HAL
archives-ouvertes.fr

L'identité des preuves : normalisation, réseaux et séparation

Jules Chouquet

▶ **To cite this version:**

Jules Chouquet. L'identité des preuves : normalisation, réseaux et séparation. Philosophie. 2016. <dumas-01427107>

HAL Id: dumas-01427107
https://dumas.ccsd.cnrs.fr/dumas-01427107

Submitted on 22 Feb 2017

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.

Université Paris–1 Panthéon–Sorbonne
UFR de Philosophie
Master Logique, Philosophie, Histoire des Sciences et de la Connaissance dir. Max Kistler
Parcours logique dir. Pierre Wagner

Spécialité : Théorie de la démonstration
Direction : Jean Fichot, Pierre Wagner

L'identité des preuves : normalisation, réseaux et séparation

Jules Chouquet

Paris, le 13 mai 2016

Résumé : La théorie de la démonstration présente divers systèmes formels de preuve permettant de représenter des démonstrations à l'aide d'objets rigoureusement définis, et dont la manipulation revêt divers intérêts. Nous nous proposons ici d'étudier la question — très débattue — de savoir à quelles conditions deux dérivations de ces systèmes représentent, décrivent, la même démonstration.

Nous étudions en particulier deux propositions de réponses, avant de mettre chacune en perspective pour une meilleure compréhension des concepts et appareils sollicités. Ces deux solutions correspondent respectivement à une relation d'équivalence induite par le processus de normalisation des dérivations défini par Gentzen dans les années 1930, et à un quotient par une représentation graphique des dérivations due à Girard (dans les années 1980) que sont les réseaux de preuve.

La Logique est une très bonne invention.

Ludwig Wittgenstein [1]

1. Lettre à Bertrand Russell, Vienne, le 6 janvier 1913. *in Correspondance (Cambridge)*, Trans–Europ–Repress, Pau, 2006 (pour la traduction française).

Table des matières

Remerciements

Je tiens à remercier en premier lieu les personnes qui m'ont aiguillé dans la compréhension de la question à laquelle je comptais m'atteler. D'abord Alberto Naibo pour ses précieuses indications thématiques et bibliographiques ; ensuite Alexis Saurin et Lionel Vaux pour les discussions éclairantes que j'ai eues avec eux à ce sujet ; Jean Fichot pour ses conseils et pour la considération dont il a fait preuve quant à mon travail.

Ensuite, dans le désordre et pour toutes sortes de raisons : V. Michele Abrusci, Arnaud Durand, Christian d'Elbée, Théo Escarret, Magali Georgeon, Hugo Herbelin, Max Kistler, Nelson Lepicouché, Marco Panza, et enfin Pierre Wagner pour avoir accepté de diriger ce mémoire.

1 Liminaires

1.1 Généralités historiques sur la théorie de la démonstration

S'il est délicat de fixer une origine nette de la théorie de la démonstration, on peut néanmoins déterminer différentes *phases* dans l'apparition des notions qui sont aujourd'hui à l'œuvre dans ce domaine. Les lignes qui suivent ne pouvant prétendre à une chronologie objective ni exhaustive, exhibent néanmoins chronologiquement les outils et l'arrière plan scientifique autour desquels tournera notre analyse.

Dans un premier temps, on peut mentionner les travaux de formalisation des raisonnements mathématiques, qui ont permis de commencer à questionner la notion de *démonstration* de façon presque autonome. Citons les travaux de Frege ([Fre84],[Fre79]), dans lesquels apparaît déjà le projet d'une « grande logique », un langage formel avec une grande expressivité permettant de traiter au moins l'arithmétique. On peut évoquer également les ambitions de Hilbert, dont le fameux *programme* consistait à écrire un système formel, à nouveau, dans lequel on pourrait démontrer toutes les propositions mathématiques vraies par des méthodes automatiques.

On sait que le système de Frege a été mis à mal par le paradoxe de Russell, montrant que l'on peut écrire dans le système formalisé une formule contradictoire (l'insuffisance du système était due à l'absence de restriction du schéma de compréhension : la célèbre loi V). On sait également que le programme de Hilbert a été anéanti par les théorèmes d'incomplétude de Gödel. Pour autant,

Hilbert aura introduit l'un des premiers systèmes de preuve formels, durant sa carrière. Ces systèmes sont constitués de règles d'inférences et d'axiomes, à partir desquels seront construites les *dérivations*. Nous ne nous étendrons pas sur ces méthodes, car si la grande simplicité de ces systèmes peut tenir lieu de vertu, nous retiendrons qu'elle les rend arides et inefficaces quant à la représentation des raisonnements démonstratifs.

Sans doute davantage que les théorèmes d'incomplétude (1931), c'est le théorème de complétude (1929) de Gödel qui aura une influence sur la théorie de la démonstration : un système déductif répondant à des contraintes relativement transparentes, logiquement parlant, permet de démontrer *toutes* les formules satisfaites dans un modèle. Nous en parlerons assez peu, souhaitant nous concentrer sur des questions syntaxiques, mais il faut noter que la pertinence d'un regard essentiellement syntaxique sans la connaissance de la complétude des systèmes déductifs, serait sans doute plus délicate à établir.

Ceci nous amène aux années 1930, où Gentzen, en réaction à ces systèmes « logicistes » ([Gen35]), introduit justement la déduction naturelle, qui se veut être apte à représenter les preuves le plus fidèlement possible au raisonnement effectif des mathématiciens. Les dérivations se construisent alors sous forme d'arbres, et Gentzen affirme que la naturalité de son système tient en grande partie à l'introduction de la notion de raisonnement hypothétique à l'intérieur même des règles de déduction.

Les axiomes des systèmes à la Hilbert sont finalement supprimés, ou internalisés dans les règles logiques, en quelque sorte. Par exemple, au lieu de poser $\mathbf{K} : \phi \to \psi \to \phi$ comme axiome (c'est le premier des systèmes propositionnels à la Hilbert), on se place dans un système où, sous l'hypothèse que la formule

ϕ est démontrée, on accorde que la formule $\psi \to \phi$ se démontre également. Ceci s'écrit comme une règle d'affaiblissement, si l'on écrit des séquents, ou comme une décharge vide en déduction naturelle standard.

Gentzen est d'avantage connu pour le théorème principal de son texte [Gen35], qui ne s'applique pas directement à la déduction naturelle, mais au calcul des séquents, système de preuve un peu moins intuitif, qu'il invente et définit dans le même texte, avant d'en prouver l'équivalence avec la déduction naturelle. Ce théorème, *hauptsatz*, est historiquement intéressant en ce qu'il définit un algorithme sur les preuves : une procédure automatique qui, d'une dérivation donnée π, extrait une nouvelle dérivation π'. La preuve devient ici un objet manipulé par des instructions, comme *l'argument* d'une fonction. Ce trait nous intéresse en ce que l'on oublie le théorème qui est prouvé, pour en manipuler les preuves de façon indépendante.

Le théorème d'élimination des coupures montre que d'une preuve contenant des « détours » — des voies indirectes, ou non analytiques, pour parvenir à sa conclusion — on peut écrire une preuve de la même conclusion sans ces détours, ils auront été éliminés durant la procédure définie par Gentzen.

Le calcul des séquents aura été inventé spécifiquement pour la preuve de ce théorème. Et bien qu'il soit démontré équivalent à la déduction naturelle, il faudra attendre les travaux de Prawitz pour avoir une élimination des coupures s'appliquant directement à ce système.

Les années 1950 verront apparaître une nouvelle découverte, paraissant anodine à ses acteurs, mais pourtant d'une fécondité encore croissante. La logique combinatoire de Curry, à l'instar de son homologue le λ-calcul de Church, fut pensée comme un système de termes s'appliquant les uns aux

autres, et muni de réductions très simples. Dans [CF58], Curry définit cette logique en posant deux *combinateurs*, **S** et **K** caractérisés par leurs règles de réductions :

- $(\mathbf{K}x)y = x$
- $\mathbf{S}xyz = xz(yz)$

Curry reconnaît dans ces combinateurs les deux axiomes des systèmes propositionnels à la Hilbert :

$\mathbf{K} : \phi \to \psi \to \phi$ et $\mathbf{S} : (\phi \to \psi \to \theta) \to (\phi \to \psi) \to (\phi \to \theta)$.

C'est la première pierre posée à l'édifice de la fameuse correspondance de Curry-Howard. Car ce que Curry reconnaît s'exprime en effet par une correspondance forte, appelée parfois même « isomorphisme » : Si l'on donne pour types aux combinateurs, des formules adaptées, comme dans ce cas, alors les applications des combinateurs entre eux correspondent aux preuves des formules par lesquelles ils sont typés. Par suite, Howard montrera dans les années 1980 que le λ-calcul correspond à la déduction naturelle intuitionniste.

Ce que l'on notera, et qui continuera par la suite à nous intéresser, c'est la notion de calcul que cette correspondance rattache fortement aux preuves formelles. La logique combinatoire et le λ-calcul sont des systèmes qui calculent *vraiment*, on peut par exemple traduire toutes les fonctions récursives dans des λ-termes (regarder exemple [Bar84]). La thèse de Church, sur laquelle nous reviendrons, pose justement que tout ce qui est intuitivement calculable, l'est également via la λ-calcul.

Un point majeur de notre étude se concentrera sur l'aspect dynamique de la correspondance de Curry-Howard. La relation $\to_\beta$ sur les λ-termes correspond au processus d'élimination des coupures sur les preuves associées. La re-

lation $\rightarrow_\eta$ correspond à l'expansion des axiomes aux atomes. On questionnera notamment les motivations et la pertinence de l'admission de l'équivalence $\beta\eta$ comme identité entre les preuves.

De cette correspondance est issu un développement important des liens entre théorie de la démonstration et algorithmique. On peut évoquer la programmation fonctionnelle des langages Caml ou Haskell (ce dernier devant justement son nom à Curry) qui sont un exemple des ponts établis entre logique et informatique. L'identité entre les preuves, à travers ce prisme, posera la même question que l'identité entre les programmes ; et la difficulté que l'on éprouve à définir en toute généralité ce qu'est une démonstration peut être vue comme l'analogue de la difficulté à définir un algorithme, le travail de Gurevitch ([Gur12]) en expose clairement les enjeux et obstacles.

Les années 1990 voient apparaître deux avancées majeures dans la théorie de la démonstration : d'une part la découverte par Tim Griffin que la correspondance de Curry-Howard peut être étendue à la logique classique (via la loi de Peirce $((\phi \rightarrow \psi) \rightarrow \phi) \rightarrow \phi$ comme typage de l'opérateur de contrôle callcc, voir [Gri90]). Cette découverte sera extrêmement féconde et donnera naissance à de nouvaux calculs comme le $\lambda\mu$-calcul de Parigot, ou le $\lambda\mu\tilde{\mu}$-calcul de Herbelin, deux systèmes permettant de donner un contenu calcultatoire aux preuves de la logique classique (déduction naturelle pour le premier, calcul des séquents pour le second).

Nous nous intéresserons à une autre avancée logique de la fin du siècle dernier, à savoir l'apparition de la logique linéaire, dont on peut lire les premières formulations dans [Gir87], l'article fondateur de Girard. Ce raffinement de la logique, distinguant les opérateurs classiques et intuitionnistes via deux

disjonctions et deux conjonctions, et contrôlant les règles structurelles par des modalités, présente une nouvelle possibilité d'écrire les démonstrations à laquelle nous porterons une attention particulière : les réseaux de preuve. Cette syntaxe graphique, rendue populaire par sa clarté et sa maniabilité, est un outil de généralisation des séquents de la logique linéaire présentant par là un lieu d'étude fécond, bien que problématique, pour la question de l'identité des preuves.

1.2 Conventions et définitions

1.2.1 Le λ-calcul

Par **λ-termes**, nous entendons l'ensemble L des termes construits sur la grammaire suivante : $V \mid \lambda x.L \mid (LL)$, où V est un ensemble dénombrable de variables notées $x, y, z, x_1, x_2, \ldots$ et quotienté par la relation d'équivalence $\equiv_\alpha$, où $M \equiv_\alpha N$ si M peut être obtenu depuis N en renommant ses variables liées de façon à éviter les captures. Ici, les **variables liées** d'un terme M étant les variables $x_1, \ldots, x_n$ apparaissant respectivement dans les sous-termes abstractions de N commençant par $\lambda x_1, \ldots, \lambda x_n$ (respectivement). Les termes de la forme $\lambda x M$ sont appelés **abstractions** et ceux de la forme (MN) sont appelés **applications**. Nous omettrons les parenthèses extérieures des applications dès que possible, s'il n'y a pas d'ambiguïté, tout en considérant que le parenthésage implicite associe à gauche (MNP abrège $(MN)P$). Nous suivons ainsi les conventions d'écriture dites « de Cambridge », que l'on trouve dans [Bar84].

On dira qu'une relation $\rightarrow^*$ **passe au contexte** si pour tous termes

$M, M', N \in \Lambda$, on a :

- $M \to^* M' \Rightarrow (MN) \to^* (M'N)$
- $M \to^* M' \Rightarrow (NM) \to^* (NM')$
- $M \to^* M' \Rightarrow \lambda x M \to^* \lambda x M'$

On notera $\Lambda = L_{/\equiv_\alpha}$ l'ensemble des λ-termes (qui sont donc des représentants d'α-classes sur L).

Le **λ-calcul** est l'ensemble des termes Λ équipé d'une relation binaire $=_\beta$ définie comme la clôture réflexive, symétrique et transitive de la relation $\to_\beta$, appelée β-réduction simple, et définie comme suit :

$$(\lambda x M)N \to_\beta M[x := N]$$

pour tous λ-termes M, N, et toute variable x, et passant au contexte.

Nous parlerons également de l'extension du calcul par la relation binaire η, qui correspond au calcul que nous venons de définir, muni en plus de la relation $=_\eta$, qui est la clôture réflexive, symétrique et transitive de la relation $\to_\eta$, appelée η-expansion, et définie comme suit :

$$M \to_\eta \lambda x M x$$

Pour tous λ-termes M, et toute variable x, et passant au contexte.

Nous parlerons souvent de la $\beta\eta$- égalité, il s'agît de la réunion des relations $=_\beta$ et $=_\eta$, abrégée $=_{\beta\eta}$.

1.2.2 Formules et $\Lambda^{\to}$

Lorsque nous évoquerons les systèmes à la Hilbert et la correspondance de Curry-Howard, on pourra se contenter du calcul propositionnel implicatif et du λ-calcul simplement typé (calcul noté $\Lambda^{\to}$). Nous utiliserons de préférence un typage à la Curry.

Nous considérons pour les formules, la grammaire suivante :

$$\Phi \ ::= \ A \ \mid \ (\Phi \to \Phi)$$

où A est un ensemble dénombrable de variables propositionnelles. On omettra à nouveau les prenthèses extérieures, mais en admettant cette fois une association implicite à droite : $\phi \to \psi \to \theta$ renvoie à $(\phi \to (\psi \to \theta))$.

Le système $\Lambda^{\to}$ est défini par les règles de dérivation suivantes, pour tous $x, y, z \in V$, tous $M, N \in \Lambda$ et tous $\phi, \psi \in \Phi$:

– Axiome-identité : $\dfrac{}{x : \phi \vdash x : \phi}\,\mathrm{Ax}$

– Abstraction/ $\to$-int : $\dfrac{\Gamma, x : \phi \vdash M : \psi}{\Gamma \vdash \lambda x M : \phi \to \psi}\,{\to}\mathrm{i}$

– Application/ $\to$elim : $\dfrac{\Gamma \vdash M : \phi \to \psi \qquad \Delta \vdash N : \phi}{\Gamma, \Delta \vdash (M)N : \psi}\,{\to}\mathrm{e}\ [\Gamma \cap \Delta = \emptyset]$

– Affaiblissement : $\dfrac{\Gamma \vdash M : \phi}{\Gamma, x : \psi \vdash M : \phi}$ Aff

– Contraction : $\dfrac{\Gamma, x : \phi, y : \phi \vdash M : \psi}{z : \phi, \Gamma \vdash M[z/x, z/y] : \psi}$ Cont

Ce système de déduction permet de comprendre ce que nous entendons par la correspondance entre le λ-calcul (pur) et la déduction naturelle : les termes écrits dans ce systèmes sont en correspondance de façon explicite avec les preuves dont en sont issus les types.

On remarque en particulier que la règle de β-réduction du λ-calcul correspond à l'élimination d'une coupure dans la preuve associée. En effet, un terme $\lambda x M$ n'est typable que par une implication $\phi \to \psi$, et ne peut s'appliquer qu'à un terme de type ϕ, par définition de la règle $\to$elim. On a donc l'introduction de l'implication, suivie de son élimination : c'est bien une coupure en déduction naturelle, qui se simplifie par la preuve de ψ donnée par $M[x := N]$ qui conserve le bon type. Cette propriété de conservation des types par réduction est appelée **réduction du sujet**.

D'autre part, la règle d'η-expansion préserve également le type, mais elle correspond dans la démonstration à une autre opération : l'extension des axiomes aux atomes.

1.2.3 Logique linéaire (fragment multiplicatif)

Le fragment multiplicatif de la logique linéaire (abrégé MLL) correspond aux formules construites sur la grammaire suivante :

$$F ::= \ X \ \mid \ F^{\perp} \ \mid \ F \parr F \ \mid \ F \otimes F$$

Nous donnons les règles du calcul des séquents associé pour A, B des formules de MLL, et Γ, Δ des ensembles de formules de MLL :

- Axiome : $\dfrac{}{\vdash A, A^{\perp}}$
- Coupure $\dfrac{\vdash \Gamma, A \qquad \vdash \Delta, A^{\perp}}{\vdash \Gamma, \Delta}$
- Tenseur : $\dfrac{\vdash \Gamma, A \qquad \vdash \Delta, B}{\vdash \Gamma, \Delta, A \otimes B}$
- Par : $\dfrac{\vdash \Gamma, A, B}{\vdash \Gamma, A \parr B}$

Les lois de De Morgan associées sont les suivantes :

- $(A \otimes B)^{\perp} \Leftrightarrow A^{\perp} \parr B^{\perp}$
- $(A \parr B)^{\perp} \Leftrightarrow A^{\perp} \otimes B^{\perp}$

1.2.4 Fragment exponentiel

Aux formules de MLL, on rajoute deux connecteurs unaires dits *exponentiels* : ? (pourquoi pas) et ! (bien sûr). On a donc pour le fragment multiplicatif

exponentiel de la logique linéaire (MELL) la grammaire suivante :

$$F ::= \ X \ \mid \ F^{\perp} \ \mid \ ?F \ \mid \ !F \ \mid \ F \parr F \ \mid \ F \otimes F$$

On ajoute les règles du calcul des séquents suivantes :

- Déréliction : $\dfrac{\vdash \Gamma, A}{\vdash \Gamma, ?A}$
- Contraction : $\dfrac{\vdash \Gamma, ?A, ?A}{\vdash \Gamma, ?A}$
- Affaiblissement : $\dfrac{\vdash \Gamma}{\vdash \Gamma, ?A}$
- Promotion : $\dfrac{\vdash A_1, \ldots, ?A_n, A}{\vdash ?A_1, \ldots, ?A_n, !A}$

Et on précise les lois de De Morgan :

- $(?A)^{\perp} \Leftrightarrow !A^{\perp}$
- $(!A)^{\perp} \Leftrightarrow ?A^{\perp}$

1.2.5 Note terminologique

Pour mener à bien le travail que nous présentons ici, il a fallu procéder parfois à des choix arbitraires de terminologie pour éviter de s'embourber dans des discussions complexes sur l'utilisation de certains mots ; où la confusion nous mènerait à des erreurs philosophiques ou à des circularités.

