Théorie de la démonstration

Pierre-Louis Curien (CNRS and University Paris 7)

cours M2 LMFI, 2009

Quelques lectures

- Olivier Laurent : Théorie de la démonstration, `http://perso.ens-lyon.fr/olivier.laurent/` (Divers)
- “Proofs and types”, J.-Y. Girard, Y. Lafont, P. Taylor, Cambridge University Press
- Pierre-Louis Curien : Introduction to linear logic and ludics, part I and part II `http://www.pps.jussieu.fr/~curien`

et aussi

- “Le point aveugle I et II”, J.-Y. Girard, Editions Hermann
- “Proof theory and automated deduction”, J. Goubault-Larrecq, I. Mackie, Kluwer
- G. Dowek, Introduction to proof theory, Démonstration automatique, Théorie des types `http://www.lix.polytechnique.fr/~dowek/cours.html`
- D. Miller, Proof search and computation `http://www.lix.polytechnique.fr/Labo/Dale.Miller/mpri/mono-jan-2009.pdf`

Objet fondamental d’étude du cours

Etude formelle des preuves (construction, transformations).

Description des preuves dans des **langages de preuves** (termes ou graphes)
Lecture de ces termes de preuves comme fonctions, ou programmes (isomorphisme de Curry-Howard)

Principaux systèmes de preuves : Hilbert, déduction naturelle, **calcul des séquents**

Principales logiques : **classique**, intuitionniste, **linéaire**

Sémantiques opérationnelle (élimination des coupures) et dénotationnelle (cohérente, obervationnellement séquentielle). Sémantique non typée (ludique).

Nous nous concentrerons sur les aspects purement propositionnels (sauf prélude).

Structure du cours

Le cours est en quatre parties :

- Première partie (ce fichier) : logique classique
- Deuxième partie : logique linéaire. Calcul des séquents, élimination des coupures, sémantique des phases, indécidabilité, réseaux de preuves, sémantique cohérente. Les sources principales sont mon Introduction to linear logic and ludics, part I (moins les aspects catégoriques de la dernière section) and part II (première section, sur les réseaux de preuves)
- Troisième partie. Sémantique séquentielle observable / bistable / de jeux pour la logique linéaire intuitionniste. La source est :
  - Pierre-Louis Curien, Sequential algorithms as bistable maps (sur ma page web)
- Quatrième partie : ludique. Les sources principales sont les deux articles suivants (`http://www.kurims.kyoto-u.ac.jp/~terui`) :
  - Kazushige Terui, Computational ludics
  - Michele Basaldella and Kazushige Terui, On the meaning of logical completeness

NB : Pour les parties 2 à 4, des transparents de liaison et de motivation arrivent !

Structure de la première partie

- Chapitre 1 : les bases. Le calcul des séquents LK de Genzen, non-déterminisme / confluence de LK. Complétude de LK.
- Chapitre 2 : une solution pour rendre l'élimination des coupures confluente : la logique classique polarisée et focalisée LKQ, et sa syntaxe de preuves confluente. Complétude de LKQ (par rapport à LK). Traduction vers la logique intuitionniste.
- Chapitre 3 : une version quotientée, fortementent focalisée de LKQ, LKQS. Complétude de LKQS (par rapport à LKQ).
- Chapitre 4 : traductions de divers lambda-calculs vers LKQ. Utilité d'une version faiblement polarisée LK_{pol} de LKQ.

Chapitre I

La logique classique propositionnelle

Styles de déduction (systèmes, règles)

Complétude du calcul des séquents

Elimination des coupures

Paire critique de Lafont

Prélude : raisonnement équationnel

On se donne une syntaxe de termes :

$$t ::= 0 \parallel St \parallel t + t$$

On se donne des axiomes (pour l'addition) :

$$\frac{}{\vdash t + 0 = t} \qquad \frac{}{\vdash t_1 + St_2 = S(t_1 + t_2)}$$

Et des règles d'inférence telles que :

$$\frac{\vdash t_1 = t_2 \quad \vdash t_2 = t_3}{\vdash t_1 = t_3} \qquad \frac{\vdash t_1 = t_2}{\vdash St_1 = St_2}$$

On peut alors construire des **arbres de preuve** :

$$\frac{\dfrac{}{t_1 + SSt_2 = S(t_1 + St_2)} \qquad \dfrac{\dfrac{}{t_1 + St_2 = S(t_1 + t_2)}}{S(t_1 + St_2) = SS(t_1 + t_2)}}{\vdash t_1 + SSt_2 = SS(t_1 + t_2)}$$

Les règles d'inférence ont des hypothèses et une conclusion. Les axiomes sont les règles d'inférence sans hypothèse.
Le symbole $\vdash$, qui ne sert encore à rien (patience), est prononcé “thèse”.

Dérivé versus admissible

Une règle **dérivée** est une “macro” obtenue par un assemblage fini des règles d’inférence. Par exemple

$$\frac{}{\vdash t_1 + SSt_2 = SS(t_1 + t_2)}$$

est un axiome dérivé. On n’a pas besoin de rentrer dans la structure de t_1, t_2 pour l’établir.

Mais l’égalité $t_1+t_2 = t_2+t_1$ n’est pas prouvable avec les axiomes donnés plus haut par une combinaison finie de règles indépendante de la structure de t_1, t_2. Par contre, pour tous t_1, t_2 l’égalité est prouvable (on ajoute la règle de symétrie de l’égalité et on montre que, disons, $t_1 + t_2$ et $t_2 + t_1$ sont tous deux égaux à $SSS0$, pour $t_1 = SS0$, $t_2 = S0$). Pour chaque choix de t_1, t_2 la preuve est différente, et peut devenir arbitrairement longue. On prouve en fait *par récurrence* que $\vdash t_1 + t_2 = t_2 + t_1$ est prouvable pour tous t_1, t_2 (il faut aussi prouver, par récurrence itou, sur la structure de t, que tout t est égal à un terme de la forme S^n0).

On dit que $\vdash t_1 + t_2 = t_2 + t_1$ est une égalité **admissible**.

Langage objet versus méta-langage

La théorie de la démonstration étudie les preuves comme n'importe quel autre objet mathématique. On ne se prive pas d'utiliser le raisonnement mathématique pour les étudier, et en utilisant le cas échéant des principes de raisonnement qui ne sont pas formalisés dans la logique étudiée.

En termes informatiques, on utilise le méta-langage pour étudier une partie des mathématiques formalisée dans un *langage objet*. On peut aussi formaliser le métalangage, regarder exactement quels principes on a utilisés pour étudier le langage objet. Par exemple, ici, notre métalangage contient le principe de récurrence.

Nous ne jouerons pas trop à ce jeu, qui peut être utile dans un sujet appelé "reverse mathematics", où on essaie de démonter des preuves pour savoir "quelle est la logique la plus faible dans laquelle elle peut se formaliser", et qui est évidemment nécessaire si l'on veut formaliser les preuves du cours dans un système comme Coq. Dans ce cours, le méta-langage, c'est "les maths".

Soulignons seulement que nous ferons sans cesse des preuves par récurrence (sur la structure des formules, sur la structure des preuves,...).

Systèmes à la Hilbert

La première présentation formelle des preuves, avant la déduction naturelle et le calcul des séquents (tous deux dus à Gentzen, début des années 1930), est attribuée à Hilbert. Il y a dans cette présentaiton un certain nombre d'axiomes, et une unique règle d'inférence, appelée modus ponens (MP) :

$$\frac{A \Rightarrow B \qquad A}{B}$$

Les axiomes ne sont pas très naturels (il est en particulier difficile de se convaincre qu'il y en a assez !). Par exemple, les deux axiomes pour l'implication sont

$$\frac{}{A \Rightarrow (B \Rightarrow A)} \qquad \frac{}{(A \Rightarrow (B \Rightarrow C)) \Rightarrow ((A \Rightarrow B) \Rightarrow (A \Rightarrow C))}$$

La formule plus simple $A \Rightarrow A$ en est conséquence (prendre $C ::= A, B ::= B \Rightarrow A$ dans le second axiome) :

$$\frac{\dfrac{\dfrac{}{(A \Rightarrow ((B \Rightarrow A) \Rightarrow A)) \Rightarrow ((A \Rightarrow (B \Rightarrow A)) \Rightarrow (A \Rightarrow A))} \qquad \dfrac{}{A \Rightarrow ((B \Rightarrow A) \Rightarrow A)}}{(A \Rightarrow (B \Rightarrow A)) \Rightarrow (A \Rightarrow A)} \qquad \dfrac{}{A \Rightarrow (B \Rightarrow A)}}{A \Rightarrow A}$$

Ce n'est pas particulièrement éclairant... et ça l'est encore moins dans les présentations traditionnelles des systèmes à la Hilbert : déduction présentée comme une suite de formule $A_1, \ldots, A_n$ telle que pour tout i, il existe $j, k < i$ tels que $A_j = A_k \Rightarrow A_i$.

On préfèrera la notion structurante d'arbre de preuve, et on peut encore améliorer un peu les choses en écrivant des **termes** de preuve.

La logique combinatoire

On associe à chaque axiome une constante (ici, K, S, respectivement) et au Modus Ponens un constructeur d'arité 2, l'*application*

$$t ::= K \mid S \mid tt$$

Il s'agit d'une syntaxe non typée. Un typage consiste à associer une formule à un terme, notation $t : A$. On peut alors décorer toute preuve :

$$\dfrac{\dfrac{\dfrac{}{S : (A \Rightarrow ((B \Rightarrow A) \Rightarrow A)) \Rightarrow ((A \Rightarrow (B \Rightarrow A)) \Rightarrow (A \Rightarrow A))} \quad \dfrac{}{K : A \Rightarrow ((B \Rightarrow A) \Rightarrow A)}}{SK : (A \Rightarrow (B \Rightarrow A)) \Rightarrow (A \Rightarrow A)} \quad \dfrac{}{K : A \Rightarrow (B \Rightarrow A)}}{SKK : A \Rightarrow A}$$

Il y a une bijection entre preuves et jugements de typage corrects.

C'est le premier pas de l'isomorphisme de Curry-Howard entre *preuves* et *programmes*. Le second est de comprendre $A \Rightarrow B$ comme $A \to B$ ("le type flèche", "les fonctions de A dans B), K comme la première projection, ..., st comme l'application d'une fonction s à un argument t.

La logique combinatoire (Schöhnfinkel, Curry, années 1920) a précédé le λ-calcul (années 1930), qui correspond à la déduction naturelle.

Les séquents

La logique classique :

$$A ::= X \parallel A \wedge A \parallel A \vee A \parallel \neg A$$

X désigne un *atome* (typiquement, une égalité $\vdash t_1 = t_2$, cf. calcul des prédicats)

Un séquent est une paire de deux *multi-ensembles* de formules Γ, Δ, notée

$$\Gamma \vdash \Delta$$

Il faut lire : “la conjonction des formules de Γ implique la disjonction des formules de Δ”. Le cas vide de la conjonction est “vrai” et le cas vide de la disjonction est “faux” (dans un ensemble ordonné avec éléments maximum et minimum, l’inf d’un ensemble vide d’éléments est le maximum et le sup de l’ensemble vide est le minimum). Donc

– $\vdash$ Δ se lit “vrai implique la disjonction des formules de Δ”, soit plus simplement “la disjonction des formules de Δ”,
– $\vdash A$ se lit “ A”,
– $\vdash$ se lit “vrai implique faux”, soit plus simplement “faux”

Calcul des séquents classique

Axiome et coupure

$$\frac{}{\Gamma, A \vdash A, \Delta} \qquad \frac{\Gamma \vdash A, \Delta \qquad \Gamma, A \vdash \Delta}{\Gamma \vdash \Delta}$$

Règles d'**introduction à droite** :

$$\frac{\Gamma, A \vdash \Delta}{\Gamma \vdash \neg A, \Delta} \qquad \frac{\Gamma \vdash A_1, \Delta \qquad \Gamma \vdash A_2, \Delta}{\Gamma \vdash A_1 \wedge A_2, \Delta}$$

$$\frac{\Gamma \vdash A_1, \Delta}{\Gamma \vdash A_1 \vee A_2, \Delta} \qquad \frac{\Gamma \vdash A_2, \Delta}{\Gamma \vdash A_1 \vee A_2, \Delta}$$

Règles d'**introduction à gauche** :

$$\frac{\Gamma \vdash A, \Delta}{\Gamma, \neg A \vdash \Delta} \qquad \frac{\Gamma, A_1, A_2 \vdash \Delta}{\Gamma, A_1 \wedge A_2 \vdash \Delta} \qquad \frac{\Gamma, A_1 \vdash \Delta \qquad \Gamma, A_2 \vdash \Delta}{\Gamma, A_1 \vee A_2 \vdash \Delta}$$

On dit que A, A_1, A_2, $\neg A$, $A_1 \wedge A_2$, $A_1 \vee A_2$ sont les formules *actives* des règles.

L'implication comme connecteur dérivé

On pose $A \Rightarrow B = \neg(A \wedge \neg B)$.

On peut alors **dériver** les deux règles d'introduction suivantes :

$$\frac{\Gamma, A \vdash B, \Delta}{\Gamma \vdash A \Rightarrow B} \qquad \frac{\Gamma \vdash A, \Delta \quad \Gamma, B \vdash \Delta}{\Gamma, A \Rightarrow B \vdash \Delta}$$

comme suit :

$$\dfrac{\dfrac{\dfrac{\Gamma, A \vdash B, \Delta}{\Gamma, A, \neg B \vdash \Delta}}{\Gamma, A \wedge \neg B \vdash \Delta}}{\Gamma \vdash \neg(A \wedge \neg B), \Delta} \qquad \dfrac{\dfrac{\dfrac{}{\Gamma \vdash A, \Delta} \quad \dfrac{\Gamma, B \vdash \Delta}{\Gamma \vdash \neg B, \Delta}}{\Gamma \vdash A \wedge \neg B, \Delta}}{\Gamma, \neg(A \wedge \neg B) \vdash \Delta}$$

Pourquoi des séquents ?

$A \vdash B$ et $\vdash A \Rightarrow B$ se lisent tous les deux comme "A implique B". Cette lecture des séquents donnée plus haut n' explique donc pas l'intérêt de la notion.

L'intérêt des séquents est de permettre d'écrire des règles qui, lues de la conclusion vers les hypothèses, permettent de **décomposer** les formules, afin d'ultimement ramener la prouvabilité d'une formule A, c'est-à-dire un séquent $\vdash A$, à l'unique axiome que A est prouvable sous l'hypothèse A (une fois éliminées les coupures, voir plus loin).

Ainsi dans $A \vdash B$ on a un accès direct aux sous-formules de $A \Rightarrow B$ et l'on peut à leur tour les décomposer, etc...

Autre motivation : Curry-Howard. Penser à une preuve de $A \Rightarrow B$ comme une fonction $x \mapsto f(x)$ d'un ensemble A vers un ensemble B, et penser à une preuve de $A \vdash B$ comme à une expression formelle t dépendant d'un paramètre x.

Souvenirs de lycée : pensez à un polynôme, disons $p(x) = x^2 + 3mx + (1 - m)$, qui dépend de la *variable* x et du *paramètre* m. Ses racines sont exprimées comme des expressions formelles dépendant de m. On a (anticipant la notion de typage) :

$$m : \mathbb{R} \vdash (x \mapsto p(x)) : \mathbb{R} \Rightarrow \mathbb{R}$$

On a aussi $\vdash (m \mapsto (x \mapsto x^2 + 3mx + (1 - m)) : \mathbb{R} \to (\mathbb{R} \to \mathbb{R})$ et $m : \mathbb{R}, x : \mathbb{R} \vdash x^2 + 3mx + (1 - m)) : \mathbb{R}$, mais c'est bien le premier typage qui reflète les rôles différents de m et de x.

