additives ou que les règles multiplicatives.

On obtient ainsi le "carré des connecteurs" :

$$\begin{array}{ccc}
\wedge^{\text{add}} & \text{—} & \wedge^{\text{mul}} \\
| & & | \\
\vee^{\text{add}} & \text{—} & \vee^{\text{mul}}
\end{array}$$

- horizontalement : conjonction vs. disjonction
- verticalement : additif vs. multiplicatif
- en diagonale : réversible vs. irréversible

Ces deux derniers choix donnent quatre groupes de règles qui sont complets : une règle de conjonction et une règle de disjonction ce qui permet de dériver les autres. On verra que les deux ont leur intérêt.

Preuve de l'élimination des coupures

Théorème 1 (Gentzen)

Soit π une preuve du séquent $\vdash \Gamma$ en calcul des séquents, il existe une preuve π' de $\vdash \Gamma$ n'utilisant pas la règle de coupure.

On utilise ici la méthode d'“élimination des coupures par substitution” plutôt que la méthode originelle de Gentzen.

DÉMONSTRATION : Soit C une coupure dans π :

$$\frac{\frac{\vdots}{\vdash \Gamma, A} R_1 \quad \frac{\vdots}{\vdash \Delta, \neg A} R_2}{\vdash \Gamma, \Delta} C$$

on définit le *type* de C par :

- C est une coupure *logique* si R_1 (resp. R_2) est une règle logique dans laquelle A (resp. $\neg A$) est principale ;
- C est une coupure *structurelle simple* si seule l'une des deux l'est ;
- C est une coupure *structurelle double* si aucune des deux ne l'est.

L'élimination des coupures logiques est donnée par les cas clefs que l'on a vus précédemment.

Pour une coupure structurelle, l'élimination est définie de la manière suivante :

- On choisit une prémisses de C pour laquelle elle est structurelle (disons π_1).
- On considère l'arbre de la formule A dans la preuve π_1 , dont les feuilles sont soit des règles d'affaiblissement (ou de manière équivalente une règle T^{add}), soit des axiomes, soit des règles logiques dans lesquelles A est principale.
- Pour une feuille affaiblissement, on remplace la règle d'affaiblissement sur A par des règles d'affaiblissement sur Δ .
- Pour une feuille axiome, on remplace l'axiome $\vdash A, \neg A$ par π_2 (qui prouve $\vdash \Delta, \neg A$).
- Pour une feuille logique, on insère, sous la conclusion $\vdash \Xi, A$ de cette règle, une coupure avec π_2 :

$$\frac{\frac{\vdots}{\vdash \Xi, A} \quad \frac{\pi_2}{\vdash \Delta, \neg A}}{\vdash \Xi, \Delta} \textit{cut}$$

- On remplace ainsi toutes les feuilles de l'arbre structurel de A dans π_1 par des Δ . On modifie alors toutes les règles concernées par cet arbre de manière à remplacer partout A par Δ et π_1 est ainsi transformée en une preuve π'_1 de $\vdash \Gamma, \Delta$.

On doit désormais montrer que l'on peut appliquer cette procédure de manière à éliminer les coupures.

À toute coupure C de π , on associe la paire (n, k) , appelée *poids* de C , où n est la taille de la formule coupée A et k vaut 0 si C est logique, 1 si C est structurelle simple et 2 si C est structurelle double. Le *poids* de π est le multi-ensemble des poids de ses coupures.

Les poids de coupures sont munis de l'ordre bien fondé donné par l'ordre lexicographique. On a les remarques suivantes sur l'évolution des poids, lors d'une étape d'élimination d'une coupure C :

- Soit C' une coupure engendrée par C avec C structurelle, c'est une coupure sur la même formule A et qui est logique si C est structurelle simple et qui est structurelle simple si C est structurelle double. Ainsi le poids de C' est strictement inférieur au poids de C .
- Soit C' une coupure engendrée par C avec C logique, c'est une coupure sur une sous-formule stricte de A donc le poids de C' est strictement inférieur au poids de C .
- Soit C_0 une coupure située au-dessous de C dans π , lors de l'élimination de C , la formule coupée de C_0 ne change pas. De plus soit son type n'est pas modifié, soit C a pour conclusion l'une des prémisses de C_0 et le type de C_0 peut passer de structurelle double à structurelle simple ou de structurelle simple à logique. Ainsi, soit le poids de C_0 n'est pas modifié, soit il diminue.

Les poids des preuves sont ordonnés par l'ordre multi-ensemble (bien fondé) engendré par l'ordre bien fondé sur les poids de coupures. Pour montrer que l'on peut éliminer les coupures dans π , il suffit donc de montrer que l'on peut toujours choisir une coupure et l'éliminer en faisant diminuer le poids de la preuve.

Soit C une coupure de π telle qu'il n'y ait aucune coupure ni dans π_1 ni dans π_2 . On note π' la preuve obtenue en éliminant C dans π . Les coupures de π' sont les mêmes que celles de π (qui sont soit au-dessous de C et leur poids peut diminuer, soit dans une position incomparable avec celle de C et leur poids n'est pas modifié), sauf C qui disparaît et sauf celles créées par l'élimination de C (éventuellement aucune) et dont les poids sont strictement inférieurs à celui de C . Ainsi le poids de π' est obtenu à partir de celui de π en supprimant le poids de C , en ajoutant des poids strictement inférieurs pour les coupures créées et en remplaçant éventuellement le poids de certaines coupures par leur nouveau poids plus petit. On obtient que le poids de π' est strictement inférieur à celui de π . \square

Remarque : On peut montrer (difficile) que la procédure d'élimination des coupures que l'on a décrite est en fait fortement normalisante.

Attention la preuve naïve, qui définirait des étapes plus élémentaires par simples commutations de paires de règles ne fonctionne pas, elle peut donner lieu à des boucles :

$$\frac{\frac{\frac{\vdash \Gamma, A, B \quad \vdash \Delta, \neg B}{\vdash \Gamma, \Delta, A} \text{ cut} \quad \vdash \Xi, \neg A}{\vdash \Gamma, \Delta, \Xi} \text{ cut}}{\vdash \Gamma, \Delta, \Xi} \text{ cut} \quad \rightsquigarrow \quad \frac{\frac{\frac{\vdash \Gamma, A, B \quad \vdash \Xi, \neg A}{\vdash \Gamma, \Xi, B} \text{ cut} \quad \vdash \Delta, \neg B}{\vdash \Gamma, \Delta, \Xi} \text{ cut}}{\vdash \Gamma, \Delta, \Xi} \text{ cut}}$$

ou :

$$\frac{\frac{\frac{\vdash \Gamma, A \quad \frac{\vdash \neg A, A}{\vdash \Gamma, A} \text{ ax}}{\vdash \Gamma, A} \text{ cut} \quad \vdash \Delta, \neg A}{\vdash \Gamma, \Delta} \text{ cut}}{\vdash \Gamma, \Delta} \text{ cut} \quad \rightsquigarrow \quad \frac{\frac{\frac{\vdash \neg A, A}{\vdash \Gamma, A} \text{ ax} \quad \vdash \Delta, \neg A}{\vdash \Gamma, \Delta} \text{ cut}}{\vdash \Gamma, \Delta} \text{ cut}}$$

et même pire :

$$\frac{\frac{\frac{\frac{\vdash A, \neg A}{\vdash A, \neg A} \text{ ax} \quad \frac{\vdash A, \neg A}{\vdash A, \neg A} \text{ ax}}{\vdash A, A, \neg A \wedge \neg A} \wedge^{\text{mul}} \quad \frac{\frac{\frac{\vdash A, \neg A}{\vdash A, \neg A} \text{ ax} \quad \frac{\vdash A, \neg A}{\vdash A, \neg A} \text{ ax}}{\vdash A \wedge A, \neg A, \neg A} \wedge^{\text{mul}}}{\vdash A, \neg A \wedge \neg A} \text{ ctr} \quad \frac{\frac{\frac{\vdash A, \neg A}{\vdash A, \neg A} \text{ ax} \quad \frac{\vdash A, \neg A}{\vdash A, \neg A} \text{ ax}}{\vdash A \wedge A, \neg A} \text{ ctr}}{\vdash A \wedge A, \neg A \wedge \neg A} \text{ cut} \quad \rightsquigarrow \quad \dots$$

Sous-formules, non contradiction

Une conséquence majeure du théorème d'élimination des coupures est la *propriété de la sous-formule* :

Proposition 2 (Sous-formule)

Si A est prouvable en calcul des séquents alors A est prouvable en n'utilisant que des sous-formules de A .

DÉMONSTRATION : Il suffit de constater en regardant chaque règle de bas en haut que cette propriété n'est violée que par la coupure (que l'on peut éliminer!). \square

En particulier, il n'est nécessaire d'utiliser que les règles logiques portant sur les connecteurs présents dans la formule que l'on veut démontrer.

Proposition 3 (Non contradiction)

Les séquents $\vdash \mathbf{F}$ et \vdash ne sont pas prouvables en calcul des séquents.

DÉMONSTRATION : Si $\vdash \mathbf{F}$ est prouvable alors \vdash aussi :

$$\frac{\vdash \mathbf{F} \quad \overline{\vdash \mathbf{T}} \text{ T}^{\text{mul}}}{\vdash} \text{ cut}$$

Si \vdash est prouvable, on considère une preuve sans coupure et on constate qu'aucune dernière règle n'a pu être appliquée. \square

Expansion des axiomes

La règle d'axiome peut s'appliquer à une formule arbitraire. Il est en fait suffisant de se la donner pour les variables : $\vdash X, \neg X$, et elle devient alors *dérivable* pour tous les autres connecteurs (on peut même choisir un style additif ou multiplicatif).

$$\frac{\frac{\overline{\vdash \neg A, A} \text{ ax} \quad \overline{\vdash \neg B, B} \text{ ax}}{\vdash \neg A \wedge \neg B, A, B} \wedge^{\text{mul}}}{\vdash \neg A \wedge \neg B, A \vee B} \vee^{\text{mul}}$$

$$\frac{\frac{\overline{\vdash \neg A, A} \text{ ax}}{\vdash \neg A \vee \neg B, A} \vee_1^{\text{add}} \quad \frac{\overline{\vdash \neg B, B} \text{ ax}}{\vdash \neg A \vee \neg B, B} \vee_2^{\text{add}}}{\vdash \neg A \vee \neg B, A \wedge B} \wedge^{\text{add}}$$

$$\frac{\overline{\vdash \mathbf{T}} \text{ T}^{\text{mul}}}{\vdash \mathbf{T}, \mathbf{F}} \text{ F}^{\text{mul}}$$

$$\frac{}{\vdash \mathbf{F}, \mathbf{T}} \text{ T}^{\text{add}}$$

$$\frac{\overline{\vdash \neg A, A} \text{ ax}}{\vdash \exists x \neg A, A} \exists$$

$$\frac{}{\vdash \exists x \neg A, \forall x A} \forall$$

La procédure qui transforme un axiome sur A en des axiomes sur les sous-formules de A (et donc sur des variables si on pousse la transformation jusqu'au bout) s'appelle l'*expansion des axiomes*.

Il s'agit là encore d'un signe de bonne interaction entre règles de connecteurs duaux.

Si on reprend les preuves de réversibilité de la [section 1.1](#), on constate qu'elles sont toutes construites sur le même schéma : on prend l'expansion d'axiome correspondant à la règle qui nous intéresse, on constate que la dernière règle est celle qui nous intéresse, on l'enlève et on coupe avec la prémisse de la règle (ce qui revient à couper sur l'expansion d'axiome, à appliquer une "étape commutative" et à retirer la dernière règle qui est celle que l'on veut inverser).

Calcul des séquents réversible sans coupure

On s'intéresse ici au calcul propositionnel uniquement.

Grâce aux inter-dérivabilités de règles, on a vu que l'on peut choisir de ne prendre comme règles logiques que \vee^{mul} , \wedge^{add} , \mathbf{F}^{mul} et \mathbf{T}^{add} qui sont toutes des règles réversibles ! Par ailleurs, on peut supprimer la règle de coupure sans changer l'expressivité.

Supposons que l'on veuille prouver un séquent $\vdash \Gamma$. On travaille de bas en haut. Puisque les règles logiques que l'on a choisies sont toutes réversibles, on peut les appliquer autant que possible et on obtient des séquents qui ne contiennent que des atomes $\vdash X_1, \dots, X_n, \neg Y_1, \dots, \neg Y_k$.

On remarque alors qu'un tel séquent est prouvable si et seulement si il existe $1 \leq i \leq n$ et $1 \leq j \leq k$ tel que $X_i = Y_j$. En effet, si c'est le cas, on applique une règle axiome et des affaiblissements. Réciproquement, les seules règles que l'on peut appliquer sont des contractions, des affaiblissements et des axiomes et on montre le résultat par récurrence sur le nombre de règles appliquées. Or cette propriété correspond exactement à l'axiome additif (que l'on avait mis de côté plus tôt).

On a ainsi montré que la prouvabilité du calcul des séquent est la même que celle du calcul obtenu en prenant comme règles : l'axiome additif et \vee^{mul} , \wedge^{add} , \mathbf{F}^{mul} et \mathbf{T}^{add} .

En utilisant cette formulation du calcul, il est facile de prouver le théorème de complétude propositionnel. On part (de bas en haut) d'un séquent $\vdash A$, on applique (de manière arbitraire) les règles logiques pour les différents connecteurs de A , et on obtient des séquents qui ne contiennent que des atomes. Par réversibilité des règles, A est prouvable si et seulement si tous ces séquents sont prouvables, c'est-à-dire si et seulement si ils contiennent tous une paire d'atomes duaux. Si A n'est pas prouvable on a donc obtenu un séquent qui ne contient pas de paire d'atomes duaux. On définit un modèle de la manière suivante : si X apparaît dans ce séquent on lui attribue la valeur 0, si $\neg X$ apparaît dans ce séquent on attribue à X la valeur 1, et pour les autres variables on choisit des valeurs arbitraires. Ainsi ce séquent a la valeur 0 dans le modèle et on montre que ceci se transmet inductivement à la conclusion donc A est réfutée par le modèle.

Une dérivation de $\vdash A$ dans ce calcul réversible propositionnel sans coupure lu de bas en haut correspond à la mise en forme normale conjonctive de A .

De même on obtient la décidabilité du calcul propositionnel. On a déjà dit que A est prouvable si et seulement si les séquents atomiques obtenus contiennent tous des paires d'atomes duaux ce qui est évidemment décidable.

Renversement

Si on travaille sur des preuves sans coupure, on peut considérer le fait d'introduire une coupure entre une preuve π et une preuve π_0 puis d'éliminer cette coupure comme une opération de transformation de π (la plupart des transformations "intéressantes" sur les preuves peuvent être décrites de cette manière!).

On a rencontré ce type de situation concernant la réversibilité (voir [section 1.1](#) et [Expansion des axiomes](#) page 24). Partant d'une preuve contenant le "connecteur réversible" qui est sans coupure, on introduit une coupure avec une expansion d'axiome. Si on élimine alors la coupure, on obtient une preuve du même séquent mais qui se termine par l'application de la règle d'introduction réversible. De manière globale, la transformation subie par la preuve correspond à faire commuter la règle réversible vers le bas avec toutes les autres règles pour l'amener en conclusion.

Théorème de Herbrand

Concernant la logique du premier ordre, on va prouver le théorème du séquent intermédiaire ainsi qu'une forme simple du théorème de Herbrand (pour les formes prénexes de la forme $\vec{\forall}\vec{\exists}$).

Une formule A est en *forme prénex* si elle s'écrit sous la forme $A = Q_1x_1 \dots Q_nx_nA_0$ où $Q_i \in \{\forall, \exists\}$ ($1 \leq i \leq n$) et A_0 est une formule sans quantificateur. On montre facilement à partir des propriétés suivantes :

$$\begin{array}{ll} (\forall xA) \wedge B \dashv\vdash \forall x(A \wedge B) & \text{si } x \notin B \\ (\forall xA) \vee B \dashv\vdash \forall x(A \vee B) & \text{si } x \notin B \\ (\exists xA) \wedge B \dashv\vdash \exists x(A \wedge B) & \text{si } x \notin B \\ (\exists xA) \vee B \dashv\vdash \exists x(A \vee B) & \text{si } x \notin B \end{array}$$

que toute formule du premier ordre est équivalente en logique classique à une formule en forme prénex.

Grâce aux inter-dérivabilités de règles, on a vu que l'on peut choisir de ne prendre comme règles logiques que \wedge^{mul} , \vee^{add} , \top^{mul} , \forall et \exists . Par ailleurs, on peut supprimer la règle de coupure sans changer l'expressivité.

Dans cette version du calcul des séquents, considérons deux applications consécutives de règles R_1 et R_2 telles que la formule principale de R_1 n'est pas active dans R_2 . Si R_1 est soit *ctr* soit *wk* et si R_2 est soit *ctr* soit *wk* soit \wedge^{mul} soit \vee^{add} , alors R_1 et R_2 commutent :

$$\begin{array}{l} \frac{\frac{\frac{\vdash \Gamma, C, C, A}{\vdash \Gamma, C, A} \text{ctr}}{\vdash \Gamma, C, A \vee B} \vee_1^{\text{add}}}{\vdash \Gamma, C, A \vee B} \text{ctr} \rightsquigarrow \frac{\frac{\vdash \Gamma, C, C, A}{\vdash \Gamma, C, C, A \vee B} \vee_1^{\text{add}}}{\vdash \Gamma, C, A \vee B} \text{ctr} \\ \\ \frac{\frac{\frac{\vdash \Gamma, C, C, B}{\vdash \Gamma, C, B} \text{ctr}}{\vdash \Gamma, C, A \vee B} \vee_2^{\text{add}}}{\vdash \Gamma, C, A \vee B} \text{ctr} \rightsquigarrow \frac{\frac{\vdash \Gamma, C, C, B}{\vdash \Gamma, C, C, A \vee B} \vee_2^{\text{add}}}{\vdash \Gamma, C, A \vee B} \text{ctr} \\ \\ \frac{\frac{\frac{\vdash \Gamma, C, C, A}{\vdash \Gamma, C, A} \text{ctr}}{\vdash \Gamma, \Delta, C, A \wedge B} \wedge^{\text{mul}}}{\vdash \Gamma, \Delta, C, A \wedge B} \wedge^{\text{mul}} \rightsquigarrow \frac{\frac{\frac{\vdash \Gamma, C, C, A}{\vdash \Gamma, \Delta, C, C, A \wedge B} \wedge^{\text{mul}}}{\vdash \Gamma, \Delta, C, A \wedge B} \text{ctr}}{\vdash \Gamma, \Delta, C, A \wedge B} \wedge^{\text{mul}} \\ \\ \frac{\frac{\frac{\frac{\vdash \Gamma, A, A, B, B}{\vdash \Gamma, A, B, B} \text{ctr}}{\vdash \Gamma, A, B} \text{ctr}}{\vdash \Gamma, A, B} \text{ctr} \rightsquigarrow \frac{\frac{\frac{\vdash \Gamma, A, A, B, B}{\vdash \Gamma, A, A, B} \text{ctr}}{\vdash \Gamma, A, B} \text{ctr}}{\vdash \Gamma, A, B} \text{ctr} \\ \\ \frac{\frac{\frac{\vdash \Gamma, A, A}{\vdash \Gamma, A} \text{ctr}}{\vdash \Gamma, A, B} \text{wk} \rightsquigarrow \frac{\frac{\frac{\vdash \Gamma, A, A}{\vdash \Gamma, A, A, B} \text{wk}}{\vdash \Gamma, A, B} \text{ctr}}{\vdash \Gamma, A, B} \text{ctr} \\ \\ \frac{\frac{\frac{\vdash \Gamma, A}{\vdash \Gamma, C, A} \text{wk}}{\vdash \Gamma, C, A \vee B} \vee_1^{\text{add}} \rightsquigarrow \frac{\frac{\frac{\vdash \Gamma, A}{\vdash \Gamma, A \vee B} \vee_1^{\text{add}}}{\vdash \Gamma, C, A \vee B} \text{wk}}{\vdash \Gamma, C, A \vee B} \text{wk} \end{array}$$

$$\frac{\frac{\frac{\vdash \Gamma, C}{\vdash \Gamma, \forall x C} \forall}{\vdash \Gamma, \forall x C, A} wk}{\vdash \Gamma, \forall x C, A} \forall \quad \rightsquigarrow \quad \frac{\frac{\frac{\vdash \Gamma, C}{\vdash \Gamma, C, A} wk}{\vdash \Gamma, \forall x C, A} \forall}{\vdash \Gamma, \forall x C, A} \forall$$

en renommant x au besoin pour qu'elle n'apparaisse pas dans A ni B ni Δ pour l'application des règles \forall .

Théorème 2 (Séquent intermédiaire)

Soit $\vdash \Gamma$ un séquent prouvable ne contenant que des formules en forme préfixe, il existe un séquent $\vdash \Delta$ sans quantificateur, une preuve π de $\vdash \Delta$ et une preuve π' de $\vdash \Gamma$ à partir de $\vdash \Delta$ n'utilisant que des règles structurelles, \forall et \exists .

DÉMONSTRATION : Soit π_0 une preuve de $\vdash \Gamma$ sans coupure, avec axiomes atomiques et des affaiblissements propositionnels telle qu'aucune règle \forall ou \exists n'est appliquée plus haut qu'une règle \wedge^{mul} ou \vee^{add} . La seule règle binaire étant \wedge^{mul} , on peut parler dans une telle preuve de l'application de règle \exists ou \forall la plus haute. Soit $\vdash \Delta$ son séquent prémisse, c'est un séquent sans quantificateur et les règles situées au-dessous ne peuvent être ni \wedge^{mul} ni \vee^{add} .

Il reste à démontrer qu'une telle preuve existe.

Puisque $\vdash \Gamma$ est prouvable, il existe une preuve π_1 sans coupure n'utilisant que les règles \wedge^{mul} , \vee^{add} , \top^{mul} , \forall et \exists et les règles structurelles. On applique l'expansion suivante aux axiomes :

$$\frac{\frac{\frac{\frac{\vdash \neg A, A}{\vdash \neg A \vee \neg B, A} ax}{\vdash \neg A \vee \neg B, A} \vee^{\text{add}} \quad \frac{\frac{\frac{\vdash \neg B, B}{\vdash \neg A \vee \neg B, B} ax}{\vdash \neg A \vee \neg B, B} \vee^{\text{add}}}{\frac{\frac{\vdash \neg A \vee \neg B, \neg A \vee \neg B, A \wedge B}{\vdash \neg A \vee \neg B, A \wedge B} \wedge^{\text{mul}}}{\vdash \neg A \vee \neg B, A \wedge B} ctr} \quad \frac{\frac{\frac{\vdash \top}{\vdash \top, \text{F}} \top^{\text{mul}}}{\vdash \top, \text{F}} wk}{\frac{\frac{\frac{\frac{\vdash \neg A, A}{\vdash \exists x \neg A, A} ax}{\vdash \exists x \neg A, A} \exists}{\vdash \exists x \neg A, \forall x A} \forall} \quad \frac{\frac{\frac{\vdash \neg A, A}{\vdash \exists x \neg A, A} ax}{\vdash \exists x \neg A, A} \exists}{\vdash \exists x \neg A, \forall x A} \forall$$

On transforme les affaiblissements sur des formules préfixes avec quantificateur en des affaiblissements propositionnels par :

$$\frac{\frac{\frac{\vdash \Gamma}{\vdash \Gamma, A} wk}{\vdash \Gamma, \exists x A} \exists \quad \frac{\frac{\frac{\vdash \Gamma}{\vdash \Gamma, A} wk}{\vdash \Gamma, \forall x A} \forall$$

quitte à bien choisir le nom x dans la règle \forall .

On considère la mesure suivante : on somme pour chaque occurrence de règle \forall ou \exists , le nombre de règles \wedge^{mul} et \vee^{add} situées au-dessous. Si la mesure vaut 0, la preuve vérifie les conditions nécessaires pour conclure. Sinon on montre qu'on peut toujours transformer la preuve pour faire décroître strictement la mesure : soit R_1 la règle \forall ou \exists la plus basse telle qu'il y ait une règle \wedge^{mul} ou \vee^{add} au-dessous et on note R_2 la plus haute parmi celles-ci. On montre par récurrence sur le nombre de règles entre R_1 et R_2 que l'on peut faire passer R_1 sous R_2 . S'il n'y a aucune règle, on applique la commutation correspondante (la mesure associée à la preuve décroît alors strictement). Sinon, les règles entre les deux sont nécessairement des règles ctr ou wk . Soit A la formule principale de R_1 , on fait commuter toutes les règles qui portent sur A avec les règles qui ne portent pas dessus (grâce aux commutations mentionnées précédemment), et on amène ainsi R_1 juste au-dessous de R_2 . \square

On peut ajouter comme commutation valide qu'une règle *ctr* ou *wk* commute vers le bas avec une règle \exists portant sur sa formule principale :

$$\frac{\frac{\frac{\vdash \Gamma, A[t/x], A[t/x]}{\vdash \Gamma, A[t/x]} \exists}{\vdash \Gamma, \exists x A} \exists}{\vdash \Gamma, \exists x A} \text{ctr} \quad \rightsquigarrow \quad \frac{\frac{\frac{\frac{\vdash \Gamma, A[t/x], A[t/x]}{\vdash \Gamma, \exists x A, A[t/x]} \exists}{\vdash \Gamma, \exists x A, \exists x A} \exists}{\vdash \Gamma, \exists x A} \text{ctr}}{\vdash \Gamma, \exists x A} \text{ctr}$$

$$\frac{\frac{\frac{\vdash \Gamma}{\vdash \Gamma, A[t/x]} \text{wk}}{\vdash \Gamma, \exists x A} \exists}{\vdash \Gamma, \exists x A} \exists \quad \rightsquigarrow \quad \frac{\frac{\vdash \Gamma}{\vdash \Gamma, \exists x A} \text{wk}}{\vdash \Gamma, \exists x A} \text{wk}$$

Théorème 3 (Herbrand)

Soit $A = \forall x_1 \dots \forall x_n \exists y_1 \dots \exists y_k A_0$ une formule en forme préfixe ($n \geq 0$, $k \geq 0$ et A_0 sans quantificateur), si A est prouvable, il existe $p \geq 1$ et des termes $(t_i^j)_{1 \leq i \leq k, 1 \leq j \leq p}$ tels que $A_0[t_1^1/y_1] \dots [t_k^1/y_k] \vee \dots \vee A_0[t_1^p/y_1] \dots [t_k^p/y_k]$ est prouvable.

DÉMONSTRATION : Par réversibilité de la règle \forall , on se ramène au cas où $\exists y_1 \dots \exists y_k A_0$ est prouvable. On applique le théorème du séquent intermédiaire pour obtenir une preuve de $\vdash \Delta$ qui suivie de règles \exists , *ctr* et *wk* donne $\vdash \exists y_1 \dots \exists y_k A_0$. En faisant commuter les \exists vers le haut dans cette partie basse de la preuve, on vérifie qu'on passe de $\vdash \Delta$ à un séquent $\vdash \Xi$ par application de règles \exists uniquement puis de $\vdash \Xi$ à $\vdash \exists y_1 \dots \exists y_k A_0$ par application de règles structurelles uniquement donc $\Xi = \exists y_1 \dots \exists y_k A_0, \dots, \exists y_1 \dots \exists y_k A_0$ ($p \geq 1$ copies de la formule). Puisque $\vdash \Delta$ est sans quantificateur, toutes les règles \exists possibles sont appliquées entre $\vdash \Delta$ et $\vdash \Xi$ fournissant les termes $(t_i^j)_{1 \leq i \leq k, 1 \leq j \leq p}$ et imposant que $\Delta = A_0[t_1^1/y_1] \dots [t_k^1/y_k], \dots, A_0[t_1^p/y_1] \dots [t_k^p/y_k]$.

Enfin, si $\vdash A_0[t_1^1/y_1] \dots [t_k^1/y_k], \dots, A_0[t_1^p/y_1] \dots [t_k^p/y_k]$ est prouvable alors $\vdash A_0[t_1^1/y_1] \dots [t_k^1/y_k] \vee \dots \vee A_0[t_1^p/y_1] \dots [t_k^p/y_k]$ également. \square

Le théorème de Herbrand est en fait un énoncé plus général pouvant être appliqué à n'importe quelle formule en forme préfixe.

Dynamique non déterministe

Si on considère l'élimination des coupures comme un processus calculatoire qui transforme une preuve en un résultat (une preuve sans coupure) (voir [chapitre 3](#)), on constate que la procédure que l'on a définie est non déterministe, il n'y a pas de "résultat" unique :

- Lors de l'élimination d'une coupure dans laquelle aucune des formules coupées n'est principale dans une règle logique, on a choisi arbitrairement une direction pour faire remonter la coupure.
- Cependant, ceci pourrait mener tout de même à un unique résultat mais la *paire critique de Lafont* nous montre le contraire :

$$\frac{\frac{\frac{\vdash \Gamma}{\vdash \Gamma, A} \text{wk}}{\vdash \Gamma, \Gamma} \text{ctr} \quad \frac{\frac{\frac{\vdash \Gamma}{\vdash \Gamma, \neg A} \text{wk}}{\vdash \Gamma, \Gamma} \text{cut}}{\vdash \Gamma} \text{ctr}}{\vdash \Gamma} \text{ctr}$$

cette preuve va se réduire en π_1 ou en π_2 selon le choix de la direction pour éliminer la coupure (à un petit rien près). Ceci montre même un non déterminisme très fort puisque

pour toute paire de résultats que l'on choisit, on construit ainsi une preuve qui peut donner les deux.

C'est une des raisons pour laquelle on souhaite briser (malheureusement?) une part de la symétrie de LK, on espère ainsi faire disparaître ce type de paires critiques.

1.3 Calcul des séquents intuitionniste (LJ)

Restriction “exactement une formule à droite”

Afin de retrouver plus de déterminisme dans l'élimination des coupures, on va briser la symétrie gauche / droite. On est obligé de revenir à un calcul bilatère. On impose que les séquents contiennent exactement une formule à droite $\Gamma \vdash A$. Parmi les règles obtenues on sélectionne le groupe identité multiplicatif (“plus primitif”) et les règles logiques additives (qui supportent mieux la contrainte sur les séquents excepté pour \rightarrow que l'on choisit multiplicative (l'implication additive n'est pas un connecteur très intuitif, et d'autre part une seule règle survit) :

$$\begin{array}{c}
\frac{}{A \vdash A} \text{ax} \qquad \frac{\Gamma \vdash A \quad \Delta, A \vdash C}{\Gamma, \Delta \vdash C} \text{cut} \\
\\
\frac{\Gamma, A, A \vdash C}{\Gamma, A \vdash C} \text{ctrL} \qquad \frac{\Gamma \vdash C}{\Gamma, A \vdash C} \text{wkL} \\
\\
\frac{\Gamma \vdash A \quad \Gamma \vdash B}{\Gamma \vdash A \wedge B} \wedge^{\text{addR}} \qquad \frac{\Gamma, A \vdash C}{\Gamma, A \wedge B \vdash C} \wedge^{\text{addL}_1} \qquad \frac{\Gamma, B \vdash C}{\Gamma, A \wedge B \vdash C} \wedge^{\text{addL}_2} \\
\\
\frac{\Gamma \vdash A}{\Gamma \vdash A \vee B} \vee^{\text{addR}_1} \qquad \frac{\Gamma \vdash B}{\Gamma \vdash A \vee B} \vee^{\text{addR}_2} \qquad \frac{\Gamma, A \vdash C \quad \Gamma, B \vdash C}{\Gamma, A \vee B \vdash C} \vee^{\text{addL}} \\
\\
\frac{}{\Gamma \vdash \mathbf{T}} \mathbf{T}^{\text{addR}} \qquad \frac{}{\Gamma, \mathbf{F} \vdash C} \mathbf{F}^{\text{addL}} \\
\\
\frac{\Gamma, A \vdash B}{\Gamma \vdash A \rightarrow B} \rightarrow^{\text{mulR}} \qquad \frac{\Gamma, B \vdash C \quad \Delta \vdash A}{\Gamma, \Delta, A \rightarrow B \vdash C} \rightarrow^{\text{mulL}} \\
\\
\frac{\Gamma \vdash A}{\Gamma \vdash \forall x A} \forall \mathbf{R} \qquad \frac{\Gamma, A^{[t/x]} \vdash C}{\Gamma, \forall x A \vdash C} \forall \mathbf{L} \qquad \frac{\Gamma \vdash A^{[t/x]}}{\Gamma \vdash \exists x A} \exists \mathbf{R} \qquad \frac{\Gamma, A \vdash C}{\Gamma, \exists x A \vdash C} \exists \mathbf{L}
\end{array}$$

avec x non libre dans Γ pour la règle $\forall \mathbf{R}$ et dans Γ et C pour la règle $\exists \mathbf{L}$.

Ces séquents intuitionnistes sont plus “intuitifs”, $A_1, \dots, A_n \vdash A$ représente une étape intermédiaire de démonstration où ayant supposé A_1, \dots, A_n , on a démontré A .

La négation a disparu. On peut la retrouver à travers la définition $\neg A = A \rightarrow \mathbf{F}$ ce qui donne les règles :

$$\frac{\Gamma, A \vdash \mathbf{F}}{\Gamma \vdash \neg A} \neg \mathbf{R} \qquad \frac{\Gamma \vdash A}{\Gamma, \neg A \vdash \mathbf{F}} \neg \mathbf{L}$$

Remarque : De manière plus générale, il est possible de définir une négation “paramétrique” pour toute formule \mathbf{R} par $\neg_{\mathbf{R}} A = A \rightarrow \mathbf{R}$ avec comme règles :

$$\frac{\Gamma, A \vdash \mathbf{R}}{\Gamma \vdash \neg_{\mathbf{R}} A} \neg_{\mathbf{R}} \mathbf{R} \qquad \frac{\Gamma \vdash A}{\Gamma, \neg_{\mathbf{R}} A \vdash \mathbf{R}} \neg_{\mathbf{R}} \mathbf{L}$$

avec comme cas particulier $\neg A = \neg_{\mathbf{F}} A$.

Dans l'étude des $\neg\neg$ -traductions qui va suivre il est possible d'utiliser $\neg_{\mathbf{R}}$. Ceci donne des résultats un peu plus généraux puisqu'on a la possibilité d'instancier \mathbf{R} ensuite (notamment par \mathbf{F}).

Compatibilité de l'élimination des coupures

On vérifie que les cas clefs appliqués aux règles que l'on a choisies sont bien définissables et que les cas structurels préservent la contrainte "exactement une formule à droite".

Propriété de la disjonction et de l'existentiel

Proposition 4 (Propriété de la disjonction)

Si $\vdash A \vee B$ est prouvable dans LJ, alors soit $\vdash A$ soit $\vdash B$ est prouvable.

DÉMONSTRATION : Soit π une preuve sans coupure de $\vdash A \vee B$, les deux seules possibilités de dernière règle sont $\vee^{\text{add}}R_1$ et $\vee^{\text{add}}R_2$. La preuve située au-dessus de cette dernière règle est alors une preuve de $\vdash A$ ou de $\vdash B$. \square

Proposition 5 (Propriété de l'existentiel)

Si $\vdash \exists xA$ est prouvable dans LJ, alors il existe t tel que $\vdash A[t/x]$ est prouvable.

DÉMONSTRATION : Soit π une preuve sans coupure de $\vdash \exists xA$, la dernière règle de π est nécessairement une règle $\exists R$ dont la prémisse est donc $\vdash A[t/x]$ pour un certain terme t . \square

Perte de symétrie et d'équivalence de connecteurs

On ne peut plus prouver $\vdash A \vee (A \rightarrow F)$, $\vdash ((A \rightarrow B) \rightarrow A) \rightarrow A$, ...

Concernant les lois de De Morgan, dans LJ on a :

$$\begin{aligned} \neg A \vee \neg B &\vdash \neg(A \wedge B) \\ \neg(A \wedge B) &\not\vdash \neg A \vee \neg B \\ \neg A \wedge \neg B &\vdash \neg(A \vee B) \\ \neg(A \vee B) &\vdash \neg A \wedge \neg B \\ \exists x \neg A &\vdash \neg(\forall x A) \\ \neg(\forall x A) &\not\vdash \exists x \neg A \\ \forall x \neg A &\vdash \neg(\exists x A) \\ \neg(\exists x A) &\vdash \forall x \neg A \\ A &\vdash \neg \neg A \\ \neg \neg A &\not\vdash A \end{aligned}$$

On garde l'équivalence entre la conjonction additive et la conjonction multiplicative mais la disjonction multiplicative n'est plus utilisable (d'où la perte du tiers exclu).

Exercice 13 (Distributivité)

Que reste-t-il des distributivités du \wedge sur le \vee et du \vee sur le \wedge ?

Restriction "au plus une formule à droite"

Il est possible de relâcher légèrement la contrainte définissant la logique intuitionniste en imposant qu'il y ait au plus une formule à droite dans les séquents. Les règles s'adaptent directement avec une correspondance entre $\Gamma \vdash$ et $\Gamma \vdash F$.

Les règles pour la négation (non paramétrique) deviennent ainsi :

$$\frac{\Gamma, A \vdash}{\Gamma \vdash \neg A} \neg R \qquad \frac{\Gamma \vdash A}{\Gamma, \neg A \vdash} \neg L$$

et on admet la règle d'affaiblissement à droite :

Attention, l'approche "naïve" qui consiste à préfixer toute formule par $\neg\neg$ fonctionne en calcul propositionnel (théorème de Glivenko) mais pas en calcul des prédicats ($\vdash \neg\neg\forall x(A \vee \neg A)$ n'est pas prouvable dans LJ).

On définit la traduction $(\cdot)^{\neg\neg}$ par :

$$(\Gamma \vdash \Delta)^{\neg\neg} = \neg_R \neg_R \Gamma^{\neg\neg}, \neg_R \Delta^{\neg\neg} \vdash R$$

$$X^{\neg\neg} = X$$

$$(A \wedge B)^{\neg\neg} = \neg_R \neg_R A^{\neg\neg} \wedge \neg_R \neg_R B^{\neg\neg}$$

$$(A \vee B)^{\neg\neg} = \neg_R \neg_R A^{\neg\neg} \vee \neg_R \neg_R B^{\neg\neg}$$

$$(A \rightarrow B)^{\neg\neg} = \neg_R \neg_R A^{\neg\neg} \rightarrow \neg_R \neg_R B^{\neg\neg}$$

$$(\neg A)^{\neg\neg} = \neg_R \neg_R \neg_R A^{\neg\neg}$$

$$(T)^{\neg\neg} = T$$

$$(F)^{\neg\neg} = F$$

$$(\forall x A)^{\neg\neg} = \forall x \neg_R \neg_R A^{\neg\neg}$$

$$(\exists x A)^{\neg\neg} = \exists x \neg_R \neg_R A^{\neg\neg}$$

Exercice 14

Montrer que $A \dashv\vdash_{LK} A^{\neg\neg}$ et donc que $\Gamma \vdash \Delta$ et $(\Gamma \vdash \Delta)^{\neg\neg}$ sont équivalents en logique classique.

Les règles sont traduites par :

(ax)

$$\frac{\neg_R A^{\neg\neg} \vdash \neg_R A^{\neg\neg} \quad ax}{\neg_R \neg_R A^{\neg\neg}, \neg_R A^{\neg\neg} \vdash R} \neg_R L$$

(cut)

$$\frac{\frac{\neg_R \neg_R \Gamma^{\neg\neg}, \neg_R \Delta^{\neg\neg}, \neg_R A^{\neg\neg} \vdash R}{\neg_R \neg_R \Gamma^{\neg\neg}, \neg_R \Delta^{\neg\neg} \vdash \neg_R \neg_R A^{\neg\neg}} \neg_R R \quad \neg_R \neg_R \Gamma'^{\neg\neg}, \neg_R \neg_R A^{\neg\neg}, \neg_R \Delta'^{\neg\neg} \vdash R}{\neg_R \neg_R \Gamma^{\neg\neg}, \neg_R \neg_R \Gamma'^{\neg\neg}, \neg_R \Delta^{\neg\neg}, \neg_R \Delta'^{\neg\neg} \vdash R} cut$$

(ctrL)

$$\frac{\neg_R \neg_R \Gamma^{\neg\neg}, \neg_R \neg_R A^{\neg\neg}, \neg_R \neg_R A^{\neg\neg}, \neg_R \Delta^{\neg\neg} \vdash R}{\neg_R \neg_R \Gamma^{\neg\neg}, \neg_R \neg_R A^{\neg\neg}, \neg_R \Delta^{\neg\neg} \vdash R} ctrL$$

(ctrR)

$$\frac{\neg_R \neg_R \Gamma^{\neg\neg}, \neg_R \Delta^{\neg\neg}, \neg_R A^{\neg\neg}, \neg_R A^{\neg\neg} \vdash R}{\neg_R \neg_R \Gamma^{\neg\neg}, \neg_R \Delta^{\neg\neg}, \neg_R A^{\neg\neg} \vdash R} ctrL$$

(wkL)

$$\frac{\neg_R \neg_R \Gamma^{\neg\neg}, \neg_R \Delta^{\neg\neg} \vdash R}{\neg_R \neg_R \Gamma^{\neg\neg}, \neg_R \neg_R A^{\neg\neg}, \neg_R \Delta^{\neg\neg} \vdash R} wkL$$

(wkR)

$$\frac{\neg_R \neg_R \Gamma^{\neg\neg}, \neg_R \Delta^{\neg\neg} \vdash R}{\neg_R \neg_R \Gamma^{\neg\neg}, \neg_R \Delta^{\neg\neg}, \neg_R A^{\neg\neg} \vdash R} wkL$$

($\wedge^{\text{add}}R$)

$$\frac{\frac{\neg_R \neg_R \Gamma^{\neg\neg}, \neg_R \Delta^{\neg\neg}, \neg_R A^{\neg\neg} \vdash R}{\neg_R \neg_R \Gamma^{\neg\neg}, \neg_R \Delta^{\neg\neg} \vdash \neg_R \neg_R A^{\neg\neg}} \neg_R R \quad \frac{\neg_R \neg_R \Gamma^{\neg\neg}, \neg_R \Delta^{\neg\neg}, \neg_R B^{\neg\neg} \vdash R}{\neg_R \neg_R \Gamma^{\neg\neg}, \neg_R \Delta^{\neg\neg} \vdash \neg_R \neg_R B^{\neg\neg}} \neg_R R}{\frac{\neg_R \neg_R \Gamma^{\neg\neg}, \neg_R \Delta^{\neg\neg} \vdash \neg_R \neg_R A^{\neg\neg} \wedge \neg_R \neg_R B^{\neg\neg}}{\neg_R \neg_R \Gamma^{\neg\neg}, \neg_R \Delta^{\neg\neg}, \neg_R (\neg_R \neg_R A^{\neg\neg} \wedge \neg_R \neg_R B^{\neg\neg}) \vdash R} \neg_R L} \wedge^{\text{add}}R$$

($\wedge^{\text{add}}L_1$)

(T^{addR})

$$\frac{\frac{}{\neg_R \neg_R \Gamma^{\neg\neg}, \neg_R \Delta^{\neg\neg} \vdash T} \text{T}^{\text{addR}}}{\neg_R \neg_R \Gamma^{\neg\neg}, \neg_R \Delta^{\neg\neg}, \neg_R T \vdash R} \neg_R L$$

(F^{addL})

$$\frac{\frac{\frac{}{\neg_R \neg_R \Gamma^{\neg\neg}, \neg_R \Delta^{\neg\neg}, F \vdash R} \text{F}^{\text{addL}}}{\neg_R \neg_R \Gamma^{\neg\neg}, \neg_R \Delta^{\neg\neg} \vdash \neg_R F} \neg_R R}{\neg_R \neg_R \Gamma^{\neg\neg}, \neg_R \neg_R F, \neg_R \Delta^{\neg\neg} \vdash R} \neg_R L$$

(∀R)

$$\frac{\frac{\frac{\neg_R \neg_R \Gamma^{\neg\neg}, \neg_R \Delta^{\neg\neg}, \neg_R A^{\neg\neg} \vdash R}{\neg_R \neg_R \Gamma^{\neg\neg}, \neg_R \Delta^{\neg\neg} \vdash \neg_R \neg_R A^{\neg\neg}} \neg_R R}{\neg_R \neg_R \Gamma^{\neg\neg}, \neg_R \Delta^{\neg\neg} \vdash \forall x \neg_R \neg_R A^{\neg\neg}} \forall R}{\neg_R \neg_R \Gamma^{\neg\neg}, \neg_R \Delta^{\neg\neg}, \neg_R \forall x \neg_R \neg_R A^{\neg\neg} \vdash R} \neg_R L$$

(∀L) en utilisant $(A[t/x])^{\neg\neg} = A^{\neg\neg}[t/x]$:

$$\frac{\frac{\frac{\neg_R \neg_R \Gamma^{\neg\neg}, \neg_R \neg_R (A[t/x])^{\neg\neg}, \neg_R \Delta^{\neg\neg} \vdash R}{\neg_R \neg_R \Gamma^{\neg\neg}, \forall x \neg_R \neg_R A^{\neg\neg}, \neg_R \Delta^{\neg\neg} \vdash R} \forall L}{\neg_R \neg_R \Gamma^{\neg\neg}, \neg_R \Delta^{\neg\neg} \vdash \neg_R \forall x \neg_R \neg_R A^{\neg\neg}} \neg_R R}{\neg_R \neg_R \Gamma^{\neg\neg}, \neg_R \neg_R \forall x \neg_R \neg_R A^{\neg\neg}, \neg_R \Delta^{\neg\neg} \vdash R} \neg_R L$$

(∃R) en utilisant $(A[t/x])^{\neg\neg} = A^{\neg\neg}[t/x]$:

$$\frac{\frac{\frac{\neg_R \neg_R \Gamma^{\neg\neg}, \neg_R \Delta^{\neg\neg}, \neg_R (A[t/x])^{\neg\neg} \vdash R}{\neg_R \neg_R \Gamma^{\neg\neg}, \neg_R \Delta^{\neg\neg} \vdash \neg_R \neg_R (A[t/x])^{\neg\neg}} \neg_R R}{\neg_R \neg_R \Gamma^{\neg\neg}, \neg_R \Delta^{\neg\neg} \vdash \exists x \neg_R \neg_R A^{\neg\neg}} \exists R}{\neg_R \neg_R \Gamma^{\neg\neg}, \neg_R \Delta^{\neg\neg}, \neg_R \exists x \neg_R \neg_R A^{\neg\neg} \vdash R} \neg_R L$$

(∃L)

$$\frac{\frac{\frac{\neg_R \neg_R \Gamma^{\neg\neg}, \neg_R \neg_R A^{\neg\neg}, \neg_R \Delta^{\neg\neg} \vdash R}{\neg_R \neg_R \Gamma^{\neg\neg}, \exists x \neg_R \neg_R A^{\neg\neg}, \neg_R \Delta^{\neg\neg} \vdash R} \exists L}{\neg_R \neg_R \Gamma^{\neg\neg}, \neg_R \Delta^{\neg\neg} \vdash \neg_R \exists x \neg_R \neg_R A^{\neg\neg}} \neg_R R}{\neg_R \neg_R \Gamma^{\neg\neg}, \neg_R \neg_R \exists x \neg_R \neg_R A^{\neg\neg}, \neg_R \Delta^{\neg\neg} \vdash R} \neg_R L$$

Proposition 6 (Correction)

Si $\Gamma \vdash \Delta$ est dérivable dans LK alors $(\Gamma \vdash \Delta)^{\neg\neg}$ est dérivable dans LJ.

DÉMONSTRATION : On vient de donner une traduction règle par règle. On préserve donc non seulement la prouvabilité mais également une certaine structure de la preuve d'origine. □

Proposition 7 (Complétude)

Si $(\Gamma \vdash \Delta)^{\neg\neg}$ est dérivable dans LJ alors $\Gamma \vdash \Delta$ est dérivable dans LK.

DÉMONSTRATION : LJ étant un sous-système de LK, il est immédiat que $(\Gamma \vdash \Delta)^{\neg\neg}$ est dérivable dans LK. On peut conclure par l'exercice 14. □

On va donner une nouvelle présentation de cette traduction de manière à pouvoir ensuite

l'optimiser. On définit la traduction $(\cdot)^{\neg\neg'}$ de la manière suivante :

$$\begin{aligned}
X^{\neg\neg'} &= \neg_{\mathbf{R}}\neg_{\mathbf{R}}X \\
(A \wedge B)^{\neg\neg'} &= \neg_{\mathbf{R}}\neg_{\mathbf{R}}(A^{\neg\neg'} \wedge B^{\neg\neg'}) \\
(A \vee B)^{\neg\neg'} &= \neg_{\mathbf{R}}\neg_{\mathbf{R}}(A^{\neg\neg'} \vee B^{\neg\neg'}) \\
(A \rightarrow B)^{\neg\neg'} &= \neg_{\mathbf{R}}\neg_{\mathbf{R}}(A^{\neg\neg'} \rightarrow B^{\neg\neg'}) \\
(\neg A)^{\neg\neg'} &= \neg_{\mathbf{R}}\neg_{\mathbf{R}}\neg_{\mathbf{R}}A^{\neg\neg'} \\
(\mathbf{T})^{\neg\neg'} &= \neg_{\mathbf{R}}\neg_{\mathbf{R}}\mathbf{T} \\
(\mathbf{F})^{\neg\neg'} &= \neg_{\mathbf{R}}\neg_{\mathbf{R}}\mathbf{F} \\
(\forall xA)^{\neg\neg'} &= \neg_{\mathbf{R}}\neg_{\mathbf{R}}\forall xA^{\neg\neg'} \\
(\exists xA)^{\neg\neg'} &= \neg_{\mathbf{R}}\neg_{\mathbf{R}}\exists xA^{\neg\neg'}
\end{aligned}$$

ainsi la traduction de toute formule commence par $\neg_{\mathbf{R}}\neg_{\mathbf{R}}$, note $(A^{\neg\neg'})^-$ la formule obtenue en supprimant la première négation de $A^{\neg\neg'}$. On traduit alors les séquents par :

$$(\Gamma \vdash \Delta)^{\neg\neg'} = \Gamma^{\neg\neg'}, (\Delta^{\neg\neg'})^- \vdash \mathbf{R}$$

On peut montrer que l'on obtient la même traduction des séquents et donc des preuves qu'avec $(\cdot)^{\neg\neg}$ (on prouvera d'abord que $\neg_{\mathbf{R}}\neg_{\mathbf{R}}A^{\neg\neg} = A^{\neg\neg'}$).

$\neg\neg$ -traduction “optimisée” (Gödel)

La traduction que l'on vient de donner est extrêmement verbeuse par son usage systématique des $\neg_{\mathbf{R}}\neg_{\mathbf{R}}$. Il est possible d'alléger cette traduction au prix d'une légère complication de la traduction des règles grâce à une analyse plus précise des questions de réversibilité.

On définit la traduction $(\cdot)^\circ$ par :

$$\begin{aligned}
(\Gamma \vdash \Delta)^\circ &= \Gamma^\circ, \neg_{\mathbf{R}}\Delta^\circ \vdash \mathbf{R} \\
X^\circ &= \neg_{\mathbf{R}}\neg_{\mathbf{R}}X \\
(A \wedge B)^\circ &= A^\circ \wedge B^\circ \\
(A \vee B)^\circ &= \neg_{\mathbf{R}}\neg_{\mathbf{R}}(A^\circ \vee B^\circ) \\
(A \rightarrow B)^\circ &= A^\circ \rightarrow B^\circ \\
(\neg A)^\circ &= \neg_{\mathbf{R}}A^\circ \\
(\mathbf{T})^\circ &= \mathbf{T} \\
(\mathbf{F})^\circ &= \neg_{\mathbf{R}}\neg_{\mathbf{R}}\mathbf{F} \\
(\forall xA)^\circ &= \forall xA^\circ \\
(\exists xA)^\circ &= \neg_{\mathbf{R}}\neg_{\mathbf{R}}\exists xA^\circ
\end{aligned}$$

ce qui “rajoute une double négation” dans la traduction des séquents mais en élimine beaucoup d'autres !

Lemme 1 (Élimination des $\neg\neg$)

Le séquent $\neg_{\mathbf{R}}\neg_{\mathbf{R}}A^\circ \vdash A^\circ$ est prouvable dans LJ.

DÉMONSTRATION : Par récurrence sur A :

$$\begin{array}{c}
\frac{}{\neg_{\mathbf{R}} X \vdash \neg_{\mathbf{R}} X} \text{ax} \\
\frac{}{\neg_{\mathbf{R}} \neg_{\mathbf{R}} X, \neg_{\mathbf{R}} X \vdash \mathbf{R}} \neg_{\mathbf{R}} \mathbf{L} \\
\frac{}{\neg_{\mathbf{R}} X \vdash \neg_{\mathbf{R}} \neg_{\mathbf{R}} \neg_{\mathbf{R}} X} \neg_{\mathbf{R}} \mathbf{R} \\
\frac{}{\neg_{\mathbf{R}} \neg_{\mathbf{R}} \neg_{\mathbf{R}} \neg_{\mathbf{R}} X, \neg_{\mathbf{R}} X \vdash \mathbf{R}} \neg_{\mathbf{R}} \mathbf{L} \\
\frac{}{\neg_{\mathbf{R}} \neg_{\mathbf{R}} \neg_{\mathbf{R}} \neg_{\mathbf{R}} X \vdash \neg_{\mathbf{R}} \neg_{\mathbf{R}} X} \neg_{\mathbf{R}} \mathbf{R}
\end{array}$$

ce qui montre de manière générale que pour toute formule G , on a $\neg_{\mathbf{R}} \neg_{\mathbf{R}} \neg_{\mathbf{R}} G \vdash \neg_{\mathbf{R}} G$ dans LJ, on obtient ainsi les cas \vee , \neg , \mathbf{F} et \exists .

$$\begin{array}{c}
\frac{}{A^\circ \vdash A^\circ} \text{ax} \\
\frac{}{A^\circ \wedge B^\circ \vdash A^\circ} \wedge^{\text{add}} \mathbf{L}_1 \\
\frac{}{A^\circ \wedge B^\circ, \neg_{\mathbf{R}} A^\circ \vdash \mathbf{R}} \neg_{\mathbf{R}} \mathbf{L} \\
\frac{}{\neg_{\mathbf{R}} A^\circ \vdash \neg_{\mathbf{R}} (A^\circ \wedge B^\circ),} \neg_{\mathbf{R}} \mathbf{R} \\
\frac{}{\neg_{\mathbf{R}} \neg_{\mathbf{R}} (A^\circ \wedge B^\circ), \neg_{\mathbf{R}} A^\circ \vdash \mathbf{R}} \neg_{\mathbf{R}} \mathbf{L} \\
\frac{}{\neg_{\mathbf{R}} \neg_{\mathbf{R}} (A^\circ \wedge B^\circ) \vdash \neg_{\mathbf{R}} \neg_{\mathbf{R}} A^\circ} \neg_{\mathbf{R}} \mathbf{R} \\
\frac{}{\neg_{\mathbf{R}} \neg_{\mathbf{R}} (A^\circ \wedge B^\circ) \vdash A^\circ} \text{cut} \\
\frac{}{\neg_{\mathbf{R}} \neg_{\mathbf{R}} (A^\circ \wedge B^\circ) \vdash A^\circ \wedge B^\circ} \wedge^{\text{add}} \mathbf{R}
\end{array}$$

$$\begin{array}{c}
\frac{}{A^\circ \vdash A^\circ} \text{ax} \quad \frac{}{B^\circ \vdash B^\circ} \text{ax} \\
\frac{}{A^\circ \rightarrow B^\circ, A^\circ \vdash B^\circ} \rightarrow^{\text{mul}} \mathbf{L} \\
\frac{}{A^\circ \rightarrow B^\circ, A^\circ, \neg_{\mathbf{R}} B^\circ \vdash \mathbf{R}} \neg_{\mathbf{R}} \mathbf{L} \\
\frac{}{A^\circ, \neg_{\mathbf{R}} B^\circ \vdash \neg_{\mathbf{R}} (A^\circ \rightarrow B^\circ)} \neg_{\mathbf{R}} \mathbf{R} \\
\frac{}{\neg_{\mathbf{R}} \neg_{\mathbf{R}} (A^\circ \rightarrow B^\circ), A^\circ, \neg_{\mathbf{R}} B^\circ \vdash \mathbf{R}} \neg_{\mathbf{R}} \mathbf{L} \\
\frac{}{\neg_{\mathbf{R}} \neg_{\mathbf{R}} (A^\circ \rightarrow B^\circ), A^\circ \vdash \neg_{\mathbf{R}} \neg_{\mathbf{R}} B^\circ} \neg_{\mathbf{R}} \mathbf{R} \\
\frac{}{\neg_{\mathbf{R}} \neg_{\mathbf{R}} (A^\circ \rightarrow B^\circ) \vdash B^\circ} \text{cut} \\
\frac{}{\neg_{\mathbf{R}} \neg_{\mathbf{R}} (A^\circ \rightarrow B^\circ), A^\circ \vdash B^\circ} \rightarrow^{\text{mul}} \mathbf{R}
\end{array}$$

$$\frac{}{\neg_{\mathbf{R}} \neg_{\mathbf{R}} \mathbf{T} \vdash \mathbf{T}} \mathbf{T}^{\text{add}} \mathbf{R}$$

$$\begin{array}{c}
\frac{}{A^\circ \vdash A^\circ} \text{ax} \\
\frac{}{\forall x A^\circ \vdash A^\circ} \forall \mathbf{L} \\
\frac{}{\forall x A^\circ, \neg_{\mathbf{R}} A^\circ \vdash \mathbf{R}} \neg_{\mathbf{R}} \mathbf{L} \\
\frac{}{\neg_{\mathbf{R}} A^\circ \vdash \neg_{\mathbf{R}} \forall x A^\circ} \neg_{\mathbf{R}} \mathbf{R} \\
\frac{}{\neg_{\mathbf{R}} \neg_{\mathbf{R}} \forall x A^\circ, \neg_{\mathbf{R}} A^\circ \vdash \mathbf{R}} \neg_{\mathbf{R}} \mathbf{L} \\
\frac{}{\neg_{\mathbf{R}} \neg_{\mathbf{R}} \forall x A^\circ \vdash \neg_{\mathbf{R}} \neg_{\mathbf{R}} A^\circ} \neg_{\mathbf{R}} \mathbf{R} \\
\frac{}{\neg_{\mathbf{R}} \neg_{\mathbf{R}} \forall x A^\circ \vdash A^\circ} \text{cut} \\
\frac{}{\neg_{\mathbf{R}} \neg_{\mathbf{R}} \forall x A^\circ \vdash \forall x A^\circ} \forall \mathbf{R}
\end{array}$$

□

On peut montrer grâce à ce lemme que la traduction des règles pour $(.)^{\neg_{\mathbf{R}}}$ se simplifie pour s'adapter à cette nouvelle traduction.

Dans le cas particulier où on se restreint aux connecteurs réversibles : \wedge , \rightarrow , \neg , \mathbf{T} et \forall , cette

traduction devient extrêmement simple sur les séquents et les formules :

$$\begin{aligned}
(\Gamma \vdash \Delta)^\circ &= \Gamma^\circ, \neg_{\mathbf{R}}\Delta^\circ \vdash \mathbf{R} \\
X^\circ &= \neg_{\mathbf{R}}\neg_{\mathbf{R}}X \\
(A \wedge B)^\circ &= A^\circ \wedge B^\circ \\
(A \rightarrow B)^\circ &= A^\circ \rightarrow B^\circ \\
(\neg A)^\circ &= \neg_{\mathbf{R}}A^\circ \\
(\mathbf{T})^\circ &= \mathbf{T} \\
(\forall xA)^\circ &= \forall xA^\circ
\end{aligned}$$

il suffit donc de mettre $\neg_{\mathbf{R}}\neg_{\mathbf{R}}$ sur les variables.

La traduction des règles devient :

(ax)

$$\frac{A^\circ \vdash A^\circ \text{ ax}}{A^\circ, \neg_{\mathbf{R}}A^\circ \vdash \mathbf{R}} \neg_{\mathbf{R}}\mathbf{L}$$

(cut)

$$\frac{\Gamma^\circ, \neg_{\mathbf{R}}\Delta^\circ, \neg_{\mathbf{R}}A^\circ \vdash \mathbf{R} \quad \frac{\Gamma'^\circ, A^\circ, \neg_{\mathbf{R}}\Delta'^\circ \vdash \mathbf{R}}{\Gamma'^\circ, \neg_{\mathbf{R}}\Delta'^\circ \vdash \neg_{\mathbf{R}}A^\circ} \neg_{\mathbf{R}}\mathbf{R}}{\Gamma^\circ, \Gamma'^\circ, \neg_{\mathbf{R}}\Delta^\circ, \neg_{\mathbf{R}}\Delta'^\circ \vdash \mathbf{R}} \text{ cut}$$

(ctrL)

$$\frac{\Gamma^\circ, A^\circ, A^\circ, \neg_{\mathbf{R}}\Delta^\circ \vdash \mathbf{R}}{\Gamma^\circ, A^\circ, \neg_{\mathbf{R}}\Delta^\circ \vdash \mathbf{R}} \text{ ctrL}$$

(ctrR)

$$\frac{\Gamma^\circ, \neg_{\mathbf{R}}\Delta^\circ, \neg_{\mathbf{R}}A^\circ, \neg_{\mathbf{R}}A^\circ \vdash \mathbf{R}}{\Gamma^\circ, \neg_{\mathbf{R}}\Delta^\circ, \neg_{\mathbf{R}}A^\circ \vdash \mathbf{R}} \text{ ctrL}$$

(wkL)

$$\frac{\Gamma^\circ, \neg_{\mathbf{R}}\Delta^\circ \vdash \mathbf{R}}{\Gamma^\circ, A^\circ, \neg_{\mathbf{R}}\Delta^\circ \vdash \mathbf{R}} \text{ wkL}$$

(wkR)

$$\frac{\Gamma^\circ, \neg_{\mathbf{R}}\Delta^\circ \vdash \mathbf{R}}{\Gamma^\circ, \neg_{\mathbf{R}}\Delta^\circ, \neg_{\mathbf{R}}A^\circ \vdash \mathbf{R}} \text{ wkL}$$

($\wedge^{\text{add}}\mathbf{R}$)

$$\frac{\frac{\frac{\Gamma^\circ, \neg_{\mathbf{R}}\Delta^\circ, \neg_{\mathbf{R}}A^\circ \vdash \mathbf{R}}{\Gamma^\circ, \neg_{\mathbf{R}}\Delta^\circ \vdash \neg_{\mathbf{R}}\neg_{\mathbf{R}}A^\circ} \neg_{\mathbf{R}}\mathbf{R} \quad \neg_{\mathbf{R}}\neg_{\mathbf{R}}A^\circ \vdash A^\circ}{\Gamma^\circ, \neg_{\mathbf{R}}\Delta^\circ \vdash A^\circ} \text{ cut} \quad \frac{\frac{\Gamma^\circ, \neg_{\mathbf{R}}\Delta^\circ, \neg_{\mathbf{R}}B^\circ \vdash \mathbf{R}}{\Gamma^\circ, \neg_{\mathbf{R}}\Delta^\circ \vdash \neg_{\mathbf{R}}\neg_{\mathbf{R}}B^\circ} \neg_{\mathbf{R}}\mathbf{R} \quad \neg_{\mathbf{R}}\neg_{\mathbf{R}}B^\circ \vdash B^\circ}{\Gamma^\circ, \neg_{\mathbf{R}}\Delta^\circ \vdash B^\circ} \text{ cut}}{\Gamma^\circ, \neg_{\mathbf{R}}\Delta^\circ \vdash A^\circ \wedge B^\circ} \wedge^{\text{add}}\mathbf{R}} \neg_{\mathbf{R}}\mathbf{L}$$

($\wedge^{\text{add}}\mathbf{L}_1$)

$$\frac{\Gamma^\circ, A^\circ, \neg_{\mathbf{R}}\Delta^\circ \vdash \mathbf{R}}{\Gamma^\circ, A^\circ \wedge B^\circ, \neg_{\mathbf{R}}\Delta^\circ \vdash \mathbf{R}} \wedge^{\text{add}}\mathbf{L}_1$$

($\wedge^{\text{add}}\mathbf{L}_2$)

$$\frac{\Gamma^\circ, B^\circ, \neg_{\mathbf{R}}\Delta^\circ \vdash \mathbf{R}}{\Gamma^\circ, A^\circ \wedge B^\circ, \neg_{\mathbf{R}}\Delta^\circ \vdash \mathbf{R}} \wedge^{\text{add}}\mathbf{L}_2$$

($\rightarrow^{\text{mul}}\mathbf{R}$)

$$\begin{array}{c}
\frac{\frac{\Gamma^\circ, A^\circ, \neg_{\mathbf{R}}\Delta^\circ, \neg_{\mathbf{R}}B^\circ \vdash \mathbf{R}}{\Gamma^\circ, A^\circ, \neg_{\mathbf{R}}\Delta^\circ \vdash \neg_{\mathbf{R}}\neg_{\mathbf{R}}B^\circ} \neg_{\mathbf{R}}\mathbf{R} \quad \neg_{\mathbf{R}}\neg_{\mathbf{R}}B^\circ \vdash B^\circ}{\frac{\Gamma^\circ, A^\circ, \neg_{\mathbf{R}}\Delta^\circ \vdash B^\circ}{\Gamma^\circ, \neg_{\mathbf{R}}\Delta^\circ \vdash A^\circ \rightarrow B^\circ} \rightarrow^{\text{mul}} \mathbf{R}} \text{cut}}{\Gamma^\circ, \neg_{\mathbf{R}}\Delta^\circ, \neg_{\mathbf{R}}(A^\circ \rightarrow B^\circ) \vdash \mathbf{R}} \neg_{\mathbf{R}}\mathbf{L} \\
(\rightarrow^{\text{mul}} \mathbf{L}) \\
\frac{\frac{\Gamma^\circ, \neg_{\mathbf{R}}\Delta^\circ, \neg_{\mathbf{R}}A^\circ \vdash \mathbf{R}}{\Gamma^\circ, \neg_{\mathbf{R}}\Delta^\circ \vdash \neg_{\mathbf{R}}\neg_{\mathbf{R}}A^\circ} \neg_{\mathbf{R}}\mathbf{R} \quad \neg_{\mathbf{R}}\neg_{\mathbf{R}}A^\circ \vdash A^\circ}{\Gamma^\circ, \neg_{\mathbf{R}}\Delta^\circ \vdash A^\circ} \text{cut} \quad \Gamma'^\circ, B^\circ, \neg_{\mathbf{R}}\Delta'^\circ \vdash \mathbf{R}}{\Gamma^\circ, \Gamma'^\circ, A^\circ \rightarrow B^\circ, \neg_{\mathbf{R}}\Delta^\circ, \neg_{\mathbf{R}}\Delta'^\circ \vdash \mathbf{R}} \rightarrow^{\text{mul}} \mathbf{L} \\
(\neg \mathbf{R}) \\
\frac{\frac{\Gamma^\circ, A^\circ, \neg_{\mathbf{R}}\Delta^\circ \vdash \mathbf{R}}{\Gamma^\circ, \neg_{\mathbf{R}}\Delta^\circ \vdash \neg_{\mathbf{R}}A^\circ} \neg_{\mathbf{R}}\mathbf{R}}{\Gamma^\circ, \neg_{\mathbf{R}}\Delta^\circ, \neg_{\mathbf{R}}\neg_{\mathbf{R}}A^\circ \vdash \mathbf{R}} \neg_{\mathbf{R}}\mathbf{L} \\
(\neg \mathbf{L}) \\
\Gamma^\circ, \neg_{\mathbf{R}}\Delta^\circ, \neg_{\mathbf{R}}A^\circ \vdash \mathbf{R} \\
(\mathbf{T}^{\text{add}}\mathbf{R}) \\
\frac{\Gamma^\circ, \neg_{\mathbf{R}}\Delta^\circ \vdash \mathbf{T}}{\Gamma^\circ, \neg_{\mathbf{R}}\Delta^\circ, \neg_{\mathbf{R}}\mathbf{T} \vdash \mathbf{R}} \mathbf{T}^{\text{add}}\mathbf{R} \\
(\forall \mathbf{R}) \\
\frac{\frac{\frac{\Gamma^\circ, \neg_{\mathbf{R}}\Delta^\circ, \neg_{\mathbf{R}}A^\circ \vdash \mathbf{R}}{\Gamma^\circ, \neg_{\mathbf{R}}\Delta^\circ \vdash \neg_{\mathbf{R}}\neg_{\mathbf{R}}A^\circ} \neg_{\mathbf{R}}\mathbf{R} \quad \neg_{\mathbf{R}}\neg_{\mathbf{R}}A^\circ \vdash A^\circ}{\Gamma^\circ, \neg_{\mathbf{R}}\Delta^\circ \vdash A^\circ} \text{cut}}{\frac{\Gamma^\circ, \neg_{\mathbf{R}}\Delta^\circ \vdash \forall x A^\circ}{\Gamma^\circ, \neg_{\mathbf{R}}\Delta^\circ, \neg_{\mathbf{R}}\forall x A^\circ \vdash \mathbf{R}} \forall \mathbf{R}} \neg_{\mathbf{R}}\mathbf{L} \\
(\forall \mathbf{L}) \text{ en utilisant } (A^{[t/x]})^\circ = A^\circ[t/x] : \\
\frac{\Gamma^\circ, (A^{[t/x]})^\circ, \neg_{\mathbf{R}}\Delta^\circ \vdash \mathbf{R}}{\Gamma^\circ, \forall x A^\circ, \neg_{\mathbf{R}}\Delta^\circ \vdash \mathbf{R}} \forall \mathbf{L}
\end{array}$$

Remarque : On pourrait encore simplifier en prenant $X^\circ = \neg_{\mathbf{R}}X$, on perd alors l'équivalence classique entre $\Gamma \vdash \Delta$ et $(\Gamma \vdash \Delta)^\circ$.