Pour autant, n'ayant d'autre choix que de s'exprimer d'une manière ou d'une autre, il a fallu évacuer certains de ces problèmes en assumant des choix

contestables, mais l'aspect pléonastique de cette dernière formule n'est-il pas en soi une première excuse à ces imprécisions lexicologiques ?

Si nous essayons d'être clair, et si la plupart du temps le contexte d'énonciation devrait nous dispenser d'une note terminologique, nous annonçons ici le choix que nous avons fait et qui sera à retenir dans la compréhension de tout notre exposé, quant aux significations des termes **preuve, démonstration, déduction, dérivation**.

S'il existe des **preuves** d'amour ou de bonne foi, ce qu'en seraient les **démonstrations** est loin d'être clair. Pour autant, dans notre contexte appuyé sur la logique formelle, nous identifierons ces deux termes et les emploierons indifféremment. Il est difficile de dire précisément à quoi ils renvoient, dans la mesure où notre mémoire se veut éclairant pour la question philosophique « Qu'est-ce qu'une preuve / Qu'est-ce qu'une démonstration ». Essayons de donner une idée, pour pouvoir les distinguer des autres termes évoqués. Une démonstration ou une preuve sera comprise comme le raisonnement conduisant depuis la compréhension des hypothèses à la conviction que la conclusion à laquelle il aboutit en découle logiquement. [2] On considère un aspect intuitif, psychologique, et non formel. Nous parlerons parfois de l'*idée de preuve* pour insister sur ce point.

Les dérivations sont le pendant définissable et formel des démonstrations. Elles sont des objets mathématiques définis formellement comme des suites de

2. Cette conviction est également relative à l'acception du bien fondé des inférences utilisées ; mais essayer d'être plus précis, à nouveau, nous pousserait à nous embourber dans des problèmes à tiroirs.

symboles, souvent comme des arbres dont les feuilles sont appelées hypothèses et le tronc conclusion. Lorsque nous emploierons le terme de **déduction**, nous parlerons le plus souvent de déduction formelle ou de système de déduction. Dans les deux cas, nous renvoyons également aux objets formels tels que les arbres du calcul des séquents et de la déduction naturelle, aux systèmes axiomatiques à la Hilbert, ou encore aux réseaux de preuve.

1.3 Motivations

Après avoir essayé de donner un aperçu du contexte historique, théorique et technique dans lequel se situera notre étude, il nous en faut déterminer les contours. Les lignes qui suivent se veulent une description du problème que nous traitons ainsi que des raisons qui peuvent pousser le logicien — mathématicien tant que philosophe — à se pencher dessus.

1.3.1 La déductibilité et les dérivations

Une vision des mathématiques, sans doute naïve mais éclairante pour notre objet, tendrait à présenter les mathématiciens et logiciens (hors théoriciens de la démonstration naturellement) comme ne s'attachant aux démonstrations que pour établir une relation de déductibilité entre les formules. Cette pratique consisterait pour le mathématicien à se demander pour un ensemble (éventuellement vide) de formules Γ si oui ou non une autre formule A en est déductible. On se demande ce qui est vrai dans la théorie, c'est-à-dire en général ce que l'on peut y démontrer. Une fois le résultat établi, on peut l'utiliser et l'admettre à loisir sans se replonger dans les détails de sa démonstration,

car l'objectif est justement d'établir des résultats.

D'autre part, la théorie de la démonstration s'intéresse d'avantage à la façon dont les théorèmes sont établis qu'aux théorèmes en eux-mêmes. Si l'on considère les travaux de Gentzen comme une première possibilité d'analyse structurelle des démonstrations, on peut voir qu'apparaissent dans ses travaux un ensemble de considérations dont la nature des théorèmes dérivés est d'importance secondaire. Quand on procède par exemple à la distinction entre les théorèmes classiques et les théorèmes intuitionnistes, on ne se demande ce qui est démontrable qu'au regard des propriétés que cela impose sur les systèmes de déduction.

Notre étude se place dans la seconde mentalité, presque poussée à l'extrême dans la mesure où l'on ne se demandera même pas ce à quoi nos dérivations aboutissent. L'objet va ici être de considérer différentes dérivations de la même formule (ou du même séquent) depuis les mêmes hypothèses et de se demander quand elles renvoient ou non à la même démonstration. On trouve dans [KK67] l'idée qu'une dérivation est la *description* d'une démonstration (Revoir 1.2.5 pour nos choix terminologiques), et c'est cette idée qui nous guidera et nous aiguillera tout le long de notre étude. On peut alors donner une première formulation de la question de l'identité : comment déterminer avec précision quand deux dérivation décrivent ou non la même preuve ?

1.3.2 La théorie de la démonstration : une théorie équationnelle ?

On peut raisonnablement se demander ce qui motive l'étude de cette question pour un mathématicien ou un philosophe. La théorie de la démonstration propose donc un travail détaillé et profond de la structure et des propriétés

des systèmes de déduction, pour résumer. Sa spécificité se concentre d'abord sur la façon de considérer les preuves en tant qu'objets pour l'étude logique, et cette étude saisit les preuves à travers lesdits systèmes.

Les preuves ne sont pas des moyens termes entre les hypothèses et les conclusions, mais des objets définis rigoureusement à travers des définitions solides, de la même façon que peuvent l'être les termes d'un langage, ou les éléments d'une structure algébrique (cette comparaison nous suivra notamment en 4.1). Dans ce dernier cas, si l'on prend l'exemple du corps $(\mathbb{R}, 0, 1, +, \times)$ et le langage du premier ordre associé, on remarque que les formules que l'on peut écrire concernent les égalités entre les termes (ici, $t ::= \ V \mid 0 \mid 1 \mid \ + (t,t) \mid \ \times (t,t)$). Les seules formules atomiques écrites dans ce langage seront des formules posant une certaine égalité entre deux termes. On pourra parler de théories équationnelles, on peut décrire les polynômes, dire s'ils ont ou non une solution, et c'est essentiellement l'intérêt d'une telle théorie : déterminer quels termes renvoient ou non au même objet. On essaiera de savoir pour quelles valeurs de x la formule $p(x) = 0$ sera vraie, où p est un polynôme.

De la même façon, il est naturel de se demander dans un cadre théorique où les objets manipulés sont les preuves elles-mêmes, à quelles conditions deux dérivations sont identiques ou non. La correspondance de Curry–Howard permettant de considérer les dérivations comme des termes nous pousse également dans cette voie, et l'on voudrait savoir quand deux λ-termes *décrivent* la même démonstration. On étudiera d'ailleurs en détail la possibilité d'utiliser $=_{\beta\eta}$ dans ce but (voir 2). On peut voir la nécessité d'identifier les dérivations comme la moindre des requêtes pour une théorie dont elles constituent les éléments de base.

1.3.3 Identité, équivalence et synonymie

Déterminer quelles dérivations sont à décréter identiques au sein d'une théorie ne relève par ailleurs pas seulement d'une nécessité mathématique, mais peut aussi se voir comme une façon d'éclairer la question plus philosophique : « qu'est-ce qu'une preuve ? ». On part en effet du principe, qui semble être communément admis, que les dérivations sont des descriptions des preuves. Pour autant, on ne sait pas exactement comment déterminer ce que sont les preuves en question, dans la mesure où on les saisit à travers leurs descriptions formelles exclusivement.

Ne pas pouvoir définir ce qu'est une preuve — comprise comme un processus non formalisé, logique, psychologique, pédagogique, épistémique — nous obstrue de fait la possibilité de pouvoir les distinguer ou les identifier de façon directe. En revanche, il peut être de circonstance de revoir la question en étudiant les objets que l'on a sous la main : les dérivations et systèmes de déduction. Pour traduire alors la notion d'identité entre preuves dans nos systèmes formels, il va falloir introduire une notion de **synonymie** entre ces dérivations, se demander quand elles ont le même sens, c'est à dire quand elles décrivent la même chose.

Pour cela, nous souhaitons établir une relation d'équivalence entre les dérivations, nous assurant que deux dérivations équivalentes décrivent deux preuves identiques, autant dire une seule et même preuve. Si l'on accepte que toute preuve est descriptible en une dérivation et que toute dérivation décrit une preuve, alors la partition définie par le quotient de la relation d'équivalence définie aura permis de discerner les preuves en ce sens : une preuve

coïncide avec une classe d'équivalence dans les dérivations. Au sein d'un système donné, on a capturé toutes les descriptions possibles de la preuve dans la classe d'équivalence. Un résultat de la sorte serait bien entendu un pas en avant pour la compréhension de ce dont nous parlons quand nous parlons de preuve ; toute la difficulté étant de donner la bonne relation d'équivalence. C'est tout le sujet de notre étude d'examiner en détail les différentes propositions qui ont pu être formulées dans ce sens, et de comprendre le lien entre ces solutions et la compréhension sous-jacente des éléments intrinsèques aux démonstrations en elles-mêmes.

1.3.4 L'informel et le rigoureux : remarque bibliographique

Kreisel parlait de rigueur informelle en évoquant la question de l'identité des preuves. L'aspect informel du problème est indubitablement lié à l'absence de notion claire pour définir les preuves. Nous y reviendrons, mais nous avons déjà évoqué la comparaison entre les preuves et les algorithmes ; les objets — même abstraits ou mentaux — que sont les procédures de calcul, les algorithmes, posent moins de problème que les démonstrations, car il semble y avoir consensus sur ce que peut être un algorithme, et la thèse de Church prétend capturer ces objets. L'aspect informel est moins présent que dans ce qui nous occupe.

Ici, on dispose d'un notion intuitive peu claire de ce que pourrait être une preuve ou une démonstration, et on se demande dans quelle mesure déterminer cette notion peut se faire à travers une étude technique et rigoureuse du pendant formel que l'on peut étudier.

Il suffit de parcourir notre bibliographie pour se faire une idée de l'im-

portance que peuvent revêtir des résultats techniques pour la compréhension du problème informel qui est le notre. La plupart des articles cités sont des articles soit historiquement fondateurs car initiant une nouvelle façon de décrire les preuves (parmi lesquels [Gen35], [Gir87]) soit d'un intérêt technique pour le développement de ces méthodes. Les textes questionnant l'identité des preuves d'un point de vue philosophique sans essayer d'apporter une solution ou une analyse mathématique ne foisonnent pas. Les articles se référant explicitement au problème comme [Wid01], [Dos03], [Hug06] présentent chacun une étude des théorèmes et résultats techniques impliqués par les éventuelles réponses proposées. On ne trouve des considérations plus théoriques guère qu'à l'état de remarques ou de paragraphes chez des auteurs comme Prawitz, Kreisel ou Troelstra ([Pra75],[Kre72],[Tro75]).

La plupart de ces articles sont en anglais, (pas [GFL55]), nous proposons une traduction française des extraits cités.

2 L'identité et la normalisation

Le procédé de normalisation des dérivations introduit par Gentzen est souvent considéré comme le premier exemple d'analyse structurelle des preuves. Sans modifier ni les hypothèses ni la conclusion, on possède un moyen de regarder la structure de la démonstration et d'en modifier les articulations. Cette modification, le procédé d'élimination des coupures, est l'objet de l'étude qui suit. Nous inspectons les solutions proposées à la question de l'identité entre preuves à travers l'idée de normalisation.

Avant d'énoncer et d'étudier cette solution, explicitement formulée par Prawitz dans [Pra75], nous jetons un œil sur les motivations qui ont conduit Gentzen à établir ces instruments d'analyse des dérivations.

2.1 Gentzen et l'*Haupsatz*

> « *Les résultats de Gentzen sont décevants pour la logique scolaire, paisible gardienne des principes du bon sens. Mais ils sont stimulants pour le philosophe, qui a toujours cru à une certaine fécondité des déductions logiques. Cette fécondité suppose des possibilités constructives indéfinies, possibilités que l'intuition fait entrevoir et qu'une technique de raisonnement comme celle de Gentzen rend explicites.* »

écrit Robert Feys dans [GFL55] vingt ans après la parution du mémoire de Gentzen ([Gen35]).

Le logicien et philosophe donne également un point de départ à l'analyse de la *naturalité* des systèmes déductifs proposés par Gentzen : « *Il a*

relevé l'usage fréquent et tout naturel, en mathématiques, de raisonnements à partir d'une supposition. »[3] Gentzen écrit en effet explicitement, dans cet article où est introduite la déduction naturelle, que l'un de ses objectifs est de formaliser en un calcul précis les déductions telles qu'elles sont formulées dans le raisonnement mathématique. L'opposition — confessée — aux formalismes axiomatiques de Frege, Russell, et surtout Hilbert s'écrit en ce sens : Gentzen veut faire rentrer la démarche de la supposition à l'intérieur du calcul. La déduction de formules à partir d'un nombre fini d'axiomes et de trois règles de réduction (dans les systèmes à la Hilbert : détachement, généralisation, instanciation) est bien efficace et générale ; mais si on la regarde comme une traduction du raisonnement mathématique effectif, on reconnaît avec grand peine l'original dans la copie. On peut s'amuser à regarder la preuve de l'identité $\phi \to \phi$ à partir des deux axiomes $K : \phi \to (\psi \to \phi)$ et $S : (\phi \to (\psi \to \theta)) \to ((\phi \to \psi) \to (\phi \to \theta))$ qui se fait par détachement sur $(SK)K$[4] : on est assez loin de l'intuition...

Si Gentzen fait *rentrer* la supposition dans le calcul, c'est dans la mesure où les axiomes sont remplacés par des règles de déduction. Et ce qui est supposé, outre la validité des règles du point de vue de la logique, n'est plus fixé par définition (comme dans les systèmes axiomatiques que Gentzen appelle *logistiques*) mais apparaît dans le calcul comme une dépendance. En cela, la supposition est inhérente à chaque déduction qui l'invoque, ce n'est plus un catalogue de formules définissant le calcul.

3. *Ibid.*

4. On pourra se reporter au manuel *Combinatory Logic* de Curry et Feys ([CF58]) pour voir comment s'articule ce système dont Curry a montré qu'il correspond au fragment implicatif des systèmes à la Hilbert.

Cette nouveauté dans le calcul des prédicats se traduit donc en déduction naturelle par la notion d'hypothèse non déchargée. Gentzen n'explicite pas en ces termes la supposition dans **NJ** et **NK**, mais se contente de laisser au lecteur *voir* qu'une assertion dépend d'une autre à un moment de la dérivation.

Le théorème d'élimination des coupures, qui trouve ici sa première formulation pour **LJ** et **LK**, définis dans le même texte exprime déjà une façon très particulière de voir les démonstrations. Ce que l'on appelle une coupure [5] est considérée par Gentzen comme un détour dans la preuve : son élimination sera un moyen d'obtenir une preuve plus directe (dans le sens de la propriété de la sous-formule).

Widebäck remarque avec justesse dans [Wid01] que l'exposition du calcul sous la forme définie par Gentzen, sous forme d'arbres (déduction naturelle ou calcul des séquents) correspond déjà à une première identification entre les preuves, Widebäck cite ces lignes : « *En exigeant que les formules soient en ordre généalogique, nous nous écartons quelque peu de l'analogie avec la raisonnement réel. Car :*

1. *Dans le raisonnement réel, par suite de la linéarité de la pensée, on a nécessairement une suite linéaire de propositions ; et*
2. *Dans le raisonnement réel, on doit ordinairement réutiliser plusieurs fois un résultat qui a déjà été obtenu, alors que l'ordre généalogique ne permet, dans chaque cas, qu'une seule application d'une formule qui a été dérivée. Ces deux divergences doivent nous permettre de donner une définition plus appropriée au concept de dérivation et n'ont rien d'essentiel. »*

5. Notons que la démonstration originale élimine la règle *Mix* de coupure–contraction.

([GFL55]).

En effet, si les permutations triviales du calcul des séquents semblent être des règles que notre critère d'identité doive effacer en quotientant les preuves, on remarque que le calcul, s'il est effectivement une traduction qui se veut fidèle du raisonnement mathématique effectif, identifie déjà un bon nombre de raisonnements. Prenons simplement l'introduction de la conjonction : on raisonne en considérant d'abord A, puis ensuite B, avant d'admettre $A \wedge B$. Alors pour n occurrences de la règle d'introduction de la conjonction dans une dérivation de **LK** ou **LJ**, on a déjà affaire à l'expression d'au moins 2^n raisonnements associés. Le deuxième point de la citation soulève la même remarque quant à la réutilisation de propositions démontrées.

Les « préférences de technicien » qu'évoque Feys dans [GFL55] (préface) semblent avoir amené Gentzen à son *Hauptsatz* non en vue d'une nouvelle conception des preuves, mais en vue de résultats dont l'élimination des coupures facilite l'obtention. Citons le théorème du séquent médian (*haupsatz* renforcé, où raffiné, dans le texte), posant qu'un séquent Γ valide composé de formules prénexes peut donner lieu à une preuve de la forme suivante :

$$\begin{array}{c} [\pi] \\ \vdash A_1, \ldots, A_n \\ | \vdots | \\ [\theta] \\ | \vdots | \\ \vdash \Gamma \end{array}$$

Où les formules $A_1, \ldots, A_n$ sont sans quantificateurs : π est une dérivation essentiellement propositionnelle ; et le « tronc » θ n'est composée que d'in-

troductions de quantificateurs $\forall$ ou $\exists$. Le séquent $\vdash A_1, \ldots, A_n$ est appelé le *séquent médian.*

Cette application permet notamment à Gentzen de donner une preuve de cohérence pour l'arithmétique faible (sans schéma de récurrence) : le séquent médian permet de réduire toute preuve de cette arithmétique à une trivialité propositionnelle reposant sur des vérités logiques communément admises.

L'élimination des coupures permet également de donner une procédure de décision pour le calcul propositionnel intuitionniste : avec la propriété de la sous-formule qui découle du théorème, depuis un séquent donné on ne peut former qu'un nombre fini de configurations arborescentes composées de sous-formules du séquent, et vérifier si ces configurations correspondent aux dérivations définies donne alors la dérivabilité ou la non-dérivabilité du séquent en question.