Affaiblissement et contraction

Ce sont les règles suivantes, dont l'importance est fondamentale :

Affaiblissement

$$\frac{\Gamma \vdash \Delta}{\Gamma, A \vdash \Delta} \qquad \frac{\Gamma \vdash \Delta}{\Gamma \vdash A, \Delta}$$

Contraction

$$\frac{\Gamma, A, A \vdash \Delta}{\Gamma, A \vdash \Delta} \qquad \frac{\Gamma \vdash A, A, \Delta}{\Gamma \vdash A, \Delta}$$

Dans la présentation que nous avons adoptée plus haut :

- L'affaiblissement est admissible : reporter la formule supplémentaire dans tous les séquents de la preuve de $\Gamma \vdash \Delta$, jusqu'aux axiomes (notre formulation de l'axiome anticipe l'affaiblissement). Dans la suite, nous n'hésiterons pas à identifier cette preuve, disons de $\Gamma, A \vdash \Delta$, avec la preuve de $\Gamma \vdash \Delta$ dont elle est obtenue.
- La contraction est dérivable (notre formulation de la règle de coupure "contient" la contraction), par exemple, à droite (et en posant $\Delta_1 = A, \Delta$) :

$$\frac{\Gamma \vdash A, A, \Delta \qquad \dfrac{}{\Gamma, A \vdash A, \Delta}}{\Gamma \vdash A, \Delta}$$

Pour clarifier la terminologie, nous appellerons règle de **coupure-contraction** la formulation (additive – coming next) que nous avons donnée de la coupure. On appellera règle de coupure tout court toute instance de cette règle *qui n'est pas* telle que l'une de ses hypotheses soit un axiome dont une formule active soit la formule active de la coupure (en d'autres termes, qui n'est pas une contraction).

Style additif, style multiplicatif

La règle suivante est (moralement) dérivable (style multiplicatif) :

$$\frac{\Gamma_1 \vdash A, \Delta_1 \quad \Gamma_2 \vdash B, \Delta_2}{\Gamma_1, \Gamma_2 \vdash A \wedge B, \Delta_1, \Delta_2}$$

puisque une preuve de $\Gamma_1 \vdash A, \Delta_1$, par affaiblissement, est aussi une preuve de $\Gamma_1, \Gamma_2 \vdash A, \Delta_1, \Delta_2$ (et de même pour B), et l'on peut donc appliquer la règle droite que nous avons adoptée plus haut (style additif).

On peut remarquer aussi que nous avons adopté un style différent pour la disjonction à droite (deux règles, style additif) et pour la conjonction à gauche (une seule règle, style multiplicatif). On peut "dériver" les styles multiplicatif et additif manquants comme suit (en utilisant la contraction et de l'affaiblissement, resp.) :

$$\frac{\dfrac{\dfrac{\Gamma \vdash A_1, A_2, \Delta}{\Gamma \vdash A_1 \vee A_2, A_2, \Delta}}{\Gamma \vdash A_1 \vee A_2, A_1 \vee A_2, \Delta}}{\Gamma \vdash A_1 \vee A_2, \Delta} \qquad \frac{\dfrac{\Gamma, A_1 \vdash \Delta}{\Gamma, A_1, A_2 \vdash \Delta}}{\Gamma, A_1 \wedge A_2 \vdash \Delta} \qquad \frac{\dfrac{\Gamma, A_2 \vdash \Delta}{\Gamma, A_1, A_2 \vdash \Delta}}{\Gamma, A_1 \wedge A_2 \vdash \Delta}$$

Pour l'instant, additif et multiplicatif sont juste des noms. On reviendra dessus avec la logique linéaire. Notons juste que sans affaiblissement et contraction, ces styles ne sont plus intertraduisibles.

Réversibilité / irréversibilité

Nos règles pour la disjonction à droite et pour la conjonction à gauche présentent une autre différence de style, plus pertinente pour l'heure : la règle conjonction à gauche est *réversible*, la disjonction à droite est *irréversible*. Une règle

$$\frac{H_1 \quad \ldots \quad H_n}{C}$$

est dite **réversible** lorsque chacune des règles

$$\frac{C}{H_1} \qquad \ldots \qquad \frac{C}{H_n}$$

est admissible ("la conclusion est équivalente aux hypothèses"). Une règle est **irréversible** lorsqu'elle n'est pas réversible.

La règle de conjonction à gauche est réversible parce que les deux sous-formules A_1 et A_2 sont gardées (elle exprime l'associativité de la conjonction dans la lecture de la partie gauche d'un séquent comme la conjonction de ses formules).
La règle de disjonction à droite est irréversible car on choisit entre A_1 et A_2 : en termes de construction de preuves, *on prend un risque*.

Donc la dichotomie réversible/irréversible s'inscrit dans une dichotomie **actif**/**passif** qui oppose qui fait des choix à qui n'en fait pas. Une telle opposition entre irréversible et réversible apparaîtra aussi respectivement entre nos règles pour la conjonction à droite et la disjonction à gauche lorsqu'il sera question de *procéduralité* (déterminisation de l'élimination des coupures).

Axiomes atomiques

On ne perd rien à restreindre l'axiome aux atomes :

$$\frac{}{\Gamma, X \vdash X, \Delta}$$

En effet

$$\frac{\dfrac{\dfrac{}{\Gamma, A \vdash A, \Delta}}{\Gamma, \neg A, A \vdash \Delta}}{\Gamma, \neg A \vdash \neg A, \Delta} \qquad \frac{\dfrac{\dfrac{}{\Gamma, A_1, A_2 \vdash A_1, \Delta} \quad \dfrac{}{\Gamma, A_1, A_2 \vdash A_2, \Delta}}{\Gamma, A_1, A_2 \vdash A_1 \wedge A_2, \Delta}}{\Gamma, A_1 \wedge A_2 \vdash A_1 \wedge A_2, \Delta} \qquad \frac{\dfrac{\dfrac{}{\Gamma, A_1 \vdash A_1, \Delta}}{\Gamma, A_1 \vdash A_1 \vee A_2, \Delta} \quad \dfrac{\dfrac{}{\Gamma, A_2 \vdash A_2, \Delta}}{\Gamma, A_2 \vdash A_1 \vee A_2, \Delta}}{\Gamma, A_1 \vee A_2 \vdash A_1 \vee A_2, \Delta}$$

De telles preuves sont appelées des *expansions* de l'atome.

Complétude de LK

Un séquent $A_1, \ldots, A_m \vdash B_1, \ldots, B_n$ est dit *satisfiable* si dans la table de vérité de la formule correspondante $(A_1 \wedge \ldots \wedge A_n) \Rightarrow (B_1 \vee \ldots \vee B_n)$ au moins une case prend la valeur “vrai”. Si c’est le cas pour toutes les cases, le séquent est dit *valide* (tautologie).

Lemme : Un séquent $A_1, \ldots, A_m \vdash B_1, \ldots, B_n$ est satisfait si et seulement si l’un des B_j est satisfait ou l’un des A_i est satisfait.

Corollaire : Un séquent atomique $X_1, \ldots, X_m \vdash Y_1, \ldots, Y_n$ est valide si et seulement si il existe i, j tels que $X_i = Y_j$ (si tous les atomes sont distincts, on peut affecter “vrai” à tous les X_i et “faux” à tous les Y_j).

Théorème : Tout séquent valide admet une preuve sans coupure dans la présentation de LK avec axiomes atomiques et toutes les règles logiques formulées de manière réversible (remplacer les deux règles pour la disjonction à droite par la règle réversible donnée plus haut).

Démonstration : On appelle essai de preuve partiel d’un séquent tout arbre de déduction utilisant les règles de la version de LK précisée ci-dessus, terminant sur ce séquent, et dont les feuilles ne sont pas nécessairement des axiomes. La présentation réversible entraîne que la validité du séquent à la racine est équivalente à la validité de toutes les feuilles de l’arbre partiel.

Comme l’axiome est atomique, et comme rien ne freine la décomposition des formules (de la racine vers les feuilles), on peut, en prenant n’importe quel ordre d’application des règles, développer un essai de preuve maximal s’arrêtant sur des séquents atomiques.

L’hypothèse de validité de la racine entraîne alors la validité de toutes ces feuilles, et le corollaire montre que les feuilles sont des axiomes : l’essai de preuve est donc une preuve.

La complétude vaut aussi a fortiori dans notre présentation de LK, puisque la règle de disjonction à droite réversible y est dérivable.

Elimination des coupures via la complétude

L'énoncé inverse est vrai :

Théorème Tout séquent prouvable dans LK avec coupure est valide.

Ce résultat (théorème de validité du calcul des séquents) est plus fort que le simple énoncé inverse, car les preuves peuvent comprendre la coupure-contraction et des axiomes non atomiques.

En combinant les deux théorèmes on obtient :

Théorème : Tout séquent prouvable dans LK est prouvable sans l'aide de la règle de coupure-contraction (et en utilisant seulement la version atomique de l'axiome).

Démonstration : Le séquent est valide, donc, par complétude, prouvable dans le système contraint.

Cette preuve ne fournit aucun renseignement sur la manière de procéder par étapes pour éliminer progressivement les coupures.

Elimination vs introduction à gauche : la déduction naturelle

Au lieu d'introduire à gauche, on peut éliminer à droite. Pour l'implication, cela donne

$$\frac{\Gamma \vdash A \Rightarrow B, \Delta \qquad \Gamma \vdash A, \Delta}{\Gamma \vdash B, \Delta}$$

Cette règle est dérivable dans notre calcul des séquents :

$$\frac{\Gamma \vdash A \Rightarrow B, \Delta \qquad \dfrac{\Gamma \vdash A, B, \Delta \quad \dfrac{}{\Gamma, B \vdash B, \Delta}}{\Gamma, A \Rightarrow B \vdash B, \Delta}}{\Gamma \vdash B, \Delta}$$

On peut aussi dériver simplement les éliminations de la conjonction :

$$\frac{\Gamma \vdash A \wedge B, \Delta}{\Gamma \vdash A, \Delta} \qquad \frac{\Gamma \vdash A \wedge B, \Delta}{\Gamma \vdash B, \Delta}$$

Cela marche moins bien pour la disjonction (voir Proofs and types). La *déduction naturelle* (basée sur les introductions à droite et les éliminations à droite) n'est vraiment satisfaisante que pour la logique intuitionniste.

Logique intuitionniste, logique linéaire

Cette logique est une **restriction** de la logique classique qui rejette les tautologies suivantes :

$$A \vee \neg A \qquad\qquad \neg\neg A \Rightarrow A$$

Historiquement, ces restrictions ont été déterminantes pour donner un sens au calcul sous-jacent à la logique, i.e. pour relier preuves et programmes. Aujourd'hui, la logique linéaire, et la logique classique vue sous l'oeil de la focalisation, relativisent l'importance de cette restriction.

La logique linéaire, qui sera étudiée plus tard dans ce cours, est, elle, née d'une **décomposition** de la logique intuitionniste, et d'une perception des connecteurs comme des ressources.

L’élimination des coupures

C’est le thème fondamental du cours : les preuves servent à calculer. Le calcul, c’est la transformation des preuves.

Théoreme Toute preuve contenant la règle de coupure peut être transformée par une suite finie de transformations locales en une preuve du même séquent sans coupure. (En conséquence, toute coupure est admissible, mais ceci affadit le résultat : tout l’intérêt est dans la dynamique, qui n’est pas dans le mot “admissible”.)

Nous ne nous occupons pas pour l’instant de prouver la terminaison de cette procédure, nous montrons juste les transformations à effectuer :

- si la formule coupée vient d’être introduite, des deux côtés *(cas logique)* : la coupure est remplacée par une ou deux coupures sur la ou les sous-formules immédiates ;
- si pour au moins l’une des hypothèses $\Gamma, A \vdash \Delta$ ou $\Gamma \vdash A, \Delta$, la formule active dans la dernière règle utilisée pour la prouver n’est pas A *(cas commutatif)*, on fait remonter la coupure sur A.

Dans les deux cas ci-dessus, on a fait quelque chose qui “fait diminuer" : la taille de la formule coupée, la hauteur de la coupure dans la preuve. Mais il y a un troisième cas plus méchant, celui où à la place d’une introduction, on a une contraction sur la formule active de la coupure. Là il y a *duplication*, ce qui rend moins évident le fait que tout ceci va terminer.

Coupures logiques

$$\dfrac{\dfrac{\Gamma \vdash A, \Delta}{\Gamma, \neg A \vdash \Delta} \qquad \dfrac{\Gamma, A \vdash \Delta}{\Gamma \vdash \neg A, \Delta}}{\Gamma \vdash \Delta} \quad \longrightarrow \quad \dfrac{\Gamma, A \vdash \Delta \qquad \Gamma \vdash A, \Delta}{\Gamma \vdash \Delta}$$

$$\dfrac{\dfrac{\Gamma, A_1 \vdash \Delta \quad \Gamma, A_1 \vdash \Delta}{\Gamma, A_1 \vee A_2 \vdash \Delta} \qquad \dfrac{\Gamma \vdash A_1, \Delta}{\Gamma \vdash A_1 \vee A_2, \Delta}}{\Gamma \vdash \Delta} \quad \longrightarrow \quad \dfrac{\Gamma, A_1 \vdash \Delta \qquad \Gamma \vdash A_1, \Delta}{\Gamma \vdash \Delta}$$

$$\dfrac{\dfrac{\Gamma, A_1, A_2 \vdash \Delta}{\Gamma, A_1 \wedge A_2 \vdash \Delta} \qquad \dfrac{\Gamma \vdash A_1, \Delta \quad \Gamma \vdash A_2, \Delta}{\Gamma \vdash A_1 \wedge A_2, \Delta}}{\Gamma \vdash \Delta} \quad \longrightarrow \quad \dfrac{\dfrac{\Gamma, A_1, A_2 \vdash \Delta \quad \Gamma, A_2 \vdash A_1, \Delta}{\Gamma, A_2 \vdash \Delta} \qquad \Gamma \vdash A_2, \Delta}{\Gamma \vdash \Delta}$$

(rappelons que nous considérons qu'une preuve de $\Gamma \vdash A_1, \Delta$ est aussi une preuve de $\Gamma, A_2 \vdash A_1, \Delta$)
Notons qu'il est plus élégant de considérer la règle suivante de *multi-coupure* comme primitive (substitution parallèle !) :

$$\dfrac{\Gamma, A_1, A_2 \vdash \Delta \quad \Gamma \vdash A_1, \Delta \quad \Gamma, A_2 \vdash \Delta}{\Gamma \vdash \Delta}$$

Coupures commutatives

$$\dfrac{\dfrac{\Gamma, A, B \vdash \Delta}{\Gamma, A \vdash \neg B, \Delta} \qquad \Gamma \vdash A, \neg B, \Delta}{\Gamma \vdash \neg B, \Delta} \quad \longrightarrow \quad \dfrac{\dfrac{\dfrac{\Gamma, A, B \vdash \neg B, \Delta \qquad \Gamma, B \vdash A, \neg B, \Delta}{\Gamma, B \vdash \neg B, \Delta}}{\Gamma \vdash \neg B, \neg B, \Delta}}{\Gamma \vdash \neg B, \Delta}$$

On ne peut donc pas éliminer le “cas particulier” que constitue la contraction. C’est du même tabac pour les autres connecteurs. Et quand on ne peut plus remonter :

$$\dfrac{\dfrac{}{\Gamma, A, B \vdash B, \Delta} \qquad \Gamma, B \vdash A, B, \Delta}{\Gamma, B \vdash B, \Delta} \quad \longrightarrow \quad \dfrac{}{\Gamma, B \vdash B, \Delta}$$

(pensez à droite à une preuve de A affaiblie). C’est une règle d’**effacement** ($y[M/x] = y$).

