CERCLES VICIEUX, MATHÉMATIQUES ET FORMALISATIONS LOGIQUES[1]

Giuseppe Longo
CNRS et Dépt. de Mathématiques et Informatique
École Normale Supérieure, Paris
http://www.dmi.ens.fr/users/longo

Resumé
Dans ce texte on analyse brièvement, et d'une façon essentiellement accessible à un lecteur humaniste, certains formes de "circularités" logiques et mathématiques (auto-appartenance, auto-application, imprédicativité ....). On essaye tout d'abord de les comprendre comme "propriétés de fermeture" de certaines structures mathématiques, qui leur donnent un sens. En fait, nombreuses circularités peuvent être comprises comme des "solutions de systèmes d'équations". La réflexion philosophique qui en suit essaye de souligner le rôle que ces circularités logiques et mathématiques ont et peuvent encore plus avoir dans nos tentatives de rendre le monde intelligible par les mathématiques.

Summary
In this text, we briefly analyse, in a style which should be accessible to a non-mathematician, some forms of circularity in Logic and Mathematics (self-membership, self-application, impredicativity ...). We then try to unify them as "closure properties" of suitable mathematical structures, which give meaning to them. As a matter of fact, the main circularities may be understood as "solutions of systems of equations". The ensuing philosophical reflection stresses the positive role that the logico-mathematical circularities have and may even more have in our endeavour to make the world intelligible by mathematical tools.

Introduction

Dans les phénomènes naturelles, mais aussi dans ceux de la pensé et dans les constructions conceptuelle, on trouve maintes formes de "circularités". Il est bien difficile de les classer, car elles se présentes sous des formes et dans des contextes très différents. On peut en citer quelques unes, en commençant par la Physique.

Considérez le "plus simples" des systèmes dynamiques : trois corps ou plus dont le mouvement est seulement réglé par la loi newtonienne de gravitation universelle. La position, la vitesse et l'accélération de chaque corps est déterminé par la position, la vitesse et l'accélération de chaque

[1] Texte d'une conférence invitée, Coll. **Logique et Sciences Humaines**, Paris, Juin 1998. Publié dans "Mathématiques et Sciences Humaines", n. 151, 2000 (http://www.ehess.fr/centres/cams/publica/msh.html).

autre corps : on ne peut pas isoler un des corps et en étudier le mouvement, car celui-ci dépend du mouvement du *système*, dans sa globalité. Le système n'est pas "stratifié". Ce problème était clair à Newton lui même et, au cours du siècle dernier une grande quantité de travail mathématique remarquable fut dédié au traitement de cette "circularité", au coeur de problèmes physiques d'importance énorme (notre système solaire en fournit un bon exemple). Poincaré, vers la fin du siècle, démontra les difficultés essentielles pour la solutions des systèmes d'équations différentielles qui décrivent ces systèmes dynamiques: elles sont due à cette circularité *physique* du système et elles en donnent la contrepartie mathématique, conceptuelle.

Passons aux phénomènes de la vie. Tout d'abord chaque être vivant représente une "unité systémique", au moins aussi complexe et "intercorrélée" que les systèmes dynamiques de la Physique. On ne peut pas comprendre les fonctions, la nature même d'une partie, d'un organe, sans la comprendre dans l'unité de l'organisme, en fait dans son rapport et ses maintes liaisons avec son écosystème. Souvent en effet des organismes différents semblent liés dans une unité systémique plus grande, par des phénomènes de symbiose, par exemple, ou d'échanges vitaux dans les quels on peut pas dire qui est "ce qui vient le premier", au cours de l'évolution, par exemple.

Que dire des processus mentaux? Le regard sur soit même, la conscience de notre propre conscience ... les réflexions cognitives sur la cognition humaines et autres jeux de mots qui sous-tendent des vrais problèmes de représentation conceptuelle.

Dans certains cas, les mathématiques aident a traiter ces problèmes ou, au moins, elles donnent des clarifications, traitent des cas particuliers, représentent avec rigueur certains systèmes. La Logique Mathématique, en particulier, a permis l'analyse et a proposé des solutions pour certaines circularités présentes dans le langage des mathématiques. On discutera d'abord de trois formes fondamentales de "circularités" traitées en Logique Mathématique, tout en essayant de trouver le sens de la méthode commune de solution : on verra en particulier que ces circularités syntactiques trouvent des solutions dans la preuve de la *fermeture*, par rapport à certains opérations, de certaines structures algébriques ou géométriques. On esquissera aussi quelques éléments du problème tel qu'il se pose dans d'autres secteurs des mathématiques.

La leçon qui devrait en traire le lecteur humaniste, philosophe ou simplement non-mathématicien, s'il y en a une, c'est que ces apparents paradoxes dans le monde ou dans nos descriptions du monde sont des défis au coeur de nos formes de connaissance, des vrais "challenges", et que les mathématiques ont su, dans certains cas (très peu à vrai dire), en donner des belles explications, sinon solutions, ou, plus simplement, des représentations efficaces, instructives, quoique très spécifiques. Un lien peut-être important ou possible entre physique, vie et pensé, d'un coté, et représentation mathématique, de l'autre.

1. Équations et Algèbre

Commençons par un cas très simple et très ancien. Ma fille revint un jour bien triste de l'école car elle n'avait pas compris comment résoudre un problème que l'enseignant lui avait posé. Dans une famille, le père a quatre ans plus que la mère, qui, à son tour, a 18 plus de la moitié de l'age du père: en déduire l'age x du père et y de la mère. Il lui paraissait impossible : comment connaître l'age de la mère, qui dépend de celui du père, qui dépend à son tour de celui de la mère ... . Ma fille ne prononça pas le mot "circularité", mais il était presque sur ses lèvres.

