HAL open science

Algorithmes et modèles : l'histoire d'une convergence

Gilles Dowek

To cite this version:

Gilles Dowek. Algorithmes et modèles : l'histoire d'une convergence. 2012. hal-04061691

HAL Id: hal-04061691

https://inria.hal.science/hal-04061691

Preprint submitted on 7 Apr 2023

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.

Algorithmes et modèles : l'histoire d'une convergence

Gilles Dowek

Dans cette leçon, je vais essayer de démontrer que *toutes les théories super-cohérentes ont la propriété d'élimination des coupures*. Toutefois, avant de commencer, je dois dire que ce théorème ne fait pas partie de ceux qui ont longtemps été des conjectures et qui, par des contributions accumulées aux cours des années, ont finalement été démontrés. C'est plutôt un théorème qui a été démontré dès qu'il a été énoncé : la difficulté était de comprendre comment l'énoncer, plutôt que d'en trouver une démonstration.

Une telle situation n'est pas rare en logique et, en particulier, en théorie de la démonstration. Il y a bien entendu, en logique comme ailleurs, des résultats qui ont longtemps été des conjectures, auxquelles des tentatives de démonstrations et des démonstrations partielles ont été apportées, jusqu'à ce qu'un jour, ils finissent par être complètement démontrés. Mais pour de nombreux résultats, la difficulté a plus été de bien poser le problème, que de le résoudre.

Diverses explications de cette observation ont été tentées. Une première est que la logique est une théorie jeune et que toutes les théories mathématiques, dans leur phase de genèse, ont été dans cette situation, où l'on cherche davantage à clarifier les concepts, qu'à démontrer des théorèmes. Si nous croyons à cette explication, la logique arrivera sans doute un jour dans une phase de maturité : ses concepts seront stabilisés et nous chercherons uniquement à résoudre des problèmes ouverts.

Une deuxième est que les objets étudiés par la logique, les démonstrations, sont un peu rugueux et que, de ce fait, nous avons toujours un peu de mal à les saisir, ce qui explique que nous soyons éternellement en train de les redéfinir, pour les appréhender plus facilement.

Une troisième enfin est que toutes les théories mathématiques sont dans ce cas. Par exemple, d'Archimède à Weierstrass, on s'est demandé ce qu'était une série convergente. Définir cette notion de convergence a beaucoup occupé les mathématiciens, autant peut-être que résoudre des problèmes sur les séries convergentes.

Je ne vais pas discuter ces hypothèses plus avant. Cette remarque avait uniquement pour but de vous inciter à vous demander si, dans vos propres domaines d'intérêt, il est plus difficile de résoudre des problèmes ou de bien les poser.

Les buts de la théorie de la démonstration

Le résultat que je veux vous présenter fait partie d'une branche de la logique appelée *la théorie de la démonstration*, qui se définit assez simplement comme la branche de la logique dans laquelle on cherche à établir des propriétés des propositions et de leurs démonstrations.

Indépendance et non-démontrabilité Un premier type de problèmes que l'on se pose à propos des démonstrations est celui de leur existence. Un résultat célèbre dans ce domaine est qu'il n'existe pas de démonstration de l'axiome des parallèles à partir des autres axiomes de la géométrie.

Des résultats de ce type s'appellent des résultats d'*indépendance* ou de *non-démontrabilité*. Ils constituent un des objectifs de la théorie de la démonstration.

Contenu algorithmique Un deuxième type de problèmes concerne le contenu algorithmique des démonstrations. Quand nous démontrons une proposition de la forme

$$\forall x \exists y \, P(x, y),$$

nous procédons bien souvent en construisant, explicitement ou implicitement, une fonction, ou plus précisément un algorithme, f qui vérifie la propriété :

$$\forall x \; P(x, f(x)).$$

Une telle fonction, un tel algorithme, s'appelle le *contenu algorithmique* de cette démonstration. Par exemple, le contenu algorithmique d'une démonstration de la proposition

$$\forall x \exists y \, (x = 2y \; ou \; x = 2y + 1),$$

est un algorithme qui divise son argument par 2.

Un problème que l'on cherche à résoudre en théorie de la démonstration est de construire des méthodes qui permettent de trouver le contenu algorithmique des démonstrations, de rendre explicite ces algorithmes souvent implicites et diffus.

Mais toutes les démonstrations n'ont pas de contenu algorithmique, ce qui mène à un autre type de problème : caractériser les démonstrations qui ont un contenu algorithmique et celles qui n'en ont pas.

Taille des démonstrations et complexité Un dernier exemple enfin. Si Γ et Γ' sont deux théories, par exemple deux ensembles d'axiomes, telles que toute proposition A qui a une démonstration dans Γ a aussi une démonstration dans Γ', nous pouvons nous interroger sur la taille des démonstrations dans une théorie et dans l'autre. Typiquement, chercher à démontrer que pour toute démonstration π dans Γ, il existe une démonstration π' dans Γ' qui est plus courte que π ou, de manière plus intéressante, exponentiellement plus courte que π.

Les recherches dans ce domaine sont particulièrement actives en ce début de XXIe siècle puisque cette notion de taille des démonstrations est liée à l'un des *Millennium Prize Problems* de l'Institut CLAY : « P différent de NP ».

Bien entendu, il ne s'agit là que de quelques exemple. Il n'est pas possible de fermer la liste des problèmes sur lesquels travaillent les théoriciens de la démonstration et il y aura demain d'autres problèmes que l'on se posera à propos des démonstrations. Il sera alors naturel de les classer dans la théorie de la démonstration.

1 Deux outils

Une grande partie de ma leçon sera consacrée à opposer deux types d'outils utilisés en théorie de la démonstration et, plus précisément, à dire qu'ils ont été opposés par le passé, mais que cette opposition n'est plus justifiée aujourd'hui. Ma leçon sera donc un moment de réconciliation : je vais essayer de montrer que ces deux types d'outils peuvent être utilisés ensemble et qu'il n'y a pas d'opposition méthodologique entre eux. Ce sera l'objet de ma conclusion. Quels sont ces outils ?

1.1 Les modèles

Le premier est la notion de *modèle*. Et pour présenter ce qu'est un modèle je vais commencer par présenter ce qu'est un *langage*.

La notion de langage Considérez les *propositions* mathématiques suivantes, les plus simples sans doute que vous ayez jamais vues :

$$\begin{gathered} 7 < 3, \\ 3 + 4 = 7, \\ 7 < 3 \textit{ et } 3 + 4 = 7, \\ \exists x\,(x + 4 = 7), \\ x + 4 = 7. \end{gathered}$$

À l'intérieur de ces propositions, nous trouvons un autre type d'expressions « 3 », « 7 », « $3 + 4$ », « $x + 4$ », etc. qui s'appellent des *termes*. Il y a entre les propositions et les termes la même opposition qu'il y a, en grammaire, entre les phrases et les groupes nominaux. Une proposition comme « $7 < 3$ » est susceptible d'être vraie ou fausse — en l'occurrence elle est fausse. À l'inverse, « 7 » n'est ni vrai ni faux : une phrase peut être jugée vraie ou fausse, mais pas un groupe nominal.

La notion de langage logique est fondée sur une opposition entre ces deux types d'expressions : des expressions qui expriment des faits et sur lesquelles nous pouvons porter un jugement de vérité, qui s'appellent des *propositions*, et des expressions qui désignent des objets et sur lesquels nous ne pouvons pas porter de jugement de vérité, qui s'appellent des *termes*.

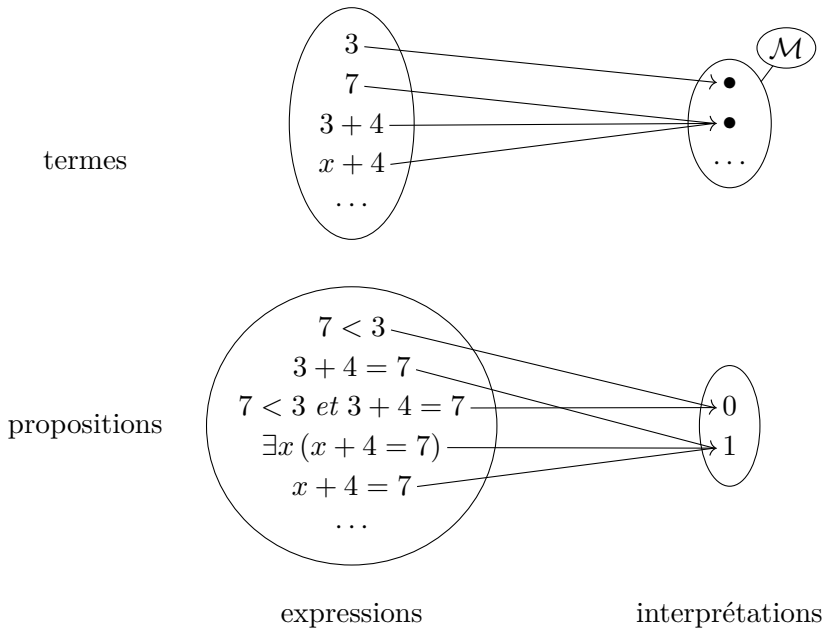

FIGURE 1 – Un modèle

Les termes sont formés à partir de *constantes*, 3, 4, 7, etc. et de *symboles de fonction*, $+$, $\times$, etc. Par exemple, le terme 4 est une constante, et le terme $3+4$ est formé en appliquant le symbole de fonction à deux termes 3 et 4.

Les propositions les plus simples sont les propositions *atomiques* comme « $7 < 3$ » ou « $3+4 = 7$ ». Elles sont formées en appliquant un *symbole de prédicat*, $=$, $<$, à un ou plusieurs termes. À partir de ces propositions atomiques, nous pouvons construire des propositions plus complexes comme « $7 < 3$ *et* $3+4 = 7$ » en utilisant des *connecteurs*, ici la conjonction *et*. Nous pouvons également former des propositions en utilisant les quantificateurs $\forall$ et $\exists$, par exemple la proposition « $\exists x\,(x + 4 = 7)$ ». À l'intérieur de cette proposition se trouve a une autre proposition : « $x + 4 = 7$ ». Mais cette proposition atomique contient une *variable* : x. Cette variable est *liée* par le quantificateur dans la proposition « $\exists x\,(x + 4 = 7)$ » alors qu'elle est *libre* dans la proposition « $x + 4 = 7$ ». De même, les termes comme « $x + 4$ » peuvent contenir des variables libres.

La notion de modèle Définir un modèle consiste à définir deux ensembles : un ensemble où interpréter les termes et un ensemble où interpréter les propositions, puis un morphisme entre les expressions et les interprétations.

Considérons la figure 1. L'ensemble où interpréter les termes est un ensemble $\mathcal{M}$ quelconque, et l'ensemble où interpréter les propositions est — pour le moment — la paire $\{0, 1\}$. Je vais beaucoup discuter du choix de cet ensemble :

deux valeurs de vérité suffisent-elles ? C'est l'un des thèmes de la leçon. Mais, pour le moment, contentons nous de cet ensemble $\{0, 1\}$.

Dans cet exemple, le terme 3 est interprété par un élément de l'ensemble $\mathcal{M}$, puis le terme 7 par un autre élément, et le terme $3 + 4$ par ce même élément. Et le terme $x + 4$, pour une raison qui reste à expliquer, est interprété par ce même élément.

Comme souvent en mathématiques, ce ne sont pas tant les ensembles en soi qui sont intéressants, que les opérations définies sur ces ensembles. Ici, comme le langage contient les constantes 3, 4 et 7, nous devons munir l'ensemble $\mathcal{M}$ d'éléments $\hat{3}$, $\hat{4}$ et $\hat{7}$ par lesquels interpréter ces constantes. Puis, comme le langage contient un symbole de fonction $+$, nous devons aussi munir cet ensemble d'une opération, notée $\hat{+}$. Nous pouvons alors construire l'interprétation de tous les termes, simplement en respectant la propriété de morphisme : l'interprétation du terme 3 est $\hat{3}$, celle du terme 4 est $\hat{4}$, celle du terme $3 + 4$ est obtenue en appliquant l'opération $\hat{+}$ aux interprétations $\hat{3}$ et $\hat{4}$ des termes 3 et 4, etc.

Nous devons cependant encore nous demander que faire avec les variables. Une telle interprétation doit, en fait, être paramétrée par sa valeur sur l'ensemble des variables. Dans cet exemple, j'avais vraisemblablement l'idée que x était interprété par le même élément que 3, $x + 4$ se retrouve alors interprété par le même élément que $3 + 7$.

Nous nous trouvons donc dans une situation similaire à celle où nous définissons un morphisme entre espaces vectoriels : nous avons juste besoin de définir l'image d'une base, puisque cela suffit à reconstituer l'image de tous les vecteurs. C'est l'ensemble des variables qui joue ici le rôle de base : une fois que nous avons défini la valeur des constantes et des symboles de fonction, chaque interprétation des variables donne une interprétation de tous les termes.

Pour interpréter les propositions atomiques, nous devons également munir l'ensemble $\mathcal{M}$, non d'opérations, mais de relations : définir autant de relations sur $\mathcal{M}$ qu'il y a de symboles de prédicats, par exemple associer, au symbole de prédicat $<$, une relation $\hat{<}$ sur $\mathcal{M}$. L'interprétation de la proposition $7 < 3$ est alors ou bien 1 si les interprétations des termes 7 et 3 sont liés par cette en relation, ou bien 0 si ce n'est pas le cas. Dans cet exemple $7 < 3$ est interprété par 0, $3+4 = 7$ par 1, etc. À nouveau l'interprétation de la proposition $x+4 = 7$, dépend de l'interprétation des variables choisie. Selon la manière dont nous interprétons x, cette proposition sera interprétée par 0 ou par 1.

Pour interpréter les propositions non atomiques enfin, nous avons besoin d'opérations, définies sur l'ensemble $\{0, 1\}$ complètement indépendamment du modèle, qui indiquent, par exemple, comment construire l'interprétation d'une conjonction quand nous connaissons celle de chacun de ses membres. Ici, il s'agit simplement de la conjonction $\tilde{et}$ définie sur $\{0, 1\}$: $1 \ \tilde{et}\ 1$ vaut 1 et $x \ \tilde{et}\ y$ vaut 0 dans tous les autres cas. Nous avons également besoin d'opérations similaires $\tilde{\Rightarrow}$, $\tilde{\forall}$, toujours sur l'ensemble $\{0, 1\}$, pour l'implication, la quantification universelle, etc.

Au bout du compte, la notion de modèle est juste un raffinement de la notion de morphisme, la seule spécificité est que l'ensemble de départ est un langage et qu'il faut donc tenir compte des variables.

Le théorème de correction Une proposition A est dite *valide* dans un modèle $\mathcal{M}$, si son interprétation est 1 dans ce modèle, quelle que soit l'interprétation des variables.

L'intérêt de cette notion vient d'un théorème, *le théorème de correction*, selon lequel une proposition démontrable est valide dans tous les modèles.