(l’autre cas de base ($x[M/x] = M$) est atteint quand la coupure est devenue une contraction)

Si pour **les deux** hypothèses $\Gamma, A \vdash \Delta$ **et** $\Gamma \vdash A, \Delta$, la formule active dans la dernière règle utilisée pour la prouver n’est pas A, on peut fait remonter la coupure sur A dans la preuve de $\Gamma, A \vdash \Delta$ **ou** de $\Gamma, A \vdash \Delta$: c’est un choix non-déterministe dont le cas extrême est la “paire critique de Lafont” – voir plus loin).

Duplication

$$\dfrac{\dfrac{\Gamma, A, A \vdash \Delta}{\Gamma, A \vdash \Delta} \qquad \Gamma \vdash A, \Delta}{\Gamma \vdash \Delta} \quad \longrightarrow \quad \dfrac{\dfrac{\Gamma, A, A \vdash \Delta \quad \Gamma, A \vdash A, \Delta}{\Gamma, A \vdash, \Delta} \qquad \Gamma \vdash A, \Delta}{\Gamma \vdash \Delta}$$

On avait déjà dupliqué une coupure plus haut (dans le cas logique $A = A_1 \wedge A_2$), mais les coupures résultantes étaient sur des formules *plus petites*. Ici on a dupliqué la *preuve* de $\Gamma \vdash A, \Delta$.

La paire critique de Lafont

Considérons deux preuves π_1, π_2 *quelconques* du même séquent $\Gamma \vdash \Delta$. Considérons les respectivement, par affaiblissement, comme des preuves de $\Gamma, A \vdash \Delta$ et $\Gamma \vdash A, \Delta$. Considérons à présent la preuve suivante π :

$$\dfrac{\dfrac{\begin{array}{c}\vdots\\ \pi_1\end{array}}{\Gamma, A \vdash \Delta} \quad \dfrac{\begin{array}{c}\vdots\\ \pi_2\end{array}}{\Gamma \vdash A, \Delta}}{\Gamma \vdash \Delta}$$

C'est une coupure gravement commutative ! Si on fait systématiquement remonter la coupure dans π_1, on ne fait essentiellement que traverser la structure de π_1, amenant la preuve π_2 aux feuilles, où elle effacée. On a donc au total essentiellement transformé π en π_1. (De façon plus simple, mais presque trop magique, on aurait une transformation directe en une seule étape de π vers π_1 en admettant explicitement la règle d'affaiblissement.)

Si au contraire on oriente systématiquement l'élimination vers la droite (remontée de π_2), on retrouve π_2.

Soit :

$$\pi_1 {}^{*}\!\longleftarrow \pi \longrightarrow^{*} \pi_2$$

et donc $\pi_1 = \pi_2$ (clôture réflexive, symétrique et transitive de $\longrightarrow$).

Mais, en vue de Curry-Howard, nous ne **voulons pas identifier toutes les preuves**.

Chapitre II

Vers Curry-Howard : des preuves aux langages de preuves

La logique classique focalisée LKQ (Curien, Munch)

Curry-Howard

Le lien entre preuves et programmes se fait en deux étapes :

1) On définit un langage qui décrit les preuves : nous l'avons fait plus haut pour un système présenté à la Hilbert (logique combinatoire).

2) On lit les termes de ce langage (c'est-à-dire, par l'étape 1, les preuves) comme des programmes dans un langage de programmation, et on lit les formules comme les types de ces programmes et des paramètres ou variables dont ils dépendent. Par exemple, pour la logique combinatoire, on lit $A \Rightarrow B$ comme le type des fonctions de A dans B.

Une variante plus mathématique est de lire les preuves comme des morphismes dans des catégories, et les formules comme des objets de ces catégories : on lira alors la conjonction comme un produit (tensoriel ou cartésien, selon son caractère irréversible ou réversible), etc... Et si vous n'avez pas de bases en catégories, on interprète les preuves comme des fonctions entre certains ensembles, et quand ces ensembles ont une certaine structure, alors les interprétations des programmes préservent (plus ou moins) ces structures.

Enfin, la correspondance associe la dynamique des preuves (l'élimination des coupures) à celle des programmes (leur exécution, décrite par une *sémantique opérationnelle*).

Preuves différentes d'un même séquent

Via Curry-Howard, nous pouvons lire une preuve de $A_1, A_2 \vdash A$ comme un programme de type A dépendant de deux paramètres $x_1 : A_1$, $x_2 : A_2$. Par exemple, l'axiome $A_1, A_2 \vdash A_1$ se lit comme le programme correspondant à la première projection. On écrit

$$x_1 : A_1, x_2 : A_2 \vdash x_1 : A_1 \qquad x_1 : A_1, x_2 : A_2 \vdash x_2 : A_2$$

Et lorsque $A_1 = A_2 = A$, on a deux termes différents correspondant à deux preuves de $A, A \vdash A$:

$$x_1 : A, x_2 : A \vdash x_1 : A \qquad x_1 : A, x_2 : A \vdash x_2 : A$$

qui doivent aussi distinctes que sont distinctes les première et deuxième projections !

Nommer les occurrences, pointer sur les formules actives

Nous avons déjà les variables pour décorer ou nommer les formules à gauche dans un séquent. Par symétrie, nous aurons aussi des variables pour nommer les formules à droite, et nous utiliserons α, β pour ces variables. Nous verrons que ce sont des variables de *continuation* : un programme attend certains paramètres $x, y, \ldots$ en entrée et son résultat peut ensuite être utilisé dans divers contextes, pour obtenir un résultat final. Si c'est ce résultat final qu'on a en tête, il est alors naturel de voir le programme comme dépendant non seulement de valeurs correspondant à ses paramètres x, y mais aussi de ces contextes, correspondant à ses paramètres $\alpha, \beta, \ldots$. Nous aurons donc des séquents décorés par des variables (en fait, à gauche, nous les décorerons par des *contre-motifs*, wait and see) :

$$x_1 : A_1, \ldots, x_m : A_m \vdash \alpha_1 : A_1, \ldots, \alpha_m : A_m$$

Ensuite, nous avons besoin d'un outil syntaxique pour distinguer les formules actives dans les règles. Tout comme dans l'axiome $\Gamma, A, A \vdash A$, il faut savoir, dans une coupure entre une preuve de $\Gamma, A, A \vdash \Delta$ avec une preuve de $\Gamma \vdash A, \Delta$, laquelle des deux occurrences à gauche est la formule coupée. Pour ce faire nous introduisons deux nouvelles sortes de séquents, en plus de $\Gamma \vdash \Delta$:

$$\Gamma \,|\, A \vdash \Delta \qquad \Gamma \vdash A \,|\, \Delta$$

Et nous associons à ces trois catégories de séquents des termes, divisés en trois catégories syntaxiques.

Premiers éléments d'un kit syntaxique (Curien-Herbelin)

Voici les trois catégories de termes, avec leur typage :

Expressions	Contextes	Commandes
$\Gamma \vdash v : A \mid \Delta$	$\Gamma \mid A \vdash \Delta$	$c : (\Gamma \vdash \Delta)$

Et voici comment exprimer la coupure-contraction, en rendant explicite la phase de choix d'une formule active :

$$\dfrac{\dfrac{\Gamma, x : A \vdash \Delta}{\Gamma \mid \tilde{\mu}x.c_2 : A \vdash \Delta} \qquad \dfrac{\Gamma \vdash \alpha : A, \Delta}{\Gamma \vdash \mu\alpha.c_1 : A \mid \Delta}}{\langle \mu\alpha.c_1 \mid \tilde{\mu}x.c_2 : A\rangle : (\Gamma \vdash \Delta)}$$

Notre syntaxe comprend jusqu'à présent :

$$\begin{aligned} v &::= x \mid \mu\alpha.c \mid \dots \\ e &::= \alpha \mid \tilde{\mu}x.c \mid \dots \\ c &::= \langle v \mid e\rangle \end{aligned}$$

La variable x est liée dans $\tilde{\mu}x.c$ (de même pour $\mu\alpha.c$) (comme x est liée dans $\int_x f(x)dx$).

On munit (premier essai) ce langage des règles de calcul suivantes :

$$\langle \mu\alpha.c \mid e\rangle \longrightarrow c[e/\alpha] \qquad \langle v \mid \tilde{\mu}x.c\rangle \longrightarrow c[v/x]$$

On retrouve la paire critique de Lafont (si α n'est pas libre dans c_1 et x n'est pas libre dans c_2) :

$$c_1 = c_1[\tilde{\mu}x.c_2 : A/\alpha] \longleftarrow \langle \mu\alpha.c_1 \mid \tilde{\mu}x.c_2 : A\rangle \longrightarrow c_2[\mu\alpha.c_1/x] = c_2$$

Discipliner les preuves : la focalisation

La recherche de preuve focalisée (Andréoli) consiste à alterner des phases à droite et à gauche :

Phase à droite : Choisir une formule à droite A, que l'on ne cessera pas de décomposer dans toutes les branches de la preuve partielle (une seule sous-formule de A dans chaque séquent, grâce au style irréversible du $\vee$ droit) jusquà rencontrer une négation ou un axiome. Si l'on atteint un axiome, la recherche de preuve est terminée dans cette branche. Si l'on atteint une négation, alors (**changement de phase**) on la fait passer à gauche.

Phase à gauche : Décomposer des formules à gauche, dans n'importe quel ordre. Chaque décomposition d'un négatif réalimente la partie droite. A tout moment (même immédiatement après le changement de phase droite$\rightarrow$gauche), on peut repasser en phase à droite (**changement de phase**).

Cette discipline donne un caractère irréversible à l'ensemble de la phase à droite, par le choix héréditaire de la formule A. En choisissant de se **focaliser** ainsi sur une formule, on prend un risque : celui de terminer sur une feuille qui n'est pas un axiome. Chaque phase à gauche est au contraire réversible (les choix successifs sont libres, en plus de la réversibilité des règles). La décision de repasser en phase à droite est à nouveau un choix (irréversible).

Cette stratégie de recherche de preuve est complète. Et ce n'est pas tout : elle nous guide pour obtenir une logique disciplinée dont l'élimination des coupures n'identifie pas toutes les preuves).

Séquents focalisés

On introduit une quatrième sorte de séquent (pour la phase irréversible) : $\Gamma \vdash A\,;\ \Delta$. Il est pratique d'associer un signe (et d'autres adjectifs en opposition) aux deux phases :

irréversible $=$ **positif** (ou actif, ou synchrone) réversible $=$ **négatif** (ou passif, ou asynchrone)

Une branche d'une preuve focalisée (sans coupure) ressemble à ceci :

$$
\begin{array}{rc}
 & \vdots \\
 & {\scriptstyle -} \\
 & \vdots \\
 & \Gamma', B \vdash \Delta' \\
\text{-} & \overline{\hphantom{\Gamma' \mid B \vdash \Delta'}} \\
 & \Gamma' \mid B \vdash \Delta' \\
\text{+/-} & \overline{\hphantom{\Gamma' \vdash \neg B\,;\ \Delta'}} \\
 & \Gamma' \vdash \neg B\,;\ \Delta' \\
 & \vdots \\
 & {\scriptstyle +} \\
 & \vdots \\
\text{+} & \overline{\hphantom{\Gamma \vdash A\,;\ A, \Delta}} \\
 & \Gamma \vdash A\,;\ A, \Delta \\
\text{-/+} & \overline{\hphantom{\Gamma \vdash A\,;\ A, \Delta}} \\
 & \Gamma \vdash \Delta
\end{array}
$$

La contraction est nécessaire à la complétude de ce système.

Deux conjonctions, deux disjonctions

Nous avions déjà différencié dans notre présentation de LK le $\vee$ à droite du $\wedge$ à gauche. Or, par dualité, une conjonction à gauche est une disjonction à droite. La discipline de focalisation étend cette dissymétrie. Nous décidons de **renommer** les connecteurs comme suit :

$$\wedge \leadsto \otimes \qquad \vee \leadsto \oplus \qquad \neg \leadsto \neg^+$$

On utilise aussi désormais P, Q pour dénoter les formules que nous dénotions jusqu'alors A, B,. . .Ce n'est pas juste un coup de peinture. On peut maintenant définir le dual $\overline{A}$ d'une formule A comme suit :

$$\overline{X} = \overline{X} \qquad \overline{P_1 \otimes P_2} = \overline{P_1} \parr \overline{P_2} \qquad \overline{P_1 \oplus P_2} = \overline{P_1} \& \overline{P_2} \qquad \overline{\neg^+ P} = \neg^- \overline{P}$$

et si l'on réorganise les séquents $P_1, \ldots, P_m \vdash Q_1, \ldots, Q_n$ en séquents unilatéraux $\vdash \overline{P_1}, \ldots, \overline{P_m}, Q_1, \ldots Q_n$, alors on voit apparaître explicitement tous ces connecteurs (avec pour chacun une règle d'introduction à droite)

$$A ::= P \mid N \qquad P ::= X \mid P \otimes P \mid P \oplus P \mid \neg^+ P \qquad N ::= \overline{X} \mid N \parr N \mid N \& N \mid \neg^- N$$

avec, par exemple :

$$\frac{\Gamma \vdash P_1\,;\ \Delta}{\Gamma \vdash P_1 \oplus P_2\,;\ \Delta} \quad \frac{\Gamma \vdash P_2\,;\ \Delta}{\Gamma \vdash P_1 \oplus P_2\,;\ \Delta} \qquad \frac{\Gamma \vdash N_1, N_2, \Delta}{\Gamma \vdash N_1 \parr N_2, \Delta}$$

La graphie des quatre connecteurs $\otimes$ (tenseur), $\oplus$ (plus), $\&$ (avec), $\parr$ (par) vient de la logique lináire. Nous verrons aussi plus tard que $\neg^+$ et $\neg^-$ cachent les *exponentielles* de la logique linéaire.

Une syntaxe focalisée : le $\mu\tilde{\mu}^{+}$-calcul

Nous avons maintenant quatre catégories de termes, avec leur typage :

Expressions	Valeurs	Contextes	Commandes composées
$\Gamma \vdash v : A \mid \Delta$	$\Gamma \vdash V : A\, ;\, \Delta$	$\Gamma \mid A \vdash \Delta$	$C : (\Gamma \vdash \Delta)$

Et la syntaxe est la suivante :

Commandes	$c ::= \langle v \mid e \rangle$
Commandes composées	$C ::= c \parallel [C \ {}^{q,q}\ C]$
Expressions	$v ::= V^{\diamond} \parallel \mu\alpha.C$
Valeurs	$V ::= x \parallel (V, V) \parallel inl(V) \parallel inr(V) \parallel e^{\bullet}$
Contextes	$e ::= \alpha \parallel \tilde{\mu}q.C$
Contremotifs	$q ::= x \parallel \alpha^{\bullet} \parallel (q, q) \parallel [q, q]$

On utilise aussi la notation $\langle V \mid e \rangle^{+}$ pour $\langle V^{\diamond} \mid e \rangle$.

Tous ces constructeurs correspondent aux règles de la logique classique focalisée.

Référence : système LC de Girard. La présentation que nous donnons ici est (essentiellement) la variante LKQ proposée par Danos et al., *avec en prime un langage de termes*.