On montre ainsi que bien que la logique intuitionniste soit un sous-système de la logique classique, elle n'en est pas pour autant moins expressive. LJ offre une analyse plus fine donc plus contrainte.

Traduction de Lafont–Reus–Streicher

Étant donnée une fonction $X \mapsto \overline{X}$ des variables dans les variables (par exemple l'identité), on définit la traduction des séquents et des formules :

$$\begin{aligned}
\overline{\Gamma \vdash \Delta} &= \neg_{\mathbf{R}}\overline{\Gamma}, \overline{\Delta} \vdash \mathbf{R} \\
\overline{A \wedge B} &= \overline{A} \vee \overline{B} \\
\overline{A \vee B} &= \overline{A} \wedge \overline{B} \\
\overline{A \rightarrow B} &= \neg_{\mathbf{R}}\overline{A} \wedge \overline{B} \\
\overline{\neg A} &= \neg_{\mathbf{R}}\overline{A} \\
\overline{\mathbf{T}} &= \mathbf{F} \\
\overline{\mathbf{F}} &= \mathbf{T}
\end{aligned}$$

Remarque :

- Dans LK, la traduction $\overline{(\cdot)}$ correspond essentiellement à une négation puisque $\neg_{\mathbf{R}}\overline{A}[\neg_{\mathbf{R}^X}/\overline{X}]$ équivaut à $\neg_{\mathbf{R}}\neg_{\mathbf{R}}A$.
- La traduction de $A \rightarrow B$ est exactement celle de $\neg A \vee B$.
- On pourrait ajouter \forall dans cette traduction mais pas \exists : la règle gauche ne se traduit pas correctement.

Les règles sont traduites par :

(ax)

$$\frac{\overline{\overline{A \vdash A}} \text{ ax}}{\neg_{\mathbf{R}}\overline{A}, \overline{A} \vdash \mathbf{R}} \neg_{\mathbf{R}}\mathbf{L}$$

(cut)

$$\frac{\frac{\neg_{\mathbf{R}}\overline{\Gamma}, \overline{\Delta}, \overline{A} \vdash \mathbf{R}}{\neg_{\mathbf{R}}\overline{\Gamma}, \overline{\Delta} \vdash \neg_{\mathbf{R}}\overline{A}} \neg_{\mathbf{R}}\mathbf{R} \quad \neg_{\mathbf{R}}\overline{\Gamma'}, \neg_{\mathbf{R}}\overline{A}, \overline{\Delta'} \vdash \mathbf{R}}{\neg_{\mathbf{R}}\overline{\Gamma}, \neg_{\mathbf{R}}\overline{\Gamma'}, \overline{\Delta}, \overline{\Delta'} \vdash \mathbf{R}} \text{ cut}$$

(ctrL)

$$\frac{\neg_{\mathbf{R}}\overline{\Gamma}, \neg_{\mathbf{R}}\overline{A}, \neg_{\mathbf{R}}\overline{A}, \overline{\Delta} \vdash \mathbf{R}}{\neg_{\mathbf{R}}\overline{\Gamma}, \neg_{\mathbf{R}}\overline{A}, \overline{\Delta} \vdash \mathbf{R}} \text{ ctrL}$$

(ctrR)

$$\frac{\neg_{\mathbf{R}}\overline{\Gamma}, \overline{\Delta}, \overline{A}, \overline{A} \vdash \mathbf{R}}{\neg_{\mathbf{R}}\overline{\Gamma}, \overline{\Delta}, \overline{A} \vdash \mathbf{R}} \text{ ctrL}$$

(wkL)

$$\frac{\neg_{\mathbf{R}}\overline{\Gamma}, \overline{\Delta} \vdash \mathbf{R}}{\neg_{\mathbf{R}}\overline{\Gamma}, \neg_{\mathbf{R}}\overline{A}, \overline{\Delta} \vdash \mathbf{R}} \text{ wkL}$$

(wkR)

$$\frac{\neg_{\mathbf{R}}\overline{\Gamma}, \overline{\Delta} \vdash \mathbf{R}}{\neg_{\mathbf{R}}\overline{\Gamma}, \overline{\Delta}, \overline{A} \vdash \mathbf{R}} \text{ wkL}$$

($\wedge^{\text{add}}\mathbf{R}$)

$$\frac{\neg_{\mathbf{R}}\overline{\Gamma}, \overline{\Delta}, \overline{A} \vdash \mathbf{R} \quad \neg_{\mathbf{R}}\overline{\Gamma}, \overline{\Delta}, \overline{B} \vdash \mathbf{R}}{\neg_{\mathbf{R}}\overline{\Gamma}, \overline{\Delta}, \overline{A} \vee \overline{B} \vdash \mathbf{R}} \vee^{\text{add}}\mathbf{L}$$

($\wedge^{\text{add}}\mathbf{L}_1$)

$$\frac{\neg_{\mathbf{R}}\overline{\Gamma}, \neg_{\mathbf{R}}\overline{A}, \overline{\Delta} \vdash \mathbf{R} \quad \frac{\frac{\overline{\overline{A \vdash A}} \text{ ax}}{\overline{A} \vdash \overline{A \vee B}} \vee^{\text{add}}\mathbf{R}_1}{\overline{A}, \neg_{\mathbf{R}}(\overline{A} \vee \overline{B}) \vdash \mathbf{R}} \neg_{\mathbf{R}}\mathbf{L}}{\frac{\neg_{\mathbf{R}}\overline{\Gamma}, \neg_{\mathbf{R}}(\overline{A} \vee \overline{B}) \vdash \neg_{\mathbf{R}}\overline{A}}{\neg_{\mathbf{R}}\overline{\Gamma}, \neg_{\mathbf{R}}(\overline{A} \vee \overline{B}), \overline{\Delta} \vdash \mathbf{R}} \text{ cut}}$$

($\wedge^{\text{add}}\mathbf{L}_2$)

$$\frac{\neg_{\mathbf{R}}\overline{\Gamma}, \neg_{\mathbf{R}}\overline{B}, \overline{\Delta} \vdash \mathbf{R} \quad \frac{\frac{\overline{\overline{B \vdash B}} \text{ ax}}{\overline{B} \vdash \overline{A \vee B}} \vee^{\text{add}}\mathbf{R}_2}{\overline{B}, \neg_{\mathbf{R}}(\overline{A} \vee \overline{B}) \vdash \mathbf{R}} \neg_{\mathbf{R}}\mathbf{L}}{\frac{\neg_{\mathbf{R}}\overline{\Gamma}, \neg_{\mathbf{R}}(\overline{A} \vee \overline{B}) \vdash \neg_{\mathbf{R}}\overline{B}}{\neg_{\mathbf{R}}\overline{\Gamma}, \neg_{\mathbf{R}}(\overline{A} \vee \overline{B}), \overline{\Delta} \vdash \mathbf{R}} \text{ cut}}$$

($\vee^{\text{add}}\mathbf{R}_1$)

$$\begin{array}{c}
\frac{\neg_{\mathbf{R}}\overline{\Gamma}, \overline{\Delta}, \overline{A} \vdash \mathbf{R}}{\neg_{\mathbf{R}}\overline{\Gamma}, \overline{\Delta}, \overline{A} \wedge \overline{B} \vdash \mathbf{R}} \wedge^{\text{addL}_1} \\
(\vee^{\text{addR}_2}) \\
\frac{\neg_{\mathbf{R}}\overline{\Gamma}, \overline{\Delta}, \overline{B} \vdash \mathbf{R}}{\neg_{\mathbf{R}}\overline{\Gamma}, \overline{\Delta}, \overline{A} \wedge \overline{B} \vdash \mathbf{R}} \wedge^{\text{addL}_2} \\
(\vee^{\text{addL}}) \\
\frac{\frac{\frac{\overline{A} \vdash \overline{A}}{\overline{A}, \overline{B} \vdash \overline{A}} \text{wkL} \quad \frac{\overline{B} \vdash \overline{B}}{\overline{A}, \overline{B} \vdash \overline{B}} \text{wkL}}{\overline{A}, \overline{B} \vdash \overline{A} \wedge \overline{B}} \wedge^{\text{addR}}}{\frac{\frac{\neg_{\mathbf{R}}\overline{\Gamma}, \neg_{\mathbf{R}}\overline{B}, \overline{\Delta} \vdash \mathbf{R}}{\overline{A}, \neg_{\mathbf{R}}(\overline{A} \wedge \overline{B}) \vdash \neg_{\mathbf{R}}\overline{B}} \neg_{\mathbf{R}}\mathbf{L}}{\overline{A}, \overline{B}, \neg_{\mathbf{R}}(\overline{A} \wedge \overline{B}) \vdash \mathbf{R}} \neg_{\mathbf{R}}\mathbf{L}}}{\overline{A}, \neg_{\mathbf{R}}(\overline{A} \wedge \overline{B}) \vdash \neg_{\mathbf{R}}\overline{B}} \neg_{\mathbf{R}}\mathbf{R}}}{\frac{\neg_{\mathbf{R}}\overline{\Gamma}, \neg_{\mathbf{R}}\overline{B}, \overline{\Delta} \vdash \mathbf{R}}{\neg_{\mathbf{R}}\overline{\Gamma}, \neg_{\mathbf{R}}(\overline{A} \wedge \overline{B}), \overline{\Delta}, \overline{A} \vdash \mathbf{R}} \neg_{\mathbf{R}}\mathbf{R}}}{\neg_{\mathbf{R}}\overline{\Gamma}, \neg_{\mathbf{R}}(\overline{A} \wedge \overline{B}), \overline{\Delta} \vdash \neg_{\mathbf{R}}\overline{A}} \neg_{\mathbf{R}}\mathbf{R}} \text{cut}}}{\frac{\neg_{\mathbf{R}}\overline{\Gamma}, \neg_{\mathbf{R}}\overline{A}, \overline{\Delta} \vdash \mathbf{R}}{\neg_{\mathbf{R}}\overline{\Gamma}, \neg_{\mathbf{R}}(\overline{A} \wedge \overline{B}), \overline{\Delta}, \overline{\Delta} \vdash \mathbf{R}} \text{ctrL}}}{\neg_{\mathbf{R}}\overline{\Gamma}, \neg_{\mathbf{R}}(\overline{A} \wedge \overline{B}), \overline{\Delta}, \overline{\Delta} \vdash \mathbf{R}} \text{ctrL}} \text{cut}}
\end{array}$$

($\rightarrow^{\text{mul}} \mathbf{R}$)

$$\frac{\frac{\frac{\neg_{\mathbf{R}}\overline{\Gamma}, \neg_{\mathbf{R}}\overline{A}, \overline{\Delta}, \overline{B} \vdash \mathbf{R}}{\neg_{\mathbf{R}}\overline{\Gamma}, \neg_{\mathbf{R}}\overline{A} \wedge \overline{B}, \overline{\Delta}, \overline{B} \vdash \mathbf{R}} \wedge^{\text{addL}_1}}{\neg_{\mathbf{R}}\overline{\Gamma}, \neg_{\mathbf{R}}\overline{A} \wedge \overline{B}, \overline{\Delta}, \neg_{\mathbf{R}}\overline{A} \wedge \overline{B} \vdash \mathbf{R}} \wedge^{\text{addL}_2}}}{\neg_{\mathbf{R}}\overline{\Gamma}, \overline{\Delta}, \neg_{\mathbf{R}}\overline{A} \wedge \overline{B} \vdash \mathbf{R}} \text{ctrL}}$$

($\rightarrow^{\text{mul}} \mathbf{L}$)

$$\frac{\frac{\frac{\frac{\overline{\neg_{\mathbf{R}}\overline{A}} \vdash \neg_{\mathbf{R}}\overline{A}}{\neg_{\mathbf{R}}\overline{A}, \overline{B} \vdash \neg_{\mathbf{R}}\overline{A}} \text{wkL} \quad \frac{\overline{B} \vdash \overline{B}}{\neg_{\mathbf{R}}\overline{A}, \overline{B} \vdash \overline{B}} \text{wkL}}{\neg_{\mathbf{R}}\overline{A}, \overline{B} \vdash \neg_{\mathbf{R}}\overline{A} \wedge \overline{B}} \wedge^{\text{addR}}}{\frac{\neg_{\mathbf{R}}\overline{A}, \overline{B} \vdash \neg_{\mathbf{R}}\overline{A} \wedge \overline{B}}{\neg_{\mathbf{R}}\overline{A}, \overline{B}, \neg_{\mathbf{R}}(\neg_{\mathbf{R}}\overline{A} \wedge \overline{B}) \vdash \mathbf{R}} \neg_{\mathbf{R}}\mathbf{L}}}{\neg_{\mathbf{R}}\overline{A}, \neg_{\mathbf{R}}(\neg_{\mathbf{R}}\overline{A} \wedge \overline{B}) \vdash \neg_{\mathbf{R}}\overline{B}} \neg_{\mathbf{R}}\mathbf{R}}}{\frac{\neg_{\mathbf{R}}\overline{\Gamma}, \overline{\Delta}, \overline{A} \vdash \mathbf{R}}{\neg_{\mathbf{R}}\overline{\Gamma}, \overline{\Delta} \vdash \neg_{\mathbf{R}}\overline{A}} \neg_{\mathbf{R}}\mathbf{R}}}{\neg_{\mathbf{R}}\overline{\Gamma}, \neg_{\mathbf{R}}\overline{\Gamma}', \neg_{\mathbf{R}}(\neg_{\mathbf{R}}\overline{A} \wedge \overline{B}), \overline{\Delta}, \overline{\Delta}' \vdash \mathbf{R}} \text{cut}} \text{cut}}$$

($\neg \mathbf{R}$)

$$\frac{\neg_{\mathbf{R}}\overline{\Gamma}, \neg_{\mathbf{R}}\overline{A}, \overline{\Delta} \vdash \mathbf{R}}{(\neg \mathbf{L})}$$

$$\frac{\frac{\frac{\neg_{\mathbf{R}}\overline{\Gamma}, \overline{\Delta}, \overline{A} \vdash \mathbf{R}}{\neg_{\mathbf{R}}\overline{\Gamma}, \overline{\Delta} \vdash \neg_{\mathbf{R}}\overline{A}} \neg_{\mathbf{R}}\mathbf{R}}{\neg_{\mathbf{R}}\overline{\Gamma}, \neg_{\mathbf{R}}\neg_{\mathbf{R}}\overline{A}, \overline{\Delta} \vdash \mathbf{R}} \neg_{\mathbf{R}}\mathbf{L}}$$

(\mathbf{T}^{addR})

$$\frac{}{\neg_{\mathbf{R}}\overline{\Gamma}, \overline{\Delta}, \mathbf{F} \vdash \mathbf{R}} \mathbf{F}^{\text{addL}}$$

(\mathbf{F}^{addL})

$$\frac{\frac{}{\neg_{\mathbf{R}}\overline{\Gamma}, \overline{\Delta} \vdash \mathbf{T}} \mathbf{T}^{\text{addR}}}{\neg_{\mathbf{R}}\overline{\Gamma}, \neg_{\mathbf{R}}\mathbf{T}, \overline{\Delta} \vdash \mathbf{R}} \neg_{\mathbf{R}}\mathbf{L}$$

Remarque : On constate que les règles \wedge^{mul} dans LJ seraient plus adaptées pour cette traduction.

Simulations de l'élimination des coupures

On montrera plus tard ([section 3.2](#)) que ces traductions ne se contentent pas de coder la prouvabilité de LK par la prouvabilité de LJ, mais qu'elles ont également une contrepartie dynamique qui relie l'élimination des coupures dans LK et celle dans LJ.

Chapitre 2

Déduction naturelle

2.1 Logique intuitionniste (NJ)

Présentation arborescente

Une preuve en *déduction naturelle* est un arbre dont les arêtes sont des formules et dont les nœuds sont des règles. Les feuilles de l'arbre sont des formules, certaines sont dites *déchargées*, les autres sont les hypothèses de la preuve.

L'arbre sans nœud (réduit à une simple formule A) est une preuve, et on construit ensuite les preuves à l'aide des règles suivantes :

$$\begin{array}{c}
 \begin{array}{ccc}
 \frac{\begin{array}{c} \vdots \\ A \end{array} \quad \begin{array}{c} \vdots \\ B \end{array}}{A \wedge B} \wedge_{\text{intro}} & \frac{\begin{array}{c} \vdots \\ A \wedge B \end{array}}{A} \wedge_{\text{elim1}} & \frac{\begin{array}{c} \vdots \\ A \wedge B \end{array}}{B} \wedge_{\text{elim2}} \\
 \begin{array}{c} [A] \\ \vdots \\ B \\ \hline A \rightarrow B \end{array} \rightarrow_{\text{intro}} & \frac{\begin{array}{c} \vdots \\ A \rightarrow B \end{array} \quad \begin{array}{c} \vdots \\ A \end{array}}{B} \rightarrow_{\text{elim}} & \\
 \frac{\begin{array}{c} \vdots \\ A \end{array}}{\forall x A} \forall_{\text{intro}} & \frac{\begin{array}{c} \vdots \\ \forall x A \end{array}}{A[t/x]} \forall_{\text{elim}} & \\
 \frac{\begin{array}{c} \vdots \\ A \end{array}}{A \vee B} \vee_{\text{intro1}} & \frac{\begin{array}{c} \vdots \\ B \end{array}}{A \vee B} \vee_{\text{intro2}} & \frac{\begin{array}{c} \vdots \\ A \vee B \end{array} \quad \begin{array}{c} [A] \\ \vdots \\ C \end{array} \quad \begin{array}{c} [B] \\ \vdots \\ C \end{array}}{C} \vee_{\text{elim}} \\
 \frac{}{\top} \top_{\text{intro}} & \frac{\begin{array}{c} \vdots \\ \mathbf{F} \end{array}}{C} \mathbf{F}_{\text{elim}} & \\
 \frac{\begin{array}{c} \vdots \\ A[t/x] \end{array}}{\exists x A} \exists_{\text{intro}} & \frac{\begin{array}{c} \vdots \\ \exists x A \end{array} \quad \begin{array}{c} [A] \\ \vdots \\ C \end{array}}{C} \exists_{\text{elim}} &
 \end{array}
 \end{array}$$

où x ne doit pas être libre dans une hypothèse pour la règle \forall_{intro} et x ne doit être libre ni dans une hypothèse (en fait pas dans les hypothèse de la dérivation de C suffit) ni dans C pour la règle \exists_{elim} .

Une règle qui décharge des hypothèses peut décharger un nombre arbitraire (y compris 0) d'occurrences de la même formule.

On peut obtenir les règles de la négation à travers la définition $\neg A = A \rightarrow F$:

$$\frac{\begin{array}{c} [A] \\ \vdots \\ F \end{array}}{\neg A} \neg_{\text{intro}} \qquad \frac{\begin{array}{c} \vdots \\ \neg A \end{array} \quad \begin{array}{c} \vdots \\ A \end{array}}{F} \neg_{\text{elim}}$$

Présentations en séquents

On considère des séquents de la forme $\Gamma \vdash A$.

$$\frac{}{A \vdash A} ax$$

$$\frac{\Gamma \vdash A \quad \Delta \vdash B}{\Gamma, \Delta \vdash A \wedge B} \wedge_{\text{intro}} \qquad \frac{\Gamma \vdash A \wedge B}{\Gamma \vdash A} \wedge_{\text{elim1}} \qquad \frac{\Gamma \vdash A \wedge B}{\Gamma \vdash B} \wedge_{\text{elim2}}$$

$$\frac{\Gamma \vdash A}{\Gamma \vdash A \vee B} \vee_{\text{intro1}} \qquad \frac{\Gamma \vdash B}{\Gamma \vdash A \vee B} \vee_{\text{intro2}} \qquad \frac{\Gamma \vdash A \vee B \quad \Delta, A, \dots, A \vdash C \quad \Xi, B, \dots, B \vdash C}{\Gamma, \Delta, \Xi \vdash C}$$

$$\frac{\Gamma, A, \dots, A \vdash B}{\Gamma \vdash A \rightarrow B} \rightarrow_{\text{intro}} \qquad \frac{\Gamma \vdash A \rightarrow B \quad \Delta \vdash A}{\Gamma, \Delta \vdash B} \rightarrow_{\text{elim}}$$

$$\frac{}{\vdash T} T_{\text{intro}} \qquad \frac{\Gamma \vdash F}{\Gamma \vdash C} F_{\text{elim}}$$

$$\frac{\Gamma \vdash A}{\Gamma \vdash \forall x A} \forall_{\text{intro}} \qquad \frac{\Gamma \vdash \forall x A}{\Gamma \vdash A[t/x]} \forall_{\text{elim}}$$

$$\frac{\Gamma \vdash A[t/x]}{\Gamma \vdash \exists x A} \exists_{\text{intro}} \qquad \frac{\Gamma \vdash \exists x A \quad \Delta, A, \dots, A \vdash C}{\Gamma, \Delta \vdash C} \exists_{\text{elim}}$$

avec x non libre dans Γ pour la règle \forall_{intro} et dans Δ et C pour la règle \exists_{elim} .

On peut également prendre des règles structurelles explicites :

$$\frac{}{A \vdash A} ax \qquad \frac{\Gamma, A, A \vdash C}{\Gamma, A \vdash C} ctrL \qquad \frac{\Gamma \vdash C}{\Gamma, A \vdash C} wkL$$

$$\frac{\Gamma \vdash A \quad \Delta \vdash B}{\Gamma, \Delta \vdash A \wedge B} \wedge_{\text{intro}} \qquad \frac{\Gamma \vdash A \wedge B}{\Gamma \vdash A} \wedge_{\text{elim1}} \qquad \frac{\Gamma \vdash A \wedge B}{\Gamma \vdash B} \wedge_{\text{elim2}}$$

$$\frac{\Gamma \vdash A}{\Gamma \vdash A \vee B} \vee_{\text{intro1}} \qquad \frac{\Gamma \vdash B}{\Gamma \vdash A \vee B} \vee_{\text{intro2}} \qquad \frac{\Gamma \vdash A \vee B \quad \Delta, A \vdash C \quad \Xi, B \vdash C}{\Gamma, \Delta, \Xi \vdash C} \vee_{\text{elim}}$$

$$\frac{\Gamma, A \vdash B}{\Gamma \vdash A \rightarrow B} \rightarrow_{\text{intro}} \qquad \frac{\Gamma \vdash A \rightarrow B \quad \Delta \vdash A}{\Gamma, \Delta \vdash B} \rightarrow_{\text{elim}}$$

$$\frac{}{\vdash T} T_{\text{intro}} \qquad \frac{\Gamma \vdash F}{\Gamma \vdash C} F_{\text{elim}}$$

$$\frac{\Gamma \vdash A}{\Gamma \vdash \forall x A} \forall_{\text{intro}} \qquad \frac{\Gamma \vdash \forall x A}{\Gamma \vdash A[t/x]} \forall_{\text{elim}} \qquad \frac{\Gamma \vdash A[t/x]}{\Gamma \vdash \exists x A} \exists_{\text{intro}} \qquad \frac{\Gamma \vdash \exists x A \quad \Delta, A \vdash C}{\Gamma, \Delta \vdash C} \exists_{\text{elim}}$$

avec x non libre dans Γ pour la règle \forall_{intro} et dans Δ et C pour la règle \exists_{elim} .

La déduction naturelle offre une syntaxe avec moins de commutations possibles de règles, la représentation des preuves y est donc plus canonique.

Équivalence des différentes présentations

On montre facilement que la première présentation en séquents est parfaitement équivalente à la présentation arborescente.

Une preuve dans la première présentation en séquents de $\Gamma \vdash A$ se traduit en une preuve dans la deuxième du séquent $\Gamma \vdash A$. On le prouve par récurrence sur la taille de la preuve. Un cas typique est celui de la règle \exists_{elim} :

$$\frac{\Gamma \vdash \exists x A \quad \frac{\Delta, A, \dots, A \vdash C}{\Delta, A \vdash C}}{\Gamma, \Delta \vdash C} \exists_{\text{elim}}$$

où, si on a k occurrences de A dans la prémisse de droite, la double ligne correspond à :

- $k - 1$ applications de la règle ctrL si $k > 1$,
- rien si $k = 1$,
- et une application de la règle wkL si $k = 0$.

Réciproquement, en partant d'une preuve du séquent $\Gamma \vdash A$, on peut construire une preuve de $\Gamma' \vdash A$ dans la première présentation en séquents où Γ' est obtenu en dupliquant certaines formules de Γ et en supprimant certaines autres. Les règles structurelles deviennent alors complètement implicites, elles sont intégrées dans les règles qui déchargent des hypothèses. On prouve le résultat par récurrence sur la taille de la preuve. On considère quelques cas typiques :

- (ctrL) Par hypothèse de récurrence, il existe un Γ' obtenu à partir de Γ, A, A en dupliquant certaines formules et en effaçant d'autres. Il est alors également obtenu ainsi à partir de Γ, A . Il suffit donc de prendre la preuve de $\Gamma' \vdash C$ obtenue par hypothèse de récurrence.
- (wkL) Par hypothèse de récurrence, il existe un Γ' obtenu à partir de Γ en dupliquant certaines formules et en effaçant d'autres. Γ' est donc obtenu à partir de Γ, A en supprimant A en plus. Il suffit donc de prendre la preuve de $\Gamma' \vdash C$ obtenue par hypothèse de récurrence.
- (\wedge_{intro}) Par hypothèses de récurrence, on obtient une preuve de $\Gamma' \vdash A$ et une preuve de $\Delta' \vdash B$ avec Γ' et Δ' obtenus à partir de Γ et Δ en dupliquant et en supprimant des formules. Par application de la règle \wedge_{intro} , on obtient une preuve de $\Gamma', \Delta' \vdash A \wedge B$, or Γ', Δ' est bien obtenu à partir de Γ, Δ en dupliquant et en supprimant des formules.
- (\exists_{elim}) Par hypothèses de récurrence, on obtient une preuve de $\Gamma' \vdash \exists x A$ et une preuve de $\Delta' \vdash C$ avec Γ' et Δ' obtenus à partir de Γ et Δ, A en dupliquant et en supprimant des formules. On applique tout d'abord à la preuve de $\Delta' \vdash C$ soit des contractions sur A si A a été dupliquée dans Δ' soit un affaiblissement si A a été supprimé dans Δ' . On obtient ainsi une preuve de $\Delta'', A \vdash C$ (où Δ'' est obtenu en supprimant dans Δ' les occurrences issues de A). Par application de la règle \exists_{elim} , on obtient une preuve de $\Gamma', \Delta'' \vdash C$, or Γ', Δ'' est bien obtenu à partir de Γ, Δ en dupliquant et en supprimant des formules.

Le séquent $\Gamma \vdash A$ est dérivable à partir du séquent $\Gamma' \vdash A$ en utilisant des contractions et des affaiblissements. Les deux séquents coïncident notamment dans le cas particulier d'une unique formule $\vdash A$.

Rédex et normalisation

Fragment réversible. Si on se restreint aux connecteurs réversibles (\wedge , \rightarrow , \top et \vee), un rédex est la succession d'une règle d'introduction et d'une règle d'élimination portant sur la même

occurrence de connecteur. Les rédex s'éliminent de la manière suivante (cas clefs) :

$$\begin{array}{ccc}
\begin{array}{c} \vdots \\ \vdots \\ \frac{A \quad B}{A \wedge B} \wedge_{\text{intro}} \\ \frac{A \wedge B}{A} \wedge_{\text{elim1}} \end{array} & \rightsquigarrow & \begin{array}{c} \vdots \\ A \end{array} \\
\\
\begin{array}{c} \vdots \\ \vdots \\ \frac{A \quad B}{A \wedge B} \wedge_{\text{intro}} \\ \frac{A \wedge B}{B} \wedge_{\text{elim2}} \end{array} & \rightsquigarrow & \begin{array}{c} \vdots \\ B \end{array} \\
\\
\begin{array}{c} [A] \\ \vdots \\ \frac{B}{A \rightarrow B} \rightarrow_{\text{intro}} \\ \frac{A \rightarrow B \quad B}{A} \rightarrow_{\text{elim}} \end{array} & \rightsquigarrow & \begin{array}{c} \dots \\ \vdots \\ A \\ \vdots \\ B \end{array} \\
\\
\begin{array}{c} \vdots \\ \frac{A}{\forall x A} \forall_{\text{intro}} \\ \frac{\forall x A}{A[t/x]} \forall_{\text{elim}} \end{array} & \rightsquigarrow & \begin{array}{c} [t/x] \\ \vdots \\ A[t/x] \end{array}
\end{array}$$

On remarque que les hypothèses peuvent être modifiées lors de la réduction mais il s'agit intuitivement de travailler aux règles structurelles près. Dans le cas clos (preuve sans hypothèse), le problème disparaît.

La preuve de terminaison est une version simplifiée de celle du calcul des séquents. On définit le poids d'un rédex comme la taille de la formule contenant le connecteur introduit et éliminé (appelée *formule de coupure*). Le poids d'une preuve est le multi-ensemble des poids de ses rédex.

Dans les cas \wedge et \forall , le poids de la preuve diminue car on supprime un rédex et si on crée de nouveaux rédex ils portent sur des formules plus petites. Pour le cas \rightarrow , on considère un rédex tel qu'il n'y ait aucun rédex au-dessus de la règle d'élimination, lorsqu'on le réduit, on ne duplique pas de rédex, on peut créer des rédex au niveau des substitutions et au niveau du rédex éliminé mais ils portent sur des formules plus petites. Le poids de la preuve diminue donc (pour l'ordre multi-ensemble).

Contrairement au calcul des séquents, on n'a ici que des cas clefs, c'est ce qui simplifie très nettement la normalisation. Il n'y a pas d'étapes commutatives.

Propriété de la sous-formule. Contrairement au calcul des séquents, il n'y a pas de règle explicite de coupure en déduction naturelle. Cependant on a pu définir une notion de rédex et montrer leur élimination. Un point important est qu'une preuve sans rédex vérifie la propriété de la sous-formule. Ce qui montre la similitude entre coupure et rédex.

Proposition 8 (Sous-formule)

Une preuve de A à partir des hypothèses Γ en déduction naturelle n'utilisant que les règles de \wedge , \rightarrow , \top et \forall et ne contenant pas de rédex ne contient que des sous-formules de Γ et A .

DÉMONSTRATION : Soit C une formule de taille maximale qui n'est pas une sous-formule de la conclusion et des hypothèses, elle est nécessairement prémisses d'une règle d'élimination

(par maximalité), et elle est également conclusion d'une règle d'introduction (par maximalité), on a donc un rédex. \square

Système complet. En présence des connecteurs \vee , \exists et \mathbf{F} , les cas clefs d'élimination des rédex ne vont pas suffire.

$$\begin{array}{ccc}
 \begin{array}{c} \vdots \\ \frac{A}{A \vee B} \vee_{\text{intro}1} \\ \hline C \end{array} & \begin{array}{c} [A] \quad [B] \\ \vdots \quad \vdots \\ C \quad C \\ \vee_{\text{elim}} \end{array} & \rightsquigarrow \begin{array}{c} \dots \quad \vdots \quad \dots \\ A \\ \vdots \\ C \end{array} \\
 \\
 \begin{array}{c} \vdots \\ \frac{B}{A \vee B} \vee_{\text{intro}2} \\ \hline C \end{array} & \begin{array}{c} [A] \quad [B] \\ \vdots \quad \vdots \\ C \quad C \\ \vee_{\text{elim}} \end{array} & \rightsquigarrow \begin{array}{c} \dots \quad \vdots \quad \dots \\ B \\ \vdots \\ C \end{array} \\
 \\
 \begin{array}{c} \vdots \\ \frac{A[t/x]}{\exists x A} \exists_{\text{intro}} \\ \hline C \end{array} & \begin{array}{c} [A] \\ \vdots \\ C \\ \exists_{\text{elim}} \end{array} & \rightsquigarrow \begin{array}{c} \vdots \\ A[t/x] \\ \vdots \\ C \end{array}
 \end{array}$$

Il est nécessaire d'ajouter des réductions commutatives pour obtenir la propriété de la sous-formule (on retrouve un défaut du calcul des séquents).

Exemple 4

Sans réductions supplémentaires, on aurait :

$$\begin{array}{c}
 \begin{array}{c} [C] \quad [C] \\ \vdots \quad \vdots \\ A \quad B \\ \wedge_{\text{intro}} \\ \hline A \wedge B \\ \exists_{\text{elim}} \\ \hline \exists x C \end{array} & \begin{array}{c} \vdots \\ \frac{A \wedge B}{A} \wedge_{\text{elim}1} \end{array}
 \end{array}$$

où $A \wedge B$ viole la propriété de la sous-formule.

On étend la notion de rédex et de réduction aux cas suivants :

$$\begin{array}{ccc}
 \begin{array}{c} \vdots \\ \frac{\mathbf{F}}{C} \mathbf{F}_{\text{elim}} \\ \hline D \end{array} & \begin{array}{c} \vdots \\ R \end{array} & \rightsquigarrow \begin{array}{c} \vdots \\ \frac{\mathbf{F}}{D} \mathbf{F}_{\text{elim}} \end{array} \\
 \\
 \begin{array}{c} [A] \quad [B] \\ \vdots \quad \vdots \\ A \vee B \quad C \quad C \\ \vee_{\text{elim}} \\ \hline C \end{array} & \begin{array}{c} \vdots \\ R \end{array} & \rightsquigarrow \begin{array}{c} [A] \quad [B] \\ \vdots \quad \vdots \\ A \vee B \quad \frac{C}{D} R \quad \frac{C}{D} R \\ \vee_{\text{elim}} \\ \hline D \end{array}
 \end{array}$$

$$\begin{array}{c}
[A] \\
\vdots \\
\exists x A \quad C \\
\hline
C \\
\hline
D \\
\hline
R \\
\exists_{\text{elim}}
\end{array}
\rightsquigarrow
\begin{array}{c}
[A] \\
\vdots \\
\exists x A \quad C \\
\hline
D \\
\hline
R \\
\exists_{\text{elim}}
\end{array}$$

où R est une règle d'élimination dans laquelle C est principale.

Remarque : Il n'est pas possible de définir des étapes commutatives plus générales (*i.e.* sans l'hypothèse “ R règle d'élimination avec C principale” à cause de cas comme :

$$\begin{array}{c}
[A] \quad [C] \quad [D] \\
\vdots \quad \vdots \quad \vdots \\
C \vee D \quad B \quad B \\
\hline
B \\
\hline
A \rightarrow B \\
\hline
\rightarrow_{\text{intro}} \\
\hline
\vee_{\text{elim}}
\end{array}
\rightsquigarrow
\begin{array}{c}
A \\
\vdots \\
C \vee D \\
\hline
B \\
\hline
A \rightarrow B \\
\hline
\rightarrow_{\text{intro}} \\
\hline
B \\
\hline
A \rightarrow B \\
\hline
\rightarrow_{\text{intro}} \\
\hline
\vee_{\text{elim}}
\end{array}$$

où A ne serait plus déchargée et donc on modifierait ce que l'on prouve.

Ce moins bon comportement (l'ajout nécessaire d'étapes commutatives) est lié au fait que les connecteurs sont irréversibles.

Dans ce cadre, où l'on a à la fois des cas clefs et des étapes commutatives, on a les propriétés suivantes : normalisation, propriété de la sous-formule et confluence (nouveau par rapport au calcul des séquents qui est liée à la diminution des commutations possibles de règles).

Exercice 15 (Normalisation)

Étendre la preuve de normalisation du cas réversible au cas complet.

Proposition 9 (Sous-formule)

La propriété de la sous-formule est vraie avec tous les connecteurs si on étend la notion de redex aux cas commutatifs.

DÉMONSTRATION : Par l'absurde, on choisit une formule C qui n'est pas sous-formule des hypothèses ou de la conclusion qui soit de taille maximale et le plus bas possible dans la preuve parmi celles-ci.

On montre que C se trouve nécessairement à un endroit où une étape de réduction s'applique. C est nécessairement principale dans une règle d'élimination sinon il existerait une occurrence de même taille ou plus grosse située plus bas. Si C est conclusion d'une règle d'introduction, une étape clef s'applique. Sinon C est conclusion d'une règle d'élimination irréversible (par maximalité C ne peut pas être conclusion d'une règle d'élimination réversible) et une étape commutative s'applique. \square

Exercice 16 (Confluence)

En suivant le modèle du λ -calcul, montrer la confluence de la normalisation.

Traduction de NJ dans LJ

On a désormais vu deux systèmes différents pour la logique intuitionniste. Afin d'étudier les relations entre ces deux systèmes, on va définir des traductions dans les deux sens.

De NJ dans LJ, les règles d'introduction sont traduites à l'identique, il faut traduire les règles d'élimination :

$$\begin{array}{c}
\frac{\Gamma \vdash A \wedge B}{\Gamma \vdash A} \wedge_{\text{elim1}} \quad \rightsquigarrow \quad \frac{\Gamma \vdash A \wedge B \quad \frac{\overline{A \vdash A} \text{ ax}}{A \wedge B \vdash A} \wedge_{\text{addL}_1}}{\Gamma \vdash A} \text{ cut} \\
\\
\frac{\Gamma \vdash A \wedge B}{\Gamma \vdash B} \wedge_{\text{elim2}} \quad \rightsquigarrow \quad \frac{\Gamma \vdash A \wedge B \quad \frac{\overline{B \vdash B} \text{ ax}}{A \wedge B \vdash B} \wedge_{\text{addL}_2}}{\Gamma \vdash B} \text{ cut} \\
\\
\frac{\Gamma \vdash A \vee B \quad \Delta, A \vdash C \quad \Xi, B \vdash C}{\Gamma, \Delta, \Xi \vdash C} \vee_{\text{elim}} \quad \rightsquigarrow \quad \frac{\Gamma \vdash A \vee B \quad \frac{\frac{\Delta, A \vdash C}{\Delta, \Xi, A \vdash C} \text{ wkL} \quad \frac{\Xi, B \vdash C}{\Delta, \Xi, B \vdash C} \text{ wkL}}{\Delta, \Xi, A \vee B \vdash C} \vee_{\text{addL}}}{\Gamma, \Delta, \Xi \vdash C} \text{ cut} \\
\\
\frac{\Gamma \vdash A \rightarrow B \quad \Delta \vdash A}{\Gamma, \Delta \vdash B} \rightarrow_{\text{elim}} \quad \rightsquigarrow \quad \frac{\Gamma \vdash A \rightarrow B \quad \frac{\Delta \vdash A \quad \overline{B \vdash B} \text{ ax}}{\Delta, A \rightarrow B \vdash B} \rightarrow_{\text{mulL}}}{\Gamma, \Delta \vdash B} \text{ cut} \\
\\
\frac{\Gamma \vdash F}{\Gamma \vdash C} F_{\text{elim}} \quad \rightsquigarrow \quad \frac{\Gamma \vdash F \quad \overline{F \vdash C} F_{\text{addL}}}{\Gamma \vdash C} \text{ cut} \\
\\
\frac{\Gamma \vdash \forall x A}{\Gamma \vdash A[t/x]} \forall_{\text{elim}} \quad \rightsquigarrow \quad \frac{\Gamma \vdash \forall x A \quad \frac{\overline{A[t/x] \vdash A[t/x]} \text{ ax}}{\forall x A \vdash A[t/x]} \forall_{\text{L}}}{\Gamma \vdash A[t/x]} \text{ cut} \\
\\
\frac{\Gamma \vdash \exists x A \quad \Delta, A \vdash C}{\Gamma, \Delta \vdash C} \exists_{\text{elim}} \quad \rightsquigarrow \quad \frac{\Gamma \vdash \exists x A \quad \frac{\Delta, A \vdash C}{\Delta, \exists x A \vdash C} \exists_{\text{L}}}{\Gamma, \Delta \vdash C} \text{ cut}
\end{array}$$

La traduction remplace les règles d'élimination par la règle d'introduction à gauche correspondante, au prix de nombreuses introductions de coupures.

On pourrait également donner une traduction directe des preuves normales en preuves sans coupure.

Simulation de la réduction par la traduction

Lemme 2 (Substitution)

Soient π une preuve de $\Gamma, A \vdash C$ et π' une preuve de $\Delta \vdash A$ dans NJ, on note π^* et π'^* leur traduction dans LJ. La preuve $\frac{\Gamma, A \vdash C \quad \Delta \vdash A}{\Gamma, \Delta \vdash C} \text{ cut}$ se réduit en la traduction de la preuve obtenue en substituant dans π les axiomes qui introduisent A par π' (ce qui donne une preuve de $\Gamma, \Delta \vdash C$).

DÉMONSTRATION : On vérifie tout d'abord que, dans π^* , A a uniquement été introduite par des axiomes (ou des affaiblissements en présence de \vee). L'élimination des coupures effectuée la substitution sur ces axiomes par π'^* . Ceci nous donne exactement la traduction de π substituée par π' . \square

On montre que chaque étape de réduction en déduction naturelle pour le fragment réversible

est simulée par des étapes d'élimination des coupures :

$$\begin{array}{c}
\frac{\frac{\Gamma \vdash A \quad \Gamma \vdash B}{\Gamma \vdash A \wedge B} \wedge^{\text{addR}} \quad \frac{\overline{A \vdash A}^{ax}}{A \wedge B \vdash A} \wedge^{\text{addL}_1} \text{cut}}{\Gamma \vdash A} \rightsquigarrow^2 \Gamma \vdash A \\
\\
\frac{\frac{\Gamma \vdash A \quad \Gamma \vdash B}{\Gamma \vdash A \wedge B} \wedge^{\text{addR}} \quad \frac{\overline{B \vdash B}^{ax}}{A \wedge B \vdash B} \wedge^{\text{addL}_2} \text{cut}}{\Gamma \vdash B} \rightsquigarrow^2 \Gamma \vdash B \\
\\
\frac{\frac{\Gamma, A \vdash B}{\Gamma \vdash A \rightarrow B} \rightarrow^{\text{mulR}} \quad \frac{\Delta \vdash A \quad \overline{B \vdash B}^{ax}}{\Delta, A \rightarrow B \vdash B} \rightarrow^{\text{mulL}} \text{cut}}{\Gamma, \Delta \vdash B} \rightsquigarrow^2 \frac{\Gamma, A \vdash B \quad \Delta \vdash A}{\Gamma, \Delta \vdash B} \text{cut} \\
\\
\frac{\frac{\Gamma \vdash A}{\Gamma \vdash \forall x A} \forall R \quad \frac{\overline{A[t/x] \vdash A[t/x]}^{ax}}{\forall x A \vdash A[t/x]} \forall L \text{cut}}{\Gamma \vdash A[t/x]} \rightsquigarrow^2 \frac{[t/x]}{\Gamma \vdash A[t/x]}
\end{array}$$

il suffit d'utiliser le [lemme 2](#) pour conclure le cas \rightarrow .

On en déduit la terminaison de la réduction en déduction naturelle à partir de celle de l'élimination des coupures dans le calcul des séquents puisque chaque étape de réduction est simulée par au moins une étape d'élimination des coupures.

Pour les connecteurs irréversibles, la simulation n'est plus si simple, on montre que l'on peut simuler par des étapes plus petites d'élimination des coupures, mais on n'a pas montré que cette procédure termine.

Traduction de LJ dans NJ

Les règles droites sont traduites par elles-mêmes. Les règles gauches sont traduites à l'aide de la règle d'élimination correspondante et d'une substitution :

$$\begin{array}{c}
\frac{\Gamma \vdash A \quad \Delta, A \vdash C}{\Gamma, \Delta \vdash C} \text{cut} \rightsquigarrow \begin{array}{c} \Gamma \\ \vdots \\ \Delta \quad A \\ \vdots \\ C \end{array} \\
\\
\frac{\Gamma, A, A \vdash C}{\Gamma, A \vdash C} \text{ctrL} \rightsquigarrow \text{implicite} \\
\\
\frac{\Gamma \vdash C}{\Gamma, A \vdash C} \text{wkL} \rightsquigarrow \text{implicite} \\
\\
\frac{\Gamma, A \vdash C}{\Gamma, A \wedge B \vdash C} \wedge^{\text{addL}_1} \rightsquigarrow \begin{array}{c} \Gamma \quad \frac{A \wedge B}{A} \wedge^{\text{elim1}} \\ \vdots \\ C \end{array} \\
\\
\frac{\Gamma, B \vdash C}{\Gamma, A \wedge B \vdash C} \wedge^{\text{addL}_2} \rightsquigarrow \begin{array}{c} \Gamma \quad \frac{A \wedge B}{B} \wedge^{\text{elim2}} \\ \vdots \\ C \end{array}
\end{array}$$

$$\begin{array}{c}
\frac{\Gamma, B \vdash C \quad \Delta \vdash A}{\Gamma, \Delta, A \rightarrow B \vdash C} \rightarrow^{\text{mul}} \mathbf{L} \quad \rightsquigarrow \quad \Gamma \quad \frac{A \rightarrow B \quad \begin{array}{c} \Delta \\ \vdots \\ A \end{array}}{B} \rightarrow_{\text{elim}} \\
\\
\frac{\Gamma, A[t/x] \vdash C}{\Gamma, \forall x A \vdash C} \forall \mathbf{L} \quad \rightsquigarrow \quad \Gamma \quad \frac{\forall x A}{A[t/x]} \forall_{\text{elim}} \\
\\
\frac{\Gamma, A \vdash C \quad \Gamma, B \vdash C}{\Gamma, A \vee B \vdash C} \vee^{\text{add}} \mathbf{L} \quad \rightsquigarrow \quad \frac{A \vee B \quad \begin{array}{c} \Gamma \quad [A] \\ \vdots \\ C \end{array}}{C} \quad \frac{\Gamma \quad [B]}{\vdots \\ C} \vee_{\text{elim}} \\
\\
\frac{}{\Gamma, \mathbf{F} \vdash C} \mathbf{F}^{\text{add}} \mathbf{L} \quad \rightsquigarrow \quad \frac{\mathbf{F}}{C} \mathbf{F}_{\text{elim}} \\
\\
\frac{\Gamma, A \vdash C}{\Gamma, \exists x A \vdash C} \exists \mathbf{L} \quad \rightsquigarrow \quad \frac{\exists x A \quad \begin{array}{c} \Gamma \quad [A] \\ \vdots \\ C \end{array}}{C} \exists_{\text{elim}}
\end{array}$$

Cette traduction n'est pas injective, on a un quotient donc une meilleure représentation des preuves. Des preuves du calcul des séquents ne différant que par des permutations "anodines" de règles sont identifiées :

$$\begin{array}{c}
\frac{\frac{A, C \vdash E}{A \wedge B, C \vdash E} \wedge^{\text{add}} \mathbf{L}_1}{A \wedge B, C \wedge D \vdash E} \wedge^{\text{add}} \mathbf{L}_1 \quad \rightsquigarrow \quad \frac{A \wedge B}{A} \wedge_{\text{elim1}} \quad \frac{C \wedge D}{C} \wedge_{\text{elim1}} \\
\vdots \\
E \\
\\
\frac{\frac{A, C \vdash E}{A, C \wedge D \vdash E} \wedge^{\text{add}} \mathbf{L}_1}{A \wedge B, C \wedge D \vdash E} \wedge^{\text{add}} \mathbf{L}_1 \quad \rightsquigarrow \quad \frac{A \wedge B}{A} \wedge_{\text{elim1}} \quad \frac{C \wedge D}{C} \wedge_{\text{elim1}} \\
\vdots \\
E
\end{array}$$

Simulation

On peut vérifier que la traduction d'une preuve sans coupure est une déduction en forme normale. En effet, lorsqu'on ajoute une règle d'élimination, la formule principale se retrouve toujours comme hypothèse ce qui ne peut pas créer de rédex au-dessus, ni au-dessous car dans les trois cas irréversible \vee , \mathbf{F} et \exists , la conclusion de la règle est conclusion de la dérivation.

Cependant la réciproque est fautive :

$$\frac{\frac{}{A \vdash A} ax \quad \frac{}{A \vdash A} ax}{A \vdash A} cut \quad \rightsquigarrow \quad A$$

et de même pour les coupures structurelles.

Les cas clefs de l'élimination des coupures dans LJ sont simulés par les réductions de NJ.

Exercice 17

En choisissant les variantes les plus appropriées de LJ et NJ, montrer les détails de cette simulation.

2.2 Logique classique (NK)

Ajout de la règle d'absurde

Pour ré-obtenir la prouvabilité de la logique classique, on peut rajouter la règle d'absurdité :

$$\frac{\vdots}{\neg\neg A} \frac{}{A}$$

Mais cette règle brise la propriété de la sous-formule. La preuve suivante ne peut pas être réduite et viole cette propriété :

$$\begin{array}{c}
 \frac{\frac{\frac{[\neg(A \vee \neg A)]}{\frac{F}{\neg\neg(A \vee \neg A)}}{\neg\neg\text{intro}}}{\neg\neg\text{elim}}}{\frac{[\neg(A \vee \neg A)]}{\frac{F}{A \vee \neg A}}{\vee\text{intro2}}}{\neg\text{intro}}}{\frac{[\neg(A \vee \neg A)]}{\frac{F}{A \vee \neg A}}{\vee\text{intro1}}}{\neg\text{elim}}}
 \end{array}$$

Remarque : On trouve également cette règle sous la forme :

$$\frac{\frac{\vdots}{F}}{A} \frac{[\neg A]}{\neg\text{intro}}$$

Présentation avec séquents à conclusions multiples

On revient à des séquents de la forme $\Gamma \vdash \Delta$.

On profite des conclusions multiples pour revenir à une règle de \vee multiplicative donc réversible, car on a vu que le comportement des règles réversibles est meilleur en déduction naturelle (pas de réductions commutatives).

En l'absence de \exists , on peut utiliser des règles réversibles pour tous les connecteurs :

$$\begin{array}{cc}
 \frac{\Gamma \vdash A, B, \Delta}{\Gamma \vdash A \vee B, \Delta} \vee_{\text{intro}}^{\text{mul}} & \frac{\Gamma \vdash A \vee B, \Delta}{\Gamma \vdash A, B, \Delta} \vee_{\text{elim}}^{\text{mul}} \\
 \frac{\Gamma \vdash \Delta}{\Gamma \vdash F, \Delta} F_{\text{intro}}^{\text{mul}} & \frac{\Gamma \vdash F, \Delta}{\Gamma \vdash \Delta} F_{\text{elim}}^{\text{mul}}
 \end{array}$$

Exemple 5 (Dédutions dans NK)

On peut prouver des formules classiques non intuitionnistes :

$$\frac{\frac{\frac{}{A \vdash A} ax}{\vdash A, \neg A} \neg_{\text{intro}}}{\vdash A \vee \neg A} \vee_{\text{intro}}$$

$$\frac{\frac{\frac{\frac{\overline{A \vdash A}^{ax}}{A \vdash B, A}^{wkR}}{(A \rightarrow B) \rightarrow A \vdash (A \rightarrow B) \rightarrow A}^{ax}}{\vdash A \rightarrow B, A} \rightarrow_{\text{intro}}}{\vdash A \rightarrow B, A} \rightarrow_{\text{elim}}}{\frac{(A \rightarrow B) \rightarrow A \vdash A, A}{(A \rightarrow B) \rightarrow A \vdash A}^{ctrR}} \rightarrow_{\text{intro}} \vdash ((A \rightarrow B) \rightarrow A) \rightarrow A$$

On retrouve $A \rightarrow B = \neg A \vee B$ avec :

$$\frac{\Gamma, A \vdash \Delta}{\Gamma \vdash \neg A, \Delta} \neg_{\text{intro}} \quad \frac{\Gamma \vdash \neg A, \Delta \quad \Gamma' \vdash A, \Delta'}{\Gamma, \Gamma' \vdash \Delta, \Delta'} \neg_{\text{elim}}$$

Rédex et normalisation

Tous les connecteurs ont des règles d'introduction réversibles ce qui dispense des étapes de réduction commutatives que l'on a vues dans NJ. On donne les étapes liées aux nouvelles règles du \vee et du \mathbf{F} :

$$\frac{\frac{\Gamma \vdash A, B, \Delta}{\Gamma \vdash A \vee B, \Delta} \vee_{\text{intro}}^{\text{mul}}}{\Gamma \vdash A, B, \Delta} \vee_{\text{elim}}^{\text{mul}} \rightsquigarrow \Gamma \vdash A, B, \Delta$$

$$\frac{\frac{\Gamma \vdash \Delta}{\Gamma \vdash \mathbf{F}, \Delta} \mathbf{F}_{\text{intro}}^{\text{mul}}}{\Gamma \vdash \Delta} \mathbf{F}_{\text{elim}}^{\text{mul}} \rightsquigarrow \Gamma \vdash \Delta$$

Cependant les multiples conclusions nous imposent une nouvelle sorte d'étape commutative :

$$\frac{\frac{\vdots}{\Gamma_0 \vdash \Delta_0} A_{\text{intro}/ax/\text{elim}}(A)}{\Gamma_1 \vdash A, \Delta_1} \rightsquigarrow \frac{\frac{\vdots}{\Gamma_0 \vdash \Delta_0} A_{\text{intro}/ax/\text{elim}}(A)}{\Gamma_1 \vdash A, \Delta_1} \vdots A_{\text{elim}} \frac{\vdots}{\Gamma_1' \vdash \Delta_1'} \vdots A_{\text{elim}} \frac{\vdots}{\Gamma_2 \vdash A, \Delta_2} \vdots A_{\text{elim}} \frac{\vdots}{\Gamma_3 \vdash \Delta_3} A_{\text{elim}}$$

On peut prouver la terminaison de la réduction comme on l'a fait dans les cas précédents. On peut le montrer comme conséquence de celle du $\lambda\mu$ -calcul simplement typé qui est plus fine.

On en déduit la propriété de la sous-formule.

DÉMONSTRATION : On considère une preuve sans rédex. Si la propriété est fautive, on choisit une occurrence C la plus basse possible parmi celles de taille maximale qui ne sont pas sous-formule des hypothèses ou des conclusions. On va montrer que C apparaît nécessairement dans un rédex ce qui donne une contradiction.

Par maximalité (et puisque qu'elle est la plus basse possible), C est nécessairement prémisses principale d'une règle d'élimination. Si C est conclusion d'une règle d'élimination, C n'est pas maximale. Si C est conclusion d'un axiome, C apparaît dans les hypothèses et ne viole pas la propriété de la sous-formule. Si C est conclusion principale d'une règle d'introduction, on a un cas clef. Sinon C donne lieu à un rédex commutatif. \square

Exercice 18

Étendre les traductions entre LJ et NJ au cas de LK et NK.

Exercice 19

À partir des traductions que l'on a vues de LK dans LJ, construire des traductions de NK dans NJ.

Chapitre 3

Curry-Howard

3.1 Systèmes de typage du λ -calcul

λ -calcul

Étant donné un ensemble dénombrable de variables, les termes du λ -calcul sont donnés par :

$$t ::= x \mid \lambda x.t \mid (t)t$$

où λ est un lieu.

La règle de β -réduction est :

$$(\lambda x.t)u \rightarrow_{\beta} t[u/x]$$

λ -calcul simplement typé additif

Le choix le plus courant de règles de typage pour le λ -calcul simplement typé (*i.e.* avec \rightarrow comme seul constructeur de type) est le suivant :

$$\frac{}{\Gamma, x : A \vdash x : A} \text{ var}$$
$$\frac{\Gamma, x : A \vdash t : B}{\Gamma \vdash \lambda x.t : A \rightarrow B} \text{ lam} \qquad \frac{\Gamma \vdash t : A \rightarrow B \quad \Gamma \vdash u : A}{\Gamma \vdash (t)u : B} \text{ app}$$

où un environnement ne contient jamais deux déclarations de type pour la même variable.

Proposition 10 (Préservation du typage)

Si t se réduit en u et si $\Gamma \vdash t : A$ alors $\Gamma \vdash u : A$.

Lemme 3 (Context minimal)

Si $\Gamma \vdash t : A$ alors $\Gamma' \vdash t : A$ où Γ' est obtenu en ne gardant dans Γ que les déclarations de type pour les variables libres de t .

λ -calcul simplement typé multiplicatif

Un autre choix possible (que l'on utilisera prioritairement ici) de règles de typage pour le λ -calcul simplement typé est le suivant :

$$\frac{}{x : A \vdash x : A} \text{ var}$$
$$\frac{\Gamma, x : A, \dots, x : A \vdash t : B}{\Gamma \vdash \lambda x.t : A \rightarrow B} \text{ lam} \qquad \frac{\Gamma \vdash t : A \rightarrow B \quad \Delta \vdash u : A}{\Gamma, \Delta \vdash (t)u : B} \text{ app}$$

où un environnement peut contenir deux déclarations de type pour la même variable à condition qu'elles soient égales.

Lemme 4 (Variables libres)

Si $\Gamma \vdash t : A$ est dérivable alors Γ contient exactement des déclarations de type pour les variables libres de t .

Proposition 11 (Préservation du typage)

Si t se réduit en u et si $\Gamma \vdash t : A$ alors $\Gamma' \vdash u : A$ où Γ' est obtenu en ne gardant dans Γ que les déclarations de type pour les variables libres de u et en dupliquant éventuellement certaines déclarations de type.

Proposition 12 (Typages additif et multiplicatif)

Si $\Gamma \vdash t : A$ en typage additif alors $\Gamma' \vdash t : A$ en typage multiplicatif où Γ' est obtenu en ne gardant dans Γ que les déclarations de type pour les variables libres de t et en dupliquant éventuellement certaines déclarations de type.

Si $\Gamma \vdash t : A$ en typage multiplicatif alors $\Gamma \vdash t : A$ en typage additif (en identifiant les éventuelles déclarations multiples de variables).

Isomorphisme de Curry-Howard

Découverte essentielle des années 70, la correspondance (ou isomorphisme) de Curry-Howard montre une connexion entre λ -calculs typés et déduction naturelle en logique intuitionniste permettant de donner une interprétation calculatoire aux preuves formelles étudiées en théorie de la démonstration.

Dans un premier temps nous allons nous focaliser sur le λ -calcul simplement typé et la déduction naturelle intuitionniste pour la logique minimale (*i.e.* avec pour seul connecteur \rightarrow).

Il suffit en fait de faire deux observations simples (mais cruciales) :

- Partant d'une dérivation de typage dans le système multiplicatif pour le λ -calcul simplement typé, si on efface toute mention de variable et de terme on obtient une preuve en déduction naturelle. La correspondance règle à règle est exacte !
- Réciproquement, si on part d'une dérivation en déduction naturelle pour la logique intuitionniste minimale, on donne des noms de variables aux hypothèses, des noms de variables aux hypothèses déchargées de manière à ce que deux hypothèses déchargées dans la même règle de $\rightarrow_{\text{intro}}$ aient le même nom (sinon on prend tous les noms distincts). Puis on ajoute des termes aux formules de haut en bas :
 - si la prémisse d'une règle $\rightarrow_{\text{intro}}$ a été annotée t on ajoute $\lambda x.t$ à la conclusion où x est le nom donné aux hypothèses déchargées dans cette occurrence de règle ;
 - si les prémisses d'une règle $\rightarrow_{\text{elim}}$ ont été annotées t et u on ajoute $(t)u$ à la conclusion on obtient alors une dérivation de typage du λ -calcul simplement typé. Au choix des noms de variable près, cette décoration est unique (en particulier unique dans le cas d'une preuve sans hypothèse).

Plutôt que de relier dérivation de typage et preuve, on peut relier directement terme et preuve en ajoutant quelques informations de typage sur les variables libres et les λ -abstractions :

$$t ::= x^A \mid \lambda x^A.t \mid (t)t$$

(en fait dans $\lambda x^A.t$, on supprime les indications de type sur les occurrences de x désormais liées dans t). En effet, pour un tel terme il y a une unique dérivation de typage possible.

Cette correspondance est un isomorphisme au sens où la connexion entre objets s'étend en une connexion entre normalisation des preuves et réduction des λ -termes. Dans le cas où le

seul connecteur est \rightarrow , il n'y a qu'une réduction qui remplace les hypothèses déchargées dans la prémisse de la règle $\rightarrow_{\text{intro}}$ par des copies de la preuve de la seconde prémisse de $\rightarrow_{\text{elim}}$. Si les termes associés à la preuve d'origine sont $\lambda x.t$ et u alors celui associé à la preuve réduite est $t[u/x]$ ce qui correspond exactement à la β -réduction. Réciproquement si on a un β -rédex dans une dérivation de typage du λ -calcul ceci correspond à la succession d'une règle de $\rightarrow_{\text{intro}}$ et d'une règle $\rightarrow_{\text{elim}}$ portant sur le même connecteur dans la preuve obtenue par effacement des termes, donc un rédex.