Théorème 1.1 (Correction) *Si A est démontrable, alors A est valide dans tous les modèles.*

Bien entendu, ce théorème, a aussi une forme contraposée : s'il existe un modèle dans lequel une proposition n'est pas valide, alors cette proposition n'est pas démontrable.

La contraposée de ce théorème répond à une question que vous vous êtes peut-être déjà posée : « Comment font les logiciens pour démontrer qu'une proposition n'est pas démontrable ? ». Une réponse serait qu'ils essayent longtemps de trouver une démonstration et que, s'ils n'y arrivent pas, ils concluent que la proposition n'est pas démontrable. Mais, bien entendu, ce n'est pas une bonne réponse. Une bonne réponse est : ils construisent un modèle dans lequel la proposition en question n'est pas valide.

On peut donc montrer qu'une proposition n'est pas démontrable avec un outil aussi simple que cette notion de modèle. Dans des textes de vulgarisation, on lit parfois : « Il y a des choses incroyables, des démonstrations que des propositions n'ont pas de démonstration ! ». En fait, comme vous le voyez, la méthode est assez simple.

Ce théorème de correction a une réciproque : « Une proposition valide dans tous les modèles est démontrable. » En contraposant, cela peut encore s'énoncer : « Si une proposition n'est pas démontrable, alors il existe un modèle dans lequel elle n'est pas valide. » Et cela signifie que cette méthode de démonstration de la non-démontrabilité — fondée sur la contraposée du théorème de correction — est universelle : à chaque fois qu'une proposition n'est pas démontrable, nous pouvons le démontrer de cette façon. La réciproque du théorème de correction s'appelle le théorème de complétude.

Théorème 1.2 (Complétude) *Si A est valide dans tous les modèles alors A est démontrable.*

Ce théorème est dû à Gödel [Gö29] — mais ce n'est pas *le* théorème de Gödel.

À titre d'exemple, nous pouvons montrer que la proposition $(P \Rightarrow Q) \Rightarrow P$, où P et Q sont des symboles de proposition, n'est pas démontrable. À la figure 1, un symbole de prédicat à deux arguments, comme $=$ ou $<$, était interprété par une relation binaire $\hat{=}$ ou $\hat{<}$ sur $\mathcal{M}$, c'est-à-dire une fonction de $\mathcal{M}^2$ dans $\{0, 1\}$. Et quand nous avons un symbole de proposition, c'est-à-dire un symbole de prédicat à 0 arguments, son interprétation est une fonction 0-aire, une fonction de $\mathcal{M}^0$ dans $\{0, 1\}$, c'est-à-dire un booléen : 0 ou 1. Il faut donc associer une valeur booléenne à P et à Q de manière à ce que l'interprétation de la proposition $(P \Rightarrow Q) \Rightarrow P$ soit 0. Il y a quatre possibilités. L'une d'elle est $\hat{P} = 0$ et $\hat{Q} = 0$.

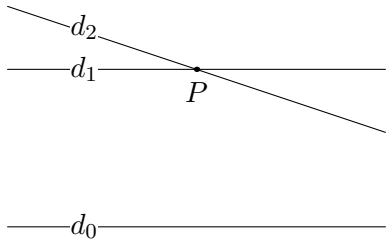

FIGURE 2 – Géométrie hyperbolique collégienne

Dans ce cas, l'interprétation de la proposition $P \Rightarrow Q$ est $0 \not\Rightarrow 0$, c'est-à-dire 1, et donc celle de la proposition $(P \Rightarrow Q) \Rightarrow P$ est $1 \not\Rightarrow 0$, c'est-à-dire 0.

Un exercice plus facile : comment démontrer qu'une proposition atomique, n'est pas démontrable ? Il suffit d'interpréter le symbole de prédicat avec lequel cette proposition est construite par la relation vide, qui ne relie aucun éléments de $\mathcal{M}$. On obtient ainsi un modèle dans lequel cette proposition n'est pas valide. Elle n'est donc pas démontrable. Il s'agit en fait d'un théorème, le théorème d'indépendance.

Théorème 1.3 (Indépendance) *Une proposition atomique n'est pas démontrable.*

Klein Cette méthode de démonstration de la non-démontrabilité est relativement récente à l'échelle de l'histoire des mathématiques. Elle a sans doute été utilisée la première fois par KLEIN en 1871 dans un article qui s'appelle *Sur la géométrie dite non euclidienne* ([Kle71, Kle97]) dans lequel il montre que l'axiome des parallèles n'est pas démontrable à partir des autres axiomes de la géométrie, c'est-à-dire que la proposition $(A_1$ *et ... et* $A_n) \Rightarrow B$ n'est pas démontrable, où B est l'axiome des parallèles et A_1, ..., A_n sont les autres axiomes de la géométrie. En fait, l'idée de la démonstration de KLEIN était déjà implicite chez BELTRAMI, quelques années plus tôt [Bel68, Bel69].

L'axiome des parallèle est un problème sur lequel on avait beaucoup réfléchi. Pendant plus de deux mille ans, entre le IIIe siècle et le XIXe siècle, on avait tenté de démontrer cet axiome à partir des autres axiomes de la géométrie — et parfois réussi, avec des démonstrations fausses bien entendu.

La preuve de KLEIN est une preuve que beaucoup de collégiens font spontanément. Vous leur dites : « J'ai une droite d_0, je prends un point P et je fais passer par P une parallèle d_1 à d_0 (figure 2). Comment faire passer par P une autre parallèle d_2 à d_0 ? ». Beaucoup de collégiens répondent qu'il suffit de pencher un tout petit peu la droite. Vous leur dites, en leur suggérant l'infini du doigt : « Mais non, ça va bien finir un jour par se couper là-bas. » Et ils répondent, indiquant l'extrémité du segment : « Mais non, puisque la droite s'arrête ici ! ». L'axiome des parallèles suppose donc implicitement que les droites peuvent se prolonger à l'infini.

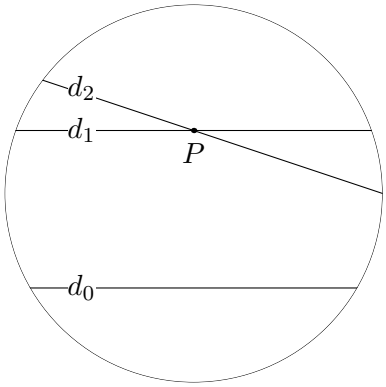

FIGURE 3 – Le modèle de KLEIN

KLEIN, au contraire, propose de ne pas prolonger les droites à l'infini. Dans son modèle (figure 3), le plan est interprété par l'intérieur du disque unité, et les droites par des segments dont les extrémités sont sur le cercle unité. Dans ce modèle, qu'il faudrait bien sûr définir plus précisément, tous les axiomes de la géométrie sont valides : par deux points il passe une et une seule droite, etc., sauf l'axiome des parallèles : par P passent une infinité de parallèles à d_0, dont d_1 et d_2. Ainsi, la proposition $(A_1 \textit{ et } ... \textit{ et } A_n) \Rightarrow B$ n'est pas valide dans ce modèle.

La première utilisation du théorème de correction, et donc de la notion de modèle, date de 1871. Pourtant la définition de cette notion de modèle, que nous devons à TARSKI, ne date que des années trente [Tar33, Tar72]. La définition est donc postérieure de soixante ans au premier théorème qui ne peut se démontrer sans elle. Pendant cette période, les démonstrations utilisaient des définitions qui n'étaient pas encore définitives.

Depuis, cette méthode a été extrêmement utilisée. FRAENKEL et MOSTOWSKI ont montré dans les années vingt que l'axiome du choix n'était pas démontrable à partir des autres axiomes de la théorie des ensembles. Et, dans les années trente, GÖDEL a montré que sa négation ne l'était pas non plus — encore une fois ça n'est pas *le* théorème de GÖDEL, c'est un autre théorème que nous devons à GÖDEL. GÖDEL également montré que la négation de l'hypothèse du continu n'était pas démontrable, puis COHEN a montré que l'hypothèse du continu elle-même n'était pas démontrable [Coh63, Coh64].

Les modèles comme structures algébriques Bien entendu, la notion de modèle est familière à tous les mathématiciens, puisqu'un modèle est un ensemble muni d'opérations et de relations, vérifiant un certain nombre de propriétés. C'est ce qui s'appelle, ailleurs qu'en logique, une *structure algébrique*.

Cette notion de modèle établit un pont entre l'algèbre et la logique. Elle permet l'utilisation d'outils algébriques en logique : tout ce que nous connaissons sur les structures en général — les notions de sous-structure, de structure quotient,

de morphisme, etc. — peut être utilisé pour construire des modèles et donc obtenir des résultats d'indépendance.

Ce point de vue algébrique peut même se radicaliser : faire de la géométrie euclidienne aujourd'hui, ce n'est plus chercher des démonstrations qui utilisent les axiomes d'Euclide, mais étudier des structures, les espaces affines, dans lesquels ces axiomes sont valides. De même, faire de la géométrie hyperbolique, ce n'est peut être pas tant chercher des démonstrations dans une théorie axiomatique particulière, qu'étudier les structures, comme celles de Klein, dans lesquelles ces axiomes sont valides.

Parler de la démontrabilité sans parler des démonstrations Un point remarquable ici est que les théorèmes de correction et de complétude peuvent se formuler comme l'équivalence suivante : une proposition A est démontrable, c'est-à-dire il existe une démonstration π de A, si et seulement si pour tout modèle $\mathcal{M}$, A est valide dans $\mathcal{M}$.

$$(\exists \pi,\ \pi \text{ est une démonstration de } A) \ \Leftrightarrow\ (\forall \mathcal{M},\ A \text{ est valide dans } \mathcal{M}).$$

La notion de démonstration apparaît à gauche de l'équivalence, mais pas à droite, où il n'est question que de propositions et de structures algébriques.

Cette équivalence permet donc de caractériser exactement la notion de démontrabilité sans parler de la notion de démonstration. Nous pouvons alors imaginer le scénario suivant :

— nous définissons la notion de démonstration, nécessaire pour définir la notion de démontrabilité et formuler l'équivalence entre la démontrabilité et la validité dans tous les modèles,
— nous démontrons cette équivalence,
— une fois cette équivalence démontrée, nous pouvons oublier la notion de démonstration.

La notion de démonstration ne sert en effet plus à rien puisque, si nous voulons démontrer par exemple qu'une proposition n'est pas démontrable, même si nous ne connaissons pas la notion de démonstration, mais si nous faisons confiance à ceux qui ont démontré cette équivalence, il suffit de trouver un modèle dans lequel cette proposition n'est pas valide.

Cette situation peut sembler bizarre : pour être théoricien de la démonstration, il n'est pas nécessaire de savoir définir la notion de démonstration. Il suffit de savoir cela a été fait une fois, de faire confiance à ceux qui ont démontré cette équivalence et de l'utiliser. Mais, en fait, cette manière de faire n'est pas si rare en mathématiques. Par exemple, qui se souvient qu'un entier relatif est un ensemble de couples d'entiers naturels ? Qui se souvient qu'un nombre réel est un ensemble de suites de Cauchy ? Peut-être même certains d'entre-vous croient-ils c'est une coupure de Dedekind, mais ça ne nous empêche pas de parler ensemble des nombres réels. Et la situation est la même avec les notions de couple ou de polynôme formel.

C'est donc une pratique assez courante en mathématiques, dont on trouve une illustration ici, que de définir une notion, démontrer un théorème que nous

pouvons appeler « fondamental » qui suffit à caractériser complètement la notion, oublier la définition, et raisonner dans la belle abstraction.

Oui mais... Cependant ce programme n'est pas sans critiques. L'une d'elles est que nous obtenons quantité de résultats relatifs à la démontrabilité — telle proposition est démontrable, telle autre ne l'est pas, si telle proposition n'est pas démontrable alors telle autre non plus, etc. — mais que nous avons perdu tout ce que nous pouvions dire, par exemple, sur le contenu calculatoire ou la taille des démonstrations. Si nous voulons de tels résultats, nous ne pouvons pas nous contenter d'utiliser ces beaux outils algébriques.

Et cela mène à une autre branche de théorie de la démonstration, déviante, qui consiste, plutôt que goûter l'ivresse des cimes algébriques, à essayer de rester plus près du sol, à préférer la notion de démonstration elle-même, même si cette notion est beaucoup plus rugueuse que celle de structure algébrique.

Dans les démonstrations, il faut par exemple vérifier que quand nous avons utilisé une variable x ici, nous n'allons pas la réutiliser là, parce que cela pourrait créer une confusion de noms — problème que les informaticiens connaissent bien. Cela mène à se demander si la proposition « pour tout x, $x = x$ » est la même que « pour tout y, $y = y$ ». Ces questions syntaxiques, masquées par l'approche algébrique, reviennent au premier plan.

1.2 Les algorithmes

Pour illustrer cette seconde démarche, je vais tenter de re-démontrer le théorème d'indépendance 1.3, sans utiliser de modèles.

Des algorithmes pour transformer les démonstrations Pour cela, je vais me concentrer sur un type particulier d'algorithmes, qui transforment les démonstrations en des démonstrations de la même proposition. En répétant cet algorithme nous irons, pas à pas, d'une démonstration quelconque vers une démonstration *canonique* de la même proposition.

Pour illustrer ce qu'est une démonstration canonique, je vais prendre un exemple. Et pour cela, je vais commencer par présenter un tout petit peu plus en détail la notion de démonstration. Il va donc falloir que nous attaquions cette partie rugueuse de cette leçon, qui est de comprendre précisément la notion de démonstration.

Les démonstrations sont construites avec des règles appelées *règles de déduction*, écrites comme des fractions, avec en haut ce que nous avons déjà démontré, et en bas ce que cette petite étape de démonstration nous permet de déduire.

La troisième règle de la table 1, *élim* énonce que si nous avons déjà démontré les propositions $A \Rightarrow B$ et A, nous pouvons en déduire la proposition B.

Dans cette règle, apparaissent également les symboles Γ et $\vdash$, car j'ai fait le choix de présenter un type de démonstrations dans lequel on déduit, non des propositions à partir d'autres propositions, mais des propositions hypothétiques à partir d'autres propositions hypothétiques. Une proposition hypothétique $\Gamma \vdash A$

$$\frac{}{\Gamma, A \vdash A}\ \textit{axiome}$$

$$\frac{\Gamma, A \vdash B}{\Gamma \vdash A \Rightarrow B}\ \textit{intro}$$

$$\frac{\Gamma \vdash A \Rightarrow B \quad \Gamma \vdash A}{\Gamma \vdash B}\ \textit{élim}$$

TABLE 1 – Règles de déduction

est formée d'une proposition A à droite du symbole $\vdash$, qui se lit « thèse », et d'un ensemble de propositions Γ, appelées *axiomes*. Et démontrer $\Gamma \vdash A$, c'est démontrer A à partir des axiomes Γ. Une démonstration d'une proposition hypothétique $\vdash A$, dans laquelle l'ensemble d'axiomes est vide, est appelée une démonstration *absolue* ou *sans axiomes* de la proposition A. C'est la notion de démonstration que nous avons utilisée depuis le début de cette leçon.

