Le Sens du calcul

Gilles Dowek

Le Sens du calcul

Gilles Dowek

Cet exposé aborde un aspect de la démonstration automatique. La démonstration automatique est une branche de l'informatique consacrée à la construction de programmes qui cherchent à démontrer des propositions. J'ai choisi ce sujet parce qu'il me semble qu'il peut apporter une petite contribution à la question générale du séminaire "Qu'est-ce qu'une logique ?".

Je dois dire, avant de commencer, que cette question me met particulièrement mal à l'aise. Elle suppose qu'il y a un certain nombre de choses qu'on appelle des logiques, par exemple, la logique du premier ordre, la logique modale, ou plus précisément telle logique modale : S4 ou S5, la logique d'ordre supérieur, etc. et qu'il faut définir cette classe de choses. Dans ce sens, la notion de "logique" me semble, sinon synonyme, au moins très proche de celle de "système formel". On peut donc donner une première définition "une logique est un système formel", ce qui nous ammène au problème de définir la notion de "système formel". Mais il me semble, et c'est là que la question me met mal à l'aise, que cette notion de système formel est déjà relativement bien définie. On ne peut donc pas faire comme si personne avant nous n'avait défini cette notion mais il me semble au contraire qu'il faut partir de cette définition.

Propositions et règles

Un système formel est donné par deux choses : un ensemble P dont les éléments s'appellent des "propositions" et un ensemble de règles R, où une règle est donnée par un certain nombre de schémas de propositions dont l'un, la conclusion, est privilégié. Ces règles définissent un sous-ensemble D de P, qui est le plus petit ensemble clos par ces règles.

On peut, par exemple, donner le système formel constitué des cinq règles suivantes : la première indique que de $A \Rightarrow B$ et A, on peut déduire B, la deuxième que de $\forall x\ A$, on peut déduire la proposition A dans laquelle on remplace la variable x par un terme quelconque, la troisième règle, sans prémisse, indique que Charles Martel est le père de Pépin le bref, la quatrième, sans prémisse également, indique que Pépin le bref est le père de Charlemagne et enfin la dernière, également sans prémisse, que le père du père de quelqu'un est son grand-père

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

$$\frac{\forall x\ A}{A[t/x]}$$

$$\frac{}{\mathit{père}(\mathit{Charles\ Martel}, \mathit{Pépin\ le\ bref})}$$

$$\frac{}{\mathit{père}(\mathit{Pépin\ le\ bref}, \mathit{Charlemagne})}$$

$$\frac{}{\forall x\ \forall y\ \forall z\ \mathit{père}(x,y) \Rightarrow \mathit{père}(y,z) \Rightarrow \mathit{grand\text{-}père}(x,z)}$$

Transcription d'un exposé au séminaire *Qu'est-ce qu'une logique ?* le Mardi 9 Avril 1996.
INRIA-Rocquencourt, B.P. 105, 78153 Le Chesnay Cedex, France.
Gilles.Dowek@inria.fr, http://pauillac.inria.fr/~dowek

Si on veut, on peut appeler “axiomes” les règles sans prémisse, mais pour la simplicité de la définition, on peut simplement les considérer comme des règles ordinaires. Dans ce système, on peut démontrer un certain nombre de propositions, par exemple que Charles Martel est le grand-père de Charlemagne. En revanche, on ne peut pas démontrer que Charlemagne est le père de Charles Martel, ce qui est d'ailleurs faux. La proposition *grand-père*(*Charlemagne*, *Charles Martel*) est dans l'ensemble P, mais pas dans l'ensemble D.

Cette définition, peut être critiquée de plusieurs façons, mais il me semble qu'on ne peut pas éviter d'en partir. Une première critique est que tombent sous cette définition beaucoup de choses qu'on ne veut pas appeler “logiques”. Par exemple, si les propositions sont 0, 1, 2, 3, etc. et qu'on donne deux règles qui indiquent que 0 est démontrable sans prémisse et que si n est démontrable, alors $n+5$ l'est aussi, l'ensemble des propositions démontrables est 0, 5, 10, etc. On ne veut pas appeler “logique” un tel objet. Un autre exemple : on prend pour P les suites finies de lettres de l'alphabet. Puis on se donne les règles suivantes : un groupe nominal suivi d'un verbe transitif suivi d'un groupe nominal est une phrase, un article suivi d'un nom commun est un groupe nominal, “le”, “l' ” et “un” sont des articles, “aviateur” et “mouton” sont des nom communs et “dessine” est un verbe transitif.

$$
\begin{gathered}
S \to GN\ VT\ GN \\
GN \to AR\ NC \\
NC \to \text{aviateur} \\
NC \to \text{mouton} \\
AR \to \text{le} \\
AR \to \text{l'} \\
AR \to \text{un} \\
VT \to \text{dessine}
\end{gathered}
$$

Ici encore, ces règles de grammaire peuvent être exprimées par un système formel. Chaque règle de grammaire se traduit par une règle de déduction, par exemple, la deuxième règle se traduit par

$$\frac{x\ GN\ y}{x\ AR\ NC\ y}$$

qui indique qu'on peut remplacer le symbole GN par la suite de symboles $AR\ NC$ et ce dans n'importe quel contexte.

On a dans l'ensemble D la phrase “L'aviateur dessine un mouton”, qui est vraie mais aussi la phrase “Le mouton dessine un aviateur” qui est fausse. C'est la grammaticalité et non la vérité qu'on définit ici. On ne veut donc pas appeler “logique” cet objet.