On obtient le lexique suivant :

logique	λ -calcul	programmation
formule	type	spécification
séquent	jugement	
règle	construction de terme	instruction
preuve	terme	programme
élimination des coupures	β -réduction	calcul
expansion des axiomes	η -expansion	
preuve sans coupure	forme normale	résultat
théorème d'élimination des coupures	normalisation	terminaison
confluence	Church-Rosser	déterminisme

Extension à la logique intuitionniste propositionnelle

Pour étendre la correspondance de Curry-Howard aux autres connecteurs propositionnels, selon le lexique établi ci-dessus, il nous faut définir de nouvelles constructions de termes correspondant à chaque règle :

$$\begin{array}{ll}
\star & (\mathbf{T}_{\text{intro}}) & \langle u, v \rangle & (\wedge_{\text{intro}}) \\
\pi_1 t & (\wedge_{\text{elim1}}) & \pi_2 t & (\wedge_{\text{elim2}}) \\
in_1 t & (\vee_{\text{intro1}}) & in_2 t & (\vee_{\text{intro2}}) \\
\delta t(x.u)(y.v) & (\vee_{\text{elim}}) & \mathcal{A}t & (\mathbf{F}_{\text{elim}})
\end{array}$$

Les règles de typage sont directement données par la décoration des règles de NJ correspondantes :

$$\begin{array}{c}
\frac{}{\vdash \star : \mathbf{T}} \qquad \frac{\Gamma \vdash u : A \quad \Delta \vdash v : B}{\Gamma, \Delta \vdash \langle u, v \rangle : A \wedge B} \qquad \frac{\Gamma \vdash t : A \wedge B}{\Gamma \vdash \pi_1 t : A} \qquad \frac{\Gamma \vdash t : A \wedge B}{\Gamma \vdash \pi_2 t : B} \\
\\
\frac{\Gamma \vdash t : A}{\Gamma \vdash in_1 t : A \vee B} \qquad \frac{\Gamma \vdash t : B}{\Gamma \vdash in_2 t : A \vee B} \\
\\
\frac{\Gamma \vdash t : A \vee B \quad \Delta, x : A \vdash u : C \quad \Xi, y : B \vdash v : C}{\Gamma, \Delta, \Xi \vdash \delta t(x.u)(y.v) : C} \\
\\
\frac{\Gamma \vdash t : \mathbf{F}}{\Gamma \vdash \mathcal{A}t : C}
\end{array}$$

On construit les règles de réduction à partir de la logique :

$$\begin{array}{l}
\pi_1 \langle u, v \rangle \rightsquigarrow u \\
\pi_2 \langle u, v \rangle \rightsquigarrow v \\
\delta in_1 t(x.u)(y.v) \rightsquigarrow u[t/x] \\
\delta in_2 t(x.u)(y.v) \rightsquigarrow v[t/y]
\end{array}$$

ainsi que les étapes commutatives :

$$\begin{aligned}
& \pi_1(\mathcal{A}t) \rightsquigarrow \mathcal{A}t \\
& \pi_2(\mathcal{A}t) \rightsquigarrow \mathcal{A}t \\
& (\mathcal{A}t)u \rightsquigarrow \mathcal{A}t \\
& \delta\mathcal{A}t(x.u)(y.v) \rightsquigarrow \mathcal{A}t \\
& \mathcal{A}\mathcal{A}t \rightsquigarrow \mathcal{A}t \\
& \pi_1(\delta t(x.u)(y.v)) \rightsquigarrow \delta t(x.\pi_1 u)(y.\pi_1 v) \\
& \pi_2(\delta t(x.u)(y.v)) \rightsquigarrow \delta t(x.\pi_2 u)(y.\pi_2 v) \\
& (\delta t(x.u)(y.v))t' \rightsquigarrow \delta t(x.(u)t')(y.(v)t') \\
& \delta(\delta t(x.u)(y.v))(x'.u')(y'.v') \rightsquigarrow \delta t(x.\delta u(x'.u')(y'.v'))(y.\delta v(x'.u')(y'.v')) \\
& \mathcal{A}\delta t(x.u)(y.v) \rightsquigarrow \delta t(x.\mathcal{A}u)(y.\mathcal{A}v)
\end{aligned}$$

Système \mathcal{F} (à la Church)

Les formules de la logique propositionnelle du second ordre sont obtenues en utilisant des variables en logique propositionnelle et en ajoutant des quantificateurs pour ces variables :

$$A ::= X \mid \neg A \mid A \wedge A \mid A \vee A \mid A \rightarrow A \mid \mathbf{T} \mid \mathbf{F} \mid \forall X A \mid \exists X A$$

Pour le calcul des séquents, on ajoute les règles :

$$\begin{array}{cc}
\frac{\Gamma \vdash A, \Delta}{\Gamma \vdash \forall X A, \Delta} \forall R & \frac{\Gamma, A[B/X] \vdash \Delta}{\Gamma, \forall X A \vdash \Delta} \forall L \\
\frac{\Gamma \vdash A[B/X], \Delta}{\Gamma \vdash \exists X A, \Delta} \exists R & \frac{\Gamma, A \vdash \Delta}{\Gamma, \exists X A \vdash \Delta} \exists L
\end{array}$$

avec $X \notin \Gamma, \Delta$ dans les règles $\forall R$ et $\exists L$.

L'élimination des coupures est obtenue comme pour la quantification du premier ordre mais à l'aide d'une substitution de formule (pas de terme). Une conséquence importante est que la taille des formules est modifiée lors de cette substitution ce qui rend impossible notre preuve de normalisation. Il est cependant possible de montrer (par des méthodes sémantiques) que ce calcul est fortement normalisant. D'autre part, la propriété de la sous-formule perd essentiellement son sens pour les formules contenant \exists .

En déduction naturelle intuitionniste, on obtient :

$$\begin{array}{cc}
\frac{\Gamma \vdash A}{\Gamma \vdash \forall X A} \forall_{\text{intro}} & \frac{\Gamma \vdash \forall X A}{\Gamma \vdash A[B/X]} \forall_{\text{elim}} \\
\frac{\Gamma \vdash A[B/X]}{\Gamma \vdash \exists X A} \exists_{\text{intro}} & \frac{\Gamma \vdash \exists X A \quad \Delta, A \vdash C}{\Gamma, \Delta \vdash C} \exists_{\text{elim}}
\end{array}$$

avec $X \notin \Gamma$ dans la règle \forall_{intro} et $X \notin \Delta, C$ dans la règle \exists_{elim} .

La réduction se passe comme au premier ordre avec une substitution de formules à la place d'une substitution de terme.

Le système \mathcal{F} (de Girard) est le λ -calcul typé associé à la déduction naturelle intuitionniste propositionnelle du second ordre restreinte aux connecteurs \rightarrow et \forall .

Les termes sont enrichis avec des constructions correspondant aux nouvelles règles :

$$t ::= x^A \mid \lambda x^A.t \mid (t)t \mid \Lambda X.t \mid (t)A$$

Les règles de typage sont :

$$\begin{array}{c}
\frac{}{x : A \vdash x^A : A} \textit{var} \\
\\
\frac{\Gamma, x : A, \dots, x : A \vdash t : B}{\Gamma \vdash \lambda x^A. t : A \rightarrow B} \textit{lam} \qquad \frac{\Gamma \vdash t : A \rightarrow B \quad \Delta \vdash u : A}{\Gamma, \Delta \vdash (t)u : B} \textit{app} \\
\\
\frac{\Gamma \vdash t : A}{\Gamma \vdash \Lambda X. t : \forall X A} \textit{gen} \qquad \frac{\Gamma \vdash t : \forall X A}{\Gamma \vdash (t)B : A^{[B/X]}} \textit{inst}
\end{array}$$

Il s'agit du système à la Church. Il est également possible de ne rien changer au langage des termes en ne modifiant pas le terme typé dans les règles \forall , mais la correspondance entre preuves et termes n'est plus aussi directe (c'est le système \mathcal{F} à la Curry).

On ajoute une règle de réduction : $(\Lambda X. t)A \rightarrow t^{[A/X]}$.

Puisque le système \mathcal{F} permet de programmer, et en particulier de coder les types de données usuels (booléens, entiers, ...), il est également possible de programmer avec les preuves de logique intuitionniste (ou classique).

Concernant certaines primitives, on obtient deux codages différents en passant par le second ordre ou de manière directe. Par exemple, on peut coder les booléens par $\Lambda X. \lambda x^X. \lambda y^X. x$ et $\Lambda X. \lambda x^X. \lambda y^X. y$ de type $\forall X (X \rightarrow X \rightarrow X)$ ou à l'aide des sommes par in_1^* et in_2^* de type $\mathbf{T} \vee \mathbf{T}$. On a ici des types prouvablement équivalents et qui possèdent tous les deux 2 formes normales et pour lesquels on peut coder un if, ce sont les critères requis pour avoir un bon codage des booléens.

On peut de même comparer le codage des paires par $\Lambda X. \lambda f^{A \rightarrow B \rightarrow X}. (f)uv$ de type $\forall X ((A \rightarrow B \rightarrow X) \rightarrow X)$ et par $\langle u, v \rangle$ de type $A \wedge B$. À nouveau les formules sont équivalentes, les termes consistent bien à mettre ensemble deux termes et on peut coder les deux projections.

Construction du $\lambda\mu$ -calcul simplement typé

La correspondance de Curry-Howard peut être étendue aux systèmes pour la logique classique du moment que leur élimination des coupures est raisonnablement déterministe si on veut obtenir de la confluence dans le λ -calcul associé. Historiquement, il a fallu du temps pour concevoir de tels systèmes (ils sont d'ailleurs apparus grâce à l'étude de Curry-Howard). Du fait de cette contrainte on va travailler avec NK et pas LK.

Afin de définir des jugements de typage de la forme $x_1 : A_1, \dots, x_n : A_n \vdash t : A \mid \alpha_1 : B_1, \dots, \alpha_m : B_m$, on modifie très légèrement NK avec des séquents de la forme $A_1, \dots, A_n \vdash A \mid B_1, \dots, B_m$ où on distingue une formule A qui correspond au type du terme. Les règles sont alors :

$$\begin{array}{c}
\frac{}{A \vdash A \mid} \textit{ax} \\
\\
\frac{\Gamma, A, A \vdash B \mid \Delta}{\Gamma, A \vdash B \mid \Delta} \textit{ctrL} \qquad \frac{\Gamma \vdash B \mid \Delta}{\Gamma, A \vdash B \mid \Delta} \textit{wkL} \\
\\
\frac{\Gamma \vdash B \mid A, A, \Delta}{\Gamma \vdash B \mid A, \Delta} \textit{ctrR} \qquad \frac{\Gamma \vdash B \mid \Delta}{\Gamma \vdash B \mid A, \Delta} \textit{wkR} \\
\\
\frac{\Gamma, A \vdash B \mid \Delta}{\Gamma \vdash A \rightarrow B \mid \Delta} \rightarrow_{\textit{intro}} \qquad \frac{\Gamma \vdash A \rightarrow B \mid \Delta \quad \Gamma' \vdash A \mid \Delta'}{\Gamma, \Gamma' \vdash B \mid \Delta, \Delta'} \rightarrow_{\textit{elim}} \\
\\
\frac{\Gamma \vdash B \mid A, \Delta}{\Gamma \vdash A \mid B, \Delta} \textit{switch}
\end{array}$$

De plus, on a vu qu'il est possible d'incorporer les règles structurelles à gauche dans la règle $\rightarrow_{\text{intro}}$, et de la même manière on peut incorporer les règles structurelles à droite dans la règle *switch* en autorisant un nombre arbitraire de B déjà présents dans le contexte de la prémisse (et identifiés avec le B que l'on ajoute) et en autorisant que A ne soit pas présent dans la prémisse :

$$\frac{\Gamma \vdash B \mid A, B, \Delta}{\Gamma \vdash A \mid B, \Delta} \textit{switch}$$

avec la possibilité que le A et le B du contexte de la prémisse soient absents. On obtient ainsi un système avec 4 règles. On construit alors le $\lambda\mu$ -calcul par Curry-Howard.

Les termes du $\lambda\mu$ -calcul sont donnés par :

$$t ::= x \mid \lambda x.t \mid (t)t \mid \mu\beta[\alpha]t$$

où μ est un lieu pour les μ -variables.

Un terme de la forme $n ::= [\alpha]t$ est appelé un terme *nommé*.

Les jugements de typage sont de la forme $x_1 : A_1, \dots, x_n : A_n \vdash t : A \mid \alpha_1 : B_1, \dots, \alpha_m : B_m$ et les règles de typage pour le calcul simplement typé sont :

$$\frac{}{x : A \vdash x : A} \textit{var} \qquad \frac{\Gamma, x : A \vdash t : B \mid \Delta}{\Gamma \vdash \lambda x.t : A \rightarrow B \mid \Delta} \textit{lam}$$

$$\frac{\Gamma \vdash u : A \rightarrow B \mid \Delta \quad \Gamma' \vdash v : A \mid \Delta'}{\Gamma, \Gamma' \vdash (u)v : B \mid \Delta, \Delta'} \textit{app} \qquad \frac{\Gamma \vdash t : A \mid \beta : B, \Delta}{\Gamma \vdash \mu\beta[\alpha]t : B \mid \alpha : A, \Delta} \textit{mu}$$

Exemple 6 (call/cc)

Le $\lambda\mu$ -terme associé à la loi de Peirce est :

$$\frac{\frac{\frac{\frac{}{x : A \vdash x : A} \textit{var}}{x : A \vdash \mu\delta[\alpha]x : B \mid \alpha : A} \textit{mu}}{\vdash \lambda x.\mu\delta[\alpha]x : A \rightarrow B \mid \alpha : A} \textit{lam}}{\frac{\frac{\frac{}{f : (A \rightarrow B) \rightarrow A \vdash f : (A \rightarrow B) \rightarrow A} \textit{var}}{f : (A \rightarrow B) \rightarrow A \vdash (f)\lambda x.\mu\delta[\alpha]x : A \mid \alpha : A} \textit{app}}{f : (A \rightarrow B) \rightarrow A \vdash \mu\alpha[\alpha](f)\lambda x.\mu\delta[\alpha]x : A \mid \alpha : A} \textit{mu}}{\vdash \lambda f.\mu\alpha[\alpha](f)\lambda x.\mu\delta[\alpha]x : ((A \rightarrow B) \rightarrow A) \rightarrow A \mid \alpha : A} \textit{lam}} \textit{lam}$$

Les règles de réduction sont alors déduites de la réduction des preuves dans NK :

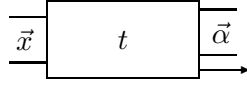
$$\begin{aligned} (\lambda x.t)u &\rightarrow_{\beta} t[u/x] \\ (\mu\alpha.n)u &\rightarrow_{\mu} \mu\alpha.n^{[\alpha](v)u}/[\alpha]v \\ [\beta]\mu\alpha.n &\rightarrow_{\rho} n^{[\beta]/\alpha} \end{aligned}$$

$\lambda\mu$ -calcul pur

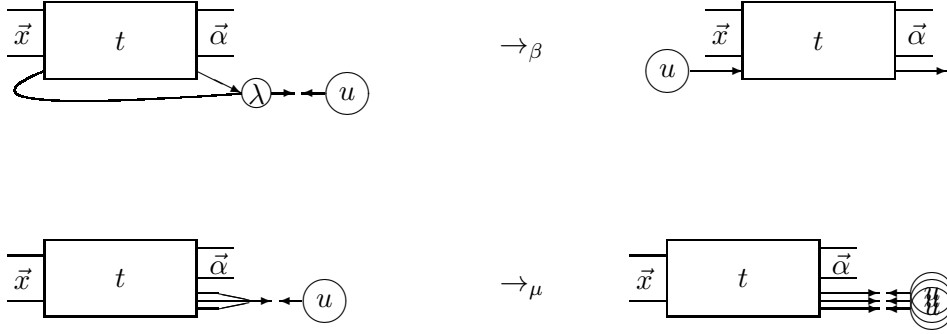
Tout comme pour le λ -calcul pur, on définit le $\lambda\mu$ -calcul pur en oubliant toute mention de type dans le $\lambda\mu$ -calcul simplement typé. Il ne reste alors que les termes et les règles de réduction β , μ et ρ .

Afin de mieux comprendre la signification calculatoire de ces règles de réduction (et notamment de la règle μ), on peut considérer les intuitions suivantes :

- Un $\lambda\mu$ -terme peut être représenté graphiquement comme un objet avec des entrées correspondant à ces λ -variables libres et des sorties : une sortie principale (la seule pour un λ -terme) et des sorties auxiliaires correspondant aux μ -variables libres :



L'application est représentée par le branchement de deux termes sur leur sortie principale. On obtient alors pour les β et μ réductions :



Lorsqu'un argument arrive sur une sortie de la forme λ , il est transféré sur les entrées qui correspondent à la variable liée. Par contre s'il arrive sur une sortie de la forme μ , il est d'abord routé vers toutes les sorties qui demandent cet argument (qui écoutent sur le canal α).

Cette représentation "jouet" prend en fait un sens parfaitement formel dans les réseaux de preuve (voir [section 10.3](#)).

- On peut comprendre le constructeur μ comme un λ infini. Si on change les notations :

$$\begin{aligned}\mu\alpha.n &\rightsquigarrow \lambda\alpha.n \\ [\alpha]t &\rightsquigarrow (t)\alpha\end{aligned}$$

la μ -réduction devient :

$$(\lambda\alpha.n)t \rightarrow \lambda\alpha.n\left[\frac{(u)t\alpha}{(u)\alpha}\right]$$

que l'on peut voir comme une β -réduction avec un λ qui n'est pas consommé et où α est une variable "persistante". Ce λ peut donc recevoir un nombre arbitraire d'arguments.

- De manière générale, la construction μ gère des paquets d'arguments (ou piles) :

$$(\mu\alpha.n)t_1 \dots t_k \rightarrow \mu\alpha.n\left[\frac{[\alpha](u)t_1 \dots t_k}{[\alpha]u}\right]$$

ainsi la pile $t_1 \dots t_k$ est transmise à tous les sous-termes qui la demandent ($[\alpha]u$).

C'est précisément ce qui se passe dans la *machine de Krivine* (KAM). Cette machine qui permet d'évaluer les λ -termes s'étend naturellement au cas du $\lambda\mu$ -calcul avec des opérations de manipulation des piles. Voici une présentation simplifiée (et donc fautive!) de la KAM :

$$\begin{array}{c} \frac{x \quad e \quad \pi}{e(x) \quad e \quad \pi} \quad \frac{\lambda x.t \quad e \quad u::\pi}{t \quad (e+x=u) \quad \pi} \quad \frac{(t)u \quad e \quad \pi}{t \quad e \quad u::\pi} \\ \\ \frac{\mu\alpha.n \quad e \quad \pi}{n \quad (e+\alpha=\pi) \quad \varepsilon} \quad \frac{[\alpha]t \quad e \quad \varepsilon}{t \quad e \quad e(\alpha)}\end{array}$$

où un état de la machine est un triplet $t \ e \ \pi$ avec t un terme, e un environnement (*i.e.* une table qui associe des termes à des λ -variables et des piles à des μ -variables) et π est une pile (*i.e.* une liste de termes).

La construction μ signifie alors “sauver la pile” et $[\alpha]$ signifie “restaurer la pile α ”.

Proposition 13 (Confluence)

La réduction du $\lambda\mu$ -calcul est confluente.

On obtient ainsi une notion de calcul qui étend le λ -calcul (noyau des langages de programmation fonctionnels) avec des *primitives de contrôle* tout en préservant les propriétés essentielles du λ -calcul. On peut ensuite réintroduire le typage et récupérer des propriétés de terminaison.

3.2 CPS-traductions

CPS-traduction issue de la $\neg\neg$ -traduction brutale

On reprend la traduction $(.)^{\neg\neg}$ dans le cadre de la déduction naturelle restreinte au connecteur \rightarrow (on utilise également \mathbf{R} pour coder $\neg_{\mathbf{R}}$). Partant de la légère modification induite par le $\lambda\mu$ -calcul, on utilise un petit raffinement lié à la formule distinguée à droite :

$$(\Gamma \vdash A \mid \Delta)^{\neg\neg} = \neg_{\mathbf{R}}\neg_{\mathbf{R}}\Gamma^{\neg\neg}, \neg_{\mathbf{R}}\Delta^{\neg\neg} \vdash \neg_{\mathbf{R}}\neg_{\mathbf{R}}A^{\neg\neg}$$

$$X^{\neg\neg} = X$$

$$(A \rightarrow B)^{\neg\neg} = \neg_{\mathbf{R}}\neg_{\mathbf{R}}A^{\neg\neg} \rightarrow \neg_{\mathbf{R}}\neg_{\mathbf{R}}B^{\neg\neg}$$

Les règles sont traduites par :

(*ax*)

$$\frac{\frac{\neg_{\mathbf{R}}\neg_{\mathbf{R}}A^{\neg\neg} \vdash \neg_{\mathbf{R}}\neg_{\mathbf{R}}A^{\neg\neg} \quad ax}{\neg_{\mathbf{R}}\neg_{\mathbf{R}}A^{\neg\neg} \vdash \mathbf{R}} \quad \frac{\neg_{\mathbf{R}}A^{\neg\neg} \vdash \neg_{\mathbf{R}}A^{\neg\neg} \quad ax}{\neg_{\mathbf{R}}\neg_{\mathbf{R}}A^{\neg\neg} \vdash \neg_{\mathbf{R}}\neg_{\mathbf{R}}A^{\neg\neg}} \rightarrow_{\text{intro}}}{\neg_{\mathbf{R}}\neg_{\mathbf{R}}A^{\neg\neg} \vdash \neg_{\mathbf{R}}\neg_{\mathbf{R}}A^{\neg\neg}} \rightarrow_{\text{elim}}$$

($\rightarrow_{\text{intro}}$)

$$\frac{\frac{\neg_{\mathbf{R}}(\neg_{\mathbf{R}}\neg_{\mathbf{R}}A^{\neg\neg} \rightarrow \neg_{\mathbf{R}}\neg_{\mathbf{R}}B^{\neg\neg}) \vdash \neg_{\mathbf{R}}(\neg_{\mathbf{R}}\neg_{\mathbf{R}}A^{\neg\neg} \rightarrow \neg_{\mathbf{R}}\neg_{\mathbf{R}}B^{\neg\neg}) \quad ax}{\neg_{\mathbf{R}}\neg_{\mathbf{R}}\Gamma^{\neg\neg}, \neg_{\mathbf{R}}\Delta^{\neg\neg}, \neg_{\mathbf{R}}(\neg_{\mathbf{R}}\neg_{\mathbf{R}}A^{\neg\neg} \rightarrow \neg_{\mathbf{R}}\neg_{\mathbf{R}}B^{\neg\neg}) \vdash \mathbf{R}} \quad \frac{\neg_{\mathbf{R}}\neg_{\mathbf{R}}\Gamma^{\neg\neg}, \neg_{\mathbf{R}}\Delta^{\neg\neg}, \neg_{\mathbf{R}}\neg_{\mathbf{R}}A^{\neg\neg} \vdash \neg_{\mathbf{R}}\neg_{\mathbf{R}}B^{\neg\neg}}{\neg_{\mathbf{R}}\neg_{\mathbf{R}}\Gamma^{\neg\neg}, \neg_{\mathbf{R}}\Delta^{\neg\neg} \vdash \neg_{\mathbf{R}}\neg_{\mathbf{R}}A^{\neg\neg} \rightarrow \neg_{\mathbf{R}}\neg_{\mathbf{R}}B^{\neg\neg}}}{\neg_{\mathbf{R}}\neg_{\mathbf{R}}\Gamma^{\neg\neg}, \neg_{\mathbf{R}}\Delta^{\neg\neg} \vdash \neg_{\mathbf{R}}\neg_{\mathbf{R}}(\neg_{\mathbf{R}}\neg_{\mathbf{R}}A^{\neg\neg} \rightarrow \neg_{\mathbf{R}}\neg_{\mathbf{R}}B^{\neg\neg})} \rightarrow_{\text{intro}}$$

($\rightarrow_{\text{elim}}$)

$$\frac{\frac{\frac{\neg_{\mathbf{R}}\neg_{\mathbf{R}}\Gamma^{\neg\neg}, \neg_{\mathbf{R}}\Delta^{\neg\neg} \vdash \neg_{\mathbf{R}}\neg_{\mathbf{R}}(\neg_{\mathbf{R}}\neg_{\mathbf{R}}A^{\neg\neg} \rightarrow \neg_{\mathbf{R}}\neg_{\mathbf{R}}B^{\neg\neg})}{\neg_{\mathbf{R}}\neg_{\mathbf{R}}\Gamma^{\neg\neg}, \neg_{\mathbf{R}}\Delta^{\neg\neg}, \neg_{\mathbf{R}}\neg_{\mathbf{R}}A^{\neg\neg} \rightarrow \neg_{\mathbf{R}}\neg_{\mathbf{R}}B^{\neg\neg}} \quad ax}{\neg_{\mathbf{R}}\neg_{\mathbf{R}}\Gamma^{\neg\neg}, \neg_{\mathbf{R}}\Delta^{\neg\neg}, \neg_{\mathbf{R}}\neg_{\mathbf{R}}A^{\neg\neg} \rightarrow \neg_{\mathbf{R}}\neg_{\mathbf{R}}B^{\neg\neg}} \quad ax}{\neg_{\mathbf{R}}\neg_{\mathbf{R}}\Gamma^{\neg\neg}, \neg_{\mathbf{R}}\Delta^{\neg\neg}, \neg_{\mathbf{R}}\neg_{\mathbf{R}}A^{\neg\neg} \rightarrow \neg_{\mathbf{R}}\neg_{\mathbf{R}}B^{\neg\neg}} \rightarrow_{\text{intro}}$$

(*mu*)

$$\frac{\frac{\frac{\neg_{\mathbf{R}}\neg_{\mathbf{R}}\Gamma^{\neg\neg}, \neg_{\mathbf{R}}\Delta^{\neg\neg}, \neg_{\mathbf{R}}B^{\neg\neg} \vdash \neg_{\mathbf{R}}\neg_{\mathbf{R}}A^{\neg\neg} \quad ax}{\neg_{\mathbf{R}}\neg_{\mathbf{R}}\Gamma^{\neg\neg}, \neg_{\mathbf{R}}\Delta^{\neg\neg}, \neg_{\mathbf{R}}B^{\neg\neg}, \neg_{\mathbf{R}}A^{\neg\neg} \vdash \mathbf{R}} \quad \frac{\neg_{\mathbf{R}}A^{\neg\neg} \vdash \neg_{\mathbf{R}}A^{\neg\neg} \quad ax}{\neg_{\mathbf{R}}\neg_{\mathbf{R}}A^{\neg\neg} \vdash \neg_{\mathbf{R}}\neg_{\mathbf{R}}A^{\neg\neg}} \rightarrow_{\text{intro}}}{\neg_{\mathbf{R}}\neg_{\mathbf{R}}\Gamma^{\neg\neg}, \neg_{\mathbf{R}}\Delta^{\neg\neg}, \neg_{\mathbf{R}}A^{\neg\neg} \vdash \neg_{\mathbf{R}}\neg_{\mathbf{R}}B^{\neg\neg}} \rightarrow_{\text{intro}}$$

Via Curry-Howard, on obtient une traduction des $\lambda\mu$ -termes simplement typés dans les λ -termes simplement typés (en plongeant les μ -variables dans les λ -variables) :

$$\begin{aligned} x &\rightsquigarrow \lambda k.(x)k \\ \lambda x.t &\rightsquigarrow \lambda k.(k)\lambda x.t^{\neg\neg} \\ (t)u &\rightsquigarrow \lambda k.(t^{\neg\neg})\lambda m.((m)u^{\neg\neg})k \\ [\alpha]t &\rightsquigarrow (t^{\neg\neg})\alpha \\ \mu\alpha.n &\rightsquigarrow \lambda\alpha.n^{\neg\neg} \end{aligned}$$

Proposition 14 (Simulation)

Si $t \rightarrow u$ dans le $\lambda\mu$ -calcul, alors $t^{\neg\neg} =_{\beta} u^{\neg\neg}$ dans le λ -calcul.

DÉMONSTRATION : La traduction de $(\lambda x.t)u$ est $\lambda k.(\lambda k'.(k')\lambda x.t^{\neg\neg})\lambda m.((m)u^{\neg\neg})k$, or :

$$\begin{aligned} \lambda k.(\lambda k'.(k')\lambda x.t^{\neg\neg})\lambda m.((m)u^{\neg\neg})k &\rightarrow \lambda k.(\lambda m.((m)u^{\neg\neg})k)\lambda x.t^{\neg\neg} \\ &\rightarrow \lambda k.((\lambda x.t^{\neg\neg})u^{\neg\neg})k \\ &\rightarrow \lambda k.(t^{\neg\neg}[u^{\neg\neg}/x])k \\ &\rightarrow t^{\neg\neg}[u^{\neg\neg}/x] && \text{car } t^{\neg\neg} \text{ commence par } \lambda \\ &\rightarrow (t[u/x])^{\neg\neg} && \text{car } u^{\neg\neg} \text{ commence par } \lambda \end{aligned}$$

La traduction de $(\mu\alpha.n)u$ est $\lambda k.(\lambda\alpha.n^{\neg\neg})\lambda m.((m)u^{\neg\neg})k$, or :

$$\begin{aligned} \lambda k.(\lambda\alpha.n^{\neg\neg})\lambda m.((m)u^{\neg\neg})k &\rightarrow \lambda k.n^{\neg\neg}[\lambda m.((m)u^{\neg\neg})k/\alpha] \\ &= \lambda\alpha.n^{\neg\neg}[\lambda m.((m)u^{\neg\neg})\alpha/\alpha] \\ &\leftarrow (\mu\alpha.n^{\neg\neg}[\alpha(v)u/\alpha v])^{\neg\neg} \end{aligned}$$

La traduction de $[\beta]\mu\alpha.n$ est $(\lambda\alpha.n^{\neg\neg})\beta$, or $(\lambda\alpha.n^{\neg\neg})\beta \rightarrow n^{\neg\neg}[\beta/\alpha] = (n[\beta/\alpha])^{\neg\neg}$. \square

Remarque : Cette traduction n'est pas surjective :

$$(\neg_{\mathbf{R}}X \vdash \neg_{\mathbf{R}}X)^{\neg\neg} = \neg_{\mathbf{R}}\neg_{\mathbf{R}}(\neg_{\mathbf{R}}X)^{\neg\neg}, \neg_{\mathbf{R}}(\neg_{\mathbf{R}}X)^{\neg\neg} \vdash \mathbf{R} = \neg_{\mathbf{R}}\neg_{\mathbf{R}}\neg_{\mathbf{R}}\neg_{\mathbf{R}}\neg_{\mathbf{R}}X, \neg_{\mathbf{R}}\neg_{\mathbf{R}}\neg_{\mathbf{R}}\neg_{\mathbf{R}}X \vdash \mathbf{R}$$

or $\neg X \vdash \neg X$ n'admet que deux preuves dans NK (resp. LK) et $\neg_{\mathbf{R}}\neg_{\mathbf{R}}\neg_{\mathbf{R}}\neg_{\mathbf{R}}\neg_{\mathbf{R}}X, \neg_{\mathbf{R}}\neg_{\mathbf{R}}\neg_{\mathbf{R}}\neg_{\mathbf{R}}X \vdash \mathbf{R}$ en a beaucoup plus dans NJ (resp. LJ).

CPS-traduction issue de la traduction de Lafont–Reus–Streicher

On reprend la CPS-traduction $\overline{(\cdot)}$ donnée à la [section 1.3](#) appliquée à la déduction naturelle et plus précisément au $\lambda\mu$ -calcul où $\Gamma \vdash A \mid \Delta = \neg_{\mathbf{R}}\overline{\Gamma}, \overline{\Delta} \vdash \neg_{\mathbf{R}}\overline{A}$:

$$\begin{aligned} \overline{x} &= \lambda\alpha.(x)\alpha \\ \overline{\lambda x.t} &= \lambda\alpha.(\overline{t}[\pi_1\alpha/x])\pi_2\alpha \\ \overline{(t)u} &= \lambda\alpha.(\overline{t})\langle \overline{u}, \alpha \rangle \\ \overline{[\alpha]t} &= (\overline{t})\alpha \\ \overline{\mu\alpha.n} &= \lambda\alpha.\overline{n} \end{aligned}$$

On considère le $\lambda\mu$ -calcul muni des réductions β , μ et ρ mais également :

$$\begin{aligned} \lambda x.(t)x &\rightarrow_{\eta} t && x \notin t \\ \mu\alpha[\alpha]t &\rightarrow_{\theta} t && \alpha \notin t \end{aligned}$$

on note $t = u$ si t et u sont reliés par la clôture réflexive, symétrique et transitive de ces règles de réduction.

Proposition 15 (Simulation)

Si $t = u$ alors $\bar{t} = \bar{u}$.

DÉMONSTRATION : On doit valider les réductions β , η , μ , ρ et θ :

$$\begin{aligned}
\overline{(\lambda x.t)u} &= \lambda\alpha.(\lambda\beta.(\bar{t}[\pi_1^\beta/x])\pi_2\beta)\langle\bar{u}, \alpha\rangle \\
&=_{\beta} \lambda\alpha.(\bar{t}[\pi_1^{\langle\bar{u}, \alpha\rangle}/x])\pi_2\langle\bar{u}, \alpha\rangle \\
&=_{\pi_2} \lambda\alpha.(\bar{t}[\pi_1^{\langle\bar{u}, \alpha\rangle}/x])\alpha \\
&=_{\pi_1} \lambda\alpha.(\bar{t}[\bar{u}/x])\alpha =_{\eta} \bar{t}[\bar{u}/x] =_{\eta} \overline{t[u/x]} \\
\overline{\lambda x.(t)x} &= \lambda\alpha.((\lambda\beta.(\bar{t}\langle x, \beta\rangle))[\pi_1^\alpha/x])\pi_2\alpha \\
&= \lambda\alpha.(\lambda\beta.(\bar{t}\langle\pi_1\alpha, \beta\rangle))\pi_2\alpha \\
&=_{\beta} \lambda\alpha.(\bar{t}\langle\pi_1\alpha, \pi_2\alpha\rangle) =_{sp} \lambda\alpha.(\bar{t})\alpha =_{\eta} \bar{t} \\
\overline{(\mu\alpha.n)t} &= \lambda\beta(\lambda\alpha.\bar{n})\langle\bar{t}, \beta\rangle \\
&=_{\beta} \lambda\beta.\bar{n}[\langle\bar{t}, \beta\rangle/\alpha] \\
&= \lambda\beta.\bar{n}[\langle\bar{u}, \bar{t}, \beta\rangle/(\bar{u})\alpha] \\
&=_{\beta} \lambda\beta.\bar{n}[(\lambda\gamma.(\bar{u})\langle\bar{t}, \gamma\rangle)\beta/(\bar{u})\alpha] \\
&= \lambda\beta.n[\langle\beta\rangle(u)t/[\alpha]u] \\
&= \overline{\mu\beta.n[\langle\beta\rangle(u)t/[\alpha]u]} \\
\overline{[\beta]\mu\alpha.n} &= (\lambda\alpha.\bar{n})\beta =_{\beta} \bar{n}[\beta/\alpha] = \overline{n[\beta/\alpha]} \\
\overline{\mu\alpha[\alpha]t} &= \lambda\alpha(\bar{t})\alpha =_{\eta} \bar{t}
\end{aligned}$$

□

Si on regarde précisément l'image de la traduction $\overline{(\cdot)}$, on constate qu'elle n'utilise que des types de la forme $P ::= X \mid \neg_{\mathbf{R}}P \wedge P, \neg_{\mathbf{R}}P$ et \mathbf{R} . On note \mathbf{NJ}_0 ce fragment de \mathbf{NJ} .

Lemme 5

Si π est une preuve de \mathbf{NJ}_0 de $\Gamma \vdash A$ avec Γ sans \mathbf{R} alors tous les séquents de π ont cette propriété.

DÉMONSTRATION : Par récurrence sur la taille de la preuve. En regardant chaque cas de dernière règle :

(ax) On applique l'hypothèse.

($\rightarrow_{\text{intro}}$) La conclusion est nécessairement de la forme $\Gamma \vdash \neg_{\mathbf{R}}P$ donc la prémisse est de la forme $\Gamma, P \vdash \mathbf{R}$ et on applique l'hypothèse de récurrence.

Les autres règles ne modifient pas le contexte. □

On utilisera désormais la notation \mathbf{NJ}_0 pour ce cas particulier. Un séquent est alors de l'une des trois formes :

$$\begin{aligned}
&\neg_{\mathbf{R}}\Gamma, \Delta \vdash P \\
&\neg_{\mathbf{R}}\Gamma, \Delta \vdash \neg_{\mathbf{R}}P \\
&\neg_{\mathbf{R}}\Gamma, \Delta \vdash \mathbf{R}
\end{aligned}$$

Par Curry-Howard, on peut associer à ces preuves des dérivations de typage du λ -calcul avec paires. On va être un peu plus précis en raffinant la grammaire des termes en trois catégories

syntaxiques qui correspondent aux trois sortes de jugements de typage :

$$\begin{aligned} p &::= \alpha \quad | \quad \langle t, p \rangle \quad | \quad \pi_2 p \\ t &::= x \quad | \quad \lambda \alpha. c \quad | \quad \pi_1 p \\ c &::= (t)p \end{aligned}$$

avec des environnements de typage de la forme $\vec{x} : \neg_{\mathbf{R}}\Gamma, \vec{\alpha} : \Delta$.

Les règles de typage obtenues sont :

$$\begin{array}{c} \frac{}{\neg_{\mathbf{R}}\Gamma, \Delta, \alpha : P \vdash \alpha : P} \qquad \frac{\neg_{\mathbf{R}}\Gamma, \Delta \vdash t : \neg_{\mathbf{R}}P \quad \neg_{\mathbf{R}}\Gamma', \Delta' \vdash p : Q}{\neg_{\mathbf{R}}\Gamma, \neg_{\mathbf{R}}\Gamma', \Delta, \Delta' \vdash \langle t, p \rangle : \neg_{\mathbf{R}}P \wedge Q} \qquad \frac{\neg_{\mathbf{R}}\Gamma, \Delta \vdash p : \neg_{\mathbf{R}}P \wedge Q}{\neg_{\mathbf{R}}\Gamma, \Delta \vdash \pi_2 p : Q} \\ \\ \frac{}{\neg_{\mathbf{R}}\Gamma, x : \neg_{\mathbf{R}}P, \Delta \vdash x : \neg_{\mathbf{R}}P} \qquad \frac{\neg_{\mathbf{R}}\Gamma, \Delta, \alpha : P \vdash c : \mathbf{R}}{\neg_{\mathbf{R}}\Gamma, \Delta \vdash \lambda \alpha. c : \neg_{\mathbf{R}}P} \qquad \frac{\neg_{\mathbf{R}}\Gamma, \Delta \vdash p : \neg_{\mathbf{R}}P \wedge Q}{\neg_{\mathbf{R}}\Gamma, \Delta \vdash \pi_1 p : \neg_{\mathbf{R}}P} \\ \\ \frac{\neg_{\mathbf{R}}\Gamma, \Delta \vdash t : \neg_{\mathbf{R}}P \quad \neg_{\mathbf{R}}\Gamma', \Delta' \vdash p : P}{\neg_{\mathbf{R}}\Gamma, \neg_{\mathbf{R}}\Gamma', \Delta, \Delta' \vdash (t)p : \mathbf{R}} \end{array}$$

La traduction $\overline{(\cdot)}$ est donc une traduction du $\lambda\mu$ -calcul dans ce λ -calcul raffiné qui traduit un terme par un terme (t) et un terme nommé par une commande (c) . On va définir une traduction $\widetilde{(\cdot)}$ dans l'autre sens mais, pour simplifier la définition, on ajoute une notation à la syntaxe du $\lambda\mu$ -calcul :

$$\kappa ::= \alpha \quad | \quad t::\kappa \quad | \quad \delta::\kappa$$

et on note :

$$\begin{aligned} [t::\kappa]u &= [\kappa](u)t \\ [\delta::\kappa]u &= [\kappa]\lambda d.u \end{aligned}$$

ce qui définit alors le $\lambda\mu$ -terme $[\kappa]t$ pour un κ et un $\lambda\mu$ -terme t quelconques. Il s'agit donc simplement d'une notation.

La traduction $\widetilde{(\cdot)}$ est donnée par :

$$\begin{aligned} \widetilde{\alpha} &= \alpha \\ \widetilde{\langle t, p \rangle} &= \widetilde{t}::\widetilde{p} \\ \widetilde{\pi_2 p} &= \delta::\widetilde{p} \\ \widetilde{x} &= x \\ \widetilde{\lambda \alpha. c} &= \mu \alpha. \widetilde{c} \\ \widetilde{\pi_1 p} &= \mu \alpha [\widetilde{p}] \lambda x. \mu \delta [\alpha] x \\ \widetilde{(t)p} &= [\widetilde{p}]\widetilde{t} \end{aligned}$$

ce qui traduit un p par un κ , un t par un $\lambda\mu$ -terme et un c par un $\lambda\mu$ -terme nommé.

Proposition 16 (Simulation)

Si $t = u$ alors $\widetilde{t} = \widetilde{u}$.

DÉMONSTRATION : On doit valider les réductions $\beta, \eta, \pi_i (\pi_i \langle t_1, t_2 \rangle \rightarrow_{\pi_i} t_i)$ et $sp (\langle \pi_1 p, \pi_2 p \rangle \rightarrow_{sp}$

p) à l'intérieur des termes. On montre d'abord par récurrence sur κ que $[\kappa]\mu\alpha.n = n^{[\kappa/\alpha]}$:

$$\begin{aligned}
[\beta]\mu\alpha.n &=_{\rho} n^{[\beta/\alpha]} \\
[t::\kappa]\mu\alpha.n &= [\kappa](\mu\alpha.n)t =_{\mu} [\kappa]\mu\alpha.n^{[\alpha](u)t/[\alpha]u} = n^{[\kappa](u)t/[\alpha]u} = n^{[t::\kappa]u/[\alpha]u} = n^{[t::\kappa/\alpha]} \\
[\delta::\kappa]\mu\alpha.n &= [\kappa]\lambda d.\mu\alpha.n \\
&=_{\beta} [\kappa]\lambda x.\mu\alpha.n^{[\alpha](\lambda d.u)x/[\alpha]u} \\
&=_{\mu} [\kappa]\lambda x.(\mu\alpha.n^{[\alpha]\lambda d.u/[\alpha]u})x \\
&=_{\eta} [\kappa]\mu\alpha.n^{[\alpha]\lambda d.u/[\alpha]u} = n^{[\kappa]\lambda d.u/[\alpha]u} = n^{[\delta::\kappa]u/[\alpha]u} = n^{[\delta::\kappa/\alpha]}
\end{aligned}$$

On en déduit simultanément que $\tilde{t} = \tilde{u}$ lorsque $t = u$ pour une des réductions, que $[\tilde{p}]t = [\tilde{q}]t$ si $p = q$ et que $\tilde{c} = \tilde{d}$ si $c = d$:

$$\begin{aligned}
\widetilde{(\lambda\alpha.c)p} &= [\tilde{p}]\mu\alpha.\tilde{c} = \tilde{c}^{[\tilde{p}/\alpha]} = \widetilde{c^{[p/\alpha]}} \\
\widetilde{\lambda\alpha.(t)\alpha} &= \mu\alpha.[\alpha]\tilde{t} =_{\theta} \tilde{t} \\
\widetilde{\pi_1\langle t, p \rangle} &= \mu\alpha[\langle t, p \rangle]\lambda x.\mu\delta[\alpha]x \\
&= \mu\alpha[\tilde{t}::\tilde{p}]\lambda x.\mu\delta[\alpha]x \\
&= \mu\alpha[\tilde{p}](\lambda x.\mu\delta[\alpha]x)\tilde{t} \\
&=_{\beta} \mu\alpha[\tilde{p}]\mu\delta[\alpha]\tilde{t} \\
&= \mu\alpha[\alpha]\tilde{t} =_{\theta} \tilde{t} \\
\widetilde{[\pi_2\langle t, p \rangle]u} &= [\delta::\langle t, p \rangle]u = [\delta::\tilde{t}::\tilde{p}]u = [\tilde{t}::\tilde{p}]\lambda d.u = [\tilde{p}](\lambda d.u)\tilde{t} =_{\beta} [\tilde{p}]u \\
\widetilde{\langle \pi_1 p, \pi_2 p \rangle} t &= [\widetilde{\pi_1 p}::\widetilde{\pi_2 p}]t \\
&= [(\mu\alpha[\tilde{p}]\lambda x.\mu\delta[\alpha]x)::\delta::\tilde{p}]t \\
&= [\delta::\tilde{p}](t)\mu\alpha[\tilde{p}]\lambda x.\mu\delta[\alpha]x \\
&= [\tilde{p}]\lambda d.(t)\mu\alpha[\tilde{p}]\lambda x.\mu\delta[\alpha]x \\
&= [\tilde{p}]\mu\beta[\beta]\lambda d.(t)\mu\alpha[\beta]\lambda x.\mu\delta[\alpha]x \\
&=_{\eta} [\tilde{p}]\lambda x.(\mu\beta[\beta]\lambda d.(t)\mu\alpha[\beta]\lambda x.\mu\delta[\alpha]x)x \\
&=_{\mu} [\tilde{p}]\lambda x.\mu\beta[\beta](\lambda d.(t)\mu\alpha[\beta](\lambda x.\mu\delta[\alpha]x)x)x \\
&=_{\beta} [\tilde{p}]\lambda x.\mu\beta[\beta](t)\mu\alpha[\beta]\mu\delta[\alpha]x \\
&=_{\rho} [\tilde{p}]\lambda x.\mu\beta[\beta](t)\mu\alpha[\alpha]x =_{\theta} [\tilde{p}]\lambda x.(t)\mu\alpha[\alpha]x =_{\theta} [\tilde{p}]\lambda x.(t)x =_{\eta} [\tilde{p}]t
\end{aligned}$$

□

On peut étendre cette traduction aux types et montrer qu'elle respecte le typage :

$$\begin{aligned}
\tilde{X} &= X \\
\neg_{\mathbf{R}}\widetilde{P \wedge Q} &= \tilde{P} \rightarrow \tilde{Q} \\
\vec{x} : \neg_{\mathbf{R}}\Gamma, \widetilde{\vec{\alpha} : \Delta} \vdash t : \neg_{\mathbf{R}}P &= \vec{x} : \tilde{\Gamma} \vdash \tilde{t} : \tilde{P} \mid \vec{\alpha} : \tilde{\Delta} \\
\vec{x} : \neg_{\mathbf{R}}\Gamma, \widetilde{\vec{\alpha} : \Delta} \vdash c : \mathbf{R} &= \vec{x} : \tilde{\Gamma} \vdash \tilde{c} \mid \vec{\alpha} : \tilde{\Delta} \\
\vec{x} : \neg_{\mathbf{R}}\Gamma, \widetilde{\vec{\alpha} : \Delta} \vdash p : P &= \vec{x} : \tilde{\Gamma} \mid \tilde{p} : \tilde{P} \vdash \vec{\alpha} : \tilde{\Delta}
\end{aligned}$$

en utilisant les règles :

$$\frac{\Gamma \vdash t : A \mid \Delta}{\Gamma \vdash [\alpha]t \mid \Delta, \alpha : A} \quad \frac{\Gamma \vdash n \mid \Delta, \alpha : A}{\Gamma \vdash \mu\alpha.n : A \mid \Delta}$$

$$\frac{}{\mid \alpha : A \vdash \alpha : A} \quad \frac{\Gamma \vdash t : A \mid \Delta \quad \Gamma' \mid \kappa : B \vdash \Delta'}{\Gamma, \Gamma' \mid t :: \kappa : A \rightarrow B \vdash \Delta, \Delta'} \quad \frac{\Gamma \mid \kappa : A \rightarrow B \vdash \Delta}{\Gamma \mid \delta :: \kappa : B \vdash \Delta}$$

Proposition 17

Si $\neg_{\mathbb{R}}\Gamma, \Delta \vdash t : \neg_{\mathbb{R}}P$ alors $\tilde{\Gamma} \vdash \tilde{t} : \tilde{P} \mid \tilde{\Delta}$.

DÉMONSTRATION : On montre d'abord, par récurrence sur κ , que si $\Gamma \mid \kappa : A \vdash \Delta$ et $\Gamma' \vdash t : A \mid \Delta'$ alors $\Gamma, \Gamma' \vdash [\kappa]t \mid \Delta, \Delta'$:

$$\frac{\Gamma \vdash t : A \mid \Delta}{\Gamma \vdash [\alpha]t \mid \Delta, \alpha : A}$$

$$\frac{\Gamma \vdash t : A \rightarrow B \mid \Delta \quad \Gamma' \vdash u : A \mid \Delta'}{\Gamma, \Gamma' \vdash (t)u : B \mid \Delta, \Delta'}$$

$$\frac{\Gamma'' \mid \kappa : B \vdash \Delta'' \quad \Gamma, \Gamma' \vdash (t)u : B \mid \Delta, \Delta'}{\Gamma, \Gamma', \Gamma'' \vdash [u :: \kappa]t \mid \Delta, \Delta', \Delta''}$$

$$\frac{\Gamma' \mid \kappa : A \rightarrow B \vdash \Delta' \quad \frac{\Gamma \vdash t : B \mid \Delta}{\Gamma \vdash \lambda d.t : A \rightarrow B \mid \Delta}}{\Gamma, \Gamma' \vdash [\delta :: \kappa]t \mid \Delta, \Delta'}$$

On montre simultanément les cas t , p et c par récurrence :

$$\frac{}{\mid \alpha : \tilde{P} \vdash \alpha : \tilde{P}}$$

$$\frac{\tilde{\Gamma} \vdash \tilde{t} : \tilde{P} \mid \tilde{\Delta} \quad \tilde{\Gamma}' \mid \tilde{p} : \tilde{Q} \vdash \tilde{\Delta}'}{\tilde{\Gamma}, \tilde{\Gamma}' \mid \tilde{t} :: \tilde{p} : \tilde{P} \rightarrow \tilde{Q} \vdash \tilde{\Delta}, \tilde{\Delta}'}$$

$$\frac{\tilde{\Gamma} \mid \tilde{p} : \tilde{P} \rightarrow \tilde{Q} \vdash \tilde{\Delta}}{\tilde{\Gamma} \mid \delta :: \tilde{p} : \tilde{Q} \vdash \tilde{\Delta}}$$

$$\frac{}{x : \tilde{P} \vdash x : \tilde{P} \mid}$$

$$\frac{\tilde{\Gamma} \vdash \tilde{c} \mid \tilde{\Delta}, \alpha : \tilde{P}}{\tilde{\Gamma} \vdash \mu\alpha.\tilde{c} : \tilde{P} \mid \tilde{\Delta}}$$

$$\frac{\frac{x : \tilde{P} \vdash x : \tilde{P} \mid}{x : \tilde{P} \vdash \mu\delta[\alpha]x : \tilde{Q} \mid \alpha : \tilde{P}}}{\tilde{\Gamma} \mid \tilde{p} : \tilde{P} \rightarrow \tilde{Q} \vdash \tilde{\Delta} \quad \vdash \lambda x.\mu\delta[\alpha]x : \tilde{P} \rightarrow \tilde{Q} \mid \alpha : \tilde{P}}}{\tilde{\Gamma} \vdash [\tilde{p}]\lambda x.\mu\delta[\alpha]x \mid \tilde{\Delta}, \alpha : \tilde{P}}$$

$$\frac{\tilde{\Gamma} \vdash \mu\alpha[\tilde{p}]\lambda x.\mu\delta[\alpha]x : \tilde{P} \mid \tilde{\Delta}}{\tilde{\Gamma} \vdash \mu\alpha[\tilde{p}]\lambda x.\mu\delta[\alpha]x : \tilde{P} \mid \tilde{\Delta}}$$

$$\frac{\tilde{\Gamma}' \mid \tilde{p} : \tilde{P} \vdash \tilde{\Delta}' \quad \tilde{\Gamma} \vdash \tilde{t} : \tilde{P} \mid \tilde{\Delta}}{\tilde{\Gamma}, \tilde{\Gamma}' \vdash [\tilde{p}]\tilde{t} \mid \tilde{\Delta}, \tilde{\Delta}'}$$

□

Pour prouver que $\overline{(\cdot)}$ est une bijection, on va montrer que $\widetilde{(\cdot)}$ est son inverse.

Proposition 18 (Plongement)

Les traductions $\overline{(\cdot)}$ et $\widetilde{(\cdot)}$ entre NK et NJ₀ sont inverses l'une de l'autre.

DÉMONSTRATION : On commence par prouver que $\widetilde{\overline{p}} = p$, $\widetilde{\overline{t}} = t$ et $\widetilde{\overline{c}} = c$. Mais avant cela on montre que si on étend la traduction $\overline{(\cdot)}$ par :

$$\begin{aligned}\overline{\alpha} &= \alpha \\ \overline{t::\kappa} &= \langle \overline{t}, \overline{\kappa} \rangle \\ \overline{\delta::\kappa} &= \pi_2 \overline{\kappa}\end{aligned}$$

alors $\overline{[\kappa]t} = (\overline{t})\overline{\kappa}$:

$$\begin{aligned}\overline{[\alpha]t} &= (\overline{t})\alpha = (\overline{t})\overline{\alpha} \\ \overline{[u::\kappa]t} &= \overline{[\kappa](t)u} = (\overline{(t)u})\overline{\kappa} = (\lambda\alpha(\overline{t})\langle \overline{u}, \alpha \rangle)\overline{\kappa} \\ &=_{\beta} (\overline{t})\langle \overline{u}, \overline{\kappa} \rangle = (\overline{t})\overline{u::\kappa} \\ \overline{[\delta::\kappa]t} &= \overline{[\kappa]\lambda d.t} = (\overline{\lambda d.t})\overline{\kappa} = (\lambda\alpha(\overline{t})\pi_2\alpha)\overline{\kappa} \\ &=_{\beta} (\overline{t})\pi_2\overline{\kappa} = (\overline{t})\overline{\delta::\kappa}\end{aligned}$$

On obtient alors :

$$\begin{aligned}\widetilde{\overline{\alpha}} &= \overline{\alpha} = \alpha \\ \widetilde{\overline{\langle t, p \rangle}} &= \widetilde{\overline{t::\overline{p}}} = \widetilde{\langle \overline{t}, \overline{p} \rangle} = \langle t, p \rangle \\ \widetilde{\overline{\pi_2\overline{p}}} &= \widetilde{\overline{\delta::\overline{p}}} = \pi_2\widetilde{\overline{p}} = \pi_2 p \\ \widetilde{\overline{x}} &= \overline{x} = \lambda\alpha.(x)\alpha =_{\eta} x \\ \widetilde{\overline{\lambda\alpha.c}} &= \overline{\mu\alpha.\widetilde{c}} = \lambda\alpha.\widetilde{c} = \lambda\alpha.c \\ \widetilde{\overline{\pi_1\overline{p}}} &= \overline{\mu\alpha[\widetilde{p}]\lambda x.\mu\delta[\alpha]x} \\ &= \lambda\alpha[\widetilde{p}]\lambda x.\mu\delta[\alpha]x \\ &= \lambda\alpha(\overline{\lambda x.\mu\delta[\alpha]x})\widetilde{p} \\ &= \lambda\alpha(\lambda\beta(\lambda d.(\pi_1\beta)\alpha)\pi_2\beta)\widetilde{p} \\ &=_{\beta} \lambda\alpha(\lambda\beta(\pi_1\beta)\alpha)\widetilde{p} \\ &=_{\beta} \lambda\alpha(\pi_1\widetilde{p})\alpha \\ &=_{\eta} \pi_1\widetilde{p} \\ &= \pi_1 p \\ \widetilde{\overline{(t)p}} &= \overline{[\widetilde{p}]t} = (\overline{t})\widetilde{\overline{p}} = (t)p\end{aligned}$$

Réciproquement, on montre que $\widetilde{t} = t$ et $\widetilde{n} = n$:

$$\begin{aligned}
\widetilde{x} &= \lambda\alpha.\widetilde{(x)}\alpha =_{\eta} \widetilde{x} = x \\
\widetilde{\lambda x.t} &= \lambda\alpha.\widetilde{(t[\pi_1\alpha/x])}\pi_2\alpha = \mu\alpha.\widetilde{(t[\pi_1\alpha/x])}\pi_2\alpha = \mu\alpha[\widetilde{\pi_2\alpha}]\widetilde{t}[\pi_1\alpha/x] \\
&= \mu\alpha[\delta::\alpha]\widetilde{t}[\pi_1\alpha/x] = \mu\alpha[\alpha]\lambda d.\widetilde{t}[\pi_1\alpha/x] = \mu\alpha[\alpha]\lambda d.\widetilde{t}[\pi_1\alpha/x] \\
&= \mu\alpha[\alpha]\lambda d.\widetilde{t}[\mu^{\beta[\alpha]}\lambda y.\mu^{\delta[\beta]}y/x] \\
&=_{\eta} \lambda x.(\mu\alpha[\alpha]\lambda d.\widetilde{t}[\mu^{\beta[\alpha]}\lambda y.\mu^{\delta[\beta]}y/x])x \\
&=_{\mu} \lambda x.\mu\alpha[\alpha](\lambda d.\widetilde{t}[\mu^{\beta[\alpha]}(\lambda y.\mu^{\delta[\beta]}y)x/x])x \\
&=_{\beta} \lambda x.\mu\alpha[\alpha]\widetilde{t}[\mu^{\beta[\alpha]}(\lambda y.\mu^{\delta[\beta]}y)x/x] \\
&=_{\beta} \lambda x.\mu\alpha[\alpha]\widetilde{t}[\mu^{\beta[\alpha]}\mu^{\delta[\beta]}x/x] \\
&=_{\rho} \lambda x.\mu\alpha[\alpha]\widetilde{t}[\mu^{\beta[\beta]}x/x] =_{\theta} \lambda x.\mu\alpha[\alpha]\widetilde{t} =_{\theta} \lambda x.\widetilde{t} = \lambda x.t \\
\widetilde{(t)u} &= \lambda\alpha(\widetilde{t})\langle\widetilde{u}, \alpha\rangle = \mu\alpha[\langle\widetilde{u}, \alpha\rangle]\widetilde{t} = \mu\alpha[\widetilde{u}::\widetilde{\alpha}]\widetilde{t} = \mu\alpha[\widetilde{u}::\alpha]\widetilde{t} = \mu\alpha[\alpha](\widetilde{t})\widetilde{u} =_{\theta} (\widetilde{t})\widetilde{u} = (t)u \\
\widetilde{[\alpha]t} &= (\widetilde{t})\alpha = [\widetilde{\alpha}]\widetilde{t} = [\alpha]\widetilde{t} = [\alpha]t \\
\widetilde{\mu\alpha.\widetilde{n}} &= \widetilde{\lambda\alpha.\widetilde{n}} = \mu\alpha.\widetilde{n} = \mu\alpha.n
\end{aligned}$$

□

Interprétation calculatoire

Si on s'intéresse uniquement au cas non typé, les CPS-traductions consistent à simuler le calcul classique à l'aide du calcul intuitionniste (ou à coder les primitives de contrôle dans les langages fonctionnels).

La μ -réduction permet de propager les éléments de la pile les uns après les autres aux sous-termes qui les demandent. Regardons ici ce que fait $(t)u_1 \dots u_n$:

$$\begin{aligned}
((t)u_1u_2u_3)^{\neg\neg} &= \lambda k_3.(\lambda k_2.(\lambda k_1.(t)\lambda m.((m)u_1)k_1)\lambda m.((m)u_2)k_2)\lambda m.((m)u_3)k_3 \\
&\rightarrow \lambda k_3.(\lambda k_2.((t)\lambda m.((m)u_1)\lambda m.((m)u_2)k_2))\lambda m.((m)u_3)k_3 \\
&\rightarrow \lambda k_3.(t)\lambda m.((m)u_1)\lambda m.((m)u_2)\lambda m.((m)u_3)k_3 \\
\overline{((t)u_1u_2u_3)} &= \lambda\alpha_3.(\lambda\alpha_2.(\lambda\alpha_1.(t)\langle u_1, \alpha_1\rangle)\langle u_2, \alpha_2\rangle)\langle u_3, \alpha_3\rangle \\
&\rightarrow \lambda\alpha_3.(\lambda\alpha_2.(t)\langle u_1, \langle u_2, \alpha_2\rangle\rangle)\langle u_3, \alpha_3\rangle \\
&\rightarrow \lambda\alpha_3.(t)\langle u_1, \langle u_2, \langle u_3, \alpha_3\rangle\rangle\rangle
\end{aligned}$$

On a affaire à des codages des listes :

$$\begin{aligned}
\lambda m.((m)u_1)\lambda m.((m)u_2)\lambda m.((m)u_3)k &= \text{Cons } u_1 (\text{Cons } u_2 (\text{Cons } u_3 k)) \\
\langle u_1, \langle u_2, \langle u_3, k\rangle\rangle\rangle &= \text{Cons } u_1 (\text{Cons } u_2 (\text{Cons } u_3 k))
\end{aligned}$$

Avec le premier codage, on récupère la tête de liste par $(l)\lambda x.\lambda y.x$ et la queue par $(l)\lambda x.\lambda y.y$. De manière générale $(\text{Cons } ul)\lambda x.t$ se réduit en $(t[u/x])l$. Avec le second codage, on obtient la tête de liste par $\pi_1 l$ et la queue par $\pi_2 l$. On a, dans les deux cas, la concaténation de listes par $l[l'/k]$ qui rajoute l' à la fin de l .

Ainsi un terme est traduit comme un fonction qui prend une liste comme argument (cette liste code la pile d'exécution) : $\neg_R \neg_R A^{\neg\neg}$ prend $\neg_R A^{\neg\neg}$ comme argument et $\neg_R \overline{A}$ prend \overline{A} comme

argument. On s'intéresse au calcul sur des objets clos (de type \mathbb{R}) : un terme et une pile associée. Il faut donc comprendre ce que vaut $(t^\bullet)l$ (où t^\bullet est l'une des deux traductions appliquée à t).

$$\begin{array}{lll}
 (x^\bullet)l & \rightsquigarrow & (x)l \quad \text{(la valeur du terme n'est pas encore connue)} \\
 ((\lambda x.t)^\bullet)\text{Cons } ul & \rightsquigarrow & (t^\bullet[u/x])l \\
 (((t)u)^\bullet)l & \rightsquigarrow & (t^\bullet)\text{Cons } u^\bullet l \\
 ((\mu\alpha.n)^\bullet)l & \rightsquigarrow & n^\bullet[l/\alpha]
 \end{array}$$

On a ainsi une gestion dynamique des piles qui peuvent se construire à tout moment.

Chapitre 4

Sémantique catégorique

4.1 Notions catégoriques élémentaires

Définition 3 (Catégorie)

Une *catégorie* \mathbb{C} est la donnée d'une classe d'*objets* et, pour chaque paire d'objets A et B , d'une classe de *morphismes* $\mathbb{C}(A, B)$ ainsi que :

- des identités $id_A \in \mathbb{C}(A, A)$ pour chaque A
 - une composition : $\mathbb{C}(A, B) \times \mathbb{C}(B, C) \rightarrow \mathbb{C}(A, C)$ pour tout A, B, C , notée $(f, g) \mapsto f ; g$
- tels que, si $f \in \mathbb{C}(A, B)$, $g \in \mathbb{C}(B, C)$ et $h \in \mathbb{C}(C, D)$:

$$\begin{aligned}id_A ; f &= f \\f ; id_B &= f \\(f ; g) ; h &= f ; (g ; h)\end{aligned}$$

Exemple 7 (Quelques catégories)

Voici quelques catégories classiques :

- Les monoïdes correspondent aux catégories à un seul objet. Les éléments du monoïde sont les flèches de cet objet dans lui-même.
- Les pré-ordres correspondent aux catégories avec au plus un morphisme de chaque objet dans un autre. Les objets sont les points du pré-ordre et il y a un morphisme de A dans B si $A \leq B$.
- Les ensembles munis des fonctions forment la *catégorie des ensembles*.
- Les groupes munis des morphismes de groupes forment la *catégorie des groupes*.
- De manière plus générale, les structures algébriques usuelles et les morphismes associés forment des catégories.
- ...

Définition 4 (Isomorphisme)

Soient \mathbb{C} une catégorie et A et B deux objets de \mathbb{C} , un *isomorphisme* de A dans B est un morphisme f de A dans B tel qu'il existe un morphisme g de B dans A avec $f ; g = id_A$ et $g ; f = id_B$.

Définition 5 (Catégorie duale)

Si \mathbb{C} est une catégorie, la *catégorie duale* \mathbb{C}^{op} a les mêmes objets que \mathbb{C} et on retourne les morphismes : $\mathbb{C}^{op}(A, B) = \mathbb{C}(B, A)$. Les identités sont les mêmes et la composition est retournée également.

Définition 6 (Catégorie produit)

Si \mathbb{C} et \mathbb{D} sont deux catégories, la *catégorie produit* $\mathbb{C} \times \mathbb{D}$ a :

- pour objets les paires d'objets (A, A') avec $A \in \mathbb{C}$ et $A' \in \mathbb{D}$
- pour morphismes les paires de morphismes : $\mathbb{C} \times \mathbb{D}((A, A'), (B, B')) = \mathbb{C}(A, B) \times \mathbb{D}(A', B')$.

Les identités sont les paires d'identités et la composition est obtenue composante par composante.

Définition 7 (Produit)

Soient \mathbb{C} une catégorie et A et B des objets de \mathbb{C} , un *produit* de A et B est un triplet $(A \times B, \pi_A, \pi_B)$ où $A \times B$ est un objet de \mathbb{C} , $\pi_A \in \mathbb{C}(A \times B, A)$ et $\pi_B \in \mathbb{C}(A \times B, B)$ tel que pour tout objet C de \mathbb{C} , tout $f \in \mathbb{C}(C, A)$ et tout $g \in \mathbb{C}(C, B)$, il existe un *unique* $\langle f, g \rangle \in \mathbb{C}(C, A \times B)$ tel que $\langle f, g \rangle ; \pi_A = f$ et $\langle f, g \rangle ; \pi_B = g$.

Un *co-produit* de A et B est un produit dans \mathbb{C}^{op} . On le note alors $(A + B, in_A, in_B)$.

Exercice 20 (Unicité du produit)

Montrer qu'un produit est unique à isomorphisme près.

Définition 8 (Objet terminal)

Soit \mathbb{C} une catégorie, un *objet terminal* dans \mathbb{C} est un objet \top tel qu'il existe exactement un morphisme dans $\mathbb{C}(A, \top)$ pour chaque A , noté $term_A$.

Un *objet initial* 0 dans \mathbb{C} est un objet terminal dans \mathbb{C}^{op} .

Définition 9 (Foncteur)

Soient \mathbb{C} et \mathbb{D} deux catégories, un *foncteur* F de \mathbb{C} dans \mathbb{D} est une fonction des objets de \mathbb{C} dans les objets de \mathbb{D} et des morphismes de $\mathbb{C}(A, B)$ dans les morphismes de $\mathbb{D}(F(A), F(B))$ (pour tout A, B) telle que, si $f \in \mathbb{C}(A, B)$ et $g \in \mathbb{C}(B, C)$:

$$\begin{aligned} F(id_A) &= id_{F(A)} \\ F(f ; g) &= F(f) ; F(g) \end{aligned}$$

Un *foncteur contravariant* de \mathbb{C} dans \mathbb{D} est un foncteur de \mathbb{C}^{op} dans \mathbb{D} .

Exemple 8 (Catégorie des catégories)

En prenant comme objets les catégories et comme morphismes les foncteurs, on obtient la *catégorie des catégories*.

Définition 10 (Bifoncteur)

Soient \mathbb{C} , \mathbb{D} et \mathbb{E} des catégories, un *foncteur binoïdal* F de \mathbb{C} et \mathbb{D} dans \mathbb{E} est donné par :

- un foncteur F_A de \mathbb{D} dans \mathbb{E} pour tout objet A de \mathbb{C}
- un foncteur $F^{A'}$ de \mathbb{C} dans \mathbb{E} pour tout objet A' de \mathbb{D}

tels que $F_A(A') = F^{A'}(A)$ pour tout objet A de \mathbb{C} et tout objet A' de \mathbb{D} .

On note alors $F(A, _)$ pour $F_A(_)$ et $F(_, A')$ pour $F^{A'}(_)$ ce qui définit les notations $F(A, A')$ ($= F_A(A') = F^{A'}(A)$), $F(A, f')$ et $F(f, A')$ mais pas $F(f, f')$!