La règle *élim* énonce donc que si nous avons déjà démontré les propositions hypothétiques $\Gamma \vdash A \Rightarrow B$ et $\Gamma \vdash A$, c'est-à-dire si nous nous avons déjà démontré les propositions $A \Rightarrow B$ et A sous les axiomes Γ, nous pouvons en déduire la proposition hypothétique $\Gamma \vdash B$, c'est-à-dire la proposition B, sous ces mêmes axiomes.

La règle *intro*, quant à elle, énonce que si nous avons démontré la proposition B sous les axiomes Γ et A, nous pouvons en déduire $A \Rightarrow B$ sous les axiomes Γ. C'est la célèbre formule que nous avons apprise au lycée : « Nous voulons montrer $A \Rightarrow B$, supposons A, démontrons B. » L'hypothèse A devient, le temps de cette démonstration, un nouvel axiome.

Enfin, la règle *axiome* permet d'utiliser les axiomes.

Ces trois règles — dont j'ai un tout petit peu simplifié le nom — font partie d'une vingtaine de règles qui permettent de construire les démonstrations. Nous pourrions passer une heure sur chacune d'elles, mais je vais essayer, dans cette leçon, de n'utiliser que ces trois là. La règle *intro* s'appelle une *règle d'introduction* parce que, quand nous la lisons de haut en bas, elle permet d'introduire un connecteur — ici une implication. Et la règle *élim* est une *règle d'élimination* parce que, quand nous la lisons de haut en bas, elle permet d'utiliser, et donc d'éliminer, un connecteur. Dans chacun des cas, il y a une seule proposition complexe : ou bien au dénominateur, auquel cas la règle explique comment construire une démonstration d'une proposition de cette forme, ou bien au numérateur, auquel cas la règle explique comment utiliser cette proposition.

Voici un exemple de démonstration de Q sous les axiomes $P \Rightarrow Q$ et P [1] :

$$\dfrac{\dfrac{\dfrac{\dfrac{}{P \Rightarrow Q, P, P \Rightarrow Q \vdash P \Rightarrow Q}\,\textit{axiome}\,[4] \quad \dfrac{}{P \Rightarrow Q, P, P \Rightarrow Q \vdash P}\,\textit{axiome}\,[5]}{P \Rightarrow Q, P, P \Rightarrow Q \vdash Q}\,\textit{élim}\,[3]}{P \Rightarrow Q, P \vdash (P \Rightarrow Q) \Rightarrow Q}\,\textit{intro}\,[2] \quad \dfrac{}{P \Rightarrow Q, P \vdash P \Rightarrow Q}\,\textit{axiome}\,[6]}{P \Rightarrow Q, P \vdash Q}\,\textit{élim}\,[1] \quad . \tag{1}$$

Pour le moment vous n'avez pas à juger du style de ma démonstration, vous avez juste à juger de sa correction. La dernière étape de la démonstration consiste, une fois que nous avons démontré $(P \Rightarrow Q) \Rightarrow Q$ et $P \Rightarrow Q$ sous les axiomes $P \Rightarrow Q$ et P, à appliquer la règle *élim* [1].

— Pour démontrer l'implication $(P \Rightarrow Q) \Rightarrow Q$ sous les axiomes $P \Rightarrow Q$ et P, il nous suffit de démontrer Q sous ces mêmes axiomes, augmentés de $P \Rightarrow Q$, puis d'appliquer la règle *intro* [2]. Pour cela, il suffit de démontrer $P \Rightarrow Q$ et P sous ce nouvel ensemble d'axiomes, puis d'appliquer la règle *élim* [3]. Dans les deux cas ce sont des axiomes, nous pouvons donc utiliser la règle *axiome* [4, 5].

— Enfin, démontrer $P \Rightarrow Q$ sous les axiomes $P \Rightarrow Q$ et P, est facile puisque c'est un axiome. La règle *axiome* permet de conclure [6].

Bien entendu, vous devez vous dire qu'il doit y a sans doute une démonstration plus directe, il n'est pas possible qu'une démonstration qui contient autant de détours soit la bonne. Effectivement, il y a une démonstration plus directe, comme nous allons le découvrir ensemble. Il y a même un algorithme qui transforme cette démonstration en la démonstration que vous avez peut-être en tête.

Mais avant cela, pourquoi peut-on dire que cette démonstration contient un détour ? Ce détour est formé par la séquence d'une règle d'introduction [2] et d'une règle d'élimination [1]. Que s'est-il passé ? Après l'élimination [3] nous avions démontré Q, c'est à peu près ce que nous voulions démontrer, tout partait bien. Mais nous avons utilisé une règle d'introduction [2] de manière à créer l'implication $(P \Rightarrow Q) \Rightarrow Q$, implication que nous avons tout de suite détruite avec une règle d'élimination [1] pour retrouver la proposition Q.

Vous pouvez imaginer une usine dans laquelle se trouve un atelier qui toute la journée fabrique des réveils, les met sur un chariot et les envoie dans un autre atelier, où ils sont démontés. Dans une usine normale, on achète des engrenages, on fabrique des réveils et on les vend. Mais c'est bien embêtant : d'abord il faut trouver des engrenages, ensuite il faut vendre les réveils et personne n'en veut. Alors, voici une manière beaucoup plus simple d'organiser cette usine : vous avez deux ateliers, un qui fabrique des réveils, l'autre qui les démonte, les réveils vont dans un sens, les engrenages vont dans l'autre, et tout le monde est content.

C'est ce que nous avons a fait ici. Nous avons un atelier qui fabrique des implications : la règle *intro* et, à peine l'implication fabriquée, nous l'envoyons vers l'atelier qui démonte les implications : la règle *élim*. Peut-être y a-t-il une organisation plus rationnelle de cette usine.

1. Les nombres entre crochets ne servent qu'à identifier les pas de la démonstration. (N.d.r.)

De manière générale De manière plus générale, quand nous avons une démonstration dans laquelle une règle d'introduction est suivie d'une règle d'élimination, nous sommes dans la situation suivante :

$$\dfrac{\dfrac{\dfrac{\pi}{\Gamma, A \vdash B}}{\Gamma \vdash A \Rightarrow B}\,\mathit{intro} \qquad \dfrac{\rho}{\Gamma \vdash A}}{\Gamma \vdash B}\,\mathit{élim}\,. \tag{2}$$

Nous avons une démonstration π de la proposition B sous les axiomes Γ, A et nous en déduisons $A \Rightarrow B$ sous les axiomes Γ. Par ailleurs, nous avons une démonstration ρ de la proposition A sous ces mêmes axiomes Γ. Puis nous combinons ces démonstrations, avec la règle *élim*, en une démonstration de la proposition B, toujours sous l'ensemble d'axiomes Γ. Une manière de simplifier cette démonstration consiste à remarquer que nous voulons démontrer B et que nous avons déjà une démonstration de B : π. Mais cette démonstration a un petit défaut : elle utilise l'axiome A, c'est-à-dire, quelque-part dans les feuilles de l'arbre que constitue la démonstration π peuvent se trouver des règles *axiome* portant sur la proposition A. C'est le moment de nous rappeler que nous savons démontrer la proposition A et que, au lieu d'utiliser le fait que c'est un axiome, nous pouvons la redémontrer.

La démonstration (2) peut donc se simplifier en une démonstration obtenue en remplaçant dans π toutes les utilisations de l'axiome A par la démonstration ρ de A.

Rappelons-nous la démonstration (1). Que se passe-t-il si nous substituons l'axiome [6] aux utilisations de l'axiome $P \Rightarrow Q$ dans la démonstration conclue par l'introduction [2] ? Nous obtenons cette démonstration :

$$\dfrac{\dfrac{}{P \Rightarrow Q, P \vdash P \Rightarrow Q}\,\mathit{axiome} \qquad \dfrac{}{P \Rightarrow Q, P \vdash P}\,\mathit{axiome}}{P \Rightarrow Q, P \vdash Q}\,\mathit{élim}\quad ,$$

qui est peut-être celle à laquelle vous avez pensé tout de suite.

Cela me permet d'introduire un peu de vocabulaire. La séquence formée d'une introduction immédiatement suivie d'une élimination s'appelle une *coupure*. Et vous avez compris qu'une démonstration *canonique*, est une démonstration qui ne contient pas de coupures.

Le théorème d'élimination des coupures Un théorème, dû à Gentzen [Gen35, Gen64], affirme que si une proposition hypothétique a une démonstration, alors elle a une démonstration canonique.

Théorème 1.4 (élimination des coupures) *Si une proposition hypothétique a une démonstration, alors elle a une démonstration canonique.*

Ce théorème peut se démontrer ainsi : comme nous l'avons vu, toute démonstration, si elle contient des coupures, se transforme en une démonstration qui contient « moins » de coupures. On peut répéter cette opération jusqu'à arriver

à une démonstration qui ne contient pas de coupures du tout, c'est-à-dire une démonstration canonique.

La difficulté n'est pas d'éliminer une coupure, nous avons vu comment le faire dans le cas général de la démonstration (2) : partant de la démonstration π, il suffit de repérer les utilisations de l'axiome A et des les remplacer par la démonstration ρ. La difficulté consiste à montrer que ce processus *termine*, c'est-à-dire qu'en éliminant une coupure, puis une deuxième, puis une troisième, etc., nous allons un jour arriver à une démonstration canonique. Pourquoi ? Parce qu'éliminer une coupure peut créer d'autres coupures. Au moment où nous réorganisons la démonstration, il se peut qu'une règle *intro* et une règle *élim* qui n'avaient jamais entendu parler l'une de l'autre se rencontrent. C'est typiquement ce qu'il se passe quand la démonstration ρ de A se termine par une règle d'introduction et l'utilisation de l'axiome A est suivie par une règle d'élimination. Ces deux règles, qui se trouvaient dans des branches différentes de la démonstration, forment désormais une coupure.

Ce sont donc uniquement des questions de terminaison qui se posent ici, et non des questions de définition du processus d'élimination progressive des coupures.

C'est bien d'éliminer les coupures dans les démonstrations, mais quel rapport avec le théorème d'indépendance 1.3, selon lequel une proposition atomique n'est pas démontrable ? Pour faire apparaître ce lien, nous avons encore besoin d'un petit lemme, selon lequel une démonstration canonique et sans axiomes se termine toujours par une règle d'introduction.

Lemme 1.1 *Une démonstration σ d'une proposition B, canonique et sans axiomes, c'est-à-dire une démonstration canonique de la proposition hypothétique $\vdash B$, se termine par une règle d'introduction.*

La démonstration du lemme procède par récurrence sur la structure arborescente de la démonstration σ. Puisque nous n'avons que trois règles, il n'y a que trois possibilités — bien entendu, la preuve se généralise si nous avons davantage de règles, mais pas n'importe quelles règles, comme nous le verrons en discutant la règle du tiers-exclu — : σ se termine ou bien par une règle *axiome*, ou bien par une règle *intro*, ou bien par une règle une règle *élim*.

— Si σ se termine par une règle *intro*, le lemme est démontré.
— σ ne peut pas se terminer par une règle *axiome* car l'ensemble d'axiomes de sa conclusion est vide.
— Il reste à démontrer que σ ne peut pas se terminer par une règle *élim*. Supposons le contraire. Dans ce cas σ est de la forme :

$$\dfrac{\dfrac{\pi}{\vdash A \Rightarrow B} \quad \dfrac{\rho}{\vdash A}}{\vdash B}\ \textit{élim}.$$

Et π est une démonstration canonique de la proposition $A \Rightarrow B$ sous un ensemble vide d'axiomes. Nous pouvons donc appliquer l'hypothèse de

récurrence : π se termine par une règle d'introduction et σ contient une coupure de la forme :

$$\dfrac{\dfrac{\dfrac{\pi'}{A \vdash B}}{\vdash A \Rightarrow B}\,\mathit{intro} \quad \dfrac{\rho}{\vdash A}}{\vdash B}\,\mathit{élim},$$

ce que nous avons exclu par hypothèse.

Une fois ce lemme démontré, nous pouvons démontrer le théorème d'indépendance : une proposition atomique n'est pas démontrable sans axiomes. Supposons qu'une proposition atomique P soit telle que la proposition hypothétique $\vdash P$ ait une démonstration π. D'après le théorème 1.4 d'élimination des coupures, $\vdash P$ a une démonstration canonique et d'après le lemme 1.1, cette démonstration se termine par une règle d'introduction. Or, la conclusion d'une telle règle est une implication, alors que P est atomique.

Au terme de ce long parcours nous aboutissons au même résultat que par la méthode algébrique, mais par un chemin tout à fait différent.

Bien entendu, le théorème d'indépendance est trivial, ce n'est pas le théorème en lui-même qui nous importe, mais le fait qu'il puisse se démontrer en utilisant deux méthodes, l'une algébrique l'autre algorithmique, qui ne semble avoir rien de commun — c'est, bien sûr, le point que je vais discuter.

L'élimination des coupures

Un meilleur exemple Un meilleur exemple que le théorème d'indépendance est le théorème d'élimination des coupures lui-même. Ce théorème affirme que si une proposition hypothétique a une démonstration, alors elle a une démonstration canonique. L'énoncé ne dit pas comment trouver la démonstration canonique, ni que le processus d'élimination progressive des coupures termine nécessairement. Et ce théorème a deux démonstrations. La première utilise l'algorithme de transformation des démonstrations que nous avons vu, mais dont nous devons encore montrer la terminaison, et la seconde, que je vais présenter tout à l'heure, repose sur des techniques de construction de modèle. Y compris jusque dans ce théorème plus ou moins fondamental de la théorie de la démonstration, deux types de méthodes permettent d'arriver au même résultat.

Le théorème d'indépendance n'est donc pas un cas isolé. Cette situation semble typique : à chaque fois que nous avons un théorème à démontrer, nous pouvons essayer de l'attaquer par des outils algébriques ou par des outils algorithmiques. Et, parfois, les deux méthodes fonctionnent.

Pourquoi un meilleur exemple ? Pourquoi ce théorème est-il un meilleur exemple que le précédent ? Pour deux raisons. La première est que ce théorème a de nombreux corollaires, ce qui fait que nous pouvons l'appeler *théorème fondamental de la théorie de la démonstration*. Quels sont ces corollaires ?

Non-démontrabilité Certains de ces corollaires sont des résultats de non-démontrabilité. Nous venons de voir l'exemple, un peu trivial, des propositions atomiques.

Complétude de méthodes de démonstration automatique Ce qui personnellement m'intéresse le plus est que ce théorème permet de démontrer que des méthodes de démonstration automatique sont complètes. Qu'est-ce que cela veut dire ? Quand nous écrivions des programmes informatiques qui ont comme but de trouver des démonstrations, si nous cherchons des démonstrations quelconques, c'est-à-dire des démonstrations qui peuvent faire des détours par n'importe quoi, nous nous mettons dans une situation difficile. Supposons, par exemple, que nous voulions démontrer que les médiatrices d'un triangle concourent, c'est le genre de théorème que ce type de système permet de démontrer. Si nous nous disons : « Une bonne idée, serait de démontrer d'une part le théorème de Fermat, et d'autre part que le théorème de Fermat implique la concourance des médiatrices. », nous partons plutôt mal [2]. Nous devrions plutôt essayer de chercher une démonstration canonique, dans laquelle nous évitons le détour par le théorème de Fermat, qui peut certainement s'éliminer. Or, la complétude de ce genre de méthodes qui ne cherchent que des démonstrations canoniques repose sur le théorème d'élimination des coupures.