La logique focalisée LKQ

$$\frac{}{\Gamma\,,\, x : P \vdash x : P\,;\, \Delta} \qquad \frac{}{\Gamma \,|\, \alpha : P \vdash \alpha : P\,,\, \Delta} \qquad \frac{\Gamma \vdash v : P \,|\, \Delta \qquad \Gamma \,|\, e : P \vdash \Delta}{\langle v \,|\, e\rangle : (\Gamma \vdash \Delta)}$$

$$\frac{C : (\Gamma\,,\, q : P \vdash \Delta)}{\Gamma \,|\, \tilde{\mu} q.C : P \vdash \Delta} \qquad \frac{C : (\Gamma \vdash \alpha : P\,,\, \Delta)}{\Gamma \vdash \mu\alpha.C : P \,|\, \Delta} \qquad \frac{\Gamma \vdash V : P\,;\, \Delta}{\Gamma \vdash V^{\diamond} : P \,|\, \Delta}$$

$$\frac{\Gamma \,|\, e : P \vdash \Delta}{\Gamma \vdash e^{\bullet} : \neg^{+} P\,;\, \Delta} \qquad \frac{\Gamma \vdash V_1 : P_1\,;\, \Delta \qquad \Gamma \vdash V_2 : P_2\,;\, \Delta}{\Gamma \vdash (V_1, V_2) : P_1 \otimes P_2\,;\, \Delta}$$

$$\frac{\Gamma \vdash V_1 : P_1\,;\, \Delta}{\Gamma \vdash inl(V_1) : P_1 \oplus P_2\,;\, \Delta} \qquad \frac{\Gamma \vdash V_2 : P_2\,;\, \Delta}{\Gamma \vdash inr(V_2) : P_1 \oplus P_2\,;\, \Delta}$$

$$\frac{C : (\Gamma \vdash \alpha : P\,,\, \Delta)}{C : (\Gamma\,,\, \alpha^{\bullet} : \neg^{+} P \vdash \Delta)} \qquad \frac{C : (\Gamma\,,\, q_1 : P_1\,,\, q_2 : P_2 \vdash \Delta)}{C : (\Gamma\,,\, (q_1, q_2) : P_1 \otimes P_2 \vdash \Delta)}$$

$$\frac{C_1 : (\Gamma\,,\, q_1 : P_1 \vdash \Delta) \qquad C_2 : (\Gamma\,,\, q_2 : P_2 \vdash \Delta)}{[C_1 \;{}^{q_1,q_2}\; C_2] : (\Gamma\,,\, [q_1, q_2] : P_1 \oplus P_2 \vdash \Delta)}$$

Recherche de preuve focalisée

Avec les termes, cela donne ceci :

$$
\dfrac{
  \dfrac{
    \begin{array}{c}
    \vdots \\
    {\scriptstyle -} \\
    \vdots \\
    \text{-}\;\dfrac{C' : (\Gamma', q : Q \vdash \Delta')}{\Gamma' \mid \tilde{\mu}q.C' : Q \vdash \Delta'}
    \end{array}
  }{\Gamma' \vdash (\tilde{\mu}q.C')^{\bullet} : \neg^{+}Q \;;\; \Delta'}\;\text{+/-}
  \quad
  \begin{array}{c}
  \vdots \\
  {\scriptstyle +} \\
  \vdots
  \end{array}
}{
  \text{-/+}\quad \dfrac{}{\Gamma \vdash V : P \;;\; \alpha : P, \Delta}\;\text{+}
}
$$

$$
\text{-/+}\;\dfrac{\Gamma \vdash V : P \;;\; \alpha : P, \Delta}{\langle V^{\diamond} \mid \alpha \rangle : (\Gamma \vdash \alpha : P, \Delta)}
$$

Traduction de LK dans LKQ

Axiome (on combine par contraction les deux axiomes directionnels de LKQ) :

$$\dfrac{\dfrac{}{\Gamma, x : P \,|\, \beta : P \vdash \beta : P, \Delta} \qquad \dfrac{\dfrac{}{\Gamma, x : P \vdash x : P \,;\, \beta : P, \Delta}}{\Gamma, x : P \vdash x^{\diamond} : P \,|\, \beta : P, \Delta}}{\langle x^{\diamond} \mid \beta \rangle : (\Gamma, x : P \vdash \beta : P, \Delta)}$$

Coupure/contraction (cf. plus haut) : $\langle \mu\alpha.C_2 \mid \tilde{\mu}q.C_1 \rangle$

Règles droites :

$$\dfrac{C : (\Gamma, q : P \vdash \Delta)}{\langle ((\tilde{\mu}q.c)^{\bullet})^{\diamond} \mid \beta \rangle : (\Gamma \vdash \beta : \neg^{+}P, \Delta)} \qquad \dfrac{C : (\Gamma \vdash \alpha_1 : P_1, \Delta)}{\langle \mu\alpha_1.c \,|\, \tilde{\mu}x_1.\langle (inl(x_1))^{\diamond} \,|\, \alpha \rangle \rangle : (\Gamma \vdash \alpha : P_1 \oplus P_2, \Delta)}$$

$$\dfrac{C_1 : (\Gamma \vdash \alpha_1 : P_1, \Delta) \qquad C_2 : (\Gamma \vdash \alpha_2 : P_2, \Delta)}{\langle \mu\alpha_2.C_2 \,|\, \tilde{\mu}x_2.\langle \mu\alpha_1.C_1 \,|\, \tilde{\mu}x_1.\langle (x_1, x_2)^{\diamond} \,|\, \alpha \rangle \rangle \rangle : (\Gamma \vdash \alpha : P_1 \otimes P_2, \Delta)}$$

Règles gauches : il n’y a rien à faire (commandes en hypothèse et conclusion dans LKQ).

A propos de l'axiome

Dans le codage de LK dans LKQ, il est important de disposer de l'axiome sur toute formule P sous la forme que nous avons indiquée : x doit être une valeur (voir le codage des règles droites pour la disjonction et la conjonction). Il est néanmoins possible de dériver des versions expansées de l'axiome, sous forme de *commandes*, par exemple :

$$
\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{}{x : P \vdash x : P \,;\, \beta : Q} \qquad \dfrac{\dfrac{}{x : P \,|\, \beta : Q \vdash \beta : Q}}{x : P \vdash \beta^\bullet : \neg^+ Q \,;\, \beta : Q}}{x : P \vdash (x, \beta^\bullet) : P \otimes \neg^+ Q \,;\, \beta : Q}}{x : P \vdash (x, \beta^\bullet)^\diamond : P \otimes \neg^+ Q \,|\, \beta : Q} \qquad \dfrac{}{|\, \alpha : P \otimes \neg^+ Q \vdash \alpha : P \otimes \neg^+ Q}}{\langle (x, \beta^\bullet)^\diamond \,|\, \alpha \rangle : (x : P \vdash \beta : Q, \alpha : P \otimes \neg^+ Q)}}{\dfrac{\langle (x, \beta^\bullet)^\diamond \,|\, \alpha \rangle : (x : P, \beta^\bullet : \neg^+ Q \vdash \alpha : P \otimes \neg^+ Q)}{\langle (x, \beta^\bullet)^\diamond \,|\, \alpha \rangle : ((x, \beta^\bullet) : P \otimes \neg^+ Q \vdash \alpha : P \otimes \neg^+ Q)}}
$$

où l'on a utilisé l'affaiblissement pour souligner que α n'est pas contractée dans la preuve.

Un exemple : le tiers exclu

$$
\begin{prooftree}
\AxiomC{}
\UnaryInfC{$x : P \vdash x : P \,;\, \alpha : P \oplus \neg^{+}P$}
\UnaryInfC{$x : P \vdash inl(x) : P \oplus \neg^{+}P \,;\, \alpha : P \oplus \neg^{+}P$}
\UnaryInfC{$x : P \vdash inl(x)^{\diamond} : P \oplus \neg^{+}P \mid \alpha : P \oplus \neg^{+}P$}
\AxiomC{}
\UnaryInfC{$x : P \mid \alpha : P \oplus \neg^{+}P \vdash \alpha : P \oplus \neg^{+}P$}
\BinaryInfC{$\langle inl(x)^{\diamond} \mid \alpha \rangle : (x : P \vdash \alpha : P \oplus \neg^{+}P)$}
\UnaryInfC{$\mid \tilde{\mu}x.\langle inl(x)^{\diamond} \mid \alpha \rangle : P \vdash \alpha : P \oplus \neg^{+}P$}
\UnaryInfC{$\vdash (\tilde{\mu}x.\langle inl(x)^{\diamond} \mid \alpha \rangle)^{\bullet} : \neg^{+}P \,;\, \alpha : P \oplus \neg^{+}P$}
\UnaryInfC{$\vdash inr((\tilde{\mu}x.\langle inl(x)^{\diamond} \mid \alpha \rangle)^{\bullet}) : P \oplus \neg^{+}P \,;\, \alpha : P \oplus \neg^{+}P$}
\AxiomC{}
\UnaryInfC{$\mid \alpha : P \oplus \neg^{+}P \vdash \alpha : P \oplus \neg^{+}P$}
\BinaryInfC{$\langle inr((\tilde{\mu}x.\langle inl(x)^{\diamond} \mid \alpha \rangle)^{\bullet}) \mid \alpha \rangle^{+} : (\vdash \alpha : P \oplus \neg^{+}P)$}
\end{prooftree}
$$

Noter l'usage essentiel de la contraction dans cette preuve focalisée. Elle nous permet de focaliser sur $\neg^{+}P$ sans perdre la possibilité de focaliser sur P plus haut dans la preuve.

Un exemple : la commutativité du tenseur

On pose $\Gamma = x_1 : P_1 \, , \, x_2 : P_2$:

$$
\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{}{\Gamma \vdash x_1 : P_1 \, ; \, \alpha : P_1 \otimes P_2} \quad \dfrac{}{\Gamma \vdash x_2 : P_2 \, ; \, \alpha : P_1 \otimes P_2}}{\Gamma \vdash (x_1, x_2) : P_1 \otimes P_2 \, ; \, \alpha : P_1 \otimes P_2} \qquad \dfrac{}{\Gamma \mid \alpha : P_1 \otimes P_2 \vdash \alpha : P_1 \otimes P_2}}{\langle (x_1, x_2) \mid \alpha \rangle^+ : \Gamma \vdash \alpha : P_1 \otimes P_2}}{\langle (x_1, x_2) \mid \alpha \rangle^+ : (x_2, x_1) : P_2 \otimes P_1 \vdash \alpha : P_1 \otimes P_2}}{\mid \tilde{\mu}(x_2, x_1).\langle (x_1, x_2) \mid \alpha \rangle^+ : P_2 \otimes P_1 \vdash \alpha : P_1 \otimes P_2}
$$

Elimination des coupures dans LKQ

Nous exprimons l'élimination des coupures dans notre langage de termes. Il y a trois sortes de règles :

– Règles de contrôle (règles absentes de LK, introduites précisément pour empêcher la paire critique de Lafont) :

$$\begin{array}{l} \langle V^{\diamond} \mid \tilde{\mu}q.C\rangle \longrightarrow C[V/q] \\ \langle \mu\alpha.C \mid e\rangle \longrightarrow C[e/\alpha] \end{array}$$

  Il faut donc ajouter à la syntaxe

$$C ::= \ldots \mid C[\sigma]$$

  où σ est un *ensemble* dont les éléments sont de la forme V/q ou e/α. (Notons qu'en effet il n'y a maintenant qu'une seule façon de réduire $\langle \mu\alpha.C_1 \mid \tilde{\mu}q.C_2\rangle$.)

– Règles logiques :

$$\begin{array}{l} C[(V_1, V_2)/(q_1, q_2), \sigma] \longrightarrow C[V_1/q_1, V_2/q_2, \sigma] \\ C[e^{\bullet}/\alpha\bullet, \sigma] \longrightarrow C[e/\alpha, \sigma] \\ [C_1 \ {}^{q_1,q_2}\ C_2][inl(V_1)/[q_1, q_2], \sigma] \longrightarrow C_1[V_1/q_1, \sigma] \\ [C_1 \ {}^{q_1,q_2}\ C_2][inr(V_2)/[q_1, q_2], \sigma] \longrightarrow C_2[V_2/q_2, \sigma] \end{array}$$

– Coupures commutatives : règles sans surprise, qui distribuent la substitution jusqu'aux feuilles ou "activent" des réductions logiques bloquées

A propos de μ : On peut noter qu'une expression $\mu\beta.C$ est seulement utilisée dans une commande $\langle \mu\beta.C \mid e\rangle$, et qu'on peut alors l'exprimer comme $\langle e^{\bullet} \mid \tilde{\mu}\beta^{\bullet}.c\rangle^{+}$, qui en deux étapes se réduit bien sur $C[e/\beta]$.

Les coupures commutatives

C'est l'ensemble suivant de règles (pour le passage des lieurs μ $\tilde{\mu}$, on renvoie au λ-calcul)

$$
\begin{array}{ll}
[C_1 \;{}^{q_1,q_2}\; C_2][\sigma] \longrightarrow [C_1[\sigma] \;{}^{q_1,q_2}\; C_2[\sigma]] & ([q_1,q_2] \notin \sigma) \\
\langle v \mid e\rangle[\sigma] \longrightarrow \langle v[\sigma] \mid v[\sigma]\rangle & \\
(V^{\diamond})[\sigma] \longrightarrow (V[\sigma])^{\diamond} & \\
(\mu\alpha.C)[\sigma] \longrightarrow \mu\alpha.(C[\sigma]) & \\
(\tilde{\mu}q.C)[\sigma] \longrightarrow \tilde{\mu}q.(C[\sigma]) & \\
(V_1,V_2)[\sigma] \longrightarrow (V_1[\sigma],V_2[\sigma]) & \\
(inl(V))[\sigma] \longrightarrow inl((V[\sigma])) & \\
(inr(V))[\sigma] \longrightarrow inr((V[\sigma])) & \\
(e^{\bullet})[\sigma] \longrightarrow (e[\sigma])^{\bullet} & \\
 & \\
(C[\sigma])[\sigma'] \longrightarrow (C[\sigma'])[\sigma[\sigma']] & (\sigma = x/[q_1,q_2],\sigma_1) \\
C[x/q,\sigma] \longrightarrow (C[\sigma])[x/q] & (q \text{ n'est pas une variable}) \\
 & \\
x[V/x,\sigma] \longrightarrow V & \\
x[\sigma] \longrightarrow x & (x \notin \sigma) \\
\alpha[e/\alpha,\sigma] \longrightarrow e & \\
\alpha[\sigma] \longrightarrow \alpha & (\alpha \notin \sigma)
\end{array}
$$

où $q \in \sigma$ veut dire que σ contient un élément V/q et où

$$(\ldots,V/q,\ldots,e/\alpha,\ldots)[\sigma'] = (\ldots,(V[\sigma'])/q,\ldots,(e[\sigma'])/\alpha,\ldots)$$

Toutes ces règles sont celles définissant usuellement la substitution dans une syntaxe avec lieurs, les deux seules règles “spéciales” sont celles du milieu, qui gèrent le cas d'une variable x substituée à un contremotif complexe.

Un isomorphisme fondamental

Les deux formules $(\neg^+ P_1) \otimes (\neg^+ P_2)$ et $\neg^+(P_1 \oplus P_2)$ sont **prouvablement isomorphes**. Cela signifie qu'il existe

$$\begin{array}{l} C_1 : (\beta^\bullet : \neg^+(P_1 \oplus P_2) \vdash \alpha : \neg^+ P_1 \otimes \neg^+ P_2) \\ C_2 : ((\alpha_1^\bullet, \alpha_2^\bullet) : \neg^+ P_1 \otimes \neg^+ P_2 \vdash \gamma : \neg^+(P_1 \oplus P_2)) \end{array}$$

tels que $\langle \mu\gamma.C_2 \,|\, \tilde{\mu}\beta^\bullet.C_1\rangle$ et $\langle \mu\alpha.C_1 \,|\, \tilde{\mu}(\alpha_1^\bullet, \alpha_2^\bullet).C_2\rangle$ se réduisent sur l'"identité" (c'est-à- dire une preuve de $((\alpha_1^\bullet, \alpha_2^\bullet) : \neg^+ P_1 \otimes \neg^+ P_2 \vdash \alpha : \neg^+ P_1 \otimes \neg^+ P_2)$, $(\beta^\bullet : \neg^+(P_1 \oplus P_2) \vdash \gamma : \neg^+(P_1 \oplus P_2))$, respectivement, obtenue comme expansion d'axiomes sur P_1 et P_2).