Rappelons que le théorème d'élimination des coupures a été adapté au système de la déduction naturelle par Prawitz dans [Pra65], bien que cette extension ait été partiellement anticipée par Gentzen. Le point qui va nous intéresser est relatif à la déduction naturelle et à Prawitz, mais c'est dans [Pra75] que nous irons chercher.

2.2 La conjecture de Prawitz

> « 2.3. *La représentation des preuves par des dérivations formelles. De la même façon que l'on demande quand deux formules définissent le même ensemble, où quand deux phrases expriment la même proposition, on cherche à établir un critère d'identité pour*

les preuves, ou une relation de "synonymie" (ou équivalence) entre les dérivations. » ([Pra75] p.237)

Il s'agit, dans le texte, du troisième des sujet de recherche que Prawitz identifie comme évidents et primordiaux en théorie de la démonstration. Mais il ne se contente pas de lister les objectifs heuristiques liés à ce domaine, il propose une réponse à cette question, dans ce que [Dos03] appelle la *conjecture de normalisation*. Cette conjecture consiste justement à considérer le processus de normalisation des preuves (sa clôture réflexive symétrique et transitive) comme relation apte à déterminer les démonstrations identiques, *synonymes*. La relation d'équivalence, correspond alors (nous en avons touché un mot en illustrant le cas de $\Lambda^{\rightarrow}$ en section 1.2.2) à la relation de β-égalité, enrichie par η. Si l'on cherche à établir une relation d'équivalence entre les dérivations, que l'on noterait $\sim_{id}$, la conjecture de Prawitz consisterait à poser la définition suivante de cette relation, pour des preuves π, π' :

$$\pi \sim_{Id} \pi' \Leftrightarrow \pi =_{\beta\eta} \pi'$$

On comprend ici la relation $=_{\beta\eta}$ comme agissant sur les preuves associées aux λ-termes pour lesquels elle est définie ; grossièrement, on utilise la notion de $\beta\eta$-égalité « à Curry-Howard près », de façon à alléger le propos.

Dans le même texte, Prawitz formule ainsi sa réponse à la question évoquée en 2.3 :

« 3.5.6 **Conjecture :** Deux dérivations représentent la même preuve si et seulement si elles sont équivalentes. »

Le terme "équivalentes" est donc à comprendre comme "ayant la même

forme normale". Avant d'évoquer des justifications plus contemporaines et techniques, il nous faut noter que cette formalisation de la notion intuitive d'identité part également d'un constat intuitif : « une réduction n'a pas d'effet sur l'identité de la preuve. » (*Op cit.* p.257), accompagné de la réserve suivante : « Il peut y avoir des doutes par rapport à [l'élimination de la disjonction] et [l'élimination du quantificateur existentiel] mais l'on doit pouvoir trouver une réduction plus directe. »

C'est ce constat qui va pousser Prawitz à juger le sens "$\Leftarrow$" non problématique, comme une « thèse raisonnable » (*Op. cit.*), avant d'admettre qu'il semble difficile de trouver des faits pour confirmer l'autre sens de l'équivalence.

Un autre point appuyant la conjecture est la cohérence que lui donnent les théorèmes de confluence. Si deux preuves sont identiques quand elles ont la même forme normale, alors l'existence de deux preuves normales distinctes de la même formule implique que toutes les preuves de mêmes conclusions ne sont pas identiques ; en vertu de la confluence des réductions.

On peut penser au pendant λ-calculatoire de ce théorème de confluence : la propriété de la vallée, corollaire du théorème de Church Rosser, pose que pour tous $t_1, t_2 \in \Lambda$, si $t_1 =_\beta t_2$ alors il existe $t_3 \in \Lambda$ tel que $t_1 \twoheadrightarrow_\beta t_3$ et $t_2 \twoheadrightarrow_\beta t_3$. ($\twoheadrightarrow_\beta$ est la clôture réflexive et transitive de $\rightarrow_\beta$). De cette propriété, il suit que l'on peut trouver deux termes qui ne sont pas β-égaux, prenons $\lambda x \lambda y x$ et $\lambda x \lambda y y$ qui sont deux termes irréductibles : s'ils étaient égaux, on pourrait les réduire à un terme commun, ce qui est manifestement impossible. La confluence a donc comme conséquence immédiate la cohérence du λ-calcul vu comme une théorie équationnelle. Du point de vue des preuves, cela revient à dire que deux preuves normales distinctes de la même formule ne sont pas

identiques selon le critère donné. Prawitz donne ici deux exemples :

$$\dfrac{\dfrac{\dfrac{A}{A \to A}}{B \to (A \to A)}}{(A \to A) \to (B \to (A \to A))} \quad \text{et} \quad \dfrac{\dfrac{A \to A}{B \to (A \to A)}}{(A \to A) \to (B \to (A \to A))}$$

Ces deux dérivations représentent pour Prawitz deux idées distinctes de preuve, on peut voir que les deux λ-termes correspondant aux deux preuves sont bien irréductibles et distincts : respectivement $\lambda z \lambda y \lambda x x$ et $\lambda y \lambda x y$. On remarque par exemple que le premier terme contient une preuve de l'identité, et pas le second.

Prawitz termine son analyse de la conjecture en affirmant qu'elle demande des raffinements, dans le sens où des dérivations diffèrent encore selon des paramètres "propres" et devraient aussi être identifiées.

La première réaction notable à ces réflexions que l'on peut citer est sans doute la publication de Kreisel dans le même volume : [Kre71]. Il présente plusieurs exigences à l'analyse sérieuse de la notion d'identité, à ce qu'il appellera plus tard ([Kre72]) la *rigueur informelle*. La première exigence est formelle, elle demande la terminaison et la confluence de la réduction. La seconde est informelle, elle demande d'une part la reconnaissance, par inspection, que la réduction préserve l'identité, et d'autre part la reconnaissance que deux dérivations normales distinctes représentent deux preuves différentes.

Kreisel réaffirme le propos de Prawitz en assertant que la réduction de la déduction naturelle satisfait bien l'exigence informelle ci-dessus, dans la mesure où elle correspond à la contraction d'une règle d'introduction suivie d'une règle d'élimination. « une telle contraction ne change clairmeent pas la preuve décrite. ». Pour ces raisons, il s'accorde avec l'idée qu'un théorème de

normalisation est l'outil adéquat à l'étude de ces exigences informelles. On peut à nouveau lire qu'il est évident que la normalisation de Prawitz préserve l'identité.

Pour traiter à proprement parler **l'équivalence** entre la réductibilité à une forme normale commune et l'identité, Kreisel va proposer de définir une relation formelle entre dérivations, que nous décrivons rapidement (car nous traitons plus bas des analyses plus complètes de cet aspect de complétude) : la relation $M(d_1, d_2)$ est définie pour deux dérivations d_1 et d_2 d'une formule de la forme $B \to \exists x A$, et en fonction d'une certaine substitution σ des termes aux variables, définie usuellement et uniformément sur les formules et les dérivations.

La relation $M(d_1, d_2)$ vaudra si pour toute dérivation d^σ de B^σ on peut donner deux termes t_1 et t_2 définis comme suit : pour $i \in 1, 2$ la jonction des dérivations d_i^σ et d^σ donne une dérivation de l'existentielle $\exists x A^\sigma$ que l'on peut instancier en $A(t_i)$, et enfin si les deux termes t_i définissent extensionnellement les mêmes fonctions.

On trouve deux analyses similaires, plus poussées, de la façon dont on peut traiter la conjecture $\pi \sim_{Id} \pi' \Leftrightarrow \pi =_{\beta\eta} \pi'$ dans [Wid01] et dans [Dos03]. Attachons-nous à comprendre cette réception contemporaine de la conjecture de Prawitz.

2.2.1 Un théorème de correction-complétude

On peut observer ensuite que les deux sens de l'équivalence ne sont pas de même nature. Le sens "$\Rightarrow$" est à assimiler à la *complétude* alors que le sens "$\Leftarrow$" à la *correction*. Remarquons qu'il n'est pas anodin de ramener le

problème de l'identité à celui d'un théorème de correction complétude ; mais l'approche qui nous occupe ici semble bien pouvoir être saisie en ces termes.

Le sens correspondant à la correction, celui que Prawitz jugeait non problématique, est justement celui qui échappe à la rigueur mathématique. Ce dont il est question est le fait que la $\beta\eta$-égalité soit adéquate à capturer la notion informelle d'identité (ici "$\sim_{Id}$"). Le sens correspondant à la complétude consiste à dire que la $\beta\eta$-égalité capture *toute* la notion.

La correction ne peut donc naturellement pas faire l'objet d'une démonstration, et c'est en ce sens qu'elle se distingue ici de la complétude : soit l'on admet que deux preuves $\beta\eta$-égales doivent être comprises comme *synonymes*, soit on le rejette. Il y a plusieurs raisons de rejeter cette idée, mais nous y reviendrons plus loin, tachant d'abord de comprendre en quoi il peut être pertinent de l'admettre.

Došen et Widebäck semblent admettre la correction, pour pouvoir obtenir des résultats mathématiques relatifs à la complétude. Ce qui est montré, c'est que si deux démonstrations $\beta\eta$-égales sont toujours comprises comme synonymes, alors toutes les preuves synonymes seront bien $\beta\eta$-égales.

Il est montré que la relation de $\beta\eta$-égalité est *Post-complète* pour les preuves, c'est-à-dire que c'est la relation la plus générale possible : si deux démonstrations que l'on considère comme identiques ne sont pas $\beta\eta$-égales, alors il faut bien déterminer une relation d'identité *plus large* que cette dernière, et c'est impossible. La seule relation par laquelle deux termes non $\beta\eta$-égaux peuvent être reliés, est la relation triviale : elle relie strictement toutes les preuves entre elles.

Éclaircissons un peu ce point, sans rentrer dans le détail des arguments

techniques de Došen ou de Widebäck, car ce résultat permet de comprendre pourquoi la conjecture de normalisation présente un intérêt malgré son aspect contre-intuitif : elle permet justement d'avoir une justification mathématique formelle d'une thèse informelle.

Prenons deux preuves π et π' du même séquent de déduction naturelle : $\Gamma \vdash \phi$. On a alors plusieurs façon d'envisager la comparaison entre les deux preuves : soit l'on constate que $\pi =_{\beta\eta} \pi'$, mais l'on n'est pas d'accord avec la correction de la conjecture de Prawitz, et l'on va dans ce cas chercher une relation plus fine que $\beta\eta$ pour pouvoir les distinguer, car deux preuves $\beta\eta$-égales peuvent être vues comme ne présentant pas la même *idée* de preuve. Soit l'on admet la correction de la conjecture, et dans ce cas, la Post-complétude nous pousse à accepter que toutes les preuves synonymes sont $\beta\eta$-égales ; car sinon on ne peut espérer de relation non triviale pour exprimer comme on le souhaite l'identité.

Il faut noter que ces résultats sont montrés pour des fragments relativement limités de la logique propositionnelle. Les résultats de maximalité (Post-complétude) sont démontrés par Došen pour le fragment conjonctif et disjonctif de la logique propositionnelle intuitionniste, sans distributivité entre la conjonction et la disjonction, et sans les constantes $\bot$ ni $\top$. Widebäck, qui écrit avant ce dernier, traite la logique implicative, son système étant le calcul $\Lambda^{\rightarrow}$ présenté en 1.2.2, mais avec un typage à la Church. L'extension a des fragments plus larges reste un problème ouvert.

2.2.2 Sémantique et généralisation

Le développement de la théorie des catégories a pu donner une nouvelle impulsion à la conjecture de normalisation, notamment depuis les travaux de Lambek donnant une sémantique dénotationnelle au λ-calcul simplement typé *via* les catégories cartésiennes closes (voir [Lam85]).

Une catégorie se définit par des objets, et des morphismes entre ces objets. La sémantique dénotationnelle interprète les preuves (λ-termes) comme des morphismes entre les objets, qui sont les formules. Une catégorie doit comporter un morphisme identité, que l'on trouve en λxx ; et respecter l'associativité de la composition desdits morphismes. Les catégories cartésiennes closes doivent également comporter un produit cartésien et un objet terminal, définis en fonction des morphismes de la catégorie en question.

Ce qui nous intéresse dans l'interprétation des preuves de la logique intuitionniste dans les catégories cartésiennes closes, est précisément que cette interprétation est **invariante par réduction**. Deux preuves β-égales auront exactement la même interprétation.

L'identification des preuves par cette sémantique efficace va alors dans le sens de la conjecture de généralisation, mais pour des raisons différentes que celles que l'on a évoquées : la sémantique dénotationnelle la plus populaire et porteuse de résultats donne une telle identification.

Des interprétations dénotationnelles rendant compte de la dynamique des preuves [6], des réductions, ont été formulées et des travaux vont dans ce sens ;

6. On pense en particulier aux 2-catégories, qui posent deux sortes de morphismes, les morphismes classiques entre objets, et des 2-morphismes, entre objets ou entre morphismes. Dans ce dernier cas, on voit comment apparaît la possibilité de rendre compte des réductions dans ce type de structure.

mais ils sont encore trop complexes et posent trop de difficultés pour que l'on puisse ici les considérer comme aptes à représenter les preuves de façon non problématique.

Došen présente, à nouveau [Dos03] une autre conjecture, dite *de généralisation*, sur laquelle on peut s'arrêter un moment. Cette conjecture se pose comme la définition d'une autre relation entre preuves prétendue apte à rendre compte de l'identité. Nous ne nous étendrons pas outre mesure sur ce point, car il présente des propriétés et des difficultés analogues à la conjecture de normalisation.

Il s'agit là de considérer que deux preuves sont synonymes si elles « généralisent dans la même direction ». C'est-à-dire si, en modifiant les variables propositionnelles, on parvient toujours à la même conclusion à partir des mêmes prémisses. L'exemple canonique choisi est celui des première et seconde projections π_1 et π_2. On distinguera en particulier les preuves $\pi_1 : \vdash A \wedge A \to A$ et $\pi_2 : \vdash A \wedge A \to A$ correspondant respectivement à l'élimination gauche et droite de la conjonction. Cette distinction sera alors justifiée par le fait que si l'on remplace une occurrence de A par B, on obtient $\pi_1 : \vdash A \wedge B \to A$ et $\pi_2 : \vdash A \wedge B \to B$.

La conjecture demande alors que deux preuves soient dites identiques si et seulement si toute procédure de ce type conserve la même conclusion pour les mêmes prémisses. La formulation que donne Došen permet d'écrire des graphes représentant les distinctions des preuves par généralisation : on dessine une arrête à gauche ou à droite, selon quelle projection on choisit pour notre preuve. En ayant montré que ces graphes forment une catégorie, la conjecture peut s'écrire en demandant qu'il existe un foncteur honnête entre

cette catégorie, et la catégorie des preuves dont on doit supposer qu'elle existe. Le problème est alors réduit à celui de l'existence d'une telle catégorie.

Sur des fragments réduits de la logique, cette conjecture coïncide avec celle de normalisation : cela tient en particulier au fait que les interprétations catégoriques sont stables par élimination des coupures. Il est important d'évoquer que la conjecture de normalisation n'est pas justifiée uniquement à travers la notion de coupure, mais aussi par des approches de la théorie de la démonstration plus générales et moins algorithmiques : on cherche des structures pour interpréter les dérivations dans certains systèmes, et les moyens d'y parvenir conduisent à la même identification (sur certains fragments). Les problèmes que posent la conjecture de généralisation et l'approche catégorique seront alors compris dans les difficultés soulevées par la normalisation.

2.2.3 Une « *thèse de Church* ? »

Došen rapproche également la conjecture de normalisation de la thèse de Church : on affirme qu'un notion informelle comme celle d'algorithme est capturée par une caractérisation formelle comme les fonctions récursives.

Ce point est contestable. Car, si l'identité intuitive entre les preuves est bien rapprochée d'une relation binaire formelle telle que $\beta\eta$, on cherche dans notre cas à trouver une manière de distinguer *intensionnellement* les démonstrations. Et la difficulté du problème vient justement du fait que l'on n'a pas à disposition un système formel qui semble absolument apte à représenter ce qu'*est* intrinsèquement une démonstration.

Si l'équivalence entre, par exemple, le λ-calcul et les machines de Turing ne fait que renforcer le contenu de la thèse de Church, c'est parce que les modèles

de calcul ne sont envisagés que par leur capacité à donner ou non un résultat selon un calcul attendu et une certaine donnée en entrée, comme l'argument d'une fonction récursive. Les théorèmes, à ce niveau, montrent l'équivalence *extensionnelle* de ces systèmes, ils calculent les mêmes choses, donc on peut prendre l'un ou l'autre, la thèse de Church se formulera de la même façon, et sa validité supposée n'est pas relative au choix que l'on fait.

La notion informelle d'algorithme est peut-être aussi délicate à saisir que celle de l'idée d'une preuve. Pour autant, les machines de Turing semblent avoir extensionnellement capturé la notion, même si cela ne donne pas une définition. On ne peut avoir le même regard sur la question de l'identité des preuves : les systèmes à la Hilbert permettent de montrer les mêmes théorèmes que la déduction naturelle, mais Gentzen ne s'en satisfaisait déjà pas : on ne s'intéresse pas à savoir si tel ou tel système formel est apte à représenter fidèlement une démonstration [7], mais à savoir quand deux démonstrations d'un système formel représentent la même idée de preuve.

La conjecture de Prawitz se distingue d'une thèse de Church en ce que la notion informelle en jeu demande un pendant intensionnel. Pour réfuter la thèse de Church, il faudrait trouver un calcul, ou l'idée d'un calcul réalisable, qu'une machine de Turing ne pourrait effectuer. Le fait que cela semble improbable renforce l'idée que la notion d'algorithme est extensionnellement capturée. La question de savoir si le λ-calcul par exemple, représente bien ce qu'est un algorithme, semble bien hors de propos pour la thèse de Church. Si

7. Auquel cas les systèmes à la Hilbert seraient exclus, et la déduction naturelle privilégiée, comme dans [Gen35], et l'on aurait avec ces considérations un début de réponse, le texte de Gentzen donnant des arguments pour juger qu'un système est plus ou moins proche du raisonnement effectif.

l'on sortait du cadre extensionnel, les différences entre les modèles de calcul deviendraient trop cruciales pour qu'on les néglige : on peut penser à la complexité algorithmique qui, au delà de l'attente du bon résultat, distingue entre les comportements des différentes machines (de Turing, à registres, RAM, automates, ...) qui pourtant calculent les mêmes fonctions.

Pour l'identité des preuves, on ne peut se contenter de l'aspect extensionnel, car l'équivalence entre les systèmes de preuves est loin de nous apporter une réponse. Et la conjecture de Prawitz pose justement que l'identité informelle est bien capturée (intensionnellement, entendons) par le formalisme de la $\beta\eta$-égalité.