Propriété de la disjonction et du témoin Je vais revenir sur la propriété de la disjonction et du témoin, mais je vous voudrais mentionner, dès maintenant que c'est cette dernière propriété qui permet d'extraire des algorithmes à partir de démonstrations constructives [3]. C'est un des buts de la théorie de la démonstration que j'ai mentionnés au début de la leçon.

La première raison de l'importance du théorème d'élimination des coupures est donc qu'il a de nombreux corollaires : c'est un résultat fondamental. La deuxième est que ce théorème est le prototype de toute une famille de théorèmes : *les* théorèmes d'élimination des coupures. Et ici, nous pouvons à la fois nous réjouir et nous désoler. Nous pouvons nous réjouir du fait que nous ayons une méthode qui a beaucoup d'applications, un théorème qui a beaucoup de généralisations. Mais quand nous avons dix théorèmes qui se ressemblent et se démontrent à peu près de la même manière, plutôt que de nous réjouir, nous avons en général tendance à nous désoler : à nous dire qu'il nous manque un théorème général. Nous aimerions bien que tous ces résultats d'élimination des coupures soient les conséquences d'un théorème plus général.

C'est une chose que les étudiants remarquent dès qu'ils commencent à faire de la théorie de la démonstration : nous leur demandons de venir à la fac tous

2. Rires dans l'assistance. (N.d.r.)

3. La propriété de la disjonction affirme que d'une démonstration constructive de $\vdash A$ *ou* B — sans axiomes donc — nous pouvons extraire une démonstration de $\vdash A$ ou une démonstration de $\vdash B$. La propriété du témoin affirme que d'une démonstration constructive de $\vdash \exists x\, P(x)$ — sans axiomes donc — nous pouvons extraire une un terme t — le témoin — et une démonstration de $\vdash P(t)$. (N.d.r.)

les jours, et tous les jours nous leur démontrons un théorème d'élimination des coupures, et tous les jours il ressemble à celui de la veille si ce n'est qu'il est un peu plus compliqué. Et certains se demandent avec raison, (1) si cela va s'arrêter un jour ou si nous allons inventer tous les jours un nouveau théorème d'élimination des coupures, et (2) si nous ne pourrions pas, en septembre, démontrer *un* théorème général et en déduire ensuite tous ces théorèmes comme des corollaires. C'est une question qui m'a longtemps occupé et je vais essayer de vous donner quelques éléments de réponse.

Cette leçon J'arrive à la fin de mon introduction. Dans cette leçon, je vais essayer de vous présenter un théorème général d'élimination des coupures qui a comme corollaires quantité de théorèmes d'élimination des coupures que nous connaissions auparavant. Surtout, je vais essayer de vous montrer que démontrer ce théorème a mené à une convergence des méthodes algébriques et des méthodes algorithmiques. Aujourd'hui, nous avons plutôt tendance à penser que ces deux types de méthodes sont juste les deux faces d'une même pièce. Ce sont deux manières de dire les choses qui, même si elles paraissent hétérogènes à première vue, reposent finalement sur les mêmes mécanismes.

Cette convergence ne s'est pas faite en un jour et j'ai isolé, de manière peut-être un peu arbitraire, cinq étapes de cette convergence. Je voudrais essayer, à la fin de la leçon, de détailler ces cinq étapes, et vous montrer comment, petit à petit, les choses se sont réorganisées de manière à ce que nous pensions aujourd'hui que ces méthodes algébriques et ces méthodes algorithmiques sont une seule et même chose.

2 Le problème des axiomes

Je vais tout d'abord m'intéresser à un type de questions d'Histoire des sciences : pourquoi n'a-t-on pas trouvé ça plus tôt ? Pourquoi Aristote n'a-t-il pas découvert la loi de Newton ? Pourquoi Ptolémée n'a-t-il pas découvert l'héliocentrisme ? Un premier type de réponse, simple, est que l'on n'avait pas d'outils techniques suffisants. Pourquoi n'a-t-on pas découvert de planète extra-solaire avant d'avoir des télescopes puissants ? Parce qu'il faut des télescopes puissants pour découvrir de telles planètes. Un autre type de réponse est que l'on était bloqué par des *a priori*, des croyances, qui laissaient penser que c'était complètement impossible. Je vais montrer que nous sommes ici un peu dans les deux cas.

Le théorème que je vais vous présenter est un théorème général d'élimination des coupures. Il affirme que toutes les théories qui sont super-cohérentes ont la propriété d'élimination des coupures. Pourquoi n'a-t-on pas trouvé cette condition suffisante — vous verrez qu'elle est relativement simple — plus tôt ? Qu'est-ce qui bloquait, qu'est-ce qui nous empêchait de la voir ? La réponse est ce que j'appelle *le problème des axiomes*. Nous étions parti d'un *a priori* selon lequel une théorie est un ensemble d'axiomes : la théorie des ensembles est un ensemble d'axiomes, l'arithmétique est un ensemble d'axiomes, la géométrie est

un ensemble d'axiomes, etc. C'est un principe qui a bien fonctionné puisque, d'Euclide à Zermelo, on a posé des axiomes et on a bien fait avancer les mathématiques ainsi. Mais je vais un peu critiquer, comme vous vous en doutez peut-être, la notion d'axiome.

Pour formuler un théorème général d'élimination des coupures, il fallait donner une définition générale de la notion de coupure. Et l'idée qu'une théorie est un ensemble d'axiomes nous a empêché de donner une telle définition. Définir une notion de coupure assez générale a donc demandé de modifier d'abord la notion de théorie.

2.1 La propriété de la disjonction

Pour le moment, mon discours est la fois très abstrait et très dogmatique. Je vais essayer de l'illustrer par un exemple.

Revenons à la propriété de la disjonction des démonstrations constructives. Selon la propriété de la disjonction, si une proposition A *ou* B a une démonstration constructive et sans axiomes — et nous allons discuter de cette hypothèse, elle est importante — alors la proposition A a une démonstration constructive et sans axiomes ou la proposition B a une démonstration constructive et sans axiomes. La première fois que l'on voit cette propriété, on se dit : « Oui, bien entendu, A *ou* B est démontrable, c'est-à-dire que A *ou* B est vrai, donc A est vrai ou B est vrai, donc A est démontrable ou B est démontrable. » Mais je vais vous donner un contre-exemple.

Voici une pièce d'un euro [4]. Si j'ouvre la fenêtre et jette la pièce, elle va tomber ou bien du coté pile ou bien du coté face [5]. Est-elle tombée du coté pile ou du coté face [6] ? Personne ne le sait et vous pouvez descendre pour voir de quel coté elle est tombée, mais je ne suis pas sûr que vous la retrouviez. Imaginez que j'aie fait cette opération au-dessus d'une fosse qui se trouve dans la mer du Japon, profonde de douze mille mètres. Là, il faut utiliser un sous-marin pour aller voir si la pièce est tombée du coté pile ou du coté face et, à nouveau, il n'est pas certain que nous retrouvions la pièce au fond de l'océan. Nous sommes donc dans une situation dans laquelle nous avons, disons, une démonstration de la proposition « la pièce est tombée du coté pile ou la pièce est tombée du coté face », mais nous n'avons aucune démonstration ni de « la pièce est tombée du coté pile », ni de « la pièce est tombée du coté face ».

Comment pouvons nous démontrer que la pièce est tombée du coté pile ou du coté face, sans démontrer ni qu'elle est tombée du coté pile, ni qu'elle est tombée du coté face ? Là, nous avons besoin d'utiliser une règle de déduction qui est tout à fait similaire aux trois règles *intro*, *élim*, *axiome* que j'ai décrites tout à l'heure : *le tiers-exclu*. Cette règle nous permet de démontrer la proposition : A *ou non* A, sans rien faire. Typiquement, elle nous permet de démontrer la proposition R *ou non* R, où R est l'hypothèse de Riemann, que nous ayons à

4. Gilles Dowek nous montre une pièce d'un euro. (N.d.r.)
5. Gilles Dowek ouvre une fenêtre de la salle de conférence et jette la pièce. (N.d.r.)
6. Rires dans l'assistance. (N.d.r.)

démontrer ni l'hypothèse de Riemann, ni sa négation. La règle du tiers-exclu invalide donc trivialement la propriété de la disjonction.

Non seulement la propriété de la disjonction n'est pas triviale, mais elle n'est pas toujours vraie. Et c'est là que l'hypothèse « démonstration constructive » est importante. Une démonstration *constructive* est une démonstration qui n'utilise pas la règle du tiers-exclu. Et, comme nous allons le voir, pour une démonstration constructive, la propriété de la disjonction est vraie. Le tiers-exclu est la seule règle de déduction, parmi celles que j'ai mentionnées, qui invalide la propriété de la disjonction.

Bien entendu, je ne vais pas discuter des questions de la forme « il faut », je ne vais pas vous dire : « Il ne faut pas utiliser le tiers-exclu » ou : « Il faut utiliser le tiers-exclu. » Je dit juste que, parmi toutes les démonstrations que nous pouvons construire, il y en a qui utilisent le tiers-exclu et d'autres non, de la même manière que, parmi tous les nombres entiers, il y en a qui sont pairs et d'autres non. Les nombres pairs ont certaines propriétés, et les démonstrations qui n'utilisent pas le tiers-exclu ont certaines propriétés, par exemple celle de la disjonction.

Comment démontre-t-on la propriété de la disjonction ? À nouveau, en utilisant le théorème d'élimination des coupures : si la proposition A *ou* B a une démonstration constructive et sans axiomes, elle a aussi une démonstration canonique, constructive et sans axiomes. Et, comme cette démonstration est canonique, constructive et sans axiomes, elle se termine par une règle d'introduction.

Il y a deux règles d'introduction de la disjonction *ou* :

$$\frac{\Gamma \vdash A}{\Gamma \vdash A \textit{ ou } B} \quad \text{et} \quad \frac{\Gamma \vdash B}{\Gamma \vdash A \textit{ ou } B}.$$

Selon la première, si nous avons démontré A sous les axiomes Γ, nous pouvons en déduire A *ou* B sous ces mêmes axiomes. Selon la seconde, si nous avons démontré B nous pouvons en déduire A *ou* B. Une démonstration canonique, constructive et sans axiomes de $\vdash A$ *ou* B se termine ou bien par la première règle auquel cas nous avons une démonstration de $\vdash A$, ou bien par la seconde auquel cas nous avons une démonstration de $\vdash B$.

Cette argumentation suppose que la démonstration de départ n'utilise pas le tiers-exclu, car le lemme 1.1 ne se généralise pas si nous ajoutons cette règle. Mais ce n'est pas le tiers-exclu qui me pose un problème ici, c'est l'hypothèse selon laquelle nous partons d'une démonstration sans axiomes.

Si nous ajoutons des axiomes Si nous ajoutons maintenant des axiomes, par exemple les axiomes de la géométrie, de l'arithmétique, de la théorie des types, ou de la théorie des ensembles, le lemme 1.1 que nous avons démontré ensemble tout à l'heure, selon lequel une démonstration canonique se termine par une règle d'introduction n'est plus vrai, parce que la démonstration peut aussi se terminer par une règle *axiome*. La démonstration ne se termine donc plus nécessairement par une règle d'introduction et il n'est plus possible de

démontrer la propriété de la disjonction comme précédemment. Cette propriété n'est d'ailleurs plus toujours vraie : si nous prenons l'axiome P *ou* Q, par exemple, alors nous pouvons démontrer P *ou* Q avec la règle *axiome*, sans, pour autant, être capable de démontrer P ou de démontrer Q. Certains axiomes invalident donc la propriété de la disjonction.

Néanmoins, les démonstrations constructives dans certaines théories, comme l'arithmétique, la théorie des types ou certaines formulations de la théorie des ensembles, ont la propriété de la disjonction. Mais le théorème d'élimination des coupures ne nous aide plus à le démontrer, puisque même si nous éliminons les coupures, du fait qu'il y a des axiomes, nous n'avons aucune raison de penser qu'une démonstration canonique se termine par une règle d'introduction.

Le*s* théorème*s* d'élimination des coupures C'est pourquoi, pour un grand nombre de théories particulières, comme l'arithmétique ou la théorie des types, on a inventé une notion particulière de coupure et démontré un théorème particulier d'élimination des coupures. Et nous pouvons affirmer avoir démontré un théorème d'élimination des coupures quand nous sommes capables de dire qu'une démonstration canonique et constructive, dans telle théorie particulière, se termine par une règle d'introduction. Nous retrouvons alors les propriétés qui nous intéressaient auparavant : la propriété de la disjonction, la propriété du témoin, la complétude de méthodes de démonstration automatique, etc. C'est ce qui explique qu'à chaque fois que nous avons une nouvelle théorie, nous avons un nouveau théorème d'élimination des coupures pour cette théorie. Et comme nous pouvons inventer tous les jours de nouveaux axiomes et de nouvelles théories, nous pouvons tous les jours essayer de démontrer de nouveaux théorèmes d'élimination des coupures...

Cependant, la chose la plus dérangeante ici n'est pas que nous ayons un théorème d'élimination des coupures pour chaque théorie : c'est que nous ayons une notion de coupure différente pour chaque théorie. Par exemple, pour l'arithmétique, il y a une notion de coupure liée à l'un des axiomes de l'arithmétique : l'axiome de récurrence. Nous avons démontré que 0 appartient à un ensemble, nous avons démontré que si n appartient à cet ensemble alors $n + 1$ aussi, et nous voulons démontrer que 1000 appartient à cet ensemble. Nous avons deux démonstrations possibles. La première est d'utiliser l'axiome de récurrence, la seconde, beaucoup plus simple, consiste à montrer que puisque 0 appartient à l'ensemble, 1 aussi, donc 2 aussi, donc 3 aussi, ... , donc 1 000 aussi. Et l'algorithme d'élimination des coupures transforme ici la première démonstration en la seconde. C'est un processus complètement nouveau, qui est propre à l'arithmétique et qui ne nous dit rien ce que devrait être une coupure en géométrie, en théorie des types ou en théorie des ensembles.

Cette situation, le fait que nous ayons une notion de coupure distincte pour chaque théorie, a été un obstacle au développement d'une théorie générale pour l'élimination des coupures. Des années soixante aux années quatre-vingt-dix, on a démontré un grand nombre de théorèmes particuliers d'élimination des coupures : on prenait une théorie, on expliquait ce qu'était une coupure pour cette théorie

et on démontrait un théorème d'élimination, souvent très intéressant, mais qui laissait le désir d'aller au-delà et d'avoir une notion générale de coupure.