Démonstration : On pose

$$\begin{array}{ll} V_1 = ((\tilde{\mu}y_1'.\langle inl(y_1')^\diamond \mid \beta\rangle)^\bullet, (\tilde{\mu}y_2'.\langle inr(y_2')^\diamond \mid \beta\rangle)^\bullet) & \vdash V_1 : \neg^+ P_1 \otimes \neg^+ P_2 \,;\, \beta : P_1 \oplus P_2 \\ V_2 = (\tilde{\mu}[y_1, y_2].[\langle y_1^\diamond \mid \alpha_1\rangle \;{}^{y_1,y_2}\; \langle y_2^\diamond \mid \alpha_2\rangle])^\bullet & (\alpha_1^\bullet, \alpha_2^\bullet) : \neg^+ P_1 \otimes \neg^+ P_2 \vdash V_2 : \neg^+(P_1 \oplus P_2)\,; \end{array}$$

Prenons $C_1 = \langle V_1^\diamond \mid \alpha\rangle$ et $C_2 = \langle V_2^\diamond \mid \gamma\rangle$. On a :

$$\begin{array}{lll} \langle \mu\gamma.C_2 \mid \tilde{\mu}\beta^\bullet.C_1\rangle & \longrightarrow^* & \langle V_2^\diamond \mid \tilde{\mu}\beta^\bullet.C_1\rangle \\ & \longrightarrow^* & \langle (V_1[V_2/\beta^\bullet])^\diamond \mid \alpha\rangle \\ & \longrightarrow & \langle (V_1[\tilde{\mu}[y_1, y_2].[\langle y_1^\diamond \mid \alpha_1\rangle \;{}^{y_1,y_2}\; \langle y_2^\diamond \mid \alpha_2\rangle]/\beta])^\diamond \mid \alpha\rangle \\ & \longrightarrow & ((\tilde{\mu}y_1'.\langle inl(y_1')^\diamond \mid \tilde{\mu}[y_1, y_2].[\langle y_1^\diamond \mid \alpha_1\rangle \;{}^{y_1,y_2}\; \langle y_2^\diamond \mid \alpha_2\rangle]\rangle)^\bullet, e^\bullet) \\ & \longrightarrow & \langle ((\tilde{\mu}y_1'.\langle y_1^\diamond \mid \alpha_1\rangle[y_1'/y_1])^\bullet, e^\bullet) \mid \alpha\rangle \\ & \longrightarrow & \langle ((\tilde{\mu}y_1'.\langle (y')_1^\diamond \mid \alpha_1\rangle)^\bullet, e^\bullet) \mid \alpha\rangle \\ & \longrightarrow^* & \langle ((\tilde{\mu}y_1'.\langle (y')_1^\diamond \mid \alpha_1\rangle)^\bullet, (\tilde{\mu}y_2'.\langle (y')_2^\diamond \mid \alpha_2\rangle^\bullet) \mid \alpha\rangle \end{array}$$

où $e = \tilde{\mu}y_2'.\langle inr(y_2')^\diamond \mid \tilde{\mu}[y_1, y_2].[\langle y_1^\diamond \mid \alpha_1\rangle \;{}^{y_1,y_2}\; \langle y_2^\diamond \mid \alpha_2\rangle]\rangle$

On peut considérer $\tilde{\mu}y_1'.\langle (y')_1^\diamond \mid \alpha_1\rangle$ comme une forme expansée de α_1 (cf. l'η-expansion $\lambda x.Mx$ de M dans le λ-calcul). Donc, "moralement", $\langle \mu\gamma.C_2 \mid \tilde{\mu}\beta^\bullet.C_1\rangle$ se réduit sur $\langle (\alpha_1^\bullet, \alpha_2^\bullet) \mid \alpha\rangle$.

Le théorème d'élimination des coupures dans LKQ

Ce résultat s'établit en trois parties :

1. Préservation du typage par les règles.
2. Existence d'une stratégie normalisante
3. Caractérisation des formes normales

Partant, disons d'une commande C : $(\Gamma \vdash \Delta)$:

1. par la propriété (2), on peut réduire C jusqu'à une forme normale C' ;
2. par la propriété (1), on a C' : $(\Gamma \vdash \Delta)$
3. par la propriété (3, C' dénote une preuve sans coupures.

Préservation du typage par les règles

Nous avons ajouté à la syntaxe, outre $C[\sigma]$:

$$v ::= \ldots \mid v[\sigma] \qquad V ::= \ldots \mid V[\sigma] \qquad e ::= \ldots \mid e[\sigma]$$

Les règles de typage pour ces nouvelles constructions sont, disons pour $C[\sigma]$:

$$\frac{\ldots \quad \Gamma \vdash V : P\,;\, \Delta \quad \ldots \quad \Gamma \,|\, e : Q \vdash \Delta \quad \ldots \quad C : (\Gamma\; \ldots, q : P, \ldots \vdash \Delta, \ldots, \alpha : Q, \ldots)}{C[\ldots, V/q, \ldots, e/\alpha] : (\Gamma \vdash \Delta)}$$

Proposition Si $t ::= C \mid v \mid V \mid e$, et si $t \longrightarrow t'$ et, disons $t = v$ et $\Gamma \vdash t : P \,|\, \Delta$, alors $\Gamma \vdash t' : P \,|\, \Delta$.

Une stratégie normalisante

On regroupe l'application des règles commutatives, en considérant comme une seule étape l'application d'une règle de contrôle ou d'une règle logique suivie d'une application maximale des règles commutatives (on peut y aller plus doucement en poussant seulement les items de la forme V/x et α/e jusqu'au bout, et ceux de la forme $V/[q_1, q_2]$ jusqu'à une commande $[C_1 \ {}^{q_1,q_2}\ C_2]$) : ce processus termine.

On remarque ensuite qu'aucune réduction de crèe de (μ) radical (parce que $\mu\alpha.C$ n'est pas une valeur). On peut donc effectuer toutes les (μ) reductions d'abord, de l'intérieur vers l'extérieur : cela termine (absence de création), et pour la suite on peut se restreindre au système sans la règle (μ).

Le *degré* d'un radical $(\tilde{\mu}^+)$ ou logique est la formule active de la règle de coupure/contraction sous-jacente. Soit t un terme : on marque toutes les occurrences de ses radicaux avec leur degré ainsi qu'une étiquette $\lambda \in \{\tilde{\mu}, L\}$ indiquant sa sorte ($(\tilde{\mu}^+)$ ou logique), et on rassemble toutes ces paires (P, λ) en un multiensemble, que nous appelons la *mesure* de t. On adopte l'extension aux multiensembles de l'ordre $(P, \tilde{\mu}) > (P, L) > (Q\tilde{\mu}) > (Q, L) > \ldots$ (Q sous-formule immédiate de P). On restreint encore la stratégie de réduction en choisissant toujours de réduire un radical de marque maximale et dont tous les sous-termes qui sont des radicaux portent une marque strictement plus petite. Alors *chaque reduction fait décroître la mesure strictement*, et la stratégie est donc normalisante. Ceci est conséquence des deux propriétés suivantes :

- Les résidus d'un radical préservent leur marque.
- Si un radical R_1 crèe un radical R_2, alors la marque de R_2 est strictement inférieure à celle de R_1 :
  - Substitution de α par $\tilde{\mu}q.C$ dans $(\langle V \mid \alpha\rangle^+)^{(P,\tilde{\mu})}$: le créateur est un radical logique $R^{(\neg^+ P,L)}$.
  - Substitution de x par $inl(V)$ or $inr(V)$ dans $[C_1 \ {}^{q_1,q_2}\ C_2][x/[q_1, q_2]]^{(P_1 \oplus P_2,L)}$: le créateur est soit un $(\tilde{\mu}^+)$ radical $R_1^{(P_1 \oplus P_2,\tilde{\mu})}$, soit un radical llogique $R_2^{(Q,L)}$ ($P_1 \oplus P_2$ sous-formule immédiate gauche ou droite de Q).
  - Création logique, typiquement $C[(V, e^\bullet/(q, \alpha^\bullet), \sigma]^{(P \otimes \neg^+ Q,L)} \longrightarrow C[(V/(q, (e^\bullet/(\alpha^\bullet)\sigma]^{(\neg^+ Q,L)}$.

Les formes normales

Dans une forme normale (i.e. une preuve qui ne peut plus être réduite), les seules occurrences possibles de

$$\left.\begin{array}{r}\langle v \mid e\rangle \\ t[\sigma]\end{array}\right\} \quad \text{sont} \quad \left\{\begin{array}{ll}\langle V^{\diamond} \mid \alpha\rangle & \text{(contraction à droite)} \\ C[x/q] & \text{(contraction à gauche)}\end{array}\right.$$

En effet :

$$\frac{\Gamma \vdash V : P\,;\, \alpha : P, \Delta \qquad \overline{\Gamma \mid \alpha : P \vdash \alpha : P, \Delta}}{\langle V^{\diamond} \mid \alpha\rangle : (\Gamma \vdash \Delta)} \qquad \frac{C : (\Gamma, x : P, q : P \vdash \Delta) \qquad \Gamma, x : P \vdash x : P\,;\, \Delta}{C[x/q] : (\Gamma \vdash \Delta)}$$

Notez que la contraction à gauche dans LK se traduit et se réduit comme suit :

$$\begin{array}{rcl}\langle \mu\alpha.\langle x^{\diamond} \mid \alpha\rangle \mid \tilde{\mu}q.C\rangle & \longrightarrow & \langle x^{\diamond} \mid \alpha\rangle[\tilde{\mu}q.C/\alpha] \\ & \longrightarrow^{*} & \langle x^{\diamond} \mid \tilde{\mu}q.C\rangle \\ & \longrightarrow & C[x/q]\end{array}$$

Donc, une preuve en forme normale est une preuve sans coupure.

Le théorème de focalisation

Une **preuve focalisée** de LK est une preuve dans LK qui, lue de bas en haut (recherche de preuve), suit la discipline focalisée.

Théorème : Tout sequent prouvable dans LK est prouvable par une preuve focalisée.

Démonstration : Soit π une preuve d'un séquent $\Gamma \vdash \Delta$:

1. On traduit cette preuve en un terme de preuve $c : \Gamma \vdash \Delta$ de LKQ.
2. On applique l'élimination des coupures à c, jusquà obtenir une forme normale c.
3. On traduit la preuve sous-jacente dans LK (par simple oubli des termes et des 4 catégories de séquents)

Déduction naturelle intuitionniste

$$\frac{}{\Gamma P \vdash P}$$

$$\frac{\Gamma, A \vdash B}{\Gamma \vdash A \Rightarrow B} \qquad \frac{\Gamma \vdash A \Rightarrow B \qquad \Gamma \vdash A}{\Gamma \vdash B}$$

$$\frac{\Gamma \vdash A, \Gamma \vdash B}{\Gamma \vdash A \wedge B} \qquad \frac{\Gamma \vdash A \wedge B}{}$$

La restriction à une seule formule à droite interdit la contraction à droite, et interdit une preuve du tiers exclu.

Traduction de LKQ vers NJ (1/2)

On fixe une formule R quelconque (cela aide de penser qu'elle représente " faux", mais n'importe quelle formule fait l'affaire).

$$X_{cps} = X \qquad (\neg^{+} P)_{cps} = R^{P_{cps}} \qquad (P \otimes Q)_{cps} = (P_{cps}) \times (Q_{cps}) \qquad P \oplus Q_{cps} = P_{cps} + Q_{cps}$$

La traduction des termes est indexée par des environnements de renommage ζ dont les éléments sont de la forme x/q (aplatissement des contremotifs).

$$(\langle v \mid e \rangle)^{\zeta}_{cps} = (v^{\zeta}_{cps})(e^{\zeta}_{cps})$$

$$x^{\zeta}_{cps} = x \quad (V_1, V_2)^{\zeta}_{cps} = ((V_1)^{\zeta}_{cps}, (V_2)^{\zeta}_{cps}) \quad inl(V_1)^{\zeta}_{cps} = inl((V_1)^{\zeta}_{cps}) \quad inr(V_2)^{\zeta}_{cps} = inr((V_2)^{\zeta}_{cps}) \quad (e^{\bullet})^{\zeta}_{cps} = e^{\zeta}_{cps}$$

$$(V^{\diamond})^{\zeta}_{cps} = \lambda k.k(V^{\zeta}_{cps}) \qquad (\mu\alpha.C)^{\zeta}_{cps} = \lambda\alpha.C^{\zeta}_{cps}$$

$$\alpha^{\zeta}_{cps} = \alpha^{\bullet} \qquad (\tilde{\mu}q.C)^{\zeta}_{cps} = \lambda z.(c^{z/q,\zeta}_{cps})$$

$$C^{z/(q_1,q_2),\zeta}_{cps} = C^{x_1/(q_1,x_1/(q_1,\zeta}_{cps}[fst(z)/x_1, snd(z)/x_2]$$

$$C^{\alpha^{\bullet}/\alpha^{\bullet},\zeta}_{cps} = C^{\zeta}_{cps}$$

$$[C_1 \;{}^{q_1,q_2}\; C_2]^{z/[q_1,q_2],\zeta}_{cps} = \textit{case}\ z\ [inl(x_1) \mapsto (C_1)^{x_1/q_1,\zeta}_{cps}, inr(x_2) \mapsto (C_2)^{x_2/q_2,\zeta}_{cps}]$$

Traduction de LKQ vers NJ (2/2)

On pose

$$\Gamma^{\zeta}_{cps} = \{z : P_{cps} \mid q : P \in \Gamma, z/q \in \zeta\} \qquad R^{\Delta_{cps}} = \{\alpha^{\bullet} : R^{P_{cps}} \mid \alpha : P \in \Delta\}$$

On a

$$\left.\begin{array}{r} c : (\Gamma \vdash \Delta) \\ \Gamma \vdash V : P \,;\, \Delta \\ \Gamma \vdash v : P \,|\, \Delta \\ \Gamma \,|\, e : P \vdash \Delta \end{array}\right\} \quad \Rightarrow \quad \left\{\begin{array}{l} \Gamma^{\zeta}_{cps} \,,\, R^{\Delta_{cps}} \vdash C^{\zeta}_{cps} : R \\ \Gamma^{\zeta}_{cps} \,,\, R^{\Delta_{cps}} \vdash V^{\zeta}_{cps} : P_{cps} \\ \Gamma^{\zeta}_{cps} \,,\, R^{\Delta_{cps}} \vdash v^{\zeta}_{cps} : R^{R^{P_{cps}}} \\ \Gamma^{\zeta}_{cps} \,,\, R^{\Delta_{cps}} \vdash e^{\zeta}_{cps} : R^{P_{cps}} \end{array}\right.$$

Théorème La traduction préserve les règles de réduction : si $t \longrightarrow t'$, alors $t^{\zeta}_{cps} \longrightarrow^{*} (t')^{\zeta}_{cps}$.

Chapitre III

La logique classique fortement focalisée LKQS.