Un *bifoncteur* de \mathbb{C} et \mathbb{D} dans \mathbb{E} est un foncteur binoïdal tel que le diagramme suivant commute :

$$\begin{array}{ccc} F(A, A') & \xrightarrow{F(A, f')} & F(A, B') \\ F(f, A') \downarrow & & \downarrow F(f, B') \\ F(B, A') & \xrightarrow{F(B, f')} & F(B, B') \end{array}$$

on peut alors noter $F(f, f') = F(A, f') ; F(f, B') = F(f, A') ; F(B, f') \in \mathbb{E}(F(A, A'), F(B, B'))$.

Exercice 21

Montrer qu'un bifoncteur de \mathbb{C} et \mathbb{D} dans \mathbb{E} est la même chose qu'un foncteur de $\mathbb{C} \times \mathbb{D}$ dans \mathbb{E} .

Définition 11 (Transformation naturelle)

Soient \mathbb{C} et \mathbb{D} deux catégories et F et G deux foncteurs de \mathbb{C} dans \mathbb{D} , une *transformation naturelle* α de F dans G est donnée par une famille $(\alpha_A)_{A \in \mathbb{C}}$ de morphismes de $F(A)$ dans $G(A)$ telle que pour tout $f \in \mathbb{C}(A, B)$, le diagramme suivant commute :

$$\begin{array}{ccc} F(A) & \xrightarrow{F(f)} & F(B) \\ \alpha_A \downarrow & & \downarrow \alpha_B \\ G(A) & \xrightarrow{G(f)} & G(B) \end{array}$$

Définition 12 (Adjonction)

Soient \mathbb{C} et \mathbb{D} deux catégories, F un foncteur de \mathbb{D} dans \mathbb{C} et G un foncteur de \mathbb{C} dans \mathbb{D} , une *adjonction* φ entre F et G est une bijection entre $\mathbb{C}(F(A'), A)$ et $\mathbb{D}(A', G(A))$ (pour tout objet A' de \mathbb{D} et tout objet A de \mathbb{C}) telle que, si $f' \in \mathbb{D}(B', A')$ et $f \in \mathbb{C}(A, B)$ le diagramme suivant commute :

$$\begin{array}{ccc} \mathbb{C}(F(A'), A) & \xrightarrow{F(f'); \dashv f} & \mathbb{C}(F(B'), B) \\ \varphi \downarrow & & \downarrow \varphi \\ \mathbb{D}(A', G(A)) & \xrightarrow{f'; \dashv G(f)} & \mathbb{D}(B', G(B)) \end{array}$$

on note souvent :

$$\frac{F(A') \rightarrow A}{A' \rightarrow G(A)} \varphi$$

S'il existe une adjonction entre F et G , on dit que F est adjoint à gauche de G (resp. G est adjoint à droite de F), noté $F \dashv G$.

Si $F \dashv G$, on peut définir deux transformations naturelles :

$$\begin{aligned} \varepsilon_A &= \varphi^{-1}(id_{G(A)}) \in \mathbb{C}(F(G(A)), A) \\ \eta_{A'} &= \varphi(id_{F(A')}) \in \mathbb{D}(A', G(F(A'))) \end{aligned}$$

donc ε est une transformation naturelle du foncteur $F \circ G$ dans le foncteur id et η est une transformation naturelle du foncteur id dans le foncteur $G \circ F$. De plus :

$$\begin{aligned} F(_) &= F(\eta_{_}); \varepsilon_{F(_)} \\ G(_) &= \eta_{G(_)}; G(\varepsilon_{_}) \end{aligned}$$

4.2 Catégories cartésiennes fermées

Définitions

Définition 13 (Catégorie cartésienne)

Une *catégorie cartésienne* est donnée par :

- un produit pour chaque paire d'objets
- un objet terminal

Exercice 22

Montrer que, si \mathbb{C} est une catégorie cartésienne, $(A, B) \mapsto A \times B$ définit un bifoncteur de \mathbb{C} et \mathbb{C} dans \mathbb{C} .

Montrer que $\langle f, g \rangle = \langle id, id \rangle ; f \times g$.

Dans une catégorie cartésienne, on peut définir les morphismes suivants :

$$\begin{aligned}
term_A & : A \longrightarrow \top \\
\Delta_A & : A \longrightarrow A \times A & = \langle id_A, id_A \rangle \\
\gamma_{A,B}^\times & : A \times B \xrightarrow{\sim} B \times A & = \langle \pi_B, \pi_A \rangle \\
unit_A^\times & : A \xrightarrow{\sim} A \times \top & = \langle id_A, term_A \rangle \\
assoc_{A,B,C}^\times & : (A \times B) \times C \xrightarrow{\sim} A \times (B \times C) & = \langle \pi_{A \times B}; \pi_A, \langle \pi_{A \times B}; \pi_B, \pi_C \rangle \rangle
\end{aligned}$$

Exercice 23

Montrer que $\pi_A = id_A \times term_B; unit_A^{\times -1}$.

Exercice 24

Montrer que les isomorphismes ci-dessus sont bien des isomorphismes.

Exercice 25

Montrer que les familles de morphismes ci-dessus sont des transformations naturelles.

Dans ce qui suit, on omettra souvent les morphismes d'associativité.

Définition 14 (Catégorie cartésienne fermée)

Une catégorie cartésienne $(\mathbb{C}, \times, \top)$ est *cartésienne fermée* si, pour chaque objet A , le foncteur $_ \times A$ de \mathbb{C} dans \mathbb{C} a un adjoint à droite que l'on note $A \rightarrow _$ (appelé *exponentiation cartésienne*). On note *curry* cette adjonction.

Dans une catégorie cartésienne fermée, on peut définir les morphismes suivants :

$$ev_{A,B} : (A \rightarrow B) \times A \longrightarrow B = curry^{-1}(id_{A \rightarrow B})$$

Lemme 6 (Naturalité de l'évaluation)

Pour tout objet A , la famille $(ev_{A,B})_{B \in \mathbb{C}}$ est une transformation naturelle :

$$\begin{array}{ccc}
(A \rightarrow B) \times A & \xrightarrow{(A \rightarrow f) \times A} & (A \rightarrow B') \times A \\
ev_{A,B} \downarrow & & \downarrow ev_{A,B'} \\
B & \xrightarrow{f} & B'
\end{array}$$

DÉMONSTRATION : On a $curry(ev_{A,B}; f) = A \rightarrow f = curry((A \rightarrow f) \times A; ev_{A,B'})$ donc le diagramme commute puisque *curry* est une bijection. \square

Proposition 19 (Bifoncteur flèche)

$(A \rightarrow _)_{A \in \mathbb{C}}$ s'étend en un bifoncteur $_ \rightarrow _$ de \mathbb{C}^{op} et \mathbb{C} dans \mathbb{C} (on dit qu'il est contravariant à gauche et covariant à droite).

DÉMONSTRATION : Si $f \in \mathbb{C}(A', A)$ et $g \in \mathbb{C}(B, B')$, on définit $f \rightarrow g = curry((A \rightarrow B) \times f; ev_{A,B}; g) \in \mathbb{C}(A \rightarrow B, A' \rightarrow B')$.

Si $f' \in \mathbb{C}(A'', A')$ et $g' \in \mathbb{C}(B', B'')$, le diagramme suivant commute :

$$\begin{array}{ccccc}
(A \rightarrow B) \times A'' & \xrightarrow{(f \rightarrow B) \times A''} & (A' \rightarrow B) \times A'' & \xrightarrow{(A' \rightarrow g) \times A''} & (A' \rightarrow B') \times A'' \\
\downarrow (A \rightarrow B) \times f' & & \downarrow (A' \rightarrow B) \times f' & & \downarrow (A' \rightarrow B') \times f' \\
(A \rightarrow B) \times A' & \xrightarrow{(f \rightarrow B) \times A'} & (A' \rightarrow B) \times A' & \xrightarrow{(A' \rightarrow g) \times A'} & (A' \rightarrow B') \times A' \\
\downarrow (A \rightarrow B) \times f & & \downarrow ev_{A', B} & & \downarrow ev_{A', B'} \\
(A \rightarrow B) \times A & & & & \\
\searrow ev_{A, B} & & & & \\
& & B & \xrightarrow{g} & B'
\end{array}$$

Les deux premiers carrés commutent par functorialité de \times . Le troisième carré commute parce que $curry(h) \times A ; ev_{A, B} = h$ si $h \in \mathbb{C}((A' \rightarrow B) \times A, B)$ puisque $curry$ est une adjonction. Enfin le quatrième carré commute par le [lemme 6](#).

Si on compose à droite par g' et si on applique $curry$ à chacun des deux bords du diagramme, on obtient :

$$\begin{aligned}
& curry(((f \rightarrow B) ; (A' \rightarrow g)) \times A'' ; (A' \rightarrow B') \times f' ; ev_{A', B'} ; g') \\
&= (f \rightarrow B) ; (A' \rightarrow g) ; curry((A' \rightarrow B') \times f' ; ev_{A', B'} ; g') \\
&= curry((A \rightarrow B) \times f ; ev_{A, B}) ; (A' \rightarrow g) ; f' \rightarrow g' \\
&= curry((A \rightarrow B) \times f ; ev_{A, B} ; g) ; f' \rightarrow g' \\
&= f \rightarrow g ; f' \rightarrow g'
\end{aligned}$$

et $curry((A \rightarrow B) \times (f' ; f) ; ev_{A, B} ; g ; g') = (f' ; f) \rightarrow (g ; g')$ qui sont donc égaux. \square

Interprétation du λ -calcul

Soit \mathbb{C} une catégorie cartésienne fermée, on va définir une interprétation des λ -termes simplement typés par des morphismes de \mathbb{C} qui traduit la β -réduction et la η -réduction par l'égalité. On dit alors que \mathbb{C} est un *modèle dénotationnel* du λ -calcul simplement typé.

On suppose fixée une interprétation de chaque variable de type X par un objet $\llbracket X \rrbracket$ de \mathbb{C} . Un type est interprété par un objet de \mathbb{C} par $\llbracket A \rightarrow B \rrbracket = \llbracket A \rrbracket \rightarrow \llbracket B \rrbracket$.

Une dérivation de typage terminant par le jugement $x_1 : A_1, \dots, x_n : A_n \vdash t : A$ est interprétée par un morphisme $\llbracket t \rrbracket$ de $\llbracket A_1 \rrbracket \times \dots \times \llbracket A_n \rrbracket$ dans $\llbracket A \rrbracket$:

$$\begin{aligned}
(var) \quad & \llbracket \Gamma \rrbracket \times \llbracket A \rrbracket \xrightarrow{\llbracket x \rrbracket = \pi_{\llbracket A \rrbracket}} \llbracket A \rrbracket \\
(lam) \quad & \llbracket \Gamma \rrbracket \xrightarrow{curry(\llbracket t \rrbracket)} \llbracket A \rrbracket \rightarrow \llbracket B \rrbracket \\
(app) \quad & \llbracket \Gamma \rrbracket \xrightarrow{\langle \llbracket t \rrbracket, \llbracket u \rrbracket \rangle} (\llbracket A \rrbracket \rightarrow \llbracket B \rrbracket) \times \llbracket A \rrbracket \xrightarrow{ev_{\llbracket A \rrbracket, \llbracket B \rrbracket}} \llbracket B \rrbracket
\end{aligned}$$

Lemme 7 (Substitution)

$$\llbracket \Gamma \rrbracket \xrightarrow{\llbracket t[u/x] \rrbracket} \llbracket B \rrbracket = \llbracket \Gamma \rrbracket \xrightarrow{\langle id_{\llbracket \Gamma \rrbracket}, \llbracket u \rrbracket \rangle} \llbracket \Gamma \rrbracket \times \llbracket A \rrbracket \xrightarrow{\llbracket t \rrbracket} \llbracket B \rrbracket$$

DÉMONSTRATION : Par récurrence sur la dérivation de $\Gamma, x : A \vdash t : B$:

- (var) Si $t = x$, $\llbracket t \rrbracket = \pi_{\llbracket A \rrbracket}$ donc $\langle id_{\llbracket \Gamma \rrbracket}, \llbracket u \rrbracket \rangle ; \llbracket t \rrbracket = \llbracket u \rrbracket$.
 (var) Si $t = y \neq x$, on a $\Gamma, x : A, y : B \vdash y : B$ et $\llbracket t \rrbracket = \pi_{\llbracket B \rrbracket}$ donc $\langle id_{\llbracket \Gamma \rrbracket}, \llbracket u \rrbracket \rangle ; \llbracket t \rrbracket = \llbracket t \rrbracket$.
 (lam) Si $t = \lambda y.t'$, on a :

$$\begin{aligned} \langle id_{\llbracket \Gamma \rrbracket}, \llbracket u \rrbracket \rangle ; \text{curry}(\llbracket t' \rrbracket) &= \text{curry}(\langle id_{\llbracket \Gamma \rrbracket}, \llbracket u \rrbracket \rangle \times \llbracket A' \rrbracket ; \llbracket t' \rrbracket) \\ &= \text{curry}(\langle id_{\llbracket \Gamma \rrbracket \times \llbracket A' \rrbracket}, \pi_{\llbracket \Gamma \rrbracket} ; \llbracket u \rrbracket \rangle ; \llbracket t' \rrbracket) \\ &= \text{curry}(\llbracket t'^u/x \rrbracket) \\ &= \llbracket (\lambda x.t')^u/x \rrbracket \end{aligned}$$

- (app) Si $t = (t')t''$, on a :

$$\begin{aligned} \langle id_{\llbracket \Gamma \rrbracket}, \llbracket u \rrbracket \rangle ; \langle \llbracket t' \rrbracket, \llbracket t'' \rrbracket \rangle ; \text{ev}_{\llbracket A' \rrbracket, \llbracket B' \rrbracket} &= \langle \langle id_{\llbracket \Gamma \rrbracket}, \llbracket u \rrbracket \rangle ; \llbracket t' \rrbracket, \langle id_{\llbracket \Gamma \rrbracket}, \llbracket u \rrbracket \rangle ; \llbracket t'' \rrbracket \rangle ; \text{ev}_{\llbracket A' \rrbracket, \llbracket B' \rrbracket} \\ &= \langle \llbracket t'^u/x \rrbracket, \llbracket t''^u/x \rrbracket \rangle ; \text{ev}_{\llbracket A' \rrbracket, \llbracket B' \rrbracket} \\ &= \llbracket ((t')t'')^u/x \rrbracket \end{aligned}$$

□

Théorème 4 (Correction)

Relativement à l'interprétation $\llbracket \cdot \rrbracket$, toute catégorie cartésienne fermée est un modèle dénotationnel du λ -calcul.

DÉMONSTRATION : On montre que $\llbracket (\lambda x.t)u \rrbracket = \llbracket t^u/x \rrbracket$:

$$\begin{array}{ccc} & (\llbracket A \rrbracket \rightarrow \llbracket B \rrbracket) \times \llbracket A \rrbracket & \\ \langle \text{curry}(\llbracket t \rrbracket), \llbracket u \rrbracket \rangle \nearrow & \uparrow & \searrow \text{ev}_{\llbracket A \rrbracket, \llbracket B \rrbracket} \\ \llbracket \Gamma \rrbracket & \text{curry}(\llbracket t \rrbracket) \times \llbracket A \rrbracket & \llbracket B \rrbracket \\ \langle id_{\llbracket \Gamma \rrbracket}, \llbracket u \rrbracket \rangle \searrow & \uparrow \llbracket t \rrbracket & \\ & \llbracket \Gamma \rrbracket \times \llbracket A \rrbracket & \end{array}$$

où le premier triangle commute par bifonctorialité de \times et le second car curry est une adjonction. On peut alors conclure par le [lemme 7](#).

On montre que $\llbracket \lambda x.(t)x \rrbracket = \llbracket t \rrbracket$ si $x \notin t$. On a une dérivation d_1 de $\Gamma, x : A \vdash t : A \rightarrow B$ à partir de laquelle on peut construire une dérivation d_2 de $\Gamma \vdash t : A \rightarrow B$ et on vérifie facilement que $\llbracket d_1 \rrbracket = \pi_{\llbracket \Gamma \rrbracket} ; \llbracket d_2 \rrbracket \in \mathbb{C}(\llbracket \Gamma \rrbracket \times \llbracket A \rrbracket, \llbracket A \rrbracket \rightarrow \llbracket B \rrbracket)$. On a alors :

$$\begin{aligned} \llbracket \lambda x.(t)x \rrbracket &= \text{curry}(\langle \llbracket d_1 \rrbracket, \pi_{\llbracket A \rrbracket} \rangle ; \text{ev}_{\llbracket A \rrbracket, \llbracket B \rrbracket}) \\ &= \text{curry}(\langle \pi_{\llbracket \Gamma \rrbracket} ; \llbracket d_2 \rrbracket, \pi_{\llbracket A \rrbracket} \rangle ; \text{ev}_{\llbracket A \rrbracket, \llbracket B \rrbracket}) \\ &= \text{curry}(\llbracket d_2 \rrbracket \times \llbracket A \rrbracket ; \text{ev}_{\llbracket A \rrbracket, \llbracket B \rrbracket}) \\ &= \llbracket d_2 \rrbracket \end{aligned}$$

□

Le modèle ensembliste

On considère l'exemple concret de la catégorie $\mathbb{E}ns$ dont les objets sont les ensembles et dont les morphismes sont les fonctions.

On a les propriétés suivantes :

- La catégorie $(\mathbb{E}ns, \times, \{\star\})$ (où \times est le produit cartésien usuel) est une catégorie cartésienne.

- La fonction qui à une fonction $f : A \times B \rightarrow C$ associe la fonction $f' : A \rightarrow C^B$ telle que $f'(x)(y) = f(x, y)$ est une adjonction entre les foncteurs $_ \times B$ et $(_)^B$

donc $(\mathbb{E}ns, \times, \{\star\})$ est une catégorie cartésienne fermée.

Il est donc possible d'interpréter le λ -calcul simplement typé dans la catégorie $\mathbb{E}ns$. L'intuition qu'un λ -terme est une fonction est alors concrètement réalisée.

Remarque : Réciproquement, toute fonction n'est pas l'interprétation d'un λ -terme. En effet, si on considère le cas particulier où on a un unique type de base o que l'on interprète par un ensemble $\llbracket o \rrbracket$ à deux points, il y a quatre éléments dans $\llbracket o \rrbracket^{\llbracket o \rrbracket}$ alors qu'il n'y a qu'un seul λ -terme clos de type $o \rightarrow o$ qui est $\lambda x.x$ (interprété par la fonction identité).

On dit que le modèle ensembliste n'est pas complet.

4.3 Catégories monoïdales

Définition 15 (Catégorie binoïdale)

Une *catégorie binoïdale* est une paire (\mathbb{C}, \odot) où \odot est un foncteur binoïdal de \mathbb{C} et \mathbb{C} dans \mathbb{C} .

Dans une telle catégorie, un morphisme $f \in \mathbb{C}(A, B)$ est *central* (noté $f \in \mathbb{C}^\bullet(A, B)$) si, pour tout $f' \in \mathbb{C}(A', B')$, les diagrammes suivants commutent :

$$\begin{array}{ccc} A \odot A' & \xrightarrow{A \odot f'} & A \odot B' \\ f \odot A' \downarrow & & \downarrow f \odot B' \\ B \odot A' & \xrightarrow{B \odot f'} & B \odot B' \end{array} \qquad \begin{array}{ccc} A' \odot A & \xrightarrow{A' \odot f} & A' \odot B \\ f' \odot A \downarrow & & \downarrow f' \odot B \\ B' \odot A & \xrightarrow{B' \odot f} & B' \odot B \end{array}$$

on peut alors noter $f \odot f' = A \odot f'$; $f \odot B' = f \odot A'$; $B \odot f' \in \mathbb{C}(A \odot A', B \odot B')$ et $f' \odot f = A' \odot f$; $f' \odot B = f' \odot A$; $B' \odot f \in \mathbb{C}(A' \odot A, B' \odot B)$.

Définition 16 (Catégorie pré-monoïdale)

Une *catégorie pré-monoïdale* est donné par $(\mathbb{C}, \odot, \mathbf{I}, (assoc_{A,B,C}^\odot)_{(A,B,C) \in \mathbb{C}^3}, (unit_A^l \odot)_{A \in \mathbb{C}}, (unit_A^r \odot)_{A \in \mathbb{C}})$ où (\mathbb{C}, \odot) est une catégorie binoïdale, \mathbf{I} est un objet de \mathbb{C} et $(assoc_{A,B,C}^\odot)_{(A,B,C) \in \mathbb{C}^3}, (unit_A^l \odot)_{A \in \mathbb{C}}$ et $(unit_A^r \odot)_{A \in \mathbb{C}}$ sont des isomorphismes naturels centraux avec :

- $assoc_{A,B,C}^\odot \in \mathbb{C}^\bullet((A \odot B) \odot C, A \odot (B \odot C))$
- $unit_A^l \odot \in \mathbb{C}^\bullet(A, A \odot \mathbf{I})$
- $unit_A^r \odot \in \mathbb{C}^\bullet(A, \mathbf{I} \odot A)$

tels que $unit_I^r \circlearrowleft = unit_I^l \circlearrowleft$ et les diagrammes suivants commutent :

$$\begin{array}{ccc}
 & (A \circlearrowleft B) \circlearrowleft (C \circlearrowleft D) & \\
 \text{assoc}_{A \circlearrowleft B, C, D}^{\circlearrowleft} \nearrow & & \searrow \text{assoc}_{A, B, C \circlearrowleft D}^{\circlearrowleft} \\
 ((A \circlearrowleft B) \circlearrowleft C) \circlearrowleft D & & A \circlearrowleft (B \circlearrowleft (C \circlearrowleft D)) \\
 \text{assoc}_{A, B, C \circlearrowleft D}^{\circlearrowleft} \searrow & & \nearrow A \circlearrowleft \text{assoc}_{B, C, D}^{\circlearrowleft} \\
 (A \circlearrowleft (B \circlearrowleft C)) \circlearrowleft D & \xrightarrow{\text{assoc}_{A, B \circlearrowleft C, D}^{\circlearrowleft}} & A \circlearrowleft ((B \circlearrowleft C) \circlearrowleft D)
 \end{array}$$

$$\begin{array}{ccc}
 & A \circlearrowleft B & \\
 \text{unit}_A^l \circlearrowleft B \swarrow & & \searrow A \circlearrowleft \text{unit}_B^r \circlearrowleft \\
 (A \circlearrowleft I) \circlearrowleft B & \xrightarrow{\text{assoc}_{A, I, B}^{\circlearrowleft}} & A \circlearrowleft (I \circlearrowleft B)
 \end{array}$$

Remarque : La propriété $unit_I^r \circlearrowleft = unit_I^l \circlearrowleft$ peut en fait se déduire des autres axiomes.

Définition 17 (Catégorie pré-monoïdale symétrique)

Une catégorie pré-monoïdale est *symétrique* si elle est munie d'un isomorphisme naturel central $(\gamma_{A,B}^{\circlearrowleft})_{(A,B) \in \mathbb{C}^2}$ avec $\gamma_{A,B}^{\circlearrowleft} \in \mathbb{C}^\bullet(A \circlearrowleft B, B \circlearrowleft A)$ tel que $\gamma_{A,B}^{\circlearrowleft}; \gamma_{B,A}^{\circlearrowleft} = id_{A \circlearrowleft B}$ et tel que les diagrammes suivants commutent :

$$\begin{array}{ccccc}
 (A \circlearrowleft B) \circlearrowleft C & \xrightarrow{\text{assoc}_{A, B, C}^{\circlearrowleft}} & A \circlearrowleft (B \circlearrowleft C) & \xrightarrow{\gamma_{A, B \circlearrowleft C}^{\circlearrowleft}} & (B \circlearrowleft C) \circlearrowleft A \\
 \gamma_{A, B \circlearrowleft C}^{\circlearrowleft} \downarrow & & & & \downarrow \text{assoc}_{B, C, A}^{\circlearrowleft} \\
 (B \circlearrowleft A) \circlearrowleft C & \xrightarrow{\text{assoc}_{B, A, C}^{\circlearrowleft}} & B \circlearrowleft (A \circlearrowleft C) & \xrightarrow{B \circlearrowleft \gamma_{A, C}^{\circlearrowleft}} & B \circlearrowleft (C \circlearrowleft A)
 \end{array}$$

$$\begin{array}{ccc}
 & A & \\
 \text{unit}_A^l \circlearrowleft \swarrow & & \searrow \text{unit}_A^r \circlearrowleft \\
 A \circlearrowleft I & \xrightarrow{\gamma_{A, I}^{\circlearrowleft}} & I \circlearrowleft A
 \end{array}$$

Remarque : Cette dernière propriété peut en fait se déduire des autres axiomes.

Définition 18 (Monoïde)

Soit $(\mathbb{C}, \circlearrowleft, I, (\text{assoc}_{A, B, C}^{\circlearrowleft})_{(A, B, C) \in \mathbb{C}^3}, (\text{unit}_A^l \circlearrowleft)_{A \in \mathbb{C}}, (\text{unit}_A^r \circlearrowleft)_{A \in \mathbb{C}})$ une catégorie pré-monoïdale, un \circlearrowleft -monoïde est un triplet $(A, c_A^{\circlearrowleft}, w_A^{\circlearrowleft})$ où A est un objet de \mathbb{C} , $c_A^{\circlearrowleft} \in \mathbb{C}^\bullet(A \circlearrowleft A, A)$ et $w_A^{\circlearrowleft} \in \mathbb{C}^\bullet(I, A)$

tel que les diagrammes suivants commutent :

$$\begin{array}{ccc}
 (A \odot A) \odot A & \xrightarrow{c_A^\odot \odot A} & A \odot A \\
 \downarrow \text{assoc}_{A,A,A}^\odot & & \searrow c_A^\odot \\
 A \odot (A \odot A) & \xrightarrow{A \odot c_A^\odot} & A \odot A \\
 & & \nearrow c_A^\odot \\
 & & A
 \end{array}$$

$$\begin{array}{ccccc}
 A \odot I & \xrightarrow{A \odot w_A^\odot} & A \odot A & \xleftarrow{w_A^\odot \odot A} & I \odot A \\
 & \searrow \text{unit}_A^{l \odot} & \downarrow c_A^\odot & \nearrow \text{unit}_A^{r \odot} & \\
 & & A & &
 \end{array}$$

Si la catégorie est de plus symétrique, un \odot -monoïde symétrique est un \odot -monoïde tel que le diagramme suivant commute :

$$\begin{array}{ccc}
 A \odot A & \xrightarrow{\gamma_{A,A}^\odot} & A \odot A \\
 \searrow c_A^\odot & & \swarrow c_A^\odot \\
 & A &
 \end{array}$$

Un \odot -comonoïde (resp. \odot -comonoïde symétrique) dans \mathbb{C} est un \odot -monoïde (resp. \odot -monoïde symétrique) dans \mathbb{C}^{op} .

Définition 19 (Morphisme de monoïde)

Soient $(\mathbb{C}, \odot, I, (assoc_{A,B,C}^\odot)_{(A,B,C) \in \mathbb{C}^3}, (unit_A^{l \odot})_{A \in \mathbb{C}}, (unit_A^{r \odot})_{A \in \mathbb{C}})$ une catégorie pré-monoïdale et $(A, c_A^\odot, w_A^\odot)$ et $(B, c_B^\odot, w_B^\odot)$ deux \odot -monoïdes de \mathbb{C} , un morphisme central $f \in \mathbb{C}^\bullet(A, B)$ est un *morphisme de \odot -monoïde* si les diagrammes suivants commutent :

$$\begin{array}{ccc}
 A \odot A & \xrightarrow{f \odot f} & B \odot B \\
 c_A^\odot \downarrow & & \downarrow c_B^\odot \\
 A & \xrightarrow{f} & B
 \end{array}
 \qquad
 \begin{array}{ccc}
 & I & \\
 w_A^\odot \swarrow & & \searrow w_B^\odot \\
 A & \xrightarrow{f} & B
 \end{array}$$

Remarque : Si \mathbb{C} a une structure de catégorie pré-monoïdale pour \odot , en prenant comme objets les \odot -monoïdes de \mathbb{C} et comme morphismes les morphismes de \mathbb{C} qui sont des morphismes de monoïde, on obtient la *catégorie des \odot -monoïdes* de \mathbb{C} notée $\odot\text{-Mon}(\mathbb{C})$ (de la même manière on peut construire la catégorie des \odot -comonoïdes de \mathbb{C} notée $\odot\text{-coMon}(\mathbb{C})$).

Définition 20 (Catégorie de monoïdes)

Une catégorie pré-monoïdale symétrique $(\mathbb{C}, \odot, I, (assoc_{A,B,C}^\odot)_{(A,B,C) \in \mathbb{C}^3}, (unit_A^{l \odot})_{A \in \mathbb{C}}, (unit_A^{r \odot})_{A \in \mathbb{C}}, (\gamma_{A,B}^\odot)_{(A,B) \in \mathbb{C}^2})$ est une *catégorie de monoïdes* si chaque objet A est donné avec une structure de monoïde

symétrique $(A, c_A^\odot, w_A^\odot)$ telle que :

$$\begin{array}{ccc}
 A \odot B \odot A \odot B & \xrightarrow{A \odot \gamma_{A,B}^\odot} & A \odot A \odot B \odot B \\
 \searrow c_{A \odot B}^\odot & & \swarrow c_A^\odot \odot c_B^\odot \\
 & A \odot B & \\
 \\
 \text{I} & \xrightarrow{\text{unit}_\text{I}^\odot} & \text{I} \odot \text{I} \\
 \searrow w_{A \odot B}^\odot & & \swarrow w_A^\odot \odot w_B^\odot \\
 & A \odot B & \\
 \\
 & & \begin{array}{c} \text{I} \\ \left. \begin{array}{c} \downarrow \\ \downarrow \end{array} \right\} w_\text{I}^\odot \\ \text{I} \end{array} \quad \begin{array}{c} \text{I} \\ \left. \begin{array}{c} \downarrow \\ \downarrow \end{array} \right\} id_\text{I} \\ \text{I} \end{array}
 \end{array}$$

Définition 21 (Catégorie monoïdale)

Une *catégorie monoïdale* $(\mathbb{C}, \otimes, 1, (assoc_{A,B,C}^\otimes)_{(A,B,C) \in \mathbb{C}^3}, (unit_A^{l \otimes})_{A \in \mathbb{C}}, (unit_A^{r \otimes})_{A \in \mathbb{C}})$ est une catégorie pré-monoïdale dans laquelle \otimes est un bifoncteur (*i.e.* tout morphisme est central).

Une *catégorie monoïdale symétrique* est une catégorie pré-monoïdale symétrique qui est monoïdale.

Exemple 9

Toute catégorie cartésienne est une catégorie monoïdale dans laquelle chaque objet a une structure de \times -comonoïde symétrique (c'est même une "catégorie de comonoïdes").

4.4 Catégories de contrôle

Définition

Une *catégorie de contrôle* est donnée par $(\mathbb{C}, \times, \top, \mathfrak{A}, \perp, (assoc_{A,B,C}^\mathfrak{A})_{(A,B,C) \in \mathbb{C}^3}, (unit_A^{l \mathfrak{A}})_{A \in \mathbb{C}}, (unit_A^{r \mathfrak{A}})_{A \in \mathbb{C}}, (\gamma_{A,B}^\mathfrak{A})_{(A,B) \in \mathbb{C}^2}, (c_A^\mathfrak{A})_{A \in \mathbb{C}}, (w_A^\mathfrak{A})_{A \in \mathbb{C}})$, où :

- $(\mathbb{C}, \times, \top)$ est une catégorie cartésienne fermée (on note $_ \rightarrow _$ l'exponentiation cartésienne).
- $(\mathbb{C}, \mathfrak{A}, \perp, (assoc_{A,B,C}^\mathfrak{A})_{(A,B,C) \in \mathbb{C}^3}, (unit_A^{l \mathfrak{A}})_{A \in \mathbb{C}}, (unit_A^{r \mathfrak{A}})_{A \in \mathbb{C}}, (\gamma_{A,B}^\mathfrak{A})_{(A,B) \in \mathbb{C}^2}, (c_A^\mathfrak{A})_{A \in \mathbb{C}}, (w_A^\mathfrak{A})_{A \in \mathbb{C}})$ est une catégorie de monoïdes.
- On a distributivité du \mathfrak{A} sur \times , *i.e.* pour tout objet C , le foncteur $C \mathfrak{A} _$ préserve les produits finis $(C \mathfrak{A} (A \times B) \simeq (C \mathfrak{A} A) \times (C \mathfrak{A} B)$ et $C \mathfrak{A} \top \simeq \top$) et, de plus les projections π_A sont toutes des morphismes de monoïde.

On peut alors définir l'isomorphisme naturel central :

$$distr_{A,B,C} = A \mathfrak{A} (B \times C) \xrightarrow{\langle A \mathfrak{A} \pi_B, A \mathfrak{A} \pi_C \rangle} (A \mathfrak{A} B) \times (A \mathfrak{A} C)$$

- On définit la *force exponentielle* $str_{A,B,C} \in \mathbb{C}((C \rightarrow A) \mathfrak{A} B, C \rightarrow (A \mathfrak{A} B))$ par curryfication de :

$$((C \rightarrow A) \mathfrak{A} B) \times C \xrightarrow{((C \rightarrow A) \mathfrak{A} B) \times (C \mathfrak{A} w_B^\mathfrak{A})} ((C \rightarrow A) \mathfrak{A} B) \times (C \mathfrak{A} B) \xrightarrow{distr_{B,C \rightarrow A,C}^{-1}} ((C \rightarrow A) \times C) \mathfrak{A} B \xrightarrow{ev_{C,A \mathfrak{A} B}}$$

où il manque certains morphismes $unit__^\mathfrak{A}$ et $\gamma__^\mathfrak{A}$.

On demande que $(str_{A,B,C})_{(A,B,C) \in \mathbb{C}^3}$ soit un *isomorphisme naturel*.

On peut définir de même : $str'_{A,B,C} \in \mathbb{C}(A \mathfrak{A} (C \rightarrow B), C \rightarrow (A \mathfrak{A} B))$. On demande que

le diagramme suivant commute :

$$\begin{array}{ccc}
(C \rightarrow A) \wp (D \rightarrow B) & \xrightarrow{\text{str}'_{C \rightarrow A, B, D}} & D \rightarrow ((C \rightarrow A) \wp B) \\
\downarrow \text{str}_{A, D \rightarrow B, C} & & \downarrow D \rightarrow \text{str}_{A, B, C} \\
C \rightarrow (A \wp (D \rightarrow B)) & \xrightarrow{C \rightarrow \text{str}'_{A, B, D}} & C \rightarrow (D \rightarrow (A \wp B)) \\
& & \nearrow \text{ccc} \\
& & D \rightarrow (C \rightarrow (A \wp B))
\end{array}$$

où *ccc* signifie que l'on applique le morphisme de catégorie cartésienne fermée canonique correspondant.

Enfin on demande que la structure de monoïde de $A \rightarrow B$ soit reliée à celle de B par la commutation des deux diagrammes suivants :

$$\begin{array}{ccc}
(A \rightarrow B) \wp (A \rightarrow B) & \xrightarrow{\text{str}'_{A \rightarrow B, B, A}} & A \rightarrow ((A \rightarrow B) \wp B) \xrightarrow{A \rightarrow \text{str}_{B, B, A}} & A \rightarrow A \rightarrow (B \wp B) \\
& \searrow c_{A \rightarrow B}^{\wp} & & \downarrow \text{ccc} \\
& & A \rightarrow B & \leftarrow \Delta_{A \rightarrow c_B^{\wp}} \\
& & & (A \times A) \rightarrow (B \wp B)
\end{array}$$

$$\begin{array}{ccc}
\perp & \xrightarrow{\text{ccc}} & \top \rightarrow \perp \\
\swarrow w_{A \rightarrow B}^{\wp} & & \swarrow \text{term}_{A \rightarrow w_B^{\wp}} \\
& & A \rightarrow B
\end{array}$$

Interprétation du $\lambda\mu$ -calcul

Soit \mathbb{C} une catégorie de contrôle, on va définir une interprétation des $\lambda\mu$ -termes simplement typés par des morphismes de \mathbb{C} qui traduit les réductions β , η , μ , ρ et θ par l'égalité.

On suppose fixée une interprétation de chaque variable de type X par un objet $\llbracket X \rrbracket$ de \mathbb{C} . Un type est interprété par un objet de \mathbb{C} par $\llbracket A \rightarrow B \rrbracket = \llbracket A \rrbracket \rightarrow \llbracket B \rrbracket$.

Une dérivation de typage terminant par le jugement $x_1 : A_1, \dots, x_n : A_n \vdash t : A \mid \alpha_1 : B_1, \dots, \alpha_m : B_m$ (resp. $x_1 : A_1, \dots, x_n : A_n \vdash n \mid \alpha_1 : B_1, \dots, \alpha_m : B_m$) est interprétée par un morphisme $\llbracket t \rrbracket$ (resp. $\llbracket n \rrbracket$) de $\llbracket A_1 \rrbracket \times \dots \times \llbracket A_n \rrbracket$ dans $\llbracket A \rrbracket \wp \llbracket B_1 \rrbracket \wp \dots \wp \llbracket B_m \rrbracket$ (resp. $\llbracket B_1 \rrbracket \wp \dots \wp \llbracket B_m \rrbracket$) :

$$\begin{aligned}
(\text{var}) \quad & \llbracket \Gamma \rrbracket \times \llbracket A \rrbracket \xrightarrow{\pi_{\llbracket A \rrbracket}} \llbracket A \rrbracket \xrightarrow{\text{unit}_A^l} \llbracket A \rrbracket \wp \perp \xrightarrow{\llbracket A \rrbracket \wp w_{\llbracket \Delta \rrbracket}} \llbracket A \rrbracket \wp \llbracket \Delta \rrbracket \\
(\text{lam}) \quad & \llbracket \Gamma \rrbracket \xrightarrow{\text{curry}(\llbracket t \rrbracket)} \llbracket A \rrbracket \rightarrow (\llbracket B \rrbracket \wp \llbracket \Delta \rrbracket) \xrightarrow{\text{str}_{\llbracket B \rrbracket, \llbracket \Delta \rrbracket, \llbracket A \rrbracket}^{-1}} (\llbracket A \rrbracket \rightarrow \llbracket B \rrbracket) \wp \llbracket \Delta \rrbracket \\
(\text{app}) \quad & \llbracket \Gamma \rrbracket \xrightarrow{\langle \llbracket t \rrbracket, \llbracket u \rrbracket \rangle} ((\llbracket A \rrbracket \rightarrow \llbracket B \rrbracket) \wp \llbracket \Delta \rrbracket) \times (\llbracket A \rrbracket \wp \llbracket \Delta \rrbracket) \xrightarrow{\text{distr}_{\llbracket \Delta \rrbracket, \llbracket A \rrbracket \rightarrow \llbracket B \rrbracket, \llbracket A \rrbracket}^{-1}} ((\llbracket A \rrbracket \rightarrow \llbracket B \rrbracket) \times \\
& \llbracket A \rrbracket) \wp \llbracket \Delta \rrbracket \xrightarrow{\text{ev}_{\llbracket A \rrbracket, \llbracket B \rrbracket} \wp \llbracket \Delta \rrbracket}} \llbracket B \rrbracket \wp \llbracket \Delta \rrbracket \\
(\text{nom}) \quad & \llbracket \Gamma \rrbracket \xrightarrow{\llbracket t \rrbracket} \llbracket A \rrbracket \wp \llbracket A \rrbracket \wp \llbracket \Delta \rrbracket \xrightarrow{c_A \wp \llbracket \Delta \rrbracket} \llbracket A \rrbracket \wp \llbracket \Delta \rrbracket \\
(\text{mu}) \quad & \llbracket \Gamma \rrbracket \xrightarrow{\llbracket n \rrbracket} \llbracket A \rrbracket \wp \llbracket \Delta \rrbracket
\end{aligned}$$

Théorème 5 (Correction)

Relativement à l'interprétation $\llbracket \cdot \rrbracket$, toute catégorie de contrôle est un modèle dénotationnel du $\lambda\mu$ -calcul.

Troisième partie
Logique linéaire

Chapitre 5

Calcul des séquents

À travers l'étude des interprétations calculatoires de la logique classique et de la logique intuitionniste, on a vu que les règles structurelles jouent un rôle clef. La logique linéaire est basée sur un contrôle strict de ces règles.

5.1 Règles

Connecteurs multiplicatifs et additifs

On considère le calcul des séquents de la logique classique *sans les règles structurelles*. Le choix d'une formulation additive ou multiplicative pour les règles prend alors toute son importance puisque les différentes formulations ne sont équivalentes que grâce aux règles structurelles.

Si on s'intéresse aux connecteurs \wedge , \vee et \neg que l'on renomme \otimes ("tenseur") pour le \wedge multiplicatif, $\&$ ("avec") pour le \wedge additif, \wp ("par") pour le \vee multiplicatif, \oplus ("plus") pour le \vee additif et $(.)^\perp$ ("orthogonal") pour \neg , on obtient les règles suivantes :

$$\begin{array}{c} \frac{}{A \vdash A} \text{ax} \qquad \frac{\Gamma \vdash A, \Delta \quad \Gamma', A \vdash \Delta'}{\Gamma, \Gamma' \vdash \Delta, \Delta'} \text{cut} \\ \\ \frac{\Gamma \vdash A, \Delta \quad \Gamma' \vdash B, \Delta'}{\Gamma, \Gamma' \vdash A \otimes B, \Delta, \Delta'} \otimes R \qquad \frac{\Gamma, A, B \vdash \Delta}{\Gamma, A \otimes B \vdash \Delta} \otimes L \\ \\ \frac{\Gamma \vdash A, B, \Delta}{\Gamma \vdash A \wp B, \Delta} \wp R \qquad \frac{\Gamma, A \vdash \Delta \quad \Gamma', B \vdash \Delta'}{\Gamma, \Gamma', A \wp B \vdash \Delta, \Delta'} \wp L \\ \\ \frac{\Gamma \vdash A, \Delta \quad \Gamma \vdash B, \Delta}{\Gamma \vdash A \& B, \Delta} \& R \qquad \frac{\Gamma, A \vdash \Delta}{\Gamma, A \& B \vdash \Delta} \& L_1 \qquad \frac{\Gamma, B \vdash \Delta}{\Gamma, A \& B \vdash \Delta} \& L_2 \\ \\ \frac{\Gamma \vdash A, \Delta}{\Gamma \vdash A \oplus B, \Delta} \oplus R_1 \qquad \frac{\Gamma \vdash B, \Delta}{\Gamma \vdash A \oplus B, \Delta} \oplus R_2 \qquad \frac{\Gamma, A \vdash \Delta \quad \Gamma, B \vdash \Delta}{\Gamma, A \oplus B \vdash \Delta} \oplus L \\ \\ \frac{\Gamma, A \vdash \Delta}{\Gamma \vdash A^\perp, \Delta} (.)^\perp R \qquad \frac{\Gamma \vdash A, \Delta}{\Gamma, A^\perp \vdash \Delta} (.)^\perp L \end{array}$$

On constate, comme dans le cas de LK, que l'on a une symétrie parfaite entre gauche et droite et que la négation linéaire $(.)^\perp$ échange les deux côtés. On peut donc utiliser une formulation

monolatère du calcul des séquents en définissant la négation par des lois de De Morgan :

$$\begin{aligned}
(X^\perp)^\perp &= X \\
(A \otimes B)^\perp &= A^\perp \wp B^\perp \\
(A \wp B)^\perp &= A^\perp \otimes B^\perp \\
(A \& B)^\perp &= A^\perp \oplus B^\perp \\
(A \oplus B)^\perp &= A^\perp \& B^\perp
\end{aligned}$$

ce qui donne $A^{\perp\perp} = A$.

On obtient les formules suivantes :

$$\begin{array}{l}
A ::= X \quad | \quad A \wp A \quad | \quad A \& A \\
\quad | \quad X^\perp \quad | \quad A \otimes A \quad | \quad A \oplus A
\end{array}$$

et on utilise des séquents de la forme $\vdash \Gamma$.

$$\begin{array}{c}
\frac{}{\vdash A^\perp, A} \text{ ax} \qquad \frac{\vdash \Gamma, A \quad \vdash \Delta, A^\perp}{\vdash \Gamma, \Delta} \text{ cut} \\
\\
\frac{\vdash \Gamma, A \quad \vdash \Delta, B}{\vdash \Gamma, \Delta, A \otimes B} \otimes \qquad \frac{\vdash \Gamma, A, B}{\vdash \Gamma, A \wp B} \wp \\
\\
\frac{\vdash \Gamma, A \quad \vdash \Gamma, B}{\vdash \Gamma, A \& B} \& \qquad \frac{\vdash \Gamma, A}{\vdash \Gamma, A \oplus B} \oplus_1 \qquad \frac{\vdash \Gamma, B}{\vdash \Gamma, A \oplus B} \oplus_2
\end{array}$$

Ce système est le fragment multiplicatif-additif de la logique linéaire que l'on note MALL. Si on ne prend que les connecteurs multiplicatifs, on obtient MLL et si on ne prend que les connecteurs additifs, on obtient ALL (peu usité).

Exercice 26

Montrer que dans ALL, un séquent prouvable contient exactement deux formules.

On peut *tenter* de donner quelques intuitions sur la signification des connecteurs :

- si on a une preuve de $A \otimes B$, elle nous fournit simultanément une preuve de A et une preuve de B
- si on a une preuve de $A \& B$, on peut l'utiliser, à notre convenance, soit comme une preuve de A soit comme une preuve de B (mais pas des deux simultanément)
- si on a une preuve de $A \oplus B$, elle nous fournit soit une preuve de A soit une preuve de B mais le choix ne nous appartient pas.

Exercice 27 (Isomorphismes)

Montrer que tous les connecteurs sont associatifs et commutatifs.

Montrer que l'on a les distributivités suivantes :

$$\begin{aligned}
A \otimes (B \oplus C) &\dashv\vdash (A \otimes B) \oplus (A \otimes C) \\
A \wp (B \& C) &\dashv\vdash (A \wp B) \& (A \wp C)
\end{aligned}$$

Il est souvent pratique de définir le connecteur “flèche linéaire” $A \multimap B$. Comme pour \rightarrow dans LK, on peut l'obtenir par négation et disjonction : $A \multimap B = A^\perp \wp B$ (ainsi $A \multimap B \simeq$

$B^\perp \multimap A^\perp$). On peut alors dériver les règles de calcul des séquents :

$$\frac{\Gamma, A \vdash B, \Delta}{\Gamma \vdash A \multimap B, \Delta} \quad \frac{\Gamma \vdash A, \Delta \quad \Gamma', B \vdash \Delta'}{\Gamma, \Gamma', A \multimap B \vdash \Delta, \Delta'}$$

$$\frac{\vdash \Gamma, A^\perp, B}{\vdash \Gamma, A \multimap B} \quad \frac{\vdash \Gamma, A \quad \vdash \Delta, B^\perp}{\vdash \Gamma, \Delta, (A \multimap B)^\perp}$$

Élimination des coupures

On va se contenter de donner les cas clefs :

$$\frac{\vdash \Gamma, A \quad \frac{\vdash A^\perp, A}{ax}}{\vdash \Gamma, A} cut \rightsquigarrow \vdash \Gamma, A$$

$$\frac{\frac{\vdash \Gamma, A \quad \vdash \Delta, B}{\vdash \Gamma, \Delta, A \otimes B} \otimes \quad \frac{\vdash \Xi, A^\perp, B^\perp}{\vdash \Xi, A^\perp \wp B^\perp} \wp}{\vdash \Gamma, \Delta, \Xi} cut \rightsquigarrow \frac{\vdash \Gamma, A \quad \frac{\vdash \Delta, B \quad \vdash \Xi, A^\perp, B^\perp}{\vdash \Delta, \Xi, A^\perp} cut}{\vdash \Gamma, \Delta, \Xi} cut$$

$$\frac{\frac{\vdash \Gamma, A \quad \vdash \Gamma, B}{\vdash \Gamma, A \& B} \& \quad \frac{\vdash \Delta, A^\perp}{\vdash \Delta, A^\perp \oplus B^\perp} \oplus_1}{\vdash \Gamma, \Delta} cut \rightsquigarrow \frac{\vdash \Gamma, A \quad \vdash \Delta, A^\perp}{\vdash \Gamma, \Delta} cut$$

$$\frac{\frac{\vdash \Gamma, A \quad \vdash \Gamma, B}{\vdash \Gamma, A \& B} \& \quad \frac{\vdash \Delta, B^\perp}{\vdash \Delta, A^\perp \oplus B^\perp} \oplus_2}{\vdash \Gamma, \Delta} cut \rightsquigarrow \frac{\vdash \Gamma, B \quad \vdash \Delta, B^\perp}{\vdash \Gamma, \Delta} cut$$

Exercice 28

Définir les étapes commutatives et montrer le théorème d'élimination des coupures.

Connecteurs exponentiels

Les systèmes que l'on a obtenus sont malheureusement “peu expressifs”. Notamment si on s'intéresse à la logique classique ou à la logique intuitionniste, il est nécessaire de pouvoir parler de règles structurelles. Tout est dans la manière de les réintroduire.

On ajoute deux connecteurs duaux : $!A$ (“bien sûr”) et $?A$ (“pourquoi pas”) avec $(!A)^\perp = ?A^\perp$ et $(?A)^\perp = !A^\perp$.

$$A ::= X \quad | \quad A \wp A \quad | \quad A \& A \quad | \quad ?A \\ | \quad X^\perp \quad | \quad A \otimes A \quad | \quad A \oplus A \quad | \quad !A$$

Au lieu d'appliquer les règles structurelles sur n'importe quelle formule, seules celles dont le connecteur principal est $?$ pourront être affaiblies et contractées (d'une certaine manière les règles structurelles deviennent des règles logiques) :

$$\frac{\vdash \Gamma, A}{\vdash \Gamma, ?A} ?d \quad \frac{\vdash \Gamma, ?A, ?A}{\vdash \Gamma, ?A} ?c \quad \frac{\vdash \Gamma}{\vdash \Gamma, ?A} ?w \quad \frac{\vdash ?\Gamma, A}{\vdash ?\Gamma, !A} !$$

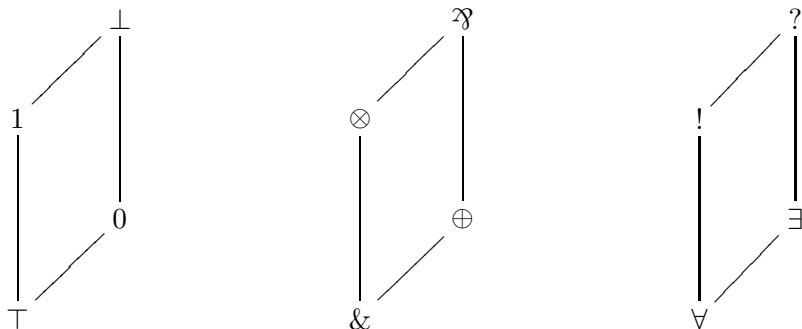
La règle $?d$ (“déréliction”) permet à toute formule de devenir sujette aux règles structurelles. Les règles $?w$ (“affaiblissement”) et $?c$ (“contraction”) sont les règles structurelles habituelles mais ne s'appliquent qu'aux formules dont le connecteur principal est $?$. La règle $!$ (“promotion”) est la plus subtile. Elle permet de rendre une formule (et surtout la preuve correspondante) duplicable (ou effaçable), mais ceci nécessite un contexte adapté. On peut comprendre $!A$ comme “ A autant de fois que l'on veut”. La règle écrite sous la forme :

Exercice 30 (Isomorphismes)

Montrer que les quatre éléments neutres sont neutres pour le connecteur correspondant et que :

$$\begin{aligned} A \otimes 0 &\simeq 0 \\ A \wp \top &\simeq \top \\ !\top &\simeq 1 \\ ?0 &\simeq \perp \end{aligned}$$

On peut résumer les rapports entre les différents connecteurs de la manière suivante :



On passe de devant à derrière en passant d'un caractère conjonctif à un caractère disjonctif (par négation $(.)^\perp$). On passe de haut en bas en passant d'un caractère multiplicatif à un caractère additif. On passe de gauche à droite en passant du cas 0-aire, au cas binaire puis au cas infinitaire.

Expansion des axiomes

Il est possible de dériver le séquent $\vdash A^\perp, A$ à partir d'axiomes portant uniquement sur des variables. Pour cela, il suffit d'utiliser les transformations suivantes :

$$\begin{aligned} \frac{}{\vdash A^\perp \otimes B^\perp, A \wp B} ax &\rightsquigarrow \frac{\frac{\frac{}{\vdash A^\perp, A} ax \quad \frac{}{\vdash B^\perp, B} ax}{\vdash A^\perp \otimes B^\perp, A, B} \otimes}{\vdash A^\perp \otimes B^\perp, A \wp B} \wp \\ \frac{}{\vdash A^\perp \oplus B^\perp, A \& B} ax &\rightsquigarrow \frac{\frac{\frac{}{\vdash A^\perp, A} ax \oplus_1 \quad \frac{}{\vdash B^\perp, B} ax \oplus_2}{\vdash A^\perp \oplus B^\perp, A} \oplus_1}{\vdash A^\perp \oplus B^\perp, A \& B} \& \\ \frac{}{\vdash !A, ?A^\perp} ax &\rightsquigarrow \frac{\frac{\frac{}{\vdash A, A^\perp} ax \quad ?d}{\vdash A, ?A^\perp} ?d}{\vdash !A, ?A^\perp} ! \\ \frac{}{\vdash 1, \perp} ax &\rightsquigarrow \frac{\frac{}{\vdash 1} 1}{\vdash 1, \perp} \perp \\ \frac{}{\vdash 0, \top} ax &\rightsquigarrow \frac{}{\vdash 0, \top} \top \end{aligned}$$

5.2 Réversibilité et focalisation

Définition 22 (Connecteur réversible)

Un connecteur \circ est réversible si lorsque $\vdash \Gamma, A$ est dérivable avec \circ connecteur principal de A , alors $\vdash \Gamma, A$ est dérivable avec comme dernière règle une règle d'introduction de \circ .

Remarque : Cette notion est liée à l'existence de règles d'introduction réversibles mais est cependant différente. Ainsi la règle de 1 est réversible mais 1 ne l'est pas à cause de $\vdash \perp, 1$ par exemple.

Les connecteurs réversibles de LL sont \wp , $\&$, \perp et \top :

$$\begin{aligned}
\vdash \Gamma, A \wp B &\rightsquigarrow \frac{\frac{\frac{\overline{\vdash A^\perp, A}^{ax} \quad \overline{\vdash B^\perp, B}^{ax}}{\vdash A^\perp \otimes B^\perp, A, B} \otimes}{\vdash \Gamma, A, B} cut}{\vdash \Gamma, A \wp B} \wp \\
\vdash \Gamma, A \& B &\rightsquigarrow \frac{\frac{\frac{\overline{\vdash A^\perp, A}^{ax}}{\vdash A^\perp \oplus B^\perp, A} \oplus_1}{\vdash \Gamma, A} cut \quad \frac{\frac{\overline{\vdash B^\perp, B}^{ax}}{\vdash A^\perp \oplus B^\perp, B} \oplus_2}{\vdash \Gamma, B} cut}{\vdash \Gamma, A \& B} \& \\
\vdash \Gamma, \perp &\rightsquigarrow \frac{\frac{\vdash \Gamma, \perp \quad \overline{\vdash 1}^1}{\vdash \Gamma} cut}{\vdash \Gamma, \perp} \perp \\
\vdash \Gamma, \top &\rightsquigarrow \overline{\vdash \Gamma, \top} \top
\end{aligned}$$

Les autres connecteurs sont irréversibles. Pour \otimes , \oplus , 1 , 0 et $?$, il suffit de considérer le cas de l'axiome $\vdash A^\perp, A$ avec pour connecteur principal de A le connecteur en cause. Pour $!$, les choses sont un peu différentes et on obtient l'irréversibilité en considérant le séquent $\vdash ?X \wp ?Y, !X^\perp$ par exemple.

Ceci nous donne une définition “négative” des connecteurs irréversibles. Il existe une propriété “duale” de la réversibilité et qui concerne les connecteurs irréversibles : la *focalisation*.

Les connecteurs réversibles sont appelés *négatifs* : \wp , $\&$, \perp et \top auxquels on ajoute également $?$. Dualement les autres connecteurs sont appelés *positifs*. Une formule est *positive* si son connecteur principal est positif et négative si son connecteur principal est négatif. La *couche positive* d'une formule est définie par : la couche positive d'une formule négative (ou d'un atome) est vide, la couche positive de 1 , 0 et $!A$ est son connecteur principal et la couche positive de $A \otimes B$ et de $A \oplus B$ est obtenue à partir de celle de A et de celle de B en ajoutant \otimes ou \oplus . Attention le connecteur $!$ n'est pas traité de la même manière que \otimes ou \oplus , ainsi la couche positive de $(X \wp Y) \otimes (1 \oplus !(\perp \otimes 0))$ est $_ \otimes (1 \oplus _)$.

Proposition 20 (Focalisation)

Soit $\vdash \Gamma$ un séquent ne contenant que des formules positives (et éventuellement des atomes), si $\vdash \Gamma$ est prouvable alors il existe une formule P dans Γ telle que $\vdash \Gamma$ soit prouvable par une preuve qui termine par les règles d'introduction de la couche positive de P (on dit alors que la preuve est focalisée).

Exemple 10 (Preuve focalisée)

La preuve suivante n'est pas focalisée :

$$\frac{\frac{\frac{\frac{\frac{}{\vdash X, X^\perp} ax}{}{\vdash X \otimes Y, X^\perp, Y^\perp} \otimes}{}{\vdash X \otimes Y, X^\perp \otimes 1, Y^\perp} \otimes_1}{}{\vdash (X \otimes Y) \oplus \perp, X^\perp \otimes 1, Y^\perp} \oplus_1}{\vdash 1} 1}{\vdash 1} 1$$

mais voici une preuve focalisée du même séquent :

$$\frac{\frac{\frac{\frac{\frac{}{\vdash X, X^\perp} ax}{}{\vdash X, X^\perp \otimes 1} \otimes}{}{\vdash X \otimes Y, X^\perp \otimes 1, Y^\perp} \otimes_1}{}{\vdash (X \otimes Y) \oplus \perp, X^\perp \otimes 1, Y^\perp} \oplus_1}{\vdash 1} 1}{\vdash 1} 1$$

5.3 Logique Linéaire Intuitionniste (ILL)

La *logique linéaire intuitionniste* ILL est obtenue à partir de la présentation bilatère de la logique linéaire en imposant que les séquents aient exactement une formule à droite $\Gamma \vdash A$. Ceci entraîne la disparition des connecteurs $(.)^\perp$, \wp , \perp et $?$ (mais on peut par contre conserver \multimap) :

$$A ::= X \mid A \multimap A \mid A \otimes A \mid A \& A \mid A \oplus A \mid !A \mid 1 \mid \top \mid 0$$

Les règles deviennent :

$$\begin{array}{c} \frac{}{A \vdash A} ax \qquad \frac{\Gamma \vdash A \quad \Delta, A \vdash C}{\Gamma, \Delta \vdash C} cut \\ \\ \frac{\Gamma \vdash A \quad \Delta \vdash B}{\Gamma, \Delta \vdash A \otimes B} \otimes R \qquad \frac{\Gamma, A, B \vdash C}{\Gamma, A \otimes B \vdash C} \otimes L \\ \\ \frac{\Gamma, A \vdash B}{\Gamma \vdash A \multimap B} \multimap R \qquad \frac{\Gamma \vdash A \quad \Delta, B \vdash C}{\Gamma, \Delta, A \multimap B \vdash C} \multimap L \\ \\ \frac{\Gamma \vdash A \quad \Gamma \vdash B}{\Gamma \vdash A \& B} \& R \qquad \frac{\Gamma, A \vdash C}{\Gamma, A \& B \vdash C} \& L_1 \qquad \frac{\Gamma, B \vdash C}{\Gamma, A \& B \vdash C} \& L_2 \\ \\ \frac{\Gamma \vdash A}{\Gamma \vdash A \oplus B} \oplus R_1 \qquad \frac{\Gamma \vdash B}{\Gamma \vdash A \oplus B} \oplus R_2 \qquad \frac{\Gamma, A \vdash C \quad \Gamma, B \vdash C}{\Gamma, A \oplus B \vdash C} \oplus L \\ \\ \frac{! \Gamma \vdash A}{! \Gamma \vdash !A} !R \qquad \frac{\Gamma, A \vdash C}{\Gamma, !A \vdash C} !L \qquad \frac{\Gamma, !A, !A \vdash C}{\Gamma, !A \vdash C} ctrL \qquad \frac{\Gamma \vdash C}{\Gamma, !A \vdash C} wkL \\ \\ \frac{}{\vdash 1} 1R \qquad \frac{\Gamma \vdash C}{\Gamma, 1 \vdash C} 1L \qquad \frac{}{\Gamma \vdash \top} \top R \qquad \frac{}{\Gamma, 0 \vdash C} 0L \end{array}$$

On peut vérifier que l'élimination des coupures de LL préserve la contrainte "exactement une formule à droite" et donc s'applique à ILL.

Afin de comparer ILL et LL, on peut définir une notion de *polarisation intuitionniste* sur les formules de LL. On obtient deux classes de formules, les formules *output* et *input* :

$$\begin{array}{l} O ::= X \mid I \wp O \mid O \wp I \mid O \otimes O \mid O \& O \mid O \oplus O \mid !O \mid 1 \mid \top_O \mid 0_O \\ I ::= X^\perp \mid O \otimes I \mid I \otimes O \mid I \wp I \mid I \oplus I \mid I \& I \mid ?I \mid \perp \mid 0_I \mid \top_I \end{array}$$

Lemme 8 (Formule output)

Si $\vdash \Gamma$ est prouvable dans le fragment de LL n'utilisant que des formules polarisées intuitionnistiquement sans utiliser la règle \top alors Γ contient exactement une formule output.

DÉMONSTRATION : Par récurrence sur la longueur de la preuve dans LL. \square

Proposition 21

En l'absence des connecteurs 0 et \top , ILL est le fragment de LL n'utilisant que les formules polarisées intuitionnistiquement.

DÉMONSTRATION : Si $\Gamma \vdash A$ est prouvable dans ILL, il l'est immédiatement dans LL. Si $\vdash \Gamma$ est prouvable dans LL en n'utilisant que des formules polarisées intuitionnistiquement, par le [lemme 8](#), on peut écrire $\vdash \Gamma$ sous la forme $\Delta \vdash A$ où Δ et A ne contiennent que des formules output donc des formules valides dans ILL et les règles de LL appliquées sont alors exactement celles de ILL. \square

On peut étendre ce résultat à \top en imposant que, dans le fragment de LL polarisé intuitionnistiquement, la règle \top introduise des séquents avec exactement une formule output.

De manière plus générale, il est naturel d'étudier le système sans éléments neutres pour obtenir des propriétés (comme ici l'existence et l'unicité d'une formule output) puis d'imposer aux éléments neutres de respecter ces propriétés (ce qui est suffisant pour qu'ils soient des éléments neutres). Les éléments neutres n'ont pas à violer des propriétés intrinsèques du système (ce qui arrive très naturellement avec \top si on ne fait pas attention).

Logique linéaire intuitionniste stricte (sILL)

Si on s'intéresse à la prouvabilité des formules, on peut également obtenir un résultat en omettant les connecteurs \oplus et 0 dans ILL. On appellera *logique linéaire intuitionniste stricte* sILL le système obtenu.

La notion de polarisation intuitionniste stricte est donnée par :

$$\begin{array}{l} o ::= X \quad | \quad i \wp o \quad | \quad o \wp i \quad | \quad o \otimes o \quad | \quad o \& o \quad | \quad !o \quad | \quad 1 \quad | \quad \top \\ i ::= X^\perp \quad | \quad o \otimes i \quad | \quad i \otimes o \quad | \quad i \wp i \quad | \quad i \oplus i \quad | \quad ?i \quad | \quad \perp \quad | \quad 0 \end{array}$$

Lemme 9 (Formules outputs strictes)

Si $\vdash \Gamma$ est prouvable dans le fragment de LL n'utilisant que des formules polarisées intuitionnistiquement strictes alors Γ contient au moins une formule output stricte.

DÉMONSTRATION : Par récurrence sur la longueur de la preuve dans LL. \square

Lemme 10 (Séquents intuitionnistes stricts)

Si π est une preuve dans le fragment de LL n'utilisant que des formules polarisées intuitionnistiquement strictes du séquent $\vdash \Gamma$ qui contient exactement une formule output stricte alors tous les séquents de π contiennent exactement une formule output stricte.

DÉMONSTRATION : Par récurrence sur la longueur de la preuve dans LL. Le cas essentiel est celui d'une preuve terminant par l'application d'une règle de \otimes introduisant $i \otimes o$:

$$\frac{\vdash \Gamma, i \quad \vdash \Delta, o}{\vdash \Gamma, \Delta, i \otimes o} \otimes$$

Par hypothèse Γ, Δ contient exactement une formule output stricte. Si elle est dans Γ , on peut appliquer l'hypothèse de récurrence aux deux prémisses et on a le résultat. Si elle est dans Δ , alors $\vdash \Gamma, i$ ne contient que des formules inputs strictes ce qui est impossible d'après le [lemme 9](#). Le cas de la coupure est traité de la même manière. \square

Proposition 22

Les formules prouvables dans sILL sont exactement les formules outputs strictes prouvables dans LL.

DÉMONSTRATION : Si A est prouvable dans sILL, elle correspond à une formule output stricte qui est prouvable dans LL : il suffit de traduire règle à règle. Pour la réciproque, on considère une preuve π n'utilisant que des formules polarisées intuitionnistiquement strictes (ce qu'on obtient facilement quitte à éliminer les coupures si nécessaire). Par le [lemme 10](#), tous les séquents de π contiennent exactement une formule output stricte. Les règles de LL appliquées sont alors exactement celles de sILL. \square

Chapitre 6

Réseaux de preuve

Les réseaux de preuve fournissent une syntaxe pour la logique linéaire qui s'abstrait de la notion de séquent et de contexte permettant une représentation plus canonique des preuves et une diminution du nombre d'étapes commutatives dans l'élimination des coupures. Cette représentation graphique fournit un objet plus géométrique pour l'étude des preuves.

6.1 MLL

Structures de preuve

Pour éviter les étapes commutatives de l'élimination des coupures, on cherche à "éviter" les contextes, on représente chaque règle par un nœud ne concernant que les formules actives (on remarque que cette approche identifie géométriquement les règles \otimes et \wp puisqu'elles possèdent, toutes les deux, deux prémisses actives et une conclusion principale).