2.2 La Déduction modulo

Aujourd'hui personne n'a une telle notion générale de coupure, c'est-à-dire personne ne sait dire : « Prenons un ensemble d'axiomes quelconque, voici ce qu'est une coupure pour cet ensemble d'axiomes. » Mais Claude Kirchner, Thérèse Hardin et moi avons proposé il y a une dizaine d'années un système qui est une solution partielle à ce problème. Ce système s'appelle *la Déduction modulo* [DHK03]. Je vais vous présenter en deux mots ce qu'est la Déduction modulo, d'abord par un slogan puis un exemple.

Le slogan affirme que les axiomes doivent être remplacés par des règles de calcul. Et nous sommes ici dans la situation du télescope : nous ne nous sommes pas rendu compte de cette possibilité plus tôt parce que nous n'avions pas de notion de règle de calcul suffisamment développée. Il n'y avait pas suffisamment d'informaticiens pour développer une notion de règle de calcul qui aurait permis aux théoriciens de la démonstration de l'utiliser ensuite. Nous pouvons donc dire ici que nous n'avons pas eu cette idée plus tôt parce que nous n'avions pas la bonne notion de règle de calcul : la notion de règle de réécriture.

L'exemple, maintenant. Vous savez que le nombre e est défini comme la somme de la série $\sum_k \frac{1}{k\,!}$. Mais que signifie la définition

$$e = \sum_k \frac{1}{k\,!} \tag{3}$$

? Nous avons deux manières de répondre à cette question.

Nous pouvons dire : « À l'origine, en plus de tous les axiomes, disons de la théorie des ensembles, nous avons posé en axiome l'égalité (3). Et à chaque fois que nous voulons remplacer e par le corps de sa définition, ou l'inverse, nous devons utiliser cet axiome. C'est une manière de voir les définitions : ce sont des axiomes. Ajouter un tel axiome ne permet pas de démontrer plus de choses : tout ce que nous pouvons démontrer après, nous pouvions déjà le démontrer avant. Mais nous pouvons mieux l'exprimer puisque nous avons des formulations plus concises.

Il y a une autre manière de voir les définitions, qui est de mettre des lunettes spéciales, dont les verres, quand y arrive le symbole e, font apparaître le terme $\sum_k \frac{1}{k\,!}$.

Bien sûr, il faut avoir le côté un peu pointilleux d'un informaticien pour se rendre compte que ces deux approches sont différentes. Mais elles sont très différentes. Dans un cas, passer de la proposition « e est irrationnel » à « $\sum_k \frac{1}{k\,!}$ est irrationnel » demande d'utiliser un axiome, une règle de déduction, remplacer ceci par cela, etc. Dans l'autre cas, la proposition « e est irrationnel » *est* la proposition « $\sum_k \frac{1}{k\,!}$ est irrationnel ».

La Déduction modulo consiste à dire que la définition « $e = \sum_k \frac{1}{k\,!}$ » n'est pas un axiome — vous avez compris que je n'aime pas trop les axiomes — mais

une règle de calcul, qui transforme le symbole e en le terme $\sum_k \frac{1}{k\,!}$. Les règles qui transforment un symbole défini en le corps de sa définition sont les plus simples, et la notion de règle de calcul ne se limite bien entendu pas à ce cas : d'autres règles permettent, par exemple, de faire des additions, des multiplications, etc. et remplacent d'autres axiomes. Il est même surprenant *a posteriori* de se dire qu'il y a eu des mathématiciens géniaux, comme Peano à la fin du XIXe siècle, pour penser qu'un axiome comme

$$\forall x\,(x + 0 = x) \tag{4}$$

était nécessaire. Avant Peano, on effectuait l'addition $x + 0$ et on obtenait x. Car avant d'avoir posé cet axiome, on savait déjà effectuer des additions.

La Déduction modulo était donc partie de cette idée de supprimer les axiomes — aussi bien l'axiome (3) que l'axiome (4) — et de les remplacer par des règles de calcul.

Les règles de calcul sont utilisées d'une manière tout à fait différente des axiomes : au cours d'une démonstration, nous pouvons nous arrêter de raisonner, effectuer un calcul — par exemple remplacer e par $\sum_k \frac{1}{k\,!}$, ou remplacer 3×7 par 21 — dans la proposition que nous sommes en train de démontrer et, quand nous avons fini de calculer, reprendre le raisonnement. La déduction est donc effectué modulo les règles de calcul.

Au début, nous pensions que nous ne pourrions pas remplacer beaucoup d'axiomes par des règles de calcul. Par exemple, nous ne voyions pas comment remplacer par une règle de calcul l'axiome de l'arithmétique selon lequel 0 n'est le successeur d'aucun nombre.

$$\forall x\ (0 \neq S(x)).$$

Nous n'arrivions pas à trouver de règle de calcul qui transformerait 0 ou $S(x)$ en quoi que soit, quand nous nous sommes rendu compte que ce n'était pas 0 ou $S(x)$ qu'il fallait récrire, mais la proposition elle-même. Une solution consiste à récrire « $0 = S(x)$ » en faux. C'est-à-dire :

$$0 = S(x) \longrightarrow \bot.$$

Une autre solution consiste à introduire un symbole de prédicat Null, et des règles de calcul qui transforment $\textsc{Null}(0)$ en vrai, et $\textsc{Null}(S(x))$ en faux. C'est-à-dire :

$$\begin{aligned} \textsc{Null}(0) &\longrightarrow \top, \\ \textsc{Null}(S(x)) &\longrightarrow \bot. \end{aligned}$$

Mais nous pouvons aller plus loin : tous les axiomes de l'arithmétique peuvent se remplacer par des règles de calcul, tous les axiomes de la théorie des types peuvent se remplacer par des règles de calcul et tous les axiomes de certaines formulations de la théorie des ensembles peuvent se remplacer par des règles de calcul. Ce dernier résultat est un travail commun avec Alexandre Miquel

[DM07]. Il ne concerne que certaines formulations de la théorie des ensembles. Nous ne savons, par exemple, pas quoi faire de l'axiome du choix. Mais nous savons quoi faire de l'axiome d'extensionnalité, alors que c'est un axiome qui n'avait pas l'air algorithmique *a priori*. Pendant longtemps, quand je faisais un exposé, je donnais l'extensionalité comme exemple d'axiome que nous ne savions pas transformer en une règle de calcul. Puis Alexandre a compris comment faire.

En cela, la Déduction modulo est une solution partielle : nous ne savons pas quantifier les théories exprimables uniquement avec des règles de calcul. Mais il commence à y avoir des théorèmes. En particulier, Guillaume Burel a donné une méthode plus ou moins automatique pour transformer les axiomes en règles de calcul. Nous n'en sommes donc plus à nous demander individuellement, comment transformer telle ou telle théorie, mais nous nous demandons s'il y a des méthodes qui prennent des axiomes, tournent une espèce de moulinette et, à la sortie, comme dans les abattoirs de Chicago, donnent des règles de calcul à la place des axiomes. Solution partielle donc, mais dont nous commençons à entrevoir la généralité.

Pour toutes les théories exprimées uniquement avec des règles de calcul, sans axiomes donc, nous pouvons définir une notion uniforme de coupure. Cette notion est proche de la notion que nous avons définie tout à l'heure : une coupure est la séquence formée d'une règle d'introduction suivie d'une règle d'élimination, à ceci près que les règles de déduction sont désormais appliquées modulo les règles de calcul.

Pour toutes les théories dans lesquelles les coupures peuvent être éliminées, nous retrouvons exactement le même argument que précédemment : comme nous n'avons pas d'axiomes, une démonstration canonique se termine par une règle d'introduction. Nous retrouvons alors la propriété de la disjonction, la propriété du témoin, la complétude de méthodes de démonstration automatique, etc.

Une notion de coupure indépendante des théories En revanche, toutes les théories n'ont pas la propriété d'élimination des coupures. Par exemple, la théorie définie par la règle

$$P \longrightarrow Q \Rightarrow P, \tag{5}$$

a la propriété d'élimination des coupures — à chaque fois que nous avons une démonstration nous avons aussi une démonstration canonique —, mais pas celle définie par la règle

$$P \longrightarrow P \Rightarrow Q. \tag{6}$$

Il est possible d'exprimer tous les axiomes de l'arithmétique, de la théorie des types, ou de la théorie des ensembles comme des règles de calcul et, dans ces trois cas, nous avons la propriété d'élimination des coupures. Mais plus que de savoir si la théorie définie par (5) ou celle définie par (6) a la propriété d'élimination des coupures, ce qui importe ici c'est que la question : « La théorie $\mathcal{R}$ — où $\mathcal{R}$ est, non un ensemble d'axiomes, mais un ensemble de règles de calcul — a-t-elle la propriété d'élimination des coupures ? » est désormais une question bien posée,

même s'il est parfois difficile d'y répondre. Quand les théories étaient définies comme des ensembles d'axiomes, la question : « Telle ou telle théorie a-t-elle la propriété d'élimination des coupures ? » n'était pas bien posée, parce que nous devions d'abord nous demander ce qu'était une coupure dans cette théorie, et il n'y avait pas de réponse uniforme.

Maintenant, une fois que nous avons transformé une théorie en un ensemble de règles de calcul $\mathcal{R}$, la question : « La théorie $\mathcal{R}$ a-t-elle la propriété d'élimination des coupures ? » est bien posée. Nous pouvons alors commencer à nous demander quelles sont les théories qui ont la propriété d'élimination des coupures et quelles sont celles qui n'ont pas cette propriété.

3 L'élimination des coupures en utilisant des modèles

Je vous avais promis de montrer comment démontrer le théorème d'élimination des coupures par une méthode algébrique d'une part, et par une méthode algorithmique d'autre part. Je présenterai ensuite une généralisation de ce théorème à la Déduction modulo et j'essaierai de montrer comment démontrer ce théorème a mené à une convergence des méthodes algébriques et des méthodes algorithmiques.

3.1 La correction et la complétude

Revenons aux théorèmes 1.1 et 1.2 de correction et de complétude. La correction affirme que si une proposition A est démontrable, alors pour tout modèle $\mathcal{M}$, A est valide dans $\mathcal{M}$. Cet énoncé vaut en fait pour toute proposition A. Nous ne l'avions pas précisé au début de la leçon mais cela va avoir son importance. Nous formulons donc la correction de la manière suivante :

Pour tout A, si A est dém. alors (pour tout $\mathcal{M}$, A est valide dans $\mathcal{M}$).

La complétude, elle aussi valable pour toute proposition A, est formulée réciproquement :

Pour tout A, si (pour tout $\mathcal{M}$, A est valide dans $\mathcal{M}$) alors A est dém.

Les parenthèses sont importantes ici : le quantificateur universel « pour tout » est à gauche de l'implication. Vous savez qu'un « pour tout » à gauche d'une implication équivaut à un « il existe » à l'extérieur [7].

Nous reformulons donc la complétude en :

Pour tout A, il existe $\mathcal{M}$ tel que (si A est valide dans $\mathcal{M}$ alors A est dém.).

Le modèle $\mathcal{M}$ est le pire que nous puissions imaginer, le plus opposé à A. Si la proposition A est valide même dans ce modèle, elle est valide dans tous les

7. En logique classique, $(\forall x\, P(x)) \Rightarrow Q$ équivaut à $\exists x\, (P(x) \Rightarrow Q)$. (N.d.r.)

modèles, et elle est donc démontrable. Bien sûr, l'équivalence des ces formulations de la complétude repose sur le tiers-exclu. Cette équivalence n'est pas elle-même constructive mais cela n'a pas d'importance ici.

Cette reformulation de la complétude, met en évidence la succession d'un « pour tout » et d'un « il existe ». Et dans une leçon de mathématiques, quand nous rencontrons une telle alternance, il est naturel de nous demander si nous pouvons permuter ces quantificateurs.

Complétude uniforme ? Cette question est formulée ici de la manière suivante : existe-t-il un modèle $\mathcal{M}$ tel que

pour tout A (si A est valide dans $\mathcal{M}$ alors A est démontrable) ?

Autrement dit, existe-t-il un modèle $\mathcal{M}$ tel que la validité dans $\mathcal{M}$ caractérise exactement la démontrabilité ?

Si les propositions sont valuées dans $\{0, 1\}$, alors la réponse est négative : cette propriété d'existence n'est pas uniforme. Pour le montrer, il suffit de penser à une théorie et une proposition telles que ni cette proposition ni sa négation ne sont démontrables dans cette théorie. Par exemple, si nous considérons une théorie sans axiomes ni règles de calcul et une proposition atomique P, alors ni P ni sa négation ne sont démontrables. De même, si nous prenons juste un symbole d'égalité $=$ et un symbole de fonction $+$, ni la commutativité $\forall x \forall y\, (x + y = y + x)$ ni sa négation ne sont démontrables : il est facile de trouver une structure algébrique commutative et une structure algébrique non commutative. En revanche, si nous nous donnons *un* modèle $\mathcal{M}$ quelconque, alors ou bien la proposition P ou bien sa négation est valide dans $\mathcal{M}$, car si P n'est pas valide dans $\mathcal{M}$, sa négation l'est. Il n'est donc pas possible de trouver un modèle valué dans $\{0, 1\}$, dans lequel la validité caractérise exactement la démontrabilité.

Le problème vient-il du fait que nous avons abusivement permuté les quantificateurs ? Non, c'est toujours une bonne idée d'essayer de permuter des quantificateurs. En revanche, la notion de modèle que nous avons introduite est trop rigide, car elle ne contient que deux valeurs de vérité : 0 et 1, alors que nous voudrions pouvoir donner à cette proposition P, qui n'est pas démontrable et dont la négation n'est pas démontrable non plus, ni la valeur 0 ni la valeur 1.

Algèbres de Boole et de Heyting Pour donner une valeur intermédiaire à la proposition P, il faut ici remplacer l'ensemble $\{0, 1\}$ par une algèbre de Boole quelconque. Qu'est-ce qu'une algèbre de Boole ? Un exemple paradigmatique est l'ensemble des parties d'un ensemble. Prenons l'ensemble des parties d'un ensemble à trois éléments. Nous avons bien sûr l'ensemble à trois éléments lui-même, qui est ce que nous appelions 1 auparavant. Nous l'ensemble vide, qui est ce que nous appelions 0. Mais nous avons aussi les singletons et les paires, qui sont des valeurs de vérité intermédiaires, qui peuvent servir à interpréter les propositions indéterminées.

La complétude uniforme vaut dans le cas des algèbres de Boole : il existe un modèle valué, non dans $\{0, 1\}$, mais dans une algèbre de Boole, dans lequel la validité caractérise exactement la démontrabilité. Il s'agit en fait d'un vieux théorème, le théorème de Lindenbaum, qui date des années 30.