Heureusement, dans ce cas, je pu facilement l'aider à reconstruire la solution du problème, dont elle avait en fait les outils. Il suffit d'écrire un petit système d'équations linéaires:

$$x = y + 4$$
$$y = 0{,}5x + 18$$

Mais ce système aussi n'est pas mal circulaire : x est fonction de y qui est fonction de x.

Les maths toutefois s'en sortent très bien, quoique le traitement de ce problème n'a pas été simple, dans toute sa généralité : il a fallu construire le corps des **nombres rationnels**, fermé par addition, soustraction, **multiplication** et **division**. Une construction qui ne fut pas immédiatement évidente pour les grecques : est ce que on peut diviser une grandeur par une grandeur? Ils se demandèrent très longtemps. Et il fallut attendre l'algèbre des arabes, Fibonacci de Pise et la théorie des nombres pour avoir des méthodes générales et uniformes de solution. C'est donc une propriété de fermeture d'une structure mathématique, le corps des rationnels, qui permet la solution du problème. En fait cette structure a été construite justement pour résoudre ce genre de problèmes. Elle explique ou "étale" la circularité ou la transfère, si on veut, sur une construction d'une autre nature : la fermeture algébrique demandée aussi est une forme de circularité, mais elle est un *théorème*, une conséquence facile de la construction des nombres rationnels à partir des entiers, qui n'a rien de circulaire. Une circularité syntactique donc, dans la définition informelle du problème, mais aussi formelle (les deux équations), est *expliquée* par un théorème de fermeture (sémantique). La structure mathématique interprète, donne signification au jeu circulaire de symboles.

2. Ensembles non-bien-fondés

Commençons cette fois par "la fin", c'est à dire par les tous derniers problèmes qui ont plus fortement contribué a revitaliser un débat en Théorie des Ensembles qui avait été étouffé au début du siècle.

En Informatique, ils existent nombreux exemples de procès qui ne s'arrêtent pas. Un système d'exploitation, par exemple, marche toujours. On n'éteint pas les ordinateurs modernes : ils sont toujours prêts à recevoir un input, y travailler, donner un résultat, attendre un autre input ... . Pour

cela, en Informatique, on utilise aussi la notion de "stream". Par exemple, $f(n) = (n, f(n+1))$ est le "stream" $(0, (1, (2, \ldots),$ qui définit la fonction f : une définition de fonction tout à fait inhabituelle en Mathématiques, mais d'usage commun dans certains secteurs de l'Informatique Théorique.

Un peu plus en général, un **système de transition** x, sur un ensemble A de constantes, un système d'exploitation par exemple, produit $a \in A$ et, après, il continue à faire x. Il y a maintes façons pour formaliser ce phénomène; on peut par exemple écrire que

$$x = (a,x).$$

Or, x sera une suite de symboles, qui représentent le calcul, et a le résumé des actions à faire (lire, calculer, écrire).

En général, il s'agit d'ensembles non structurés ou de listes de symboles. La Théorie des Ensembles est donc le contexte privilégié pour aborder ces problèmes. Suivant la notation ensembliste de paire la plus canonique, on écrit alors $(a,x) = \{\{a\},\{a,x\}\}$. Notre équation devient dans ce contexte

$$x = \{\{a\},\{a,x\}\}.$$

Mais il y a ici quelque chose qui cloche : l'ensemble x est défini en terme de soi même, car x en est un élément d'un ensemble qui ... est un élément de x. Mais il y a pire. Parfois les processus, en Informatique, se croisent : il font des calculs en concurrence. Chacun procède en échangeant des messages avec l'autre ou en utilisant les résultats du calcul de l'autre :

$$x = (a,y)$$
$$y = (b,x)$$

x fait a, ensuite relance à y, qui fait b et fait appel à x. En termes ensemblistes,

$$x = \{\{a\},\{a,y\}\}$$
$$y = \{\{b\},\{b,x\}\}$$

Ce système ressemble beaucoup aux équations de la §.1. Mais maintenant c'est n'est plus la vieille crainte du géomètre grecque, mal à l'aise avec le calcul algébrique, qui nous empêche de travailler, c'est plutôt l'interdit de Russell, contre les définitions "circulaires", qui nous tombe sur la tête:

«Whatever involves all of the collection must not be one of the collection» (B. Russell, 1908).

Cet interdit, au cours de ce siècle, à aidé a construire des théories logiques remarquables, par richesse mathématique et clarté conceptuelle : le monde, stratifié, propageait la "certitude" du bas, les atomes, vers le haut, en les composant par niveaux bien différenciés. Le travail en Théorie des Ensembles et Logique de Zermelo, Fraenkel, von Neumann, Bernays, Gödel et maints autres mathématiciens se plasma autour de la Théorie des Types de Russell (sans toujours respecter la forme la plus stricte de stratification); le nom et la méthode fut aussi à l'origine des Théories des Types de Church à Martin-Löf à Girard (théories au coeur de mes intérêts depuis longtemps, mais la théorie de ce dernier violait dès sa première formulation l'interdit, comme on verra).

Quant à l'Informatique, l'importance de la notion de type peut être comprise par analogie avec la Physique Mathématique. "Type", en Logique, correspond à ce qui est, en Physique, le concept de "dimension". En particulier, les termes des équations de la Physique possèdent des dimensions (force, vitesse, accélération ...). Voila donc l'intérêt du typage dans les langages de programmation : le contrôle des types donne une méthode partielle, mais efficace, de contrôle de la correction d'un programme. Si le programme est bien typé, il a des bonne chances d'être correct (bien conçu, bien écrit); il n'en a aucune s'il est mal typé. Exactement comme une équation de la Physique, dont la dimension doit être la même, avant et après les calculs, pour que elle soit correcte.