Une définition d'un ensemble D comme le plus petit sous-ensemble d'un ensemble P clos par un certain nombre de règles s'appelle une “définition inductive”. N'importe quelle définition inductive n'est pas une logique. On peut donc restreindre cette définition en indiquant que les éléments de P doivent être des propositions assertoriques. On doit alors commencer par définir la notion de proposition assertorique. Une proposition assertorique est une chose susceptible d'être vraie, pour définir ce qu'est une proposition assertorique, il faut donc définir d'abord la notion de vérité, et si on pense que “vrai” est synonyme de “démontrable dans une certaine logique”, pour définir la notion de vérité, il faut d'abord définir celle de logique, ce qui nous ramène à notre point de départ. Il faudrait donc définir l'une des trois notions : logique, proposition ou vérité sans utiliser les deux autres, et je ne vois pas comment le faire.

Cette critique consiste à dire que la définition d'une logique comme une définition inductive est trop vaste, elle capture trop de choses, elle capture certes les logiques comme celle ci-dessus mais aussi d'autres choses qui ne sont pas des logiques. On n'a donc pas suffisamment restreint la définition.

Je ne vais pas m'étendre sur ce type de critiques, car je pense que d'autres orateurs du séminaire auront des avis plus éclairés que le mien sur cette question. Je vais, en revanche, prendre le point de vue inverse : non seulement, cette définition capture trop de choses, mais également, elle n'en capture pas assez : une logique n'est pas toujours une définition inductive. La logique que j'ai donnée plus haut est une définition inductive, mais ce n'est pas le cas de toutes les logiques. Plus précisément, une logique n'est pas toujours

uniquement une définition inductive, on retrouve toujours cette idée de règle de déduction, mais complétée par d'autres éléments.

Le calcul

Bien avant de savoir construire un raisonnement, nous savions déjà faire des additions (par exemple, ajouter 9 et 57). Faire une addition sur des nombres en notation décimale demande une technique assez sophistiquée. Une méthode plus simple consiste à noter le nombre 9 par neuf bâtons et 57 par cinquante sept bâtons

||||||||| + ||||||||||||||||||||||||||||||||||||||||||||||||||||||||||||||||||||||||||

et pour faire l'addition, on efface alors un à un les bâtons à gauche du signe + en en ajoutant un à droite chaque fois

|||||||| + |||||||||||||||||||||||||||||||||||||||||||||||||||||||||||||||||||||||||||

Quand il ne reste plus de bâtons à gauche

+|||||||||||||||||||||||||||||||||||||||||||||||||||||||||||||||||||||||||||||||||||

on peut effacer le signe "+" et on obtient le résultat : 66

|||||||||||||||||||||||||||||||||||||||||||||||||||||||||||||||||||||||||||||||||||

Ce type d'expressions peut s'écrire dans un langage du premier ordre, avec un symbole zéro (0) et un symbole successeur (S) et les règles que nous avons utilisées pour effectuer l'addition peuvent se traduire comme des règles de transformation sur les termes de ce langage :

$$0 + y \text{ se transforme en } y$$

$$S(x) + y \text{ se transforme en } x + S(y)$$

On peut dire que ces règles sont des "règles de calcul", car partant de n'importe quel terme, par exemple le terme $9 + 57$, en appliquant ces règles un certain nombre de fois, on finit par obtenir un terme, par exemple 66, auquel aucune règle ne peut plus s'appliquer. Ceci est une propriété de terminaison. Il est, par exemple, impossible d'avoir une règle

$$x + y \text{ se transforme en } y + x$$

puisque $0 + 1$ pourrait se transformer en $1 + 0$ qui se transforme en $0 + 1$, et ce à l'infini. Avec ce type de règles on sort donc du cadre du calcul.

L'autre propriété qui définit le calcul, la confluence, consiste à dire que quelle que soit la manière dont on applique les règles, s'il s'avère que deux règles peuvent s'appliquer en même temps, elles mènent, au bout du compte, au même résultat. Par exemple, on ne peut pas avoir deux règles

$$0 \oplus y \text{ se transforme en } 0$$

$$x \oplus 1 \text{ se transforme en } 1$$

Le terme $0 \oplus 1$ se transformerait à la fois en 0 par la première règle et en 1 par la seconde. Ici, on est encore sorti du cadre du calcul car on a deux résultats pour le terme de départ. Ces propriétés de terminaison et de confluence impliquent que chaque terme se réduit en une forme unique, l'existence est une conséquence de la propriété de terminaison et l'unicité de la confluence.

Le raisonnement

Pourquoi ne pouvons nous pas nous contenter du calcul et avons nous eu besoin de passer du calcul au raisonnement ? Parce que, outre les propositions telles que $9 + 57 = 66$, nous voulons également établir des propositions générales, qui parlent non d'un nombre particulier mais de tous les nombres à la fois, par exemple

$$0 + x = x$$
$$S(x) + y = S(x + y)$$

La première proposition peut s'établir avec les règles ci-dessus. Dans l'expression $0 + x$, nous ne connaissons pas x, mais c'est un certain nombre de bâtons qu'on peut mettre dans une boîte, et le terme $0 + \square$ se transforme par la première règle en $\square$, sans ouvrir la boîte. Mais ce n'est pas le cas de toutes les propositions générales, en particulier la seconde proposition ne peut pas s'établir ainsi. Tout ce qu'on peut faire avec le terme $S(x) + y$ c'est le transformer en $x + S(y)$. Et avec le terme $S(x + y)$, on ne peut rien faire. Cette proposition est un exemple de propositions qu'on peut démontrer en arithmétique uniquement en utilisant le principe de récurrence. On préfère donc oublier cet aspect de calcul et utiliser un outil plus puissant : la déduction. Ces règles de calcul sont supprimées et deviennent des axiomes

$$\forall y \ (0 + y = y)$$
$$\forall x \ \forall y \ (S(x) + y = x + S(y))$$

En démonstration automatique, on en vient à se demander si c'est une bonne idée de remplacer ainsi les règles de calcul par des axiomes.