Le tiers-exclu est toujours valide dans les modèles valués dans $\{0, 1\}$ et de même, il est toujours valide dans les modèles valués dans une algèbre de Boole : si nous prenons une partie d'un ensemble, son complémentaire puis leur réunion, nous obtenons l'ensemble tout entier. C'est pour cela que l'on a inventé une généralisation des algèbres de Boole, les algèbres de Heyting, qui permettent d'avoir des théorèmes de correction et de complétude pour les démonstrations constructives. Je ne vais pas entrer dans les détails de ce qu'est une algèbre de Heyting, je vais juste vous donner un exemple. Au lieu de prendre l'ensemble des parties d'un ensemble, prenons l'ensemble des ouverts d'un espace topologique. Considérons $\mathbb{R}$, par exemple, et au lieu de considérer toutes ses parties, ne considérons que ses parties ouvertes. Dans une telle algèbre, nous ne pouvons pas interpréter la négation comme le complémentaire, car en général, le complémentaire d'un ouvert n'est pas un ouvert. Nous interprétons alors la négation par la fonction qui à chaque ouvert associe l'intérieur de son complémentaire. L'ensemble des nombres strictement positifs est un ouvert. Son complémentaire, l'ensemble de nombres négatifs ou nuls, n'est pas un ouvert, et son intérieur est l'ensemble des nombres strictement négatifs. Mais l'union de l'ensemble des nombres strictement positifs et de sa « négation », l'ensemble des nombres strictement négatifs, ne couvre pas l'ensemble des réels tout entier, puisqu'il manque zéro. Le tiers-exclu n'est donc pas valide dans un modèle valué dans une telle algèbre. Voici donc comment le fait de passer des algèbres de Boole aux algèbres de Heyting permet d'éliminer le tiers-exclu.

3.2 L'élimination des coupures

Revenons à la question de la démonstration du théorème d'élimination des coupures en utilisant la correction et la complétude. Vous vous souvenez que la correction affirme que si une proposition A a une démonstration alors elle est valide dans tout modèle $\mathcal{M}$. Puis la complétude affirme que si la proposition A est valide dans tout modèle $\mathcal{M}$, alors elle a une démonstration :

$$A \text{ a une dém.} \xrightarrow{\text{corr.}} (\forall \mathcal{M}\, A \text{ est valide dans } \mathcal{M}) \xrightarrow{\text{comp.}} A \text{ a une dém.}$$

Nous allons transformer un tout petit peu la complétude et montrer que si la proposition A est valide dans tout modèle $\mathcal{M}$ alors elle a une démonstration *canonique*. Cette propriété s'appelle la complétude *renforcée*. Au lieu de montrer simplement qu'il existe une démonstration de A, nous montrons quelque-chose de plus fort : qu'il existe une démonstration canonique de A.

$$A \text{ a une dém.} \xrightarrow{\text{corr.}} (\forall \mathcal{M}\, A \text{ est valide ds } \mathcal{M}) \xrightarrow{\text{comp. renf.}} A \text{ a une dém. can.}$$

Et en utilisant la correction d'une part, la complétude renforcée d'autre part, nous pouvons démontrer le théorème d'élimination des coupures : si une proposition A a une démonstration, alors elle a une démonstration canonique.

Complétude uniforme renforcée Plus précisément, plutôt qu'un théorème de complétude renforcée, nous démontrons, en général, un théorème de complétude *uniforme* renforcée : il existe un modèle $\mathcal{M}$, tel que pour toute proposition A, si A est valide dans $\mathcal{M}$, alors A a une démonstration canonique. Il s'agit d'une variation sur le théorème de Lindenbaum.

Et nous n'avons maintenant besoin que d'un cas particulier du théorème de correction, selon lequel si une proposition A est démontrable alors elle est valide dans ce modèle-là.

$$A \text{ a une dém.} \xrightarrow{\text{corr.}} A \text{ est valide dans } \mathcal{M} \xrightarrow{\text{comp. renf. unif.}} A \text{ a une dém. can.}$$

Je ne vais pas expliquer comment construire ce modèle, mais ce n'est pas très difficile. Cette méthode fournit donc une démonstration algébrique du théorème d'élimination des coupures.

Je viens de vous présenter cette démonstration dans le cas sans théorie, c'est-à-dire sans axiomes ni règles de calcul. Mais Olivier Hermant, dans sa thèse, a étendu ce principe de construction de modèles à nombre de théories en Déduction modulo, dont nous savons de cette façon démontrer l'élimination de coupures.

4 L'élimination des coupures en utilisant des algorithmes

Maintenant, comment démontrer l'élimination des coupures en utilisant des algorithmes ? Nous avons déjà commencé à le voir tout à l'heure. Nous avons un algorithme qui transforme une démonstration qui contient une coupure en une démonstration dans laquelle cette coupure est éliminée, plus proche donc d'une démonstration canonique. Nous pouvons itérer cet algorithme : nous éliminons une coupure, puis une autre, etc. La question qui se pose est alors celle de la terminaison de cet algorithme.

4.1 La démonstration de Tait

Une démonstration de terminaison est due à William Tait [Tai67]. Et la méthode utilisée par Tait a, par la suite, été reprise et étendue de nombreuses fois. Essentiellement, cette démonstration procède par récurrence sur la structure arborescente des démonstrations.

Par exemple, considérons une démonstration π qui se conclut par la règle *élim*

$$\dfrac{\dfrac{\pi_1}{\vdash A \Rightarrow B} \quad \dfrac{\pi_2}{\vdash A}}{\vdash B}\,\textit{élim}.$$

Cette démonstration π contient deux démonstrations plus petites, π_1 et π_2. Et ce que Tait aurait sans doute souhaité démontrer, c'est que si l'élimination

progressive des coupures termine dans π_1 et dans π_2, alors elle termine dans π. De cette façon, en raisonnant par récurrence sur la structure des démonstrations, il serait arrivé à démontrer que l'élimination progressive des coupures termine dans toutes les démonstrations.

Malheureusement, cela ne marche pas. Alors Tait a fait ce que l'on fait toujours quand on a une démonstration par récurrence qui ne marche pas : on essaye de démontrer quelque-chose de plus fort. Bien sûr c'est plus difficile : le cas de base est plus difficile, et même l'étape de récurrence est plus difficile. Mais l'hypothèse de récurrence est plus forte. Et donc, si on a bien dosé la force de ce que l'on démontre, on peut faire passer la démonstration.

Tait a donc renforcé la propriété de terminaison en une propriété appelée la *réductibilité*.

4.2 La réductibilité

Je ne vais pas vous dire en détail ce qu'est la réductibilité, juste que la réductibilité d'une démonstration est relative à la proposition démontrée. Une démonstration π étant donnée, on ne peut pas dire : « π est une démonstration réductible. », il faut dire : « π est une démonstration réductible de A. » Et, à vrai dire, le coup de génie de Tait a été de définir la notion de réductibilité non par récurrence sur la structure des démonstrations, mais par récurrence sur la structure des propositions. Par exemple, à partir de l'ensemble R_A des démonstrations réductibles d'une proposition A et de l'ensemble R_B des démonstrations réductibles d'une proposition B, Tait nous donne une opération $\tilde{\Rightarrow}$, que je ne vais pas décrire, mais qui permet la construction de l'ensemble $R_{A\Rightarrow B}$ des démonstrations réductibles de $A \Rightarrow B$.

$$R_{A\Rightarrow B} = R_A \tilde{\Rightarrow} R_B.$$

Et de même pour les autres connecteurs.

La démonstration de Tait consiste donc à définir les ensembles de démonstrations réductibles de toute proposition A par récurrence sur la structure des propositions, puis à démontrer que toutes les démonstrations d'une proposition A sont des démonstrations réductibles de A, par récurrence sur la structure des démonstrations, et à en déduire enfin la terminaison de l'algorithme d'élimination progressive des coupures et la propriété d'élimination des coupures.

Deux méthodes Ces deux méthodes de démonstration de l'élimination des coupures — en utilisant des modèles d'une part, et des algorithmes d'autre part — s'appliquent-elles aux mêmes théories ? Encore une fois, c'est une question que nous n'étions pas capables de poser avant d'avoir une notion générale de théorie et de coupure pour cette théorie. C'est donc une question que nous avons pu nous poser que dans les dix dernières années. Nous espérions que la réponse serait positive, mais elle est négative. Il s'agit encore d'un résultat d'Olivier Hermant qui a montré l'existence de théories en Déduction modulo qui ont la propriété d'élimination des coupures, mais pour lesquelles l'algorithme

d'élimination progressive des coupures ne termine pas toujours : il existe une démonstration telle que si nous éliminons une coupure dans cette démonstration, puis une autre, puis une autre encore, etc. nous ne terminons pas, mais telle qu'il existe une démonstration canonique de la même proposition — que l'algorithme d'élimination progressive des coupures ne trouve donc pas.

Il y a beaucoup de débats autour de cet exemple : sommes nous en train de démontrer que la terminaison de l'algorithme d'élimination progressive des coupures n'est pas équivalente à l'élimination des coupures, ou est-ce juste que cet algorithme est trop naïf et que nous devons en proposer un plus complexe de manière à rétablir cette équivalence ?

Le point sur lequel je vais insister — pour la dernière fois, puisque je vais commencer à dire le contraire — c'est qu'il y a deux types de méthodes : d'un coté les méthodes à base de modèles et de l'autre cette démonstration qui prouve la terminaison d'un algorithme. Ces méthodes ne s'appliquent pas aux mêmes théories et donnent vraiment l'impression d'être comme l'huile et l'eau, utiles toutes les deux, mais impossible à mélanger.

5 Les cinq étapes de la convergence

Je vais maintenant essayer de montrer le contraire : je vais montrer comment, petit à petit, ces deux méthodes se sont rapprochées pour qu'aujourd'hui, nous les considérons comme les deux faces d'une même pièce. Et cela s'est fait en cinq étapes.

5.1 Les cinq étapes

5.1.1 Les candidats de réductibilité

Première étape, l'introduction par Jean-Yves Girard en 1970 [Gir71] d'une notion qui élabore sur la notion de réductibilité de Tait : la notion de *candidat de réductibilité*.

Girard a introduit cette notion pour démontrer l'élimination des coupures pour une théorie particulière, la théorie des types simples, qui est une variante de la théorie des ensembles. Cette théorie a une certaine importance et Gaisi Takeuti [Tak53] avait conjecturé, au début des années cinquante, qu'elle avait l'élimination des coupures. Dag Prawitz et Moto-o Takahashi [Pra68, Tak67] d'un côté, avec des méthodes à base de modèles, et Jean-Yves Girard de l'autre, avec des méthodes à base d'algorithmes, ont démontré que c'était le cas. Ces résultats sont donc une exception à la remarque que j'ai faite au début de cette leçon, puisqu'ils ont fermé une conjecture posée des années plus tôt.

Girard est donc parti de la démonstration de Tait, il a essayé de la généraliser de manière à démontrer l'élimination des coupures pour cette théorie, et il est arrivé à la conclusion que pour définir l'ensemble des démonstrations réductibles d'une proposition A, il lui fallait quantifier sur les ensembles de démonstrations réductibles de toute proposition B : pour pouvoir définir R_A, il aurait fallu avoir déjà défini tous les R_B, mais R_A est l'un des R_B.

Et, pour ce sortir de cette circularité, Girard a appliqué ce que j'appelle « le principe du capitaine du bateau des mutins ». Il y a une mutinerie à bord, le capitaine veut mettre aux fers le chef des mutins, mais il ne sait pas qui c'est. Une solution est de mettre tous les marins aux fers. Mais, ensuite, qui va faire marcher le bateau ? Cependant, même s'il ne sait pas exactement qui est le chef des mutins, le capitaine sait qu'il y a quelques fortes têtes à bord, et d'autres marins qui n'ont pas le charisme nécessaire pour mener une mutinerie. Il lui suffit donc de mettre les fortes têtes aux fers : ces fortes têtes sont ce que l'on appelle des « candidats de chef des mutins ».

De la même façon, nous ne pouvons pas quantifier sur tous les ensembles de démonstrations réductibles — ce serait circulaire — ni sur tous les ensemble de démonstrations — cela reviendrait à mettre tous les marins aux fers —, nous quantifions donc sur les ensembles de démonstrations qui sont des « candidats de réductibilité ».

Ce qui importe ici, c'est que, dans la preuve de Tait, il y avait une propriété « être une preuve réductible de A », alors que dans la preuve de Girard, il y a un ensemble des preuves réductibles de A et que cet ensemble appartient lui-même à un ensemble $\mathcal{C}$ des candidats de réductibilité, sur les éléments duquel on quantifie.

Plus tard, Michel Parigot a montré qu'une fois que l'on a défini les opérations de Tait, comme $\tilde{\Rightarrow}$, l'ensemble des candidats de réductibilité a une définition très simple [Par97] : il s'agit juste du plus petit ensemble clos par ces opérations.

Voilà pour la première étape : l'introduction des candidats de réductibilité et surtout de l'ensemble $\mathcal{C}$ des candidats de réductibilité, muni d'un certain nombre d'opérations $\tilde{\Rightarrow}$, etc., qui commence donc à ressembler à une algèbre.

5.1.2 Les candidats de réductibilité comme valeurs de vérité

La deuxième étape est une remarque due à Benjamin Werner. Sans doute aussi à d'autres, mais c'est de Benjamin que je la tiens. D'abord, Thierry Coquand a étendu la démonstration de Girard à un système appelé le Calcul des constructions [Coq85]. Puis Benjamin Werner a étendue cette démonstration au Calcul des constructions inductives [Wer94], qui est le langage qui sous-tend le système Coq. Mais il n'est pas très important pour nous aujourd'hui de savoir de quoi il s'agit précisément.

Pendant des années, j'ai partagé un bureau avec Benjamin. Je ne comprenais pas toujours les détails de son travail, mais à chaque fois qu'il l'expliquait au tableau à quelqu'un, il utilisait une notation « $[\![A]\!]$ », qui est une notation traditionnelle pour l'interprétation d'une proposition dans un modèle. Mais quand je lui demandais si $[\![A]\!]$ était une telle interprétation, il répondait que non : c'était le candidat de réductibilité associé à la proposition A, ce que l'on notait R_A auparavant.

Mais cette coïncidence de notation n'était pas fortuite. Elle manifestait une intuition qu'il y avait un point commun entre les candidats de réductibilité et les valeurs de vérité. Un candidat de réductibilité, comme une valeur de vérité est quelque chose que l'on associe à une proposition. De plus le candidat associé

à la proposition $A \Rightarrow B$ s'obtient à partir de celui associé à la proposition A et de celui associé à la proposition B en appliquant une opération $\tilde{\Rightarrow}$

$$[\![A \Rightarrow B]\!] = [\![A]\!] \tilde{\Rightarrow} [\![B]\!].$$

de la même manière que, dans un modèle, la valeur de vérité de la proposition $A \Rightarrow B$ s'obtient à partir de celle de la proposition A et de celle de proposition B en appliquant une autre opération $\tilde{\Rightarrow}$

$$[\![A \Rightarrow B]\!] = [\![A]\!] \tilde{\Rightarrow} [\![B]\!].$$

Ce changement de notation a donc précipité l'idée que le candidat de réductibilité associé à une proposition était à rapprocher de la valeur de vérité de cette proposition dans un modèle.