Cette application du typage est une des motivations des plus récentes et importantes pour l'actualité des Théorie des Types; elle est au moins aussi importantes que la recherche des "certitudes stratifiés", qui en ont motivé l'essor en Logique. Le fait que les types correspondent bien au dimensions de la Physique nous confirme qu'il s'agit d'une belle construction, efficace comme la notion de force ou accélération en physique. Mais les mathématiques sont des *constructions possibles* : d'autres parcours de ceux qui en ont été à l'origine peuvent avoir des retombées au moins aussi importantes sur la compréhension du monde. Comme l'on verra, on peut avoir même des Théories de Types qui gardent leur fonctions clés (le contrôle de correction partielle, par exemple) et qui, toutefois, représentent des circularités fortement expressives.

Revenons donc à nos équations circulaires dessus, où $x \in x$ et $y \in x \in y$. Comment s'en sortir? Comme dans la §.1, avec les équations linéaires : il faut construire une structure mathématique qui soit fermée par rapport à la "bonne" notion structurelle, correspondante à la formalisation équationnelle (et à l'intuition qui nous l'a imposé). Bref, il faut construire des univers (ensemblistes) qui soient fermés par des **chaînes descendantes**, car si on admet $... x_n \in x_{n-1} \in ... \in x_o$ on a aussi $x \in x$ et $y \in x \in y$. Il s'agit de concevoir des structures fermées par ces chaînes, comme les rationnels sont fermés par les opérations impliquées dans les équations linéaires, la multiplication et la division. Si on libère l'esprit des interdits des pères fondateurs, ceci n'est pas difficile à concevoir, car, après tout, la notion d'appartenance "$\in$" n'est qu'un ordre partiel et rien n'empêche de "voir" des ordres (partiels) descendants : la suites des entiers relatifs, par exemple. Mais gardez même votre bonne intuition de platoniciens naïfs et continuez à comprendre "$\in$" comme "vraie" appartenance d'un ensemble à un autre : qu'y a-t-il de mal à concevoir une chaîne descendante d'ensembles $... x_n \in x_{n-1} ... \in x_o$, de plus en plus petits ? Depuis deux ou trois siècles nous avons l'habitudes, en mathématique, de concevoir des limites, des infinitésimaux, des suites "décroissantes" sans fin et des algèbres, les nombres réels, fermés par ces suites infinies. Pourquoi les nombres pourraient être de plus en plus petits, tandis que les ensembles ne pourraient pas se réduire, en se télescopant l'un dans l'autre, au de là de ce qu'on peut voir par n'importe quel microscope ? Non, pour les "purs et durs" de la stratifications, les nombres, nos mesures du monde, peuvent se réduire arbitrairement, tandis que les ensembles

commencent, bien visibles, au niveau des "atomes" (les urelements des théories des ensembles avec atomes) ou, pire, démarrent avec le vide Ø et, puis, par un acte de création parenthétisée, donnent l'Univers : {Ø}, {{Ø}}, {{{Ø}}}, ...

2.1 Axiomes d'Anti-Fondation (AFA).

Au début du siècle, les Théories des Ensembles de Cantor et Frege durent être sérieusement revue par un paradoxe trop connu. On pouvait s'en sortir de plusieurs façons : en restreignant le domaine de la négation, en admettant la formation d'ensembles seulement à partir d'ensembles (axiome de compréhension restreint), en stratifiant l'univers des ensembles par des types. La première solution fut privilégié dans l'approche fonctionnel de Church, dont on parlera dans la §.3; les deux dernières solutions furent bien plus largement retenues et développées, en ajoutant généralement un conditions supplémentaires : pas de chaînes descendantes d'ensembles ou "tout ensemble est bien-fondé" (**Axiome de Fondation**, Fraenkel, 1922, et von Neumann, 1925). Seulement quelques mathématiciens isolés, comme Mirimanoff en 1917 et Finsler en 1926, eurent l'audace d'explorer des sentiers dangereux : les ensembles "extraordinaires" de Mirimanoff n'étaient pas bien-fondés. D'autres à citer sont Specker, en 1957, Dana Scott, dans une note célèbre, mais non publiée de 1960, et Boffa, en 1967 : ces travaux démontraient entre autre l'indépendance de l'Axiome de Fondation, en construisant des modèles non-bien-fondé des Théories des Ensembles plus à la mode, comme ZF, NBG (voir [Aczel,1988] pour une brève histoire de ces chaînes infinies en Théorie des Ensembles). On peut donc avoir Types, Ensembles et Classes, comme dans ZF, NBG etc ... sans Axiome de Fondation : on peut violer l'interdit de Russell et travailler dans des cadres bien solides.