Un programme de démonstration automatique est un programme auquel on peut poser une question, par exemple "est ce que $x+S(y) = S(x+y)$?" et qui répond "oui", éventuellement en donnant une démonstration du théorème. Ce type de programmes ne permet pas, aujourd'hui, de démontrer des théorèmes difficiles, mais il s'avère que dans beaucoup d'applications concrètes en informatique, il est utile de pouvoir démontrer automatiquement des propositions comme celle-ci, même si leurs démonstrations sont triviales du point de vue mathématique.

On veut aussi pouvoir demander à ce type de programmes "est ce que $9 + 57 = 66$?", et on se trouve dans une situation paradoxale, où pour établir cette proposition, le programme est obligé d'en chercher une démonstration en arithmétique. On a donc un programme qui, certes sait faire des démonstrations pour établir des phrases générales, mais qui, quand on lui demande d'effectuer un simple calcul, situation où un ordinateur devrait avoir une certaine facilité, essaye de démontrer cette proposition par tous les moyens possibles. Il y a beaucoup de manières de démontrer cette proposition, par exemple en utilisant la commutativité de l'addition, on peut se ramener à la question "est ce que $57+9 = 66$?", en utilisant certains des axiomes on peut se ramener à la question "est ce que $10 + 56 = 66$?". On peut aussi se ramener à la question "est ce que $8 + 58 = 66$?" et cette voie de recherche est la bonne, puisque c'est elle qui, en quelque sorte, simule le calcul et mène à la question "est ce que $0 + 66 = 66$?" qui peut être résolue par l'un des axiomes, mais entre-temps on explore toutes les autres voies qui mènent à des impasses, comme celle qui consiste à permuter les deux membres à l'infini.

Le calcul et le raisonnement

On aimerait, quand on utilise ce type de techniques, avoir la possibilité de poser des questions générales comme "est ce que $x + S(y) = S(x + y)$?" qu'on ne sait pas traiter autrement que par la recherche d'une démonstration, mais aussi garder l'efficacité habituelle des ordinateurs pour résoudre les problèmes simples. On ne veut donc pas abolir la différence entre le calcul et le raisonnement.

Cette idée a été très bien formulée par Gordon Plotkin en 1972[1] quand il a remarqué qu'avec l'unique axiome

$$\forall x \ \forall y \ \forall z \ (x + (y + z) = (x + y) + z)$$

[1] G. Plotkin, Building-in equational theories, *Machine Intelligence*, 7 (1972) p. 73-90

un programme de démonstration automatique passait une grande partie de son temps à réarranger les parenthèses dans un sens ou dans l'autre sans rien produire d'intéressant.

L'idée est donc de ne pas abandonner cette notion de calcul dans la définition d'une logique. En arithmétique, par exemple, on garde les deux règles :

$$0 + y \text{ se transforme en } y$$

$$S(x) + y \text{ se transforme en } x + S(y)$$

On étend leur utilisation en les appliquant aux propositions, ce qui permet de dire non seulement que le terme $9 + 57$ se réduit sur le terme 66, mais également que la proposition $9 + 57 = 66$ se réduit sur la proposition $66 = 66$. De même, la proposition $9 + 57 = 65$ se réduit sur la proposition $66 = 65$. On peut alors quotienter l'ensemble P des propositions par la relation "avoir la même forme réduite". On identifie ces deux expressions en les considérant comme représentantes d'un objet plus général : l'ensemble des propositions qui ont la même forme réduite qu'elles. Une formulation équivalente consiste à dire qu'on démontre uniquement des propositions réduites, et que $9 + 57 = 66$ n'est pas une proposition, mais une pré-proposition qui se calcule en $66 = 66$.

Quand on demande à un ordinateur de démontrer la proposition $9 + 57 = 66$, il commence par réduire cette proposition en $66 = 66$. Cette proposition a une démonstration beaucoup plus simple : il suffit d'appliquer le principe d'identité, c'est-à-dire l'axiome $\forall x\ (x = x)$. Appliquer les règles de calcul pour réduire la proposition $9 + 57 = 66$ et obtenir $66 = 66$ a naturellement un coût, mais ce coût est bien moindre que celui de l'exploration de toutes les possibilités dans le cas de la recherche d'une démonstration en arithmétique.

Que devient alors l'axiome $\forall y\ (0+y = y)$? En l'absence de règles de calcul, on avait besoin de cet axiome pour démontrer la proposition $9+57 = 66$. Quand on ajoute les règles de calcul, cette proposition se démontre par le principe d'identité, et cet axiome n'est plus nécessaire. Il semble y avoir une redondance entre l'axiome et la règle de calcul. En fait l'axiome lui-même est un représentant de sa forme réduite $\forall y\ (y = y)$. De même l'axiome $\forall x\ \forall y\ (S(x) + y = x + S(y))$ est un représentant de sa forme réduite $\forall x\ \forall y\ (x + S(y) = x + S(y))$. Ces axiomes, qui sont conséquences du principe d'identité, peuvent être supprimés.