5.1.3 L'introduction des domaines

La troisième étape a alors consisté en un travail commun avec Benjamin Werner [DW03], au cours duquel nous avons démontré l'élimination des coupures pour un vaste ensemble de théories en Déduction modulo. Nous avons repris cette idée que l'ensemble $\mathcal{C}$ des candidats de réductibilité était un ensemble où interpréter les propositions : à chaque proposition, on associait un élément, non plus de $\{0, 1\}$, mais de cet ensemble $\mathcal{C}$ introduit par Girard.

Mais, chose surprenante, dans les démonstrations que Benjamin faisait auparavant, il n'y avait pas d'ensemble où interpréter les termes. Cette bizarrerie vient de ce que Benjamin travaillait alors sur des questions, non de théorie de la démonstration, mais de lambda-calcul. Or, dans ce cadre, la notion de terme n'est pas très claire : il n'y a plus véritablement de distinctions entre les termes, les propositions et les démonstrations. Et, de ce fait, il y avait avait une notion bizarre de modèle, sans domaine d'interprétation des termes.

Un point essentiel de notre démonstration a donc été l'introduction d'un tel domaine. Introduire un domaine d'interprétation des termes avait deux avantages. D'abord un avantage technique : les démonstrations devenaient tout d'un coup beaucoup plus faciles, parce qu'au lieu de devoir associer un candidat à une proposition complexe comme $P(t_1, \ldots, t_n)$, nous devions juste associer des objets du domaine aux termes t_1, …, t_n, puis fabriquer un candidat à partir des ces objets :

$$[\![P(t_1, \ldots, t_n)]\!] = \hat{P}([\![t_1]\!], \ldots, [\![t_n]\!]).$$

Cette décomposition simplifiait, voire illuminait, certaines constructions. Mais au-delà de cette dimension technique, il y avait une dimension tactique : nous voulions nous rapprocher de la notion courante de modèle.

En introduisant ces domaines, nous sommes arrivés à l'idée que pour démontrer qu'une certaine théorie en Déduction modulo avait la propriété d'élimination des coupures, il suffisait de construire un modèle valué non dans $\{0, 1\}$, mais dans l'algèbre $\mathcal{C}$ des candidats de réductibilité.

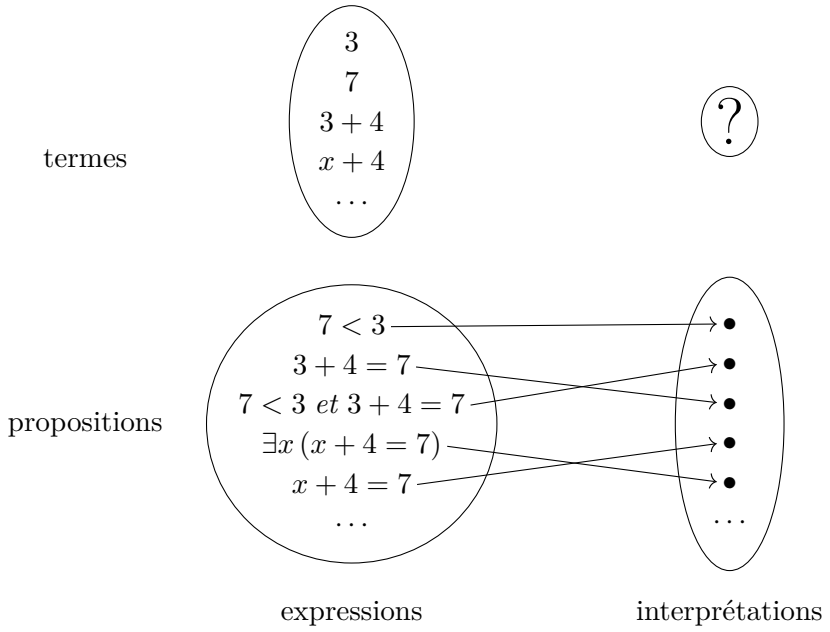

FIGURE 4 – Quel domaine d'interprétation des termes ?

Dans un modèle, les valeurs de vérité appartiennent à l'ensemble $\{0, 1\}$, à une algèbre de BOOLE ou à une algèbre de HEYTING. Mais les candidats de réductibilité appartenaient à l'ensemble $\mathcal{C}$. Était-ce une algèbre de BOOLE, une algèbre de HEYTING, auquel cas cette notion de modèle valué dans $\mathcal{C}$ aurait été un cas particulier d'une notion déjà connue ? Nous n'en savions rien.

5.1.4 Les pré-algèbres de Heyting

Ceci nous mène à la quatrième étape. Nous n'espérions pas trop que l'ensemble des candidats de réductibilité soit une algèbre de BOOLE, mais nous avions quelque espoir que ce soit une algèbre de HEYTING.

Or, qu'est-ce qui caractérise une algèbre de BOOLE ou de HEYTING ? Repensez, par exemple, à l'ensemble des parties d'un ensemble. Cette algèbre est naturellement ordonnée par l'inclusion. Plus généralement, les algèbres de BOOLE et les algèbres de HEYTING sont toujours des structures ordonnées.

Longtemps, nous nous sommes demandé quelle relation d'ordre mettre sur l'ensemble des candidats de réductibilité de manière à ce que les constructions de TAIT pour le « et », pour le « ou », etc., soient des bornes inférieures et supérieures, comme dans n'importe quelle algèbre de HEYTING. Et là nous sommes arrivés à un résultat négatif. Dans n'importe quelle algèbre de HEYTING, si nous prenons l'élément maximal $\tilde{\top}$ qui interprète naturellement la proposition « vrai » notée $\top$, et si nous construisons l'implication $\tilde{\top} \mathrel{\tilde{\Rightarrow}} \tilde{\top}$, nous obtenons

encore l'élément maximal de cette algèbre de Heyting :

$$(\tilde{\top} \tilde{\Rightarrow} \tilde{\top}) = \tilde{\top}.$$

Or, cette égalité n'est pas vérifiée par l'algèbre des candidats. L'algèbre des candidats n'est donc pas une algèbre de Heyting.

Nous avions donc un modèle dans lequel les propositions étaient valuées dans une algèbre qui n'était pas une algèbre de Heyting. Cette notion demandait donc à être étendue.

Les algèbres de valeurs de vérité Pourquoi, après tout, faudrait-il qu'un ensemble de valeurs de vérité soit ordonné ? Les algèbres de Boole et les algèbres de Heyting sont ordonnées, mais à quoi servent ces relations d'ordre ? N'est-ce pas juste une espèce de tropisme vers les relations d'ordre qui nous a menés à définir les algèbres de Boole et les algèbres de Heyting comme des structures ordonnées ?

Nous avons besoin qu'un ensemble de valeurs de vérités soit muni d'opérations, $\tilde{\Rightarrow}$, $\tilde{\forall}$, etc. pour pouvoir interpréter l'implication, le quantificateur universel, etc. Nous avons ensuite besoin que soit défini un sous-ensemble de valeurs de vérité positives, pour caractériser les propositions valides. Dans une algèbre de Boole ou une algèbre de Heyting, cet ensemble est le singleton qui contient l'élément maximal, mais il n'y a pas de raison d'imposer à cet ensemble d'être un singleton. Enfin, troisième ingrédient, nous avons besoin de conditions de clôture sur cet ensemble de valeurs de vérité positives, qui correspondent aux règles de déduction. Si, par exemple, les propositions $A \Rightarrow B$ et A sont interprétées par des valeurs de vérité positives, alors la proposition B doit aussi être interprétée par une valeur de vérité positive : la règle *élim* induit une condition de clôture sur l'ensemble des valeurs de vérité positives.

J'avais alors proposé d'une manière très *ad hoc* d'appeler « algèbre de valeurs de vérité » [Dow07] tout ensemble qui vérifiait ces propriétés : être muni d'opérations permettant d'interpréter les propositions, d'un ensemble de valeurs de vérité positives et de conditions de clôture. Les algèbres de Heyting étaient des algèbres de valeurs de vérité et l'ensemble des candidats de réductibilité était également une algèbre de valeurs de vérité.

La notion d'algèbre de Heyting était donc étendue en une classe d'algèbres dans laquelle on pouvait faire rentrer les candidats. Malheureusement, cette définition très *ad hoc* qui prenait les conditions minimales pour avoir un théorème de correction et de complétude était un peu frustrante.

Des ordres aux pré-ordres Par la suite, Thierry Coquand a proposé de définir, sur chaque algèbre de valeurs de vérité, une relation $\leq$ à partir des opérations de l'algèbre. Je ne vais pas vous expliquer comment on définit cette relation, mais ce n'est pas difficile. Cette relation est réflexive, transitive, elle satisfait toutes les propriétés d'une algèbre de Heyting sauf une : elle n'est pas antisymétrique. Ce n'est pas une relation d'ordre, mais une relation de pré-ordre.

Là encore, avoir fait un peu d'informatique aide. Nous pourrions nous désoler que cette relation ne soit pas antisymétrique. Mais, en informatique, nous savons que la notion importante n'est pas la notion d'ordre, mais celle de pré-ordre. Par exemple, quand nous construisons les rationnels comme des ensembles de fractions, nous aboutissons à une définition où chaque rationnel est un ensemble infini de fractions. Et quand nous voulons programmer les rationnels, il n'est pas pratique de devoir représenter des ensembles infinis. Depuis longtemps, nous savons que, quand nous programmons des rationnels dans les systèmes de calcul formel, nous n'utilisons pas la notion de rationnel à proprement parler, mais seulement celle de fraction. Nous n'utilisons pas non plus d'opération d'égalité : les fractions $4/8$ et $3/6$ sont manifestement différentes puisque leurs numérateurs sont différents. En revanche, nous avons une relation qui relie deux fractions si ces fractions représentent le même rationnel. Et, bien entendu, si nous tentons de définir un ordre sur les fractions, nous obtenons une relation réflexive et transitive, mais pas antisymétrique : si nous avons $a \leq b$ et $b \leq a$ nous savons que les fractions a et b représentent le même rationnel, qu'elles n'ont aucune raison d'être la même fraction.

Les relations d'ordre sont souvent obtenues par la violence d'un quotient appliqué à une relation de pré-ordre — c'est d'ailleurs par un quotient que Lindenbaum avait obtenu une algèbre de Boole. Si nous ne quotientons pas, tout fonctionne, mais nous avons des pré-ordre et non des ordres. Là où, cinquante ans plus tôt, nous aurions cherché à quotienter à tout prix, nous nous sommes satisfaits d'un pré-ordre. En quotientant l'ensemble des fractions, nous obtenons une infinité de rationnels, mais en quotientant l'ensemble des candidats de réductibilité, nous obtenons un singleton : tout s'écrase sur un même point. C'est une structure où quotienter fait perdre beaucoup d'information.

De ce fait, les algèbres de valeurs de vérités ont changé de nom et sont maintenant appelées des « pré-algèbres de Heyting ».

La super-cohérence Une chose nous a surpris : à une exception près, toutes les théories pour lesquelles nous avions construit un modèle valué dans l'algèbre $\mathcal{C}$ des candidats de réductibilité, avaient aussi un modèle valué dans n'importe quelle pré-algèbre de Heyting. En fait, l'algèbre des candidats est tellement compliquée que, quand on essaie de fabriquer un modèle valué dans cette algèbre, on n'utilise aucune de ses propriétés : on connaît trop peu de choses sur l'algèbre des candidats pour que la construction ne soit pas complètement générale.

Cela nous a amenés à définir une notion de théorie super-cohérente — théorie au sens d'ensemble de règles de calcul, encore une fois. Une théorie est super-cohérente si elle a un modèle valué dans une pré-algèbre de Heyting, non seulement pour une algèbre particulière — auquel cas on dit simplement qu'elle est cohérente — mais pour toutes.

Définition 5.1 (Super-cohérence) *Une théorie est super-cohérente si elle a modèle valué dans $\mathcal{B}$ pour toute pré-algèbre de Heyting $\mathcal{B}$.*

Une théorie super-cohérente, puisqu'elle a un modèle valué dans $\mathcal{B}$ pour toute pré-algèbre de Heyting $\mathcal{B}$, a en particulier un modèle valué dans l'algèbre $\mathcal{C}$ des

candidats de réductibilité. L'algorithme d'élimination progressive des coupures termine donc dans cette théorie.

Vous voyez le chemin le parcouru : nous sommes arrivés à définir une propriété algébrique, la super-cohérence, qui implique une propriété algorithmique, la terminaison de l'algorithme d'élimination progressive des coupures. Il ne restait alors plus qu'une étape : faire le lien avec les démonstrations algébriques d'élimination des coupures, dont je vous ai parlé tout à l'heure.

5.1.5 De la super-cohérence à l'élimination des coupures par les modèles

On doit à nouveau cette étape à Olivier Hermant [DH12]. Je m'étais posé la question : « Quand une théorie est super-cohérente, n'y a-t-il pas une démonstration plus simple du fait qu'elle a la propriété d'élimination des coupures ? » : non de la terminaison de l'algorithme d'élimination progressive des coupures, uniquement de l'existence d'une démonstration canonique. Et j'avais montré que l'on pouvait obtenir un tel résultat, avec une algèbre $\mathcal{C}'$ plus simple que celle des candidats de réductibilité : au lieu de considérer, comme éléments de cette algèbre, des ensembles de démonstrations, on remplaçait chaque démonstration par sa conclusion et on obtenait des ensembles de propositions conditionnelles. La super-cohérence, impliquait l'existence d'un modèle valué dans cette algèbre $\mathcal{C}'$, qui impliquait à son tour l'élimination des coupures.

Dans mon esprit, cette démonstration était juste une variation sur la démonstration fondée sur la terminaison de l'algorithme d'élimination progressive des coupures. Mais, en la lisant, Olivier Hermant s'est rendu compte que cette démonstration pouvait se reformuler comme une démonstration de complétude uniforme renforcée, ce que je n'avais pas vu. Et il a construit, à partir du modèle valué dans $\mathcal{C}'$, un autre modèle tel que la validité dans ce modèle impliquait l'existence d'une démonstration canonique.

À partir de l'hypothèse de super-cohérence, nous avions donc la possibilité, non seulement de montrer la terminaison de l'algorithme d'élimination des coupures, mais également de montrer la complétude uniforme renforcée, qui était la base des démonstrations algébriques traditionnelles d'élimination des coupures.

5.2 Le théorème et ses prolongements

Voici, finalement, le théorème auquel je voulais aboutir.

Théorème 5.1 *La super-cohérence est une condition suffisante à l'élimination des coupures.*

Ce théorème a deux démonstrations : l'une à base d'algorithmes, l'autre à base de modèles. La seule différence réside dans le choix de l'algèbre : dans un cas, l'algèbre $\mathcal{C}$ des candidat de réductibilité de Girard, dans l'autre, cette algèbre $\mathcal{C}'$ où nous élaguons toutes les preuves pour ne leur laisser que leurs conclusions. À partir de l'algèbre $\mathcal{C}$, nous obtenons la terminaison de l'algorithme

d'élimination progressive des coupures, et donc l'élimination des coupures par la voie algorithmique, à partir de l'algèbre $\mathcal{C}'$ nous obtenons la complétude uniforme renforcée et donc l'élimination des coupures par la voie algébrique.