Définition 23 (Graphes)

Un *graphe orienté* G est donné par deux ensembles G_0 (*nœuds*) et G_1 (*arêtes*) et deux fonctions \mathbf{s} (*source*) et \mathbf{b} (*but*) de G_1 dans G_0 .

Un *chemin* dans un graphe orienté est une suite a_1, \dots, a_k (où $k \geq 0$ est la *longueur* du chemin) d'arêtes telle que pour tout $2 \leq i \leq k$, $\mathbf{s}(a_i) = \mathbf{b}(a_{i-1})$. On dit qu'il s'agit d'un chemin de $\mathbf{s}(a_1)$ à $\mathbf{b}(a_k)$ ou de a_1 à a_k .

Un graphe orienté est *acyclique* s'il n'existe aucun chemin de longueur non nulle allant d'un nœud à lui-même.

Si $n \in G_0$, on appelle *prémisses* de n les arêtes dont le but est n et *conclusions* de n les arêtes dont la source est n .

Un *graphe (non orienté)* est donné par deux ensembles G_0 et G_1 et par une fonction \mathbf{e} de G_1 dans les parties de G_0 à un ou deux éléments.

Un *chemin* dans un graphe (non orienté) est une suite a_1, \dots, a_k (où $k \geq 0$ est la *longueur* du chemin) d'arêtes telle qu'il existe une suite de nœuds n_0, \dots, n_k avec, pour tout $1 \leq i \leq k$, $\mathbf{e}(a_i) = \{n_{i-1}, n_i\}$. On dit qu'il s'agit d'un chemin de n_0 à n_k ou de a_1 à a_k .

Un graphe non orienté est *acyclique* s'il n'existe aucun chemin de longueur non nulle allant d'un nœud à lui-même.

Un graphe non orienté est *connexe* si pour tout couple de sommets (n_1, n_2) il y a un chemin de n_1 à n_2 .

Étant donné un graphe orienté, le graphe non orienté associé est obtenu en prenant pour tout a dans G_1 , $\mathbf{e}(a) = \{\mathbf{s}(a), \mathbf{b}(a)\}$.

Définition 24 (Graphe étiqueté)

Un *graphe étiqueté* par un ensemble \mathcal{L} est un graphe G muni d'une fonction de l'ensemble de ses arêtes G_1 dans \mathcal{L} .

Les graphes que l'on va considérer sont des graphes étiquetés par des formules. L'étiquette d'une arête sera souvent appelée son *type*.

Définition 25 (Sortes de nœud)

Une *sorte de nœud* s est donnée par deux entiers $\mathbf{p}(s)$ et $\mathbf{c}(s)$ (le nombre de prémisses et le nombre de conclusions) et des contraintes sur les étiquettes des prémisses et des conclusions de la forme : *si les étiquettes des i^e , j^e et k^e prémisses sont ... et celles des m^e et n^e conclusions sont ... alors celle de la p^e conclusion (ou prémisses) est*

Un *alphabet de nœuds* est un ensemble de sortes de nœuds.

On s'intéresse pour l'instant aux sortes de nœuds suivantes :

- sorte ax : aucune prémisses, deux conclusions, si l'étiquette de la première conclusion est A alors celle de la deuxième est A^\perp
- sorte cut : deux prémisses, aucune conclusion, si l'étiquette de la première prémisses est A alors celle de la deuxième est A^\perp
- sorte \otimes : deux prémisses, une conclusion, si l'étiquette de la première prémisses est A et celle de la deuxième prémisses est B alors celle de la conclusion est $A \otimes B$
- sorte \wp : deux prémisses, une conclusion, si l'étiquette de la première prémisses est A et celle de la deuxième prémisses est B alors celle de la conclusion est $A \wp B$
- sorte \otimes_1 : une prémisses, une conclusion, si l'étiquette de la prémisses est A alors celle de la conclusion est $A \otimes B$ (où B peut être une formule quelconque)
- sorte \otimes_2 : une prémisses, une conclusion, si l'étiquette de la prémisses est B alors celle de la conclusion est $A \otimes B$ (où A peut être une formule quelconque)
- sorte \wp_1 : une prémisses, une conclusion, si l'étiquette de la prémisses est A alors celle de la conclusion est $A \wp B$ (où B peut être une formule quelconque)
- sorte \wp_2 : une prémisses, une conclusion, si l'étiquette de la prémisses est B alors celle de la conclusion est $A \wp B$ (où A peut être une formule quelconque)
- sorte \wp_0 : aucune prémisses, une conclusion, l'étiquette de la conclusion est $A \wp B$ (où A et B peuvent être des formules quelconques)

Définition 26 (Module)

Un *module* \mathcal{M} sur l'alphabet de nœuds \mathcal{A} est un graphe orienté acyclique $(G_0, G_1, \mathbf{s}, \mathbf{b})$ où G_0 se décompose en trois ensembles disjoints $G_0 = P \uplus N \uplus C$ avec la propriété que :

- aucune arête n'a pour but un élément de P ,
- aucune arête n'a pour source un élément de C ,
- chaque élément de P est source d'exactly une arête,
- chaque élément de C est but d'exactly une arête.

Les éléments de N s'appellent les *nœuds* de \mathcal{M} .

Ce graphe est étiqueté par des formules (de LL) et muni de :

- une fonction de N dans \mathcal{A}
- pour chaque nœud n de sorte s , une bijection de $\{1, \dots, \mathbf{p}(s)\}$ dans l'ensemble des prémisses de n et une bijection de $\{1, \dots, \mathbf{c}(s)\}$ dans l'ensemble des conclusions de n

de manière à ce que, pour chaque nœud, les formules associées aux prémisses et aux conclusions vérifient les contraintes données par sa sorte.

Les arêtes dont la source est dans P sont appelées les *prémisses* de \mathcal{M} . Les arêtes dont le but est dans C sont appelées les *conclusions* de \mathcal{M} et un nœud dont toutes les conclusions sont des conclusions de \mathcal{M} est appelé nœud *terminal* de \mathcal{M} .

Définition 27 (Structure de preuve)

Une *structure de preuve* \mathcal{S} sur l'alphabet de nœuds \mathcal{A} est un module sur \mathcal{A} tel que P est vide.

On appelle *structures de preuve multiplicatives* les structures de preuve sur l'alphabet de nœuds $\{ax, cut, \otimes, \wp\}$ (une sorte de nœud par règle considérée).

Remarque : Une structure de preuve multiplicative est automatiquement acyclique (par contraintes de typage).

Étant donnée une structure de preuve \mathcal{S} et un sous-ensemble de ses arêtes, on obtient naturellement un module \mathcal{M} sur le même alphabet de nœuds de la manière suivante :

- les arêtes de \mathcal{M} sont celles sélectionnées,
- un nœud de \mathcal{S} est dans \mathcal{M} si toutes ses prémisses et toutes ses conclusions sont sélectionnées,
- la source (resp. le but) d'une arête est la (resp. le) même dans \mathcal{M} que dans \mathcal{S} si le nœud est dans \mathcal{M} , sinon c'est un nouvel élément de P (resp. C),
- les autres données sont obtenues par restriction de celles de \mathcal{S} .

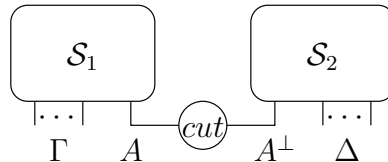
Puisque l'on parle ici de graphes, nous allons adopter une présentation graphique des structures de preuve et des modules qui évite d'énumérer les nombreux éléments qui les définissent. Les nœuds seront représentés par des cercles (contenant la sorte associée) et les arêtes par des traits reliant leur source et leur but. La source d'une arête sera celle de ses extrémités la plus haute et son but sera la plus basse. Les formules associées aux arêtes seront représentées à côté de celles-ci (et parfois omises quand il est possible de les déduire des formules voisines). La numérotation des prémisses et des conclusions d'un nœud sera donnée de gauche à droite. Les éléments de P et de C ne seront jamais représentés, les arêtes dont la source est dans P seront représentées comme des traits vers le haut partant de leur but et les arêtes dont le but est dans C seront représentées comme des traits vers le bas partant de leur source. Pour simplifier l'écriture, on notera une suite d'arêtes dont les types sont les formules de la suite Γ par deux arêtes séparées par des points de suspension (le nombre de formules dans Γ donne ainsi le nombre d'arêtes concernées).

On traduit les preuves du calcul des séquents MLL (sans éléments neutres) en structures de preuve multiplicatives par :

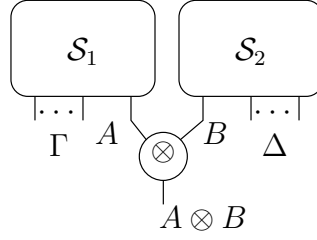
- règle ax : la structure de preuve obtenue contient un unique nœud avec deux conclusions :



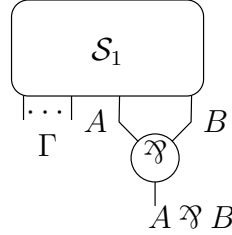
- règle cut : si \mathcal{S}_1 et \mathcal{S}_2 sont les structures de preuve associées aux deux prémisses de la règle, la structure de preuve associée à la preuve complète est obtenue en ajoutant un nœud cut entre les arêtes correspondant aux occurrences de formules actives dans la règle :



- règle \otimes : si \mathcal{S}_1 et \mathcal{S}_2 sont les structures de preuve associées aux deux prémisses de la règle, la structure de preuve associée à la preuve complète est obtenue en ajoutant un nœud \otimes entre les arêtes correspondant aux occurrences de formules actives dans la règle :



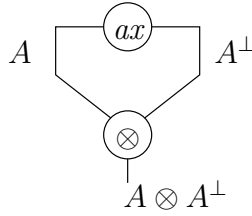
- règle \wp : si \mathcal{S}_1 est la structure de preuve associée à la prémisse de la règle, la structure de preuve associée à la preuve complète est obtenue en ajoutant un nœud \wp entre les arêtes correspondant aux occurrences de formules actives dans la règle :



On appelle *réseaux de preuve* les structures de preuve qui sont l'image d'une preuve de calcul des séquents par cette traduction.

Critère de correction

On peut facilement voir que toute structure de preuve multiplicative n'est pas un réseau de preuve, comme le montre l'exemple suivant :



si cette structure de preuve multiplicative était un réseau de preuve, $A \otimes A^\perp$ serait prouvable et ce n'est pas le cas.

Pour caractériser celles qui le sont (sans faire référence au calcul des séquents), on utilise un *critère de correction*. Celui que nous étudions ici est dû à Danos-Regnier.

Définition 28 (graphe de correction)

Un *graphe de correction* est une structure de preuve sur l'alphabet de nœuds $\{ax, cut, \otimes, \wp_1, \wp_2\}$.

Étant donnée une structure de preuve multiplicative \mathcal{S} contenant k nœuds de sorte \wp , un graphe de correction \mathcal{G} est un graphe de correction de \mathcal{S} s'il est obtenu à partir de \mathcal{S} de la manière suivante : on ajoute k nouveaux nœuds dans C , puis chaque nœud n de sorte \wp est transformé en un nœud de sorte \wp_1 ou \wp_2 en choisissant l'un des nouveaux éléments de C comme le but de l'une des prémisses, *i.e.* on choisit une des prémisses a de n , et si on avait $b(a) = n$ dans \mathcal{S} , on aura $b(a) \in C$ dans \mathcal{G} .

Remarque : C'est ici qu'on réintroduit une différence entre \otimes et \wp alors que ces deux sortes de nœuds sont traitées de la même manière dans les structures de preuve (bien que la logique fasse la différence).

Définition 29 (Critère de Danos-Regnier)

Une structure de preuve multiplicative non vide \mathcal{S} est *correcte* si les graphes non orientés associés aux graphes de correction de \mathcal{S} sont tous acycliques et connexes.

Proposition 23 (Correction des réseaux)

Tout réseau de preuve satisfait le critère de Danos-Regnier.

DÉMONSTRATION : Par récurrence sur la taille de la preuve dont le réseau est la traduction, en considérant chaque dernière règle possible :

- règle ax : Le réseau a un nœud et deux arêtes, un unique graphe de correction qui est lui-même et qui est acyclique et connexe.
- règle cut : Un graphe de correction du réseau est obtenu en choisissant un graphe de correction pour chacun des réseaux obtenus pour les prémisses de la règle et en les reliant par le nœud cut . Par hypothèse de récurrence, ces deux graphes de correction sont acycliques et connexes, en les reliant par un unique chemin on obtient à nouveau un graphe acyclique et connexe.
- règle \otimes : Comme pour cut .
- règle \wp : Un graphe de correction du réseau est obtenu en choisissant un graphe de correction du réseau obtenu pour la prémisse et en ajoutant soit un nœud de sorte \wp_1 soit un nœud de sorte \wp_2 . Partant d'un graphe acyclique et connexe, on obtient ainsi nécessairement un graphe acyclique et connexe. \square

Théorème 6 (Séquentialisation)

Une structure de preuve multiplicative correcte est un réseau de preuve.

La démonstration de ce résultat nécessite d'introduire la notion d'*empire* et de prouver certaines de ses propriétés. On ne considère désormais (et jusqu'à la preuve du théorème) que des structures de preuve sans coupure, *i.e.* sans nœud de sorte cut (l'idée étant qu'on pourra les remplacer par des \otimes).

Si a est une arête dont on veut préciser le type A , on utilisera souvent la notation a^A .

Définition 30 (a -graphe de correction)

Soit a une arête de la structure de preuve multiplicative \mathcal{S} , un a -*graphe de correction* de \mathcal{S} est une structure de preuve sur l'alphabet de nœuds $\{ax, \otimes, \otimes_1, \otimes_2, \wp_0, \wp_1, \wp_2\}$ obtenue à partir d'un graphe de correction de \mathcal{S} en déconnectant a du nœud dont elle est prémisse (*i.e.* son but est désormais un nouvel élément de C). Le a -graphe de correction associé au graphe de correction \mathcal{G} est noté $\mathcal{G} \upharpoonright_a$.

Dans une structure de preuve multiplicative correcte, un a -graphe de correction a au plus deux composantes connexes.

Définition 31 (Empire)

Soit a une arête de la structure de preuve multiplicative \mathcal{S} , l'*empire* de a , noté $\mathbf{emp}(a)$, est le module de \mathcal{S} obtenu en ne conservant que les arêtes qui sont connectées à a dans tous les (graphes non orientés associés aux) a -graphes de correction de \mathcal{S} .

Lemme 11 (Constitution d'un empire)

Soient \mathcal{S} une structure de preuve multiplicative correcte et a une arête de \mathcal{S} , on a les propriétés suivantes :

- si b^B et c^{B^\perp} sont les conclusions d'un nœud ax , $b \in \mathbf{emp}(a)$ si et seulement si $c \in \mathbf{emp}(a)$
- si b^B et c^C sont les prémisses d'un nœud \wp dont a n'est pas prémisse, la conclusion $d^{B\wp C}$ du nœud est dans $\mathbf{emp}(a)$ si et seulement si b et c y sont

- si a est prémisses d'un nœud, sa conclusion n'est pas dans $\mathbf{emp}(a)$
- $\mathbf{emp}(a)$ est clos vers le haut : les prémisses d'un nœud dont la conclusion est dans $\mathbf{emp}(a)$ sont dans $\mathbf{emp}(a)$
- $\mathbf{emp}(a)$ est “souvent” clos vers le bas : si $b \in \mathbf{emp}(a)$ est la prémisses d'un nœud dont la conclusion n'est pas dans $\mathbf{emp}(a)$ alors soit a est prémisses de ce nœud, soit c'est un nœud \mathfrak{X} et l'autre prémisses n'est pas dans $\mathbf{emp}(a)$

DÉMONSTRATION : – La définition d'un a -graphe de correction ne touche pas à la source des arêtes donc ne peut pas déconnecter les arêtes d'un nœud ax de ce nœud. b^B et c^{B^\perp} sont donc reliées dans tout a -graphe de correction (y compris si l'une des deux est a) puisqu'elles sont connectées au nœud.

- Si les deux prémisses sont dans $\mathbf{emp}(a)$, dans tout a -graphe de correction, la conclusion est reliée à l'une des deux (puisque a n'est pas prémisses) et elles sont toutes les deux reliées à a donc la conclusion est reliée à a .

Si $d^{B^{\mathfrak{X}}C}$ est dans $\mathbf{emp}(a)$, soit \mathcal{G} un graphe de correction, dans $\mathcal{G} \upharpoonright_a$ l'une des deux prémisses est reliée à la conclusion (elle-même reliée à a), on va montrer que les deux prémisses sont reliées ce qui permet de conclure. Dans \mathcal{G} , un tel chemin existe (et ne passe pas par d sinon en basculant le \mathfrak{X} vers la prémisses reliée à la conclusion de d , *i.e.* en déconnectant l'autre prémisses, on obtiendrait un cycle), il suffit de montrer qu'il ne passe pas par a . Si c'était le cas, on pourrait choisir de basculer le \mathfrak{X} pour relier $d^{B^{\mathfrak{X}}C}$ à la prémisses qui arrive à a par le bas, ce qui nous donne le graphe de correction \mathcal{G}' . Ceci ne touche pas au chemin puisqu'il ne passe pas par d . d ne pourrait alors pas être reliée à a dans $\mathcal{G}' \upharpoonright_a$ (car le chemin de d à a dans \mathcal{G}' est unique par acyclicité et est coupé dans $\mathcal{G}' \upharpoonright_a$).

- Si a est prémisses d'un nœud \mathfrak{X} , on choisit un a -graphe de correction \mathcal{G} qui positionne le \mathfrak{X} vers a et puisque cette arête est déconnectée du nœud \mathfrak{X} dans $\mathcal{G} \upharpoonright_a$, la conclusion n'est plus reliée à a (pas d'autre chemin possible par acyclicité).

Si a est prémisses d'un nœud \otimes , s'il existe un chemin entre la conclusion et a dans un a -graphe de correction $\mathcal{G} \upharpoonright_a$, alors il y a un cycle dans \mathcal{G} .

- On vient de voir que si la conclusion est dans $\mathbf{emp}(a)$, a ne peut pas être prémisses. Le cas d'un nœud \mathfrak{X} a donc été traité juste avant : si la conclusion est dans $\mathbf{emp}(a)$, les deux prémisses aussi.

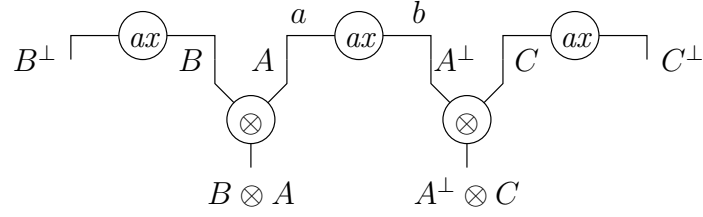
Dans le cas d'un \otimes , puisque a n'est pas prémisses, la conclusion est reliée aux deux prémisses dans tout a -graphe de correction donc la conclusion est dans $\mathbf{emp}(a)$ si et seulement si les deux prémisses le sont aussi (et si et seulement si l'une des deux prémisses l'est).

- Si a n'est pas prémisses et si le nœud est un \otimes , on vient de voir que la conclusion est dans $\mathbf{emp}(a)$ dès que l'une des prémisses l'est. Si a n'est pas prémisses et s'il s'agit d'un nœud \mathfrak{X} , on a déjà vu que la conclusion n'est pas dans $\mathbf{emp}(a)$ si et seulement si l'une des prémisses au moins ne l'est pas. □

Lemme 12 (Emboîtement d'empires)

Soit \mathcal{S} une structure de preuve multiplicative correcte, si l'arête b n'appartient pas à l'empire de l'arête a , alors soit $\mathbf{emp}(a) \subset \mathbf{emp}(b)$ soit $\mathbf{emp}(a) \cap \mathbf{emp}(b) = \emptyset$.

Attention, ce résultat est faux si $b \in \mathbf{emp}(a)$, on peut très bien avoir $a \in \mathbf{emp}(b)$ avec un recouvrement non trivial des deux empires, voir a^A et b^{A^\perp} dans la structure de preuve suivante :



DÉMONSTRATION : On considère un graphe de correction \mathcal{G} ayant les propriétés suivantes :

- si b est prémisses d'un nœud \mathfrak{N} , on positionne ce nœud vers b
- si a est prémisses d'un nœud \mathfrak{N} dont la conclusion est dans $\mathbf{emp}(b)$ (ce qui exclut le cas précédent par le lemme 11), on positionne ce nœud vers a
- pour tout *autre* nœud \mathfrak{N} dont la conclusion n'est pas dans $\mathbf{emp}(b)$, on sait par le lemme 11 qu'au moins une des prémisses n'est pas dans $\mathbf{emp}(b)$ et on positionne le \mathfrak{N} vers une telle prémisses
- pour tout *autre* nœud \mathfrak{N} dont la conclusion est dans $\mathbf{emp}(b)$ mais pas dans $\mathbf{emp}(a)$, de même on peut positionner le \mathfrak{N} vers une prémisses qui n'est pas dans $\mathbf{emp}(a)$.

On montre que les arêtes connectées à b dans $\mathcal{G} \upharpoonright_b$ sont exactement l'empire de b : une arête qui relierait $\mathbf{emp}(b)$ à son complémentaire serait, d'après le lemme 11, soit b , soit une prémisses de nœud \mathfrak{N} mais ceci est impossible par construction de \mathcal{G} .

On montre de même que la seule arête de $\mathbf{emp}(b)$ dans \mathcal{G} qui peut relier $\mathbf{emp}(a)$ à son complémentaire est a car la seule autre possible est b et $b \notin \mathbf{emp}(a)$.

On montre alors le lemme :

- Si $a \in \mathbf{emp}(b)$, soit c une arête de $\mathbf{emp}(a)$, elle est reliée à a dans $\mathcal{G} \upharpoonright_a$. Si ce chemin passe par b , soit c est reliée à b en passant par le nœud dont b est conclusion et ce morceau de chemin est dans $\mathcal{G} \upharpoonright_b$ donc $c \in \mathbf{emp}(b)$, soit a est reliée à b en passant par le nœud dont b est conclusion et ce morceau de chemin est dans $\mathcal{G} \upharpoonright_b$ et sort de $\mathbf{emp}(a)$ (car $b \notin \mathbf{emp}(a)$) mais pour cela il faut emprunter a (d'après la remarque ci-dessus) ce qui est impossible dans $\mathcal{G} \upharpoonright_a$. Si le chemin ne passe pas par b , il est dans $\mathcal{G} \upharpoonright_b$ et $c \in \mathbf{emp}(b)$.
- Si $a \notin \mathbf{emp}(b)$, il n'y a pas d'arête entre $\mathbf{emp}(a)$ et son complémentaire dans $\mathbf{emp}(b)$ et $b \notin \mathbf{emp}(a)$ donc aucune arête de $\mathbf{emp}(b)$ ne peut être dans $\mathbf{emp}(a)$, les empires sont disjoints. \square

Lemme 13 (Empire)

Soit \mathcal{S} une structure de preuve multiplicative correcte, l'empire de a dans \mathcal{S} est la plus grosse sous-structure de preuve multiplicative correcte de \mathcal{S} ayant a comme conclusion.

DÉMONSTRATION : – C'est une structure de preuve multiplicative car c'est un module clos vers le haut : si une arête b conclusion d'un nœud n est dans $\mathbf{emp}(a)$, par le lemme 11, toutes les prémisses de n sont dans $\mathbf{emp}(a)$.

- Elle a a comme conclusion par le lemme 11.
- Elle est correcte : soit \mathcal{G} un graphe de correction de $\mathbf{emp}(a)$, c'est un sous-graphe d'un graphe de correction \mathcal{G}_0 de \mathcal{S} que l'on peut construire comme dans la preuve du lemme 12 pour que les arêtes de \mathcal{G}_0 reliées à a dans $\mathcal{G}_0 \upharpoonright_a$ soient celles de $\mathbf{emp}(a)$. Ainsi \mathcal{G} est acyclique puisque \mathcal{G}_0 l'est, de plus il est connexe car toute arête de \mathcal{G} est connectée à a dans $\mathcal{G}_0 \upharpoonright_a$ donc dans \mathcal{G} car le chemin ne peut sortir de \mathcal{G} que par a .
- C'est la plus grosse : soit \mathcal{S}' une sous-structure de preuve multiplicative correcte de \mathcal{S} de conclusion a et soit b une arête de \mathcal{S}' , pour tout graphe de correction \mathcal{G} de \mathcal{S} il existe un chemin dans \mathcal{S}' de b à a , donc qui arrive sur a par le haut. Ce chemin est dans $\mathcal{G} \upharpoonright_a$ et $b \in \mathbf{emp}(a)$. \square

Lemme 14 (Tenseur scindant)

Soit \mathcal{S} une structure de preuve multiplicative correcte sans nœud \mathfrak{A} terminal et possédant au moins un nœud \otimes terminal, un de ces nœuds a la propriété qu'en le supprimant on sépare \mathcal{S} en deux structures de preuve multiplicatives correctes (on dit qu'il s'agit d'un nœud \otimes scindant).

DÉMONSTRATION : On choisit une prémisses de nœud \otimes terminal a telle que $\mathbf{emp}(a)$ est maximal pour l'inclusion parmi les empires de prémisses de nœud \otimes terminal. On montre que les conclusions de $\mathbf{emp}(a)$ (autres que a) sont des conclusions de \mathcal{S} . Sinon, par le [lemme 11](#), on aurait une conclusion b de $\mathbf{emp}(a)$ prémisses d'un nœud \mathfrak{A} qui se trouve lui-même nécessairement héréditairement au-dessus de la prémisses c d'un nœud \otimes terminal qui n'est pas dans $\mathbf{emp}(a)$ (à cause de la clôture vers le haut du [lemme 11](#)). Or b est dans $\mathbf{emp}(c)$ et dans $\mathbf{emp}(a)$ donc, par le [lemme 12](#), $\mathbf{emp}(a) \subset \mathbf{emp}(c)$ ce qui contredit la maximalité de $\mathbf{emp}(a)$.

En supprimant dans \mathcal{S} le nœud \otimes terminal dont a est prémisses on obtient deux graphes : $\mathbf{emp}(a)$ et le reste. Par le [lemme 13](#), $\mathbf{emp}(a)$ est une structure de preuve correcte. On a également que le reste est une structure de preuve et vérifie le critère de correction. \square

On peut alors démontrer le [théorème 6](#) :

DÉMONSTRATION : Par récurrence sur le nombre de nœuds de la structure de preuve multiplicative correcte \mathcal{S} , en considérant les cas suivants :

- Si \mathcal{S} a un nœud \mathfrak{A} terminal, en supprimant ce nœud on obtient une structure de preuve multiplicative correcte, et on peut conclure par hypothèse de récurrence.
- Si \mathcal{S} n'a pas de nœud \mathfrak{A} terminal, mais possède au moins un nœud *cut* ou un nœud \otimes , on considère la structure de preuve multiplicative \mathcal{S}' obtenue en remplaçant tout nœud *cut* de \mathcal{S} de prémisses a^A et b^{A^\perp} par un nœud \otimes dont la conclusion a type $A \otimes A^\perp$. \mathcal{S}' est une structure de preuve multiplicative correcte, n'a pas de nœud \mathfrak{A} terminal, a un nœud \otimes terminal et, par le [lemme 14](#), \mathcal{S}' a un nœud \otimes scindant. Le nœud *cut* ou \otimes de \mathcal{S} correspondant à ce nœud est scindant dans \mathcal{S} , on peut donc appliquer l'hypothèse de récurrence aux deux structures de preuve multiplicatives correctes obtenues.
- Si \mathcal{S} n'a ni nœud *cut*, ni nœud \mathfrak{A} ou \otimes terminal, \mathcal{S} ne contient que des nœuds ax . Par connexité de l'unique graphe de correction, \mathcal{S} ne contient qu'un seul nœud ax et est la traduction d'une règle ax . \square

On peut raffiner cette démonstration pour extraire de toute structure de preuve multiplicative correcte, non seulement une preuve mais une preuve *focalisée* (on s'intéresse ici au cas sans coupure). Il suffit pour cela de choisir un nœud \otimes *héréditairement scindant*. Ceci permet de prouver la propriété de focalisation ([proposition 20](#)) puisque partant d'une preuve, on peut calculer le réseau associé et le séquentialiser en une preuve focalisée.

Lemme 15 (Tenseur héréditairement scindant)

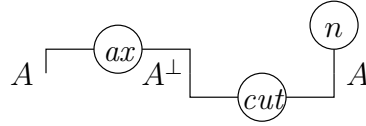
Soit \mathcal{S} une structure de preuve multiplicative correcte sans nœud \mathfrak{A} terminal et possédant au moins un nœud \otimes terminal, un de ces nœuds a la propriété qu'il est scindant et que s'il est conclusion de nœuds \otimes ceux-ci sont également scindants avec la propriété que ... (on dit qu'il s'agit d'un nœud \otimes héréditairement scindant).

DÉMONSTRATION : Par le [lemme 14](#), il existe un nœud \otimes scindant n . Soient \mathcal{S}_1 et \mathcal{S}_2 les structures de preuve correctes obtenues en supprimant n dans \mathcal{S} , par hypothèse de récurrence, soit \mathcal{S}_i possède un nœud \mathfrak{A} terminal, soit elle possède un nœud \otimes héréditairement scindant n_i . Si l'un des n_i existe et n'est pas prémisses de n alors il est héréditairement scindant pour \mathcal{S} , sinon n est héréditairement scindant. \square

Élimination des coupures

Pour éliminer les coupures dans les structures de preuve multiplicatives, on définit les deux étapes élémentaires de réduction suivantes qui sont des réécritures de graphe.

L'étape ax remplace un module :

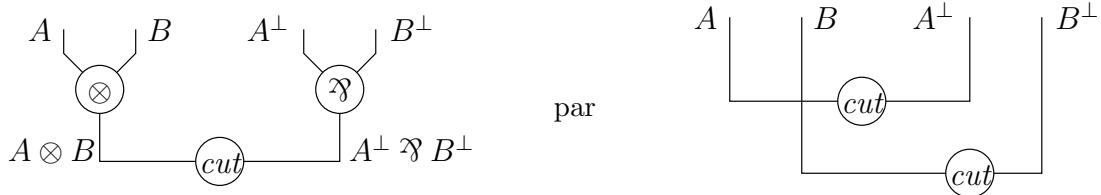


avec $a^A \neq b^A$ où a est la conclusion non coupée du nœud ax et b est la conclusion du nœud n , par :



où la conclusion du nœud n est l'arête a .

L'étape \otimes/\wp remplace un module



Proposition 24 (Préservation de la correction par réduction)

Si la structure de preuve multiplicative correcte \mathcal{S} se réduit en \mathcal{S}' alors \mathcal{S}' est correcte.

DÉMONSTRATION : Le cas d'une réduction ax est immédiat.

Pour une réduction \otimes/\wp , soient a^A et b^B les prémisses du nœud de sorte \otimes et c^{A^\perp} et d^{B^\perp} celles du nœud de sorte \wp . Supposons qu'il y ait un cycle dans un graphe de correction de \mathcal{S}' . S'il ne passe par aucune des deux coupures c'est également un cycle dans un graphe de correction de \mathcal{S} . S'il passe uniquement par la coupure $a-c$ (resp. $b-d$), on se place dans le graphe de correction de \mathcal{S} associé à celui de \mathcal{S}' en basculant le \wp vers c (resp. d). S'il passe par les deux coupures, soit il relie a et b et c'est un cycle dans un graphe de correction de \mathcal{S} , soit il relie $a-c$ et $b-d$ ou $a-d$ et $b-c$ et dans le graphe de correction de \mathcal{S} associé en basculant le \wp de façon arbitraire on obtient un cycle.

Soit \mathcal{G}' un graphe de correction \mathcal{S}' , et soit \mathcal{G} le graphe de correction de \mathcal{S} obtenu à partir de \mathcal{G}' en basculant le \wp vers d . Par connexité, toute arête de \mathcal{G} est reliée à a , b , c ou d . Donc dans \mathcal{G}' , on a au plus deux composantes connexes : les arêtes reliées à $a-c$ et celles reliées à $b-d$. Si, hors du module, c est reliée à a ou b on aurait un cycle dans \mathcal{G} , c doit être reliée aux autres donc à d . D'où on déduit que c et d sont reliées dans \mathcal{G}' qui est donc connexe. \square

Proposition 25 (Normalisation forte)

Soit \mathcal{R} un réseau de preuve, toute coupure de \mathcal{R} peut être réduite et le nombre d'étapes de réduction jusqu'à la forme normale est borné par le nombre de nœuds de \mathcal{R} .

DÉMONSTRATION : Par correction on n'a pas de coupure sur les deux conclusions d'un même nœud ax donc l'une des deux étapes élémentaires de réduction peut s'appliquer. De plus l'application d'une telle étape fait décroître strictement le nombre de nœuds de \mathcal{R} d'où la borne. \square

Lemme 16 (Sous-diamant)

Si le réseau \mathcal{R} se réduit en \mathcal{R}_1 par une étape de réduction r_1 et en \mathcal{R}_2 par une étape de réduction r_2 alors il existe \mathcal{R}' tel que \mathcal{R}_1 et \mathcal{R}_2 se réduisent en \mathcal{R}' par au plus une étape de réduction.

DÉMONSTRATION : – Si r_1 et r_2 sont la même étape de réduction, on a $\mathcal{R}' = \mathcal{R}_1 = \mathcal{R}_2$.

- Si r_1 et r_2 sont des étapes \otimes/\mathfrak{A} distinctes, en appliquant r_2 dans \mathcal{R}_1 et r_1 dans \mathcal{R}_2 , on obtient le même \mathcal{R}' .
- De même si l'une est une étape \otimes/\mathfrak{A} et l'autre est une étape ax .
- Si r_1 et r_2 sont des étapes ax distinctes portant sur les coupures c_1 et c_2 :
 - si $c_1 = c_2$ sont conclusions de deux nœuds ax différents, on a $\mathcal{R}' = \mathcal{R}_1 = \mathcal{R}_2$
 - si $c_1 \neq c_2$ sont conclusions d'un même nœud ax sur lequel portent r_1 et r_2 , on a $\mathcal{R}' = \mathcal{R}_1 = \mathcal{R}_2$
 - si $c_1 \neq c_2$ et r_1 et r_2 portent sur des nœuds ax différents, en appliquant r_2 dans \mathcal{R}_1 et r_1 dans \mathcal{R}_2 , on obtient le même \mathcal{R}' . \square

Proposition 26 (Confluence)

La réduction des réseaux de preuve est confluente.

DÉMONSTRATION : On montre, par récurrence sur $n + p$, que si \mathcal{R} se réduit en \mathcal{R}_1 en n étapes et si \mathcal{R} se réduit en \mathcal{R}_2 en p étapes alors il existe \mathcal{R}' tel que \mathcal{R}_1 se réduit en \mathcal{R}' en $p' \leq p$ étapes et \mathcal{R}_2 se réduit en \mathcal{R}' en $n' \leq n$ étapes.

- Si $(n, p) = (0, 0)$, on a $\mathcal{R}' = \mathcal{R}_1 = \mathcal{R}_2 = \mathcal{R}$.
- Si $(n, p) = (1, 0)$, on a $\mathcal{R}' = \mathcal{R}_1$.
- Si $(n, p) = (0, 1)$, on a $\mathcal{R}' = \mathcal{R}_2$.
- Sinon on a un couple $(n + 1, p + 1)$, soit \mathcal{R}'_1 le réseau obtenu après une étape dans la réduction de \mathcal{R} à \mathcal{R}_1 et de même pour \mathcal{R}'_2 . Par le [lemme 16](#), il existe \mathcal{R}'' tel que \mathcal{R}'_1 et \mathcal{R}'_2 se réduisent en \mathcal{R}'' en au plus une étape. Par hypothèse de récurrence appliquée à \mathcal{R}'_2 , \mathcal{R}'' et \mathcal{R}_2 , il existe \mathcal{R}''_2 tel que \mathcal{R}'' se réduit en \mathcal{R}''_2 en au plus p étapes et \mathcal{R}_2 se réduit en \mathcal{R}'' en au plus une étape. Par hypothèse de récurrence appliquée à \mathcal{R}'_1 , \mathcal{R}_1 et \mathcal{R}''_2 , il existe \mathcal{R}' tel que \mathcal{R}_1 se réduit en \mathcal{R}' en moins de $p + 1$ étapes et \mathcal{R}''_2 se réduit en \mathcal{R}' en moins de n étapes. On en déduit que \mathcal{R}_2 se réduit en \mathcal{R}' en moins de $n + 1$ étapes. \square

Éléments neutres

Dès que l'on cherche à étendre la notion de réseaux aux autres connecteurs, des difficultés apparaissent. Avec les éléments neutres, on ne définira pas de critère de correction exact mais seulement un critère de correction faible : tout réseau est faiblement correct mais toute structure de preuve faiblement correcte n'est pas nécessairement un réseau.

On considère deux nouvelles sortes de nœuds :

- sorte 1 : aucune prémisse, une conclusion, l'étiquette de la conclusion est 1
- sorte \perp : aucune prémisse, une conclusion, l'étiquette de la conclusion est \perp

On appelle *structures de preuve multiplicatives avec éléments neutres* les structures de preuve sur l'alphabet de nœuds $\{ax, cut, \otimes, \mathfrak{A}, 1, \perp\}$.

Les graphes de correction sont définis de la même manière que sans éléments neutres, ce sont des structures de preuve sur l'alphabet de nœuds $\{ax, cut, \otimes, \mathfrak{A}_1, \mathfrak{A}_2, 1, \perp\}$.

Définition 32 (Critère de correction faible)

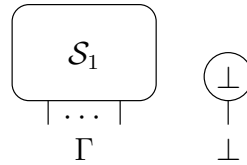
Une structure de preuve multiplicative avec éléments neutres non vide \mathcal{S} est *faiblement correcte* si les graphes non orientés associés aux graphes de correction de \mathcal{S} sont tous acycliques et possèdent une composante connexe de plus que de nœuds de sorte \perp .

On étend la traduction des preuves du calcul des séquents en structures de preuve par :

– règle 1 :

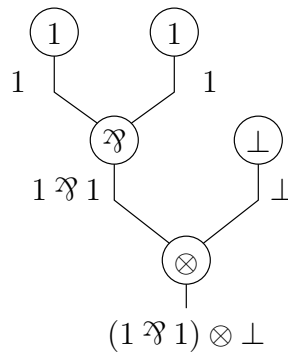


– règle \perp :



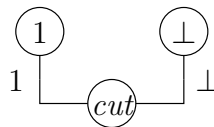
et on vérifie que tout réseau de preuve est une structure de preuve faiblement correcte.

La structure de preuve multiplicative avec éléments neutres suivante :



est faiblement correcte mais n'est pas un réseau (en particulier, la formule $(1 \wp 1) \otimes \perp$ n'est pas prouvable).

L'étape élémentaire de réduction $1/\perp$ remplace un module :



par le module vide.

Proposition 27 (Préservation de la correction faible par réduction)

Si la structure de preuve multiplicative avec éléments neutres faiblement correcte \mathcal{S} se réduit en \mathcal{S}' alors \mathcal{S}' est faiblement correcte.

DÉMONSTRATION : On a déjà montré un certain nombre de résultats dans la [proposition 24](#).

Concernant l'acyclicité, il ne reste qu'à vérifier le cas de la réduction $1/\perp$ qui ne peut pas créer de cycle puisqu'elle ne fait que supprimer des arêtes.

Pour l'étape ax , dans tout graphe de correction, on remplace un chemin par une arête ce qui ne modifie pas le nombre de composantes connexes et on ne touche pas aux nœuds de sorte \perp .

Pour l'étape \otimes/\wp , par acyclicité des graphes de correction du module initial, aucune composante connexe ne contient à la fois b et a, c ou d . Si on compare à un graphe de correction qui a basculé le \wp vers c , on ne modifie rien aux connexions entre a et c , on déconnecte b de a et c et on la reconnecte à d . Ainsi on crée une composante connexe en déconnectant b de a et c et on la fusionne avec celle de d en reconnectant. Le nombre de composantes connexes et de nœuds de sorte \perp n'est donc pas modifié.

Pour l'étape $1/\perp$, dans tout graphe de correction, le module effacé est une composante connexe. On efface en même temps un nœud de sorte \perp . On garde bien une composante connexe de plus que de nœuds de sorte \perp . \square

La nouvelle étape élémentaire de réduction fait également décroître le nombre de nœuds de la structure de preuve et vérifie la propriété de sous-diamant. On en déduit que les réseaux de preuve multiplicatifs avec éléments neutres ont les propriétés de normalisation forte et de confluence.

6.2 MELL

Comme nous l'avons vu, l'introduction des connecteurs 1 et \perp complique l'étude des réseaux de preuve. Nous allons constater que les connecteurs exponentiels ajoutent encore quelques difficultés.

Structures de preuve exponentielles

On considère les nouvelles sortes de nœuds suivantes :

- sorte $!$: une prémisses, une conclusion, si l'étiquette de la prémisses est A alors celle de la conclusion est $!A$
- sorte $?p$: une prémisses, une conclusion, la prémisses et la conclusion ont la même étiquette $?A$ (où A peut être une formule quelconque)
- sorte $?d$: une prémisses, une conclusion, si l'étiquette de la prémisses est A alors celle de la conclusion est $?A$
- sorte $?w$: aucune prémisses, une conclusion, l'étiquette de la conclusion est $?A$ (où A peut être une formule quelconque)
- sorte $?c$: deux prémisses, une conclusion, les deux prémisses et la conclusion ont la même étiquette $?A$ (où A peut être une formule quelconque)
- sorte $?c_1$: une prémisses, une conclusion, la prémisses et la conclusion ont la même étiquette $?A$ (où A peut être une formule quelconque)
- sorte $!_i$ ($i \in \mathbb{N}$) : aucune prémisses, $i+1$ conclusions, la première conclusion a pour étiquette $!A$ (où A peut être une formule quelconque) et les autres conclusions ont pour étiquettes des formules $?A_i$ (où A_i peut être une formule quelconque)

Une nouvelle difficulté apparaît avec la règle $!$ qui est fortement contextuelle : le contexte d'une telle règle doit être constitué uniquement de formules commençant par $?$. Il est alors nécessaire d'introduire une information supplémentaire dans les structures de preuve : les boîtes.

Une *structure de preuve exponentielle* est une structure de preuve sur l'alphabet de nœuds $\{ax, cut, \otimes, \wp, !, ?p, ?d, ?w, ?c\}$ munie d'une fonction qui associe à chaque nœud n de sorte $!$ une sous-structure de preuve dont les conclusions sont n et des nœuds de sorte $?p$, appelée *boîte* de n . On demande de plus que tout nœud de sorte $?p$ soit conclusion d'une unique boîte et que deux boîtes soient toujours soit incluses l'une dans l'autre soit disjointes.

La *profondeur* d'un nœud (ou d'une arête) est le nombre de boîtes auxquelles il appartient.

Étant donnée une boîte, on appelle *porte principale* son unique conclusion de sorte $!$ et *portes auxiliaires* ses conclusions de sorte $?p$. Graphiquement, la boîte d'un nœud $!$ sera représentée dans un rectangle passant par ce nœud et par les portes auxiliaires.

Du fait de la règle $?w$ très similaire à la règle \perp , on ne va pas pouvoir donner de critère de correction mais seulement un critère de correction faible.

Définition 33 (graphe de correction)

Un *graphe de correction* est une structure de preuve sur l'alphabet de nœuds $\{ax, cut, \otimes, \wp_1, \wp_2, ?d, ?w, ?c_1\} \cup \{!_i \mid i \in \mathbb{N}\}$.

Étant donnée une structure de preuve exponentielle \mathcal{S} , un graphe de correction \mathcal{G} est un graphe de correction de \mathcal{S} s'il est obtenu à partir de \mathcal{S} de la manière suivante :

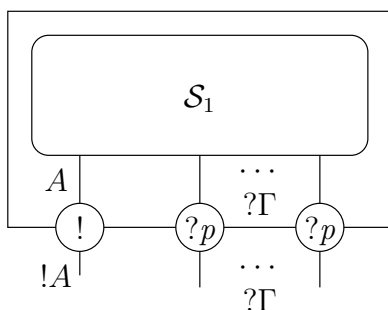
- On considère, soit les nœuds à profondeur 0, soit ceux à profondeur 0 dans une boîte.
- On remplace chaque nœud de sorte $!$ dont la boîte a pour conclusions des arêtes de type $!A, ?A_1, \dots, ?A_i$ par un nœud de sorte $!_i$ ayant ces arêtes comme conclusions.
- Chaque nœud de sorte \mathfrak{A} est transformé en un nœud de sorte \mathfrak{A}_1 ou \mathfrak{A}_2 en ajoutant un nouvel élément dans C qui devient le but de l'une des prémisses.
- Chaque nœud de sorte $?c$ est transformé en un nœud de sorte $?c_1$ en ajoutant un nouvel élément dans C qui devient le but de l'une des prémisses.

Définition 34 (Critère de correction faible)

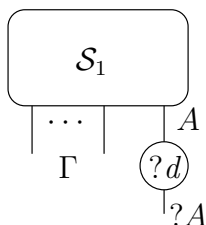
Une structure de preuve exponentielle non vide \mathcal{S} est *faiblement correcte* si les graphes non orientés associés aux graphes de correction de \mathcal{S} sont tous acycliques et possèdent une composante connexe de plus que de nœuds de sorte $?w$.

On traduit les preuves du calcul des séquents MELL en structures de preuve exponentielles par :

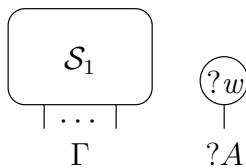
- règle $!$:



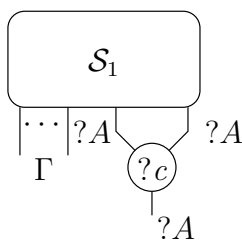
- règle $?d$:



- règle $?w$:



- règle $?c$:



Proposition 28 (Correction faible des réseaux)

Tout réseau de preuve est faiblement correct.

DÉMONSTRATION : On étend la preuve du cas multiplicatif en ajoutant les nouvelles règles :

- règle ! : À partir de la profondeur 1, le critère de correction faible est vérifié puisqu'il l'est pour le réseau associé à la prémisse de la règle. À profondeur 0, on a un unique nœud dans le graphe de correction qui n'est pas de sorte $?w$ ce qui vérifie le critère.
- règle $?d$: Un graphe de correction est obtenu en choisissant un graphe de correction du réseau obtenu pour la prémisse et un ajoutant un nœud et une arête sans ajouter de cycle ni modifier le nombre de composantes connexes.
- règle $?c$: Un graphe de correction est obtenu en choisissant un graphe de correction du réseau obtenu pour la prémisse et un ajoutant un nœud et une arête (sous la prémisse du nœud $?c$ qui a été choisie) sans ajouter de cycle ni modifier le nombre de composantes connexes.
- règle $?w$: Un graphe de correction est obtenu en choisissant un graphe de correction du réseau obtenu pour la prémisse et un ajoutant un nœud et une arête déconnectés du reste. On ne crée pas de cycle, on ajoute une composante connexe et un nœud de sorte $?w$. □

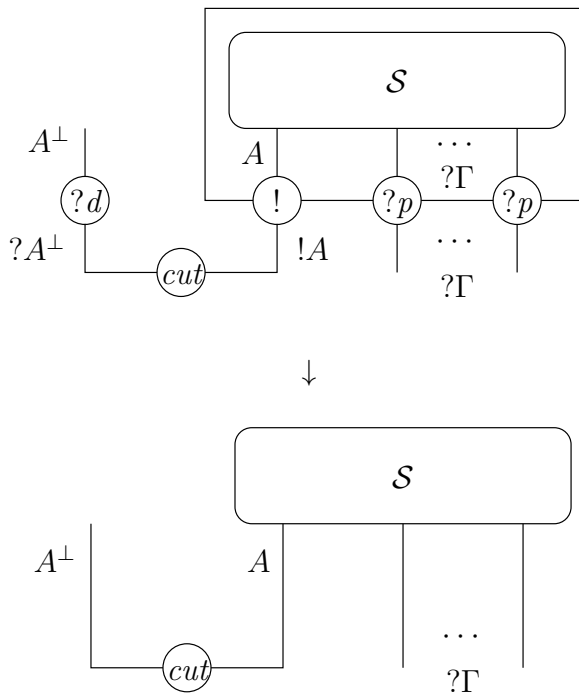
Théorème 7 (Séquentialisation sans $?w$)

Une structure de preuve exponentielle faiblement correcte sans nœud de sorte $?w$ est un réseau de preuve.

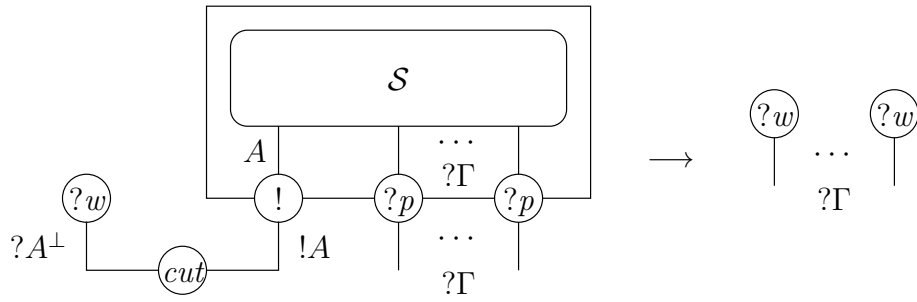
Élimination des coupures

On introduit 4 nouvelles étapes élémentaires de réduction :

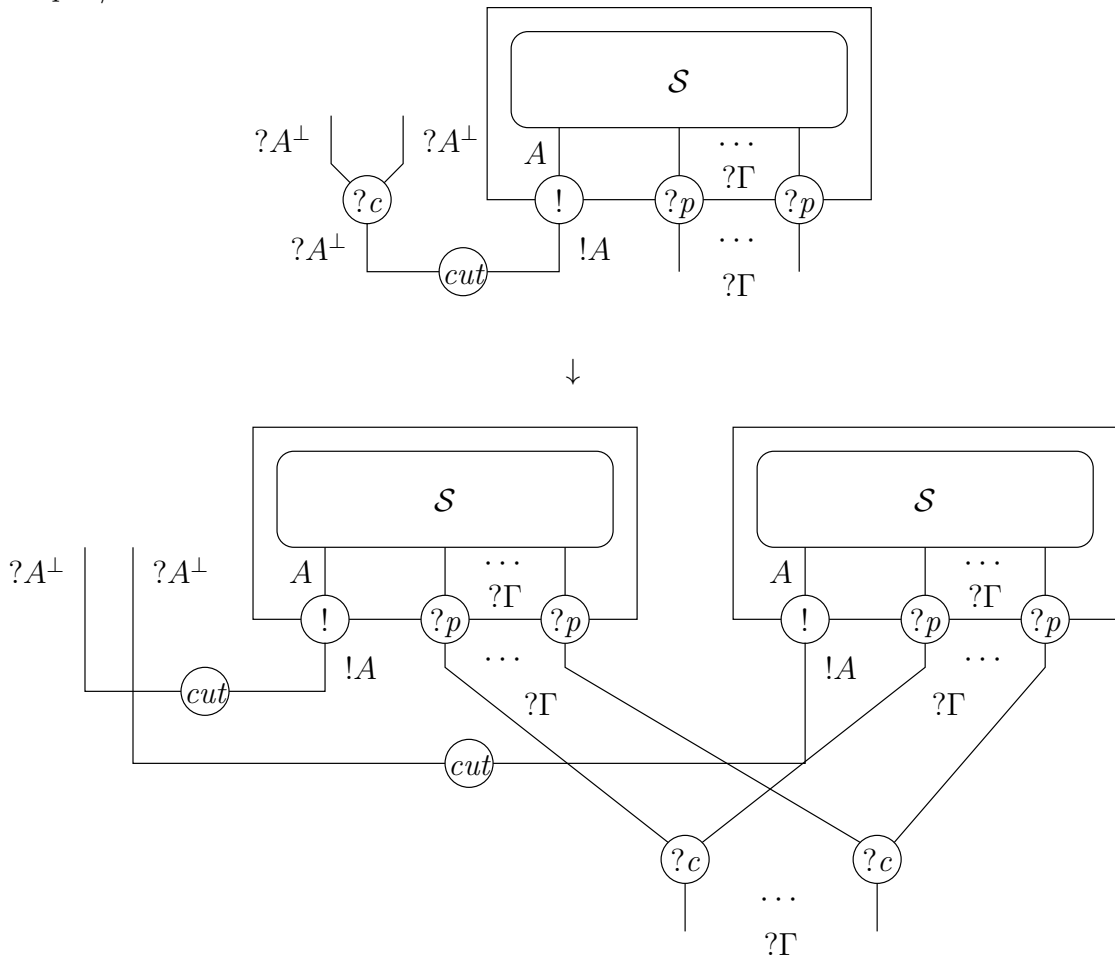
- étape $!/?d$:



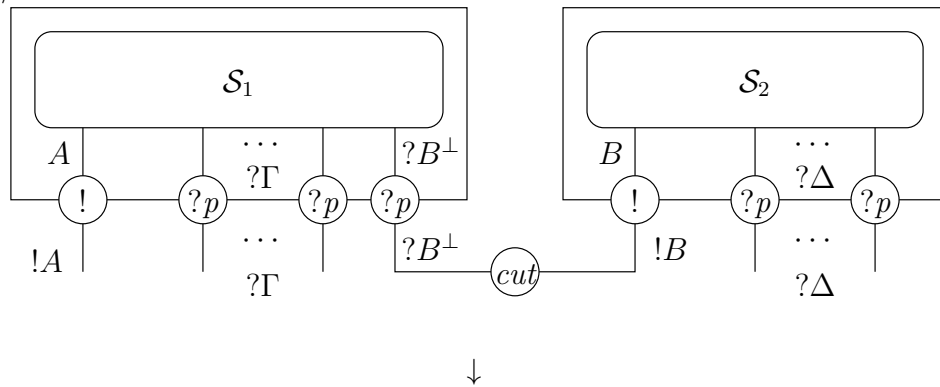
- étape $!/?w$:

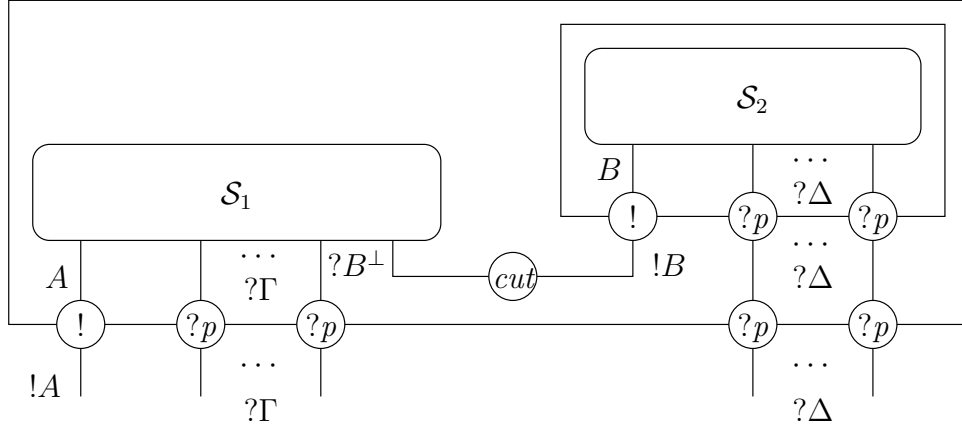


– étape !/?c :



– étape !/! :





Proposition 29 (Préservation de la correction faible par réduction)

Si la structure de preuve exponentielle faiblement correcte \mathcal{S} se réduit en \mathcal{S}' alors \mathcal{S}' est faiblement correcte.

DÉMONSTRATION : – Pour une étape $!/?d$, un graphe de correction \mathcal{G}' de \mathcal{S}' nous donne un graphe de correction \mathcal{G}_0 de \mathcal{S} à profondeur 0 et un graphe de correction \mathcal{G}_1 de \mathcal{S} à profondeur 1. Ces deux graphes sont acycliques, donc remplacer un nœud de \mathcal{G}_1 par \mathcal{G}_0 ne peut pas créer de cycle. De même, lors de cette substitution, on remplace une composante connexe (celle qui contient le nœud $!$) par autant de composantes connexes que de nœuds $?w$ plus un dans la boîte ce qui préserve l'invariant.

- Pour une étape $!/?w$, on supprime des arêtes ce qui ne peut pas créer de cycle et on remplace une composante connexe avec un nœud $?w$ par k composantes connexes avec k nœuds $?w$ ce qui préserve l'invariant.
- Pour une étape $!/?c$, soient a et b les deux prémisses du nœud $?c$. On considère un graphe de correction de \mathcal{S}' . S'il possède un cycle, on regarde la partie du cycle extérieure au module :
 - soit c'est l'intégralité du cycle et on a un cycle dans un graphe de correction de \mathcal{S} ,
 - soit elle relie deux portes auxiliaires c et d , et on a un cycle dans un graphe de correction de \mathcal{S} ,
 - soit elle relie une porte auxiliaire à a (resp. b), et en basculant le nœud $?c$ vers a (resp. b) on obtient un cycle dans un graphe de correction de \mathcal{S} ,
 - soit elle relie uniquement a et b mais ça ne peut pas donner lieu à un cycle car a et b ne sont jamais reliées à l'intérieur du module quel que soit le graphe de correction de \mathcal{S}' .

Concernant le nombre de composantes connexes, on ne change pas le nombre de nœuds $?w$ à profondeur 0. Avant réduction, le module relie toutes les conclusions des nœuds $?p$ à l'une des prémisses du nœud $?c$ alors qu'après réduction elles sont reliées soit à l'une soit à l'autre. Ceci ne peut rien changer au nombre de composantes connexes puisqu'on a vu que : les prémisses du nœud $?c$ et les portes auxiliaires de la boîte ne peuvent être reliées hors du module dans aucun graphe de correction de \mathcal{S} et deux portes auxiliaires non plus.

À l'intérieur des boîtes, on a des structures de preuve faiblement correctes.

- Pour une étape $!/!$, à profondeur 0, on remplace deux nœuds reliés par une arête par un seul nœud (non $?w$) ce qui préserve la correction faible. À profondeur 1, on ajoute un nœud (non $?w$) relié à un autre déjà présent par une arête ce qui préserve la correction faible. À profondeur 2, on retrouve une sous-structure de preuve déjà présente donc faiblement correcte. \square

Proposition 30 (Normalisation faible)

La réduction des réseaux de preuve MELL est normalisante.

DÉMONSTRATION : On appelle *coupure de type exponentiel* toute coupure dont la formule coupée est $!A/?A^\perp$. Les autres coupures sont dites *de type multiplicatif*. En particulier les coupures ax peuvent être de type soit multiplicatif soit exponentiel.

Dans un réseau, on appelle *chemin sans rebond* un chemin qui s'il arrive dans un nœud par une conclusion continue par une prémisse et réciproquement sauf pour les boîtes exponentielles où s'il arrive par la conclusion de la porte principale il repart par une conclusion de porte auxiliaire et réciproquement et s'il arrive par la prémisse de la porte principale il s'arrête (s'il arrive par une prémisse de porte auxiliaire, il continue en descendant par la conclusion). Pour les nœuds ax et cut , s'il arrive par une arête, il doit repartir par l'autre. Un tel chemin maximal (pour l'inclusion) ne peut avoir comme extrémités que une conclusion du réseau, un nœud $?w$, une conclusion de porte principale de boîte sans porte auxiliaire ou une prémisse de porte principale de boîte.

On considère un réseau sans coupure de type multiplicatif. On considère un chemin sans rebond partant d'une arête de type $?A$ en descendant. On montre par récurrence sur la longueur d'un tel chemin que toute coupure empruntée par ce chemin est empruntée de la prémisse $?$ vers la prémisse $!$: en descendant, le chemin ne peut pas passer par un nœud $!$ car il sortirait d'une boîte (or il doit s'arrêter dans ce cas), s'il arrive dans une coupure (elle est de type exponentiel par hypothèse) c'est forcément par la prémisse $?$, il remonte donc par une arête $!$ et ne peut arriver que sur une boîte ou un nœud ax et dans les deux cas il repart en descendant par une arête $?$ et on peut appliquer l'hypothèse de récurrence à la suite du chemin. De plus on va montrer qu'un tel chemin est acyclique. Remarquons tout d'abord que la profondeur n'augmente jamais le long d'un tel chemin et donc s'il y a un cycle il est à profondeur constante. Si un tel cycle existe, on considère un cycle minimal (ce qui entraîne qu'on n'arrive jamais dans un nœud par deux arêtes différentes), on a alors un cycle dans le graphe de correction qui choisit de préserver les arêtes par lesquelles passe le cycle. On peut ainsi définir un ordre partiel sur les coupures : c_1 est plus petite que c_2 si il existe un chemin sans rebond partant de la prémisse $!$ de c_1 (vers le haut) et arrivant à c_2 . On dira qu'une coupure (de type exponentiel) est *maximale* si elle est maximale pour cet ordre partiel.

La *taille de l'arbre* $?$ d'une arête de type $?$ est 0 si elle est conclusion d'un nœud ax , 1 si elle est conclusion d'un nœud $?d$ ou $?w$, 1 plus la somme des tailles des arbres $?$ des prémisses si elle est conclusion d'un nœud $?c$ et 1 plus la taille de l'arbre $?$ de l'arête à l'intérieur de la boîte si elle est porte auxiliaire de boîte.

On définit la taille d'une coupure de type multiplicatif comme $(|A|, 0)$ où A est la formule coupée et la taille d'une coupure de type exponentiel comme $(|A|, t)$ où A est la formule coupée et t est la taille de l'arbre $?$ de la prémisse $?$ de la coupure. Les tailles de coupures sont ordonnées par ordre lexicographique. La taille d'un réseau est le multi-ensemble des tailles de ses coupures.

On montre que l'on peut toujours réduire une coupure de manière à faire décroître la taille du réseau :

- S'il y a une coupure ax de type multiplicatif, on la réduit, cela supprime une coupure, ne modifie aucune formule coupée ni aucun arbre $?$.
- S'il y a une coupure \otimes/\wp , on la réduit, cela supprime une coupure, rajoute deux coupures sur des formules strictement plus petites, ne modifie pas les autres formules coupées, ni aucun arbre $?$.
- S'il n'y a pas de coupure de type multiplicatif, on choisit une coupure de type exponentiel

maximale et de profondeur maximale parmi celles-ci. On vérifie tout d'abord que dans le cas d'une coupure avec une boîte, cette boîte ne peut pas contenir de coupure. En effet si c est la coupure que l'on considère et si c' est une coupure dans la boîte : soit c' est maximale et c n'était pas de profondeur maximale, soit c' est majorée et toutes les coupures qui majorent c' sont dans la boîte, on choisit une c'' maximale parmi celles-ci, elle est maximale et c n'est pas de profondeur maximale, soit enfin c' est majorée par au moins une coupure c'' à profondeur strictement inférieure et dans ce cas c est majorée par c'' donc n'est pas maximale.

On remarque de plus que dans les différentes étapes de réduction possibles, les autres formules coupées ne sont pas modifiées et les seules arêtes $?$ modifiées sont les portes auxiliaires de boîte (ou l'autre conclusion du nœud ax) mais celles-ci ne peuvent pas faire partie de l'arbre $?$ d'une formule coupée par maximalité de la coupure réduite. Les poids des autres coupures ne sont donc pas modifiés. On considère maintenant chaque cas :

- Pour une coupure ax dont l'arête commune à l'axiome et à la coupure est $?A$, on supprime une coupure (et on ne modifie bien aucun arbre $?$ pour une raison un petit peu différente des autres cas).
- Pour une coupure ax dont l'arête commune à l'axiome et à la coupure est $!A$, on supprime une coupure.
- Pour une coupure $!/?d$, on remplace une coupure par une coupure portant sur une formule strictement plus petite.
- Pour une coupure $!/?w$, on supprime une coupure.
- Pour une coupure $!/?c$, on remplace une coupure par deux coupures portant sur la même formule mais dont la taille de l'arbre $?$ décroît strictement. On ne duplique pas de coupure puisque la boîte ne contient pas de coupure.
- Pour une coupure $!/!$, on remplace une coupure par une coupure portant sur la même formule mais dont la taille de l'arbre $?$ décroît strictement. \square

Théorème 8 (Confluence et normalisation forte)

La réduction des réseaux de preuve MELL est confluente et fortement normalisante.

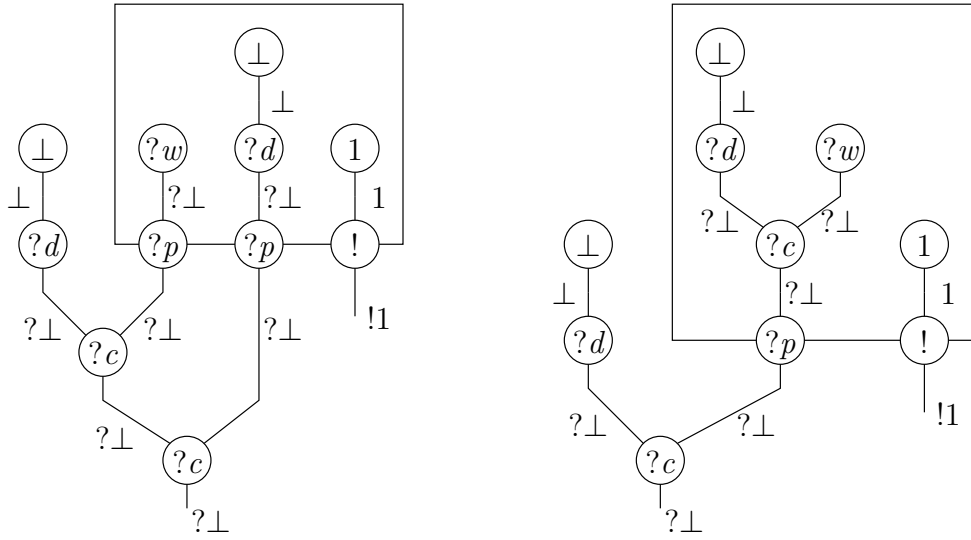
Nœuds $?$ généralisés

On peut définir une syntaxe alternative pour les réseaux de preuve de MELL utilisant des *nœuds $?$ généralisés*. Les nœuds $?d$, $?c$ et $?w$ sont remplacés par une unique famille de sortes de nœud :

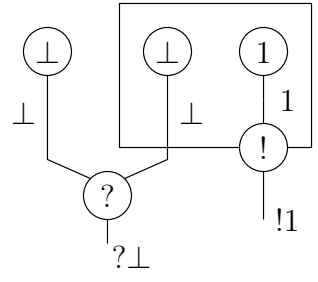
- sorte $?_i$ ($i \in \mathbb{N}$) : i prémisses, une conclusion, les i prémisses ont la même étiquette A et la conclusion a pour étiquette $?A$

Les structures de preuve exponentielles sont alors construites sur l'alphabet de nœuds $\{ax, cut, \otimes, \wp, !\} \cup \{?_i \mid i \in \mathbb{N}\}$ (dans les cas particuliers $?_0$ et $?_1$, on parlera parfois par abus de langage de nœuds de sorte $?w$ et $?d$). Les boîtes ont pour conclusion un nœud $!$ et des nœuds $?_i$ (mais tout nœud $?_i$ n'est pas nécessairement porte auxiliaire d'une boîte et un nœud $?_i$ peut être porte auxiliaire de plusieurs boîtes). On interdit de plus aux nœuds ax d'introduire des formules $!A$ et $?A$ (ainsi toute arête de type $?A$ est conclusion d'un nœud de sorte $?_i$).