Donnons quelques exemples de règles : en arithmétique, on a les deux règles déjà données et des règles similaires pour la multiplication. Si on peut transformer non seulement les termes mais aussi les propositions, on peut ajouter les règles :

$$S(x) = S(y) \text{ se transforme en } x = y$$

$$S(x) = 0 \text{ se transforme en } \bot$$

$$0 = S(x) \text{ se transforme en } \bot$$

$$0 = 0 \text{ se transforme en } \top$$

Le troisième et le quatrième axiome de Peano

$$\forall x\ \forall y\ (S(x) = S(y) \Rightarrow x = y)$$

$$\forall x\ \neg(0 = S(x))$$

deviennent superflus puisqu'ils se transforment en

$$\forall x\ \forall y\ (x = y \Rightarrow x = y)$$

et

$$\forall x\ \neg\bot$$

qui sont des théorèmes du calcul des prédicats. Seul le schéma de récurrence reste comme axiome.

Un autre exemple est la règle de calcul de l'associativité

$$(x + y) + z \text{ se transforme en } x + (y + z)$$

Dans certaines formulations de la théorie des ensembles l'axiome

$$x \in \{x|A\} \Leftrightarrow A$$

peut être remplacé par la règle

$$t \in \{x|A\} \text{ se transforme en } A[t/x]$$

Dans les formalisations des mathématiques qui s'appuient, non sur la notion d'ensemble, mais sur celle de fonction, on note $x \mapsto t$ la fonction qui a x associe t, par exemple $x \mapsto x + 2$. On peut alors remplacer l'axiome

$$(x \mapsto t)(x) = t$$

par la règle

$$(x \mapsto t)(u) \text{ se transforme en } t[u/x]$$

Dans toutes ces théories, ajouter ces règles permet de supprimer des axiomes et de rendre les démonstrations plus courtes puisque certains arguments calculatoires en sont supprimés. On distingue ainsi le calcul qui est pris en charge par ces règles, du raisonnement qui reste dans les démonstrations formelles qui sont plus courtes, plus informatives et plus faciles à trouver.

Décidabilité de la relation entre démonstrations et propositions

Étendre ainsi la notion de système formel sur des ensembles de propositions ou sur des propositions réduites pose quelques problèmes. En particulier, il se pose la question de savoir si les démonstrations restent convaincantes. Quand on regarde une démonstration, aussi complexe soit-elle, on doit être capable de vérifier, étape par étape, qu'elle est correcte. Sinon, ce n'est pas une démonstration. La démonstration doit véhiculer toute l'information nécessaire pour que le lecteur puisse lui-même se convaincre que la justesse de ce qui est démontré. Par exemple, si on a la démonstration

$$\frac{\forall x\ (x = x)}{66 = 66}$$

et qu'on prétend que c'est une démonstration de la proposition $9 + 57 = 66$, il faut faire un tout petit effort pour se convaincre que la démonstration est correcte. Il faut se convaincre que la conclusion $66 = 66$ de cette démonstration et la proposition $9 + 57 = 66$ appartiennent bien à la même classe, c'est-à-dire qu'elles ont la même forme réduite. Pour cela, il faut calculer les formes réduites de ces deux propositions. Il y a un peu de travail à faire, mais ce travail peut être fait car le système des règles de calcul a les propriétés de terminaison et de confluence, ce qui permet de réduire les propositions et de vérifier que leurs formes réduites sont identiques. Il n'y a donc pas de perte d'information en passant d'une démonstration en arithmétique à une démonstration dans le quotient. L'information qui semble perdue n'est pas pertinente car il est possible de la reconstituer.

Mais, il y a plus grave : toujours avec cette règle d'élimination du quantificateur universel, on prend un autre axiome

$$\forall x\ \mathit{pair}(x + x)$$

et on donne la démonstration

$$\frac{\forall x\ \mathit{pair}(x + x)}{\mathit{pair}(14)}$$

Pour vérifier que cette étape de démonstration est correcte, il faut retrouver le terme par lequel la variable x a été remplacée. Ici, on devine que c'est le terme 7. On peut d'ailleurs se demander, même quand il n'y a pas de règles de calcul si une application de la règle d'élimination du quantificateur universel peut toujours être vérifiée. Par exemple, pourquoi est on convaincu que la démonstration

$$\frac{\forall x\ \mathit{pair}(x + x)}{\mathit{pair}(7 + 7)}$$

est correcte ? C'est parce qu'il est possible de comparer les propositions "*pair*$(x+x)$" et "*pair*$(7+7)$" pour trouver que la variable x a été substituée par 7. Cette comparaison a un nom technique, elle s'appelle le "filtrage". Le filtrage dans les langages de premier ordre est décidable. Mais, quand on a des règles de calcul, le problème est un peu différent : le problème est de de savoir s'il est possible de substituer la variable x dans la proposition *pair*$(x+x)$ par un terme, non pour obtenir la proposition *pair*(14), mais une proposition qui a même forme réduite que *pair*(14). La décidabilité de ce problème dépend beaucoup des règles de calcul considérées. Avec des règles pour l'addition et la multiplication, le filtrage est décidable, si on ajoute la soustraction il devient indécidable.

Quand les règles de calcul sont telles que filtrage est indécidable, il faut changer un peu la grammaire des démonstrations pour qu'on puisse continuer à les vérifier : il faut indiquer le terme substitué dans la règle d'élimination du quantificateur universel pour qu'il n'y ait plus rien à deviner. Alors, pour vérifier une démonstration, il suffit de substituer la variable dans la prémisse de la règle par le terme donné et de vérifier que la proposition obtenue a la même forme réduite que la conclusion.

Si on formule les raisonnements, non en déduction naturelle, mais dans les systèmes à la Frege-Hilbert, le même problème se pose pour savoir si l'ensemble des formes réduites des axiomes logiques $\forall x\ A \Rightarrow A[t/x]$ est décidable.