Au cours des années '70, Ennio De Giorgi, qui enseignait Analyse Mathématique à la Scuola Normale Superiore de Pise, animait un séminaire de Logique[2]. Dans ce séminaire, il proposa, avec l'audace et la naïveté du grand mathématicien, un cadre original pour les fondements de l'Analyse, qu'il aimait appeler la "Théorie Cadre". Puisque les mathématiciens n'aiment pas des restrictions a priori dans leurs constructions conceptuelles (encore moins si dictés par des logiciens en quête de certitudes), il inventa une série d'axiomes, qu'il dénomma de "libre construction", de nature essentiellement algébriques. Parmi ces axiomes, il y avait différentes constructions possibles de chaînes descendantes. Marco Forti et Furio Honsell, qui participaient à ce séminaire, comme tout mathématicien intéressé à la Logique à Pise, développèrent la "Teoria Quadro", en ajoutant leur propres idées, [Forti&Honsell,1983]. Leur travail est considéré un pivot de l'analyse des axiomes

[2] Ennio De Giorgi est décédé quelques mois avant la date de ce colloque. Son enseignement, ses idées, son enthousiasme, son talent extraordinaire ont été pour moi, et pour plusieurs générations de mathématiciens italiens, le point de départ de notre travail et une référence permanente.

d'anti-fondation (AFA, anti-foundation axiom) : des références à leurs nombreux articles se trouvent dans [Aczel,1988] et [Barwise&Moss,1996].

Voyons donc de quoi il s'agit. Un système d'équations comme

$$x = \{a,y\}$$
$$y = \{b,x\}$$

spécifie une fonction e de l'ensemble $X = \{x,y\}$ des variables dans l'ensemble $P(X \cup A)$ des parties de X et $A = \{a,b\}$, les valeurs constantes : dans ce cas, $e(x) = \{a,y\}$, $e(y) = \{b,x\}$.

Définition *Un **système (plat) d'équations** est un triplé $E = (X,A,e)$, où X et A sont des ensembles disjoints et e est un fonction de X dans $P(X \cup A)$. Une **solution** s et une fonction de domaine X dans l'univers des ensembles telle que*

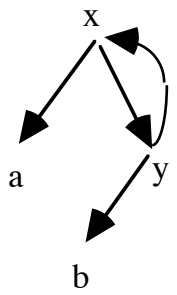
$$s(x) = \{s(y) / \ y \in b(x)\} \cup c(x)$$

où $b(x) = e(x) \cap X$ est l'ensemble des variables des quelles x dépend immédiatement et $c(x) = e(x) \cap A$ est l'ensemble de constantes des quelles x dépend immédiatement.

Axiome d'Anti-Fondation (AFA) *Tout système (plat) d'équations E a une et une seule solution s.*

On peut facilement donner un simple modèle de l'anti-fondation sur les graphes. Un **arbre** est un ordre partiel, avec un plus grand élément r (la racine) et tels que pour tout élément a (noeud ou feuille) de l'arbre il existe une seule chaîne $a \leq ... \leq r$. Les arbre sont stratifiés : ils n'ont pas de cycles. Un **graphe** est un ensemble de noeuds et de relations orientées entre noeuds : donc les arbres sont, en particulier, des graphes connectés, avec élément maximum et sans cycles. Évidemment, graphes et arbres mathématiques peuvent être infinis.

Les arbres permettent d'interpréter la "bonne-fondation", si l'ordre partiel interprète "$\in$", dans le sens que $a \leq b$ (a est un **fils** de b) interprète $a \in b$. Les graphes avec cycles donnent des modèles pour l'anti-fondation. Celui en figure est une solution du système d'équations $x = \{a,y\}$ et $y = \{b,x\}$.



Plus en général, une **décoration** d'un graphe est une affectation d'un ensemble a chaque noeud du graphe, telle que les éléments de l'ensemble affecté à chaque noeud sont les ensembles affectés à ses fils. L'axiome AFA devient alors :

Chaque graphe a une et une seule décoration.

Il est clair que l'égalité entre ensemble (ou axiome d'extensionalité) se complique : on ne peut pas contrôler simplement si, à chaque niveau de la stratification, il y a les mêmes éléments, comme en présence de l'Axiome de Fondation. On peut toutefois définir la notion de "bisimulation", sorte de comparaison entre ordre partiel, qui force l'égalité des ensembles. Il arrive que cette même notion, pour laquelle on renvoi à [Aczel,1988] et [Barwise&Moss,1996], est très importante en Informatique. Elle permet de comparer des procès différents qui procèdent en s'échangeant des messages, comme dans le "Calculus of Comunicating Systems" [Milner,1991] : en fait, l'analyse sémantique du calcul de Milner est à l'origine des travaux des Aczel sur AFA. Et la plupart des systèmes d'ordinateurs sont, aujourd'hui, distribués et concurrents et toujours en fonction.

D'autres applications sont présentées dans [Barwise&Moss,1996] (sémantique de la logique modale, automates déterministes ...). Ce texte donne aussi une preuve de cohérence relative de la Théorie ZFA = ZFC+AFA (Zermelo-Fraenkel avec Axiome de Choix et AFA). On y construit en effet, à partir d'un modèle de ZFC, un modèle de ZFA.

3. Définitions récursives de fonctions et de types.

En Arithmétique on défini souvent des fonctions par **récursion**; informellement, une fonction est définie récursivement si elle est définie en terme d'elle même. Une simple définition **récursives primitives** est la définition de la fonction factoriel $f(n) = n!$:

$$f(0) = 1 \text{ et } f(n) = n \times f(n-1).$$

Donc $n! = n \times (n-1)! = 1 \times 2 \times 3 \ldots \times n$.

Parfois, la récursion peut apparemment mélanger langage et métalangage :

$$expo(x,n) = x \times x \times \ldots \times x \qquad \text{"n fois"}$$

où "n fois" de cette définition informelle reste en dehors du langage objet (celui auquel appartiennent les symboles de fonctions et les opérations arithmétiques de base). Toutefois, en écrivant

$$expo(x,0) = 1 \text{ et } expo(x,n+1) = x \times expo(x,n)$$

on peut traiter le problème : ces fonctions se décrivent très bien dans maints systèmes pour la calculabilité, en particulier si on observe que (..)!, le factoriel, et expo sont des points fixes de certaines expressions, celles décrites à la droite des équations qui les définissent formellement.