Nous reviendrons plus loin, en 4.1 avec l'analyse de Troelstra, sur cette distinction entre une identité extensionnelle et une identité intensionnelle.

Et s'il semble, pour les raisons évoquées, difficile de réfuter la thèse de Church avec un argument solide, la conjecture de Prawitz paraît plus fragile en ce qu'elle peut être remise en question, si l'on n'est simplement pas d'accord avec le fait que l'identité *à laquelle on pense* correspond à $\beta\eta$.

2.3 Les limites de la normalisation

On a vu que la conjecture offrait un résultat de complétude intéressant *via* la maximalité de la relation envisagée. Mais il est essentiel de se souvenir que ces résultats sont conditionnés à l'admission de l'aspect *correction* de la conjecture, celui que Prawitz jugeait non problématique. Or, c'est justement parce que cette implication ($\pi =_{\beta\eta} \pi' \Rightarrow \pi \sim_{Id} \pi'$) est indémontrable qu'il est légitime de la contester sans réfutation formelle.

Sans donner une réponse positive à la question de l'identité, plusieurs raisons nous poussent à considérer la $\beta\eta$-égalité comme « trop large ». Et les résultats de maximalité ne sont finalement pas pour aller contre cette idée.

Avant de formuler des critiques pour le moins anachroniques, en ce qui concerne la conjecture de Prawitz, on peut revenir au texte de Kreisel déjà évoqué, l'article publié dans le même volume que celui de Prawitz où est appuyée la conjecture : Kreisel émet ([Kre71], P.117) déjà des réserves intéressantes. On peut lire « Le critère évacue, plutôt que de les résoudre, les questions à propos de l'identité des preuves ou, en effet, de la nature des preuves. »puis « le critère ci-dessus a un intérêt pédagogique : il confirme l'hypothèse selon laquelle *rien* de précis (et raisonnable) ne peut être fait sur les questions de synonymie entre les preuves. »

Cette première observation est relativement limpide, on ne cherche pas à établir un critère d'identité qui paie la fécondité mathématique au prix d'une perte notable de clarté. La théorie, sans être elle-même impénétrable semble pouvoir nous éloigner de la connaissance des objets dont on veut traiter. On cherche à savoir comment identifier les preuves pour comprendre son idée, sa structure inhérente, ou quelque chose comme ça. Nous voyons plus bas que la conjecture de normalisation nous met face à des objets, qui sont donc des classes d'équivalence, difficiles à apprécier *en tant que* preuves, tant ces classes sont larges. C'est en ce sens que l'on peut comprendre les termes de Kreisel, la question est évacuée car on traite le problème sans mieux connaître ce qu'est une preuve. Nous avons deux raisons de penser que la conjecture nous éloigne de la connaissance des preuves.

Premièrement, nous allons montrer que le critère paraît trop large pour

être raisonnable : ainsi il capture bien l'identité, mais il capture plus que cela et pour cette raison, on pourrait croire que la question de l'identité est traitée sans s'être demandé *pourquoi* il identifie les preuves. L'idée que le critère conserve *clairement* l'identité d'une preuve n'est pas suffisant.

Deuxièmement, on peut voir une confusion entre les notions d'équivalence, d'identité, et de parenté. Le fait qu'une dérivation *paraisse* conserver son identité quand on la réduit est à prendre avec plus de délicatesse : les deux dérivations se ressemblent, mais l'on n'a aucune raison de penser qu'elles représentent absolument et strictement la même preuve. On pourrait dire que la parenté entre une dérivation et sa réduction, ou son extension, relève de la ressemblance, et non de la synonymie. Ce point est crucial pour comprendre la suite, car si la synonymie en tant que relation d'équivalence peut être un bon candidat pour appréhender l'identité, ce n'est pas le cas de la ressemblance qui n'est pas une relation transitive.

Constater localement que la contraction d'une coupure en déduction naturelle semble anodine et conserver la figure et l'idée de la preuve, cela ne doit pas nous permettre de croire que l'on a bien une relation d'équivalence, et qu'une suite arbitrairement grande d'extensions ne va pas, à terme, effacer la ressemblance. On serait alors bien en peine de ramener cette ressemblance des dérivations à une identité des preuves.

Nous avons deux façons d'envisager cette perte de ressemblance : d'abord la question de la taille, relative en un sens à la ressemblance physique entre démonstrations qui s'atténuerait en voyant une différence de grandeur trop importante entre les deux, au fil des réductions ou extensions. Ensuite, une perte plus immédiate et essentielle que l'on pourrait voir dans la perte ou le

gain d'analyticité d'une démonstration. Nous verrons en quoi le fait qu'une preuve sans coupure soit analytique peut la distinguer fondamentalement de cette preuve étendue avec des coupures, nous invoquerons les notions algorithmiques sous-jacentes à cette distinction.

2.3.1 Complexité et ordres de grandeur

On a dit un mot de l'aspect intuitif et proche du raisonnement de la déduction naturelle, qui semblait être la première motivation de Gentzen. Nous allons maintenant évoquer une toute autre propriété de ce système de preuve, qui éclairera peut-être les réticences que l'on peut avoir à considérer les coupures comme négligeables du point de vue de l'identité entre preuves.

Dans [Boo84], Boolos étudie une démonstration dans deux systèmes de preuve différents, la déduction naturelle d'une part (s'appuyant sur la logique élémentaire de Mate), et d'autre part la méthode des arbres (il donne pour exemples les systèmes de la logique formelle de Jeffrey, ou de la logique du premier ordre de Smullyan).

Les preuves de la méthode des arbres peuvent être aisément transcrites en déduction naturelle, mais Boolos examine la traduction opposée étudie une preuve particulière d'une formule simple en déduction naturelle pour voir comment la reproduire avec la méthode des arbres.

Boolos traite, pour tout entier n, l'inférence H_n qui part de quatre hypothèses :

1. Pour tous entiers x, y, z, $x + (y + z) = (x + y) + z$
2. La fonction $d(x) = x + x$ pour tout entier x.

3. Pour tout entier x, $L(x) \rightarrow L(x+1)$

4. $L(1)$

pour en conclure $L(d^{2^n}(1))$.

Il s'agit donc simplement, à partir de la commutativité de l'addition, d'une fonction double, et d'une propriété supposée vraie pour tous les entiers, mais par récurrence à partir de 1, de montrer qu'elle est vraie pour un entier assez grand. La conclusion semble plus que triviale, dans la mesure où l'idée même de récurrence entraîne que des points 4 et 5, on puisse affirmer $\forall x L(x)$, et éliminer le quantificateur de façon à appliquer la propriété à n'importe quel entier.

On ne dispose pas d'un schéma-axiome de récurrence permettant de faire une preuve aussi directe, mais Boolos montre que la plus courte preuve de H_n en déduction naturelle contient strictement moins de symboles que $16(2^n + 8n + 21)$, alors que la plus petite dérivation par la méthode des arbres contient strictement plus de 2^{2^n} symboles.

Il en conclut que pour la preuve de H_7, qui prend un peu plus d'une page à écrire en déduction naturelle [8], demanderait avec la méthode des arbres plus de 2^{128} symboles, ce qui excède « le nombre de nanosecondes écoulées depuis le Big Bang ».

On a tendance à rapprocher cette conclusion de la relation entre une preuve avec coupures et une preuve analytique. C'est que Boolos affirme que ce gouffre séparant les deux preuves écrites dans les deux systèmes tient au fait que la déduction naturelle « permet le développement et l'utilisation de conclusions

8. Pour moins de 3280 symboles (3175), supposés répartis en moyenne à hauteur de 5 symboles par mot, de 400 mots par page

subisidaires (...) de lemmes. ». Or, on remarque sans trop de difficulté que la méthode des arbres ne fournit que des preuves analytiques, consistant essentiellement en la décomposition des formules selon certaines règles. Finalement, c'est l'absence de coupures qui donne sa taille déraisonnable à cette preuve.

Boolos souligne la « différence significative dans la façon dont [les méthodes de logique] peuvent démontrer la validité, une différence qui résulte parfois d'une disparité frappante dans l'efficacité ou la vitesse avec laquelle une inférence peut être montrée valide. » Montrer, par exemple, en déduction naturelle que la dérivabilité de $A \to B$ et de A entraîne celle de B est immédiat, le faire en méthode des arbres demande beaucoup de travail.

Cette étude est plus frappante, et elle a l'avantage de considérer des preuves dont la taille dépend (dans les deux cas) de la longueur de la formule à démontrer. Mais même en restant à l'intérieur du même système de preuve, on peut trouver des preuves avec coupures dont les pendants analytiques prennent une taille démesurée. Par ailleurs, l'inverse est envisageable : il suffit de prolonger la branche axiome d'une preuve (en déduction naturelle ou en calcul des séquents) par un nombre arbitrairement grand de combinaisons axiome/coupure.

L'identité des preuves vue à travers la $\beta\eta$-égalité pose donc déjà ce premier problème : sont identifiées des dérivations dont les ordres de grandeurs varient sans aucune borne. L'approche de Cook et Reckhow ([CR74]) visant à caractériser les systèmes de preuves avec une borne polynomiale (pour un polynôme sur la taille de la preuve, là où [Boo84] traitait de polynômes en la taille de la formule à prouver [9].) sur la longueur d'exécution de leur vérification

9. La distinction n'est pas anodine, car [CR74] caractérise des systèmes de preuve :

permet déjà de voir comment espérer saisir un ensemble de preuves suffisamment large, sans risquer l'explosion de la taille des dérivations. Pour autant,si cela donne un critère pour raffiner la définition d'un système de preuve, cela ne permet pas vraiment de traiter l'identité des preuves, surtout si l'on veut définir une relation d'équivalence entre les dérivations de systèmes formels de déduction différents.

La difficulté soulevée ici n'est pas une objection nette à la conjecture de normalisation (on a vu en 2.3.2 qu'il semble théoriquement impossible d'en proposer) et se fonde sur un présupposé qui n'a rien de certain mais fait plutôt appel à l'intuition. Dire qu'une dérivation courte et une dérivation exponentiellement plus grande que la première ne semblent pas pouvoir décrire le même raisonnement déductif, c'est déjà supposer un lien entre la dérivation et la preuve ; et un lien qui demande une concordance de taille entre les dérivations d'une même preuve. Ce point pourrait bien sûr être contestable, car il n'est appuyé par aucun argument sérieux, mais dans la mesure où l'on n'a pas de notion précise et définie de "preuve" ou de "raisonnement déductif" ici, faire appel à l'intuition en manipulant des ordres de grandeur n'est pas hors de propos : considérer que l'argument de la taille n'est pas concluant, c'est aussi déjà supposer que l'élimination ou l'introduction de coupures est strictement redondante, nous mettons en doute cette affirmation dans les lignes qui suivent.

---

les tables de vérité, ou le calcul des séquents fournissent des preuves vérifiables en temps polynomial sur la taille de la preuve ; or on a vu qu'une preuve, même du calcul des séquents, peut être arbitrairement grande et donc dépasser exponentiellement la taille de la formule, auquel cas la vérification prendrait un temps au moins exponentiel sur la taille de la formule (même si polynomial ou linéaire sur la taille de la preuve).

2.3.2 Valeurs et calcul

On peut soulever une distinction entre des preuves $\beta\eta$-égales que l'on ne voudrait pas voir absorbées par un critère d'identité, qui est une distinction peut-être plus intrinsèque à la structure des preuves que l'on manipule.

Á travers la correspondance de Curry-Howard, et même pour son expression la plus basique, que nous avons présentée en 1.2.2, on peut voir une preuve avec coupure(s) comme un terme à calculer, et une preuve sans coupure comme le résultat d'un calcul, c'est-à-dire une *valeur*. La distinction peut ici sembler cruciale si l'on regarde l'aspect justement calculatoire des preuves.

Donnons quelques outils techniques pour mieux comprendre ce point à travers la représentation de l'arithmétique dans le λ-calcul.

Définition 2.3.2 (Addition sur les entiers de Church dans $\Lambda^{\rightarrow}$)

- On définit pour tout $n \in \mathbb{N}$ l'**entier de Church** $\underline{n}$ comme le λ-terme suivant : $\lambda z \lambda s\ s^n z$. Ce sont les entiers écrits en unaire : on peut voir la variable z comme l'entier 0, et la variable s comme le successeur.
- On définit le λ-terme **addition** A comme ceci : $A := \lambda n \lambda m \lambda s \lambda z (ns)(ms)z$.
- On définit **le type** N **des entiers naturels** comme la formule suivante : $(\phi \to \phi) \to (\phi \to \phi)$.

Le lecteur pourra vérifier que pour tout entier $n \in \mathbb{N}$, le terme défini $\underline{n}$ est bien typable par N, et que pour tous $n, m \in \mathbb{N}$, on a bien $A\ \underline{n}\ \underline{m} =_\beta \underline{n+m}$.

Les définitions ci-dessus suffisent à illustrer notre propos, mais rappelons que toutes les fonctions récursives de l'arithmétique autres que l'addition sont également représentables dans Λ et présentent les mêmes propriétés.

On ne le montrera pas ici, mais il faut retenir que tous les termes de type N se réduisent à un entier de Church. Notons qu'en parlant des réductions du λ-calcul sur les entiers, nous parlons des termes correspondant aux preuves de la formule N. Les preuves ayant la même forme normale sont donc β-égales à la même preuve correspondant à un certain entier de Church ; deux preuves n'ayant pas la même forme normale correspondant à deux entiers différents. Voir pour plus de détails [Bar84].

La différence entre un terme β-long (contenant des *redex*, analogues des coupures) et un terme évalué ne semble pas être négligeable. On peut reconnaître dans la conjecture de normalisation la volonté d'identifier (ici) les termes de type N correspondant au même entier. En effet, $1 + 1 + \cdots + 1$ (12 fois), $6 + 6$, 12, $4 + 4 + 4$, etc... écrits avec les termes définis plus haut sont tous identifiés par la $\beta\eta$-égalité (β suffit). Et en ce sens, l'idée de « synonymie »dont parle Prawitz prend un sens en s'accordant avec les égalités arithmétiques. Pour autant, cette identité, si l'on remarque à nouveau qu'elle peut être pertinente pour les mathématiciens en vertu des résultats qu'elle permet d'exhiber, est ici aussi extensionnelle. Et pour cela, elle est à nouveau insatisfaisante pour le philosophe, même du point de vue calculatoire des preuves.

En effet, on ne peut s'accommoder d'une caractérisation nous conduisant à dire qu'exprimer « $3+5$ » est la même chose qu'exprimer « 8 ». On pourrait dire que le premier terme *appelle* un calcul, ce qui n'est pas le cas du second. La distinction que l'on cherche à établir entre la structure des différentes preuves ne saurait nous conduire à admettre que, par exemple, les jugements « $3 + 5 = 8$ » et « $8 = 8$ » sont le même jugement, bien que la validité

des deux et la dénotation des termes impliqués soit la même : le *mode de désignation*, si l'on veut être frégéen, est à prendre en compte si l'on compare des expressions entre elles. La notion de calcul ou de décomposition est bien à l'œuvre dans le comportement d'une preuve vue à travers la correspondance de Curry-Howard.

On peut également évoquer le choix des stratégies de réduction du λ calcul qui nécessite la différence entre un terme à calculer et une valeur. La stratégie de l'appel par valeur [10] qui est parfois plus efficace en terme de temps ou d'espace de la réduction nécessite cette distinction au sein même du calcul.

Pour revenir aux preuves à proprement parler, il semble que la distinction entre terme β-long et valeur éclaire la différence entre preuve normale et preuve avec coupure. L'analyticité d'une preuve normale lui donne un caractère différent d'une autre, et la conjecture de Prawitz semble à nouveau donner un critère d'identification trop extensionnel pour être philosophiquement convainquant, malgré les arguments mathématiques qui permettent pour autant de comprendre ses intérêts et enjeux.

La méthode peut être un autre angle d'approche de cette distinction. Si l'on quitte les termes de $\Lambda^{\rightarrow}$ pour se concentrer à nouveau sur les dérivations, on peut considérer l'utilisation des coupures comme une méthode de preuve, qui correspond à la démonstration et l'utilisation d'un lemme. Pratiquement, on n'utilise pas la même méthode de démonstration si l'on se passe de l'utilisation des *conclusions subsidiaires*, pour reprendre le terme de Boolos.

10. Cette stratégie consiste à n'autoriser la réduction $(\lambda x M)V \rightarrow M[x := V]$ que si le terme V est une valeur. Si ce n'est pas le cas, on procède aux réductions dans V selon la même restriction jusqu'à obtenir une valeur (si V a une forme normale, ce qui est toujours le cas dans $\Lambda^{\rightarrow}$ mais pas dans Λ).

L'analyticité des dérivations peut être vue comme représentant un cheminement mental direct, sans détours, finalement comme une technique de démonstration hautement spécifique.

3 L'identité et les réseaux

3.1 Les invariants de preuve et l'approche de Hughes

3.1.1 Le vingt-quatrième problème de Hilbert

Dominic Hughes propose dans [Hug06] une approche de l'identité des preuves différente de celles de Widebäck et Došen. La question est posée dans une direction différente, on ne se demande plus comment reconnaître deux preuves identiques (pas directement), mais on se demande ce qui, d'une dérivation à l'autre, peut varier ou non selon si elles représentent la même idée de preuve.

La recherche proposée est celle d'un **invariant** de preuve, et Hughes s'appuie sur la formulation du vingt-quatrième problème de Hilbert tel qu'il est identifié dans [Thi03]. L'historien des mathématiques extrait des manuscrits de Hilbert, entre autres, le passage suivant :

> Le vingt-quatrième problème de ma conférence de Paris était : un critère de simplicité, ou une preuve de la simplicité maximale de certaines preuves. Développer une théorie des méthodes de preuve dans les mathématiques en général. Donné un ensemble de conditions, il ne peut y avoir qu'une seule preuve la plus simple. Plus généralement, s'il y a deux preuves d'un même théorème, on doit continuer jusqu'à avoir dérivé l'une de l'autre, ou jusqu'à ce que les conditions variantes utilisées dans les deux preuves deviennent assez évidentes.

Hughes interprète le vingt-quatrième problème problème de Hilbert comme

la recherche d'invariants et d'une relation d'équivalence adéquate pour donner des distinctions raisonnables et pertinentes entre les démonstrations. Ce qui semble ici essentiel, c'est de pouvoir donner un moyen de *comparer* les preuves en utilisant cette notion d'invariant.

Ce qui, pour Hughes, est suggéré par Hilbert, c'est une analogie entre les preuves et les objets géométriques étudiés du point de vue de la topologie. L'équivalence d'homotopie, en topologie, relie des objets géométriques obéissant à une même structure, et ce terme de structure est à comprendre dans un sens mathématique précis que nous ne développerons pas, mais nous essayons tout de même de comprendre l'idée générale en donnant des exemples, pour mieux saisir le lien avec la relation d'équivalence entre preuves que l'on cherche à tracer.