Démonstration automatique

En démonstration automatique, quelle que soit la méthode utilisée, on doit souvent comparer des propositions. Par exemple, si on a un axiome

$$\forall x\ (0 \leq x)$$

et qu'on cherche à démontrer la proposition

$$\exists y\ (y \leq 7)$$

on compare les proposition $0 \leq x$ et $y \leq 7$ ce qui nous suggère d'utiliser l'axiome dans le cas $x = 7$ et de démontrer la conclusion dans le cas $y = 0$, et donc la démonstration

$$\dfrac{\dfrac{\forall x\ (0 \leq x)}{0 \leq 7}}{\exists y\ (y \leq 7)}$$

Ce problème de comparaison, qui s'appelle l'"unification", ressemble beaucoup au filtrage. La seule différence est que dans le cas du filtrage les variables n'apparaissaient que dans l'un des termes comparés, alors qu'ici elles peuvent apparaître dans les deux.

Dans un système logique qui comprend des règles de déduction et des règles de calcul, les problèmes qui sont posés ne sont plus des problèmes d'unification ordinaires, mais des problèmes d'unification modulo les règles de calcul. C'est ce qu'on appelle l'"unification équationnelle". L'algorithme pour l'unification simple, est essentiellement composé d'une règle de décomposition, qui transforme l'équation $(0 \leq x) = (y \leq 7)$ en le système $y = 0, x = 7$. La comparaison des propositions $0 \leq x + 3$ et $y \leq 7$ échoue : certes l'équation $(0 \leq x + 3) = (y \leq 7)$ se simplifie en $0 = y, x + 3 = 7$ mais dans la seconde de ces équations le symbole de fonction est "+" dans l'un des termes et "S" dans l'autre, en substituant les variables, on ne peut pas changer ces symboles de fonction, et donc l'équation n'a pas de solution.

Si on compare maintenant ces deux termes modulo les règles de calcul, il y a une solution $x = 4$ qui apparaît. En effet, le terme $4 + 3$ se réduit sur le terme 7. Comment peut-on trouver ce terme ? Outre la décomposition, on a une seconde règle, la "surréduction", qui demande de substituer les variables par n'importe quel terme qui amène une réduction, par exemple dans le cas de l'équation $x + 3 = 7$ on substitue la variable x par le terme $S(x')$, le terme $S(x') + 3$ se réduit alors en $x' + 4$. En répétant cette opération, on obtient l'équation $x'''' + 7 = 7$, et on substitue x'''' par 0, ce qui donne $x = 4$.

Qu'est-ce qu'une logique ?

Nous avons donc vu comment ajouter un processus de calcul à une logique et les différences que cela induit pour la vérification des démonstrations et la recherche automatique des démonstrations.

Je pense que vous avez deviné la petite pierre que je voudrais apporter à la question "Qu'est-ce qu'une logique ?". La thèse que je voudrais défendre est qu'une logique est composée non seulement de règles de déduction, mais aussi de règles de calcul. Bien entendu, pour chaque logique définie par des règles de déduction et des règles de calcul, on peut construire une logique qui n'a que des règles de déduction et qui démontre les mêmes propositions, l'ensemble des propositions démontrables est le même, mais les démonstrations sont différentes.

Je voudrais, pour terminer, citer deux applications de cette idée. La première reste dans le cadre de l'informatique théorique et la seconde en sort.

Programmer en langage mathématique

La première est la programmation des ordinateurs en langage mathématique. Si on emprunte une somme e à une banque et qu'on la rembourse en n mensualités et que t est le taux d'intérêt mensuel, le montant des mensualités est donné par la formule

$$f(e,t,n) = \frac{et}{1-1/(1+t)^n}$$

Pour calculer le montant de ces mensualités, l'employé de banque tape sur son ordinateur la somme empruntée, par exemple 30000 francs, le nombre de mensualités, par exemple 24, et le taux d'intérêt, par exemple 0.0064, et l'ordinateur affiche la somme à rembourser chaque mois. Le programme qui transforme l'information e,t,n en $f(e,t,n)$ n'est, d'un certain point de vue, rien d'autre que la fonction f. Ce que l'ordinateur affiche est un terme u tel que $f(30000, 0.0064, 24) = u$ soit une proposition vraie. Mais cette condition n'est pas suffisante : le terme $f(30000, 0.0064, 24)$ la vérifie car la proposition

$$f(30000, 0.0064, 24) = f(30000, 0.0064, 24)$$

est vraie. Mais si c'est ce terme qui s'affiche sur l'écran de l'ordinateur, cela n'aide pas beaucoup à savoir si on pourra rembourser ces mensualités ou non. On n'attend pas non plus que s'affiche le terme $1300+60-7$, ce qu'on veut c'est le terme 1353. Ce terme est ce qu'on appelle une "valeur". L'ordinateur doit donc calculer la valeur associée au terme $f(30000, 0.0064, 24)$. Identifier programmes et fonctions n'est donc utile que si on formalise les mathématiques dans un système qui comprend des règles de déduction et des règles de calcul, telles que les valeurs soient les formes réduites pour ces règles de calcul.