Le premier de ces systèmes fut la **Logique Combinatoire** de Curry (1929). Inspiré par des idée en algèbre de Schoenfinkel (1924), il s'agit d'un jeu formel de règles basé sur deux symboles **S** et **K** et deux axiomes **K**MN = M et **S**PQR = PR(QR), qui permettent de manipuler

formellement toute suite finie de **S** et **K**. Ensuite, Herbrand et Gödel proposèrent des systèmes de fonctions, plus "mathématiques", dans leurs fameux ouvrage de '30 et '31. Remarquable surprise, tous ces différentes théories, y compris les révolutionnaires Machines de Turing (1936), caractérisent la même classe de fonctions arithmétique, les fonctions **calculables** ou récursives partielles; un résultat démontré en '36 par différents auteurs, dont Kleene et Turing. Au coeur de la preuve d'équivalence se trouve le **λ−calcul** de Church (1932), une extension de la Logique de Curry, voir [Barendregt,1984] (les rapports entre la Logique Combinatoire et le λ−calcul et leurs modèles sont assez subtiles, voir [Hindley&Longo,1978]).

L'idée de Church fut d'exprimer formellement la *dépendance fonctionnelle* : si f(x,y), par exemple, est une fonction de deux variables, on "met en évidence" la dépendance de f par rapport à y par la **λ−abstraction** : λy.f(x,y). Alors, l'application de ce nouveau terme à un argument a, disons, dévient (λy.f(x,y))a = f(x,a). En considérant une variable à la fois :

$$\text{(Axiome } \beta) \qquad (\lambda x.g(x))a = g(a)$$

(l'opérateur d'abstraction λx.... **lie** la variable x (libre) dans g(x), comme { x / b(x) } lie x dans le prédicat b; l'axiome β explicite l'opération de remplacement).

Plus formellement, les **termes** du λ-calcul sont :

les variables x, y, z .... et b(c), λx.b, si b, c sont des termes.

Observez que on n'a pas interdit b(b). Donc λx.x(x) est un terme du langage. En fait, l'expressivité computationnelle du λ-calcul, se base justement sur la possibilité de décrire dans le langage le terme

$$\mathbf{Y} = \lambda y.\lambda x.(y(x(x)))(\lambda x.(y(x(x))))$$

basé sur l'autoapplication. Il est bien facile d'observer, en utilisant l'axiome (β), que **Y**(b) = b(**Y**(b)), pour tout terme b. Si on pose donc pour $f_o = \mathbf{Y}(b)$, alors $f_o = b(f_o)$. Bref, f_o est définie récursivement, en termes de b, ou f_o est le point fixe de b.

Toutefois, il ne faut pas oublier que ces systèmes étaient proposés pour travailler en Théorie de la Démonstration et pour y exprimer les mathématiques et leur logique. On voulait donc avoir dans le langage un terme pour la négation, disons neg; mais alors, pour $f_o = \mathbf{Y}(neg)$, on a $f_o = neg(f_o)$, ce qui contredit la signification "entendue" de neg (paradoxe de Curry,1932).

Notez comme ce paradoxe ressemble à celui de Russell en Théorie des Ensembles : si on interprète x∈x par x(x) et "l'abstraction d'ensembles", { x / b}, par l'abstraction fonctionnelle λx.b, on obtient alors un autre terme fort intéressant, qui est **Y** sans les variables y,

$$(\lambda x.x(x))(\lambda x.x(x)) \approx \{x / x \in x\} \in \{x / x \in x\}$$

Comme dans le cas de la Théorie des Ensembles, on peut s'en sortir de différentes façons : empêcher, par l'interdit russellien, que un terme b s'applique à soi même, en stratifiant les termes en différents types, ou restreindre (ou enlever) la négation du langage et laisser b(b).

Une conséquence de cette deuxième audace est donc l'existence, dans le langage, du terme

$(\lambda x.x(x))(\lambda x.x(x))$, qui ne termine pas : appliquez l'axiome (β) et vous verrez que le terme entre immédiatement dans un cycle. Rien de grave, la divergence essentielle ou "non-arrêt", n'est pas un défaut, comme l'Informatique démontra plus tard : le "paradoxe de Russell" se transforme encore une fois en une richesse expressive, si au lieu de se poser des interdits, on l'analyse mathématiquement. En fait, la Logique Combinatoire et le λ–calcul sans types ont une grande expressivité : les fonctions partielles récursives (les fonctions qui peuvent diverger) sont "strictement plus" des fonctions totales, car pas toute fonction récursive partielle admet une extension totale récursive. Et c'est ainsi que l'on arrive à calculer la même classe que les systèmes de Herbrand, Gödel et Turing. De plus, en absence de négation explicite dans le langage, il n'y a pas de paradoxes, car la **cohérence** est démontrée par le Théorème de Church-Rosser (1936) : un de ses corollaires nous assure que pas toute égalité entre termes est dérivable.

3.1 Sémantique Mathématique

Toutefois, un problème se pose : quelle est le *sens mathématique* de l'auto-application, c'est à dire de x(x) ou f(f), mais aussi des **SSK(SK)KK** "sans signification" de la Logique Combinatoire ? Existe-t-elle une "structure mathématique" telle que ses éléments, ses fonctions, puissent "s'appliquer" à eux-mêmes ?