Sur des objets géométriques en trois dimensions, on peut se représenter l'équivalence d'homotopie comme le *nombre de trous* des objets en question. Par exemple, une sphère sera équivalente à un disque ou un bol ; et un anneau sera équivalent à une tasse (avec anse, *a fortiori*) : dans les deux cas, on peut passer de l'un à l'autre par des « déformations lisses », tant que l'on ne *déchire* pas la figure.

Cette illustration donne une idée assez claire du type de relation que l'on veut établir ; l'interprétation de cette analogie reste à donner. L'invariant, dans le cas des objets géométriques, est le *groupe fondamental* auquel les objets sont associés, et qui correspond intuitivement au nombre de "trous" des figures en trois dimensions. On a une fonction qui à tout objet lui associe son groupe fondamental, et deux objets sont en relation d'équivalence d'homotopie s'ils sont associés au même groupe fondamental.

Pour Hughes, les déformations lisses, les transformations anodines des preuves correspondraient aux permutations locales des règles ; là où les duplications ou suppressions de morceaux entiers de la preuve correspondraient à des déchirures, et pourraient donc donner lieu à des objets distincts. On voit déjà comment on s'éloigne radicalement de la conception envisagée par Prawitz et Kreisel, la normalisation pouvant comprendre des transformations non-lisses, et changer les propriétés de la preuve manipulée.

Notons que L'analogie entre l'équivalence d'homotopie et l'identité des preuves était déjà formulée par kreisel, qui à la fin de [Kre71] la présentait en des termes similaires « Au risque d'expliquer *obscurum per obscurius* ».

On ne dispose pas immédiatement d'un invariant entre les preuves qui seraient équivalentes par permutations locales. Le point commun entre deux dérivations variant à travers ce type de déformations n'est pas clair ; on doit établir une façon de représenter cette classe d'équivalence, dans la mesure où l'existence d'un témoin canonique [11] ne semble pas être ici de circonstance. Les permutations, en effet, ne permettent pas d'ordonner d'une quelconque façon les dérivations transformées. On n'a pas accès à une réduction telle que $\rightarrow_\beta$, car une permutation locale ne rend pas une preuve plus simple ou plus analytique, ou plus "quoi que ce soit".

3.1.2 Les preuves combinatoires

Ce qui correspondra alors au groupe fondamental, dans l'analogie proposée, sera la « preuve combinatoire ». Hughes traite la logique propositionnelle

11. Pour la conjecture de normalisation, le représentant canonique des classes d'équivalence n'était autre que la preuve normale, ce qui était cohérent avec la conjecture.

classique, et se démarque subtilement de l'approche traditionnelle des réseaux de preuve, mais nous retiendrons l'intuition commune aux deux syntaxes avant de traiter les réseaux de façon plus poussée.

L'idée, dans les grandes lignes, des preuves combinatoire est d'écrire la formule à prouver et de marquer les occurrences d'axiomes et de conjonctions sur les atomes concernés. Sur la formule, deux variables propositionnelles p et $\neg p$ introduits dans la preuve par un axiome, seront marqués de la même couleur. Par ailleurs, dès l'introduction d'une conjonction pour une formule $\phi \wedge \psi$, tous les atomes de ϕ seront reliés (par une arrête, dans la présentation de Hughes) à tous les atomes de ψ.

Nous n'allons pas rentrer dans les détails de ces constructions, car ce qui nous intéresse, c'est comment la question de l'identité a mené Hughes à considérer cette approche du problème, et en quoi les réseaux de preuves présentent des propriétés tout à fait intéressantes pour le traiter. Les preuves combinatoires n'identifient pas exactement les mêmes dérivations que les réseaux pour la logique propositionnelle classique tels qu'ils sont définis dans [Gir91], mais nous gardons à l'esprit la volonté de caractériser les preuves par la construction des formules, tout en oubliant tant que possible l'aspect séquentiel des systèmes formels de dérivation ; et nous basculerons donc vers la logique linéaire pour laquelle la notion de réseau a été initialement formulée et pour laquelle elle s'applique sans doute de la façon la plus claire.

3.2 Les réseaux de preuve pour la logique linéaire

Dans [Gir87], Girard présente la logique linéaire et les réseaux de preuve. Cette logique que l'on présente souvent comme un « raffinement de la logique intuitionniste » va essentiellement nous intéresser à travers la syntaxe graphique permettant d'exprimer les démonstrations que constituent les réseaux de preuves. On a donné en 1.2.3 et en 1.2.4 la syntaxe des formules de la logique linéaire (des fragments qui vont nous occuper) et les règles du calcul des séquents associé dans la version unilatère, adaptée à la traduction en réseaux.

Une caractéristique des réseaux de preuves pertinente en ce qui nous concerne est que leur aspect graphique permet de voir, à proprement parler, la structure de la preuve représentée. Les axiomes, constructions, coupures et conclusions, apparaissent simultanément, et la perte de séquentialité permet un aperçu de la structure de la démonstration que l'on pourrait qualifier de planaire. Nous expliquons ici comment se définissent et se comportent ces structures.

Les permutations locales entre règles de calcul des séquents, que l'on souhaiterait pouvoir absorber dans notre critère d'identité ont le bon goût de disparaître dans les réseaux. Ces règles de permutation, qui correspondent finalement à un ordre d'introduction des connecteurs arbitraire et dont l'interversion est anodine quant à la *forme*, à l'*idée* de la preuve, apparaissent comme relatives à la séquentialité des arbres de preuves.

Prenons par exemple deux preuves de MLL illustrant cet aspect. Supposons que l'on ait une preuve $\pi_1 : \vdash \Delta, C, D, A$ et une preuve $\pi_2 : \vdash \Gamma, B$. Selon le choix de l'ordre d'introduction des connecteurs binaires, on peut voir deux

dérivations différentes du même séquent, soient Π :

$$\dfrac{\dfrac{\dfrac{[\pi_1]}{\vdash \Delta, C, D, A} \quad \dfrac{[\pi_2]}{\vdash \Gamma, B}}{\vdash \Delta, \Gamma, C, D, A \otimes B}}{\Delta, \Gamma, C \parr D, A \otimes B}$$

et Π' :

$$\dfrac{\dfrac{\dfrac{\dfrac{[\pi_1]}{\vdash \Delta, C, D, A}}{\vdash \Delta, C \parr D, A} \quad \dfrac{[\pi_2]}{\vdash \Gamma, B}}{\vdash \Delta, \Gamma, C \parr D, A \otimes B}}{\Delta, \Gamma, C \parr D, A \otimes B}$$

C'est ce type de permutations, dont l'on peut par exemple trouver une étude dans [Kle51], qui rendent le calcul des séquents (ou la déduction naturelle) inadéquats pour représenter les démonstrations en toute généralité : on voit cette fois distinguées des dérivations représentant intuitivement la même preuve.

Ce point pourrait être contesté, on pourrait déclarer que construire une formule avant une autre relève d'une divergence dans le raisonnement. Pour autant, cette position mettrait fin au débat dans la mesure où l'on serait à terme conduit à abandonner également la déduction naturelle, dont Gentzen expliquait déjà dans [Gen35] qu'elle absorbait la linéarité du raisonnement par sa structure arborescente (ici, c'étaient plutôt les branchements scindant l'arbre en composantes parallèles qui étaient visées). On devrait alors retourner à une présentation des démonstrations rédigées en langue naturelle, ce qui ne laisse espérer aucune notion de synonymie intéressante pour le logicien qui s'intéresse aux preuves. La question de savoir quand deux raisonnements rédigés de la sorte sont identiques reviendrait à trouver par exemple des équivalences sémantiques strictes entre les termes, ou encore à trouver une traduction dans une autre langue naturelle. Mais il ne semble pas que le refus de

l'identité entre (ici) Π et Π' puisse nous amener à un critère d'identité entre les démonstrations qui soit intéressant. Là où la $\beta\eta$-égalité identifiait trop de preuves, ne pas identifier ces deux dernières pourrait annuler la perspective même d'une identification entre deux dérivations syntaxiquement distinctes.

S'il a été montré que le quotient des dérivations par $=_\beta$ est maximal, on peut voir le quotient par permutations comme minimal. Avec l'α-équivalence, on pourrait dire que c'est la moindre des distinctions à absorber si l'on souhaite s'abstraire un tant soit peu de l'identité lexicographique des dérivations.

La propriété que revêtent les réseaux de preuves et qui leur permet d'identifier Π et Π' est justement l'absence de séquentialité dans leur syntaxe. Les réseaux représentent des dérivations dans un calcul des séquents à conclusions multiples. Les différentes formules-conclusions d'une preuve seront représentées comme des arrêtes pendantes parallèles du réseau, ce qui annulera la nécessité d'ordonner l'introduction des connecteurs.

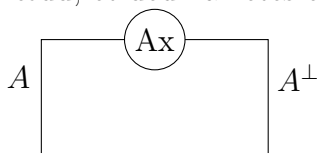
Strassburger, qui a dans [Str06] étudié le lien entre les réseaux et la question de l'identité entre preuves, en donnera la caractérisation suivante : « Un réseau de preuve est une présentation relevant de la théorie des graphes ou de la géométrie qui capture l'essence d'une preuve et qui est libre de toute bureaucratie syntaxique » ([Str06], p.4) Nous essaierons de voir en effet comment les réseaux s'affranchissent de cette *bureaucratie*, comme l'écrirait Girard, et quelles réserves il peut y avoir à admettre complètement l'aptitude des réseaux à représenter absolument l'essence des démonstrations.

3.2.1 La syntaxe des réseaux

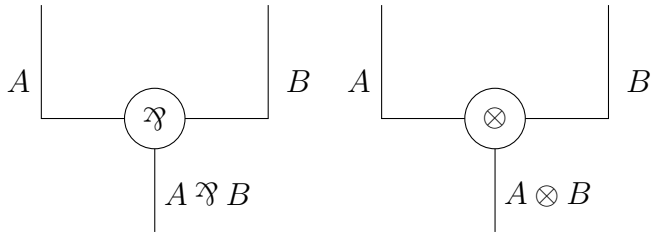
Un réseau de preuve est un graphe dont les arrêtes sont étiquetées par des formules de MLL. Les nœuds correspondent aux constructeurs de formules $\parr$ et $\otimes$. On supposera que les axiomes des démonstrations n'impliqueront que des atomes propositionnels, et l'on considère pour cela que notre ensemble de formules est quotienté par les lois de De Morgan que l'on a données, de façon à ce que la négation, dans nos preuves, ne s'applique qu'aux formules atomiques. Cette convention usuelle est sans danger, et l'on peut s'en passer, mais elle permet notamment d'avoir une notion de réseau un peu plus souple et d'une présentation plus claire. Il s'agit, en logique linéaire, de considérer que l'on a pratiqué l'η-expansion sur les preuves jusqu'à remonter aux atomes.

De haut en bas, un réseau se présente comme suit :

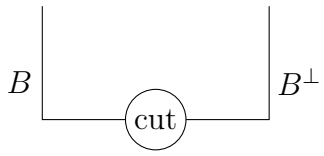
– Des nœuds axiomes dont descendent les arrêtes correspondant aux formules duales, représentés par un graphe de la sorte, comportant un nœud, et deux arrêtes étiquetées :



– Des nœuds pour les constructions binaires $\parr$ et $\otimes$:



et un nœud pour la coupure :



– Les arrêtes pendantes correspondant aux conclusions, pour une preuve se concluant sur un séquent à n formules :

3.2.2 Les critères de correction

On peut désormais voir comment une preuve du calcul des séquents pour MLL peut être écrite dans ce formalisme. Nous donnerons un exemple plus bas. Pour autant, un graphe dessiné selon les constructions ci-dessus ne correspondra pas toujours à une preuve de MLL. Pour les dérivations en séquents, vérifier la correction d'une preuve pouvait se faire en inspectant les constructions utilisées, et en vérifiant qu'elles respectaient les règles d'introduction définies pour ces mêmes constructeurs. Ici, il a fallu introduire des ***critères de correction*** permettant de distinguer entre une *structure* de preuve et un *réseau* de preuve. Une structure de preuve étant un graphe respectant les constructions données, et un réseau de preuve étant une structure de preuve correspondant à une dérivation du calcul des séquents. En voici quelques

exemples (on peut en trouver une présentation précise dans [BDS14]).

Le critère de correction le plus immédiat est celui justement de la traduction depuis le calcul des séquents ; une structure de preuve peut être dite un réseau si l'on exhibe une traduction depuis une dérivation de séquents donnant la structure en question.

Dans l'article fondateur, [Gir87], Girard a donné un premier critère de correction invoquant le parcours d'une particule à travers les fils d'une structure, qui selon certaines règles de circulation dépendant des connecteurs, pouvait effectuer des voyages "courts" ou "longs", selon le type de parcours. Une structure de preuve était alors certifiée comme réseau de preuve si elle n'admettait que des voyages longs.

Des critères basés sur la réécriture de graphes ont aussi été donnés. On donne des règles de transformation de la structure de preuve, également en fonction des connecteurs impliqués, et si la structure, au terme de l'algorithme de réécriture, revêt la forme demandée, elle sera avérée comme étant un réseau de preuve. Le critère de contractilité, par exemple, demande, après avoir remplacé les nœuds par des points et apparié certaines arrêtes, que la structure puisse se réduire en un point unique (voir à nouveau [BDS14].

Peut-être le plus populaire et intuitif, donnons le critère de Danos-Régnier (issu de l'article [DR89]). Ce critère demande de voir les nœuds $\parr$ comme des *interrupteurs*, et de ne conserver pour chaque nœud qu'une seule de ses arrêtes-prémisses. Le graphe issu d'un choix de prémisse pour chaque nœud $\parr$ est appelé graphe de correction (pour une structure donnée, comportant n occurrences de $\parr$, cela fait donc 2^n graphes de correction possibles). Et l'on dit alors qu'une structure de preuve est un réseau si et seulement si tout ses

graphes de correction sont acycliques et connexes.

On évoquera plus loin un critère moins intuitif (et moins graphique) d'acyclicité adapté à une présentation des réseaux plus générale que celle, usuelle, que nous avons donnée.

Les structures avérées correctes sont aussi dites *séquentialisables*, c'est à dire qu'elles peuvent être mises sous la forme séquentielle des arbres de preuve, *i.e* traduites dans le calcul des séquents.

3.2.3 Un exemple de déséquentialisation

Pour illustrer comment les réseaux parviennent bien à représenter la structure d'une preuve en permettant l'oubli d'informations séquentielles liées aux permutations globales, reprenons un exemple. Nous donnons d'abord deux dérivations en calcul des séquents pour MLL, et montrons qu'elles se traduisent dans le même réseau.

Soit π_1 la dérivation suivante :

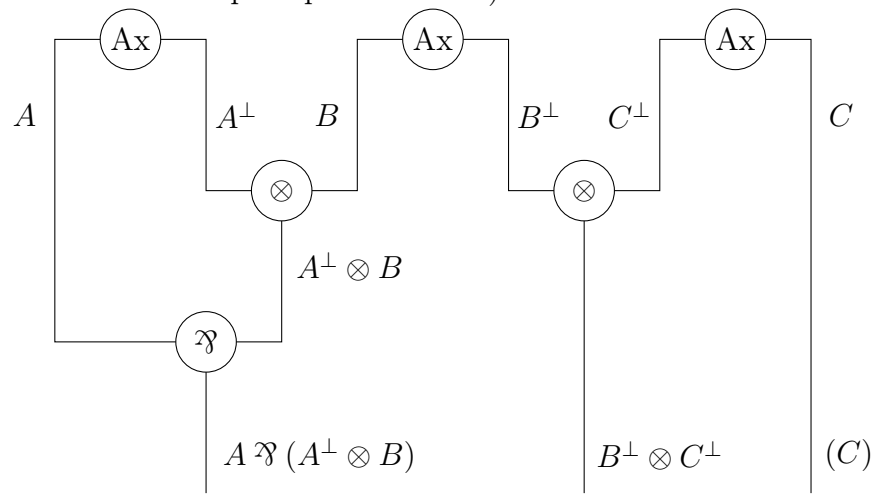
$$\dfrac{\dfrac{\dfrac{\dfrac{}{\vdash A, A^\perp} \quad \dfrac{}{\vdash B, B^\perp}}{\vdash A^\perp \otimes B, A, B^\perp} \quad \dfrac{}{\vdash C, C^\perp}}{\vdash A^\perp \otimes B, A, B^\perp \otimes C^\perp, C}}{\vdash (A^\perp \otimes B) \parr A, B^\perp \otimes C^\perp, C}$$

Et soit π_2 la dérivation suivante :

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

Nous sommes manifestement dans le même cas que pour Π et Π' données plus haut, l'ordre d'application de la règle $\parr$ et de la règle $\otimes$ est la seule chose

variante d'une dérivation à l'autre, et l'on souhaiterait pouvoir identifier de même π_1 et π_2. Le réseau correspondant aux deux preuves est le suivant (on a commuté le $\parr$ pour plus de clarté) :



On peut voir dans cette figure comment la syntaxe des réseaux absorbe les permutations locales en procédant à un oubli de séquentialité : on peut voir que le branchement entre le sous-réseau associé à l'axiome impliquant $C, C^\perp$ et le reste de la structure (par le tenseur de droite) est indépendant du branchement entre les deux arrêtes (du même sous réseau, cette fois) liées par le $\parr$. La hiérarchie chronologique qu'impose la structure cumulative des dérivations de séquents entre les applications de règles logiques est ici obsolète. On est parvenu à conserver une hiérarchie structurelle, arborescente, mais qui est intrinsèquement liée à la nature des formules, et donc en lien fort avec la structure de la preuve.

Le réseau montre explicitement les rapports entre la façon dont une for-

mule se compose [12] structurellement, et comment sa validité est établie : par réduction aux axiomes. Une preuve comportant des hypothèses libres verrait des arrêtes seules pendre du haut du réseau sans être reliées à des liens axiome.

On peut sans difficulté ici vérifier que le réseau est correct, séquentialisable. D'une part parce qu'il est issu de la traduction d'une preuve du calcul des séquents. Mais sans accès à cette preuve ou à cette traduction, on peut revenir au critère de [DR89] invoquant les graphes de correction : il n'y a qu'un seul nœud $\parr$; donc les deux seuls graphes de correction sont les deux réseaux dans lesquels on a retiré l'une ou l'autre des arrêtes-prémisses du $\parr$. Les deux graphes résultant des choix sont manifestement connexes et acycliques, et satisfont donc bien le critère en question.

3.3 Généralisations des réseaux

L'identité des preuves vue à travers les réseaux nous apporte déjà un formalisme intéressant pour s'affranchir des permutations locales tout en conservant raisonnablement les structures des démonstrations (on n'identifie pas une preuve normale à ses formes étendues comportant des coupures).