Pour les fonctions explicitement définissables comme celles-ci, l'arithmétique convient. Mais si on veut utiliser toute la puissance des définitions mathématiques, c'est-à-dire utiliser l'opérateur de descriptions qui permet de définir la fonction prédécesseur sur les nombres relatifs comme la fonction qui à x associe l'unique nombre dont le successeur est x, alors il faut un système de calcul sur ces termes qui est relativement sophistiqué et qui demande en particulier de faire des démonstrations mathématiques des objets à part entière, de manière à ce que l'opérateur de descriptions prenne en argument une démonstration que la définition est correcte, c'est-à-dire que pour tout nombre x il existe un nombre y tel que x soit le successeur de y, et le système de calcul doit, entre autres, éliminer les coupures dans ces démonstrations. En effet, si on se contente de la définition "l'unique nombre dont le successeur est égal à x" sans donner de démonstration qu'un tel nombre existe, on ne voit pas par quel miracle on trouverait 4 en appliquant cette expression à 5. En revanche, si on donne aussi une démonstration constructive la proposition "pour tout x, il existe y tel que le successeur de y est égal à x", appliquer cette démonstration au nombre 5 crée une coupure dont l'élimination produit le nombre 4. La théorie des types de Martin-Löf[2], Le Calcul des constructions[3] et le

[2] P. Martin-Löf, *Intuitionnistic type theory*, Bibliopolis, Napoli (1984)

[3] Th. Coquand, G. Huet, *The calculus of constructions*, Information and Computation 76 (1988) p. 74-85.

Calcul des constructions inductives[4] sont des exemples de tels systèmes.

Le sens

La seconde application que je voudrais mentionner est l'impact de cette définition de la notion de logique sur la définition de la notion de sens. Le sens d'une proposition, qu'on oppose à la dénotation, est défini par Frege dans *Les lois fondamentales de l'arithmétique* : "Nos stipulations déterminent à quelles conditions ce nom [de valeur de vérité] dénote le vrai. Le sens de ce nom est la pensée que ces conditions sont remplies." En des termes plus modernes, Michael Dummett définit ainsi le sens : "Nous n'expliquons plus le sens d'un énoncé en stipulant sa valeur de vérité en termes des valeurs de vérité de ses constituants mais en stipulant à quelles conditions on peut l'asserter et ce en termes des conditions auxquelles ses constituants eux-mêmes peuvent être assertés."[5]. Autrement dit, le sens d'un énoncé A, est ce qu'il faut faire pour asserter cet énoncé, pour le démontrer. Le sens d'un énoncé de la forme "A et B" est ce qu'il faut faire pour asserter cet énoncé et ce qu'il faut faire c'est asserter A et asserter B. Cela donne la règle de déduction naturelle d'introduction de la conjonction "et". Cette règle est le sens de la conjonction "et". Et ce sens, nous ne savons pas l'exprimer autrement qu'en donnant cette règle.

Cette notion de sens permet de définir le sens des connecteurs et des quantificateurs. On peut également définir ainsi le sens des symboles de prédicat et de fonction d'un langage, par exemple, la notion de parallèle est définie par les axiomes de la géométrie. Cette idée rejoint celle de Poincaré selon laquelle les axiomes de la géométrie sont des "définitions déguisées". On n'a pas d'autre moyen de définir la notion de parallèle qu'en donnant les axiomes de la géométrie. Cela marche bien pour expliquer le sens de petits bouts de phrases : les connecteurs, les quantificateurs, les symboles de prédicat, etc. Mais cela peut-il nous aider à comprendre le sens de phrases complètes ?

Plus simplement cela peut-il nous aider à comprendre à quelle condition deux propositions A et B ont le même sens. Si on parvient à définir cette relation d'équivalence "avoir même sens que", on pourra se contenter de définir le sens d'une proposition comme sa classe d'équivalence pour cette relation. Cela permet d'évacuer le problème de la nature du sens et de le définir, en quelque sorte, à un isomorphisme près. Si on suit cette définition du sens comme "condition d'assertabilité", deux propositions A et B ont le même sens si ce qu'il faut faire pour démontrer A est la même chose que ce qu'il faut faire pour démontrer B. Mais, dans un cadre dans lequel on n'a que des règles de déduction, une démonstration ne peut être à la fois une démonstration de A et une démonstration de B que si A et B sont identiques. Si elles sont différentes, deux propositions ont donc toujours un sens différent, car elles ne peuvent pas partager de démonstration.

Quand on définit une logique avec des règles de déduction et des règles de calcul, on a une équivalence plus faible selon laquelle deux propositions ont le même sens si elles ont la même forme réduite, c'est-à-dire sont égales dans le quotient. Autrement dit, le calcul n'a pas de sens : calculer dans une proposition n'affecte pas le sens de la proposition.

Une première conséquence est que le sens d'une proposition dépend des conventions de calcul choisies. Si on ne prend aucune règle de calcul, les propositions $9 + 57 = 66$ et $66 = 66$ ont des sens différents. En revanche, si on prend les règles de l'addition comme des règles de calcul, ces deux propositions ont le même sens. Il y a quelque chose d'un peu choquant à ce que le sens d'une proposition dépende de conventions. Mais le même problème se pose avec la dénotation : l'hypothèse du continu ne dénote "vrai" ou "faux" qu'en fonction des axiomes qu'on pose, c'est-à-dire des conventions de raisonnement. De la même manière que la dénotation d'une proposition est déterminé par les conventions de raisonnement, le sens d'une proposition est déterminé par les conventions de calcul.

Une autre conséquence, qui est plus troublante, est que le problème de l'égalité de sens de deux propositions est décidable, puisqu'il suffit de comparer leur formes réduites. Mais pourrions nous dire que deux propositions ont le même sens si en les regardant nous n'étions pas capables de nous en rendre compte ?

[4]Ch. Paulin-Mohring, Inductive definitions in the system coq, rules and properties, Typed lambda calculi and applications, Lecture Notes in Computer Science 664, Springer-Verlag (1993) pp. 328-345.