Il suffirait de construire un espace X qui soit *isomorphe* à son propre espace $X \to X$ (ou X^X) de fonctions (ou endomorphismes) : alors un élément serait aussi une fonction (à isomorphisme près), une fonction serait un élément et on pourrait interpréter l'application formelle, linguistique, par l'application fonctionnelle, en fait de "tout élément à tout élément".

Bref, il suffit de résoudre, comme dans les cas précédents, des équations, en fait l'équation :

$$(1) \quad X = X \to X$$

où "=" est l'isomorphisme, dans une catégorie d'objets à construire, comme il fallut construire, à partir des entiers, les rationnels, les réels, ou, dans un modèle de ZFC, les ensembles avec des chaînes descendantes. Les mathématiques des "domaines de calculabilité" (Scott, 1970) permettent de résoudre maintes équations bien plus complexes, comme

$$X = A + B \times X + X \to X$$

où les inconnus sont à interpréter comme des *ensembles structurés* ou des objets de catégories non-triviales (voir [Amadio,Curien,1998] pour une synthèse récente). La difficulté devrait être claire : sauf si l'on prend X égal à un singleton, aucun ensemble fini ou infini peut satisfaire l'équation (1); mais le singleton est très peu intéressant, car $X \to X$ (et donc X) doit contenir toutes les fonctions calculables.

La solution de Scott se base sur la construction d'une catégorie d'espaces topologiques dont on démontre qu'elle est *fermé par les limites de certaines chaînes descendantes d'exponentiels* (limites inverses):

$$... < D_n < D_{n-1} < ... < D_o$$

où "<" est une "immersion isomorphe" et $D_n \equiv D_{n-1} \rightarrow D_{n-1}$ est le domaine des endomorphismes continues sur D_{n-1} : à la limite, on obtient $D_\infty = D_\infty \rightarrow D_\infty$. Dans un certain sens, il s'agit de montrer la structure "non-bien-fondée" de certaines catégories, par rapport à "<", et de construire des limites.

Encore une fois, donc, une propriété de fermeture d'une structure mathématique suffit à résoudre la "circularité" syntactique. L'apparent paradoxe est interprété par un très beau théorème de fermeture; ses développements en Théorie des Catégories permettent une analyse fine des différentes structures sémantiques pour la Logique Combinatoire, le λ-calcul et d'autres systèmes pour la calculabilité (voir [Smith&Plotkin,1982], par exemple; dans [Longo&Moggi,1991] et [Longo,1984] on caractérise les modèles de la Logique Combinatoire, en termes catégoriques, et on classifie les modèles d'autres théories).

Les applications en Informatique de cette méthode ont été nombreuses, car, en programmation, on défini souvent des **types des données** par des équations du gendre (un type, en Informatique, aussi bien qu'en Logique, est une "collection" de données):

$$\begin{aligned} \text{Valeurs} &= \text{Constants} + \text{Closures} \\ \text{Environnements} &= \text{Variables} \rightarrow \text{Valeurs} \\ \text{Closures} &= \text{Variables} \times \text{Expressions} \times \text{Environnements} \end{aligned}$$

forme plus complexe, mais tout à fait similaire, de l'équation (1) plus haut (voir aussi [Amadio,Curien,1998]).

Les méthodes de solution de ces équations, en tant que *définitions récursives de types*, donnent facilement une signification (une solution) aussi aux *définitions récursives de fonctions*. En effet, ces solutions sont données dans des catégories dont les morphismes sont des fonctions continues; alors une définition récursive (de fonction) est interprété comme point fixe, à la Knaster-Tarski, d'une fonction (d'un fonctionnel) continu, voir [Scott,1970-1980; Amadio&Curien,1998].

4. Théories imprédicatives des Ensembles et des Types

Ensembles

Un ensemble b est **défini imprédicativement** si il est donné sous la forme

$$b = \{ x \mid \forall y \in A.P(x,y) \}$$

(l'ensemble des x tel que pour tout y dans A on a P(X,Y)) où b peut être un élément de A, c'est-à-dire de la collection qui sert à le définir.

En fait, l'ensemble infini plus important qui soit, les entiers **N**, est défini, en logique classique, d'une façon imprédicative:

$$\mathbf{N} = \{ x \ / \ \forall X \, (\forall y \, (y \in X \ \rightarrow \ y+1 \in X) \ \rightarrow \ 0 \in X \ \rightarrow \ x \in X) \}$$

où X "varie" sur une collection d'ensembles qui contiennent N (ou X peut-être l'ensemble **N** même que nous sommes en train de définir).

Le définition que nous venons de donner est au **second ordre**, car elle utilise des variable (majuscule) dont on suppose que la signification soit différente de celle des variables du premier ordre (minuscules): elles varient sur des ensembles, aux quels appartiennent, en tant que éléments, les interprétation des variables du premier ordre. La Théories Descriptives des Ensembles, par exemple, fait un vaste usage des définitions imprédicatives au second ordre, comme l'axiome de compréhension que l'on vient d'utiliser pour définir **N**, voir [Moschovakis, 1980]. Le continu mathématique, avec ses bornes supérieures et inférieures et en tant "tout" imprédicativement lié à ses parties, est aussi communément donné de façon imprédicative; la représentation de l'espace et, surtout, du temps phénoménologique y gagne énormément (en Analyse le problème se pose depuis H. Weyl et a été traité en profondeur par maints logiciens, e.g. Kreisel, Wang, Shutte, Feferman, Simpson ... , avec des philosophies bien différentes de celle de cet auteur, voir [Longo,1987; Longo,1998]).