Il s'agit de quotienter des preuves qui ne diffèrent que par l'ordre d'introduction de connecteurs à gauche (donc réversibles), qui n'a pas d'importance (cf. p. 32), et d'être ainsi encore plus fidèle à la notion de focalisation. Voir p. 65 pour un exemple.

A partir de la p.60, j'ai repris (faute de temps) des transparents en anglais. Voir aussi l'article

P.-L. Curien and Guillaume Munch-Maccagnoni, The duality of computation under focus

qui est à la base de toute cette première partie du cours. Il y a quelques conflits de terminologie entre les transparents qui suivent et cet article. En particulier, LK_{pol} remplace ici (avantageusement) LKQC.

Une lecture complémentaire (optionnelle) :

Guillaume Munch-Maccagnoni, Focalisation and classical realisability (`http://perso.ens-lyon.fr/guillaume.munch`)

Le système LKQS

Le système LKQS est obtenu en restreignant les règles de LKQ comme suit :

1. Les variables x sont seulement de type atomique :

$$\frac{}{\Xi, x : X \vdash x : X \ ; \ \Delta}$$

2. On note Ξ un contexte gauche uniquement constitué de *formules atomiques* soit $\Xi = x_1 : P_1, \ldots, x_n : P_n$ (notons que $q : X$ implique nécessairement que q est une variable), et on restreint les règles de LKQ en remplaçant partout Γ par Ξ dans toutes les règles qui concernent (en hypothèse ou en conclusion) les expressions, les valeurs (autres que x) et les contextes :

$$\frac{}{\Xi \,|\, \alpha : P \vdash \alpha : P \ , \ \Delta} \qquad \frac{\Xi \vdash v : P \,|\, \Delta \qquad \Gamma \,|\, e : P \vdash \Delta}{\langle v \,|\, e \rangle : (\Xi \vdash \Delta)} \qquad \frac{C : (\Xi \ , \ q : P \vdash \Delta)}{\Xi \,|\, \tilde{\mu} q.C : P \vdash \Delta}$$

(toutes les règles sauf les trois dernières). Le but de cette restriction est de contraindre le système à des phases négatives maximales :

$$\cfrac{\cfrac{\vdots \atop C' : (\Xi', q : Q \vdash \Delta')}{\Xi' \,|\, \tilde{\mu} q.C' : Q \vdash \Delta'}\ -}{\Xi' \vdash (\tilde{\mu} q.C')^{\bullet} : \neg^{+} Q \ ; \ \Delta'}\ +/- \atop \vdots$$

Autrement dit, la formule Q est l'objet d'une *focalisation négative* : elle doit être entièrement décomposée, puis une phase positive suivra, avec une decompostion entière à droite, etc. . ..

Complétude de LKQS (1/2)

Théorème : Le système LKQS est complet pour LKQ (et donc pour LK) : si C : $(\Gamma \vdash \Delta)$ dans LKQ, alors $\Gamma \vdash \Delta$ est prouvable dans LKQS.

Démonstration : La seule difficulté consiste à trouver la bonne charge inductive. On définit une relation de réécriture entre ensembles S de séquents comme suit :

$$
\begin{array}{l}
(\Gamma, \neg^+ P \vdash \Delta), \mathrm{S} \longrightarrow (\Gamma \vdash P, \Delta), \mathrm{S} \\
(\Gamma, P_1 \otimes P_2 \vdash \Delta), \mathrm{S} \longrightarrow (\Gamma, P_1, P_2 \vdash \Delta), \mathrm{S} \\
(\Gamma, P_1 \oplus P_2 \vdash \Delta), \mathrm{S} \longrightarrow (\Gamma, P_1 \vdash \Delta), (\Gamma, P_2 \vdash \Delta), \mathrm{S}
\end{array}
$$

Une forme normale pour cette notion de réécriture est clairement un ensemble de séquents de la forme $\Xi \vdash \Delta$. Il est facile de voir que $\longrightarrow$ est confluente et fortement normalisante. Par définition de cette relation, on a que si $\mathrm{S} \longrightarrow^* \mathrm{S}'$, alors les propriétés suivantes sont équivalentes (aussi bien dans LKQ que dans LKQS) :

1. tous les séquents de S sont prouvables ;
2. tous les séquents de S' sont prouvables.

On montre, par récurrence sur la taille de la preuve :

1. Si C : $(\Gamma \vdash \Delta)$ dans LKQ et si $(\Gamma \vdash \Delta) \longrightarrow^* \mathrm{S}$, alors tous les séquents de S sont prouvables dans LKQS.
2. Si $\Gamma \vdash v : P \,|\, \Delta$ dans LKQ et si S est la forme normale de $(\Gamma \vdash \Delta)$, alors, pour tout $(\Xi \vdash \Delta')$ de S, le séquent $\Xi \vdash P \,|\, \Delta'$ est prouvable dans LKQS, et de même pour les valeurs et les contextes de LKQ.

On détaille deux cas dans le transparent suivant.

Complétude de LKQS (1/2)

Coupure/contraction : Soit S tel que $(\Gamma \vdash \Delta) \longrightarrow^* \mathrm{S}$. Soit S' la forme normale de $(\Gamma \vdash \Delta)$. Par hypothèse de récurrence, pour tout $(\Xi \vdash \Delta'')$ dans S', $(\Xi \vdash P \,|\, \Delta'')$ et $(\Xi \,|\, P \vdash \Delta'')$ sont prouvables dans LKQS, donc $(\Xi \vdash \Delta'')$ est prouvable dans LKQS. Or, par définition de $\longrightarrow$, si $(\Gamma' \vdash \Delta') \in \mathrm{S}$, il existe un sous-ensemble S'' de S' tel que $(\Gamma' \vdash \Delta') \longrightarrow^* \mathrm{S}''$. A fortiori, tous les séquents de S'' sont prouvables dans LKQS. Donc $(\Gamma' \vdash \Delta')$ est prouvable dans LKQS.

Axiome : Soit $\Xi, x : P \vdash x : P\,;\, \Delta$. Il faut montrer que, pour tout $(\Xi \vdash \Delta')$ dans la forme normale de $(\Gamma, P \vdash \Delta)$, $(\Xi \vdash P\,;\, \Delta')$ est prouvable dans LKQS. On montre par récurrence sur P que la propriété est vraie, pour tous Γ, Δ :

1. $P = P_1 \otimes P_2$: Comme $(\Xi \vdash \Delta')$ est aussi dans la forme normale de $(\Gamma, P_1, P_2 \vdash \Delta)$, on a par récurrence que $(\Xi \vdash P_1\,;\, \Delta')$ et $(\Xi \vdash P_2\,;\, \Delta')$ sont prouvables dans LKQS, et donc $(\Xi \vdash P\,;\, \Delta')$ aussi.
2. $P = P_1 \oplus P_2$: Le séquent $(\Xi \vdash \Delta')$ est dans la forme normale de $(\Gamma, P_1 \vdash \Delta)$ ou de $(\Gamma, P_2 \vdash \Delta)$. Donc, par récurrence, on a disons $\Xi \vdash P_1\,;\, \Delta')$, et donc $(\Xi \vdash P\,;\, \Delta')$ aussi.
3. $P = \neg^+ Q$: Comme $(\Gamma, \neg^+ Q \vdash \Delta) \longrightarrow (\Gamma \vdash Q, \Delta)$, on a que, par définition de la relation $\longrightarrow$, $\Delta = Q, \Delta'$. On en conclut (sans récurrence) :

$$\Xi \vdash \alpha^\bullet : P\,;\, Q, \Delta'$$

dans LKQS.

Elimination des coupures dans LKQS

Dans LKQS, les règles commutatives d'élimination des coupures se résument à la définition standard de la substitution (sans les deux règles spéciales, puisque, dans LKQS, quand on rencontre x/q, q doit être une variable), et (dans la tradition du λ-calcul) peuvent être laissées implicites, ce que l'on note $C\{\sigma\}$:

$$
\begin{array}{l}
\langle V^{\diamond} \mid \tilde{\mu}q.C\rangle \longrightarrow C[V/q] \\
\langle \mu\alpha.C \mid e\rangle \longrightarrow C\{e/\alpha\} \\
\\
C[(V_1,V_2)/(q_1,q_2),\sigma] \longrightarrow C[V_1/q_1,V_2/q_2,\sigma] \\
C[e^{\bullet}/\alpha\bullet,\sigma] \longrightarrow C[e/\alpha,\sigma] \\
[C_1 \ {}^{q_1,q_2}\ C_2][inl(V_1)/[q_1,q_2],\sigma] \longrightarrow C_1[V_1/q_1,\sigma] \\
[C_1 \ {}^{q_1,q_2}\ C_2][inr(V_2)/[q_1,q_2],\sigma] \longrightarrow C_2[V_2/q_2,\sigma] \\
\\
C[\sigma] \longrightarrow C\{\sigma\} \quad (\text{ si } \sigma \text{ ne contient que des } V/x \text{ ou des } e/\alpha)
\end{array}
$$

Où les contremotifs rencontrent les motifs (1/2)

On définit une syntaxe de motifs :

$$p ::= x \mid \alpha^\bullet \mid (p,p) \mid inl(p) \mid inr(p)$$

On peut redéfinir la syntaxe des valeurs comme suit :

$$\begin{array}{l} \mathcal{V} ::= x \mid e^\bullet \\ V ::= p \, \langle \mathcal{V}_i / i \mid i \in p \rangle \end{array}$$

où

- $\mathcal{V}_i = y$ si $i = x$, et $\mathcal{V}_i = e^\bullet$ si $i = \alpha^\bullet$
- $i \in p$, ($i = x$ or $i = \alpha^\bullet$) est défini comme suit :

$$\frac{}{x \in x} \quad \frac{}{\alpha^\bullet \in \alpha^\bullet} \quad \frac{i \in p_1}{i \in (p_1, p_2)} \quad \frac{i \in p_2}{i \in (p_1, p_2)} \quad \frac{i \in p_1}{i \in inl(p_1)} \quad \frac{i \in p_2}{i \in inr(p_2)}$$

Où les contremotifs rencontrent les motifs (2/2)

On peut alors reformuler les règles logiques d'élimination des coupures en termes d'interaction entre motifs et contremotifs (ce qui justifie la terminologie) :

$$\frac{V = p\,\langle \ldots y/x, \ldots, e^\bullet/\alpha^\bullet, \ldots \rangle \qquad C[p/q] \longrightarrow^* c}{C[V/q] \longrightarrow c\{\ldots y/x, \ldots, e/\alpha, \ldots\}}$$

Remarquer que nous considérons maintenant que la réduction logique et commutative de $C[V/q]$ se fait en **une seule étape** : chaque formule est considérée comme un connecteur synthétique (composé selon q).

Voici les règles qui permettent de réécrire $C[p/q]$:

$$\begin{array}{l}
C[(V_1, V_2)/(q_1, q_2), \sigma] \longrightarrow C[V_1/q_1, V_2/q_2, \sigma] \\
C[e^\bullet/\alpha\bullet, \sigma] \longrightarrow C[e/\alpha, \sigma] \\
[C_1 \;{}^{q_1,q_2}\; C_2][inl(V_1)/[q_1, q_2], \sigma] \longrightarrow C_1[V_1/q_1, \sigma] \\
[C_1 \;{}^{q_1,q_2}\; C_2][inr(V_2)/[q_1, q_2], \sigma] \longrightarrow C_2[V_2/q_2, \sigma]
\end{array}$$

Example : patterns for $P = X \otimes (Y \oplus \neg^{+}Q)$

Focusing on the right yields two possible proof searches :

$$\dfrac{\Gamma \vdash x'\{\mathcal{V}_{x'}\} : X \,;\, \Delta \qquad \dfrac{\Gamma \vdash y'\{\mathcal{V}_{y'}\} : Y \,;\, \Delta}{\Gamma \vdash inl(y'))\{\mathcal{V}_{y'}\} : Y \oplus \neg^{+}Q \,;\, \Delta}}{\Gamma \vdash (x', inl(y'))\{\mathcal{V}_{x'}, \mathcal{V}_{y'}\} : X \otimes (Y \oplus \neg^{+}Q) \,;\, \Delta}$$

$$\dfrac{\Gamma \vdash x'\{\mathcal{V}_{x'}\} : X \,;\, \Delta \qquad \dfrac{\Gamma \vdash \alpha'^{\bullet}\{\mathcal{V}_{\alpha'^{\bullet}}\} : \neg^{+}Q \,;\, \Delta}{\Gamma \vdash inr(\alpha'^{\bullet}))\{\mathcal{V}_{\alpha'^{\bullet}}\} : Y \oplus \neg^{+}Q \,;\, \Delta}}{\Gamma \vdash (x', inr(\alpha'^{\bullet}))\{\mathcal{V}_{x'}, \mathcal{V}_{\alpha'^{\bullet}}\} : X \otimes (Y \oplus \neg^{+}Q) \,;\, \Delta}$$

Example : counterpattern for $P = X \otimes (Y \oplus \neg^{+} Q)$

The counterpattern describes the tree structure of P (ludics like, but more precise) = reversible decomposition of P on the left :

$$\cfrac{\cfrac{c_1 : (\Gamma\ ,\ x : X\ ,\ y : Y \vdash \Delta) \quad c_2 : (\Gamma\ ,\ x : X\ ,\ \alpha^{\bullet} : \neg^{+} Q \vdash \Delta)}{[c_1 \ {}^{y,\alpha^{\bullet}}\ c_2] : (\Gamma\ ,\ x : X\ ,\ [y, \alpha^{\bullet}] : Y \oplus \neg^{+} Q \vdash \Delta)}}{[c_1 \ {}^{y,\alpha^{\bullet}}\ c_2] : (\Gamma\ ,\ (x, [y, \alpha^{\bullet}]) : X \otimes (Y \oplus \neg^{+} Q) \vdash \Delta)}$$

Key observation. The leaves of the decomposition are in one-to-one correspondence with the counterpatterns p for the (irreversible) decomposition of P on the right :

$$[c_1 \ {}^{y,\alpha^{\bullet}}\ c_2][p_1/q] = c_1\{x'/x, y'/y\}$$
$$[c_1 \ {}^{y,\alpha^{\bullet}}\ c_2][p_2/q] = c_2\{x'/x, \alpha'/\alpha\}$$

where $q = (x, [y, \alpha^{\bullet}])$, $p_1 = (x', inl(y'))$, $p_2 = (x', inr(\alpha'^{\bullet}))$.