[5]M. Dummett, Philosophie de la logique, *Minuit* (1991) p. 67

Questions

Question : Est-ce que la proposition $66 = 66$ est dans la même classe que $65 = 65$?
Réponse : Cela dépend des conventions. Si on prend la règle de calcul

$$S(x) = S(y) \text{ se transforme en } x = y$$

alors $66 = 66$ se trouve être dans la même classe que $65 = 65$, qui est lui-même dans la même classe que $0 = 0$, et si on prend également la règle

$$0 = 0 \text{ se transforme en } \top$$

également dans la même classe que la proposition $\top$. Mais, encore une fois, poser cette question est un peu la même chose que demander si l'hypothèse du continu est vraie ou fausse. La réponse dépend des conventions qu'on s'est fixées. On est aussi libre de choisir ses règles de calcul, que de choisir ses axiomes et ses règles de déduction.

Q : Combien y a-t-il de classes d'équivalences ?
R : Cela dépend encore des conventions, mais le système de déduction est indécidable, le nombre de classes est nécessairement infini.

Q : Les propositions A et "A et A" ont-elles même sens ?
R : Dans les exemples que j'ai donnés, j'ai commencé par des règles qui s'appliquaient à des termes, puis à des règles qui s'appliquaient à des propositions atomiques, on peut continuer en donnant des règles qui s'appliquent à des propositions composées. Dans ce cas, on peut choisir des règles de manière à ce que les propositions A et "A et A" aient même sens.

Q : Il semble y avoir une grande liberté dans le choix des règles ?
R : De la même manière qu'il y a un théorème d'incomplétude qui montre que chaque fois qu'on a un système d'axiome, on peut l'enrichir, il y a un théorème d'indécidabilité qui montre que chaque fois qu'on a un ensemble de règles de calcul, il y a une proposition qui n'est pas établie par ce système de calcul et donc qu'on peut l'enrichir par de nouvelles règles de manière à établir cette proposition. De la même manière qu'il n'y a pas une vérité absolue indépendante des axiomes qu'on utilise pour raisonner, il n'y a pas de sens absolu indépendant des règles de calcul (de l'ensemble des transformations qui préservent le sens).

Q : Quel sens attribuer aux énoncés non démontrables ?
R : C'est vrai que si on dit A et B ont le même sens s'ils ont les mêmes démonstrations, alors deux énoncés non démontrables ont toujours même sens. Donc le petit théorème de Fermat et le grand théorème de Fermat n'ont pas le même sens, mais leurs négations si (si la théorie des ensembles est cohérente).

Une solution serait de dire que A et B ont le même sens si "être une démonstration de A" est intentionnellement égal à "être une démonstration de B". Deux propositions ont le même sens si l'intentionnalité d'être une démonstration de A et d'être une démonstration de B sont égales. Mais ici, l'intentionnalité, ce n'est jamais qu'un autre nom pour le sens. Cette définition est donc circulaire.

On peut alors dire que deux propositions ont le même sens si les démonstrations de A et les démonstrations de B sont les mêmes dans tous les systèmes d'axiomes. La manière dont on démontre une proposition dans tel ou tel système d'axiomes donne une indication sur son sens. Cela résout le problème pour les propositions indéterminées (par exemple, l'hypothèse du continu), mais pas pour les négations de propositions démontrables, par exemple les négations de tautologies, ces propositions ne sont démontrables que dans des systèmes incohérents, donc elles ont des démonstrations triviales dans tous les systèmes d'axiomes dans lesquels elles sont démontrables.

Pour ces propositions, je ne sais pas répondre autre chose que "posons par principe que deux propositions ont le même sens, si elles ont la même forme réduite". Dans ce cas deux propositions qui ont le même sens ont les mêmes démonstrations, mais deux propositions peuvent avoir le même ensemble de démonstrations

sans avoir le même sens. Cela dit, ce cas ne se produit que si cet ensemble de démonstrations est vide, c'est-à-dire quand les propositions ne sont pas démontrables.

Q : Peut-on dire que deux propositions ont le même sens s'il y a un algorithme qui transforme toute démonstration de l'une en une démonstration de l'autre ?

R : Oui, mais pas n'importe quel algorithme. Sinon toutes les propositions démontrables ont le même sens, car les fonctions constantes sont calculables.

Q : Est-ce qu'on peut dire que définir une logique par des règles de déduction et des règles de calcul revient à découper les sens en deux fragments : un sens qui se rapporte aux règles de déduction, qui confine aux situations d'indécidabilité qui est le sens qu'on ne peut pas réduire à du calcul et un sens mécanisable qu'on peut se permettre d'éliminer en quotientant les énoncés par un ensemble de règles de calcul approprié ?

R : Il me semble que le premier sens, c'est la dénotation. Si le petit théorème de Fermat et le grand théorème de Fermat sont tous les deux démontrables, ils ont la même dénotation. En revanche ils n'ont pas le même sens, car ils ne véhiculent pas la même information. Donc, avoir le même sens, ce n'est pas être équivalent logiquement. Le sens c'est quelque chose de plus fin et qui, me semble-t-il, relève uniquement du calcul. Si pour décider que deux propositions ont le même sens, il faut encore donner un argument, il ne me semble pas qu'on puisse dire qu'elles ont le même sens.

Q : Peut-on filer la métaphore pour dire qu'on a une esquisse d'un modèle de la compréhension dans la conversation qui consisterait à supposer chez celui qui écoute, une tentative de construire une démonstration de ce que dit l'autre, de construire le sens de ce que dit l'autre ?