Les méthodes à base de modèles et d'algorithmes d'élimination progressive des coupures Finalement, vous avez compris que ces méthodes sont juste les deux faces d'une même pièce. Elles utilisent la même propriété, la super-cohérence, et seul le choix de l'algèbre varie : l'algèbre $\mathcal{C}$ dans un cas, l'algèbre $\mathcal{C}'$ dans l'autre.

La conclusion est que les méthodes algorithmiques ne sont pas si déviantes. Quand ces méthodes sont arrivées au début des années soixante-dix, elles manifestaient la volonté de tourner le dos à l'algèbre, de dire que la voie algébrique était bien connue désormais et qu'il fallait chercher ailleurs de nouvelles idées. Je n'ai jamais compris si qualifier ces méthodes de déviantes était péjoratif ou mélioratif. J'ai l'impression que c'était plutôt mélioratif à cette époque. Mais nous nous apercevons *a posteriori* que ces méthodes ne s'éloignaient finalement pas tant que cela de l'algèbre. Pasteur aurait peut-être dit dit qu'un peu d'algorithmique éloigne de l'algèbre, mais que beaucoup y ramène [8]. Il y a des structures algébriques derrière les deux types de méthodes, et nous comprenons maintenant très bien leur correspondance.

Un problème ouvert Je vais terminer sur un problème ouvert. Ce théorème appelle une réciproque : « La super-cohérence est-elle uniquement une condition suffisante d'élimination des coupures, ou est-elle aussi une condition nécessaire ? », ce qui signifierait que l'élimination des coupures est une propriété strictement algébrique qui n'a rien à voir avec les démonstrations. La réponse est négative puisqu'Olivier Hermant a montré l'existence de théories qui ont la propriété d'élimination des coupures sans avoir la propriété de terminaison de l'algorithme d'élimination progressive des coupures. Si ces théories étaient super-cohérentes, alors cet algorithme terminerait, ce qui n'est pas le cas.

En revanche, nous pouvons nous demander si la terminaison de l'algorithme d'élimination progressive des coupures est équivalente à la super-cohérence. Et là, nous conjecturons plutôt que oui, parce que nous n'avons pas trouvé de contre-exemple.

Denis Cousineau a construit une algèbre $\mathcal{C}''$ qui est une variation de l'algèbre des candidats de réductibilité. Et il a montré que la terminaison de l'algorithme d'élimination progressive des coupures était équivalente à l'existence d'un modèle valué dans cette algèbre. C'est un résultat vraiment important parce que, pour la première fois, une propriété de terminaison implique l'existence d'un modèle.

La situation est donc la suivante : d'une part la terminaison de l'algorithme d'élimination progressive des coupures implique l'existence d'un modèle valué dans $\mathcal{C}''$, d'autre part la super-cohérence implique la terminaison de l'algorithme d'élimination progressive des coupures. Que nous manque-t-il pour arriver à l'équivalence de la terminaison de l'algorithme d'élimination progressive des

8. Selon Pasteur : « Un peu de science éloigne de Dieu, mais beaucoup y ramène. » (N.d.r.)

coupures et de la super-cohérence ? Il ne nous reste plus qu'à montrer que l'existence d'un modèle valué dans $\mathcal{C}''$ implique la super-cohérence, c'est-à-dire l'existence d'un modèle pour n'importe quelle pré-algèbre de Heyting. Cette propriété est sans doute équivalente au fait que l'algèbre $\mathcal{C}''$ est initiale dans la catégories des pré-algèbres de Heyting : une fois que nous avons a un modèle valué dans $\mathcal{C}''$, nous devrions être capable de le transformer en un modèle valué dans n'importe quelle pré-algèbre de Heyting. Malheureusement, nous n'avons aucune idée de ce à quoi ressemble cette catégorie des pré-algèbres de Heyting, nous ne savons pas caractériser les morphismes entre pré-algèbres de Heyting. Nous sommes donc loin de savoir si cet objet est initial ou non dans cette catégorie. Pour les algébristes, il y a là un problème intéressant et difficile.

Je vous remercie.

Questions

Question de Jacques Henry Est-ce que les algèbres de Boole et de Heyting ont un rapport avec la logique floue ? Le 0 interprète le faux, le 1 interprète le vrai, mais il y a quelque chose qui n'est plus ni 0 ni 1.

Réponse de Gilles Dowek Le point commun avec la logique floue, c'est qu'il y a plus de deux valeurs de vérité. Mais, dans une algèbre de Boole ou dans une algèbre de Heyting, nous n'avons aucune raison de nous limiter à des valeurs qui sont des nombres réels compris entre 0 et 1. Comme nous l'avons vu, ces valeurs de vérité peuvent, par exemple, être des ensembles de démonstrations.

Question de Bruno Courcelle Quand on a des preuves de terminaison, est-ce que l'on peut évaluer la longueur d'un calcul ?

Réponse de Gilles Dowek Je ne connais pas bien les travaux sur cette question, mais la réponse est plutôt négative. Nous pouvons voir les démonstrations comme des algorithmes et donc nous demander ce que nous pouvons calculer avec ces algorithmes. Or, nous pouvons calculer énormément de fonctions : toutes les fonctions qui sont prouvablement totales dans les théories considérées. Dans la théorie des types simples en particulier, nous pouvons calculer, par exemple, la fonction Ackermann [9] : et itérer une fonction un nombre de fois égal à $\mathrm{ack}(n)$. Nous ne pouvons pas pas espérer n^2 ou n^3, nous ne sommes pas du tout dans ces domaines-là.

9. La fonction d'Ackermann est la fonction à deux variables entières définie par :

$$\mathrm{Ack}(p,q) = \begin{cases} q+1 & \text{si } p=0, \\ \mathrm{Ack}(p-1,1) & \text{si } p>0 \text{ et } q=0, \\ \mathrm{Ack}(p-1,\mathrm{Ack}(p,q-1)) & \text{si } p>0 \text{ et } q>0. \end{cases}$$

Cette fonction croît très rapidement. À titre d'exemple, $\mathrm{Ack}(4,2) = 2^{65536} - 3$. Gilles Dowek fait ici référence à la fonction $\mathrm{ack}(n)$ définie par $\mathrm{Ack}(n,n)$ qui elle-même croît plus rapidement que toute itération de la fonction exponentielle. (N.d.r.)

En revanche, des questions de complexité se posent effectivement pour des logiques particulières, où l'on n'a pas toutes les règles de déduction. En particulier en logique linéaire, où on arrive à obtenir des caractérisations de classes de complexité intéressantes.

Question de Jean Bétréma Ce que je me rappelle de Scott quand j'étais petit, c'est qu'il s'agissait de logique et que ça ne parlait que d'ensembles ordonnés. Ça me semblait très bizarre. D'où vient cette importance des ensembles ordonnés en logique ?

Réponse de Gilles Dowek Il y a trois réponses à cette question. La première : les ensembles ordonnés sont partout, la notion est très générale. Pourquoi y a-t-il des entiers en logique ? Simplement, parce qu'il y a des entiers partout. Bon, c'est une réponse un peu faible.

Une autre tient aux problèmes auxquels Scott s'est intéressé. La notion de terminaison introduit naturellement une comparaison entre algorithmes : « Cet algorithme termine sur plus de valeurs d'entrée que celui-là. » C'est une relation d'ordre. Au delà de la terminaison, il y a la notion de quantité d'information. Un algorithme est un processus qui donne de l'information de manière un peu continue, disons. Il calcule, il donne de l'information, il calcule, il donne de l'information, etc. Et il est naturel de comparer les algorithmes de ce point de vue : « Cet algorithme donne plus d'information que celui-là. » C'est aussi une relation d'ordre. Les relations d'ordre chez Scott sont souvent de cette nature.

Puis la troisième réponse tient à un tropisme vers les relations d'ordre. Si un mathématicien, comme Scott, peut voir une relation d'ordre, il la voit. En revanche, s'il ne peut voir qu'une relation réflexive et transitive mais pas antisymétrique, il risque de penser que c'est un objet moins intéressant.

Cette différence entre ordres et pré-ordres est intéressante. Je n'ai rien contre les relations d'ordre, mais je me demande si, au lycée par exemple, il ne faudrait pas enseigner la notion de relation de pré-ordre avant celle de relation d'ordre.

Question de Sylvain Salvati En quoi les modèles dérivés des candidats de réductibilité se distinguent des espaces cohérents définis par Girard ?

Réponse de Gilles Dowek Dans les espaces cohérents, on cherche à interpréter les démonstrations elles-mêmes. On a une notation symbolique — un arbre, un lambda-terme ou quelque-chose comme ça — qui a l'air de n'être qu'un enregistrement *ad hoc* des étapes de construction d'une démonstration, et on se demande comment interpréter cette démonstration en un objet mathématique plus compréhensible.

Ici, nous ne cherchons pas à interpréter les démonstrations, mais les propositions. Et nous utilisons les démonstrations pour fabriquer des ensembles qui servent à interpréter ces propositions. Le but est donc assez différent.

Cela dit, dans les deux cas on cherche des algèbres là où on a des arbres et des algorithmes. Il y a donc peut-être des liens profonds à faire surgir. Mais pour le moment, je ne vois pas lesquels.

Références

[Bel68] Eugenio Beltrami, *Saggio di interpetrazione della geometria non-euclidea*, Giornale di Matematiche **VI** (1868), 284–312.

[Bel69] ———, *Essai d'interprétation de la géométrie non euclidienne*, Annales scientifiques de l'École Normale Supérieure **6** (1869), 251–288, Traduction de [Bel68] par J. Hoüel, http://www.numdam.org/item?id=ASENS_1869_1_6__251_0.

[Coh63] Paul Joseph Cohen, *The independence of the continuum hypothesis*, Proceedings of the National Academy of Sciences of the United States of America **50** (1963), no. 6, 1143–1148, http://www.ncbi.nlm.nih.gov/pmc/articles/PMC221287/.

[Coh64] ———, *The independence of the continuum hypothesis, II*, Proceedings of the National Academy of Sciences of the United States of America **51** (1964), no. 1, 105–110, http://www.ncbi.nlm.nih.gov/pmc/articles/PMC300611/.

[Coq85] Thierry Coquand, *Une Théorie des Constructions*, Ph.D. thesis, Paris 7, 1985.

[DH12] Gilles Dowek and Olivier Hermant, *A Simple Proof That Super-Consistency Implies Cut Elimination* , Notre Dame Journal of Formal Logic **53** (2012), no. 4, 439–456.

[DHK03] Gilles Dowek, Thérèse Hardin, and Claude Kirchner, *Theorem Proving Modulo*, Journal of Automated Reasoning **31** (2003), no. 1, 33–72, http://dx.doi.org/10.1023/A:1027357912519.

[DM07] Gilles Dowek and Alexandre Miquel, *Cut elimination for Zermelo set theory*, http://www-roc.inria.fr/who/Gilles.Dowek/Publi/zermodulo.pdf, 2007.

[Dow07] Gilles Dowek, *Truth Values Algebras and Proof Normalization*, Types for proofs and programs (Thorsten Altenkirch and Conor McBride, eds.), Lecture Notes in Computer Science, vol. 4502/2007, 2007, http://dx.doi.org/10.1007/978-3-540-74464-1_8, pp. 110–124.

[DW03] Gilles Dowek and Benjamin Werner, *Proof Normalization Modulo*, Journal of Symbolic Logic **68** (2003), no. 4, 1289–1316, http://www.jstor.org/stable/4147763.

[Gen35] Gerhard Karl Erich Gentzen, *Untersuchungen über das logische Schließen. I*, Mathematische Zeitschrift **39** (1935), no. ?, 176–210, http://www.digizeitschriften.de/dms/img/?PPN=GDZPPN002375508.

[Gen64] ———, *Investigations into Logical Deduction*, American Philosophical Quarterly **1** (1964), no. 4, 288–306, Traduction de [Gen35] par Manfred E. Szabo, http://www.jstor.org/stable/20009142.

[Gir71] Jean-Yves Girard, *Une extension de l'interpretation de Gödel à l'analyse et son application à l'elimination des coupures dans l'analyse et la theorie des types*, Proceedings of the Second Scandinavian Logic Symposium (Jens Erik Fenstad, ed.), Studies in logic and the foundations of mathematics, vol. 63, North-Holland, 1971, pp. 63–92.

[Gö29] Kurt Gödel, *Über die Vollständigkeit des Logikkalküls*, Ph.D. thesis, Universität Wien, 1929.

[Kle71] Felix Klein, *Über die sogenannte Nicht-euklidische Geometrie*, Mathematische Annalen **4** (1871), no. 4, 573–625, http://dx.doi.org/10.1007/BF02100583.

[Kle97] ———, *Sur la géométrie dite non euclidienne*, Annales de la faculté des sciences de Toulouse **11** (1897), no. 4, G1–G62, Traduction de [Kle71] par L. Laugel, http://www.numdam.org/item?id=AFST_1897_1_11_4_G1_0.

[Par97] Michel Parigot, *Proofs of Strong Normalisation for Second Order Classical Natural Deduction*, Journal of Symbolic Logic **62** (1997), no. 4, 1461–1479, http://www.jstor.org/stable/2275652.

[Pra68] Dag Prawitz, *Hauptsatz for Higher Order Logic*, The Journal of Symbolic Logic **33** (1968), no. 3, 452–457, http://www.jstor.org/stable/2270331.

[Tai67] William Walker Tait, *Intensional Interpretations of Functionals of Finite Type I*, Journal of Symbolic Logic **32** (1967), no. 2, 198–212, http://www.jstor.org/stable/2271658.

[Tak53] Gaisi Takeuti, *On a Generalized Logic Calculus*, Japanese Journal of Mathematics **23** (1953), 39–96, Errata, ibid, vol. 24 (1954), 149–156, à vérifier.

[Tak67] Moto-o Takahashi, *A proof of cut-elimination in simple type theory*, Journal of the Mathematical Society of Japan **19** (1967), no. 4, 399–410, http://dx.doi.org/10.2969/jmsj/01940399.

[Tar33] Alfred Tarski, *Pojęcie prawdy w językach nauk dedukcyjnych*, Éditeur ?, 1933, http://www.archiwum.wfis.uw.edu.pl/bibfis/index.php?option=com_content&view=article&id=129.

[Tar72] ———, *Le Concept de vérité dans les langages formalisés*, Logique, Sémantique, Métamathématique, 1923–1944, Armand Colin, 1972, À vérifer, 2 volumes. Traduction de [Tar33] par ?

[Wer94] Benjamin Werner, *Une Théorie des Constructions Inductives*, Ph.D. thesis, Université Denis Diderot Paris 7, 1994, http://tel.archives-ouvertes.fr/tel-00196524/.