Types

Dans le système F de J.-Y. Girard on quantifie aussi au second ordre. En bref, si on définie

Types = "la collection de tous les types"

(ou de toutes les propositions), on admet dans le langage le *type* $\forall X \in \text{Types}.A$, pour tout type A. C'est-à-dire, on forme un nouveau type, $\forall X \in \text{Types}.A$, en utilisant la quantification sur la collection de *tous les types*, dont fait partie ce même type que nous sommes en train de définir. Plus ou moins formellement:

$$(\forall X \in \text{Types}.A) \in \text{Types}$$

Grâce à cette forte circularité le système est très expressif. Premièrement, ses termes sont tous typés, on ne perd pas, donc, ce contrôle partiel de correction que les types permettent (que l'on a comparé au contrôle de dimension en physique) et qui est absent dans les systèmes sans types. De plus, il permet aussi de décrire à son intérieur une quantité remarquable de fonctions récursive: toutes celles démontrablement totales dans l'Arithmétique du second ordre, ce qui est vraiment beaucoup (voir [Girard&al.,1989]

Malgré cette forte circularité, le système est démontrablement cohérent. Un théorème (difficile) de normalisation garantie l'impossibilité de la dérivation d'une contradiction. Les enjeux de la preuve sont, en bref, les suivants. D'abord, une "forte charge inductive" (ce qui entraîne directement sa version forte, entre autres). Dans l'induction on utilise le lemme de König. Ce lemme n'est pas constructif, dans le sens de l'intuitionnisme orthodoxe. Il dit: "tout arbre infini à branchement fini possède une branche infinie". Le problème est que, même si les noeuds de l'arbre

sont étiquettés et l'arbre est "effectivement engendré" (il est construit par une fonction, un processus calculable), un ordinateur ne pourrait pas trouver la branche infinie (plus précisément: on ne peut pas donner une règle, écrire un programme, de génération de la branche infinie, car l'ordinateur devrait faire des allées retour d'explorations, en effaçant et reconstruisant sa mémoire d'une façon non effective).

En plus, la preuve à la Tait-Girard se base sur un axiome de compréhension du second ordre imprédicatif, comme ceux utilisés en Théorie des Ensembles:

$$\exists X.\forall x(x\in X \leftrightarrow A(x)).$$

Cet axiome permet de "construire" un type à partir d'une formule A arbitraire (voir [Girard&al.,1989] pour les détails).

4.1 Sémantique Mathématique des Types Imprédicatifs

Encore une fois il s'agit de construire des structures mathématiques, des catégories en fait, qui soient fermées pour les opérations entendues. Mais quelles opérations? Une quantification universelle, comme celle qui apparaît en $\forall X\in Types.A$, est une conjonction infinie ("pour tout X, A est vrai"). Or, la signification catégorique de la conjonction logique "&" est le produit "×", le produit cartésien bien familier. Il faudra donc construire une catégorie qui soit fermée par produits infinis et *indexés sur elle même*. Or, la Théorie des Catégories donne des notions très précises qui correspondent, avec rigueur, à cette intuition de produit infini, dans le cas du premier ordre, depuis les travaux de Lawvere, ainsi qu'au second ordre (voir [Lambek&Scott,1986; Asperti&Longo,1991]). Informellement, si la (collection des objets de la) catégorie, disons $\mathbf{C}$, interprète (la collection) Types, il faut interpréter

$$(\forall X\in Types.A) \in Types$$

comme la possibilité que $\mathbf{C}$ contienne le produit qui interprète $\forall X\in Types.A$, disons $\Pi_{X\in\mathbf{C}}\ A$, un produit qui, dans le modèle, est indexé sur la catégorie $\mathbf{C}$ elle-même. Bref, il faut associer les notions formelles à gauche aux structures à droite dans le schéma suivant:

$$\begin{aligned} Types &\sim \mathbf{C} \\ \& &\sim \times \\ \forall X\in Types.A &\sim \Pi_{X\in\mathbf{C}}\ A \\ (\forall X\in Types.A) \in Types &\sim (\Pi_{X\in\mathbf{C}}\ A) \in \mathbf{C} \end{aligned}$$

Une catégorie avec une telle propriété de fermeture s'appelle "petite complète" (small complete). Le fait qu'une catégorie relativement simple, construite sur les sous-ensembles des nombres entiers, soit petite complète, fut remarqué en 1984 par Eugenio Moggi à Pise (dans un message de courrier

électronique (!), un système d'échange d'information qui venait de démarrer). Son idée a été développée par maints auteurs (voir [Hyland,1988; Pitts,1987;Longo&Moggi,1991]). Encore une fois, une propriété de fermeture mathématique donne un sens très solide à une notion logique, les définitions imprédicatives de la Théorie des Types. Évidemment, on a pu ensuite construire plusieurs catégories avec cette propriété de fermeture (voir [Asperti&Longo,1991]).

Il y a une connexion facile à démontrer entre la sémantique à la Moggi et les modèles du système sans types. Toute structure catégorique qui satisfait l'équation $X = X \to X$ permet de construire un modèle de $(\forall X \in Types.A) \in Types$. Il ne paraît pas possible faire la construction inverse (pas tout modèle des types imprédicatifs permet de construire un modèle du système sans types). La relation entre anti-fondation et auto-application n'est pas bien connue non plus : il n'y a pas de résultats qui permettent ou interdisent de passer d'un modèle de l'une à un modèle de l'autre.

Le système de Types de Girard a eu maints applications, surtout informatiques. Certains **Langages de Programmation** se basent sur ce système (CLU, ML polymorphe, Quest, ...). Leur sémantique a été donnée dans les termes que l'on vient d'esquisser (e.g. [Cardelli&Longo,1991]. En **Démonstration Automatique**, Coq est une système construit sur une extension des types imprédicatifs (le **Calcul des Construction** de [Coquand&Huet,1988]).