R : Oui, mais cette reconstruction doit rester dans un cadre décidable. Si je dis "Charles Martel est le père de Pépin le bref et Pépin le bref est le père de Charlemagne, donc Charles Martel est le grand-père de Charlemagne", je suppose que tu sais que le père du père de quelqu'un c'est son grand-père. Mais si j'ai appris, il y a cinq minutes que la troisième guerre mondiale était déclenchée, et que je sais que je suis le seul à le savoir ici, je ne peux pas te parler en supposant que tu le sais. Il faut que je considère que ce qui est implicite dans ce que je dis, tu le sais ou que tu peux en reconstruire la démonstration en un temps borné. Il faut que nous soyons d'accord sur ce que nous reconnaissons comme implicite. Je ne peux supposer que tu sais des choses uniquement dans un cadre décidable. Quand on communique des démonstrations dans un système constitué de règles de déduction et de règles de calcul, l'implicite est exactement avec ce qui est traité par les règles de calcul.

Q : Si on admet cette idée que dans une certaine mesure on joue avec une notion de cadre, et que chaque interlocuteur tente de reconstruire les démonstrations de ce que dit l'autre, où est cette propriété de la logique, sur laquelle tu es resté très discret, et qui est la possibilité d'élimination des coupures ? Quand ces démonstrations que chacun construit, sont-elles mises en branle dans un processus de calcul ?

R : C'est quand on utilise l'opérateur de descriptions. Au lieu de dire "le nombre 4", je dis "le prédécesseur de 5", où le prédécesseur de x est défini comme l'unique nombre dont le successeur est x et je sais que tu connais une démonstration que tout entier relatif a un prédécesseur (ou bien parce que je t'ai communiqué cette démonstration, ou bien parce qu'elle est dans nos présupposés). Si tu veux connaître la valeur du nombre que j'ai désigné, il te faut éliminer les coupures.

Q : Mais je ne vais pas toujours faire cela, je vais me contenter de connaître une démonstration de la bonne facture de la définition du prédécesseur, et je vais continuer à utiliser l'expression "le prédécesseur de 5".

R : Si je te demande de mettre le prédécesseur de 5 francs dans un parcmètre, il faudra faire le calcul pour mettre 4 francs.

Q : Pour répondre à la question "Qu'est-ce qu'une logique ?", tu as très peu fait appel à la notion de validité.

R : J'ai compris la question "Qu'est-ce qu'une logique ?" comme "Comment peut-on définir la notion de vérité ?". De ce point de vue, il ne me semble pas que la notion de validité dans un modèle (ou dans tous les modèles) soit pertinente, car cette définition présuppose une notion de vérité pour les jugements de la

forme “la proposition A est valide dans le modèle M”. En revanche cette notion de validité est centrale pour l'étude de ces systèmes logiques (cohérence, indépendance, etc.). Elle est aussi centrale pour comprendre comment on peut axiomatiser les mathématiques avec la théorie des ensembles et continuer, malgré tout, à faire de la géométrie avec les axiomes d'Euclide : le théorème de complétude indique que les théorèmes de la géométrie d'Euclide peuvent se reformuler comme des théorèmes de la théorie des ensembles concernant les modèles de cette théorie.

Q : En utilisant la notion de “dénotation”, tu utilises pourtant une notion de vérité-correspondance.

R : Non, j'utilise une notion de vérité-démontrabilité. Je dis qu'une proposition a la dénotation “vrai” quand elle est démontrable et “faux” quand sa négation est démontrable. J'utilise aussi la notion de “avoir même dénotation que” pour dire “être prouvablement égal (ou prouvablement équivalent) à”. À aucun moment je ne suppose que toutes les propositions ont “vrai” ou “faux” pour dénotation.

Q : Mais Frege définit la notion de sens d'un énoncé comme les conditions auxquelles cet énoncé dénote le “vrai” (au sens de la vérité-correspondance).

R : C'est pour cela que je me suis référé à la définition donnée par Dummett du sens comme comme conditions d'assertabilité (de démontrabilité) et non à la définition originale de Frege.

Q : La définition du sens que tu as utilisée est assez différente de celle de Frege, également parce que, pour Frege 2^4 et 4^2 ont la même dénotation, mais pas même sens, car le mode de donation de l'objet n'est pas le même. Même s'il y a quelque chose de plus proche entre 2^4 et 4^2 qu'entre 2^4 et n'importe quelle autre définition du même objet.

R : Si on suppose que 2^4 et 4^2 ont des sens distincts, je ne vois pas ce qui pourrait avoir même sens que 2^4, si ce n'est l'expression 2^4 elle-même. Si pour avoir même sens, deux expressions ou deux propositions doivent avoir exactement le même mode de donation, “avoir même sens” devient synonyme de “être la même expression”. Dans ce cas la notion de sens n'apporte plus grand chose. L'égalité de sens me semble être intermédiaire entre l'égalité de dénotation et l'égalité syntaxique.

Q : Cela dit, on peut penser que dans certaines situations 2^4 et 4^2 ont le même sens, et dans d'autres non, puisque ce qui est implicite peut varier en fonction des interlocuteurs.

R : Oui.

Q : Cette démarcation entre ce qui est vrai par le calcul et ce qui demande une démonstration peut se comparer avec la démarcation des propriétés d'anneau des entiers relatifs au sein de toutes leurs propriétés.

R : Oui, dans les deux cas on isole un sous-ensemble des connaissances qu'on utilise.

Q : Il y a une stratégie de la démarcation entre calcul et déduction. On pose la ligne de démarcation pour certaines raisons.

R : Oui, on cherche à pousser la démarcation le plus loin possible. Mais on peut toujours la pousser encore un peu.

Q : Parmi toutes ces connaissances, quelles sont celles qui sont justiciables d'un traitement par le calcul ?

R : Il y a l'élimination des coupures, ce qui fait déjà pas mal de choses.