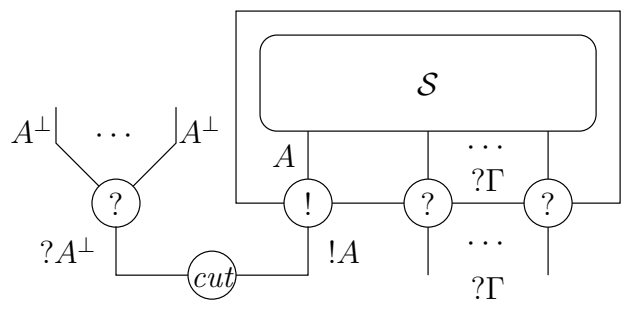
Cette syntaxe réalise un quotient par rapport à la syntaxe précédente. Les réseaux suivants :



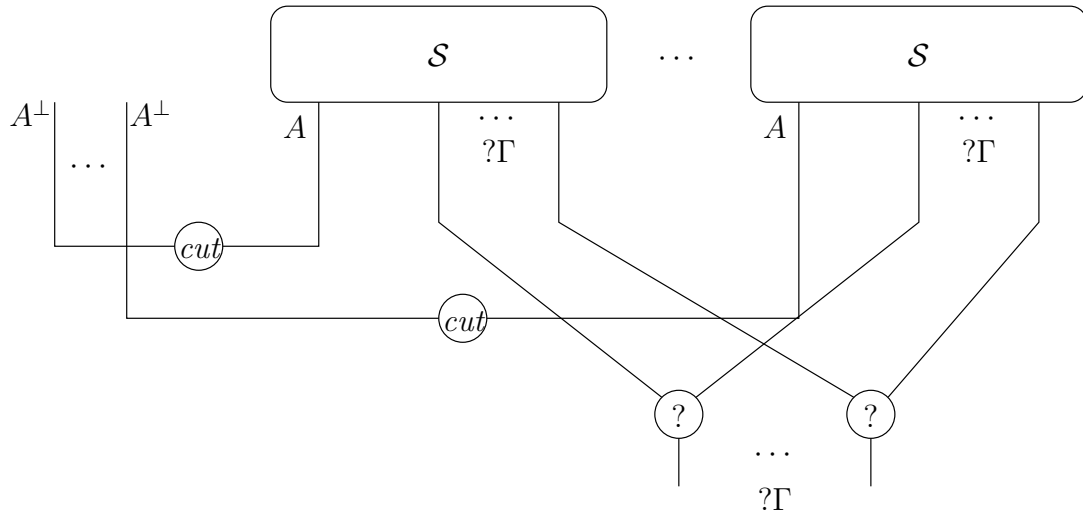
sont tous les deux représentés par :



On définit une unique étape de réduction exponentielle !/? qui regroupe les quatre de la syntaxe originelle :



↓



Il faut noter que les nœuds de sorte $?$ portes auxiliaires de la boîte peuvent également être portes auxiliaires d'autres boîtes (et toutes les arêtes prémisses de ces nœuds ne sont pas représentées). Si le nœud de sorte $?$ prémisses de la coupure est porte auxiliaire de boîtes, ceux du module réduit deviennent portes auxiliaires de ces boîtes.

6.3 Autres connecteurs

L'utilisation de boîtes permet d'intégrer les autres connecteurs aux réseaux de preuve mais n'est pas une solution satisfaisante pour l'élimination des coupures. Un des principaux enjeux de la théorie des réseaux de preuve est de trouver des solutions alternatives.

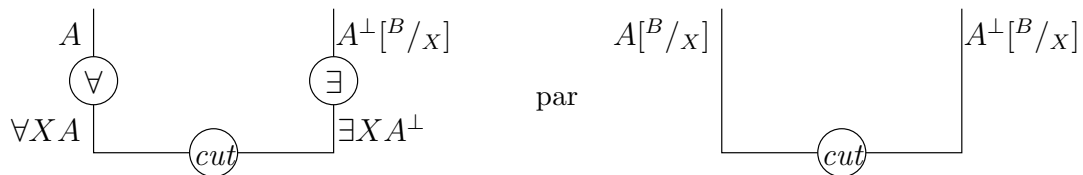
Quantificateurs

On ne donnera que quelques éléments concernant les réseaux de preuve pour les quantificateurs. En particulier on ne parlera pas de critère de correction même si un tel critère existe.

On considère les nouvelles sortes de nœuds suivantes :

- sorte \forall : une prémisses, une conclusion, si l'étiquette de la prémisses est A alors celle de la conclusion est $\forall X A$
- sorte \exists : une prémisses, une conclusion, si l'étiquette de la conclusion est $\exists X A$ alors celle de la prémisses est $A^{[B/X]}$ (où B peut être une formule quelconque)

La nouvelle étape de réduction \forall/\exists remplace le module



à condition que X ne soit pas libre dans B et effectue la substitution $[B/X]$ dans toute la structure de preuve.

Additifs

On n'abordera pas ici la question beaucoup plus complexe des réseaux de preuve avec connecteurs additifs.

Chapitre 7

Traductions des logiques intuitionniste et classique

Afin de montrer que la logique linéaire est un système suffisamment expressif, nous allons donner des traductions des logiques intuitionniste et classique dans LL.

7.1 Squelettes

Avant d'étudier les traductions dans LL, nous allons aborder rapidement la question inverse : la logique linéaire a été introduite comme un raffinement de la logique intuitionniste et de la logique classique, est-il possible d'oublier cette finesse et de retrouver une preuve classique ou intuitionniste à partir d'une preuve linéaire ?

Concrètement on définit une fonction des formules linéaires dans les formules habituelles qui oublie les distinctions introduites dans LL. On parle de *squelette* d'une formule :

$$\begin{array}{ll} \underline{X} = X & \underline{X^\perp} = \neg X \\ \underline{A \otimes B} = \underline{A} \wedge \underline{B} & \underline{A \wp B} = \underline{A} \vee \underline{B} \\ \underline{A \& B} = \underline{A} \wedge \underline{B} & \underline{A \oplus B} = \underline{A} \vee \underline{B} \\ \underline{\perp} = \text{T} & \underline{\perp} = \text{F} \\ \underline{\top} = \text{T} & \underline{0} = \text{F} \\ \underline{!A} = \underline{A} & \underline{?A} = \underline{A} \end{array}$$

et donc $\underline{A^\perp} = \neg \underline{A}$

Le squelette d'une preuve est obtenu en remplaçant toutes les formules par leur squelette. Rien ne garantit que la preuve obtenue soit une preuve valide dans un quelconque système, il faut vérifier la correction de chaque règle.

LL

Le squelette d'une preuve de LL est une preuve de LK :

- les squelettes des règles *ax* et *cut* sont les règles correspondantes de LK
- les squelettes des règles multiplicatives et additives sont les règles correspondantes de LK
- les squelettes de la prémisses et de la conclusion de la règle ! sont identiques, on obtient donc toujours une "règle" valide (et de même pour la règle ?*d*)
- les squelettes des règles ?*c* et ?*w* sont les règles *ctr* et *wk* de LK

En particulier si $\vdash \Gamma$ est prouvable dans LL, alors $\vdash \underline{\Gamma}$ est prouvable dans LK.

Exemple 11

Le squelette de la preuve de LL suivante :

$$\frac{\frac{\frac{\overline{\vdash X^\perp, X}}{ax}}{\vdash X^\perp, ?X} ?d}{\vdash X^\perp \oplus !Y, ?X} \oplus_1 \quad \frac{\frac{\overline{\vdash X^\perp, X}}{ax}}{\vdash X^\perp, ?X} ?d}{\vdash (X^\perp \oplus !Y) \otimes X^\perp, ?X} \otimes}{\vdash (X^\perp \oplus !Y) \otimes X^\perp, ?X} ?c}{\vdash ((X^\perp \oplus !Y) \otimes X^\perp) \wp ?X} \wp$$

est la preuve de LK :

$$\frac{\frac{\frac{\overline{\vdash \neg X, X}}{ax}}{\vdash \neg X \vee Y, X} \vee^{\text{add}}_1 \quad \frac{\overline{\vdash \neg X, X}}{ax}}{\vdash (\neg X \vee Y) \wedge \neg X, X, X} \wedge^{\text{mul}}}{\vdash (\neg X \vee Y) \wedge \neg X, X} \text{ctr}}{\vdash ((\neg X \vee Y) \wedge \neg X) \vee X} \vee^{\text{mul}}$$

ILL

On ajoute pour les formules :

$$\underline{A \multimap B} = \underline{A} \rightarrow \underline{B}$$

Le squelette d'une preuve de ILL est une preuve de LJ :

- les squelettes des règles *ax* et *cut* sont les règles correspondantes de LJ
- les squelettes des règles multiplicatives et additives sont les règles correspondantes de LJ
- les squelettes des règles !R et !L sont les règles triviales (prémisse et conclusion identiques)
- les squelettes des règles *ctr*L et *wk*L sont les règles correspondantes de LJ

En particulier si $\Gamma \vdash A$ est prouvable dans ILL, alors $\underline{\Gamma} \vdash \underline{A}$ est prouvable dans LJ.

Exemple 12

Le squelette de la preuve de ILL suivante :

$$\frac{\frac{\frac{\overline{X \vdash X}}{ax}}{X, !Y \vdash X} \text{wkL}}{\frac{X \vdash !Y \multimap X}{!X \vdash !Y \multimap X} !L} \multimap R}{!X \vdash Y \oplus (!Y \multimap X)} \oplus R_2$$

est la preuve de LJ :

$$\frac{\frac{\frac{\overline{X \vdash X}}{ax}}{X, Y \vdash X} \text{wkL}}{X \vdash Y \rightarrow X} \rightarrow^{\text{mul}} R}{X \vdash Y \vee (Y \rightarrow X)} \vee^{\text{add}} R_2$$

7.2 Logique intuitionniste

Traduction de Girard

Cette traduction correspond à la manière historique dont J.-Y. Girard a construit la logique linéaire à partir d'une analyse de la logique intuitionniste dans le modèle des espaces cohérents.

On traduit la logique intuitionniste dans la logique linéaire intuitionniste par :

$$\begin{aligned}
X^\bullet &= X \\
(A \rightarrow B)^\bullet &= !A^\bullet \multimap B^\bullet \\
(A \wedge B)^\bullet &= A^\bullet \& B^\bullet \\
\mathbf{T}^\bullet &= \top \\
(A \vee B)^\bullet &= !A^\bullet \oplus !B^\bullet \\
\mathbf{F}^\bullet &= 0 \\
(\Gamma \vdash A)^\bullet &= !\Gamma^\bullet \vdash A^\bullet
\end{aligned}$$

On va donner la traduction de la déduction naturelle NJ dans ILL. Puisque la traduction des séquents fait commencer toute formule à gauche par !, la traduction des règles structurales gauches est immédiate. Pour les autres règles :

$$\begin{aligned}
\frac{}{A \vdash A} ax &\rightsquigarrow \frac{\frac{}{A^\bullet \vdash A^\bullet} ax}{!A^\bullet \vdash A^\bullet} !L \\
\frac{\Gamma, A \vdash B}{\Gamma \vdash A \rightarrow B} \rightarrow_{\text{intro}} &\rightsquigarrow \frac{!\Gamma^\bullet, !A^\bullet \vdash B^\bullet}{!\Gamma^\bullet \vdash !A^\bullet \multimap B^\bullet} \multimap R \\
\frac{\Gamma \vdash A \rightarrow B \quad \Delta \vdash A}{\Gamma, \Delta \vdash B} \rightarrow_{\text{elim}} &\rightsquigarrow \frac{\frac{!\Delta^\bullet \vdash A^\bullet}{!\Delta^\bullet \vdash !A^\bullet} !R \quad \frac{}{B^\bullet \vdash B^\bullet} ax}{!\Gamma^\bullet \vdash !A^\bullet \multimap B^\bullet \quad \frac{!\Delta^\bullet, !A^\bullet \multimap B^\bullet \vdash B^\bullet}{!\Delta^\bullet, !A^\bullet \multimap B^\bullet \vdash B^\bullet} \multimap L}{!\Gamma^\bullet, !\Delta^\bullet \vdash B^\bullet} cut \\
\frac{\Gamma \vdash A \quad \Gamma \vdash B}{\Gamma \vdash A \wedge B} \wedge_{\text{intro}} &\rightsquigarrow \frac{!\Gamma^\bullet \vdash A^\bullet \quad !\Gamma^\bullet \vdash B^\bullet}{!\Gamma^\bullet \vdash A^\bullet \& B^\bullet} \&R \\
\frac{\Gamma \vdash A \wedge B}{\Gamma \vdash A} \wedge_{\text{elim1}} &\rightsquigarrow \frac{\frac{}{A^\bullet \vdash A^\bullet} ax}{A^\bullet \& B^\bullet \vdash A^\bullet} \&L_1}{!\Gamma^\bullet \vdash A^\bullet \& B^\bullet} cut \\
\frac{\Gamma \vdash A \wedge B}{\Gamma \vdash B} \wedge_{\text{elim2}} &\rightsquigarrow \frac{\frac{}{B^\bullet \vdash B^\bullet} ax}{A^\bullet \& B^\bullet \vdash B^\bullet} \&L_2}{!\Gamma^\bullet \vdash A^\bullet \& B^\bullet} cut \\
\frac{}{\Gamma \vdash \mathbf{T}} \mathbf{T}_{\text{intro}} &\rightsquigarrow \frac{}{!\Gamma^\bullet \vdash \top} \top R \\
\frac{\Gamma \vdash A}{\Gamma \vdash A \vee B} \vee_{\text{intro1}} &\rightsquigarrow \frac{\frac{!\Gamma^\bullet \vdash A^\bullet}{!\Gamma^\bullet \vdash !A^\bullet} !}{!\Gamma^\bullet \vdash !A^\bullet \oplus !B^\bullet} \oplus R_1 \\
\frac{\Gamma \vdash B}{\Gamma \vdash A \vee B} \vee_{\text{intro2}} &\rightsquigarrow \frac{\frac{!\Gamma^\bullet \vdash B^\bullet}{!\Gamma^\bullet \vdash !B^\bullet} !}{!\Gamma^\bullet \vdash !A^\bullet \oplus !B^\bullet} \oplus R_2
\end{aligned}$$

$$\begin{array}{c}
\frac{\Gamma \vdash A \vee B \quad \Delta, A \vdash C \quad \Delta, B \vdash C}{\Gamma, \Delta \vdash C} \vee_{\text{elim}} \quad \rightsquigarrow \quad \frac{\frac{\frac{! \Delta^\bullet, !A^\bullet \vdash C^\bullet \quad ! \Delta^\bullet, !B^\bullet \vdash C^\bullet}{! \Delta^\bullet, !A^\bullet \oplus !B^\bullet \vdash C^\bullet} \oplus L}{! \Gamma^\bullet, ! \Delta^\bullet \vdash C^\bullet} \text{cut}}{! \Gamma^\bullet \vdash !A^\bullet \oplus !B^\bullet} \\
\\
\frac{\Gamma \vdash F}{\Gamma \vdash C} F_{\text{elim}} \quad \rightsquigarrow \quad \frac{! \Gamma^\bullet \vdash 0 \quad \overline{0 \vdash C^\bullet}}{! \Gamma^\bullet \vdash C^\bullet} 0L \text{cut}
\end{array}$$

Proposition 31 (Équiprouvabilité)

A est prouvable en logique intuitionniste si et seulement si A^\bullet est prouvable en logique linéaire intuitionniste.

DÉMONSTRATION : La traduction transforme toute dérivation de $\vdash A$ dans NJ en une dérivation de $\vdash A^\bullet$ dans ILL. Réciproquement, partant d'une preuve de $\vdash A^\bullet$ dans ILL, son squelette est une dérivation de $\vdash A$ dans LJ car $\underline{A^\bullet} = A$. \square

Concernant le lien avec LL, clairement si A est prouvable intuitionnistiquement, A^\bullet est prouvable dans LL. La réciproque est également claire en l'absence de T et F (donc de 0 et \top) car dans ce cas la prouvabilité dans LL d'une formule linéaire intuitionniste entraîne sa prouvabilité dans ILL (voir [section 5.3](#)). En présence de T et F, ce résultat reste en fait correct.

Seconde traduction de Girard

On va se restreindre ici au cas du connecteur \rightarrow même si cette traduction peut s'étendre aux autres connecteurs :

$$\begin{aligned}
X^\bullet &= !X \\
(A \rightarrow B)^\bullet &= !(A^\bullet \multimap B^\bullet) \\
(\Gamma \vdash A)^\bullet &= \Gamma^\bullet \vdash A^\bullet
\end{aligned}$$

On va donner la traduction de la déduction naturelle NJ dans ILL. Puisque la traduction de toute formule commence par !, la traduction des règles structurelles gauches est immédiate. Pour les autres règles :

$$\begin{array}{c}
\frac{}{A \vdash A} ax \quad \rightsquigarrow \quad \frac{}{A^\bullet \vdash A^\bullet} ax \\
\\
\frac{\Gamma, A \vdash B}{\Gamma \vdash A \rightarrow B} \rightarrow_{\text{intro}} \quad \rightsquigarrow \quad \frac{\frac{\Gamma^\bullet, A^\bullet \vdash B^\bullet}{\Gamma^\bullet \vdash A^\bullet \multimap B^\bullet} \multimap R}{\Gamma^\bullet \vdash !(A^\bullet \multimap B^\bullet)} !R \\
\\
\frac{\Gamma \vdash A \rightarrow B \quad \Delta \vdash A}{\Gamma, \Delta \vdash B} \rightarrow_{\text{elim}} \quad \rightsquigarrow \quad \frac{\frac{\frac{\Delta^\bullet \vdash A^\bullet \quad \overline{B^\bullet \vdash B^\bullet}}{\Delta^\bullet, A^\bullet \multimap B^\bullet \vdash B^\bullet} \multimap L}{\Gamma^\bullet \vdash !(A^\bullet \multimap B^\bullet)} !L}{\Gamma^\bullet, \Delta^\bullet \vdash B^\bullet} \text{cut}
\end{array}$$

Comme pour la traduction précédente, A est intuitionnistiquement prouvable si et seulement si A^\bullet est prouvable dans ILL (et, en l'absence de 0 et \top , si et seulement si A^\bullet est prouvable dans LL).

Traduction du λ -calcul dans les réseaux

Les deux traductions que l'on a données n'ont été présentées que pour ce qui concerne la prouvabilité (aspects statiques). Afin de parler des aspects dynamiques (simulation de la réduction par l'élimination des coupures), nous allons reprendre la première traduction de Girard comme une traduction du λ -calcul pur dans une version pure des réseaux de preuve exponentiels.

On peut utiliser les réseaux de preuve dans un cadre non typé (ceci concerne les deux syntaxes que l'on a décrites pour MELL mais on va ici se concentrer sur celle avec ? généralisés). Il s'agit de restreindre les types à ceux nécessaires pour traduire le connecteur \rightarrow de la logique intuitionniste et de les quotienter par la traduction de l'équation $o \rightarrow o = o$ (qui définit le λ -calcul pur à partir du λ -calcul simplement typé). Ceci modifie les types des sortes de nœuds :

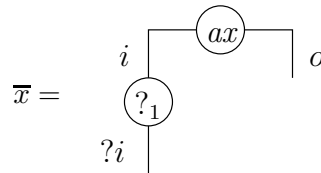
- sorte ax : aucune prémisses, deux conclusions, les étiquettes des conclusions sont o et i
- sorte cut : deux prémisses, aucune conclusion, si l'étiquette de la première prémisses est A alors celle de la deuxième est A^\perp
- sorte \otimes : deux prémisses, une conclusion, l'étiquette de la première prémisses est $!o$, celle de la deuxième prémisses est i et celle de la conclusion est i
- sorte \wp : deux prémisses, une conclusion, l'étiquette de la première prémisses est $?i$, celle de la deuxième prémisses est o et celle de la conclusion est o
- sorte $!$: une prémisses, une conclusion, l'étiquette de la prémisses est o et celle de la conclusion est $!o$
- sorte $?_k$ ($k \in \mathbb{N}$) : k prémisses, une conclusion, les prémisses ont toutes l'étiquette i et la conclusion a pour étiquette $?i$ (on utilisera la notation $?$ quand on ne voudra pas préciser k)

au lieu d'un ensemble de formules, on n'utilise que quatre types pour les arêtes : i , o , $?i$ et $!o$ (avec sous-entendu : $?i \wp o = o$ et $!o \otimes i = i$). De plus, on considère ici les réseaux de preuve à l'ordre des prémisses de nœuds de sorte $?_k$ près.

Comme dans le cas typé, les boîtes ont pour conclusion un nœud de sorte $!$ et des nœuds de sorte $?_k$ (mais tout nœud $?_k$ n'est pas nécessairement porte auxiliaire d'une boîte et un nœud $?_k$ peut être porte auxiliaire de plusieurs boîtes).

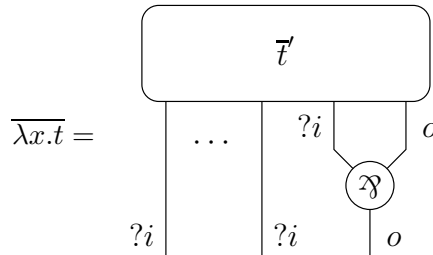
En utilisant la première traduction de Girard, on peut traduire tout λ -terme en un réseau de MELL. On va ici retravailler cette traduction dans le cas pur. On traduit un λ -terme par un réseau sans coupure multiplicative et ayant une conclusion o et autant de conclusions $?i$ qu'il y a de variables libres dans le λ -terme.

- variable :



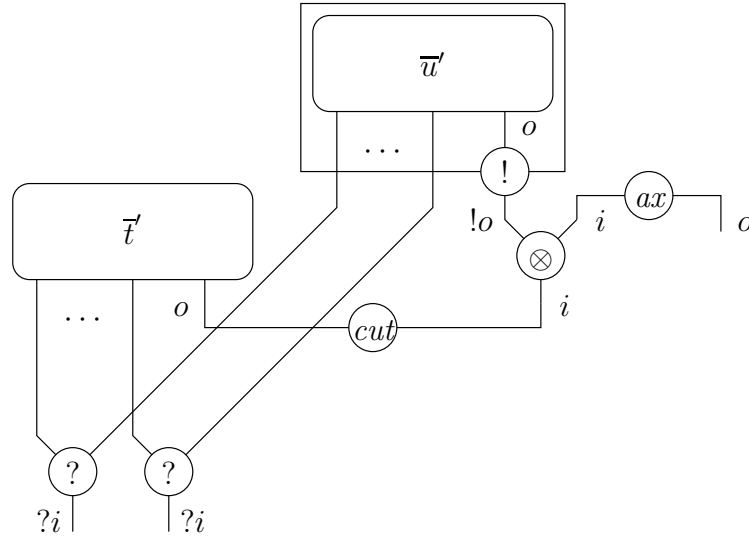
- abstraction :

On note \bar{t}' le réseau obtenu à partir de \bar{t} en ajoutant un nœud de sorte $?_0$ si x n'est pas libre dans t .



- application :

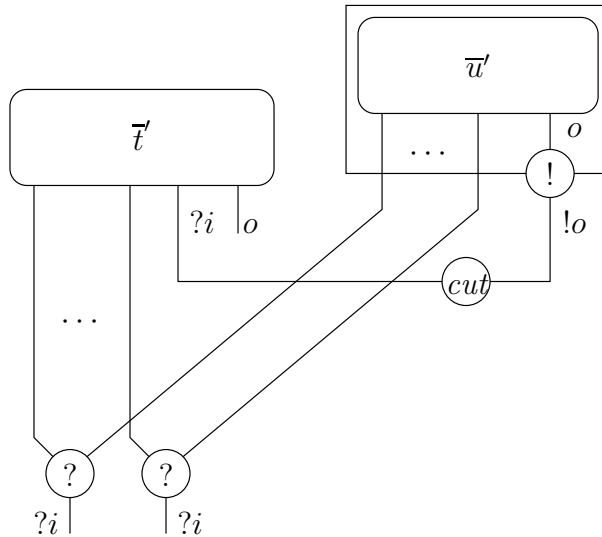
Soit \bar{t}' (resp. \bar{u}') le réseau obtenu en ajoutant à \bar{t} (resp. \bar{u}) des nœuds de sorte $?_0$ pour chaque variable libre de u (resp. t) qui n'est pas libre dans t (resp. u). Pour obtenir $(\bar{t})u$, on considère le réseau suivant :



dans lequel on identifie deux par deux les nœuds $?$ de \bar{t}' et de \bar{u}' introduisant les $?i$: les conclusions $?i$ de \bar{t}' et de \bar{u}' sont toutes conclusions de nœuds $?$ et correspondent chacune à une variable libre de t ou u , pour chaque variable libre de t ou u on remplace les deux nœuds $?$ correspondants par un seul ayant comme prémisses toutes celles des deux nœuds d'origine. Ce réseau contient une coupure multiplicative que l'on réduit (par une étape \otimes/\wp puis par une étape ax si t est une λ -abstraction et par une étape ax seulement sinon).

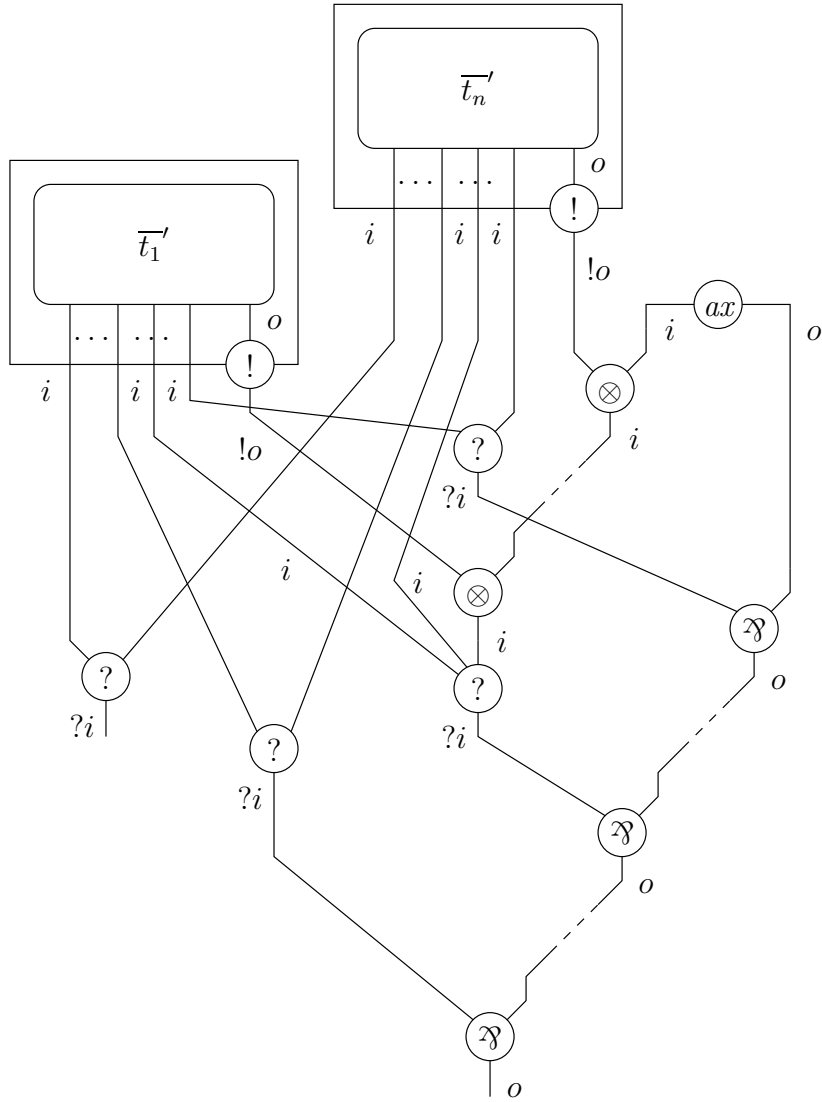
Cette traduction a la propriété que \bar{t} contient une coupure si et seulement si t contient un rédex.

DÉMONSTRATION : On vérifie facilement que la traduction d'un rédex $(\lambda x.t)u$ est le réseau :



qui contient une coupure.

Si t ne contient pas de rédex, c'est une forme normale $t = \lambda \vec{y}.(x)t_1 \dots t_n$ avec t_1, \dots, t_n eux-mêmes en forme normale. On montre par récurrence sur la taille de t que sa traduction ne contient pas de coupure : par hypothèse de récurrence, c'est le cas pour les traductions de t_1, \dots, t_n et celle de t est obtenue par :

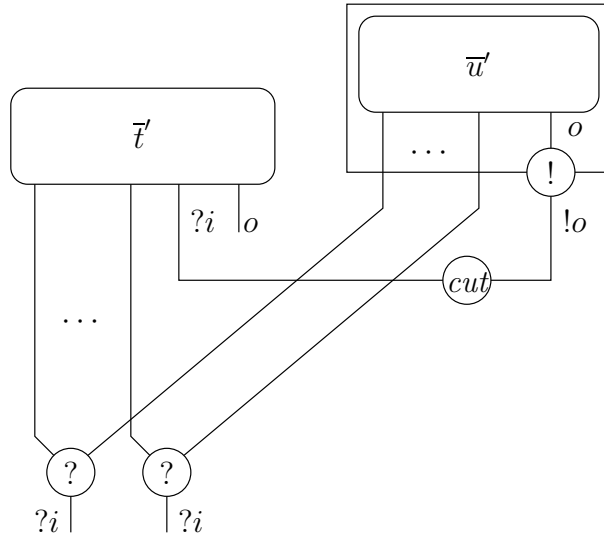


et ne contient pas de coupure.

□

Lemme 17 (Substitution)

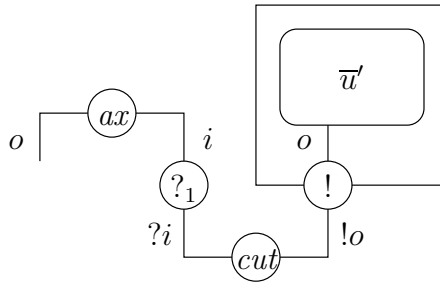
Le réseau $(\lambda x.t)u$:



se réduit en au moins une étape en $\overline{t[u/x]}$ auquel on ajoute des nœuds de sorte $?_0$ pour chaque variable libre de u qui a disparu dans la réduction.

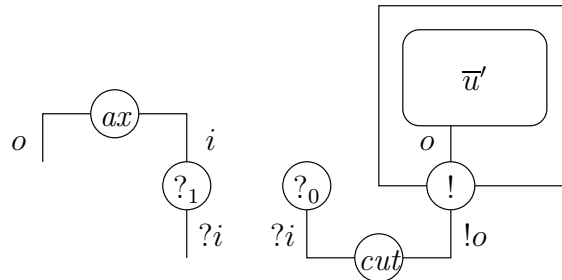
DÉMONSTRATION : Par récurrence sur t , en montrant de plus que la réduction en question commence par réduire la coupure exponentielle entre \overline{t} et \overline{u} : (pour rendre les dessins plus lisibles dans cette preuve, on ne représentera pas les contextes inutiles des réseaux)

– Si $t = x$, on obtient le réseau :



qui se réduit en deux étapes en \overline{u} .

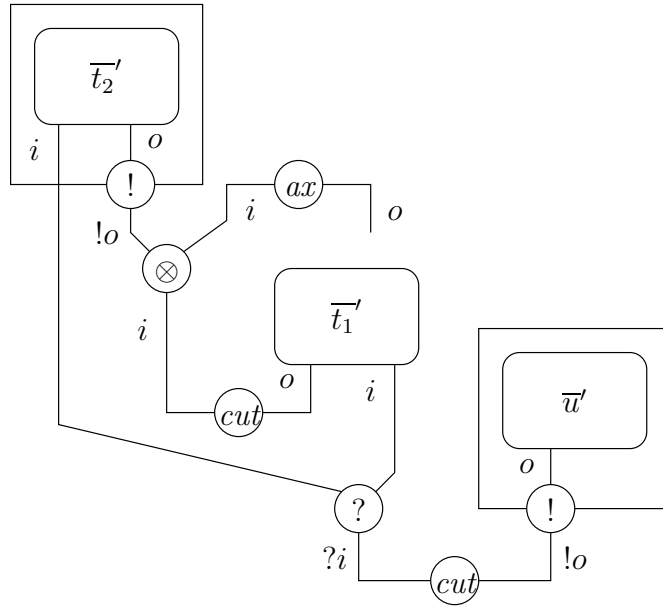
– Si $t = y \neq x$, on obtient le réseau :



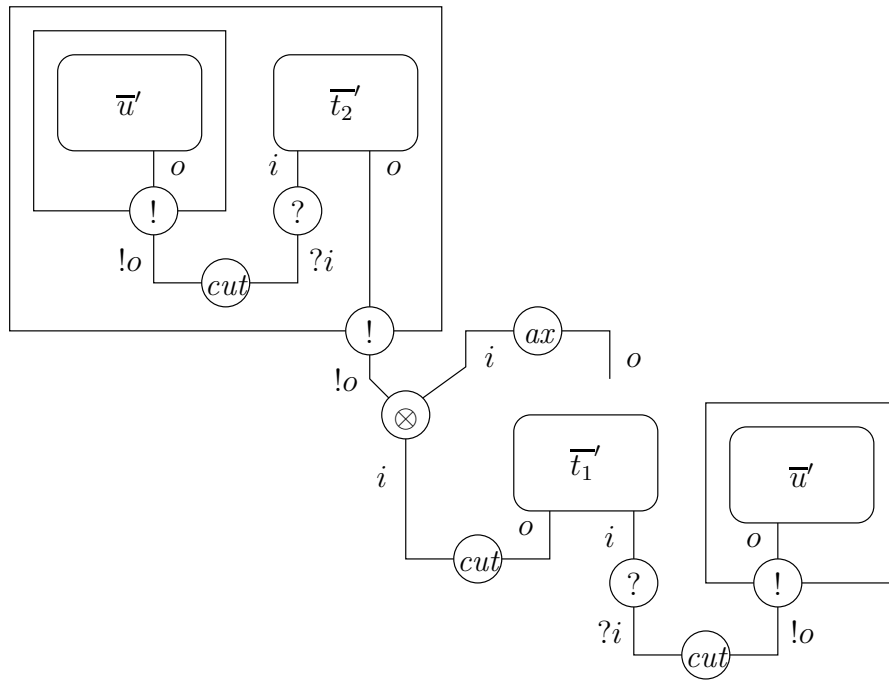
dans lequel, si y est libre dans u , le nœud $?$ correspondant est identifié avec le nœud de sorte $?_1$. Par une étape de réduction, on obtient \overline{y} avec des nœuds de sorte $?_0$ pour les variables libres de u différentes de y .

– Si $t = \lambda y.t_1$, on applique l'hypothèse de récurrence à t_1 . On vérifie que, puisque $y \notin u$, le nœud de sorte $?_0$ correspondant à y ajouté à u dans la traduction de $(\lambda x.t_1)u$ disparaît quand on traduit le λy .

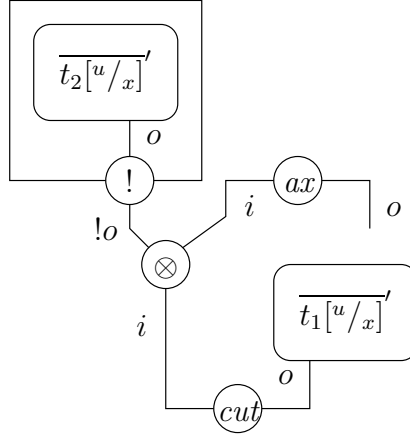
– Si $t = (t_1)t_2$, on considère le réseau \mathcal{R} suivant :



qui se réduit en $\overline{(\lambda x.(t_1)t_2)u}$. Considérons également le réseau \mathcal{R}' suivant :



par hypothèse de récurrence, il se réduit en :



qui se réduit par définition de la traduction en $\overline{(t_1[u/x])t_2[u/x]}$. Or \mathcal{R} et \mathcal{R}' donnent le même réseau après la réduction de la coupure de \mathcal{R} et des deux coupures de \mathcal{R}' (qui ont bien été réduites lors de l'application de l'hypothèse de récurrence) donc \mathcal{R} se réduit (en au moins une étape) en $\overline{(t_1[u/x])t_2[u/x]}$. En faisant commuter la réduction multiplicative et la réduction exponentielle, on en déduit que $\overline{(\lambda x.(t_1)t_2)u}$ se réduit en au moins une étape en $\overline{(t_1)t_2[u/x]}$ (avec les nœuds de sorte $?_0$ nécessaires). \square

Proposition 32 (Simulation)

Si t se réduit en t' alors \bar{t} se réduit en au moins une étape en \bar{t}' (à des nœuds de sorte $?_0$ terminaux près).

DÉMONSTRATION : Si le rédex correspond à une coupure à profondeur 0, il suffit d'appliquer le lemme 17. Sinon, à la profondeur où se trouve la coupure associée au rédex, on ajoute des nœuds de sorte $?_0$, mais par définition de la syntaxe avec nœuds $?$ généralisés, ces nœuds de sorte $?_0$ sortent des boîtes et, soit sont absorbés par un autre nœud $?$ et disparaissent, soit sont terminaux. \square

On en déduit que la normalisation forte des réseaux MELL implique celle du λ -calcul simplement typé puisque la traduction s'étend naturellement au typage et traduit un λ -terme simplement typé en un réseau typé dans MELL.

Remarque : On peut également donner la traduction (et montrer la simulation) dans le cas du λ -calcul simplement typé additif ce qui simplifie les choses et fait disparaître les questions de nœuds de sorte $?_0$ terminaux.

7.3 Logique classique

Par ajout de connecteurs exponentiels, on peut transformer les deux traductions de Girard pour la logique intuitionniste en traductions de la logique classique (on choisit ici NK) dans LL.

On se restreint au connecteur \rightarrow même si ces traductions peuvent s'étendre aux autres connecteurs.

La t-traduction

$$\begin{aligned}
 X^\bullet &= X \\
 (A \rightarrow B)^\bullet &= ?!A^{\bullet\perp} \wp ?B^\bullet \\
 (\Gamma \vdash \Delta)^\bullet &= \vdash ?!\Gamma^{\bullet\perp}, ?\Delta^\bullet
 \end{aligned}$$

Puisque la traduction des séquents fait commencer toute formule par ?, la traduction des règles structurelles est immédiate. Pour les autres règles :

$$\begin{array}{c}
\frac{}{A \vdash A} \text{ax} \quad \rightsquigarrow \quad \frac{}{\vdash !A^{\bullet\perp}, ?A^{\bullet}} \text{ax} \\
\frac{\Gamma, A \vdash B, \Delta}{\Gamma \vdash A \rightarrow B, \Delta} \rightarrow_{\text{intro}} \quad \rightsquigarrow \quad \frac{\vdash ?!\Gamma^{\bullet\perp}, ?!A^{\bullet\perp}, ?B^{\bullet}, ?\Delta^{\bullet}}{\vdash ?!\Gamma^{\bullet\perp}, ?!A^{\bullet\perp} \wp ?B^{\bullet}, ?\Delta^{\bullet}} \wp \\
\frac{\Gamma \vdash A \rightarrow B, \Delta \quad \Gamma' \vdash A, \Delta'}{\Gamma, \Gamma' \vdash B, \Delta, \Delta'} \rightarrow_{\text{elim}} \quad \rightsquigarrow \quad \frac{\vdash ?!\Gamma'^{\bullet\perp}, ?A^{\bullet}, ?\Delta'^{\bullet}}{\vdash ?!\Gamma'^{\bullet\perp}, !?A^{\bullet}, ?\Delta'^{\bullet}} ! \quad \frac{}{\vdash !B^{\bullet\perp}, ?B^{\bullet}} \text{ax} \\
\frac{\vdash ?!\Gamma^{\bullet\perp}, ?(!A^{\bullet\perp} \wp ?B^{\bullet}), ?\Delta^{\bullet}}{\vdash ?!\Gamma^{\bullet\perp}, ?(!A^{\bullet\perp} \wp ?B^{\bullet}), ?\Delta^{\bullet}} \quad \frac{\vdash ?!\Gamma'^{\bullet\perp}, !?A^{\bullet} \otimes !B^{\bullet\perp}, ?B^{\bullet}, ?\Delta'^{\bullet}}{\vdash ?!\Gamma'^{\bullet\perp}, !(?!A^{\bullet} \otimes !B^{\bullet\perp}), ?B^{\bullet}, ?\Delta'^{\bullet}} !}{\vdash ?!\Gamma^{\bullet\perp}, ?!\Gamma'^{\bullet\perp}, ?B^{\bullet}, ?\Delta^{\bullet}, ?\Delta'^{\bullet}} \text{cut} \otimes
\end{array}$$

On montre ainsi que si $\vdash A$ est prouvable dans NK, alors $\vdash ?A^{\bullet}$ est prouvable dans LL. Réciproquement, si $\vdash ?A^{\bullet}$ est prouvable dans LL, alors $\vdash A$ est prouvable dans LK (donc dans NK) car il suffit de considérer le squelette de la preuve (puisque $\underline{?A^{\bullet}} = A$).

La q-traduction

$$\begin{aligned}
X^{\bullet} &= !X \\
(A \rightarrow B)^{\bullet} &= !(A^{\bullet\perp} \wp ?B^{\bullet}) \\
(\Gamma \vdash \Delta)^{\bullet} &= \vdash \Gamma^{\bullet\perp}, ?\Delta^{\bullet}
\end{aligned}$$

Puisque la traduction des séquents et des formules fait commencer toute formule par ?, la

traduction des règles structurelles est immédiate. Pour les autres règles :

$$\begin{array}{c}
\frac{}{A \vdash A} ax \quad \rightsquigarrow \quad \frac{}{\vdash A^{\star\perp}, A^{\star}} ax \\
\frac{}{\vdash A^{\star\perp}, ?A^{\star}} ?d \\
\\
\frac{\Gamma, A \vdash B, \Delta}{\Gamma \vdash A \rightarrow B, \Delta} \rightarrow_{\text{intro}} \quad \rightsquigarrow \quad \frac{\frac{\vdash \Gamma^{\star\perp}, A^{\star\perp}, ?B^{\star}, ?\Delta^{\star}}{\vdash \Gamma^{\star\perp}, A^{\star\perp} \wp ?B^{\star}, ?\Delta^{\star}} \wp}{\frac{\vdash \Gamma^{\star\perp}, !(A^{\star\perp} \wp ?B^{\star}), ?\Delta^{\star}}{\vdash \Gamma^{\star\perp}, !(A^{\star\perp} \wp ?B^{\star}), ?\Delta^{\star}} !} ?d \\
\\
\frac{\Gamma \vdash A \rightarrow B, \Delta \quad \Gamma' \vdash A, \Delta'}{\Gamma, \Gamma' \vdash B, \Delta, \Delta'} \rightarrow_{\text{elim}} \quad \rightsquigarrow \quad \frac{\frac{\frac{\frac{\frac{\vdash \Gamma^{\star\perp}, A^{\star}}{\vdash A^{\star\perp}, A^{\star}} ax \quad \frac{\vdash !B^{\star\perp}, ?B^{\star}}{\vdash !B^{\star\perp}, ?B^{\star}} ax}{\vdash A^{\star\perp}, A^{\star} \otimes !B^{\star\perp}, ?B^{\star}} \otimes}{\vdash A^{\star\perp}, ?(A^{\star} \otimes !B^{\star\perp}), ?B^{\star}} ?d}{\vdash \Gamma'^{\star\perp}, ?A^{\star}, ?\Delta'^{\star} \quad \frac{\vdash !A^{\star\perp}, ?(A^{\star} \otimes !B^{\star\perp}), ?B^{\star}}{\vdash !A^{\star\perp}, ?(A^{\star} \otimes !B^{\star\perp}), ?B^{\star}} !} cut}{\frac{\vdash \Gamma'^{\star\perp}, ?(A^{\star} \otimes !B^{\star\perp}), ?B^{\star}, ?\Delta'^{\star}}{\vdash \Gamma'^{\star\perp}, !(A^{\star} \otimes !B^{\star\perp}), ?B^{\star}, ?\Delta'^{\star}} !} cut} cut \\
\frac{\vdash \Gamma^{\star\perp}, !(A^{\star\perp} \wp ?B^{\star}), ?\Delta^{\star} \quad \frac{\vdash \Gamma'^{\star\perp}, ?(A^{\star} \otimes !B^{\star\perp}), ?B^{\star}, ?\Delta'^{\star}}{\vdash \Gamma'^{\star\perp}, !(A^{\star} \otimes !B^{\star\perp}), ?B^{\star}, ?\Delta'^{\star}} !} cut}{\vdash \Gamma^{\star\perp}, \Gamma'^{\star\perp}, ?B^{\star}, ?\Delta^{\star}, ?\Delta'^{\star}} cut
\end{array}$$

On montre ainsi que si $\vdash A$ est prouvable dans NK, alors $\vdash ?A^{\star}$ est prouvable dans LL. Réciproquement, si $\vdash ?A^{\star}$ est prouvable dans LL, alors $\vdash A$ est prouvable dans LK (donc dans NK) car il suffit de considérer le squelette de la preuve (puisque $\underline{?A^{\star}} = A$).

Chapitre 8

Modèles

8.1 Sémantique catégorique

Catégories de Seely

On va continuer l'introduction de notions catégoriques commencée au [chapitre 4](#) pour donner les structures qui permettent de définir les modèles de la logique linéaire.

Définition 35 (Foncteur monoïdal)

Étant données deux catégories monoïdales $(\mathbb{C}, \otimes, 1, (assoc_{A,B,C}^\otimes)_{(A,B,C) \in \mathbb{C}^3}, (unit_A^{l\otimes})_{A \in \mathbb{C}}, (unit_A^{r\otimes})_{A \in \mathbb{C}})$ et $(\mathbb{D}, \boxtimes, I, (assoc_{A',B',C'}^{\boxtimes})_{(A',B',C') \in \mathbb{D}^3}, (unit_{A'}^{l\boxtimes})_{A' \in \mathbb{D}}, (unit_{A'}^{r\boxtimes})_{A' \in \mathbb{D}})$, on dit que $(F, (m_{A,B})_{(A,B) \in \mathbb{C}}, n)$ est un *foncteur monoïdal* de \mathbb{C} dans \mathbb{D} si :

- F est un foncteur de \mathbb{C} dans \mathbb{D} ,
- $(m_{A,B})_{(A,B) \in \mathbb{C}}$ est une transformation naturelle de $F(-) \boxtimes F(-)$ dans $F(- \otimes -)$,
- n est un morphisme de \mathbb{D} de I dans $F(1)$
- les diagrammes suivants commutent :

$$\begin{array}{ccc}
 (F(A) \boxtimes F(B)) \boxtimes F(C) & \xrightarrow{assoc_{F(A),F(B),F(C)}^{\boxtimes}} & F(A) \boxtimes (F(B) \boxtimes F(C)) \\
 \downarrow m_{A,B} \boxtimes F(C) & & \downarrow F(A) \boxtimes m_{B,C} \\
 F(A \otimes B) \boxtimes F(C) & & F(A) \boxtimes F(B \otimes C) \\
 \downarrow m_{A \otimes B, C} & & \downarrow m_{A, B \otimes C} \\
 F((A \otimes B) \otimes C) & \xrightarrow{F(assoc_{A,B,C}^\otimes)} & F(A \otimes (B \otimes C))
 \end{array}$$

$$\begin{array}{ccc}
 F(A) & \xrightarrow{unit_{F(A)}^{\boxtimes}} & F(A) \boxtimes I \\
 \searrow F(unit_A^{l\otimes}) & & \downarrow F(A) \boxtimes n \\
 & & F(A) \boxtimes F(1) \\
 & & \downarrow m_{A,1} \\
 & & F(A \otimes 1)
 \end{array}
 \qquad
 \begin{array}{ccc}
 F(A) & \xrightarrow{unit_{F(A)}^{r\boxtimes}} & I \boxtimes F(A) \\
 \searrow F(unit_A^{r\otimes}) & & \downarrow n \boxtimes F(A) \\
 & & F(1) \boxtimes F(A) \\
 & & \downarrow m_{1,A} \\
 & & F(1 \otimes A)
 \end{array}$$

Si \mathbb{C} et \mathbb{D} sont monoïdales symétriques avec comme symétries $(\gamma_{A,B}^\otimes)_{(A,B) \in \mathbb{C}^2}$ et $(\gamma_{A',B'}^{\boxtimes})_{(A',B') \in \mathbb{D}^2}$,

on dit qu'il s'agit d'un foncteur monoïdal *symétrique* si le diagramme suivant commute :

$$\begin{array}{ccc} F(A) \boxtimes F(B) & \xrightarrow{\gamma_{F(A),F(B)}^{\boxtimes}} & F(B) \boxtimes F(A) \\ m_{A,B} \downarrow & & \downarrow m_{B,A} \\ F(A \otimes B) & \xrightarrow{F(\gamma_{A,B}^{\otimes})} & F(B \otimes A) \end{array}$$

Si $(m_{A,B})_{(A,B) \in \mathbb{C}}$ et n sont des isomorphismes, on dit qu'il s'agit d'un foncteur monoïdal *fort* (si ce sont des égalités, on parle de foncteur monoïdal *strict*).

Définition 36 (Catégorie monoïdale symétrique fermée)

Soit $(\mathbb{C}, \otimes, 1, (assoc_{A,B,C}^{\otimes})_{(A,B,C) \in \mathbb{C}^3}, (unit_A^l)^{\otimes})_{A \in \mathbb{C}}, (unit_A^r)^{\otimes})_{A \in \mathbb{C}}, (\gamma_{A,B}^{\otimes})_{(A,B) \in \mathbb{C}^2}$ une catégorie monoïdale symétrique, on dit qu'elle est *monoïdale symétrique fermée* si, pour chaque objet A , le foncteur $_ \otimes A$ de \mathbb{C} dans \mathbb{C} a un adjoint à droite que l'on note $A \multimap _$ (appelé *exponentiation monoïdale*). On note *curry* cette adjonction.

Remarque : En particulier, toute catégorie cartésienne fermée est une catégorie monoïdale symétrique fermée.

Dans une catégorie monoïdale symétrique fermée, on peut définir les morphismes suivants :

$$ev_{A,B} : (A \multimap B) \otimes A \longrightarrow B = curry^{-1}(id_{A \multimap B})$$

Proposition 33 (Bifoncteur flèche)

$(A \multimap _)_{A \in \mathbb{C}}$ s'étend en un bifoncteur $_ \multimap _$ de \mathbb{C}^{op} et \mathbb{C} dans \mathbb{C} .

DÉMONSTRATION : C'est en fait ce que l'on a prouvé dans la [proposition 19](#). On n'a pas utilisé le fait que la catégorie était cartésienne fermée mais uniquement le fait plus général qu'elle était monoïdale symétrique fermée. \square

Les catégories monoïdales symétriques fermées définissent les modèles de la logique linéaire intuitionniste multiplicative (IMLL). Une telle catégorie qui est de plus cartésienne, co-cartésienne ou les deux permet d'interpréter IMLL avec $(\&, \top)$, avec $(\oplus, 0)$ ou tout IMALL.

Définition 37 (Catégorie \star -autonome)

Une catégorie monoïdale symétrique fermée est \star -autonome si elle possède un *objet dualisant* \perp , c'est-à-dire un objet \perp tel que pour tout objet A , le morphisme $curry(\gamma_{A,A \multimap \perp}^{\otimes}; ev_{A,\perp}) : A \longrightarrow (A \multimap \perp) \multimap \perp$ est un isomorphisme.

Dans une catégorie \star -autonome, on notera souvent A^\perp pour $A \multimap \perp$. En utilisant que la famille $(curry(\gamma_{A,A \multimap \perp}^{\otimes}; ev_{A,\perp}))_{A \in \mathbb{C}}$ est un isomorphisme naturel du foncteur id dans le foncteur $(_)^\perp$, on peut définir le bifoncteur \wp avec $A \wp B = (A^\perp \otimes B^\perp)^\perp \simeq A^\perp \multimap B \simeq B^\perp \multimap A$. On montre par ailleurs que $1 \simeq \perp^\perp$.

Les catégories \star -autonomes fournissent les modèles de MLL, et les catégories \star -autonomes cartésiennes fournissent les modèles de MALL.

Définition 38 (Monade)

Soit \mathbb{C} une catégorie, une *monade* sur \mathbb{C} est un triplet $(T, (\eta_A)_{A \in \mathbb{C}}, (\mu_A)_{A \in \mathbb{C}})$ où T est un foncteur de \mathbb{C} dans \mathbb{C} , $(\eta_A)_{A \in \mathbb{C}}$ est une transformation naturelle de id dans T et $(\mu_A)_{A \in \mathbb{C}}$ est une transformation naturelle de T^2 dans T et les diagrammes suivants commutent :

$$\begin{array}{ccc} T^3(A) & \xrightarrow{T(\mu_A)} & T^2(A) \\ \mu_{T(A)} \downarrow & & \downarrow \mu_A \\ T^2(A) & \xrightarrow{\mu_A} & T(A) \end{array} \qquad \begin{array}{ccccc} & & \eta_{T(A)} & & T(\eta_A) \\ & & \longleftarrow & T(A) & \longrightarrow & T^2(A) \\ & \mu_A & \searrow & \downarrow id_A & \swarrow & \mu_A \\ & & & T(A) & & \end{array}$$

Une *co-monade* $(T, (\varepsilon_A)_{A \in \mathbb{C}}, (\delta_A)_{A \in \mathbb{C}})$ sur \mathbb{C} est une monade sur \mathbb{C}^{op} .

Exemple 13

Soient \mathbb{C} et \mathbb{D} deux catégories, F un foncteur de \mathbb{D} dans \mathbb{C} , G un foncteur de \mathbb{C} dans \mathbb{D} , et φ une adjonction entre F et G , si $(\varepsilon_A)_{A \in \mathbb{C}}$ et $(\eta_{A'})_{A' \in \mathbb{D}}$ sont les deux transformations naturelles définies après la [définition 12](#) alors $(GF, \eta, G\varepsilon F)$ est une monade sur \mathbb{D} .

Définition 39 (Catégorie de Seely)

Une *catégorie de Seely* est donnée par :

$$(\mathbb{C}, \otimes, 1, \multimap, \perp, \&, \top, !, (assoc_{A,B,C}^{\otimes})_{(A,B,C) \in \mathbb{C}^3}, (unit_A^{l \otimes})_{A \in \mathbb{C}}, (unit_A^{r \otimes})_{A \in \mathbb{C}}, (\gamma_{A,B}^{\otimes})_{(A,B) \in \mathbb{C}^2}, (\varepsilon_A)_{A \in \mathbb{C}}, (\delta_A)_{A \in \mathbb{C}}, (m_{A,B})_{(A,B) \in \mathbb{C}}, n)$$

où :

- $(\mathbb{C}, \otimes, 1, \multimap, \perp, (assoc_{A,B,C}^{\otimes})_{(A,B,C) \in \mathbb{C}^3}, (unit_A^{l \otimes})_{A \in \mathbb{C}}, (unit_A^{r \otimes})_{A \in \mathbb{C}}, (\gamma_{A,B}^{\otimes})_{(A,B) \in \mathbb{C}^2})$ est une catégorie \star -autonome cartésienne (les produits étant donnés par $(\&, \top)$)
- $(!, (\varepsilon_A)_{A \in \mathbb{C}}, (\delta_A)_{A \in \mathbb{C}})$ est une *co-monade* sur \mathbb{C}
- $(!, (m_{A,B})_{(A,B) \in \mathbb{C}}, n)$ est un foncteur monoïdal symétrique fort de $(\mathbb{C}, \&, \top, (assoc_{A,B,C}^{\&})_{(A,B,C) \in \mathbb{C}^3}, (unit_A^{l \&})_{A \in \mathbb{C}}, (unit_A^{r \&})_{A \in \mathbb{C}}, (\gamma_{A,B}^{\&})_{(A,B) \in \mathbb{C}^2})$ dans $(\mathbb{C}, \otimes, 1, (assoc_{A,B,C}^{\otimes})_{(A,B,C) \in \mathbb{C}^3}, (unit_A^{l \otimes})_{A \in \mathbb{C}}, (unit_A^{r \otimes})_{A \in \mathbb{C}}, (\gamma_{A,B}^{\otimes})_{(A,B) \in \mathbb{C}^2})$
- le diagramme suivant commute :

$$\begin{array}{ccc} !A \otimes !B & \xrightarrow{m_{A,B}} & !(A \& B) \\ \downarrow \delta_A \otimes \delta_B & & \downarrow \delta_{A \& B} \\ !!A \otimes !!B & \xrightarrow{m_{!A, !B}} & !(A \& !B) \end{array}$$

Proposition 34 (Catégorie de co-Kleisli)

Soit \mathbb{C} une catégorie de Seely, la catégorie dont les objets sont les mêmes que pour \mathbb{C} et dont les morphismes de A dans B sont $\mathbb{C}(!A, B)$ (appelée *catégorie de co-Kleisli de la co-monade !*) est une *catégorie cartésienne fermée*.

Il s'agit d'une version sémantique de la traduction de Girard de LJ dans LL (voir [section 7.2](#)).

Interprétation de LL

On va montrer que les catégories de Seely fournissent les modèles de LL en donnant une interprétation des preuves de LL comme des morphismes d'une catégorie de Seely.

Lemme 18 (\otimes -comonoïde $!A$)

Dans une catégorie de Seely, tout objet $!A$ est muni d'une structure de \otimes -comonoïde symétrique $(!A, c_{!A}^{\otimes}, w_{!A}^{\otimes})$.

DÉMONSTRATION : On définit :

$$\begin{aligned} c_{!A}^{\otimes} &= !A \xrightarrow{! \Delta_A} !(A \& A) \xrightarrow{m_{A,A}^{-1}} !A \otimes !A \\ w_{!A}^{\otimes} &= !A \xrightarrow{! term_A} !\top \xrightarrow{n^{-1}} 1 \end{aligned}$$

et on vérifie que, puisque $(!, (m_{A,B})_{(A,B) \in \mathbb{C}}, n)$ est monoïdal symétrique fort et puisque $(A, \Delta_A, term_A)$ est un $\&$ -comonoïde symétrique, les diagrammes requis commutent. \square

Lemme 19 (Monoïdalité de ! pour \otimes)

Si \mathbb{C} est une catégorie de Seely, ! est un foncteur monoïdal symétrique $(!, (m'_{A,B})_{(A,B) \in \mathbb{C}}, n')$ de $(\mathbb{C}, \otimes, 1)$ dans la catégorie $(\otimes\text{-coMon}(\mathbb{C}), \otimes, 1)$ des \otimes -comonoïdes symétriques de \mathbb{C} .

DÉMONSTRATION : On définit :

$$\begin{aligned} m'_{A,B} &= !A \otimes !B \xrightarrow{m_{A,B}} !(A \& B) \xrightarrow{\delta_{A \& B}} !!(A \& B) \xrightarrow{!m_{A,B}^{-1}} !(A \otimes !B) \xrightarrow{!(\varepsilon_A \otimes \varepsilon_B)} !(A \otimes B) \\ n' = 1 &\xrightarrow{n} !\top \xrightarrow{\delta_{\top}} !!\top \xrightarrow{!n^{-1}} !1 \end{aligned}$$

et on vérifie que les diagrammes requis commutent. \square

Une preuve π dont la conclusion est un séquent $\vdash \Gamma = \vdash A_1, \dots, A_n$ est interprétée comme un morphisme $[\pi]$ de 1 dans $[\Gamma] = [A_1] \wp \dots \wp [A_n]$ où chaque formule est interprétée par l'objet correspondant (une fois fixée une interprétation arbitraire des variables par des objets).

On va abondamment utiliser le fait que, dans une catégorie \star -autonome, se donner un morphisme de 1 dans $A \wp B$ ou de A^\perp dans B ou de B^\perp dans A ou de $A^\perp \otimes B^\perp$ dans \perp revient au même.

On omettra le plus souvent les morphismes d'associativité et de commutativité des structures monoïdales.

- règle *ax* : l'identité $id_{[A]}$ est un morphisme de $[A]$ dans $[A]$.
- règle *cut* : partant d'un morphisme f de $[\Gamma^\perp]$ dans $[A]$ et d'un g morphisme de $[A]$ dans $[\Delta]$, la composition $f ; g$ donne un morphisme de $[\Gamma^\perp]$ dans $[\Delta]$.
- règle \otimes : partant d'un morphisme f de $[\Gamma^\perp]$ dans $[A]$ et d'un morphisme g de $[\Delta^\perp]$ dans $[B]$, le bifoncteur \otimes donne un morphisme $f \otimes g$ de $[\Gamma^\perp] \otimes [\Delta^\perp]$ dans $[A] \otimes [B]$.
- règle \wp : l'interprétation de la prémisse et de la conclusion sont les mêmes.
- règle 1 : l'identité id_1 est un morphisme de $[1]$ dans $[1]$.
- règle \perp : partant d'un morphisme f de $[\Gamma^\perp]$ dans $[A]$, en le composant avec $unit_{[A]}^{\wp}$ on obtient un morphisme $f ; unit_{[A]}^{\wp}$ de $[\Gamma^\perp]$ dans $[A] \wp [\perp]$.
- règle $\&$: partant d'un morphisme f de $[\Gamma^\perp]$ dans $[A]$ et d'un morphisme g de $[\Gamma^\perp]$ dans $[B]$, on obtient un morphisme $\langle f, g \rangle$ de $[\Gamma^\perp]$ dans $[A] \& [B]$.
- règle \oplus_1 : partant d'un morphisme f de $[A^\perp]$ dans $[\Gamma]$, en le composant à gauche avec $\pi_{[A^\perp]}$ on obtient un morphisme $\pi_{[A^\perp]} ; f$ de $[A^\perp] \& [B^\perp]$ dans $[\Gamma]$.
- règle \oplus_2 : partant d'un morphisme f de $[B^\perp]$ dans $[\Gamma]$, en le composant à gauche avec $\pi_{[B^\perp]}$ on obtient un morphisme $\pi_{[B^\perp]} ; f$ de $[A^\perp] \& [B^\perp]$ dans $[\Gamma]$.
- règle \top : le morphisme $term_{[\Gamma^\perp]}$ va de $[\Gamma^\perp]$ dans \top .
- règle ! : partant d'un morphisme f de $[!A_1^\perp] \otimes \dots \otimes [!A_n^\perp]$ dans $[A]$, le morphisme $!f$ va de $![!A_1^\perp] \otimes \dots \otimes [!A_n^\perp]$ dans $![A]$, on le compose à gauche par les morphismes m'_{\perp} appropriés pour obtenir un morphisme de $![!A_1^\perp] \otimes \dots \otimes [!A_n^\perp]$ dans $![A]$ et encore à gauche par $\delta_{[A_1^\perp]} \otimes \dots \otimes \delta_{[A_n^\perp]}$ et on obtient un morphisme de $![A_1^\perp] \otimes \dots \otimes [A_n^\perp]$ dans $![A]$.
- règle ?*d* : partant d'un morphisme f de $[A^\perp]$ dans $[\Gamma]$, en le composant à gauche avec $\varepsilon_{[A^\perp]}$ on obtient un morphisme $\varepsilon_{[A^\perp]} ; f$ de $![A^\perp]$ dans $[\Gamma]$.
- règle ?*c* : partant d'un morphisme f de $[!A^\perp] \otimes [!A^\perp]$ dans $[\Gamma]$, en le composant à gauche avec $c_{[!A^\perp]}^{\otimes}$ on obtient un morphisme $c_{[!A^\perp]}^{\otimes} ; f$ de $![A^\perp]$ dans $[\Gamma]$.
- règle ?*w* : partant d'un morphisme f de 1 dans $[\Gamma]$, en le composant à gauche avec $w_{[!A^\perp]}^{\otimes}$ on obtient un morphisme $w_{[!A^\perp]}^{\otimes} ; f$ de $![A^\perp]$ dans $[\Gamma]$.

Théorème 9 (Correction)

Si la preuve π se réduit en π' par élimination des coupures alors $[\pi] = [\pi']$.

8.2 Orthogonalité

Orthogonalité ensembliste

Étant donnés deux ensembles E et F , une *orthogonalité ensembliste* \perp sur E et F est un sous-ensemble de $E \times F$. Si $e \in E$ et $f \in F$, on note $e \perp f$ si $(e, f) \in \perp$. Si X est un sous-ensemble de E , on définit $X^\perp = \{f \in F \mid \forall x \in X, x \perp f\}$ qui est un sous-ensemble de F . Si Y est un sous-ensemble de F , on définit $Y^\perp = \{e \in E \mid \forall y \in Y, e \perp y\}$ qui est un sous-ensemble de E .