The correspondence associated with pattern-counterpattern interaction

Let $C : (\Gamma\ ,\ q : P \vdash \Delta)$ (uniquely associated with P, up to weakening). The mapping

$$p \mapsto c \qquad (C[p/q] \longrightarrow^* c\ \ ,\ \ q, C \text{ fixed})$$

is a one-to-one correspondence between

$$\{p \mid q \perp p\} \quad \text{and} \quad \{c \mid c \in C\}$$

where $c \in C$ and $q \perp p$ are the predicates defined by

$$\frac{}{c \in c} \qquad \frac{c \in C_1}{c \in [C_1\ {}^{q_1,q_2}\ C_2]} \qquad \frac{c \in C_1}{c \in [C_1\ {}^{q_1,q_2}\ C_2]}$$

$$\frac{}{x \perp x} \qquad \frac{}{\alpha^\bullet \perp \alpha^\bullet} \qquad \frac{q_1 \perp p_1 \quad q_2 \perp p_2}{(q_1, q_2) \perp (p_1, p_2)} \qquad \frac{q_1 \perp p_1}{[q_1, q_2] \perp inl(p_1)} \qquad \frac{q_2 \perp p_2}{[q_1, q_2] \perp inr(p_2)}$$

Reformulation of the $\mu\tilde{\mu}^{+}$-calculus

$$
\begin{aligned}
&c ::= \langle V \mid e \rangle^{+} \\
&C ::= c \parallel [C \; {}^{q,q} \; C] \\
&\mathcal{V} ::= x \parallel e^{\bullet} \\
&V ::= p\{\mathcal{V}_i \mid i \in p\} \\
&e ::= \alpha \parallel \tilde{\mu} q.C
\end{aligned}
$$

$$
\begin{aligned}
&p ::= x \parallel \alpha^{\bullet} \parallel (p,p) \parallel inl(p) \parallel inr(p) \\
&q ::= x \parallel \alpha^{\bullet} \parallel (q,q) \parallel [q,q]
\end{aligned}
$$

The big step $\mu\tilde{\mu}^{+}$-calculus

Thanks to the pattern-counterpattern correspondence, we can quotient over the “bureaucracy” of compound commands, and arrive at a *big step* calculus.

$$
\begin{array}{l}
c ::= \langle v^{\diamond} \mid e\rangle \\
\mathcal{V} ::= x \mid\mid e^{\bullet} \\
V ::= p\,\langle \mathcal{V}_i/i \mid i \in p\rangle \\
e ::= \alpha \mid\mid \tilde{\mu}q.\{p \mapsto c_p \mid q \perp p\} \\
\\
q ::= x \mid\mid \alpha^{\bullet} \mid\mid (q,q) \mid\mid [q,q] \\
p ::= x \mid\mid \alpha^{\bullet} \mid\mid (p,p) \mid\mid inl(p) \mid\mid inr(p)
\end{array}
$$

cf. Zeilberger : $\{p \mapsto c \mid q \perp p\}$ as a function from patterns to commands.

With a **unique** reduction rule (that embodies control, logical and commutative rules !) :

$$(\tilde{\mu}^{+}) \qquad \langle (p\,\langle \ldots, y/x, \ldots, e^{\bullet}/\alpha^{\bullet} \ldots\rangle)^{\diamond} \mid \tilde{\mu}q.\{p \mapsto c_p \mid q \perp p\}\rangle \quad \rightarrow \quad c_p\,\{\ldots, y/x, \ldots, e/\alpha, \ldots\rangle\}$$

(select field p, and then substitute).

The specification of $q \perp p$ ($x \perp y$ only for $y = x$) eliminates the need to α-rename c_p.

The quotient to the big step calculus

Consider $P = (P_1 \oplus P_2) \otimes (Q_1 \oplus Q_2)$. Then a proof of $(\Gamma,\ q : P \vdash \Delta)$ $(q = ([x_1, x_2], [y_1, y_2])$ combines four commands :

$$\begin{array}{ll} c_{11} : (\Gamma,\ x_1 : P_1\,,\ y_1 : Q_1 \vdash \Delta) & c_{12} : (\Gamma,\ x_1 : P_1\,,\ y_2 : Q_2 \vdash \Delta) \\ c_{21} : (\Gamma,\ x_2 : P_2\,,\ y_1 : Q_1 \vdash \Delta) & c_{22} : (\Gamma,\ x_2 : P_2\,,\ y_2 : Q_2 \vdash \Delta) \end{array}$$

The $LK_{\tilde{\mu}}$-contexts $\tilde{\mu}q.[[c_{11}, c_{12}], [c_{21}, c_{22}]]$ and $\tilde{\mu}q.[[c_{11}, c_{21}], [c_{12}, c_{22}]]$ are both mapped to

$$\tilde{\mu}q.\{p_{11} \mapsto c_{11}, \ldots, p_{22} \mapsto c_4\} \quad \text{where} \quad \begin{cases} p_{11} = (inl(x_1), inl(y_1)) \\ \vdots \\ p_{22} = (inr(x_2), inr(y_2)) \end{cases}$$

Translating back to the $\mu\tilde{\mu}^{+}$-calculus

$$
\begin{aligned}
&\underline{x\{y\}} = y\\
&\underline{\alpha^\bullet\{e^\bullet\}} = e^\bullet\\
&\underline{(p_1,p_2)\{\mathcal{V}_i \mid i \in (p_1,p_2)\}} = (\underline{p_1\{\mathcal{V}_i \mid i \in p_1\}}\,,\ \underline{p_2\{\mathcal{V}_i \mid i \in p_2\}})\\
&\underline{inl(p_1)\{\mathcal{V}_i \mid i \in inl(p_1)\}} = inl(\underline{p_1\{\mathcal{V}_i \mid i \in p_1\}})\\
&\underline{inl(p_2)\{\mathcal{V}_i \mid i \in inl(p_2)\}} = inl(\underline{p_2\{\mathcal{V}_i \mid i \in p_2\}})\\
&\underline{\tilde{\mu}q.\{p \mapsto c_p \mid q \perp p\}} = \tilde{\mu}q.\underline{\phi_q} \quad (\phi_q(p) = c_p)
\end{aligned}
$$

where $\underline{\phi_L}$ is defined (non-deterministically) by :

$$
\begin{aligned}
&\underline{\phi_{L_1,(q_1,q_2),L_2}} = \underline{\phi_{L_1,q_1,q_2,L_2}}\\
&\underline{\phi_{L_1,[q_1,q_2],L_2}} = [\underline{\phi_{L_1,q_1,L_2}}, \underline{\phi_{L_1,q_2,L_2}}]\\
&\underline{\phi_L} = \phi(L) \quad (L \text{ atomic})
\end{aligned}
$$

where (with L_i, L_i' of same length, $i = 1,2$)

$$
\begin{aligned}
&\phi_{L_1,q_1,q_2,L_2}(L_1', p_1, p_2, L_2') = \phi_{L_1,(q_1,q_2),L_2}(L_1', (p_1,p_2), L_2')\\
&\phi_{L_1,q_1,L_2}(L_1', p_1, L_2') = \phi_{L_1,[q_1,q_2],L_2}(L_1', inl(p_1), L_2')\\
&\phi_{L_1,q_2,L_2}(L_1', p_2, L_2') = \phi_{L_1,[q_1,q_2],L_2}(L_1', inl(p_2), L_2')
\end{aligned}
$$

and L is atomic when each item of L is an x or an $\alpha^\bullet$

System LKQS

Typing rules : the old ones for $\alpha, x, e^\bullet, c$ +

$$\frac{\ldots \qquad \Gamma \vdash \mathcal{V}_i : P_i \,;\, \Delta \quad ((i : P_i) \in \Gamma(p, P)) \qquad \ldots}{\Gamma \vdash p\{\mathcal{V}_i \mid i \in p\} : P \,;\, \Delta}$$

$$\frac{\ldots \qquad c_p : (\Gamma \,,\, \Gamma(p, P) \vdash \Delta) \quad (q \perp p) \qquad \ldots}{\Gamma \mid \tilde{\mu} q.\{p \mapsto c_p \mid q \perp p\} \vdash \Delta}$$

where $\Gamma(p, P)$ must be successfully defined as follows :

$$\begin{array}{l}
\Gamma(x, X) = (x : X) \\
\Gamma(\alpha^\bullet, \neg^+ P) = (\alpha^\bullet : \neg^+ P) \\
\Gamma((p_1, p_2), P_1 \otimes P_2) = \Gamma(p_1, P_1) \,,\, \Gamma(p_2, P_2) \\
\Gamma(inl(p_1), P_1 \oplus P_2) = \Gamma(p_1, P_1) \\
\Gamma(inl(p_2), P_1 \oplus P_2) = \Gamma(p_2, P_2)
\end{array}$$

Böhm trees

In the multiplicative case (no C, $inl(V)$, $inr(V)$, $[q_1, q_2]$), there is a unique p such that $q \perp q$, namely q, and the syntax boils down to

$$\mathcal{V} ::= x \parallel e^\bullet \quad V ::= p\{\mathcal{V}_i \mid i \in p\} \quad v ::= x \parallel \tilde{\mu}q.\{c\} \quad c = \langle V \mid \alpha \rangle^+$$

Compare with (CBN) **Böhm trees** : $\boxed{M ::= \overbrace{\lambda \vec{x}.\underbrace{P}_{c}}^{e} \qquad P ::= y \underbrace{\overbrace{M_1}^{\mathcal{V}} \ldots \overbrace{M_n}^{\mathcal{V}}}_{V}}$

For example, if M_j translates to e_j ($j = 1, 2, 3$), then $\lambda x_1 x_2.x M_1 M_2 M_3$ translates to

$$\tilde{\mu}(\overline{x_1}^\bullet, \overline{x_2}^\bullet, y).\langle q\{\mathcal{V}_i \mid i \in p\} \mid \overline{x} \rangle^+$$

where $q = (\alpha_1^\bullet, \alpha_2^\bullet, \alpha_3^\bullet, z)$, $\mathcal{V}_{z_j} = (e_j)^\bullet$ ($j = 1, 2, 3$), and $\mathcal{V}_z = y$.

A nice junction (optionnel !)

Compare with my syntax for ludics (Introduction to linear logic and ludics, part II, `www.pps.jussieu.fr/~curien`) :

$$\overbrace{M}^{e} ::= \{\overbrace{J}^{p} \mapsto \lambda\{x_j \mid j \in J\}.P_J \mid \overbrace{J \in \mathcal{N}}^{q \perp p}\}$$

$$\underbrace{P}_{c} ::= (x \cdot \underbrace{\overbrace{I}^{p})\{M_i \mid i \in I\}}_{V} \parallel \Omega \parallel \maltese$$

Note that p is more precise than I (finite tree of all subaddresses versus the set of immediate subaddresses) : this could lead to a ludics with axioms (and without faxes).

Chapitre IV

Codage des λ-calculs :

- par valeur (ou “strict”)
- par nom (ou “paresseux”)
- “mixte" : certains langages admettent des caractéristiques strictes *et* paresseuses. Pour les traduire dans LKQ (puis le cas échéant les implémenter via cette traduction), il est plus naturel de traduire d’abord vers une version *faiblement polarisée* de LKQ, LK_{pol}, définie plus bas (p. 78 et suivantes).

A derived operator and a derived rule

We define :

$$V^{\blacklozenge} = \tilde{\mu}\alpha^{\bullet}.\langle V \mid \alpha\rangle^{+}$$

which satisfies the following (derived) rule :

$$(\blacklozenge^{+}) \qquad \langle e^{\bullet} \mid v^{\blacklozenge}\rangle^{+} \quad \rightarrow \quad \langle V \mid e\rangle^{+}$$

Indeed :

$$\langle e^{\bullet} \mid V^{\blacklozenge}\rangle^{+} = \langle e^{\bullet} \mid \tilde{\mu}\alpha^{\bullet}.\langle V \mid \alpha\rangle^{+}\rangle^{+} \quad \longrightarrow_{(\tilde{\mu}^{+})} \quad \langle V \mid \alpha\rangle^{+}[e^{\bullet}/\alpha^{\bullet}] \longrightarrow^{*} \langle V \mid e\rangle^{+}$$

The coercion from e to $e^{\bullet}$ acts thus as a “freezing”, which the $\blacklozenge$ construct permits to unfreeze (cf. Zeilberger, Munch).

CBV encoding of the simply-typed $\lambda\mu$-calculus in the $\mu\tilde{\mu}^{+}$-calculus

$$A ::= X \mid A \rightarrow A$$

Translation of types :

$$\begin{aligned}
&[\![X]\!]^{+}_{\mathrm{v}} = X \\
&[\![A \rightarrow B]\!]^{+}_{\mathrm{v}} = \neg^{+}([\![A]\!]^{+}_{\mathrm{v}} \otimes \neg^{+}[\![B]\!]^{+}_{\mathrm{v}})
\end{aligned}$$

CBV translation of terms (if $\Gamma \vdash s : A \mid \Delta$ and then $[\![\Gamma]\!]^{+}_{\mathrm{v}} \vdash [\![s]\!]^{+}_{\mathrm{v}} : [\![A]\!]^{+}_{\mathrm{v}} \mid [\![\Gamma]\!]^{+}_{\mathrm{v}}$) :

$$\begin{aligned}
&[\![x]\!]^{+}_{\mathrm{v}} = x^{\diamond} \\
&[\![\lambda x.s]\!]^{+}_{\mathrm{v}} = ((\tilde{\mu}(x, \alpha^{\bullet}).\langle [\![s]\!]^{+}_{\mathrm{v}} \mid \alpha \rangle)^{\bullet})^{\diamond} \\
&[\![st]\!]^{+}_{\mathrm{v}} = \mu\alpha.\langle [\![t]\!]^{+}_{\mathrm{v}} \mid \tilde{\mu}x.\langle [\![s]\!]^{+}_{\mathrm{v}} \mid ((x, \alpha^{\bullet})^{\diamond})^{\blacklozenge} \rangle\rangle \\
&[\![\mu\alpha.[\beta]s]\!]^{+}_{\mathrm{v}} = \mu\alpha.\langle [\![s]\!]^{+}_{\mathrm{v}} \mid \beta \rangle
\end{aligned}$$

A simple CBV calculation

Computing $\Delta\Delta$ (with $\Delta = \lambda x.xx$) :

We have :

$[\![\Delta\Delta]\!]^{+}_{\mathtt{v}} = \mu\gamma.c$ where $(c = \langle e^{\bullet} \mid \tilde{\mu}z.\langle(e^{\bullet} \mid (z,\gamma^{\bullet})^{\blacklozenge})\rangle^{+}\rangle^{+}$ and $e = \tilde{\mu}(x,\alpha^{\bullet}).\langle x \mid \tilde{\mu}y.\langle x \mid (y, c$

And we compute as follows :

$$
\begin{array}{lll}
c = \langle e^{\bullet} \mid \tilde{\mu}z.\langle(e^{\bullet}) \mid ((z,\gamma^{\bullet})^{\blacklozenge}\rangle^{+}\rangle^{+} & & \\
& \longrightarrow_{(\blacklozenge^{+})} & \langle e^{\bullet} \mid \tilde{\mu}z.\langle(z,\gamma^{\bullet})^{\blacklozenge}) \mid e\rangle^{+}\rangle^{+} \\
& \longrightarrow_{(\tilde{\mu}^{+})} & \langle((e^{\bullet},\gamma^{\bullet}) \mid e\rangle^{+} \\
& = & \langle(e^{\bullet},\gamma^{\bullet}) \mid \tilde{\mu}(x,\alpha^{\bullet}).\langle x \mid \tilde{\mu}y.\langle x \mid (y,\alpha^{\bullet})^{\blacklozenge}\rangle^{+}\rangle^{+}\rangle^{+} \\
& \longrightarrow_{(\tilde{\mu}^{+})} & c
\end{array}
$$

Embedding the deterministic calculi of Curien-Herbelin

We can embed the $\overline{\lambda}\mu\tilde{\mu}_Q$-calculus (based on implication and difference) in the $\mu\tilde{\mu}^+$-calculus (extended with expressions, cf. above) as follows.

We define :

$$P_1 \to^+ P_2 = \neg^+(P_1 \otimes \neg^+ P_2) \qquad P_2 -^+ P_1 = (\neg^+ P_1) \otimes P_2$$

$$\begin{array}{ll} \lambda x.v = (\tilde{\mu}(x, \alpha^\bullet).\langle v \mid \alpha \rangle)^\bullet & \beta\lambda.e = \tilde{\mu}(\beta^\bullet, x).\langle x^\diamond \mid e \rangle \\ V \cdot e = \tilde{\mu}\alpha^\bullet.\langle (V, e^\bullet)^\diamond \mid \alpha \rangle & e \cdot V = (e^\bullet, V) \end{array}$$

The $\overline{\lambda}\mu\tilde{\mu}_T$-calculus can be embedded dually (in the dual calculus) :

$$\begin{array}{l} N_1 \to^- N_2 = (\neg^- N_1) \parr N_2 \\ N_2 -^- N_1 = \neg^-(N_1 \parr \neg^- N_2) \end{array}$$

$P_2 -^+ P_1$ is the dual of the negative implication.