Pour autant, précisons qu'il nous est encore permis à travers cette approche de faire des choix de présentation qui peuvent faire varier la traduction des preuves au point de changer les distinctions ou identifications effectuées ci-dessus. Nous dressons le portrait rapide de deux présentations alternatives illustrant ce point.

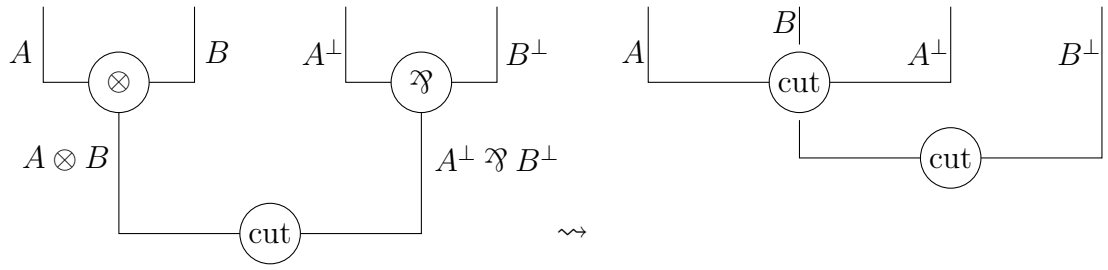
12. En partant des atomes, puisque l'on a demandé le quotient des formules par les lois de De Morgan.

3.3.1 Les réseaux d'interaction et les réductions dans les réseaux

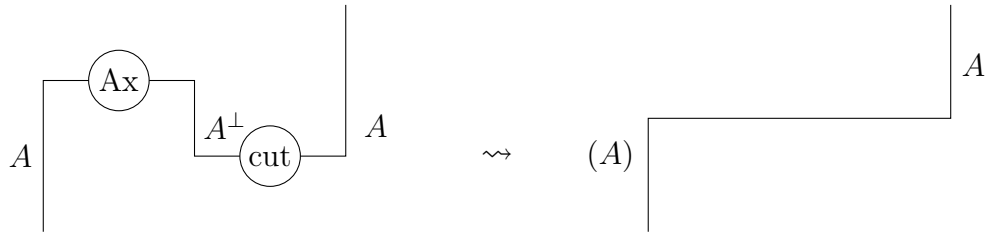
Dans [Laf90], Lafont introduit les réseaux d'interactions, qui sont une forme abstraite des réseaux de preuve (il décrit dans [Laf95] comment ces derniers l'ont conduit à penser cette nouvelle notion de réseaux, et en donne une description très claire). Les réseaux d'interaction retiennent surtout l'aspect dynamique des réseaux de preuve : l'aspect local de l'élimination des coupures.

Un point des réseaux classiques que nous n'avons pas encore abordé est celui des réductions. Il faut dire que si la normalisation dans les réseaux est un processus rendu clair par le côté graphique et local, ce n'est pas un argument excessivement pertinent pour notre propos ; la question de l'identité n'en est ni éclairée ni obscurcie. Pour autant, on peut la présenter succinctement pour comprendre en quoi elle est justement *locale*.

Pour le fragment multiplicatif de la logique linéaire, il n'y a que deux types de coupures à envisager : entre deux formules $A \otimes B$ et $A^{\perp} \parr B^{\perp}$, et entre deux atomes A et $A^{\perp}$. Pour réduire une coupure multiplicative, il s'agit de considérer la configuration qui est à l'œuvre dans le réseau pour modifier le branchement correspondant à la coupure (on supprime les connecteurs binaires, de façon à la faire *remonter*, comme dans les réductions du calcul des séquents), sans toucher au reste de la structure. Le schéma de réduction est le suivant :



Quant à la réduction axiome-coupure, elle se présente comme suit :



On peut dans un premier temps constater que ces réductions préservent bien les formules comme étiquettes à l'entrée et à la sortie du branchement considéré. Le fait que l'on ait pas à intervenir sur les constructions autres que celles indiquées correspond à l'aspect local que nous avons évoqué.

Les réseaux d'interaction sont une généralisation des réseaux de preuve motivée par la dynamique des réductions de cette interface graphique pour les démonstrations de la logique linéaire. L'interaction va généraliser la coupure multiplicative à d'autres types de connecteurs (appelés combinateurs d'interaction), et dont les différentes réductions donneront lieu à un modèle de calcul extensionnellement équivalent aux machines de Turing et au λ-calcul.

D'ailleurs, de la même façon que l'on considère pour le λ-calcul l'aspect

calculatoire des réductions, les réseaux d'interaction (comportant trois combinateurs ϵ, γ, δ, voir [Laf97]) oublient l'aspect logique lié aux formules pour se concentrer sur les réductions en elles-mêmes ; la notion de preuve s'efface un peu.

L'écriture des réseaux de preuves sous la forme de réseaux d'interaction a pourtant un intérêt pour nous, qui concerne le typage de ces réseaux. Un réseau peut être typé par des formules, dans le sens suivant : pour chaque arrête, on lui donne (par exemple) le type A si on la parcourt dans un sens, et le type $A^{\perp}$ si on la parcourt dans l'autre. Cette écriture permet en particulier de ne plus écrire les nœuds correspondant à l'axiome et à la coupure. On n'a donc pas de règle de coupure avec axiome, ce qui est finalement une identification non triviale de certaines preuves.

En effet, faire une réduction axiome/coupure revient à conserver une unique arrête (graphiquement, on tord ou retend le fil, ce qui ne change rien à la structure). Pour autant, si deux dérivations β-égales sur les axiomes sont identifiées, les coupures multiplicatives ne sont pas rendues triviales, et la dynamique de réduction des coupures donne bel et bien lieu à des réseaux d'interaction différents.

3.3.2 Une écriture des réseaux sous forme de termes

On peut évoquer une autre présentation des réseaux qui a l'avantage d'évacuer son aspect graphique, et d'en montrer une écriture linéaire. L'intérêt pour nous est ici de voir que le point de vue de la théorie des graphes n'est pas une fatalité quand on veut prendre une approche des preuves ayant les bonnes propriétés que l'on a vues avec les réseaux.

Ces réseaux, qui s'écrivent sous formes de suites de termes, avec des constructeurs, on été notamment étudiés par Ehrhard dans [Ehr14] pour formuler un nouveau critère de correction (qui avait en fait déjà été formulé de façon équivalente avec des graphes alternés par Rétoré dans [Ret99]).

On décrit les structures de preuves à l'aide de variables et des constructeurs $\otimes$ et $\parr$ correspondant aux connecteurs de MLL. Les variables vont deux par deux (quant elles sont introduites par des axiomes) et correspondent aux atomes propositionnels. On écrira $(x, \overline{x})$ pour représenter les réseau-axiome prouvant $\vdash A, A^{\perp}$. Ce réseau est constitué de deux termes, chaque terme correspondant à une formule. Et inductivement, si l'on a un terme t_1 correspondant à une formule F_1 et un terme t_2 correspondant à une formule F_2, on construit le terme $t_1 \otimes t_2$ (resp. $t_1 \parr t_2$) pour avoir un terme correspondant à $F_1 \otimes F_2$ (resp. $F_1 \parr F_2$).

On peut écrire dans cette syntaxe le réseau donné en 3.2.3. On écrit la structure ainsi : $x \parr (\overline{x} \otimes y), \overline{y} \otimes z, \overline{z}$. Nous voyons alors les formules comme des types donnés aux termes du réseau. Ainsi, on se donne Φ est un contexte, précisant que x est de type A (et $\overline{x}$ de type $A^{\perp}$, par définition), y de type B, et z de type C. De cette façon, la conclusion des preuves π_1 et π_2 données en 3.2.3 est vue comme le type de nos termes, et l'on peut écrire

$$\Phi = x : A, y : B, z : C \vdash x \parr (\overline{x} \otimes y), \overline{y} \otimes z : A \parr (A \otimes B), B^{\perp} \otimes C^{\perp}, C$$

On dispose pour cette structure d'un critère de correction basé sur des espaces cohérents additifs associés aux structures de preuves. On a repris ces idées dans [Cho15] pour montrer comment étendre cette syntaxe et ce critère

à des réseaux pour MELL, et d'autre part comment s'assurer de la connexité des réseaux (le critère d'Ehrhard s'appliquait aux structures non connexes, pour un calcul des séquents disposant d'une règle Mix).

3.4 Difficultés et insuffisances

Ce qui vient d'être dit permet de voir comment les réseaux de preuves apportent d'intéressantes réponses à la question de l'identité, et on en a évoqué différentes présentations pour en montrer la souplesse (on peut choisir d'absorber ou non certaines réductions avec l'interaction, on peut se passer de l'interface graphique pour une formalisation plus précise). On peut émettre une conjecture qui semblera alors plus fine que la conjecture de normalisation : deux preuves sont synonymes si elles se traduisent dans le même réseau (ou un réseau isomorphe [13], selon les choix de traduction, de typage, et de présentation). Le choix de la traduction permettrait justement de poser éventuellement des contraintes ou des souplesses sur la relation d'identité définie.

Naturellement, si cette conjecture était admissible sans aucune réserve, l'étude que nous proposons n'aurait pas lieu d'être et la question de l'identité des preuves ne serait pas un problème logique et philosophique, mais une définition non ambiguë. Les difficultés que pose la réponse apportée par les réseaux sont essentiellement liées au langage à laquelle elle s'applique, et pour deux raisons principales. La première est l'inaptitude des réseaux à représenter convenablement des fragments non négligeables de la logique ; la seconde

13. On peut choisir l'isomorphisme de graphes, sans précision des formules comme types si l'on prend les réseaux d'interaction. On peut aussi définir une équivalence sur les réseaux écrits comme des termes : une équivalence de substitution comme $\equiv_\alpha$ où l'on renomme simultanément x et $\overline{x}$ pour toute variable x, en évitant les captures. On peut alors se passer des contextes et du typage, pour la conjecture.

tient au fait que dans les cas où l'on peut augmenter la puissance du langage, on observe une certaine régression des qualités de nos outils : la séquentialité s'introduit insidieusement dans les structures obtenues, et fait apparaître à nouveau le fantôme des permutations locales et de l'ordre d'introduction arbitraire des connecteurs.

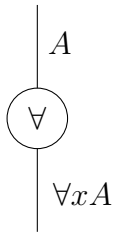
3.4.1 Les extensions inadéquates

Un premier point à soulever dans l'incapacité des réseaux à s'adapter de façon satisfaisante aux langages que l'on utilise en logique, est que l'on n'est pas parvenu, jusqu'à maintenant en tout cas, à donner une notion de réseaux claire et simple pour le fragment additif de la logique linéaire (correspondant à la disjonction intuitionniste $\oplus$ et à la conjonction additive &.) Les propositions lisibles pour traiter ce problème introduisent des réseaux avec des *tranches*, nous ne nous étendrons pas sur cette solution, et retiendrons qu'elle n'est pas d'une simplicité comparable à celle des réseaux pour MLL et que la définition de réseaux pour ALL ou MALL est un sujet de recherche encore ouvert.

L'approche de Hughes — qui, rappelons-le, ne définissait pas exactement des réseaux, mais des *preuves combinatoires*, qui sont fondées sur la même idée — se restreignait à la logique classique propositionnelle. Il précise en effet que c'est une étape nécessaire avant de pouvoir traiter éventuellement des pans plus larges de la logique : « *You can't run before you can walk* » [Hug06].

On peut alors penser à ce à quoi ressembleraient des réseaux (ou des preuves combinatoires) pour un langage du premier ordre. Les réseaux usuels adaptés à cette logique existent bien, mais on peut remettre en question leur aptitude à représenter l'idée ou la structure d'une preuve. Ces réseaux

étendent donc les constructions propositionnelles avec des nœuds unaires pour les quantificateurs $\forall$ et $\exists$. Une arrête de type A passant par un nœud $\forall$ deviendra alors une arrête de type $\forall x A$, par exemple :



Les difficultés que cela présente ne sont pas d'ordre technique, mais on peut se demander en quoi une telle construction rend bien compte du procédé de la quantification, où comment elle permet de rendre compte de la dynamique des substitutions de façon explicite et visible dans les réseaux.

3.4.2 Les extensions problématiques

La deuxième difficulté que présentent les extensions des réseaux à des logiques plus complètes est celle posée par l'ajout d'exponentielles au langage. Passer de MLL à MELL nous fait gagner en pouvoir d'expression, et l'on retrouve une des caractéristiques importantes de la logique linéaire : les règles structurelles contrôlées par les modalités ? et !.

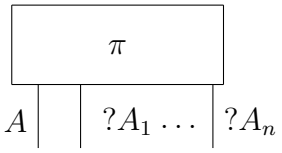
On a donné les règles du calcul des séquents pour le fragment exponentiel de la logique linéaire en 1.2.4. Sans dresser explicitement sa traduction en réseaux, on peut remarquer que la contraction se comporte comme un $\parr$, que la déréliction se comporte comme le $\forall$ désigné plus haut, et l'affaiblissement peut être représenté comme une contraction sans prémisse. Ces constructions

ne sont pas problématiques et les réseaux obtenus ressemblent alors à ceux que l'on avait en 1.2.3. C'est la règle de la promotion qui va poser problème

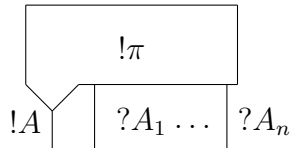
Il faut trouver une façon de la représenter qui rende bien compte de son caractère spécifique. Nous rappelons qu'en calcul des séquents, cette règle prend la forme suivante

$$\frac{\vdash ?A_1, \ldots, ?A_n, A}{\vdash ?A_1, \ldots, ?A_n, !A}\ !$$

En étant contraignante sur les formules du contexte — qui doivent être de la forme $?A$ — cette règle nous pousse à revoir nos réseaux en y introduisant des boîtes. Ainsi, la règle de promotion demande d'enregistrer la structure à partir de laquelle on promeut une formule : graphiquement, l'idée est de l'encadrer, de l'emboîter, et de n'en récupérer que les conclusions. Pour une structure π représentée ainsi :



la promotion donnera la boîte :



On a ainsi accès à une information dont on ne peut se dispenser sans perdre la correction du système : on sait à quel *moment* de la construction du réseau la promotion a été effectuée. C'est comme cela que l'on est sûr de bien correspondre à l'inférence souhaitée.

Le problème est donc niché ici : on ne peut plus regarder nos réseaux à plat, comme déséquentialisations de dérivations. Les structures acquièrent une *profondeur* en ce qu'on emboîte le réseau à chaque application de la règle de promotion. La séquentialité est ici, car cet emboîtement justement peut

revêtir l'aspect arbitraire que l'on avait vu avec l'ordre d'introductions des connecteurs multiplicatifs.

Par exemple, il va de soi qu'une contraction sur deux formules du contexte peut être faite avant ou après une promotion. Les prémisses et conclusions de cette inférence étant respectivement $?A, ?A$ et $?A$, cette règle est indépendante de la promotion que l'on peut faire avant ou après ; de même que l'introduction d'un $\parr$ était indépendante de celle d'un $\otimes$ dans les dérivations traitées en 3.2.

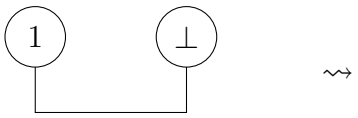
On attendrait des réseaux qu'ils puissent à nouveau aplatir ces permutations, mais rien de convaincant n'a aujourd'hui été proposé dans cette voie ; ce que l'on a gagné en pouvoir d'expression, on l'a perdu en retombant dans la séquentialité. Notre outil d'identification des preuves semble faillir à revêtir les qualités pour lesquelles on l'a choisi quand on veut se placer dans une logique expressive.

Le même problème se pose si l'on veut considérer MLL avec les unités 1 et $\bot$. On se rappelle que les unités vrai et faux posaient déjà problème dans l'article de Došen et le poussaient à restreindre les conjectures considérées. De la même façon, si la règle d'introduction pour 1 ne pose pas de problème : $\dfrac{}{\vdash 1}$, ce n'est pas le cas de la règle pour $\bot$:

$$\frac{\vdash \Gamma}{\vdash \Gamma, \bot}$$

Ici, le problème tient également au fait que l'introduction de la constante soit contraignante sur le contexte : il doit être non vide. Ici, si l'on ne respecte pas cette condition, on perd la correction de nos réseaux, car la réduction impliquant les unités est la suivante [14] :

14. Nous nous contentons d'évoquer les unités pour MLL, pour un exposé complet et



On se retrouve avec un réseau vide à droite. Pour peu que $\perp$ ait été introduit sans autres arrêtes pendantes, cela nous conduirait à admettre la validité du séquent vide. Pour être sûr que nos unités ne risquent pas de donner lieu à des phénomènes d'incorrection, on est à nouveau contraint d'introduire des boîtes pour chaque introduction de $\perp$ et de retomber dans les travers évoqués ci-dessus.

3.5 Conclusions sur les réseaux

Revenons sur l'étude que nous proposons. La question de l'identité des preuves semble trouver une réponse des plus fines et prometteuses dans l'approche par les réseaux de preuve. On arrive à percevoir la façon dont se structure une preuve et à évacuer des détails jugés trop fins pour être retenus dans une généralisation pertinente des dérivations syntaxiques.

Prétendant avoir expliqué en quoi les formalismes représentant des réseaux de preuve sont particulièrement satisfaisants pour traiter la question, l'on veut insister sur ce que signifient les insuffisances soulignées. Il ne s'agît pas d'affirmer que les réseaux sont par nature limités pour exprimer les démonstrations de façon adéquate et pertinente pour nous. On n'est pas dans le cas de la conjecture de normalisation que l'on a rejeté car elle identifiait *de facto* des

clair des réseaux, réductions, et critères de correction pour tous les fragments considérés, se référer à [Laf95].

dérivations que nous pouvons juger trop distinctes l'une de l'autre.

Ici, les réseaux sont satisfaisants, mais incomplets. On peut supposer qu'il n'existera jamais de syntaxe similaire à celle des réseaux dénuée de toute séquentialité et capable d'exprimer bon nombre de logiques expressives.

Pour autant, cela n'est pas prouvé, l'insuffisance est encore d'ordre technique : on ne parvient pas à améliorer cet outil pour le rendre aussi souple que le calcul des séquents (par exemple) et conservant les mêmes propriétés que celles que possèdent les réseaux pour MLL, que l'on perd avec le premier ordre, les unités, ou les exponentielles. Rien en principe ne nous interdit de supposer que l'on parvienne à une telle notion. On peut tout de même supposer, au regard des différentes et conséquentes recherches que ces questions suscitent, que si une syntaxe de réseaux assez souple doit apparaître un jour, la probabilité qu'elle soit simple et intuitive paraît sensiblement mince.