Lemme 20 (Clôture)

Soient X, X_1 et X_2 des sous-ensembles de E et Y, Y_1 et Y_2 des sous-ensembles de F :

- $X_1 \subseteq X_2 \Rightarrow X_2^\perp \subseteq X_1^\perp$ et $Y_1 \subseteq Y_2 \Rightarrow Y_2^\perp \subseteq Y_1^\perp$
- $X \subseteq X^{\perp\perp}$ et $Y \subseteq Y^{\perp\perp}$
- $X^\perp = X^{\perp\perp\perp}$ et $Y^\perp = Y^{\perp\perp\perp}$
- $X = X^{\perp\perp}$ si et seulement si il existe $Y \subseteq F$ tel que $X = Y^\perp$ (et $Y = Y^{\perp\perp}$ si et seulement si il existe $X \subseteq E$ tel que $Y = X^\perp$)

DÉMONSTRATION : On montre les propriétés pour X, X_1 et X_2 :

- Soit $f \in X_2^\perp$, pour tout $x \in X_1$, on a $x \in X_2$ donc $x \perp f$. D'où $X_2^\perp \subseteq X_1^\perp$.
- Soit $x \in X$, pour tout $f \in X^\perp$, par définition de X^\perp , on a $x \perp f$, donc $x \in X^{\perp\perp}$.
- On a déjà vu que $X^\perp \subseteq (X^\perp)^{\perp\perp}$, et de $X \subseteq X^{\perp\perp}$, on déduit $(X^{\perp\perp})^\perp \subseteq X^\perp$.
- Si $X = X^{\perp\perp}$, alors $X = (X^\perp)^\perp$. Si $X = Y^\perp$, on a $X = Y^\perp = Y^{\perp\perp\perp} = (Y^\perp)^{\perp\perp} = X^{\perp\perp}$.

Les autres propriétés sont obtenues de manière symétrique. \square

Un sous-ensemble X de E (ou Y de F) est appelé un *fait* si $X = X^{\perp\perp}$.

Orthogonalité catégorique

Étant donnés une catégorie \mathbb{C} et deux objets I et J de \mathbb{C} , une *orthogonalité catégorique* entre I et J est une famille \perp d'orthogonalités ensemblistes \perp_A (indexées par les objets A de \mathbb{C}) entre $\mathbb{C}(I, A)$ et $\mathbb{C}(A, J)$.

Définition 40 (Orthogonalité monoïdale)

Si $(\mathbb{C}, \otimes, 1, (assoc_{A,B,C}^\otimes)_{(A,B,C) \in \mathbb{C}^3}, (unit_A^l)_{A \in \mathbb{C}}, (unit_A^r)_{A \in \mathbb{C}}, (\gamma_{A,B}^\otimes)_{(A,B) \in \mathbb{C}^2})$ est une catégorie monoïdale symétrique fermée et J est un objet de \mathbb{C} , on dit qu'une orthogonalité catégorique \perp entre I et J est une *orthogonalité monoïdale* si :

- tenseur : si $u \in \mathbb{C}(I, A)$, $v \in \mathbb{C}(I, B)$ et $z \in \mathbb{C}(A \otimes B, J)$,

$$u \perp_A \langle z \mid v \rangle_B \wedge v \perp_B \langle z \mid u \rangle_A \iff u \tilde{\otimes} v \perp_{A \otimes B} z$$

- implication : si $u \in \mathbb{C}(I, A)$, $f \in \mathbb{C}(A, B)$ et $y \in \mathbb{C}(B, J)$,

$$u \perp_A f ; y \wedge u ; f \perp_B y \iff \text{cũrry}(f) \perp_{A \multimap B} u \tilde{\circ} y$$

- isomorphismes : si $u \in \mathbb{C}(I, D)$ et $y \in \mathbb{C}(E, J)$,

$$u ; \varphi \perp_E y \iff u \perp_D \varphi ; y$$

pour chaque isomorphisme φ de D dans E issu de la structure monoïdale de \mathbb{C} : $assoc_{A,B,C}^\otimes$, $unit_A^l$, $unit_A^r$ ou $\gamma_{A,B}^\otimes$

– stabilité du tenseur : si $U \subseteq \mathbb{C}(1, A)$ et $V \subseteq \mathbb{C}(1, B)$,

$$(U^{\perp\perp} \tilde{\otimes} V^{\perp\perp})^{\perp} = (U^{\perp\perp} \tilde{\otimes} V)^{\perp} = (U \tilde{\otimes} V^{\perp\perp})^{\perp}$$

– stabilité de l'implication : si $U \subseteq \mathbb{C}(1, A)$ et $Y \subseteq \mathbb{C}(B, J)$,

$$(U^{\perp\perp} \tilde{\circ} Y^{\perp\perp})^{\perp} = (U^{\perp\perp} \tilde{\circ} Y)^{\perp} = (U \tilde{\circ} Y^{\perp\perp})^{\perp}$$

Les notations utilisées sont :

$$\langle z \mid u \rangle_A = B \xrightarrow{\text{unit}_B^{\otimes r}} 1 \otimes B \xrightarrow{u \otimes \text{id}_B} A \otimes B \xrightarrow{z} C$$

$$\langle z \mid v \rangle_B = A \xrightarrow{\text{unit}_A^{\otimes l}} A \otimes 1 \xrightarrow{\text{id}_A \otimes v} A \otimes B \xrightarrow{z} C$$

$$u \tilde{\otimes} v = 1 \xrightarrow{\text{unit}_1^{\otimes r}} 1 \otimes 1 \xrightarrow{u \otimes v} A \otimes B$$

$$u \tilde{\circ} y = A \multimap B \xrightarrow{u \multimap y} 1 \multimap C \xrightarrow{\cong} C$$

$$\text{cũrry}(f) = 1 \xrightarrow{\text{cũrry}(\text{unit}_A^{\otimes r-1}; f)} A \multimap B$$

(étendues point par point pour les ensembles de morphismes).

On dit qu'un morphisme $f \in \mathbb{C}(A, B)$ est *focal* par rapport à $U \subseteq \mathbb{C}(1, A)$ et $Y \subseteq \mathbb{C}(B, J)$ si pour tout $u \in U$ et tout $y \in Y$:

$$u ; f \perp_B y \iff u \perp_A f ; y$$

La condition (isomorphismes) de la [définition 40](#) est donc une condition de focalité des isomorphismes de la structure de catégorie monoïdale symétrique.

Lemme 21 (Focalité et bi-orthogonal)

Soient $f \in \mathbb{C}(A, B)$, $U \subseteq \mathbb{C}(1, A)$ et $Y \subseteq \mathbb{C}(B, J)$,

– si f est focal par rapport à $U^{\perp\perp}$ et Y alors :

$$\forall u \in U \ u ; f \in Y^{\perp} \iff \forall u' \in U^{\perp\perp} \ u' ; f \in Y^{\perp}$$

– si f est focal par rapport à U et $Y^{\perp\perp}$ alors :

$$\forall y \in Y \ f ; y \in U^{\perp} \iff \forall y' \in Y^{\perp\perp} \ f ; y' \in U^{\perp}$$

DÉMONSTRATION : Si f est focal par rapport à $U^{\perp\perp}$ et Y :

$$\begin{aligned} \forall u' \in U^{\perp\perp} \ u' ; f \in Y^{\perp} &\iff \forall u' \in U^{\perp\perp} \forall y \in Y \ u' ; f \perp_B y \\ &\iff \forall u' \in U^{\perp\perp} \forall y \in Y \ u' \perp_A f ; y \\ &\iff \forall y \in Y \ f ; y \in U^{\perp\perp\perp} = U^{\perp} \\ &\iff \forall u \in U \forall y \in Y \ u \perp_A f ; y \\ &\iff \forall u \in U \forall y \in Y \ u ; f \perp_B y \\ &\iff \forall u \in U \ u ; f \in Y^{\perp} \end{aligned}$$

Si f est focal par rapport à U et $Y^{\perp\perp}$:

$$\begin{aligned} \forall y' \in Y^{\perp\perp} \ f ; y' \in U^{\perp} &\iff \forall u \in U \forall y' \in Y^{\perp\perp} \ u \perp_A f ; y' \\ &\iff \forall u \in U \forall y' \in Y^{\perp\perp} \ u ; f \perp_B y' \\ &\iff \forall u \in U \ u ; f \in Y^{\perp\perp\perp} = Y^{\perp} \\ &\iff \forall u \in U \forall y \in Y \ u ; f \perp_B y \\ &\iff \forall u \in U \forall y \in Y \ u \perp_A f ; y \\ &\iff \forall y \in Y \ f ; y \in U^{\perp} \end{aligned}$$

□

Exemple 14

Si \mathbb{C} est une catégorie et I et J sont deux objets de \mathbb{C} , à tout sous-ensemble F de $\mathbb{C}(I, J)$, on peut associer l'orthogonalité catégorique $\perp_A^F = \{(u, x) \in \mathbb{C}(I, A) \times \mathbb{C}(A, J) \mid u; x \in F\}$ entre I et J . Une telle orthogonalité \perp^F est dite *focale* et F est appelé son *foyer*.

Si $(\mathbb{C}, \otimes, 1, (assoc_{A,B,C}^{\otimes})_{(A,B,C) \in \mathbb{C}^3}, (unit_A^l)^{\otimes})_{A \in \mathbb{C}}, (unit_A^r)^{\otimes})_{A \in \mathbb{C}}, (\gamma_{A,B}^{\otimes})_{(A,B) \in \mathbb{C}^2})$ est une catégorie monoïdale symétrique fermée, J est un objet de \mathbb{C} et F est un sous-ensemble de $\mathbb{C}(1, J)$, l'orthogonalité focale \perp^F est une orthogonalité monoïdale. De plus tout morphisme $f : A \rightarrow B$ est focal par rapport à $\mathbb{C}(1, A)$ et $\mathbb{C}(B, J)$ pour cette orthogonalité.

Catégorie d'orthogonalité**Définition 41** (Catégorie d'orthogonalité)

Soient \mathbb{C} une catégorie, I et J deux objets de \mathbb{C} et \perp une orthogonalité catégorique entre I et J , la *catégorie d'orthogonalité* $\mathbb{C}_{I,J}^{\perp}$ a :

- pour objets les paires (A, U) où A est un objet de \mathbb{C} et U est un sous-ensemble de $\mathbb{C}(I, A)$ tel que $U = U^{\perp\perp}$,
- pour morphismes de (A, U) dans (B, V) , les morphismes f de $\mathbb{C}(A, B)$ tels que :

$$\begin{aligned} \forall u \in U \quad u; f &\in V \\ \forall y \in V^{\perp} \quad f; y &\in U^{\perp} \end{aligned}$$

Théorème 10 (Catégorie d'orthogonalité monoïdale)

Si $(\mathbb{C}, \otimes, 1, (assoc_{A,B,C}^{\otimes})_{(A,B,C) \in \mathbb{C}^3}, (unit_A^l)^{\otimes})_{A \in \mathbb{C}}, (unit_A^r)^{\otimes})_{A \in \mathbb{C}}, (\gamma_{A,B}^{\otimes})_{(A,B) \in \mathbb{C}^2})$ est une catégorie monoïdale symétrique fermée, J est un objet de \mathbb{C} et \perp est une orthogonalité monoïdale entre 1 et J , alors $\mathbb{C}_{1,J}^{\perp}$ est munie d'une structure de catégorie monoïdale symétrique fermée avec :

$$\begin{aligned} 1 &= (1, \{id_1\}^{\perp\perp}) \\ (A, U) \otimes (B, V) &= (A \otimes B, (U \tilde{\otimes} V)^{\perp\perp}) \\ (A, U) \multimap (B, V) &= (A \multimap B, (U \tilde{\multimap} V^{\perp})^{\perp}) \end{aligned}$$

DÉMONSTRATION : On note d'abord que f est un morphisme de (A, U) dans (B, V) dans $\mathbb{C}_{1,J}^{\perp}$ si et seulement si $c\tilde{u}rry(f) \in (U \tilde{\multimap} V^{\perp})^{\perp}$. Cela découle de la [définition 41](#) et de la [définition 40](#) (implication).

- Soient $f : (A, U) \rightarrow (B, V)$ et $g : (A', U') \rightarrow (B', V')$ deux morphismes de $\mathbb{C}_{1,J}^{\perp}$, on montre que $f \otimes g$ est un morphisme de $(A, U) \otimes (A', U')$ dans $(B, V) \otimes (B', V')$. Par la remarque précédente, cela revient à montrer que $c\tilde{u}rry(f \otimes g) \in ((U \tilde{\otimes} U')^{\perp\perp} \tilde{\multimap} (V \tilde{\otimes} V')^{\perp\perp\perp})^{\perp}$. Or on a, par stabilité de l'implication :

$$((U \tilde{\otimes} U')^{\perp\perp} \tilde{\multimap} (V \tilde{\otimes} V')^{\perp\perp\perp})^{\perp} = ((U \tilde{\otimes} U') \tilde{\multimap} (V \tilde{\otimes} V')^{\perp})^{\perp}$$

En appliquant la propriété (implication) de la [définition 40](#), montrer que $c\tilde{u}rry(f \otimes g) \in ((U \tilde{\otimes} U') \tilde{\multimap} (V \tilde{\otimes} V')^{\perp})^{\perp}$ revient à montrer que :

$$\begin{aligned} \forall u \in U \quad \forall u' \in U' \quad \forall z \in (V \tilde{\otimes} V')^{\perp} \quad & (u \tilde{\otimes} u'); (f \otimes g) \perp_{B \otimes B'} z \\ \wedge \quad u \tilde{\otimes} u' \perp_{A \otimes A'} (f \otimes g); z & \end{aligned}$$

La première propriété revient à $(u; f) \tilde{\otimes} (u'; g) \perp z$ qui s'obtient par $u; f \in V^{\perp\perp} = V$ et $u'; g \in V'^{\perp\perp} = V'$. La seconde propriété se montre grâce à la condition (tenseur) de la [définition 40](#) :

$$u \tilde{\otimes} u' \perp_{A \otimes A'} (f \otimes g); z \iff u \perp_A \langle (f \otimes g); z \mid u' \rangle_{A'} \wedge u' \perp_{A'} \langle (f \otimes g); z \mid u \rangle_A$$

Les deux composantes de la conjonction se montrent de manière symétrique, on se concentre sur la première :

$$u \perp\!\!\!\perp_A \langle (f \otimes g) ; z \mid u' \rangle_{A'} \iff u \perp\!\!\!\perp_A f ; \langle z \mid u' ; g \rangle_{B'}$$

Par définition de $f : (A, U) \rightarrow (B, V)$, il suffit donc de montrer que $\langle z \mid u' ; g \rangle_{B'} \in V^\perp$, ce qui découle de la condition (tenseur) de la [définition 40](#) et de $u' ; g \in V'$.

- On veut maintenant que montrer que $h : (A, U) \otimes (A', U') \rightarrow (B, V)$ si et seulement si $\text{curry}(h) : (A, U) \rightarrow (A', U') \multimap (B, V)$. D'après la remarque faite au début de la preuve, cela revient à prouver que $\text{cũrry}(h) \in ((U \otimes U')^\perp \multimap V^\perp)^\perp$ si et seulement si $\text{cũrry}(\text{curry}(h)) \in (U \multimap (U' \multimap V^\perp))^{\perp\perp}$. Par stabilité de l'implication ceci revient à $\text{cũrry}(h) \in ((U \otimes U') \multimap V^\perp)^\perp$ si et seulement si $\text{cũrry}(\text{curry}(h)) \in (U \multimap (U' \multimap V^\perp))^{\perp\perp}$. On a, en utilisant à nouveau la remarque de début de preuve, $\text{cũrry}(h) \in ((U \otimes U') \multimap V^\perp)^\perp$ si et seulement si pour tous $u \in U, u' \in U', y \in V^\perp$:

$$\begin{aligned} & u \tilde{\otimes} u' ; h \perp\!\!\!\perp_B y \wedge u \tilde{\otimes} u' \perp\!\!\!\perp_{A \otimes A'} h ; y \\ \iff & u' ; \langle h \mid u \rangle_A \perp\!\!\!\perp_B y \wedge u \perp\!\!\!\perp_A \langle h ; y \mid u' \rangle_{A'} \wedge u' \perp\!\!\!\perp_{A'} \langle h ; y \mid u \rangle_A \\ \iff & u' ; \langle h \mid u \rangle_A \perp\!\!\!\perp_B y \wedge u \perp\!\!\!\perp_A \langle h \mid u' \rangle_{A'} ; y \wedge u' \perp\!\!\!\perp_{A'} \langle h \mid u \rangle_A ; y \\ \iff & \text{cũrry}(\langle h \mid u \rangle_A) \perp\!\!\!\perp_{A' \multimap B} u' \multimap y \wedge u \perp\!\!\!\perp_A \langle h \mid u' \rangle_{A'} ; y \\ \iff & u ; \text{curry}(h) \perp\!\!\!\perp_{A' \multimap B} u' \multimap y \wedge u \perp\!\!\!\perp_A \text{curry}(h) ; u' \multimap y \\ \iff & \text{cũrry}(\text{curry}(h)) \perp\!\!\!\perp_{A \multimap A' \multimap B} u \multimap (u' \multimap y) \end{aligned}$$

c'est-à-dire $\text{cũrry}(\text{curry}(h)) \in (U \multimap (U' \multimap V^\perp))^{\perp\perp}$.

- On montre également que les différents isomorphismes issus de la structure monoïdale symétrique de \mathbb{C} sont des (iso)morphismes dans $\mathbb{C}_{1,J}^\perp$. Soient $(A, U), (B, V)$ et (C, W) trois objets de $\mathbb{C}_{1,J}^\perp$, en utilisant la stabilité du tenseur, on a :

$$\begin{aligned} ((U \tilde{\otimes} V)^\perp \tilde{\otimes} W)^\perp &= ((U \tilde{\otimes} V) \tilde{\otimes} W)^\perp \\ (U \tilde{\otimes} (V \tilde{\otimes} W))^\perp &= (U \tilde{\otimes} (V \tilde{\otimes} W)^\perp)^\perp \end{aligned}$$

D'après le [lemme 21](#), $f \in ((U \tilde{\otimes} V) \tilde{\otimes} W)^\perp$ et $h \in (U \tilde{\otimes} (V \tilde{\otimes} W))^\perp$ alors $f ; \text{assoc}_{A,B,C}^\otimes \in (U \tilde{\otimes} (V \tilde{\otimes} W))^\perp$ car $\text{assoc}_{A,B,C}^\otimes$ est focal. Si $g \in (U \tilde{\otimes} V) \tilde{\otimes} W$ et $h \in (U \tilde{\otimes} (V \tilde{\otimes} W))^\perp$, $g \perp\!\!\!\perp_{(A \otimes B) \otimes C} \text{assoc}_{A,B,C}^\otimes ; h \iff g ; \text{assoc}_{A,B,C}^\otimes \perp\!\!\!\perp_{A \otimes (B \otimes C)} h$ (par focalité de $\text{assoc}_{A,B,C}^\otimes$) donc $\text{assoc}_{A,B,C}^\otimes ; h \in ((U \tilde{\otimes} V) \tilde{\otimes} W)^\perp$.

On traite de même le cas de $\text{unit}_A^l \otimes, \text{unit}_A^r \otimes$ et $\gamma_{A,B}^\otimes$.

La commutation des différents diagrammes découle quant à elle des commutations dans \mathbb{C} , ce qui conclut la preuve. \square

Les constructions de catégorie d'orthogonalité peuvent s'étendre aux connecteurs additifs et exponentiels et à la logique linéaire classique.

8.3 Modèle relationnel

On s'intéresse désormais à un modèle concret (mais dont la dualité est dégénérée) de LL.

À toute formule de MELL on associe un ensemble $|A|$ appelé *trame* de la manière suivante : on suppose fixé un ensemble $|X| = |X^\perp|$ pour chaque variable, puis :

$$\begin{aligned} |A \otimes B| &= |A| \times |B| \\ |A \wp B| &= |A| \times |B| \\ |1| &= \{\star\} \\ |\perp| &= \{\star\} \\ |!A| &= \mathcal{M}_{fin}(|A|) \\ |?A| &= \mathcal{M}_{fin}(|A|) \end{aligned}$$

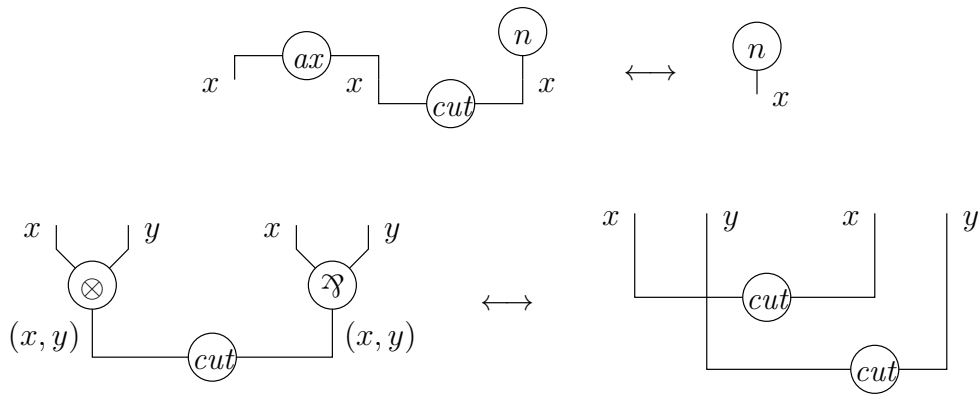
où $\mathcal{M}_{fin}(E)$ est l'ensemble des multi-ensembles finis d'éléments de E . De sorte que pour toute formule A , on a $|A| = |A^\perp|$.

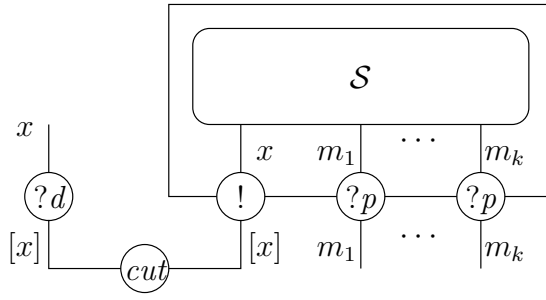
Une *pseudo-expérience* d'un réseau \mathcal{R} est une fonction qui associe à chaque arête à profondeur 0 de \mathcal{R} un élément de la trame de la formule associée. On appelle *résultat* de la pseudo-expérience les éléments associés aux conclusions du réseau. Une *expérience* est une pseudo-expérience telle que :

- Les éléments associés aux deux conclusions d'un nœud ax sont les mêmes.
- Les éléments associés aux deux prémisses d'un nœud cut sont les mêmes.
- L'élément associé à la conclusion d'un nœud \otimes ou \wp est le couple des éléments associés à ses prémisses.
- Si l'élément associé à la prémisses d'un nœud $?d$ est x , celui associé à sa conclusion est $[x]$.
- L'élément associé à la conclusion d'un nœud $?w$ est $[\]$.
- L'élément associé à la conclusion d'un nœud $?c$ est la somme des éléments associés à ses prémisses.
- Si les éléments associés aux conclusions d'une boîte sont m_0 pour la porte principale et m_1, \dots, m_k pour les portes auxiliaires alors il existe $p \geq 0$ expériences du réseau situé à l'intérieur de la boîte de résultats $(x_0^i, n_1^i, \dots, n_k^i)_{1 \leq i \leq p}$ avec $m_0 = [x_0^1, \dots, x_0^p]$ et pour chaque $1 \leq j \leq k$, $m_j = n_j^1 + \dots + n_j^p$.

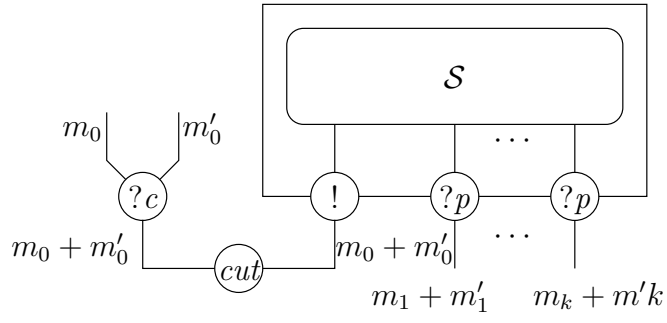
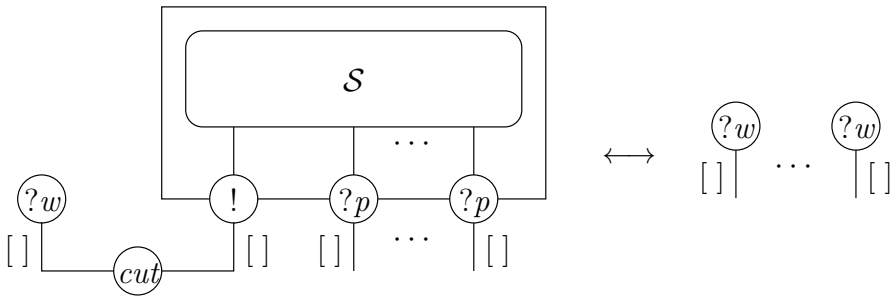
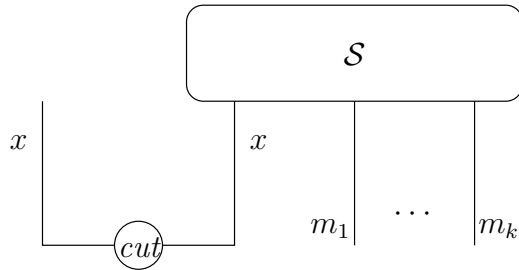
L'interprétation relationnelle $\llbracket \mathcal{R} \rrbracket$ d'un réseau \mathcal{R} est l'ensemble des résultats des expériences de \mathcal{R} .

Pour montrer la préservation de la sémantique par réduction, on montre que si \mathcal{R} se réduit en \mathcal{R}' alors, à toute expérience de \mathcal{R} , on peut associer une expérience de \mathcal{R}' de même résultat, et réciproquement. On montre comment faire le lien entre les expériences d'un module et celles du module réduit (on n'indique pas ici les types des arêtes mais uniquement les valeurs associées aux arêtes par les expériences) :

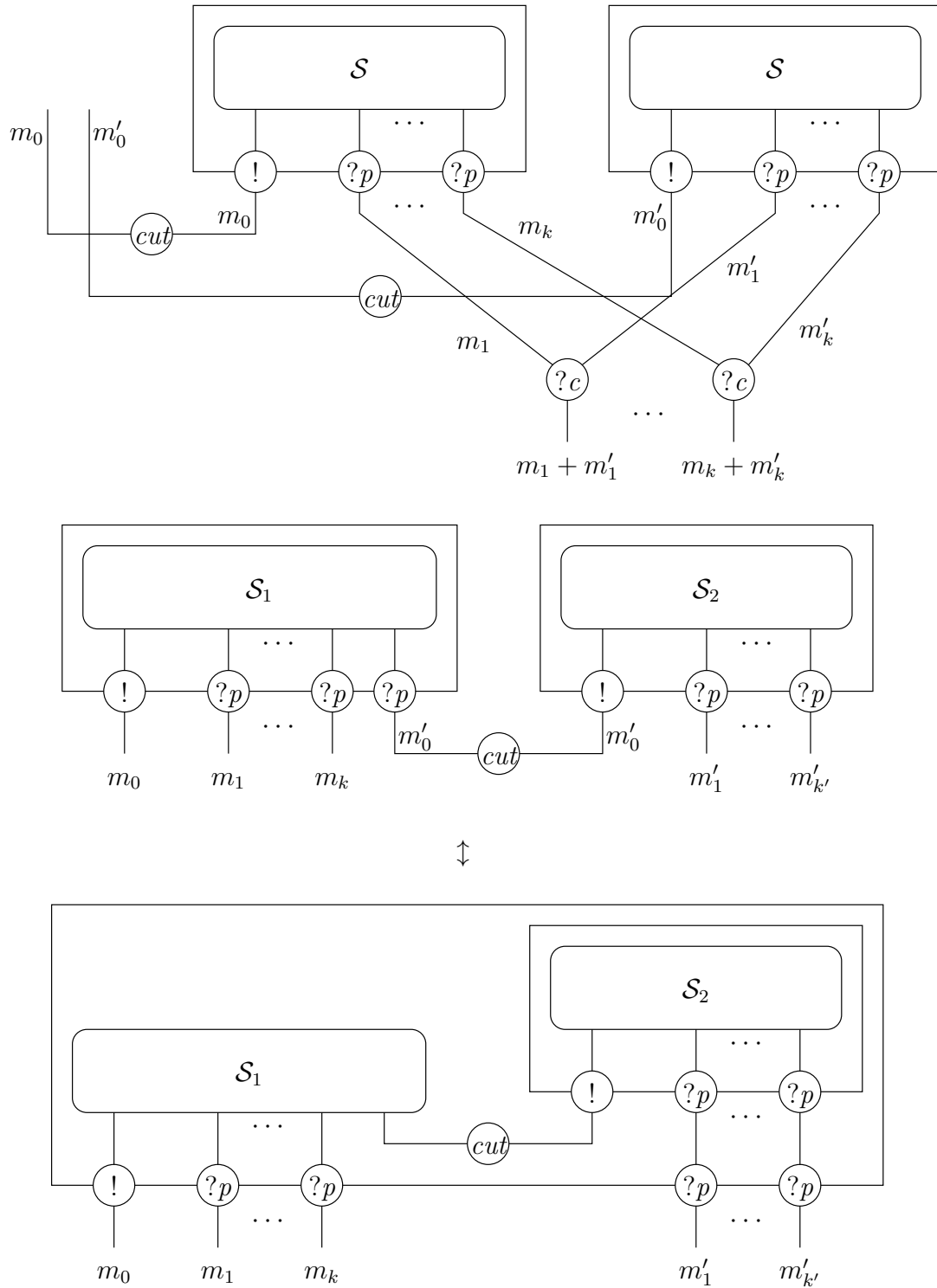




\updownarrow



\updownarrow



Le multi-ensemble m'_0 se décompose en une somme $m'_0 = n_1 + \dots + n_p$ correspondant aux différents multi-ensembles issus des expériences de \mathcal{S}_1 . Les expériences de \mathcal{S}_2 peuvent donc être regroupées selon le n_i dans lequel elles induisent un élément. Avant réduction, on effectue toutes ses expériences et on somme les résultats sur les différentes portes auxiliaires pour obtenir $m'_1, \dots, m'_{k'}$. Après réduction, pour chaque expérience de \mathcal{S}_1 , on effectue les expériences correspondant à n_i dont on somme les résultats sur les portes auxiliaires. Ces résultats sont ensuite re-sommés lorsque i varie pour finalement obtenir $m'_1, \dots, m'_{k'}$.

Ce modèle s'étend sans problème aux connecteurs additifs par :

$$\begin{aligned} |A \& B| &= |A| \uplus |B| \\ |A \oplus B| &= |A| \uplus |B| \\ |\top| &= \emptyset \\ |0| &= \emptyset \end{aligned}$$

Cependant, en l'absence de notion de réseau satisfaisante pour ces connecteurs, on est obligé de définir l'interprétation directement en calcul des séquents ce qui complique la preuve de préservation par élimination des coupures.

Remarque : On peut vérifier que ce modèle est non dégénéré (*i.e.* il existe deux preuves différentes d'un même séquent dont les interprétations sont différentes) en calculant l'interprétation des codages des booléens : les deux preuves de $\vdash 1 \oplus 1$ (ou avec $\vdash (X^\perp \wp X^\perp) \wp (X \otimes X)$ dans MLL).

De manière générale, il est également possible de passer par la caractérisation catégorique des modèles de LL en montrant que l'on a une catégorie de Seely et que l'interprétation que l'on a définie est bien l'interprétation générale de LL dans ces catégories.

Soit $\mathbb{R}el$ la catégorie dont les objets sont les ensembles et dont les morphismes de E dans F sont les relations entre E et F (*i.e.* les sous-ensembles de $E \times F$) :

- l'identité de E dans E est donnée par $\{(e, e) \mid e \in E\}$,
- la composition d'une relation r de E dans F et d'une relation s de F dans G est donnée par $\{(e, g) \mid \exists f \in F, (e, f) \in r \wedge (f, g) \in s\}$.

La catégorie $\mathbb{R}el$ est une catégorie de Seely avec pour \otimes le produit cartésien \times , pour $\&$ l'union disjointe \uplus et pour co-monade ! l'opération $E \mapsto \mathcal{M}_{fn}(E)$.

Exemple 15 (Évaluation)

Le morphisme $ev_{E,F}$ est $\{(((e, f), e), f) \mid e \in E \wedge f \in F\} \subset ((E \times F) \times E) \times F$.

Remarque : La catégorie \star -autonome sous-jacente a la propriété que $1 = \perp$ et $\otimes = \wp$, on dit alors qu'il s'agit d'une *catégorie compacte fermée*.

8.4 Modèle cohérent

On ne traite ici que le fragment multiplicatif.

Espaces cohérents

Un *espace cohérent* X est une paire $(|X|, \circ_X)$ où $|X|$ est un ensemble et \circ_X est une relation binaire réflexive et symétrique sur $|X|$ appelée *relation de cohérence* :

- $\forall x \in |X|, x \circ_X x$
- $\forall (x, y) \in |X|^2, x \circ_X y \Rightarrow y \circ_X x$

On introduit des variantes de la relation de cohérence :

- $x \frown_X y$ si $x \circ_X y$ et $x \neq y$ (*cohérence stricte*)
- $x \smile_X y$ si $\neg x \circ_X y$ (*incohérence stricte*)
- $x \succsim_X y$ si $x \smile_X y$ ou $x = y$ (*incohérence*)

On peut vérifier que la donnée de l'une des quatre relations $\circ_X, \frown_X, \succsim_X$ ou \smile_X permet de déterminer les trois autres.

Si X est un espace cohérent, on définit son *espace dual* $X^\perp = (|X|, \succ_X)$ qui est aussi un espace cohérent. En général $X \neq X^\perp$ (si $X = (\{a, b\}, \{(a, a), (b, b), (a, b), (b, a)\})$ alors $X^\perp = (\{a, b\}, \{(a, a), (b, b)\})$) mais on a toujours $X^{\perp\perp} = X$.

Une *clique* c de l'espace cohérent X (noté $c \sqsubseteq X$) est un sous-ensemble de $|X|$ tel que si $x \in c$ et $y \in c$ alors $x \circ_X y$. Tout espace cohérent possède au moins une clique : la clique vide.

On définit différentes constructions d'espaces cohérents :

- $1 = \perp = (\{\star\}, \{(\star, \star)\})$ est l'unique (à isomorphisme près) espace cohérent à un seul point
- $X \otimes Y = (|X| \times |Y|, \circ_{X \otimes Y})$ avec $(x, y) \circ_{X \otimes Y} (x', y') \iff x \circ_X x' \wedge y \circ_Y y'$
- $X \wp Y = (|X| \times |Y|, \circ_{X \wp Y})$ avec $(x, y) \circ_{X \wp Y} (x', y') \iff x \circ_X x' \vee y \circ_Y y'$
- $X \multimap Y = (|X| \times |Y|, \circ_{X \multimap Y})$ avec

$$(x, y) \circ_{X \multimap Y} (x', y') \iff x \circ_X x' \Rightarrow y \circ_Y y'$$

$$(x, y) \circ_{X \multimap Y} (x', y') \iff x \circ_X x' \Rightarrow y \circ_Y y' \wedge y \succ_Y y' \Rightarrow x \succ_X x'$$

On a $1^\perp = \perp = 1 = \perp^\perp$, $(X \otimes Y)^\perp = X^\perp \wp Y^\perp$, $(X \wp Y)^\perp = X^\perp \otimes Y^\perp$, et $X \multimap Y = X^\perp \wp Y$.

La *sémantique cohérente* interprète une preuve de la logique linéaire de conclusion $\vdash A_1, \dots, A_n$ comme une clique de l'espace cohérent $\llbracket A_1 \rrbracket \wp \dots \wp \llbracket A_n \rrbracket$ (une fois que l'on a associé un espace cohérent $\llbracket X \rrbracket$ à chaque atome X). L'interprétation d'un réseau de preuve est donnée, comme pour le modèle relationnel, par l'ensemble des résultats d'expériences. On en déduit immédiatement qu'elle est préservée par élimination des coupures. Il convient cependant de montrer que l'interprétation d'un réseau de preuve est une clique.

Théorème 11 (Cohérence)

Si \mathcal{R} est un réseau de preuve de conclusions A_1, \dots, A_n alors $\llbracket \mathcal{R} \rrbracket$ est une clique de l'espace cohérent $\llbracket A_1 \rrbracket \wp \dots \wp \llbracket A_n \rrbracket$.

DÉMONSTRATION : On considère deux expériences e et e' de \mathcal{R} de résultats $r = (a_1, \dots, a_n)$ et $r' = (a'_1, \dots, a'_n)$. Si $r = r'$ alors $r \circ r'$, si il existe $1 \leq i \leq n$ tel que $a_i \circ_{A_i} a'_i$ alors $r \circ r'$, et s'il existe $1 \leq i \leq n$ tel que $a_i \succ_{A_i} a'_i$ alors on va montrer qu'il existe $1 \leq j \leq n$ tel que $a_j \circ_{A_j} a'_j$ donc à nouveau $r \circ r'$.

Supposons qu'il existe $1 \leq i \leq n$ tel que $a_i \succ_{A_i} a'_i$. On va décrire comment construire un chemin dans \mathcal{R} partant de la conclusion de \mathcal{R} de type A_i et tel que :

- si le chemin passe dans une arête α de \mathcal{R} en montant alors $e(\alpha) \succ e'(\alpha)$,
- si le chemin passe dans une arête α de \mathcal{R} en descendant alors $e(\alpha) \circ e'(\alpha)$.

Si le chemin arrive en montant dans la conclusion $\alpha : A$ d'un axiome, on a $e(\alpha) \succ_A e'(\alpha)$ et on continue en descendant dans l'autre conclusion $\beta : A^\perp$ de cet axiome avec $e(\beta) = e(\alpha) \circ_{A^\perp} e'(\alpha) = e'(\beta)$.

Si le chemin arrive en montant dans la conclusion $\alpha : A \otimes B$ d'un nœud \otimes de prémisses $\beta : A$ et $\gamma : B$, on a $e(\alpha) \succ_{A \otimes B} e'(\alpha)$ donc $e(\beta) \succ_A e'(\beta)$ ou $e(\gamma) \succ_B e'(\gamma)$ et on continue en montant dans l'arête qui convient (on choisit arbitrairement si les deux conviennent).

Si le chemin arrive en montant dans la conclusion $\alpha : A \wp B$ d'un nœud \wp de prémisses $\beta : A$ et $\gamma : B$, on a $e(\alpha) \succ_{A \wp B} e'(\alpha)$ donc $e(\beta) \succ_A e'(\beta)$ ou $e(\gamma) \succ_B e'(\gamma)$ et on continue en montant dans β si elle convient et dans γ sinon.

Le chemin ne peut pas arriver en montant dans la conclusion α un nœud 1 ou \perp puisqu'on aurait $e(\alpha) = e'(\alpha)$ et pas incohérence stricte.

Si le chemin arrive en descendant dans la prémisses $\alpha : A$ d'une coupure, on a $e(\alpha) \circ_A e'(\alpha)$ et on continue en montant dans l'autre prémisses $\beta : A^\perp$ de cette coupure avec $e(\beta) = e(\alpha) \circ_{A^\perp} e'(\alpha) = e'(\beta)$.

Si le chemin arrive en descendant dans la prémisses $\alpha : A$ d'un nœud \otimes dont l'autre prémisses est $\beta : B$ et la conclusion est $\gamma : A \otimes B$, on a $e(\alpha) \circ_A e'(\alpha)$:

- si $e(\beta) \smile_B e'(\beta)$, on continue en montant dans β ,
- si $e(\beta) \supset_B e'(\beta)$, alors $e(\gamma) \frown_{A \otimes B} e'(\gamma)$ et on continue en descendant dans γ .

Si le chemin arrive en descendant dans la prémisses $\alpha : A$ d'un nœud \mathfrak{X} dont l'autre prémisses est $\beta : B$ et la conclusion est $\gamma : A \mathfrak{X} B$, on a $e(\alpha) \frown_A e'(\alpha)$ donc $e(\gamma) \frown_{A \mathfrak{X} B} e'(\gamma)$ et on continue en descendant dans γ .

On montre que les chemins ainsi construits sont acycliques. Sinon on considère un cycle minimal. S'il ne contient pas les deux prémisses d'un même nœud \mathfrak{X} alors il est inclus dans un graphe de correction ce qui est impossible. S'il contient les deux prémisses d'un même nœud \mathfrak{X} , il arrive nécessairement en descendant sur les prémisses (en montant on va toujours vers la même prémisses par construction et, puisqu'on ne passe jamais directement d'une prémisses à l'autre d'un nœud \mathfrak{X} , on ne peut pas à la fois monter et descendre dans un même nœud \mathfrak{X} car sinon on aurait à la fois $e(\gamma) \frown_{A \mathfrak{X} B} e'(\gamma)$ et $e(\gamma) \smile_{A \mathfrak{X} B} e'(\gamma)$ sur la conclusion γ du nœud), mais dans ce cas il n'est pas minimal puisqu'on a un sous-cycle strict en partant de la conclusion et en atteignant la prémisses atteinte en second.

Considérons maintenant un chemin maximal. Il est fini puisqu'il ne contient pas de cycle et que \mathcal{R} est fini. Il termine alors nécessairement en descendant dans une conclusion $c_j : A_j$ (dans tous les autres cas, on a défini une manière d'étendre le chemin) et donc $a_j \frown_{A_j} a'_j$ puisque le chemin arrive en descendant. \square

Remarque : Dans la preuve du théorème précédent, seule l'acyclicité des graphes de correction est utilisée. Une réciproque montre d'ailleurs que si l'interprétation relationnelle d'une structure de preuve sans coupures est une clique (en interprétant les variables par des espaces raisonnables) alors ses graphes de correction sont acycliques.

Catégorie $\mathbb{C}oh$

Soit $\mathbb{C}oh$ la catégorie dont les objets sont les espaces cohérents et dont les morphismes de X dans Y sont les cliques de $X \multimap Y$:

- l'identité de X dans X est donnée par $\{(x, x) \mid x \in |X|\}$,
- la composition d'une clique c de $X \multimap Y$ et d'une clique c' de $Y \multimap Z$ est donnée par $c ; c' = \{(x, z) \mid \exists y \in |Y|, (x, y) \in c \wedge (y, z) \in c'\}$.

On vérifie que l'identité est une clique de $X \multimap X$ pour tout espace cohérent X , et que, pour toutes cliques de $X \multimap Y$ et $Y \multimap Z$, leur composée est une clique de $X \multimap Z$.

Remarque : Si c est une clique de $X \multimap Y$ et c' est une clique de $Y \multimap Z$ et si $(x, z) \in c ; c'$ alors le point $y \in |Y|$ tel que $(x, y) \in c$ et $(y, z) \in c'$ est unique : si $(x, y) \in c$ et $(x, y') \in c$ alors $y \supset_Y y'$ et si $(y, z) \in c'$ et $(y', z) \in c'$ alors $y \smile_Y y'$, donc $y = y'$.

La catégorie $\mathbb{C}oh$ est une catégorie \star -autonome avec \perp comme objet dualisant.

Orthogonalité de cohérence

Soit E un ensemble, on considère l'*orthogonalité ensembliste de cohérence* sur $\mathcal{P}(E)$ (et lui-même) définie par $a \perp\!\!\!\perp b$ si $\text{card}(a \cap b) \leq 1$. Soit A un fait de $\mathcal{P}(E)$ pour cette orthogonalité, A est clos par sous-ensemble. En effet si $x_1 \subseteq x_2 \in A$, pour tout $y \in A^{\perp\!\!\!\perp}$, $\text{card}(x_1 \cap y) \leq \text{card}(x_2 \cap y) \leq 1$ donc $x_1 \perp\!\!\!\perp y$ d'où $x_1 \in A^{\perp\!\!\!\perp\!\!\!\perp} = A$.

Si A est un fait de $\mathcal{P}(E)$, on définit $a_1 \supset_A a_2$ par $\{a_1, a_2\} \in A$ ($\{a_1, a_2\} \subseteq E$). On définit également $|A| = \{e \in E \mid e \supset_A e\}$. Si $a_1 \supset_A a_2$ alors $a_1 \in |A|$ et $a_2 \in |A|$ puisque A est clos par sous-ensemble. \supset_A est une relation réflexive et symétrique sur $|A|$ donc $(|A|, \supset_A)$ est un espace cohérent. Si c est une clique de $(|A|, \supset_A)$ alors $c \in A$ (pour tout $y \in A^{\perp\!\!\!\perp}$, si $\{a_1, a_2\} \subseteq c \cap y$

alors $\{a_1, a_2\} \subseteq \{a_1, a_2\} \cap y$ mais comme $a_1 \supset_A a_2$ on a $\{a_1, a_2\} \perp\!\!\!\perp y$ avec $\{a_1, a_2\} \subseteq y$ d'où $a_1 = a_2$ et donc $c \perp\!\!\!\perp y$, *i.e.* $c \in A^{\perp\!\!\!\perp} = A$.

Réciproquement, soit X un espace cohérent on considère l'ensemble de ses cliques \mathcal{C} qui est un sous-ensemble de $\mathcal{P}(|X|)$. Pour l'orthogonalité de cohérence, $\mathcal{C} = \mathcal{D}^{\perp\!\!\!\perp}$ où \mathcal{D} est l'ensemble des cliques de l'espace cohérent X^{\perp} . En effet, si $c \in \mathcal{C}$ et $d \in \mathcal{D}$, et si $e_1, e_2 \subseteq c \cap d$ alors $e_1 \supset_X e_2$ et $e_1 \supset_{X^{\perp}} e_2$ donc $e_1 = e_2$ et $c \perp\!\!\!\perp d$ *i.e.* $\mathcal{C} \subseteq \mathcal{D}^{\perp\!\!\!\perp}$, et réciproquement si $a \in \mathcal{D}^{\perp\!\!\!\perp}$ et $\{e_1, e_2\} \subseteq a$ on a, pour tout $d \in \mathcal{D}$, $\text{card}(\{e_1, e_2\} \cap d) \leq \text{card}(a \cap d) \leq 1$ donc $e_1 \supset_X e_2$ (sinon $e_1 \wedge_{X^{\perp}} e_2$ donc $\{e_1, e_2\} \in \mathcal{D}$ et $\text{card}(\{e_1, e_2\} \cap \{e_1, e_2\}) = 2$), d'où $\mathcal{D}^{\perp\!\!\!\perp} \subseteq \mathcal{C}$. On en déduit que \mathcal{C} est un fait. On peut alors définir $\supset_{\mathcal{C}}$ comme précédemment et on a $x_1 \supset_X x_2$ si et seulement si $x_1 \supset_{\mathcal{C}} x_2$ ($x_1 \supset_X x_2$ si et seulement si $\{x_1, x_2\}$ est une clique de X , ce qui équivaut à $\{x_1, x_2\} \in \mathcal{C}$ c'est-à-dire à $x_1 \supset_{\mathcal{C}} x_2$).

Les espaces cohérents peuvent donc être définis comme les faits de l'orthogonalité de cohérence.

La structure monoïdale de la catégorie **Coh** peut être obtenue comme la catégorie d'orthogonalité pour l'orthogonalité de cohérence à partir de la catégorie **Rel** (entre l'objet $\{\star\}$ et l'objet $\{\star\}$).

8.5 Géométrie de l'interaction

La géométrie de l'interaction est basée sur l'idée d'interpréter une preuve de LL (ou un réseau) comme l'ensemble de ses chemins persistants (*i.e.* qui ne sont pas détruits par l'élimination des coupures). Le travail consiste alors à donner des caractérisations alternatives de cette notion de persistance.

On interprète ici un réseau MELL comme une machine (la IAM) dont un *état* est donné par le choix d'une arête, le choix d'une direction ("vers le haut" ou "vers le bas") et le choix d'un jeton valide pour cette arête.

Un *jeton* est un triplet (X, b, σ) . On dit que ce jeton est valide pour l'arête a de type A si X est une occurrence d'atome dans A , b est une pile d'entiers de longueur p où p est la profondeur de a dans le réseau, et σ est une pile d'entiers de longueur n où n est le nombre de connecteurs exponentiels (! et ?) dans le champ desquels se trouve X dans A .

Un *état initial* (resp. *état final*) est un état pour lequel l'arête choisie est une conclusion du réseau et la direction est "vers le haut" (resp. "vers le bas") (ce qui entraîne que b est la pile vide).

On suppose données deux injections r et s de \mathbb{N} dans \mathbb{N} d'images disjointes et une injection $\langle -, - \rangle$ de $\mathbb{N} \times \mathbb{N}$ dans \mathbb{N} . Les *transitions* de la IAM sont données par :

- si un jeton arrive en montant dans un nœud ax , il repart en descendant dans l'autre conclusion (en changeant l'occurrence d'atome en l'occurrence duale)
- si un jeton arrive en descendant dans une coupure, il repart en montant dans l'autre prémisses (en changeant l'occurrence d'atome en l'occurrence duale)
- si un jeton arrive en montant dans un nœud \otimes ou \wp , il repart en montant dans la prémisses dans laquelle se trouve l'occurrence d'atome du jeton
- si un jeton arrive en descendant dans un nœud \otimes ou \wp , il repart en descendant dans la conclusion
- si un jeton (X, b, σ) arrive en descendant dans un nœud $?d$, on passe à l'état $(X, b, 0.\sigma)$ descendant dans la conclusion
- si un jeton $(X, b, 0.\sigma)$ arrive en montant dans un nœud $?d$, on passe à l'état (X, b, σ) montant dans la prémisses
- si un jeton $(X, b, i.\sigma)$ arrive en descendant dans la prémisses gauche d'un nœud $?c$, on passe à l'état $(X, b, r(i).\sigma)$ descendant dans la conclusion

- si un jeton $(X, b, i.\sigma)$ arrive en descendant dans la prémissse droite d'un nœud $?c$, on passe à l'état $(X, b, s(i).\sigma)$ descendant dans la conclusion
- si un jeton $(X, b, r(i).\sigma)$ arrive en montant dans la conclusion d'un nœud $?c$, on passe à l'état $(X, b, i.\sigma)$ montant dans la prémissse gauche
- si un jeton $(X, b, s(i).\sigma)$ arrive en montant dans la conclusion d'un nœud $?c$, on passe à l'état $(X, b, i.\sigma)$ montant dans la prémissse droite
- si un jeton $(X, i.b, \sigma)$ arrive en descendant dans la prémissse d'un nœud $!$, on passe à l'état $(X, b, i.\sigma)$ descendant dans la conclusion
- si un jeton $(X, b, i.\sigma)$ arrive en montant dans la conclusion d'un nœud $!$, on passe à l'état $(X, i.b, \sigma)$ montant dans la prémissse
- si un jeton $(X, i.b, j.\sigma)$ arrive en descendant dans la prémissse d'un nœud $?p$, on passe à l'état $(X, b, \langle i, j \rangle.\sigma)$ descendant dans la conclusion
- si un jeton $(X, b, \langle i, j \rangle.\sigma)$ arrive en montant dans la conclusion d'un nœud $?p$, on passe à l'état $(X, i.b, j.\sigma)$ montant dans la prémissse

On peut vérifier que ces transitions préservent le fait que le jeton soit valide dans l'arête associée. Les transitions de la IAM sont réversibles.

Lemme 22 (Accès à b)

Si on considère une suite de transitions partant en montant dans une conclusion de l'intérieur d'une boîte avec le jeton (X, b, σ) et terminant en descendant dans une conclusion de ce même intérieur de boîte (le tout sans jamais sortir de la boîte) alors le jeton obtenu est (Y, b, σ') . De plus on peut considérer la suite de transitions partant de (X, b', σ) et on obtiendra (Y, b', σ') .

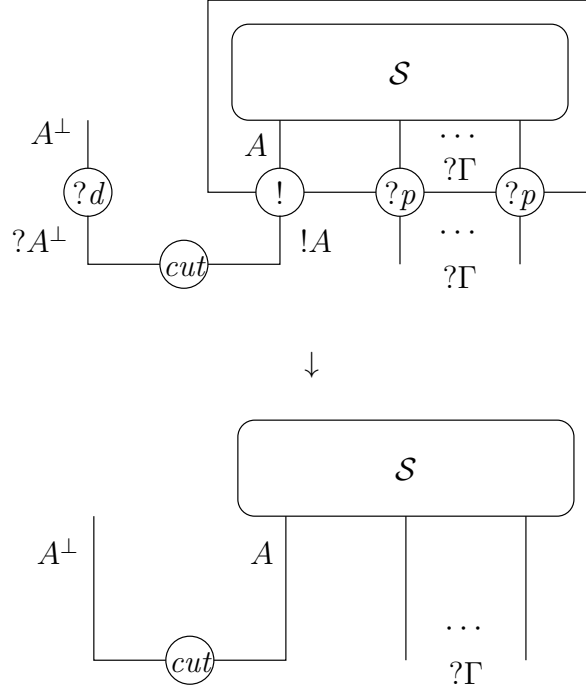
DÉMONSTRATION : On montre que toute transition qui ne concerne que des arêtes de profondeur supérieure ou égale à p agit sur le jeton (X, b, σ) indépendamment des p derniers éléments de b et ne les modifie pas. \square

On va montrer que les réductions multiplicatives préservent l'interprétation par la Gol. En l'absence de réduction multiplicative, comme on l'a vu dans la preuve de la [proposition 30](#) on peut définir la notion de coupure exponentielle maximale. Si on s'intéresse à un réseau n'ayant aucun connecteur $?$ dans les formules de ses conclusions, la boîte prémissse d'une coupure exponentielle maximale n'a pas de porte auxiliaire (sinon en descendant sous une telle porte auxiliaire on ne peut arriver que dans une conclusion, ce qui est impossible par hypothèse sur les connecteurs $?$, ou dans une coupure, ce qui est impossible par maximalité de la coupure de départ). On va montrer que lors de la réduction d'une telle coupure l'interprétation n'est pas modifiée non plus. Plus précisément on montrera que suite à l'entrée d'un jeton dans le module que l'on réduit, il y a boucle avant si et seulement si il y a boucle après, il y a blocage avant si et seulement si il y a blocage après et sinon le jeton qui ressort n'est pas modifié par la réduction. Par réversibilité des transitions, on ne considère qu'un sens à chaque fois.

- Étape ax : pas de blocage, ni de boucle possible ni avant ni après et le jeton reste le même dans les deux cas.
- Étape \otimes/\mathfrak{A} : pas de blocage, ni de boucle possible ni avant ni après et :
 - avant réduction : on arrive dans la prémissse gauche (resp. droite) du \otimes et on a $(X, b, \sigma) \rightsquigarrow (X, b, \sigma) \rightsquigarrow (X^\perp, b, \sigma) \rightsquigarrow (X^\perp, b, \sigma)$ qui remonte dans la prémissse gauche (resp. droite) du \mathfrak{A}
 - après réduction : on arrive dans la prémissse de la coupure de gauche (resp. droite) et on a $(X, b, \sigma) \rightsquigarrow (X^\perp, b, \sigma)$ qui remonte dans l'autre prémissse de la coupure de gauche (resp. droite)
- Étape $!/?d$:
 - avant réduction : le jeton (X, b, σ) arrive dans la déréluction, on a $(X, b, \sigma) \rightsquigarrow (X, b, 0.\sigma) \rightsquigarrow (X^\perp, b, 0.\sigma) \rightsquigarrow (X^\perp, 0.b, \sigma)$ à l'intérieur de la boîte

- après réduction : le jeton (X, b, σ) arrive dans la coupure, on a $(X, b, \sigma) \rightsquigarrow (X^\perp, b, \sigma)$ dans ce qui était la boîte
- par le [lemme 22](#), il y a donc boucle avant si et seulement si il y a boucle après et blocage avant si et seulement si il y a blocage après, sinon :
- avant réduction : un jeton $(Y, 0.b, \sigma')$ ressort de la boîte, on a $(Y, 0.b, \sigma') \rightsquigarrow (Y, b, 0.\sigma') \rightsquigarrow (Y^\perp, b, 0.\sigma') \rightsquigarrow (Y^\perp, b, \sigma')$ qui remonte au-dessus de la dérélition
 - après réduction : par le [lemme 22](#), le jeton (Y, b, σ') ressort de la boîte, on a $(Y, b, \sigma') \rightsquigarrow (Y^\perp, b, \sigma')$ qui remonte au-dessus de la dérélition
- Étape $!/?w$: le module réduit n'ayant aucune communication avec le reste du réseau, aucun jeton ne peut y entrer.
 - Étape $!/?c$: on ne traite que le cas où on arrive par la prémisse gauche de la contraction, l'autre cas étant extrêmement similaire.
 - avant réduction : le jeton $(X, b, i.\sigma)$ arrive dans la prémisse gauche de la contraction, on a $(X, b, i.\sigma) \rightsquigarrow (X, b, r(i).\sigma) \rightsquigarrow (X^\perp, b, r(i).\sigma) \rightsquigarrow (X^\perp, r(i).b, \sigma)$ à l'intérieur de la boîte
 - après réduction : le jeton $(X, b, i.\sigma)$ arrive dans la coupure, on a $(X, b, i.\sigma) \rightsquigarrow (X^\perp, b, i.\sigma) \rightsquigarrow (X^\perp, i.b, \sigma)$ dans la première copie de la boîte
- par le [lemme 22](#), il y a donc boucle avant si et seulement si il y a boucle après et blocage avant si et seulement si il y a blocage après, sinon :
- avant réduction : un jeton $(Y, r(i).b, \sigma')$ ressort de la boîte, on a $(Y, r(i).b, \sigma') \rightsquigarrow (Y, b, r(i).\sigma') \rightsquigarrow (Y^\perp, b, r(i).\sigma') \rightsquigarrow (Y^\perp, b, i.\sigma')$ qui remonte dans la prémisse gauche de la contraction
 - après réduction : par le [lemme 22](#), le jeton $(Y, i.b, \sigma')$ ressort de la boîte, on a $(Y, i.b, \sigma') \rightsquigarrow (Y, b, i.\sigma') \rightsquigarrow (Y^\perp, b, i.\sigma')$ qui remonte dans la prémisse de la coupure
- Étape $!/!$: le calcul se passe de la même manière avant et après réduction jusqu'à ce qu'un jeton $(X, i.b, j.\sigma)$ arrive en descendant dans la conclusion de la première boîte qui est coupée (à l'intérieur de la boîte)
 - avant réduction : on a $(X, i.b, j.\sigma) \rightsquigarrow (X, b, \langle i, j \rangle.\sigma) \rightsquigarrow (X^\perp, b, \langle i, j \rangle.\sigma) \rightsquigarrow (X^\perp, \langle i, j \rangle.b, \sigma)$ qui remonte dans la prémisse de la porte principale de la deuxième boîte
 - après réduction : on a $(X, i.b, j.\sigma) \rightsquigarrow (X^\perp, i.b, j.\sigma) \rightsquigarrow (X^\perp, j.i.b, \sigma)$ dans la prémisse de la porte principale de la deuxième boîte
- par le [lemme 22](#), il y a donc boucle avant si et seulement si il y a boucle après et blocage avant si et seulement si il y a blocage après, sinon :
- avant réduction : un jeton $(Y, \langle i, j \rangle.b, \sigma')$ ressort de la deuxième boîte, on a $(Y, \langle i, j \rangle.b, \sigma') \rightsquigarrow (Y, b, \langle i, j \rangle.\sigma') \rightsquigarrow (Y^\perp, b, \langle i, j \rangle.\sigma') \rightsquigarrow (Y^\perp, i.b, j.\sigma')$ qui remonte dans la première boîte par la prémisse de la porte auxiliaire coupée
 - après réduction ; le jeton $(Y, j.i.b, \sigma')$ ressort de la boîte, on a $(Y, j.i.b, \sigma') \rightsquigarrow (Y, i.b, j.\sigma') \rightsquigarrow (Y^\perp, i.b, j.\sigma')$ qui remonte dans la première boîte par la prémisse de la coupure
- le calcul est ensuite le même avant et après réduction (en refaisant le même raisonnement si le calcul passe à nouveau par la coupure).

Remarque : On peut voir que pour les autres réductions exponentielles le jeton peut être modifié :



Si un jeton (X^\perp, b, σ) dans la boîte montant par la prémisses de la porte principale donne (Y, b, i, σ') descendant dans la prémisses d'une porte auxiliaire, alors (X, b, σ) descendant dans la prémisses de la déréluction va donner $(Y, b, \langle 0, i \rangle, \sigma')$ avant réduction et (Y, b, i, σ') après. Essayer de corriger ce cas avec $\langle 0, i \rangle = i$ mènerait à une interprétation dégénérée.

Étant donnée une conclusion a de type A d'un réseau \mathcal{R} et une paire (X, σ) où X est une occurrence d'atome dans A et σ une pile d'entiers dont la longueur est le nombre de connecteurs exponentiels dans le champ desquels se trouve X dans A , on peut exécuter la IAM à partir de l'état initial obtenu en mettant le jeton (X, ε, σ) montant dans a . Soit la machine se bloque dans un état non final (aucune transition ne s'applique plus), soit elle boucle, soit elle atteint un état final et fournit une paire (Y, σ') et une conclusion a' où se situe le jeton. On définit ainsi une fonction partielle $\llbracket \mathcal{R} \rrbracket$ par $(a, X, \sigma) \mapsto (a', Y, \sigma')$. Dans le cas particulier d'un réseau sans connecteur exponentiel dans les conclusions, cette fonction partielle se résume à $(a, X) \mapsto (a', Y)$ (et s'il n'y a qu'une conclusion il reste $X \mapsto Y$). Par réversibilité des transitions, cette fonction partielle est une bijection partielle.

Théorème 12 (Correction de la Gol)

Si \mathcal{R} est un réseau sans connecteur ? dans ses conclusions et si \mathcal{R} se réduit en \mathcal{R}' alors $\llbracket \mathcal{R} \rrbracket = \llbracket \mathcal{R}' \rrbracket$.

DÉMONSTRATION : On considère la forme normale \mathcal{R}_0 de \mathcal{R} (qui est aussi celle de \mathcal{R}' par confluence) et on montre que $\llbracket \mathcal{R} \rrbracket = \llbracket \mathcal{R}_0 \rrbracket$ ce qui suffit ensuite pour conclure. Pour cela il suffit de montrer que l'interprétation est préservée pour les étapes multiplicatives et exponentielles avec boîte sans porte auxiliaire.

Pour une telle étape de réduction, soit le calcul de la IAM ne fait pas passer le jeton par le module modifié et les deux fonctions partielles ont la même valeur, soit le jeton passe par le module et, pour chaque passage, il y a une boucle dans un cas si et seulement si il y en a une dans l'autre, il y a un blocage dans un cas si et seulement si il y en a un dans l'autre, et sinon le calcul continue avec la même valeur du jeton dans les deux cas. La valeur des deux fonctions partielles est donc la même. \square

Proposition 35 (Terminaison et non blocage)

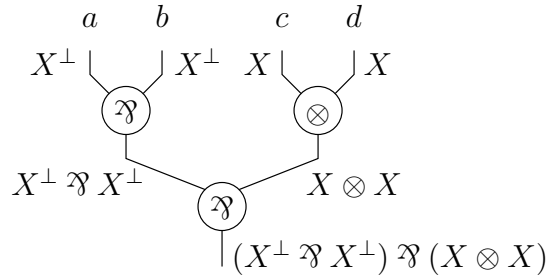
Dans un réseau sans ? dans les conclusions, le calcul de la IAM à partir d'un état initial termine toujours et ne bloque jamais.

DÉMONSTRATION : Par le [théorème 12](#), il suffit de s'intéresser au cas d'un réseau sans coupure.

Le seul moyen de bloquer est en montant dans une arête de type ?A, mais il n'y en a aucune dans un tel réseau. Le calcul consiste donc toujours à partir d'une conclusion, à monter jusqu'à un axiome et à redescendre dans une conclusion, ce qui termine. \square

La fonction $\llbracket \mathcal{R} \rrbracket$ définie par la Gol est donc une fonction totale.

Pour montrer que cette sémantique n'est pas dégénérée, on considère les réseaux de conclusion $(X^\perp \wp X^\perp) \wp (X \otimes X)$. Il en existe exactement deux sans coupure et avec axiomes expansés :



avec les nœuds ax entre a et c et entre b et d ou entre a et d et entre b et c . Si on note X_1^\perp l'occurrence de X^\perp correspondant à l'arête a et X_2^\perp celle correspondant à b et de même X_1 pour c et X_2 pour d , les sémantiques respectives de ces deux réseaux sont :

$$\begin{array}{l} X_1^\perp \leftrightarrow X_1 \\ X_2^\perp \leftrightarrow X_2 \end{array} \quad \text{et} \quad \begin{array}{l} X_1^\perp \leftrightarrow X_2 \\ X_2^\perp \leftrightarrow X_1 \end{array}$$

elles sont bien différentes et peuvent servir de codage des booléens. Ainsi la sémantique d'un réseau n'est pas toujours préservée par réduction mais celles de toutes ses projections sur ces booléens multiplicatifs le sont, ce qui suffit en pratique. On a ici une notion de sémantique plus faible qu'habituellement.

Remarque : Certaines réductions ne préservent pas l'interprétation par la géométrie de l'interaction. Cette interprétation ne donne donc pas lieu à une catégorie de Seely.

Remarque : Les chemins persistants sont exactement ceux pour lesquels il existe un état initial tel que le jeton parcourt ce chemin lors de l'exécution de la IAM.

Proposition 36 (Correction booléenne)

Si \mathcal{R} de conclusion $(X^\perp \wp X^\perp) \wp (X \otimes X)$ se réduit en \mathcal{R}' alors $\llbracket \mathcal{R} \rrbracket = \llbracket \mathcal{R}' \rrbracket$.

On peut étendre ce résultat à tout produit tensoriel de la formule $(X^\perp \wp X^\perp) \wp (X \otimes X)$ avec elle-même un nombre arbitraire de fois.

Chapitre 9

Complexité

L'introduction explicite des connecteurs exponentiels en logique linéaire permet, en modifiant les règles correspondantes, de maîtriser la complexité de l'élimination des coupures. On va voir ici deux exemples : **ELL** pour la complexité élémentaire (tours d'exponentielles) et **LLL** pour la complexité polynomiale.

9.1 ELL

Syntaxe

Le (fragment multiplicatif exponentiel du) système **ELL** est obtenu en modifiant les règles exponentielles : la déréliction et la promotion sont supprimées et on ajoute la règle de *promotion fonctorielle* :

$$\frac{\vdash \Gamma, A}{\vdash ?\Gamma, !A} !f$$

avec comme étape d'élimination des coupures :

$$\frac{\frac{\vdash \Gamma, A}{\vdash ?\Gamma, !A} !f \quad \frac{\vdash \Delta, A^\perp, B}{\vdash ?\Delta, ?A^\perp, !B} !f}{\vdash ?\Gamma, ?\Delta, !B} cut \quad \rightsquigarrow \quad \frac{\vdash \Gamma, A \quad \vdash \Delta, A^\perp, B}{\vdash \Gamma, \Delta, B} cut}{\vdash ?\Gamma, ?\Delta, !B} !f$$

De ce fait on perd les deux implications $!A \multimap !!A$ et $!A \multimap A$ (et $!!A \multimap !A$).