What about CBN ?

CBN is negative, i.e., the CBN translation of $A \rightarrow B$ is a negative type. Hence, in the setting of $LK_{\tilde{\mu}}$, the CBN translation of a term will be a context, which one then should rather call a negative expression (of negative type), and to stress this, we could write

$$\Gamma \vdash e : \overline{P} \,|\, \Delta$$

for

$$\Gamma \,|\, e : P \vdash \Delta$$

We refrain from doing this now. We shall do it later, placing also $\overline{\Delta}$ on the left, which is even better : we shall move from (folded formulas + bilateral) to (unfolded and **richer** syntax + monolateral).

CBN encoding of the simply-typed λ-calculus in the $\mu\tilde{\mu}^{+}$-calculus

$$A ::= X \mid A \to A$$

Translation of types :

$$\llbracket X \rrbracket^{+}_{\mathtt{n}} = X$$
$$\llbracket A \to B \rrbracket^{+}_{\mathtt{n}} = (\neg^{+}\llbracket A \rrbracket^{+}_{\mathtt{n}}) \otimes \llbracket B \rrbracket^{+}_{\mathtt{n}}$$

CBN translation of terms (if $\Gamma \vdash s : A$, then $(\mid \llbracket s \rrbracket^{+}_{\mathtt{n}} : \llbracket A \rrbracket^{+}_{\mathtt{n}} \vdash \llbracket \Gamma \rrbracket^{+}_{\mathtt{n}})$, where $\llbracket \Gamma \rrbracket^{+}_{\mathtt{n}} = \{\overline{x} : \llbracket B \rrbracket^{+}_{\mathtt{n}} \mid x : P \in \Gamma\}$) :

$$\llbracket x \rrbracket^{+}_{\mathtt{n}} = \overline{x}$$
$$\llbracket \lambda x.s \rrbracket^{+}_{\mathtt{n}} = \tilde{\mu}(\overline{x}^{\bullet}, y).\langle y \mid \llbracket s \rrbracket^{+}_{\mathtt{n}} \rangle^{+}$$
$$\llbracket st \rrbracket^{+}_{\mathtt{n}} = \tilde{\mu}y.\langle (\llbracket t \rrbracket^{+}_{\mathtt{n}})^{\bullet}, y) \mid \llbracket s \rrbracket^{+}_{\mathtt{n}} \rangle^{+}$$

Of course, the translation extends to the $\lambda\mu$-calculus.
Both CBV and CBN translations make sense in an untyped setting.

Mixing call-by-name and call-by-value

In a call-by-name ambience, some call-by-value zone can be forced, like in

$$(\lambda(x,y).M_1)M_2$$

The function can only be called when M_2 has been evaluated to a (strict) pair (P_1, P_2) and then proceeds with $M_1[P_1/x\ ,\ P_2/y]$.

Thus, we want to give to $(\lambda(x,y).M_1)$ the type

$$(A_1 \otimes A_2) \to^{\mathtt{n}} A_2$$

where $A \to^{\mathtt{n}} B = (\uparrow \overline{A}) \parr B$.
($\otimes$ positive, $\to^n$ negative)

The $\mu\tilde{\mu}$-calculus (1/2)

Commands	$c ::= \langle v \mid e \rangle$
Compound commands	$C ::= c \parallel [C \ ^{\kappa,\kappa}\ C]$
Substitutable terms	$t ::= V \parallel e$
Positive expressions	$v ::= V^{\diamond} \parallel \mu\alpha.C$
Values	$V ::= x \parallel (t,t) \parallel inl(t) \parallel inr(t) \parallel t^{\bullet}$
Negative expressions	$e ::= \overline{\alpha} \parallel \tilde{\mu}q.C$
Declarations	$\kappa ::= q \parallel \overline{\alpha}$
Counterpatterns	$q ::= x \parallel \kappa^{\bullet} \parallel (\kappa,\kappa) \parallel [\kappa,\kappa]$

The $\mu\tilde{\mu}$-calculus (2/2)

$$
\begin{array}{lrcl}
(\mu) & \langle \mu\alpha.c \mid e \rangle & \to & c[e/\overline{\alpha}] \\
(\tilde{\mu}) & \langle V^{\diamond} \mid \tilde{\mu}q.C \rangle & \to & C[V/q]
\end{array}
$$

$$C[V/q] = c\,\sigma \quad \text{if} \quad \lceil C\,,\,\{(V/q)\}\rceil \longrightarrow^{*} \lceil c\,,\,\sigma\rceil$$

$$
\begin{array}{lcl}
\lceil C\,,\,\{(t_1,t_2)/(\kappa_1,\kappa_2)\} \cup \sigma\rceil & \longrightarrow & \lceil C\,,\,\{t_1/\kappa_1, t_2/\kappa_2\} \cup \sigma\rceil \\
\lceil [C_1 \;{}^{\kappa_1,\kappa_2}\; C_2]\,,\,\{inl(t_1)/[\kappa_1,\kappa_2]\} \cup \sigma\rceil & \longrightarrow & \lceil C_1\,,\,\{t_1/\kappa_1\} \cup \sigma\rceil \\
\lceil [C_1 \;{}^{\kappa_1,\kappa_2}\; C_2]\,,\,\{inr(t_2)/[\kappa_1,\kappa_2]\} \cup \sigma\rceil & \longrightarrow & \lceil C_2\,,\,\{t_2/\kappa_2\} \cup \sigma\rceil \\
\lceil C\,,\,\{e^{\bullet}/\overline{\alpha}^{\bullet}\} \cup \sigma\rceil & \longrightarrow & \lceil C\,,\,\{e/\overline{\alpha}\} \cup \sigma\rceil \\
\lceil C\,,\,\{V^{\bullet}/q^{\bullet}\} \cup \sigma\rceil & \longrightarrow & \lceil C\,,\,\{V/q\} \cup \sigma\rceil
\end{array}
$$

The system LK$_{pol}$ (1/3)

$$
\begin{aligned}
A &::= P \parallel N \\
P &::= X \parallel A \otimes A \parallel A \oplus A \parallel (\downarrow A) \\
N &::= \overline{X} \parallel A ⅋ A \parallel A \& A \parallel (\uparrow A)
\end{aligned}
$$

Four kinds of judgements :

$$C : (\Lambda \vdash) \qquad (\Lambda \vdash v : P \,|\,) \qquad (\Lambda \vdash V : P\,;\,) \qquad (\Lambda \vdash e : N \,|\,)$$

We write $(\Lambda \vdash t : A \,|\,)$ collectively for $\left\{ \begin{array}{ll} (\Lambda \vdash V : P\,;\,) & (t = V, A = P) \\ (\Lambda \vdash e : N \,|\,) & (t = e, A = N) \end{array} \right.$ and we write $\kappa : A$ collectively for $\left\{ \begin{array}{ll} \overline{\alpha} : N & (\kappa = \overline{\alpha}, A = N) \\ q : P & (\kappa = q, A = P) \end{array} \right.$

The system LK$_{pol}$ (2/3)

$$\frac{}{\Lambda\,,\ x : P \vdash x : P\,;} \qquad \frac{\Lambda \vdash t : A \,|}{\Lambda \vdash t^{\bullet} :\downarrow A\,;}$$

$$\frac{\Lambda \vdash t_1 : A_1 \,| \qquad \Lambda \vdash t_2 : A_2 \,|}{\Lambda \vdash (t_1, t_2) : A_1 \otimes A_2\,;}$$

$$\frac{\Lambda \vdash t_1 : A_1 \,|}{\Lambda \vdash inl(t_1) : A_1 \oplus A_2\,;} \qquad \frac{\Lambda \vdash t_2 : A_2 \,|}{\Lambda \vdash inr(t_2) : A_1 \oplus A_2\,;}$$

$$\frac{\Lambda \vdash V : P\,;}{\Lambda \vdash V^{\diamond} \,|} \qquad \frac{C : (\Lambda\,,\ \overline{\alpha} : N \vdash)}{\Lambda \vdash \mu\alpha.C : \overline{N} \,|}$$

$$\frac{}{\Lambda\,,\ \overline{\alpha} : N \vdash \overline{\alpha} : N \,|} \qquad \frac{C : (\Lambda\,,\ q : P \vdash)}{\Lambda \vdash \tilde{\mu}q.C : \overline{P} \,|}$$

The system LK$_{pol}$ (3/3)

$$\frac{\Lambda \vdash v : P \mid \qquad \Lambda \vdash e : \overline{P} \mid}{\langle v \mid e \rangle : (\Lambda \vdash)}$$

$$\frac{c : (\Lambda\,,\ \kappa : A \vdash)}{c : (\Lambda\,,\ \kappa^{\bullet} : \downarrow A \vdash)} \qquad \frac{C : (\Lambda\,,\ \kappa_1 : A_1\,,\ \kappa_2 : A_2 \vdash)}{C : (\Lambda\,,\ (\kappa_1, \kappa_2) : A_1 \otimes A_2 \vdash)}$$

$$\frac{C_1 : (\Lambda\,,\ \kappa_1 : A_1 \vdash) \qquad C_2 : (\Lambda\,,\ \kappa_2 : A_2 \vdash)}{[C_1 \ {}^{q_1, q_2}\ C_2] : (\Lambda\,,\ [\kappa_1, \kappa_2] : A_1 \oplus A_2 \vdash)}$$

Translating CBN λ-calculus with strict pairs (1/2)

$$s ::= x \parallel ss \parallel \lambda x.s \parallel (s, s) \parallel \lambda(x, y).s$$
$$A ::= \overline{X} \parallel A \times A \parallel A \to A$$

$$\frac{\Gamma\,,\, x_1 : A_1\,,\, x_2 : A_2 \vdash s : B}{\Gamma \vdash \lambda(x_1, x_2).s : (A_1 \times A_2) \to B} \qquad \frac{\Gamma \vdash s_1 : A_1 \qquad \Gamma \vdash s_2 : A_2}{\Gamma \vdash (s_1, s_2) : A_1 \times A_2}$$

$$(\lambda(x_1, x_2).s)(s_1, s_2) \longrightarrow s[s_1/x_1\,,\, s_2/x_2]$$

Translating CBN λ-calculus with strict pairs (2/2)

$$[\![\overline{X}]\!] = \overline{X} \qquad [\![A \times B]\!] = [\![A]\!] \otimes [\![B]\!] \qquad [\![A \to B]\!] = (\uparrow \overline{A}) \otimes B$$

We take a bijection mapping variables $x : N$ ($N = \overline{X}$ or $N = A \to B$) to variables $\overline{\alpha} : [\![N]\!]$. We set :

$\xi = x^\diamond$ if $x : P$ ($P = A \otimes B$) and $\xi = \overline{\alpha}$ if $x : N$
$\{v \mid e\} = \langle v \mid e \rangle$ and $\{e \mid v\} = \langle v \mid e \rangle$
$\nu\overline{\beta} = \mu\beta$ and $\nu q = \tilde{\mu} q$

$$\begin{aligned}
&[\![x]\!] = \xi \\
&[\![\lambda x.s]\!] = \tilde{\mu}(\xi^\bullet, \zeta).\{\zeta \mid [\![s]\!]\} \\
&[\![\lambda(x_1, x_2).s]\!] = \tilde{\mu}((\xi_1, \xi_2)^\bullet, \zeta).\{\zeta \mid [\![s]\!]\} \\
&[\![st]\!] = \nu\zeta.\langle([\![t]\!]^\bullet, \zeta)^\diamond \mid [\![s]\!]\rangle \\
&[\![(s_1, s_2)]\!] = \mu\alpha.\{[\![s_1]\!] \mid \nu\zeta_1.\{[\![s_2]\!] \mid \nu\zeta_2.\langle(x, y)^\diamond \mid \overline{\alpha}\rangle\}\}
\end{aligned}$$

(one can easily extend to $s ::= \ldots \parallel inl(s) \parallel inr(s) \parallel \lambda[inl(y).s \mid inr(z).s]$)

Note that we can limit the use of $\mu\alpha$ to be linear in α.

Translating the $\mu\tilde{\mu}$-calculus back to the $\mu\tilde{\mu}^{+}$-calculus

Cases where the translation does not merely commute with the syntax :

$$
\begin{array}{l}
x^\dagger = x \quad inl(e)^\dagger = inl((e^\dagger)^\bullet) \quad inr(e)^\dagger = inl((e^\dagger)^\bullet) \quad (V^\bullet)^\dagger = V^\dagger \\
(V,e)^\dagger = (V^\dagger,(e^\dagger)^\bullet) \quad (e,V)^\dagger = ((e^\dagger)^\bullet,V^\dagger) \quad (e_1,e_2)^\dagger = ((e_1^\dagger)^\bullet,(e_2^\dagger)^\bullet) \\
\overline{\alpha}^\dagger = \alpha \quad (\tilde{\mu}q.C)^\dagger = \tilde{\mu}q^\dagger.C^\dagger
\end{array}
$$

$$
\begin{array}{l}
x^\dagger = x \quad (\overline{\alpha}^\bullet)^\dagger = \alpha^\bullet \quad (q^\bullet)^\dagger = q^\dagger \\
(q,\overline{\alpha})^\dagger = (q^\dagger,\alpha^\bullet) \quad (\overline{\alpha},q)^\dagger = (\alpha^\bullet,q^\dagger) \quad (\overline{\alpha},\overline{\beta})^\dagger = (\alpha^\bullet,\beta^\bullet) \\
[q,\overline{\alpha}]^\dagger = [q^\dagger,\alpha^\bullet] \quad [\overline{\alpha},q]^\dagger = [\alpha^\bullet,q^\dagger] \quad [\overline{\alpha},\overline{\beta}]^\dagger = [\alpha^\bullet,\beta^\bullet]
\end{array}
$$

Translating LK$_{pol}$ back to LKQ

We define $N^\dagger = \overline{\overline{N}^\dagger}$, and we define $P^\dagger$ as follows (cases where the translation does not merely commute with the syntax) :

$$
\begin{aligned}
&(P \otimes N)^\dagger = P^\dagger \otimes \neg^+(\overline{N}^\dagger)\\
&(N \otimes P)^\dagger = \neg^+(\overline{N}^\dagger) \otimes P^\dagger\\
&(N_1 \otimes N_2)^\dagger = \neg^+(\overline{N_1}^\dagger) \otimes \neg^+(\overline{N_2}^\dagger)\\
\\
&(P \oplus N)^\dagger = P^\dagger \oplus \neg^+(\overline{N}^\dagger)\\
&(N \oplus P)^\dagger = \neg^+(\overline{N}^\dagger) \oplus P^\dagger\\
&(N_1 \oplus N_2)^\dagger = \neg^+(\overline{N_1}^\dagger) \oplus \neg^+(\overline{N_2}^\dagger)\\
\\
&(\downarrow N)^\dagger = \neg^+(\overline{N}^\dagger)\\
&(\downarrow P)^\dagger = P^\dagger
\end{aligned}
$$

A whole chain of translations

$$\begin{array}{c}\text{Your favourite } \lambda\text{-calculus based language} \\ \downarrow_1 \\ \mu\widetilde{\mu} \\ \downarrow_2 \\ \mu\widetilde{\mu}^+ \\ \downarrow_3 \\ \lambda\text{-calculus} \\ \downarrow_4 \\ \text{Linear logic}\end{array}$$

The so-called CPS translation is $\rightarrow_1$ through $\rightarrow_3$, but in fact, all the real work (encoding of a reduction strategy) is made at $\rightarrow_1$ time.