4 Révisions et compréhensions de l'identité

4.1 Égalité extensionnelle et intensionnelle

Nous avons déjà dit un mot dans 2.2.3 de la distinction entre une identité extensionnelle et intensionnelle entre les preuves. L'idée étant que la conjecture de Prawitz identifiait des preuves extensionnellement égales, là où l'on souhaitait pouvoir donner un critère d'identité plus fin, rendant compte d'une similarité intensionnelle entre les dérivations. Nous revenons sur ce point pour mieux comprendre la nécessité de trouver une égalité qui ne soit ni complètement en extension, ni complètement en extension.

Dans [Tro75], Troelstra explicite cette distinction et montre comment elle s'applique à la théorie de la démonstration, en particulier sur la question de l'identification des démonstrations. La différence entre les deux notions peut être résumée ainsi :

- Deux objets, ou outils, seront dits **extensionnellement** égaux (on pourra noter $o_1 =_e o_2$) s'ils ont le même pouvoir. Il peut s'agir du pouvoir expressif ou déductif par exemple. Ici, l'extension peut être comprise comme l'ensemble des choses exprimées, ou calculées par les instances comparées (les exemples clarifieront).
- Deux objets ou outils seront dits **intesionnellement** égaux s'ils nous sont donnés de la même façon (ce sont les termes de Troelstra).

L'exemple donné dans l'article est le suivant : on définit deux additions $+$ et $+'$ par la procédure récursive habituelle, en commutant l'argument sur lequel se fait l'appel récursif.

- $x + 0 = x$
- $x + s(y) = s(x + y)$
- $0 +' x = 0$
- $s(y) +' x = s(y + x)$

Les deux opérations sont extesionnellement équivalentes car elles permettent de calculer rigoureusement les mêmes résultats. En revanche, elles sont intensionnellement distinctes en ce qu'elles ne correspondent pas exactement à la même procédure de calcul, les deux constructions telles qu'elles nous sont données ci-dessus ne le sont pas de la même façon. L'aspect extensionnel retient les résultats, l'aspect intensionnel retient la construction. Cet exemple peut sembler inutilement tatillon, mais Troelstra en donne un autre qui illustre comment notre distinction peut conduire à des différences de résultats.

Prenons l'énumération des ensembles récursivement énumérables (telle que définie dans le premier chapitre de [CL93] par exemple) $(W_i)_{i\in\mathbb{N}}$. On rappelle qu'un ensemble récursivement énumérable correspond au domaine d'une fonction récursive. Il existe pour ces ensembles un théorème de point fixe posant que, pour tous x, y, il existe deux fonctions récursives ϕ et ψ telles que $W_x \cup W_y = W_{\phi(x,y)} \cup W_{\psi(x,y)}$.

Si l'on considère l'identité extensionnelle entre ensembles récursivement énumérables, il est aisé de trouver x et x' distincts tels que $W_x =_e W_{x'}$. Il suffit de prendre pour W_x et $W_{x'}$ deux domaines identiques de deux fonctions récursives distinctes. On construit également W_y et $W_{y'}$.

Hors, le théorème de point fixe pour les ensembles récursivement énumérables s'appuyant sur un théorème de point fixe pour les fonctions récursives, il va de soi que $\phi(x, y) = \phi(x', y')$ est une équation fausse en toute généralité. Le théorème construisant naturellement la fonction ϕ (idem pour ψ à partir

des fonctions récursives d'indices x et y dont W_x et W_y sont les domaines, on ne peut espérer raisonnablement qu'elle donne l'indice du même ensemble avec des arguments ne correspondant pas aux mêmes fonctions récursives.

Si l'on se contentait ici de l'égalité extensionnelle, et que l'on s'autorisait à substituer dans les équations les termes égaux (et ce n'est pas trop demander pour un raisonnements portant sur des équations entre termes), on serait conduit à admettre l'égalité suivante

$$W_x \cup W_y = W_{\phi(x',y')} \cup W_{\psi(x',y')}$$

et il suit des remarques précédentes que cette équation ne peut être vraie en toute généralité. Troelstra précise qu'il n'existe en effet pas de théorème de point fixe similaire pour une théorie prenant les ensembles récursivement énumérables avec les identités extensionnelles induites.

L'identité extensionnelle se laisse appréhender sans difficulté, il s'agît de comparer des ensembles ou des résultats en examinant quantitativement leur contenu. L'identité intensionnelle en revanche est plus délicate à comprendre. L'importance que Troelstra, traitant essentiellement dans le texte des mathématiques constructives, accorde à la *construction* permet de saisir un peu mieux ce que l'on entend par là, et de faire le lien avec l'identité des preuves.

L'auteur prend l'exemple d'un langage arithmétique standard : $\{0, s, +, \times\}$ où s est la fonction successeur. L'idée est que l'on peut voir les termes clos de ce langage de deux façons. On peut considérer d'une part que chaque terme clos est la description d'un entier.

Remarque : Le fait que chaque terme clos de ce langage corres-

ponde à un entier n'est pas trivial. Mais on peut aisément remarquer que tous ces termes sont typables par un type de base N, avec $0 : N, s : N \to N$, $+, \times : (N \to N) \to N$. Et on peut montrer que tout terme se réduit en un numéral de la forme $s^n(0)$ à travers les règles inductives définissant les opérations. Cette propriété est similaire au fait que tout habitant du type des entiers dans le système F se réduise en un entier de Church.

De cette façon, si l'on voit chaque terme comme la description d'un entier dont la description canonique serait le numéral $s^n(0)$, l'identité extensionnelle correspond à l'identité arithmétique. Deux termes seront dits identiques s'ils décrivent le même nombre.

D'autre part, l'identité intensionnelle telle que nous l'avons présentée consiste à identifier les termes qui nous *sont donnés* de la même façon, et dans ce cas précis : qui correspondent à la même construction. L'identité ici est alors syntaxique, dans la mesure où la construction d'un terme correspond à son écriture dans le langage que nous considérons. Pour revenir aux ensembles récursivement énumérables, on pourrait dire que pour $x \neq y$ tels que $W_x =_e W_y$ l'égalité intensionnelle échoue ici en ce que les indices des ensembles ne sont pas les mêmes. Pour autant, la distinction syntaxique qui peut paraître trop rigide ou arbitraire est ici le symptôme d'une différence en intension des ensembles : on ne les a pas construits de la même manière, les fonctions récursives dont on a pris le domaine de définition ne *sont* pas les mêmes objets.

Pour donner de la profondeur à l'identité intensionnelle, il faut donc prendre un point de vue différent sur la signification des constructions considérées. On ne se contentera pas de dire que deux termes clos, dans notre exemple, dé-

crivent (ou pas) le même entier, mais qu'ils décrivent une **procédure de calcul**. On revient à l'idée que les termes $2+3$ et 5 ne décrivent pas la même chose. On voit apparaître la pertinence de cette distinction pour ce qui nous occupe, si l'on relit la distinction entre valeurs et calculs que l'on a présentée en 2.3.2.

L'égalité syntaxique que l'on retient alors comme capturant l'aspect intensionnel des termes entretient un lien fort avec l'idée de construction. De la même façon, on transpose les deux significations des termes aux dérivations (ce qui, *via* Curry-Howard, est plus que justifié) en partant du principe qu'une déduction formelle décrit une démonstration.

On arrive ici à un point crucial de notre étude. Selon la façon dont on va décider d'interpréter les dérivations, un critère d'identité pourra être accepté ou rejeté. Troelstra ne rejette pas entièrement la conjecture de Prawitz, mais il précise qu'elle s'applique à des dérivations dont il faut déterminer explicitement qu'on interprète comme descriptions de « preuves directes », dont les descriptions canoniques seraient les preuves sans coupures. Si nous décidons de considérer un concept plus général de preuve, faisant appel par exemple à la notion de construction, où celle de calcul par réduction, la conjecture sera fausse. Et l'on parle toujours de la partie "correction" de la conjecture, celle qui était jugée non problématique par son auteur. On peut maintenant voir qu'elle est conditionnée à une conception précise et non explicitée des démonstrations. Le fait que toute dérivation décrive la démonstration directe correspondante ne va pas de soi. L'analogie avec le langage de l'arithmétique $L_{\mathbb{N}}$ peut être résumée ainsi :

Conjecture de Prawitz	vraie	fausse
Signification d'une dérivation	description d'une "preuve directe"	Description d'un concept plus général de preuve
Signification d'un terme de $L_{\mathbb{N}}$	description d'un entier	description d'un calcul
Signification d'un terme de $\Lambda^{\rightarrow}$	description d'une valeur	description d'un programme

La dernière ligne du tableau reprend la correspondance de Curry-Howard utilisée dans les définitions de notre partie 1.2.2 pour comprendre le lien entre la distinction que Troelstra effectue pour les termes et celle que nous avons traitée en 2.3.2 pour les dérivations.

Troelstra parvient après ces réflexions à considérer les dérivations dans le détail. Il reprend une idée de Kreisel pour distinguer la preuve de $53 + 27 = 27{+}52$ issue d'une preuve de $\forall x \forall y x{+}y = y{+}x$ dont on a instancié les variables universelles, d'une preuve de la même formule issue de l'évaluation des deux termes de l'addition. Widebäck, toujours dans [Wid01], ne trouve pas cette séparation justifiée et affirme qu'elle suppose — ce qui n'est pas immédiat à son sens — d'une part l'existence d'une évaluation numérique, et d'autre part que cette évaluation ne présuppose pas la commutativité de l'addition : la computation pourrait se généraliser à une preuve de commutativité.

Cette critique demande donc qu'on essaie de défendre la position de Troelstra. Se donnant les règles classiques pour l'égalité de la déduction naturelle pour le langage $L_{\mathbb{N}}$, ainsi que des axiomes standard pour l'addition, 0, et le successeur, la symétrie de l'égalité, on peut dériver sans grande difficulté, par exemple $s^2(0) + s^3(0) = s^3(0) + s^2(0)$.

$$\dfrac{\dfrac{\dfrac{}{s^5(0) = s^5(0)}}{s(s(0 + s^3(0))) = s^5(0)}}{s(0) + s^3(0)) = s^5(0)}$$

$$\dfrac{\dfrac{\dfrac{\dfrac{}{s(s(s^3(0))) = s(s(s^3(0)))} \quad \dfrac{\forall x(x = 0 + x)}{0 + s^3(0) = s^3(0)}}{s(s(0 + s^3(0))) = s(s(s^3(0)))}}{s(s(0 + s^3(0))) = s^5(0)}}{s(0) + s^3(0)) = s^5(0)}$$

$$\dfrac{\dfrac{\dfrac{\dfrac{}{s(s(0) + s^3(0)) = s(s(0) + s^3(0))} \quad \dfrac{\forall x \forall y s(x) + y = s(x + y)}{s(0) + s^3(0) = s(0 + s^3(0))}}{s(s(0) + s^3(0)) = s(s(0 + s^3(0)))}}{s(0) + s^3(0)) = s^5(0)}$$

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{}{s(s(0) + s^3(0)) = s(s(0) + s^3(0))} \quad \dfrac{\forall x \forall y s(x) + y = s(x + y)}{s(0) + s^3(0) = s(0 + s^3(0))}}{s(s(0) + s^3(0)) = s(s(0 + s^3(0)))}}{s(0) + s^3(0)) = s^5(0)}}{s(s(0)) + s^3(0) = s^5(0)}$$

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{}{s(s(0) + s^3(0)) = s(s(0) + s^3(0))} \quad \dfrac{\forall x \forall y s(x) + y = s(x + y)}{s(0) + s^3(0) = s(0 + s^3(0))}}{s(s(0) + s^3(0)) = s(s(0 + s^3(0)))}}{s(0) + s^3(0)) = s^5(0)} \quad \dfrac{\forall x \forall y s(x) + y = s(x + y)}{s(s(0)) + s^3(0) = s(s(0) + s^3(0))}}{s(s(0)) + s^3(0) = s^5(0)}$$

On se dispensera de l'évaluation du membre droit de l'équation qui se comporte de la même façon, et on se contentera de remarquer que seule, la définition inductive de l'addition a été utilisée comme hypothèse. Cette preuve requiert moins d'informations que la précédente, dans la mesure où l'on n'a pas eu besoin de montrer la commutativité de l'addition en général : on n'a pas eu besoin de faire appel au principe de récurrence, ce qui est une opération non négligeable. De plus, cela montre qu'une preuve particulière de la sorte ne généralise à une preuve de commutativité qu'en faisant appel à un axiome supplémentaire, à savoir l'axiome d'induction. On peut d'ailleurs voir à cette moitié de preuve particulière de commutativité pourquoi la possibilité d'introduire et d'éliminer des coupures avec des résultats généraux permet notamment à Boolos de voir rentrer la taille astronomique d'une preuve normale dans une page avec lemmes. On note ici que l'on a fait passer deux opérations successeurs de l'autre côté du signe + (sur le membre gauche), et l'on voit graphiquement qu'il y a trois sous-preuves à notre dérivation : une pour le 0, et deux autres pour les deux symboles s. On reste sur quelque chose de

conséquent, même si l'exemple est ici moins dégénéré.

Si la commutativité de l'addition est présupposée dans une preuve particulière, c'est d'une façon assez lointaine, car ce ne sont pas les mêmes outils de preuve utilisés dans les deux cas. Par ailleurs, il faut bien reconnaître que l'addition *est* commutative, et que l'usage que l'on fait d'une opération est aussi bien un usage de ses propriétés algébriques. Ainsi, on ne montre pas cette propriété en général, mais c'est bien l'utiliser d'une certaine façon que de montrer qu'elle est vraie pour un cas particulier. Peut-être en ce sens faut-il comprendre la possibilité d'une telle présupposition. Mais dans ce cas, la preuve par induction de $\forall x \forall y(x + y = y + x)$ agit de même et on est conduits à des apories ou à vouloir montrer des choses qui ne soient pas impliquées de quelque manière par nos hypothèses.

4.2 La formalisation et les registres : conditions de possibilité de la séparation

Un point que nous n'avons encore fait qu'évoquer est celui de la formalisation et de ses liens avec la question de l'identité. On peut remarquer que ces sujets sont interdépendants : la façon que l'on a de répondre à l'un donne une heuristique à l'autre. En effet, si l'on considère qu'un langage formel est adéquat pour formaliser les raisonnements, il le sera en particulier pour les démonstrations, et c'est en travaillant sur ce langage et les preuves qui y seront formalisées que l'on aura une chance de comprendre comment distinguer deux démonstrations où quand elles correspondent au même raisonnement. D'un autre côté, si l'on trouve une relation apte à représenter l'équivalence *dans*

l'idée des preuves, alors les classes d'équivalence de cette relation donneront des indications à qui veut représenter ces raisonnements dans un certain langage en capturant ni plus ni moins que la procédure mentale correspondant à la preuve.

Nous ne proposerons pas ici, bien entendu, de formalisation adéquate de la logique dans un langage particulier : les débats que cela peut engendrer ainsi que les difficultés que posent chaque tentative, parlent pour eux-mêmes. Au moins justifient-ils de penser que répondre ici à cette question philosophique serait bien trop ambitieux pour ce mémoire et nous écarterait de notre propos.

On peut lire dans l'introduction du livre *Why prove it again ?* [Daw15], qui recense différentes preuves de théorèmes mathématiques, que, « intuitivement, [deux preuves] sont différentes quand elles utilisent des concepts ou tactiques différentes ». (p.1) On peut dire que jusqu'à maintenant, on a surtout évoqué les différences entre preuves à partir des tactiques qui permettaient de les distinguer (utiliser ou non un lemme par exemple, serait de l'ordre d'un choix de tactique). L'idée que deux preuves puissent différer sur les concepts invoqués ne va pas de soi lorsqu'on se concentre sur les dérivations qui sont l'objet de la théorie de la démonstration.

Le premier exemple pris dans le livre est celui de l'équation $1+3+5+\cdots+(2n-1) = n^2$ qui admet plusieurs preuves. Une de celles-ci est graphique, on représente les unités par des blocs, formant un carré. Et l'on remarque depuis un bloc à un angle (pour 1), que pour passer a un carré d'un côté plus large, on ajoute deux rangées de blocs sur deux côtés adjacents, et un bloc pour les relier. L'égalité se vérifie graphiquement sans problème. Une autre preuve graphique est décrite, donnant une version "en escalier" de la démonstration.

La deuxième preuve se fait par induction, par un raisonnement arithmétique simple. Une autre preuve, due à Gauss, consiste en un raisonnement arithmétique dupliquant, inversant la série, puis pratiquant dessus diverses opérations jusqu'à obtenir l'équation voulue. On a ici manifestement deux tactiques différentes, mais utilisant toutes deux des calculs arithmétiques. Les deux preuves (arithmétiques) n'utilisent manifestement pas les mêmes outils : la première utilise le principe d'induction, alors que la seconde consiste à manipuler une série quelconque pour montrer le résultat.

Les deux preuves graphiques comme les deux preuves arithmétiques correspondent à des tactiques différentes dans un même registre. On voit assez clairement en quoi elles peuvent différer. C'est le passage d'un registre à un autre qui semble plus problématique. Il semble d'abord assez évident qu'une preuve graphique ne peut être identifiée avec une preuve arithmétique. Pour autant, la difficulté majeure est que l'on ne semble pas pouvoir déterminer de façon précise une méthode de comparaison des arguments de registres distincts.

On peut concevoir aisément deux représentations, l'une graphique et l'autre arithmétique, du même raisonnement démonstratif. La séparation devient ici quasiment intraitable comment savoir si la preuve par les blocs n'est pas une façon de se représenter la preuve par la méthode de Gauss ? Où même avec la preuve par induction, car c'est bien en constatant le passage d'un niveau n à un autre que l'on peut se laisser convaincre par la figure. Le fait d'avoir fait appel à des intuitions différentes ne nous assure en rien que les concepts d'inférence soient distincts. Si la divergence est pratique, pédagogique, lexicale, comment être sûr de n'avoir pas séparé abusivement ?

Les différents aspects que nous avons traités de la question de l'identité entre les preuves se concentraient sur la possibilité d'identifier ou de distinguer les dérivations d'une *même syntaxe*. La difficulté que l'on essaie ici d'identifier semble montrer que cette approche, derrière les intérêts théoriques et techniques qu'elle apporte, semble réduite à l'ambition de pouvoir traiter toutes les démonstrations mathématiques dans un seul formalisme. Ajoutons que ce formalisme ne devrait présenter aucune des lacunes que nous avons exhibées dans les langages présentés, comme les réseaux, le calcul des séquents ou le λ-calcul.

Dans le livre *Raisonnements divins*, [AZ04] donne ainsi (entre autres) deux preuves de l'infinité des nombres premiers : la première, celle d'Euclide bien connue, et l'autre s'appuyant sur la théorie des groupes et le théorème de Lagrange. Si l'on disposait d'un langage permettant de donner des preuves de théorèmes issus de domaines aussi divers que l'algèbre et la théorie des nombres, on pourrait se demander quels sont les principes communs aux deux preuves, quitte à éliminer les coupures correspondant à l'application du théorème de Lagrange par exemple.