On associe naturellement une syntaxe de réseaux de preuve à ce système en supprimant la sorte $?d$ dans les réseaux de preuve exponentiels et en modifiant la sorte $?p$ pour qu'elle corresponde à la règle $!f$:

- sorte $?p$: une prémisses, une conclusion, si l'étiquette de la prémisses est A alors celle de la conclusion est $?A$

Ces réseaux vérifient une propriété de *stratification* : la profondeur d'un nœud qui n'est pas de sorte *cut* ne change pas durant l'élimination des coupures (celle du nœud *cut* que l'on réduit peut augmenter et celle des autres nœuds *cut* n'est pas modifiée non plus). De plus la réduction d'une coupure exponentielle à profondeur p ne peut pas donner de coupure multiplicative à profondeur p .

On peut donc réduire un réseau de la manière suivante : on se place à la plus petite profondeur contenant une coupure et on va tout d'abord réduire toutes les coupures de cette profondeur. Pour simplifier on suppose qu'il s'agit de la profondeur 0. On réduit toutes les coupures multiplicatives ce qui fait diminuer le nombre de nœuds multiplicatifs (le nombre d'étapes est donc majoré par le nombre de nœuds multiplicatifs à profondeur 0). On a ensuite un réseau

sans coupure multiplicative, on considère une coupure exponentielle maximale à profondeur 0 (au sens de la preuve de la [proposition 30](#)). On réduit une telle coupure ce qui fait diminuer strictement le nombre de nœuds de conclusion ? à partir desquels on peut atteindre un nœud *cut* (par un chemin sans rebond à profondeur 0 descendant dans la conclusion ?). Ce nombre d'étapes exponentielles est donc majoré par le nombre de nœuds exponentiels du réseau initial. On peut ainsi éliminer toutes les coupures à profondeur 0 d'un réseau \mathcal{R} en moins de $|\mathcal{R}|$ étapes.

Une étape de réduction peut au plus multiplier par 3 la taille du réseau. Après la réduction des coupures de profondeur 0, on obtient donc un réseau de taille majorée par $3^{|\mathcal{R}|} \times |\mathcal{R}| \leq 3^{3^{|\mathcal{R}|}}$. On montre alors (par récurrence sur d) qu'un réseau de profondeur d peut être réduit en moins de $3^{\dot{3}^{|\mathcal{R}|}}$ (tour de hauteur $2d + 1$) étapes (en donnant un réseau de taille majorée par $3^{\dot{3}^{|\mathcal{R}|}}$ de hauteur $2d + 2$).

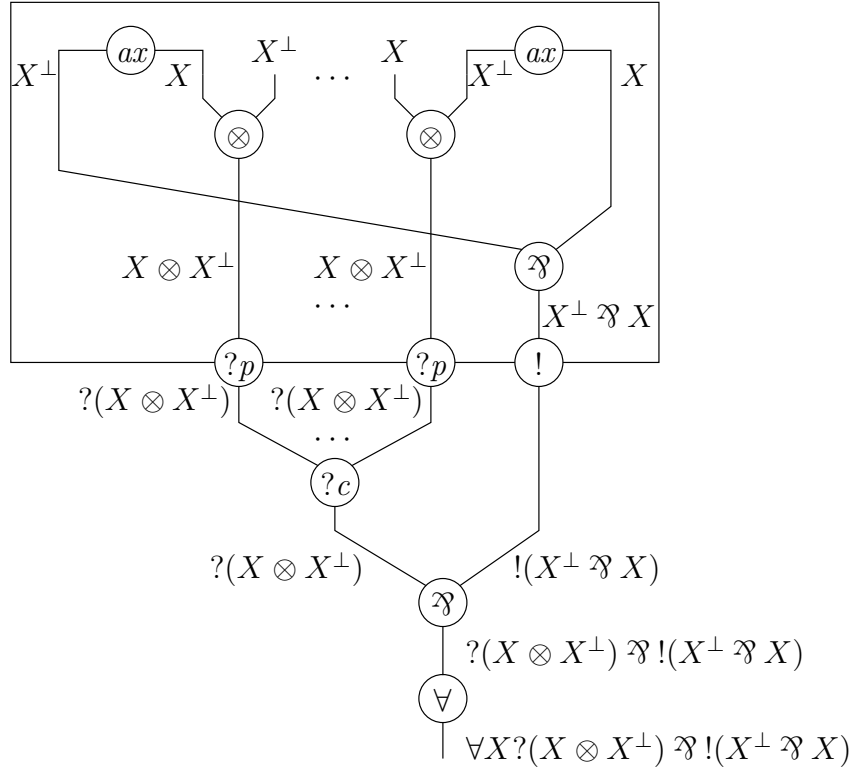
Remarque : On admettra que ces résultats peuvent s'étendre aux réseaux avec quantificateurs en négligeant la question du critère de correction. Les bornes sur les tailles de réseaux et les nombres d'étapes de réduction n'étant pas dépendantes de la taille des formules, le fait que l'étape de réduction \forall/\exists fasse diminuer la taille du réseau (comme les coupures multiplicatives) permet de conclure.

Programmation

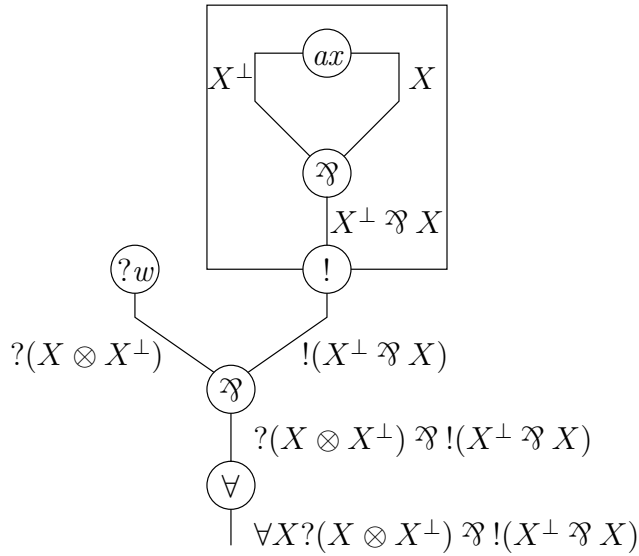
Une fonction f des entiers dans les entiers est de *complexité élémentaire* s'il existe un entier p tel que pour tout n , $f(n)$ se calcule en moins de $2^{\dot{2}^n}$ (tour de hauteur p) étapes (dans une machine de Turing par exemple).

Si on choisit de coder les entiers par le type usuel du système \mathcal{F} traduit dans LL, on obtient : $\forall X!(!X \multimap X) \multimap (!X \multimap X)$. Cependant on vérifie facilement que les codages des entiers de Church sont typables par $\forall X!(X \multimap X) \multimap (X \multimap X)$.

Dans ELL, on est amené à utiliser $\mathbb{N} = \forall X!(X \multimap X) \multimap !(X \multimap X) = \forall X?(X \otimes X^\perp) \wp !(X^\perp \wp X)$ (le type précédent n'étant pas dérivable pour tous les entiers dans ELL). Les entiers sont représentés par la traduction des entiers de Church avec des boîtes placées pour respecter les contraintes de ELL et le type ci-dessus. Pour l'entier $n \geq 1$ on obtient :



avec $n + 1$ nœuds ax ce qui donne un réseau de taille $4n + 4$. Et pour 0 :



de taille 6. On peut par ailleurs vérifier qu'il n'y a pas d'autre réseau sans coupure (avec axiomes expansés et à la structure des arbres ? près) dans ELL de conclusion \mathbb{N} .

Représenter une fonction f de k entiers dans les entiers dans ELL signifie trouver une preuve (que l'on peut supposer sans coupure) de $\vdash \mathbb{N}^\perp, \dots, \mathbb{N}^\perp, !^p \mathbb{N}$ (k occurrences de \mathbb{N}^\perp) telle qu'en la coupant sur la représentation de n_1, \dots, n_k et en éliminant les coupures on obtienne la représentation de $f(n_1, \dots, n_k)$ suivie de p règles $!f$. Considérons le cas d'une fonction unaire. Supposons que le réseau \mathcal{R} est de profondeur d , la normalisation de \mathcal{R} coupé sur la représentation

de $n \neq 0$ se fait donc en moins de $3^{\binom{d}{3} |\mathcal{R}| + 4n + 4}$ de hauteur $2d + 1$. La complexité du calcul est élémentaire.

En itérant la représentation de $x \mapsto x + 1$ sur 0, on obtient une représentation de $x \mapsto x$ de conclusion $\vdash \mathbb{N}^\perp, !\mathbb{N}$. Cette preuve ne modifie donc pas l'entier représenté mais agit sur le type, on parle de *coercion*. On a défini c_1 de conclusion $\vdash \mathbb{N}^\perp, !\mathbb{N}$, on peut ensuite définir c_p de conclusion $\vdash \mathbb{N}^\perp, !^p\mathbb{N}$ par $c_{k+1} = !c_k \circ c_1$.

- Pour composer les fonctions de plusieurs arguments, les coercions sont nécessaires. En effet si on a représenté une fonction unaire par π_1 de conclusion $\vdash \mathbb{N}^\perp, !^p\mathbb{N}$ et une fonction binaire par π_2 de conclusion $\vdash \mathbb{N}^\perp, \mathbb{N}^\perp, !^q\mathbb{N}$, pour les composer et obtenir une preuve de conclusion $\vdash \mathbb{N}^\perp, \mathbb{N}^\perp, !^n\mathbb{N}$ on doit passer par :

$$\frac{\frac{\frac{c_p}{\vdash \mathbb{N}^\perp, !^p\mathbb{N}} \quad \frac{\frac{\frac{\pi_1}{\vdash \mathbb{N}^\perp, !^p\mathbb{N}} \quad \frac{\frac{\pi_2}{\vdash \mathbb{N}^\perp, \mathbb{N}^\perp, !^q\mathbb{N}}}{\vdash \mathbb{N}^\perp, \mathbb{N}^\perp, !^{p+q}\mathbb{N}} !f}{\vdash \mathbb{N}^\perp, \mathbb{N}^\perp, !^{p+q}\mathbb{N}} !f}{\vdash \mathbb{N}^\perp, \mathbb{N}^\perp, !^{p+q}\mathbb{N}} cut}{\vdash \mathbb{N}^\perp, \mathbb{N}^\perp, !^{p+q}\mathbb{N}} cut$$

9.2 LLL

Syntaxe

Pour définir LLL, on opère un raffinement supplémentaire en introduisant une nouvelle modalité \S (et son dual $\bar{\S}$ avec $(\S A)^\perp = \bar{\S} A^\perp$ et $(\bar{\S} A)^\perp = \S A^\perp$) que l'on peut considérer comme une forme affaiblie de $!$. Les règles sont :

$$\frac{\vdash \Gamma, \Delta, A}{\vdash ?\Gamma, \bar{\S}\Delta, \S A} \S \quad \frac{\vdash \Pi, A}{\vdash ?\Pi, !A} !f$$

où Π est soit vide soit réduit à une formule. On a également la contraction et l'affaiblissement mais pas de déréluction ni de promotion usuelle.

On obtient un principe de déréluction faible $!A \multimap \S A$. On perd $!A \otimes !B \multimap !(A \otimes B)$ remplacé par $\S A \otimes \S B \multimap \S(A \otimes B)$. Par contre on a $!A \multimap !A \otimes !A$ (contraction) mais pas $\S A \multimap \S A \otimes \S A$.

Les nouvelles étapes clefs d'élimination des coupures sont :

$$\frac{\frac{\frac{\vdash \Pi, A}{\vdash ?\Pi, !A} !f \quad \frac{\vdash A^\perp, \Gamma, \Delta, B}{\vdash ?A^\perp, ?\Gamma, \bar{\S}\Delta, \S B} \S}{\vdash ?\Pi, ?\Gamma, \bar{\S}\Delta, \S B} cut}{\vdash ?\Pi, ?\Gamma, \bar{\S}\Delta, \S B} \S \quad \frac{\vdash \Pi, A \quad \vdash A^\perp, \Gamma, \Delta, B}{\vdash \Pi, \Gamma, \Delta, B} cut}{\vdash ?\Pi, ?\Gamma, \bar{\S}\Delta, \S B} \S \quad \rightsquigarrow$$

$$\frac{\frac{\frac{\vdash \Gamma, \Delta, A}{\vdash ?\Gamma, \bar{\S}\Delta, \S A} \S \quad \frac{\vdash A^\perp, \Gamma', \Delta', B}{\vdash \bar{\S}A^\perp, ?\Gamma', \bar{\S}\Delta', \S B} \S}{\vdash ?\Gamma, ?\Gamma', \bar{\S}\Delta, \bar{\S}\Delta', \S B} cut}{\vdash ?\Gamma, ?\Gamma', \bar{\S}\Delta, \bar{\S}\Delta', \S B} \S \quad \frac{\vdash \Gamma, \Delta, A \quad \vdash A^\perp, \Gamma', \Delta', B}{\vdash \Gamma, \Gamma', \Delta, \Delta', B} cut}{\vdash ?\Gamma, ?\Gamma', \bar{\S}\Delta, \bar{\S}\Delta', \S B} \S \quad \rightsquigarrow$$

les étapes $!/?w$, $!/?c$ et $!/!$ étant contraintes du fait que la règle $!f$ a au plus une formule de contexte.

La syntaxe de réseaux de preuve associée utilise les nouvelles sortes de nœuds suivantes :

- sorte \S : une prémisses, une conclusion, si l'étiquette de la prémisses est A alors celle de la conclusion est $\S A$
- sorte $\bar{\S}p$: une prémisses, une conclusion, si l'étiquette de la prémisses est A alors celle de la conclusion est $\bar{\S}A$

avec des boîtes pour chaque nœud de sorte \S ayant un nombre arbitraire de nœuds de sortes $?p$ et $\bar{\S}p$ comme portes auxiliaires et des boîtes pour chaque nœud de sorte $!$ avec au plus une porte auxiliaire qui, de plus, doit être de sorte $?p$.

Remarque : En remplaçant \S par $!$, on transforme toute preuve de LLL en une preuve de ELL et de plus on simule la réduction (une étape par une étape).

Ces réseaux LLL vérifient la même propriété de stratification que les réseaux de ELL. De plus, la réduction d'une coupure exponentielle ($?/!$) ne peut pas donner de coupure \S ni multiplicative à profondeur 0 et la réduction d'une coupure \S ne peut pas donner de coupure multiplicative à profondeur 0 (ni exponentielle d'ailleurs). On peut donc réduire profondeur par profondeur (en profondeurs croissantes) en prenant d'abord les réductions multiplicatives puis les réductions \S et enfin les réductions exponentielles. On sait déjà grâce au cas ELL, que la réduction à profondeur 0 de \mathcal{R} nécessite au plus $|\mathcal{R}|$ étapes.

Dans un réseau \mathcal{R} avec uniquement des coupures exponentielles, on définit le poids w_n d'un nœud n par :

- si n est un nœud $!$ à profondeur 0 alors soit k le nombre de nœuds $?c$ tels qu'il existe un chemin (sans rebond à profondeur 0 partant en descendant dans la conclusion) qui arrive à n , soit x la taille du réseau à l'intérieur de la boîte, et soit p le nombre de portes auxiliaires de la boîte, on prend $w_n = (k + 1)(x + p + 1)$,
- si n est un nœud $?p$ ou cut à profondeur 0, $w_n = 0$,
- si n est un autre nœud à profondeur 0, $w_n = 1$,
- sinon $w_n = 0$.

et on définit $w_{\mathcal{R}} = \sum_{n \in \mathcal{R}} w_n$.

Lors de la réduction, les étapes multiplicatives et \S font diminuer la taille du réseau, puis les étapes exponentielles font décroître (au sens large) $w_{\mathcal{R}}$. De plus, pour tout réseau avec coupures exponentielles uniquement $w_{\mathcal{R}} \leq |\mathcal{R}|^2$:

$$\begin{aligned}
w_{\mathcal{R}} &\leq |\mathcal{R}|_{nb} + \sum_{\substack{n \text{ nœud } ! \\ \text{à profondeur } 0}} (k_n + 1)(x_n + p_n + 1) \\
&\leq |\mathcal{R}|_{nb} + \sum_{\substack{n \text{ nœud } ! \\ \text{à profondeur } 0}} (|\mathcal{R}|_{nb} + 1)(x_n + p_n + 1) \\
&\leq |\mathcal{R}|_{nb} + (|\mathcal{R}|_{nb} + 1) \sum_{\substack{n \text{ nœud } ! \\ \text{à profondeur } 0}} x_n + p_n + 1 \\
&\leq |\mathcal{R}|_{nb} + (|\mathcal{R}|_{nb} + 1)|\mathcal{R}|_b \\
&\leq (|\mathcal{R}|_{nb} + |\mathcal{R}|_b)^2 = |\mathcal{R}|^2
\end{aligned}$$

où $|\mathcal{R}|_{nb}$ est le nombre de nœuds ni $!$ ni $?p$ à profondeur 0 et $|\mathcal{R}|_b$ est le nombre total d'autres nœuds dans \mathcal{R} . Par ailleurs, pour un réseau sans coupure à profondeur 0, $w_{\mathcal{R}} = |\mathcal{R}|$. On en déduit qu'après réduction à profondeur 0 la taille du réseau \mathcal{R}' obtenu est majorée par $|\mathcal{R}|^2$ ($|\mathcal{R}'| = w_{\mathcal{R}'} \leq w_{\mathcal{R}} \leq |\mathcal{R}|^2$).

Le nombre d'étapes pour éliminer complètement les coupures dans un réseau \mathcal{R} de profondeur d est donc un polynôme en $|\mathcal{R}|$ de degré 2^d (et a une taille majorée par $|\mathcal{R}|^{2^{d+1}}$).

Programmation

Comme pour ELL, il faut trouver un type adapté pour les entiers, c'est ici $\mathbb{N} = \forall X!(X \multimap X) \multimap \S(X \multimap X) = \forall X?(X \otimes X^\perp) \wp \S(X^\perp \wp X)$. La représentation des entiers dans LLL se fait comme dans ELL en remplaçant la règle $!$ par une règle \S .

On peut représenter des fonctions des entiers dans les entiers par des preuves de conclusion $\vdash \mathbb{N}^\perp, \dots, \mathbb{N}^\perp, \S^p \mathbb{N}$. Si on considère le cas unaire et pour un entier $n \neq 0$, on normalise un réseau

Remarque : Dans ce chapitre, on n'a considéré que les fragments multiplicatifs exponentiels (avec quantificateurs) de ELL et LLL. Il est possible d'introduire les connecteurs additifs dans ces systèmes (et c'est même fort utile pour certains codages) mais cela rend leur présentation plus complexe.

Chapitre 10

Polarisation

10.1 Logique linéaire polarisée

On a vu à la [section 5.2](#) que les connecteurs non exponentiels de LL se séparent en deux familles : les connecteurs négatifs \wp , $\&$, \perp et \top (et même \forall) qui sont réversibles et les connecteurs positifs \otimes , \oplus , 1 et 0 (et même \exists) qui vérifient la propriété de focalisation.

On peut également remarquer que si on restreint la traduction de Girard (vue à la [section 7.2](#)) aux connecteurs \rightarrow , \wedge et \top de LJ (qui sont précisément ceux pour lesquels la normalisation dans NJ ne nécessite pas d'étapes commutatives), on n'obtient que des formules négatives à condition de définir la polarité de $!$ comme allant de négatif à positif (et dualement pour $?$).

Si on restreint les formules de LL pour qu'elles respectent ces polarités, on obtient :

$$\begin{array}{l} P ::= X^\perp \mid P \otimes P \mid P \oplus P \mid 1 \mid 0 \mid !N \\ N ::= X \mid N \wp N \mid N \& N \mid \perp \mid \top \mid ?P \end{array}$$

où le choix pour les variables est arbitraire. Ceci contient l'image de la traduction de Girard (restreinte) qui est donc à la fois à image dans ILL et dans ce fragment polarisé LL_{pol} de LL.

Remarque : Tous les isomorphismes que l'on a vus dans LL respectent la polarisation (*i.e.* ne font intervenir que des interactions entre connecteurs qui sont correctement polarisées). Par exemple : $!(N \& M) = !N \otimes !M$.

Lemme 23 (Formule positive)

Si $\vdash \Gamma$ est prouvable dans le fragment polarisé de LL sans la règle \top alors Γ contient au plus une formule positive.

DÉMONSTRATION : Par récurrence sur la taille de la preuve. □

Comme on l'a déjà discuté pour ILL, il est alors naturel de demander que la règle \top introduise au plus une formule positive. On obtient ainsi le système LL_{pol} .

On va voir que les formules polarisées ont des propriétés très particulières vis-à-vis des règles structurelles.

Définition 42 (Formules $!/?$ -fixes)

Une formule A de LL est *!-fixe* (resp. *?-fixe*) si $A \vdash !A$ est dérivable (resp. $?A \vdash A$ est dérivable). Ce qui entraîne que A est *!-fixe* si et seulement si A^\perp est *?-fixe*.

Lemme 24 (Préservation des formules fixes)

On a les propriétés suivantes :

- $!A$, 1 et 0 sont *!-fixes*

- $?A, \perp$ et \top sont $?-fixes$
- si A et B sont $!-fixes$ alors $A \otimes B$ et $A \oplus B$ aussi
- si A et B sont $?-fixes$ alors $A \wp B$ et $A \& B$ aussi

DÉMONSTRATION : On ne traite que le cas des formules $!-fixes$ puisque celui des formules $?-fixes$ est le dual.

Par récurrence sur la taille de la formule :

$$\begin{array}{c}
\frac{\overline{\vdash ?A^\perp, !A} \text{ ax}}{\vdash ?A^\perp, !!A} ! \quad \frac{\overline{\vdash 1} 1}{\vdash !1} !}{\vdash \perp, !1} \perp \quad \frac{}{\vdash \top, !0} \top \\
\\
\frac{\overline{\vdash A^\perp, A} \text{ ax} \quad \overline{\vdash B^\perp, B} \text{ ax}}{\vdash A^\perp, B^\perp, A \otimes B} \otimes}{\vdash ?A^\perp, B^\perp, A \otimes B} ?d}{\vdash ?A^\perp, ?B^\perp, A \otimes B} ?d}{\vdash A^\perp, !A \quad \vdash ?A^\perp, ?B^\perp, !(A \otimes B)} !}{\vdash B^\perp, !B \quad \vdash A^\perp, ?B^\perp, !(A \otimes B)} \text{ cut}}{\vdash A^\perp, B^\perp, !(A \otimes B)} \text{ cut}}{\vdash A^\perp \wp B^\perp, !(A \otimes B)} \wp \\
\\
\frac{\overline{\vdash A^\perp, A} \text{ ax}}{\vdash A^\perp, A \oplus B} \oplus_1}{\vdash ?A^\perp, A \oplus B} ?d}{\vdash A^\perp, !A \quad \vdash ?A^\perp, !(A \oplus B)} !}{\vdash A^\perp, !A \quad \vdash ?A^\perp, !(A \oplus B)} \text{ cut}}{\vdash A^\perp, !(A \oplus B)} \text{ cut}}{\vdash B^\perp, !B \quad \vdash ?B^\perp, !(A \oplus B)} !}{\vdash B^\perp, !B \quad \vdash ?B^\perp, !(A \oplus B)} \text{ cut}}{\vdash A^\perp \& B^\perp, !(A \oplus B)} \&
\end{array}$$

□

Remarque : Il est intéressant de remarquer que la structure de ces preuves est très similaire à celle des preuves utilisées dans le [lemme 1 page 36](#) (dans la mesure où $\neg_R \neg_R A$ et $?A$ se correspondent).

Proposition 37 (Règles structurelles généralisées)

Si A est $?-fixe$ et \mathcal{N} ne contient que des formules $?-fixes$ alors les règles structurelles généralisées suivantes sont dérivables dans **LL** :

$$\frac{\vdash \Gamma}{\vdash \Gamma, A} ?w \quad \frac{\vdash \Gamma, A, A}{\vdash \Gamma, A} ?c \quad \frac{\vdash \mathcal{N}, B}{\vdash \mathcal{N}, !B} !$$

DÉMONSTRATION : En utilisant la preuve de $\vdash !A^\perp, A$ (et de même pour $N \in \mathcal{N}$) :

$$\frac{\frac{\vdash \Gamma}{\vdash \Gamma, ?A} ?w \quad \vdash !A^\perp, A}{\vdash \Gamma, A} \text{ cut}}{\vdash \Gamma, A, A} ?d}{\vdash \Gamma, ?A, ?A} ?c}{\vdash \Gamma, ?A \quad \vdash !A^\perp, A} \text{ cut}}{\vdash \Gamma, A} \text{ cut}$$

$$\frac{\frac{\frac{\vdash \mathcal{N}, B}{\vdash ?\mathcal{N}, B} ?d \quad (N \in \mathcal{N})}{\vdash ?\mathcal{N}, !B} ! \quad \vdash !N^\perp, N}{\vdash \mathcal{N}, !B} cut$$

□

Si on ajoute à LL_{pol} que les variables négatives sont $?$ -fixes, on en déduit que toute formule négative est $?$ -fixe (et que toute formule positive est $!$ -fixe) et que les règles structurelles généralisées sont dérivables pour toute formule négative. Partant de cette idée, le système LLP est défini en ajoutant à LL_{pol} les règles structurelles généralisées :

$$\frac{\vdash \Gamma}{\vdash \Gamma, N} ?w \quad \frac{\vdash \Gamma, N, N}{\vdash \Gamma, N} ?c \quad \frac{\vdash \mathcal{N}, N}{\vdash \mathcal{N}, !N} !$$

où \mathcal{N} ne contient que des formules négatives. Ce qui donne en particulier que toute formule négative est $?$ -fixe et toute formule positive est $!$ -fixe.

Du fait de cette extension des règles structurelles, LLP n'est pas tout à fait un sous-système de LL .

On vérifie facilement que le lemme de la formule positive reste valide dans LLP .

Remarque : Le connecteur $!$ est réversible dans LLP : si $\vdash \Gamma, !A$ est prouvable dans LLP , alors par le lemme de la formule positive Γ ne contient que des formules négatives et on peut dériver :

$$\frac{\frac{\frac{\overline{\vdash A^\perp, A} ax}{\vdash ?A^\perp, A} ?d}{\vdash \Gamma, !A} cut}{\frac{\vdash \Gamma, A}{\vdash \Gamma, !A} !}$$

10.2 Réseaux polarisés

Les structures de preuve pour MELLP (le fragment multiplicatif-exponentiel de LLP) sont les mêmes que pour MELL en contraignant les formules à être polarisées et en autorisant l'affaiblissement, la contraction et les portes auxiliaires de boîtes à porter sur des formules négatives :

- sorte ax : aucune prémisses, deux conclusions, si l'étiquette de la première conclusion est A alors celle de la deuxième est A^\perp
- sorte cut : deux prémisses, aucune conclusion, si l'étiquette de la première prémisses est A alors celle de la deuxième est A^\perp
- sorte \otimes : deux prémisses, une conclusion, si l'étiquette de la première prémisses est P et celle de la deuxième prémisses est Q alors celle de la conclusion est $P \otimes Q$
- sorte \wp : deux prémisses, une conclusion, si l'étiquette de la première prémisses est N et celle de la deuxième prémisses est M alors celle de la conclusion est $N \wp M$
- sorte 1 : aucune prémisses, une conclusion, l'étiquette de la conclusion est 1
- sorte \perp : aucune prémisses, une conclusion, l'étiquette de la conclusion est \perp
- sorte $!$: une prémisses, une conclusion, si l'étiquette de la prémisses est N alors celle de la conclusion est $!N$
- sorte $?p$: une prémisses, une conclusion, la prémisses et la conclusion ont la même étiquette N
- sorte $?d$: une prémisses, une conclusion, si l'étiquette de la prémisses est P alors celle de la conclusion est $?P$
- sorte $?w$: aucune prémisses, une conclusion, l'étiquette de la conclusion est N

- sorte $?c$: deux prémisses, une conclusion, les deux prémisses et la conclusion ont la même étiquette N
- sorte $!_i$ ($i \in \mathbb{N}$) : aucune prémisse, $i+1$ conclusions, la première conclusion a pour étiquette $!N$ (où N peut être une formule négative quelconque) et les autres conclusions ont pour étiquettes des formules N_i (où N_i peut être une formule négative quelconque)

Un *graphe de correction* est obtenu de la manière suivante :

- On considère, soit les nœuds à profondeur 0, soit ceux à profondeur 0 dans une boîte.
- On remplace chaque nœud de sorte $!$ dont la boîte a pour conclusions des arêtes de type $!N, N_1, \dots, N_i$ par un nœud de sorte $!_i$ ayant ces arêtes comme conclusions.

De plus, on oriente désormais les arêtes positives vers le haut et les arêtes négatives vers le bas. On peut remarquer que la somme des tailles des graphes de correction est égale à la taille de la structure de preuve (la complexité du critère va donc être moindre que dans le cas non polarisé).

Une structure de preuve est correcte si :

- chaque graphe de correction est un graphe orienté acyclique
- chaque graphe de correction possède exactement une conclusion positive ou un nœud de sorte $?d$

Une structure de preuve correcte est naturellement munie d'un ordre partiel sur les nœuds (et de même pour les arêtes) par : $n_1 \leq n_2$ s'il existe un chemin orienté allant de n_1 à n_2 dans un graphe de correction.

Définition 43 (Arbre positif)

Un *arbre positif* est une structure de preuve avec une unique conclusion positive définie par récurrence :

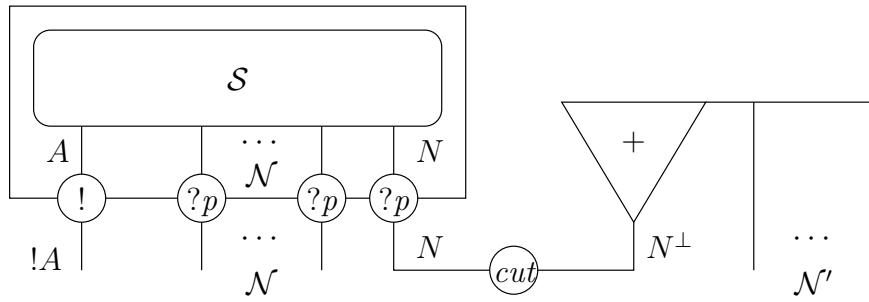
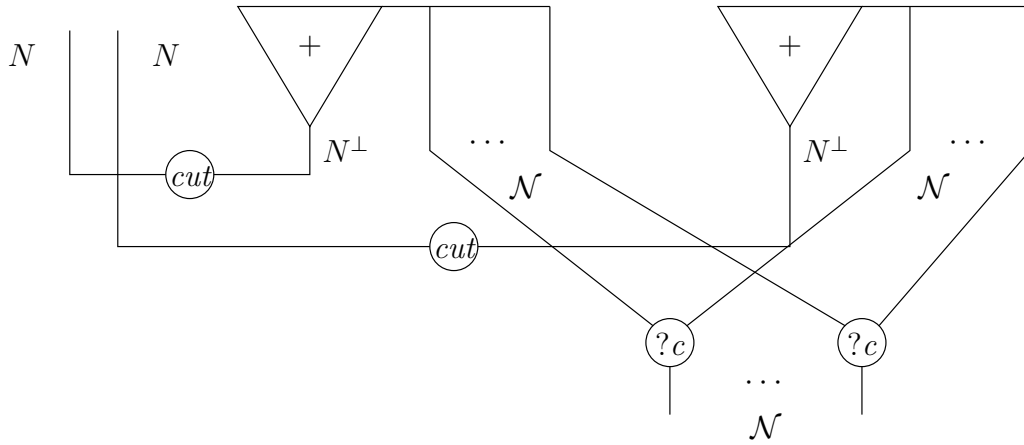
- un nœud ax est un arbre positif,
- une boîte exponentielle est un arbre positif,
- un nœud 1 est un arbre positif,
- en ajoutant un nœud \otimes entre les conclusions positives de deux arbres positifs, on obtient un arbre positif.

Lemme 25 (Royaume positif)

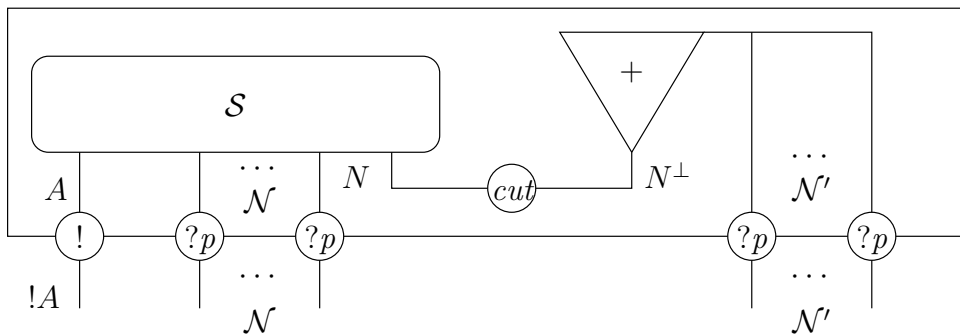
Au-dessus de toute arête positive se trouve un arbre positif, de plus cet arbre positif est le royaume de l'arête (i.e. la plus petite sous-structure de preuve correcte ayant cette arête comme conclusion).

DÉMONSTRATION : Par récurrence sur le nombre de nœuds situés au-dessus de l'arête a concernée (i.e. tels qu'il existe un chemin orienté allant du nœud à l'arête dans la structure de preuve), sachant qu'une arête positive est nécessairement conclusion d'un nœud $ax, 1, \otimes$ ou $!$:

- Si l'arête est conclusion d'un nœud ax , ce nœud ax constitue un arbre positif, est une structure de preuve correcte et toute structure de preuve ayant a comme conclusion contient nécessairement ce nœud.
- Si l'arête est conclusion d'un nœud 1 , ce nœud 1 constitue un arbre positif, est une structure de preuve correcte et toute structure de preuve ayant a comme conclusion contient nécessairement ce nœud.
- Si l'arête est conclusion d'un nœud \otimes de prémisses b et c , par hypothèses de récurrences, b et c sont conclusions d'arbres positifs qui sont leurs royaumes. En ajoutant le nœud \otimes , on obtient encore un arbre positif et ajouter un nœud \otimes entre deux structures de preuve correctes donne une structure de preuve correcte. Enfin, la plus petite structure de preuve correcte ayant a comme conclusion doit nécessairement contenir le nœud \otimes et les royaumes des prémisses, c'est donc cet arbre positif.



↓



Proposition 38 (Préservation de la correction par réduction)

Si la structure de preuve polarisée correcte \mathcal{S} se réduit en \mathcal{S}' alors \mathcal{S}' est correcte.

DÉMONSTRATION : On considère chaque étape de réduction :

- (ax) On raccourcit un chemin ce qui ne peut pas créer de cycle. On ne touche pas aux conclusions positives ni aux nœuds $?d$.
- (\otimes/\wp) On raccourcit des chemins, on en supprime d'autres, on ne touche pas aux conclusions positives ni aux nœuds $?d$.
- ($1/\perp$) On supprime une partie du réseau sans toucher aux conclusions positives ni aux nœuds $?d$.
- ($?d/!$) Dans le réseau réduit, un cycle ne peut pas passer par l'intérieur de la boîte (sans être entièrement à l'intérieur) puisqu'il n'y a que des conclusions négatives (donc des arêtes sortantes). On supprime un nœud $?d$ à profondeur 0 et on en ajoute un qui était à l'intérieur de la boîte.

- (?w/!) On supprime des arêtes ce qui ne peut pas créer de cycle et on ne touche ni aux conclusions positives ni aux nœuds ?d.
- (?c/!) On ne crée pas de nouveau chemin orienté entre les arêtes de la frontière du module réduit (on n'en supprime pas non plus) ce qui ne peut pas créer de cycle. On ne touche ni aux conclusions positives ni aux nœuds ?d.
- (!/!) On raccourcit des chemins ce qui ne peut pas créer de cycle, et on ne touche ni aux conclusions positives ni aux nœuds ?d. \square

On peut définir une traduction des réseaux de MELLP dans les réseaux de MELL en appliquant la transformation suivante sur les formules :

$$\begin{array}{ll}
\overline{X} &= ?X & \overline{X^\perp} &= !X^\perp \\
\overline{N \wp M} &= ?(\overline{N} \wp \overline{M}) & \overline{P \otimes Q} &= !(\overline{P} \otimes \overline{Q}) \\
\overline{N \& M} &= ?(\overline{N} \& \overline{M}) & \overline{P \oplus Q} &= !(\overline{P} \oplus \overline{Q}) \\
\overline{\perp} &= ?\perp & \overline{1} &= !1 \\
\overline{\top} &= ?\top & \overline{0} &= !0 \\
\overline{?P} &= ?\overline{P} & \overline{!N} &= !\overline{N}
\end{array}$$

La traduction des réseaux est obtenue en traduisant les types, en ajoutant un nœud ?d sous chaque arête négative et un nœud ! sous chaque arête positive (avec comme boîte l'arbre positif de cette arête).

Proposition 39 (Injectivité et simulation stricte)

Cette traduction des réseaux de MELLP dans les réseaux de MELL est injective et est une simulation stricte.

Proposition 40 (Normalisation forte)

La réduction des réseaux MELLP est fortement normalisante.

DÉMONSTRATION : En utilisant la normalisation forte des réseaux de MELL et la simulation stricte : si il existait une suite infinie de réductions dans MELLP, par simulation stricte, il en existerait une dans MELL ce qui contredirait la normalisation forte de MELL. \square

Proposition 41 (Confluence)

La réduction des réseaux MELLP est confluente.

DÉMONSTRATION : Si \mathcal{R} se réduit en deux formes normales $\overline{\mathcal{R}}_1$ et $\overline{\mathcal{R}}_2$ alors $\overline{\mathcal{R}}$ se réduit en $\overline{\mathcal{R}}_1$ et en $\overline{\mathcal{R}}_2$ (formes normales). Par confluence de MELL, $\overline{\mathcal{R}}_1 = \overline{\mathcal{R}}_2$ et par l'injectivité de la traduction on en déduit que $\mathcal{R}_1 = \mathcal{R}_2$. \square

10.3 Traduction de NK

On va reprendre la \mathfrak{t} -traduction vue à la [section 7.3](#). Grâce aux règles structurelles généralisées, il est possible de définir cette traduction de NK à image dans LLP en prenant les mêmes définitions que pour la traduction de Girard pour NJ :

$$\begin{aligned}
X^\bullet &= X \\
(A \rightarrow B)^\bullet &= ?A^{\bullet\perp} \wp B^\bullet \\
(\Gamma \vdash \Delta)^\bullet &= \vdash ?\Gamma^{\bullet\perp}, \Delta^\bullet
\end{aligned}$$

en effet cette formulation est équivalente à la précédente dès que A^\bullet est ?-fixe pour toute formule A (ce qui est le cas dans LLP puisque A^\bullet est négative).

Puisque les règles structurelles à gauche peuvent être traduites par les règles structurelles sur des formules ? et les règles structurelles à droite par les règles structurelles généralisées aux formules négatives, la traduction des preuves est donnée par :

$$\begin{array}{c}
\frac{}{A \vdash A} ax \quad \rightsquigarrow \quad \frac{}{\vdash A^{\bullet\perp}, A^\bullet} ax \\
\frac{}{\vdash ?A^{\bullet\perp}, A^\bullet} ?d \\
\\
\frac{\Gamma, A \vdash B, \Delta}{\Gamma \vdash A \rightarrow B, \Delta} \rightarrow_{\text{intro}} \quad \rightsquigarrow \quad \frac{\vdash ?\Gamma^{\bullet\perp}, ?A^{\bullet\perp}, B^\bullet, \Delta^\bullet}{\vdash ?\Gamma^{\bullet\perp}, ?A^{\bullet\perp} \wp B^\bullet, \Delta^\bullet} \wp \\
\\
\frac{\Gamma \vdash A \rightarrow B, \Delta \quad \Gamma' \vdash A, \Delta'}{\Gamma, \Gamma' \vdash B, \Delta, \Delta'} \rightarrow_{\text{elim}} \quad \rightsquigarrow \quad \frac{\frac{\vdash ?\Gamma'^{\bullet\perp}, A^\bullet, \Delta'^\bullet}{\vdash ?\Gamma'^{\bullet\perp}, !A^\bullet, \Delta'^\bullet} ! \quad \frac{}{\vdash B^{\bullet\perp}, B^\bullet} ax}{\vdash ?\Gamma'^{\bullet\perp}, !A^\bullet \otimes B^{\bullet\perp}, B^\bullet, \Delta'^\bullet} \otimes \\
\frac{\vdash ?\Gamma^{\bullet\perp}, ?A^{\bullet\perp} \wp B^\bullet, \Delta^\bullet \quad \vdash ?\Gamma'^{\bullet\perp}, !A^\bullet \otimes B^{\bullet\perp}, B^\bullet, \Delta'^\bullet}{\vdash ?\Gamma^{\bullet\perp}, ?\Gamma'^{\bullet\perp}, B^\bullet, \Delta^\bullet, \Delta'^\bullet} cut
\end{array}$$

ce qui est essentiellement la même chose que pour la traduction de Girard de NJ dans ILL.

Si on regarde cette traduction comme allant du $\lambda\mu$ -calcul dans les réseaux polarisés, on obtient une extension de celle du λ -calcul dans les réseaux de MELL (dont on peut remarquer qu'elle était en fait à image dans MELL_{pol}). La simulation de la réduction est vraie mais n'est plus stricte. Cette traduction du $\lambda\mu$ -calcul dans les réseaux polarisés peut être définie dans un cadre typé mais également dans un cas pur en définissant des *réseaux polarisés purs*.

Remarque : Ainsi les modèles de LLP sont donnés par les catégories de contrôle (en interprétant les formules négatives par des objets, donc des \wp -monoïdes).

Dans le cas de la \mathfrak{q} -traduction, il n'y a pas de simplification immédiate car la partie de cette traduction que l'on a présentée (connecteur \rightarrow) est naturellement polarisée : toute formule de NK est traduite par une formule polarisée. Si on étendait la traduction au connecteur \wedge par exemple, on verrait que le cas polarisé est à nouveau plus simple que celui de LL.

Annexes

Annexe A

Calcul des séquents classique (LK)

A.1 Calcul bilatère

Formules et séquents

Étant donné un langage de termes du premier ordre, les formules sont :

$$A ::= X t_1 \dots t_n \mid \neg A \mid A \wedge A \mid A \vee A \mid A \rightarrow A \mid \mathbf{T} \mid \mathbf{F} \mid \forall x A \mid \exists x A$$

Les séquents sont de la forme $\Gamma \vdash \Delta$.

Règles

Groupe identité multiplicatif.

$$\frac{}{A \vdash A} \text{ax}^{\text{mul}} \qquad \frac{\Gamma \vdash A, \Delta \quad \Gamma', A \vdash \Delta'}{\Gamma, \Gamma' \vdash \Delta, \Delta'} \text{cut}^{\text{mul}}$$

Groupe identité additif.

$$\frac{}{\Gamma, A \vdash A, \Delta} \text{ax}^{\text{add}} \qquad \frac{\Gamma \vdash A, \Delta \quad \Gamma, A \vdash \Delta}{\Gamma \vdash \Delta} \text{cut}^{\text{add}}$$

Groupe structurel.

$$\frac{\Gamma \vdash \Delta}{\sigma(\Gamma) \vdash \tau(\Delta)} \text{ech}$$
$$\frac{\Gamma, A, A \vdash \Delta}{\Gamma, A \vdash \Delta} \text{ctrL} \qquad \frac{\Gamma \vdash A, A, \Delta}{\Gamma \vdash A, \Delta} \text{ctrR}$$
$$\frac{\Gamma \vdash \Delta}{\Gamma, A \vdash \Delta} \text{wkL} \qquad \frac{\Gamma \vdash \Delta}{\Gamma \vdash A, \Delta} \text{wkR}$$

Groupe logique multiplicatif.

$$\begin{array}{c}
\frac{\Gamma \vdash A, \Delta \quad \Gamma' \vdash B, \Delta'}{\Gamma, \Gamma' \vdash A \wedge B, \Delta, \Delta'} \wedge^{\text{mulR}} \qquad \frac{\Gamma, A, B \vdash \Delta}{\Gamma, A \wedge B \vdash \Delta} \wedge^{\text{mulL}} \\
\\
\frac{\Gamma \vdash A, B, \Delta}{\Gamma \vdash A \vee B, \Delta} \vee^{\text{mulR}} \qquad \frac{\Gamma, A \vdash \Delta \quad \Gamma', B \vdash \Delta'}{\Gamma, \Gamma', A \vee B \vdash \Delta, \Delta'} \vee^{\text{mulL}} \\
\\
\frac{}{\vdash \top} \top^{\text{mulR}} \qquad \frac{\Gamma \vdash \Delta}{\Gamma, \top \vdash \Delta} \top^{\text{mulL}} \\
\\
\frac{\Gamma \vdash \Delta}{\Gamma \vdash \text{F}, \Delta} \text{F}^{\text{mulR}} \qquad \frac{}{\text{F} \vdash} \text{F}^{\text{mulL}} \\
\\
\frac{\Gamma, A \vdash \Delta}{\Gamma \vdash \neg A, \Delta} \neg\text{R} \qquad \frac{\Gamma \vdash A, \Delta}{\Gamma, \neg A \vdash \Delta} \neg\text{L} \\
\\
\frac{\Gamma, A \vdash B, \Delta}{\Gamma \vdash A \rightarrow B, \Delta} \rightarrow^{\text{mulR}} \qquad \frac{\Gamma, B \vdash \Delta \quad \Gamma' \vdash A, \Delta'}{\Gamma, \Gamma', A \rightarrow B \vdash \Delta, \Delta'} \rightarrow^{\text{mulL}}
\end{array}$$

Groupe logique additif.

$$\begin{array}{c}
\frac{\Gamma \vdash A, \Delta \quad \Gamma \vdash B, \Delta}{\Gamma \vdash A \wedge B, \Delta} \wedge^{\text{addR}} \qquad \frac{\Gamma, A \vdash \Delta}{\Gamma, A \wedge B \vdash \Delta} \wedge^{\text{addL}_1} \qquad \frac{\Gamma, B \vdash \Delta}{\Gamma, A \wedge B \vdash \Delta} \wedge^{\text{addL}_2} \\
\\
\frac{\Gamma \vdash A, \Delta}{\Gamma \vdash A \vee B, \Delta} \vee^{\text{addR}_1} \qquad \frac{\Gamma \vdash B, \Delta}{\Gamma \vdash A \vee B, \Delta} \vee^{\text{addR}_2} \qquad \frac{\Gamma, A \vdash \Delta \quad \Gamma, B \vdash \Delta}{\Gamma, A \vee B \vdash \Delta} \vee^{\text{addL}} \\
\\
\frac{}{\Gamma \vdash \top, \Delta} \top^{\text{addR}} \qquad \frac{}{\Gamma, \text{F} \vdash \Delta} \text{F}^{\text{addL}} \\
\\
\frac{\Gamma, A \vdash \Delta}{\Gamma \vdash \neg A, \Delta} \neg\text{R} \qquad \frac{\Gamma \vdash A, \Delta}{\Gamma, \neg A \vdash \Delta} \neg\text{L} \\
\\
\frac{\Gamma, A \vdash \Delta}{\Gamma \vdash A \rightarrow B, \Delta} \rightarrow^{\text{addR}_1} \qquad \frac{\Gamma \vdash B, \Delta}{\Gamma \vdash A \rightarrow B, \Delta} \rightarrow^{\text{addR}_2} \qquad \frac{\Gamma \vdash A, \Delta \quad \Gamma, B \vdash \Delta}{\Gamma, A \rightarrow B \vdash \Delta} \rightarrow^{\text{addL}}
\end{array}$$

Groupe logique quantification.

$$\begin{array}{c}
\frac{\Gamma \vdash A, \Delta}{\Gamma \vdash \forall x A, \Delta} \forall\text{R} \qquad \frac{\Gamma, A^{[t/x]} \vdash \Delta}{\Gamma, \forall x A \vdash \Delta} \forall\text{L} \\
\\
\frac{\Gamma \vdash A^{[t/x]}, \Delta}{\Gamma \vdash \exists x A, \Delta} \exists\text{R} \qquad \frac{\Gamma, A \vdash \Delta}{\Gamma, \exists x A \vdash \Delta} \exists\text{L}
\end{array}$$

avec la contrainte que x ne doit pas être libre dans Γ ni Δ pour les règles $\forall\text{R}$ et $\exists\text{L}$.

A.2 Calcul monolatère

Formules et séquents

Étant donné un langage de termes du premier ordre, les formules sont :

$$A ::= Xt_1 \dots t_n \mid \neg Xt_1 \dots t_n \mid A \wedge A \mid A \vee A \mid \mathbf{T} \mid \mathbf{F} \mid \forall x A \mid \exists x A$$

Les séquents sont de la forme $\vdash \Gamma$.

Règles

$$\begin{array}{c}
 \frac{}{\vdash A, \neg A} \text{ax} \qquad \frac{\vdash \Gamma, A \quad \vdash \Delta, \neg A}{\vdash \Gamma, \Delta} \text{cut} \\
 \\
 \frac{\vdash \Gamma, A, A}{\vdash \Gamma, A} \text{ctr} \qquad \frac{\vdash \Gamma}{\vdash \Gamma, A} \text{wk} \\
 \\
 \frac{\vdash \Gamma, A \quad \vdash \Delta, B}{\vdash \Gamma, \Delta, A \wedge B} \wedge^{\text{mul}} \qquad \frac{\vdash \Gamma, A, B}{\vdash \Gamma, A \vee B} \vee^{\text{mul}} \\
 \\
 \frac{\vdash \Gamma, A \quad \vdash \Gamma, B}{\vdash \Gamma, A \wedge B} \wedge^{\text{add}} \qquad \frac{\vdash \Gamma, A}{\vdash \Gamma, A \vee B} \vee_1^{\text{add}} \qquad \frac{\vdash \Gamma, B}{\vdash \Gamma, A \vee B} \vee_2^{\text{add}} \\
 \\
 \frac{}{\vdash \mathbf{T}} \mathbf{T}^{\text{mul}} \qquad \frac{\vdash \Gamma}{\vdash \Gamma, \mathbf{F}} \mathbf{F}^{\text{mul}} \qquad \frac{}{\vdash \Gamma, \mathbf{T}} \mathbf{T}^{\text{add}} \\
 \\
 \frac{\vdash \Gamma, A}{\vdash \Gamma, \forall x A} \forall \qquad \frac{\vdash \Gamma, A[t/x]}{\vdash \Gamma, \exists x A} \exists
 \end{array}$$

avec la contrainte que x ne doit pas être libre dans Γ pour la règle \forall .

Annexe B

Calcul des séquents intuitionniste (LJ)

Formules et séquents

Étant donné un langage de termes du premier ordre, les formules sont :

$$A ::= Xt_1 \dots t_n \mid A \wedge A \mid A \vee A \mid A \rightarrow A \mid \mathbf{T} \mid \mathbf{F} \mid \neg A \mid \forall x A \mid \exists x A$$

Les séquents sont de la forme $\Gamma \vdash A$.

Règles

$$\begin{array}{c} \frac{}{A \vdash A} \text{ax} \qquad \frac{\Gamma \vdash A \quad \Delta, A \vdash C}{\Gamma, \Delta \vdash C} \text{cut} \\ \\ \frac{\Gamma, A, A \vdash C}{\Gamma, A \vdash C} \text{ctrL} \qquad \frac{\Gamma \vdash C}{\Gamma, A \vdash C} \text{wkL} \\ \\ \frac{\Gamma \vdash A \quad \Gamma \vdash B}{\Gamma \vdash A \wedge B} \wedge^{\text{addR}} \qquad \frac{\Gamma, A \vdash C}{\Gamma, A \wedge B \vdash C} \wedge^{\text{addL}_1} \qquad \frac{\Gamma, B \vdash C}{\Gamma, A \wedge B \vdash C} \wedge^{\text{addL}_2} \\ \\ \frac{\Gamma \vdash A}{\Gamma \vdash A \vee B} \vee^{\text{addR}_1} \qquad \frac{\Gamma \vdash B}{\Gamma \vdash A \vee B} \vee^{\text{addR}_2} \qquad \frac{\Gamma, A \vdash C \quad \Gamma, B \vdash C}{\Gamma, A \vee B \vdash C} \vee^{\text{addL}} \\ \\ \frac{}{\Gamma \vdash \mathbf{T}} \mathbf{T}^{\text{addR}} \qquad \frac{}{\Gamma, \mathbf{F} \vdash C} \mathbf{F}^{\text{addL}} \\ \\ \frac{\Gamma, A \vdash B}{\Gamma \vdash A \rightarrow B} \rightarrow^{\text{mul R}} \qquad \frac{\Gamma, B \vdash C \quad \Delta \vdash A}{\Gamma, \Delta, A \rightarrow B \vdash C} \rightarrow^{\text{mul L}} \\ \\ \frac{\Gamma, A \vdash \mathbf{F}}{\Gamma \vdash \neg A} \neg\text{R} \qquad \frac{\Gamma \vdash A}{\Gamma, \neg A \vdash \mathbf{F}} \neg\text{L} \\ \\ \frac{\Gamma \vdash A}{\Gamma \vdash \forall x A} \forall\text{R} \qquad \frac{\Gamma, A[t/x] \vdash C}{\Gamma, \forall x A \vdash C} \forall\text{L} \qquad \frac{\Gamma \vdash A[t/x]}{\Gamma \vdash \exists x A} \exists\text{R} \qquad \frac{\Gamma, A \vdash C}{\Gamma, \exists x A \vdash C} \exists\text{L} \end{array}$$

avec x non libre dans Γ pour la règle $\forall\text{R}$ et dans Γ et C pour la règle $\exists\text{L}$.

Annexe C

Calcul des séquents linéaire (LL)

C.1 Calcul bilatère

Formules et séquents

Étant donné un langage de termes du premier ordre, les formules sont :

$$A ::= X t_1 \dots t_n \mid A \wp A \mid A \& A \mid \perp \mid \top \mid ?A \mid \forall x A \\ \mid A^\perp \mid A \otimes A \mid A \oplus A \mid 1 \mid 0 \mid !A \mid \exists x A$$

Les séquents sont de la forme $\Gamma \vdash \Delta$.

Règles

Groupe identité.

$$\frac{}{A \vdash A} ax \qquad \frac{\Gamma \vdash A, \Delta \quad \Gamma', A \vdash \Delta'}{\Gamma, \Gamma' \vdash \Delta, \Delta'} cut$$

Groupe négation.

$$\frac{\Gamma, A \vdash \Delta}{\Gamma \vdash A^\perp, \Delta} (\cdot)^\perp R \qquad \frac{\Gamma \vdash A, \Delta}{\Gamma, A^\perp \vdash \Delta} (\cdot)^\perp L$$

Groupe multiplicatif.

$$\frac{\Gamma \vdash A, \Delta \quad \Gamma' \vdash B, \Delta'}{\Gamma, \Gamma' \vdash A \otimes B, \Delta, \Delta'} \otimes R \qquad \frac{\Gamma, A, B \vdash \Delta}{\Gamma, A \otimes B \vdash \Delta} \otimes L \\ \frac{\Gamma \vdash A, B, \Delta}{\Gamma \vdash A \wp B, \Delta} \wp R \qquad \frac{\Gamma, A \vdash \Delta \quad \Gamma', B \vdash \Delta'}{\Gamma, \Gamma', A \wp B \vdash \Delta, \Delta'} \wp L \\ \frac{}{\vdash 1} 1R \qquad \frac{\Gamma \vdash \Delta}{\Gamma, 1 \vdash \Delta} 1L \\ \frac{\Gamma \vdash \Delta}{\Gamma \vdash \perp, \Delta} \perp R \qquad \frac{}{\perp \vdash} \perp L$$

Groupe additif.

$$\begin{array}{c}
\frac{\Gamma \vdash A, \Delta \quad \Gamma \vdash B, \Delta}{\Gamma \vdash A \& B, \Delta} \&R \qquad \frac{\Gamma, A \vdash \Delta}{\Gamma, A \& B \vdash \Delta} \&L_1 \qquad \frac{\Gamma, B \vdash \Delta}{\Gamma, A \& B \vdash \Delta} \&L_2 \\
\frac{\Gamma \vdash A, \Delta}{\Gamma \vdash A \oplus B, \Delta} \oplus R_1 \qquad \frac{\Gamma \vdash B, \Delta}{\Gamma \vdash A \oplus B, \Delta} \oplus R_2 \qquad \frac{\Gamma, A \vdash \Delta \quad \Gamma, B \vdash \Delta}{\Gamma, A \oplus B \vdash \Delta} \oplus L \\
\frac{}{\Gamma \vdash \top, \Delta} \top R \qquad \frac{}{\Gamma, 0 \vdash \Delta} 0L
\end{array}$$

Groupe exponentiel.

$$\begin{array}{c}
\frac{\Gamma \vdash A, \Delta}{\Gamma \vdash ?A, \Delta} ?R \qquad \frac{! \Gamma, A \vdash ? \Delta}{! \Gamma, ?A \vdash ? \Delta} ?L \\
\frac{! \Gamma \vdash A, ? \Delta}{! \Gamma \vdash !A, ? \Delta} !R \qquad \frac{\Gamma, A \vdash \Delta}{\Gamma, !A \vdash \Delta} !L \\
\frac{\Gamma \vdash ?A, ?A, \Delta}{\Gamma \vdash ?A, \Delta} ctrR \qquad \frac{\Gamma, !A, !A \vdash \Delta}{\Gamma, !A \vdash \Delta} ctrL \\
\frac{\Gamma \vdash \Delta}{\Gamma \vdash ?A, \Delta} wkR \qquad \frac{\Gamma \vdash \Delta}{\Gamma, !A \vdash \Delta} wkL
\end{array}$$

Groupe quantification.

$$\begin{array}{c}
\frac{\Gamma \vdash A, \Delta}{\Gamma \vdash \forall x A, \Delta} \forall R \qquad \frac{\Gamma, A[t/x] \vdash \Delta}{\Gamma, \forall x A \vdash \Delta} \forall L \\
\frac{\Gamma \vdash A[t/x], \Delta}{\Gamma \vdash \exists x A, \Delta} \exists R \qquad \frac{\Gamma, A \vdash \Delta}{\Gamma, \exists x A \vdash \Delta} \exists L
\end{array}$$

avec la contrainte que x ne doit pas être libre dans Γ ni Δ pour les règles $\forall R$ et $\exists L$.

C.2 Calcul monolatère

Formules et séquents

Étant donné un langage de termes du premier ordre, les formules sont :

$$A ::= X t_1 \dots t_n \mid A \wp A \mid A \& A \mid \perp \mid \top \mid ?A \mid \forall x A \\ \mid X^\perp t_1 \dots t_n \mid A \otimes A \mid A \oplus A \mid 1 \mid 0 \mid !A \mid \exists x A$$

Les séquents sont de la forme $\vdash \Gamma$.

Règles

Groupe identité.

$$\frac{}{\vdash A^\perp, A} ax \qquad \frac{\vdash \Gamma, A \quad \vdash \Delta, A^\perp}{\vdash \Gamma, \Delta} cut$$

Groupe multiplicatif.

$$\frac{\vdash \Gamma, A \quad \vdash \Delta, B}{\vdash \Gamma, \Delta, A \otimes B} \otimes \qquad \frac{\vdash \Gamma, A, B}{\vdash \Gamma, A \wp B} \wp \\ \frac{}{\vdash 1} 1 \qquad \frac{\vdash \Gamma}{\vdash \Gamma, \perp} \perp$$

Groupe additif.

$$\frac{\vdash \Gamma, A \quad \vdash \Gamma, B}{\vdash \Gamma, A \& B} \& \qquad \frac{\vdash \Gamma, A}{\vdash \Gamma, A \oplus B} \oplus_1 \qquad \frac{\vdash \Gamma, B}{\vdash \Gamma, A \oplus B} \oplus_2 \\ \frac{}{\vdash \Gamma, \top} \top$$

Groupe exponentiel.

$$\frac{\vdash \Gamma, A}{\vdash \Gamma, ?A} ?d \qquad \frac{\vdash ?\Gamma, A}{\vdash ?\Gamma, !A} ! \qquad \frac{\vdash \Gamma, ?A, ?A}{\vdash \Gamma, ?A} ?c \qquad \frac{\vdash \Gamma}{\vdash \Gamma, ?A} ?w$$

Groupe quantification.

$$\frac{\vdash \Gamma, A}{\vdash \Gamma, \forall x A} \forall \qquad \frac{\vdash \Gamma, A[t/x]}{\vdash \Gamma, \exists x A} \exists$$

avec la contrainte que x ne doit pas être libre dans Γ pour la règle \forall .

Table des matières

I	Une introduction	3
	Présentation de la notion de séquent	5
	Quelques preuves formalisées dans une théorie avec axiomes	5
	Catalogue de règles de dérivation avec séquents	8
	Correction des règles	8
	Zoologie des règles	9
II	Logiques classique et intuitionniste	11
1	Calcul des séquents	13
1.1	Calcul des séquents classique (LK)	13
	Calcul des séquents propositionnel	13
	Calcul des séquents du 1 ^{er} ordre	15
	Symétries, équivalences de connecteurs,	16
	Calcul des séquents monolatère	18
	Réversibilité / irréversibilité	19
1.2	Élimination des coupures	20
	Cas clefs	20
	Additif / multiplicatif	21
	Preuve de l'élimination des coupures	22
	Sous-formules, non contradiction	24
	Expansion des axiomes	24
	Calcul des séquents réversible sans coupure	25
	Renversement	25
	Théorème de Herbrand	26
	Dynamique non déterministe	29
1.3	Calcul des séquents intuitionniste (LJ)	30
	Restriction "exactement une formule à droite"	30
	Compatibilité de l'élimination des coupures	31
	Propriété de la disjonction et de l'existentiel	31
	Perte de symétrie et d'équivalence de connecteurs	31
	Restriction "au plus une formule à droite"	31
	Logique minimale	32
	$\neg\neg$ -traduction "brutale"	32
	$\neg\neg$ -traduction "optimisée" (Gödel)	36
	Traduction de Lafont–Reus–Streicher	39
	Simulations de l'élimination des coupures	42

2	Déduction naturelle	43
2.1	Logique intuitionniste (NJ)	43
	Présentation arborescente	43
	Présentations en séquents	44
	Équivalence des différentes présentations	45
	Rédex et normalisation	45
	Traduction de NJ dans LJ	48
	Simulation de la réduction par la traduction	49
	Traduction de LJ dans NJ	50
	Simulation	51
2.2	Logique classique (NK)	52
	Ajout de la règle d'absurde	52
	Présentation avec séquents à conclusions multiples	52
	Rédex et normalisation	53
3	Curry-Howard	55
3.1	Systèmes de typage du λ -calcul	55
	λ -calcul	55
	λ -calcul simplement typé additif	55
	λ -calcul simplement typé multiplicatif	55
	Isomorphisme de Curry-Howard	56
	Extension à la logique intuitionniste propositionnelle	57
	Système \mathcal{F} (à la Church)	58
	Construction du $\lambda\mu$ -calcul simplement typé	59
	$\lambda\mu$ -calcul pur	60
3.2	CPS-traductions	62
	CPS-traduction issue de la $\neg\neg$ -traduction brutale	62
	CPS-traduction issue de la traduction de Lafont–Reus–Streicher	63
	Interprétation calculatoire	69
4	Sémantique catégorique	71
4.1	Notions catégoriques élémentaires	71
4.2	Catégories cartésiennes fermées	73
	Définitions	73
	Interprétation du λ -calcul	75
	Le modèle ensembliste	76
4.3	Catégories monoïdales	77
4.4	Catégories de contrôle	80
	Définition	80
	Interprétation du $\lambda\mu$ -calcul	81
III	Logique linéaire	83
5	Calcul des séquents	85
5.1	Règles	85
	Connecteurs multiplicatifs et additifs	85
	Élimination des coupures	87
	Connecteurs exponentiels	87
	Éléments neutres	88

	Expansion des axiomes	89
5.2	Réversibilité et focalisation	90
5.3	Logique Linéaire Intuitionniste (ILL)	91
	Logique linéaire intuitionniste stricte (sILL)	92
6	Réseaux de preuve	95
6.1	MLL	95
	Structures de preuve	95
	Critère de correction	98
	Élimination des coupures	103
	Éléments neutres	104
6.2	MELL	106
	Structures de preuve exponentielles	106
	Élimination des coupures	108
	Nœuds ? généralisés	112
6.3	Autres connecteurs	114
	Quantificateurs	114
	Additifs	114
7	Traductions des logiques intuitionniste et classique	115
7.1	Squelettes	115
	LL	115
	ILL	116
7.2	Logique intuitionniste	117
	Traduction de Girard	117
	Seconde traduction de Girard	118
	Traduction du λ -calcul dans les réseaux	119
7.3	Logique classique	124
	La τ -traduction	124
	La q -traduction	125
8	Modèles	127
8.1	Sémantique catégorique	127
	Catégories de Seely	127
	Interprétation de LL	129
8.2	Orthogonalité	131
	Orthogonalité ensembliste	131
	Orthogonalité catégorique	131
	Catégorie d'orthogonalité	133
8.3	Modèle relationnel	135
8.4	Modèle cohérent	138
	Espaces cohérents	138
	Catégorie $\mathbb{C}oh$	140
	Orthogonalité de cohérence	140
8.5	Géométrie de l'interaction	141

9	Complexité	147
9.1	ELL	147
	Syntaxe	147
	Programmation	148
9.2	LLL	151
	Syntaxe	151
	Programmation	152
10	Polarisation	155
10.1	Logique linéaire polarisée	155
10.2	Réseaux polarisés	157
10.3	Traduction de NK	161
A	Calcul des séquents classique (LK)	165
A.1	Calcul bilatère	165
	Formules et séquents	165
	Règles	165
A.2	Calcul monolatère	167
	Formules et séquents	167
	Règles	167
B	Calcul des séquents intuitionniste (LJ)	169
	Formules et séquents	169
	Règles	169
C	Calcul des séquents linéaire (LL)	171
C.1	Calcul bilatère	171
	Formules et séquents	171
	Règles	171
C.2	Calcul monolatère	173
	Formules et séquents	173
	Règles	173