Quel sera alors le langage permettant de décrire les raisonnements s'appliquant aussi bien aux treillis qu'aux triangles ? aussi bien aux nombres transcendants qu'aux modèles monstres ? Tant d'objets, tant de concepts différents et complexes, comment les appréhender tous, ou même espérer les décrire dans une grammaire unique ou dans des systèmes déductifs corrects et complets ? Pour quelle sémantique ?

Les problèmes philosophiques et logiques qui sous-tendent toutes ces questions nous poussent à penser que posé en ces termes, la question de la re-

cherche d'un langage compétent pour notre objet n'a pas beaucoup de sens. Et si l'on sort des systèmes déductifs formels pour se questionner sur les différentes preuves de la pratique mathématique, l'interpénétrabilité des registres et l'impossibilité d'une séparation honnête nous pousse à réduire la question de l'identité entre les preuves à celle de la formalisation des raisonnements mathématiques dans un langage convenable [15].

4.3 Digression aristotélicienne – une comparaison qualitative des preuves

A-t-on aujourd'hui fait mieux qu'Aristote pour déterminer l'essence du raisonnement démonstratif ? C'est la question que l'on peut se poser si l'on relit à la lueur de notre problème les *Seconds analytiques* ([Ari05]). On se rappelle que le cadre démonstratif se réduisait à la syllogistique appliquée au langage naturel, ce qui aujourd'hui peut sembler relativement éloigné de nos préoccupations. Pour autant, la caractérisation qui est faite du syllogisme démonstratif, celui qui définit la science, pose entre autres deux contraintes intéressantes sur les preuves : elles doivent être au plus haut degré de généralité, et partir de principes adaptés. Expliquons grossièrement de quoi il s'agit avant d'essayer de justifier cette référence pour éclairer la question au regard des perspectives aristotéliciennes.

L'idée est ici de retenir une comparaison *qualitative* des démonstrations [16].

15. Par « convenable », nous entendons un langage qui se laisse domestiquer pour pratiquer sur lui une théorie de la démonstration acceptable. Par « acceptable », nous entendons acceptable...

16. Notons que la distinction entre dérivation formelle et démonstration est ici ambiguë. Nous ne nous plongerons pas dans ce problème complexe et admettrons que, dans la mesure où les syllogismes sont écrits en langue naturelle et censés structurer le raisonnement autant

Le problème n'est plus de trouver une bonne relation d'identité, mais il se pose comme la recherche de la meilleure preuve d'un théorème. Les critères de distinction et les possibilités de juger une preuve meilleure qu'une autre nous donneront un aperçu d'une séparation qualitative entre les preuves telle que nous souhaitons l'attribuer ici au philosophe.

L'exemple qui nous éclairera ici sera celui de la preuve qu'un triangle isocèle a ses angles égaux à deux droits. Exemple qui apparaît à de multiples reprises dans le texte, notamment en 85a(20-30). Aristote compare implicitement deux preuves de cette propriété pour un objet particulier. La première pourrait se schématiser comme ceci :

$$\dfrac{\dfrac{[\text{donnée de } t \text{ un triangle isocèle}]}{t \text{ est un triangle} \wedge t \text{ est isocèle}} \qquad \dfrac{\text{Tout triangle a ses angles égaux à deux droits}}{\text{Tout triangle isocèle a ses angles égaux à deux droits}}}{t \text{ a ses angles égaux à deux droits}}$$

Et la seconde pourrait de même s'écrire comme cela :

$$\dfrac{\dfrac{[\text{donnée de } t \text{ un triangle isocèle}]}{t \text{ est un triangle}} \qquad \text{Tout triangle a ses angles égaux à deux droits}}{t \text{ a ses angles égaux à deux droits}}$$

Pour Aristote, ces deux preuves sont fondamentalement distinctes, et seule la première correspond a une vraie démonstration scientifique. Le problème qui entache la première est relatif au choix des principes du syllogisme (dans notre schéma : l'inférence binaire). On montre que t a ses angles égaux à deux droits car il est un triangle isocèle. Le problème est lié au degré de généralité des prémisses qui est ici trop bas.

qu'en favoriser l'exposition, on écrit une démonstration sans question de formalisation.

La seconde preuve est adéquate en ce qu'elle prend le triangle *en tant que* triangle pour montrer la propriété. Le prendre en tant que triangle isocèle était une erreur scientifique. La validité du syllogisme n'est pas suffisante à en faire une preuve convenable, et on peut attribuer ce point à l'aspect épistémique qu'attache Aristote au syllogisme lorsqu'il le veut *scientifique*[17]. L'idée est que la première preuve ne nous apporte qu'une connaissance imparfaite de la propriété comme de l'objet. Montrer que t a ses angles égaux à deux droits parce que c'est un triangle isocèle, c'est déjà partir du mauvais pied. Si l'on veut comprendre que t a la propriété parce que tous les triangles l'ont et que c'en est un, il faut se restreindre à la seconde preuve qui élimine l'attribut "isocèle" dans la prémisse du syllogisme.

On peut remarquer que conserver la prémisse "t est isocèle" dans la première preuve impose de rajouter que ce qui est vrai pour tout triangle l'est pour tout isocèle : c'est une forme d'affaiblissement du théorème général. Par ailleurs, le terme "isocèle" est éliminé dans l'application syllogistique, si l'on pense à la déduction naturelle, le passage de la première à la seconde preuve relève de la contraction d'une coupure, ou de quelque chose de très similaire. Là où l'on a pu dire qu'une preuve avec coupure contenait plus d'information qu'une preuve analytique (ici, celle où les prémisses sont adaptées à la conclusion), Aristote en introduisant une valeur épistémique aux preuves, paraît affirmer qu'elle en contient *trop* ; et qu'ainsi les *détours* dont parlait Gentzen seraient un obstacle à une connaissance scientifique qui doit saisir les propriétés des objets de la façon la plus générale possible. C'est bien le triangle

17. Dans les *Seconds Analytiques*, l'objet est justement de définir le syllogisme scientifique, qui constitue la seule vraie démonstration. Nous n'irons pas plus loin dans l'exégèse du texte.

l'objet le plus général possédant la propriété d'avoir ses angles égaux à deux droits, et le montrer en le prenant en tant que triangle, c'est apporter une meilleure connaissance de la propriété établie.

Pousser plus loin l'étude du syllogisme scientifique nous mènerait trop loin de notre objet, et nous devrons nous contenter de l'évocation qui vient d'être faite. Soulignons néanmoins que la définition que produit Aristote de la science et qui le pousse à déterminer ce qu'est une *vraie démonstration* nous donne des éléments de réflexion non obsolètes quant à la possibilité de comparer les démonstrations de façon qualitative en introduisant un critère épistémique, comme celui-ci fondé sur la généralité des prémisses.

Certes, un critère de comparaison des preuves n'est pas une relation d'équivalence apte à capturer l'identité. Mais cela pourrait être un point de départ pour une approche différente des démonstrations. La comparaison donne un critère de séparation, mais pas d'identification. On sait quand deux preuves sont de qualités différentes et représentent *a fortiori* deux raisonnements distincts ; pour autant, on serait en peine de savoir comment rigoureusement identifier (ou non) deux preuves du même degré de généralité, de même qualité : cela ne suffit pas nécessairement pour établir qu'il s'agît du même raisonnement.

On peut attribuer cette difficulté au caractère "non formalisé" de la théorie de la démonstration syllogistique, dans le sens où l'on a pas ici de langage exclusivement déductif duquel la description serait un objet dont l'on pourrait parler dans un métalangage. Mais affirmer cela peut aussi être une manière un peu facile d'évacuer une difficulté plus profonde : l'aspect qualitatif de notre approche des preuves ne permet peut-être pas d'identification justement parce

qu'il fait entrer en jeu des éléments non syntaxiques à notre appréhension des preuves, ce qui nous prive peut-être par principe de la possibilité d'une relation d'équivalence et de synonymie entre les preuves qui soit qualitative. Ce n'est qu'une hypothèse, et l'examen de cette question demanderait une étude plus profonde.

5 Conclusions

De l'étude livrée dans ces pages, quelles conclusions peut-on extraire ? Il peut sembler frustrant de voir que toutes les solutions proposées à la question de l'identité revêtent chacune à sa façon un caractère insatisfaisant. Mais se contenter de ces observations ne rendrait pas justice aux travaux mentionnés, au moins pour ceux qui ont proposé une réponse au problème.

Nous espérons qu'un éclaircissement a été apporté non pas seulement à l'identité des démonstrations dans les systèmes de preuve, mais qu'ont été ouvertes au moins les perspectives suivantes :

1. Apporter des considérations donnant un regard, que l'on espère éclairant, sur la relation entre les dérivations formelles et les preuves *intuitives* ou *mentales* ; et en cela de donner une éventuelle ouverture à la question de savoir comment définir proprement ce qu'est une preuve.

2. Exhiber l'intérêt, et même la nécessité, de traiter un problème touchant à la philosophie de la logique à l'aide d'appareils techniques relativement sophistiqués. Ce point consisterait dans la façon de comprendre la possibilité de dresser (ou non) une relation entre une notion formelle et une notion informelle en manipulant des concepts et des outils logiques non triviaux.

3. A l'opposé, tenter de circonscrire avec justesse la capacité des outils mathématiques à répondre carrément à une question philosophique. Distinguer l'utilisation de la logique mathématique pour comprendre la façon dont on peut appréhender un problème, et la possibilité d'y répondre formellement.

Ne retenir que les difficultés posées par les réponses techniques serait se restreindre au troisième point. Par ailleurs, si l'on cherche à mieux comprendre en quoi la notion de preuve peine à être capturée par une définition formelle, il semble que les points 1 et 2 sont des points incontournables de l'argumentation établissant ces insuffisances.

On peut au contraire ce concentrer sur la façon dont ces éléments font entrevoir à la fois le problème et les objets qui y sont impliqués. Capturer l'identité, c'est capturer en extension les preuves, comme nous le prétendions en introduction. Par là, il ne faut sans doute pas voir un échec à la compréhension des preuves par le logicien, mais plutôt le gain d'une pluralité de points du vue, qui ne peut qu'être bénéfique : si les réseaux comme la normalisation ne suffisent pas à satisfaire complètement nos attentes, ils ont le bon goût d'avoir chacun un intérêt spécifique et incompressible dans l'appréhension du concept de preuve.

Une autre direction à la poursuite de cette étude serait d'étudier non pas le lien entre la théorie de la démonstration et les preuves *mentales*, mais davantage le lien entre la logique et les mathématiques. Il semble que l'étude des raisonnements mathématiques effectifs telle que livrée dans [AZ04] et [Daw15] ne puisse être capturée par la logique, ou du moins par la théorie de la démonstration. Ainsi, proposer un raisonnement abstrait et théorique sur les démonstrations et les relations qu'elles entretiennent avec leur pendant formalisé (ou axiomatisé) n'est peut-être pas envisageable dans le cadre de la vraie pratique mathématique ; et il semble qu'il faille alors se contenter d'une version caricaturale, abstraite et simpliste [18] des démonstrations, telles que

18. Dans le sens où l'on ne cherche pas en général à formaliser les preuves de théorèmes

les dérivations ou les réseaux. Reste à discuter la pertinence ou la possibilité d'une conciliation entre l'analyse logique des raisonnements déductifs et l'activité des mathématiciens observable dans les publications et les laboratoires.

mathématiques complexes, quand on travaille en déduction naturelle ou en calcul de séquents par exemple

Références

[Ari05] Aristote. *Seconds Analytiques*. GF Flammarion, 2005.

[AZ04] Martin Aigner and Günter M. Ziegler. *Proofs from THE BOOK (3. ed.)*. Springer, 2004.

[Bar84] H.P. Barendregt. *The lambda calculus : its syntax and semantics*. Studies in logic and the foundations of mathematics. North-Holland, 1984.

[BDS14] Marc Bagnol, Amina Doumane, and Alexis Saurin. Analyse de dépendances et correction des réseaux de preuve. In *25. Journées francophones des langages applicatifs, Fréjus, France, January 8-11, 2014.*, pages 159–174, 2014.

[Boo84] George Boolos. Don't eliminate cut. *Journal of Philosophical Logic*, 13(4) :373–378, November 1984.

[CF58] H.B. Curry and R. Feys. *Combinatory Logic*. Number vol. 1 in Combinatory Logic. North-Holland Publishing Company, 1958.

[Cho15] Jules Chouquet. Exponentielles et connexité dans les réseaux à la Ehrhard. *Université Paris-Diderot, mémoire de master. Dir. Lionel Vaux (Aix-Marseille Université, Institut de mathématiques de Luminy)*, (Non publié), 2015.

[CL93] R. Cori and D. Lascar. *Logique mathématique : Fonctions récursives, théorème de Gödel, théorie des ensembles, théorie des modèles*. Axiomes (Paris). Masson, 1993.

[CR74] Stephen A. Cook and Robert A. Reckhow. On the lengths of proofs in the propositional calculus (preliminary version). In *Proceedings of the 6th Annual ACM Symposium on Theory of Computing, April 30 - May 2, 1974, Seattle, Washington, USA*, pages 135–148, 1974.

[Daw15] J.W. Dawson. *Why Prove it Again ? : Alternative Proofs in Mathematical Practice*. Springer International Publishing, 2015.

[Dos03] Kosta Dosen. Identity of proofs based on normalization and generality. *Bulletin of Symbolic Logic*, 9(4) :477–503, 2003.

[DR89] Vincent Danos and Laurent Regnier. The structure of multiplicatives. *Archive for Mathematical Logic*, 28(3) :181–203, 1989.

[Ehr14] Thomas Ehrhard. A new correctness criterion for MLL proof nets. In *Joint Meeting of the Twenty-Third EACSL Annual Conference on Computer Science Logic (CSL) and the Twenty-Ninth Annual ACM/IEEE Symposium on Logic in Computer Science (LICS), CSL-LICS '14, Vienna, Austria, July 14 - 18, 2014*, pages 38 :1–38 :10, 2014.

[Fre79] G. Frege. *Begriffsschrift, Eine Der Arithmetischen Nachgebildete Formelsprache Des Reinen Denkens.* 1879.

[Fre84] G. Frege. *Die Grundlagen der Arithmetik : eine logisch mathematische Untersuchung über den Begriff der Zahl.* W. Koebner, 1884.

[Gen35] G. Gentzen. Untersuchungen über das logische schließen i. *Mathematische Zeitschrift*, 39 :176–210, 1935.

[GFL55] G. Gentzen, R. Feys, and J. Ladrière. *Recherches sur la déduction logique : Traduction et commentaire.* Philosophie de la matière. Presses universitaires de France, 1955.

[Gir87] Jean-Yves Girard. Linear logic. *Theor. Comput. Sci.*, 50 :1–102, 1987.

[Gir91] Jean-Yves Girard. A new constructive logic : Classical logic. *Mathematical Structures in Computer Science*, 1(3) :255–296, 1991.

[Gri90] Timothy Griffin. A formulae-as-types notion of control. In *Conference Record of the Seventeenth Annual ACM Symposium on Principles of Programming Languages, San Francisco, California, USA, January 1990*, pages 47–58, 1990.

[Gur12] Yuri Gurevich. What is an algorithm ? In Mária Bieliková, Gerhard Friedrich, Georg Gottlob, Stefan Katzenbeisser, and György Turán, editors, *SOFSEM 2012 : Theory and Practice of Computer Science - 38th Conference on Current Trends in Theory and Practice of Computer Science, Špindlerův Mlýn, Czech Republic, January 21-27, 2012. Proceedings*, volume 7147 of *Lecture Notes in Computer Science*, pages 31–42. Springer, 2012.

[Hug06] Dominic J. D. Hughes. Towards hilbert's 24^{th} problem : Combinatorial proof invariants : (preliminary version). *Electr. Notes Theor. Comput. Sci.*, 165 :37–63, 2006.

[KK67] Georg. Kreisel and J. L. Krivine. *Elements of mathematical logic. (Model theory) [By] G. Kreisel and J. L. Krivine.* North Holland Pub. Co Amsterdam, 1967.

[Kle51] Stephen Cole Kleene. Permutability of inferences in gentzens calculi lk and lj. In *BULLETIN OF THE AMERICAN MATHEMATICAL SOCIETY*, volume 57, pages 485–485. AMER MATHEMATICAL SOC 201 CHARLES ST, PROVIDENCE, RI 02940-2213, 1951.

[Kre71] G. Kreisel. A survey of proof theory {II}. In J.E. Fenstad, editor, *Proceedings of the Second Scandinavian Logic Symposium*, volume 63 of *Studies in Logic and the Foundations of Mathematics*, pages 109 – 170. Elsevier, 1971.

[Kre72] Georg Kreisel. Informal rigour and completeness proofs. In Imre Lakatos, editor, *Problems in the Philosophy of Mathematics*, pages 138–157. North-Holland, 1972.

[Laf90] Yves Lafont. Interaction nets. In *Conference Record of the Seventeenth Annual ACM Symposium on Principles of Programming Languages, San Francisco, California, USA, January 1990*, pages 95–108, 1990.

[Laf95] Yves Lafont. From proof nets to interaction nets. *London Mathematical Society Lecture Note Series*, pages 225–248, 1995.

[Laf97] Yves Lafont. Interaction combinators. *Inf. Comput.*, 137(1) :69–101, 1997.

[Lam85] Joachim Lambek. Cartesian closed categories and typed lambda-calculi. In *Combinators and Functional Programming Languages, Thirteenth Spring School of the LITP, Val d'Ajol, France, May 6-10, 1985, Proceedings*, pages 136–175, 1985.

[Pra65] D. Prawitz. *Natural deduction : a proof-theoretical study*. Stockholm studies in philosophy. Almqvist & Wiksell, 1965.

[Pra75] Dag Prawitz. Ideas and results in proof theory. north-holland publishing company, amsterdam and london. *Journal of Symbolic Logic*, 40 :232–234, 6 1975.

[Ret99] Christian Retoré. Handsome proof-nets : R&b-graphs, perfect matchings and series-parallel graphs. 1999.

[Str06] Lutz Straßburger. Proof Nets and the Identity of Proofs. Research Report RR-6013, INRIA, 2006.

[Thi03] Rüdger Thiele. Hilbert's twenty-fourth problem. *The American Mathematical Monthly*, 110(1) :1–24, 2003.

[Tro75] A Troelstra. Non-extensional equality. *Fundamenta Mathematicae*, 82(4) :307–322, 1975.

[Wid01] F. Widebäck. *Identity of Proofs*. Acta Universitatis Stockholmiensis. Almqvist & Wiksell International, 2001.