4.2 Quantification Universelle et Preuves

Carnap, dans un article de 1931 sur Erkenntnis, défend contre Russell l'utilisation en Mathématiques des définitions imprédicatives. Son argument, en bref, est le suivant. L'enjeu d'une proposition mathématique est dans la possibilité de la démontrer (ou de pouvoir l'utiliser dans une preuve). Mais, comment prouvons-nous, en mathématiques, une propriété donnée sous forme imprédicative, disons $\forall X \in Prop.A$?

Normalement, on ne va pas "inspecter" tous les cas possibles, c'est à dire on ne démontre pas $[B/X]A$ pour tout B, ce qui inclurait le cas $B \equiv \forall X \in Prop.A$, en odeur de circularité. Plutôt, on démontre $[B/X]A$ pour B *arbitraire* ou *générique*. Bref, même pour comprendre le second ordre, il s'agit de faire référence au premier ordre, car, en mathématiques, on démontre une propriété $\forall x.P(x)$ des nombres réels, en prouvant $P(r)$ pour r arbitraire, sans inspecter tous les réels; le point essentiel étant que l'on n'utilise dans la preuve *que* le "type" de r et aucune autre propriété (spécifique) de r. Autrement dit, la preuve utilise seulement le fait que r est un réel (son type donc).

En Théorie des Types, ou les propositions sont des types et les preuves des termes, l'analyse des preuves est suffisamment fine pour nous permettre de mieux définir ce que c'est qu'une preuve par rapport à un élément "générique"; de plus, un résultat récent rend très solide les définitions imprédicatives données à son intérieur.

Dans le système de Girard, la preuve de $[B/X]A$ est un terme a tel que $a \in [B/X]A$. On dira

que B est **générique** et a est **prototype**, s'il existe a': A tel que [B/X]a' = a ∈ [B/X]A ([Fruchart&Longo,1998]). Par l'axiome (β), cela nous permet d'abstraire une preuve de l'énoncé général:

$$\lambda X \in Types.a' \in (\forall X \in Types.A)$$

car $(\lambda X \in Types.a')B = [B/X]a' = a \in [B/X]A$.

Est-ce que la définition de preuve prototype est une bonne définition? Est-ce qu'elle donne d'un façon "canonique" une preuve de $\forall X \in Types.A$? Pour une simple extension de la théorie de l'égalité entre termes, on a le résultat suivant:

Théorème (Généricité). *Soit a', a'' ∈ (∀X ∈Types.A). Si pour un type B, [B/X]a' = [B/X]a'', on a alors a' = a''.*

La démonstration est plutôt complexe (voir [Longo&al.,1993]). Elle assure que, si pour *un seul* type B, a' et a'' coïncident, alors il sont égaux partout. Donc, dès que l'on sait que a est une preuve prototype (ce qui est décidable), on a une preuve et une seule de la proposition (ou du type) universel *(le théorème n'est évidemment pas vrai pour la quantification au premier ordre !)*. En conclusion, au moins pour ce qui en est à la Théorie des Types, la méthode mathématique "des preuves prototype" sur "argument génériques" est bien licite et solide, même (et surtout) dans le cas imprédicatif (voir [Fruchart&Longo,1998]).

5. Le Théorème de Kruskal et la Forme Finie de Friedman

Nous montrerons ici le rôle d'un principe structurel du bon ordre et sa relation à l'imprédicativité dans la preuve, grâce à un exemple relativement récent et de très grand intérêt: la version finie du Théorème de Kruskal due à Friedman, connue comme FFF (Friedman's Finite Form, voir [Friedman,1981; Harrington&al.,1985]). FFF est un exemple récent et concret de l'incomplétude de l'Arithmétique formelle. C'est à dire, on donne un "simple" énoncé formalisable dans l'Arithmétique, FFF, que aucun principe de preuve purement syntactique et finitaire arrive à démontrer. Toutefois, le travail sur les structures d'ordre des entiers, des suites finies, des arbres finis et infinis, permet de démontrer l'énoncé, comme propriété des nombres entiers. De plus, l'énoncé implique un principe essentiellement imprédicatif: le bon ordre jusqu'au (premier) ordinal imprédicatif, comme on essayera d'expliquer.

5.1 Pas de désordre total chez les arbres

Une relation "≤" est un **pre-ordre** si elle est réflexive et transitive. Un pre-ordre est un **ordre partiel** si il est aussi antisymétrique, c-à-d. $x \leq y$ et $y \leq x$ implique $x = y$. Un ordre partiel est

total, si pour tout x et y, on a $x \leq y$ ou $y \leq x$. Il est **bien fondé** si il n'y a pas de suites infinies descendantes (c-à-d., $x_{i1} > x_{i2} > x_{i3} > \ldots$). Un **bon ordre** est un ordre total et bien fondé (ou, ce qui revient au même, tout sous-ensemble possède un plus petit élément). Une suite est un ensemble qui est donné dans un ordre (total), e.g. une suite dans A est une fonction $a : \omega \rightarrow A$, où ω sont les entiers et $a_n = a(n)$.

On démontre facilement que tout ensemble bien ordonné réalise l'induction.

5.1.1. Définition. *Un **arbre fini** T est un ordre partiel avec un plus petit élément, la **racine**, et tel que, si $a \in T$, alors $\{x / x \leq a\}$, la **branche** qui précède a, est totalement ordonné.*

Une **immersion** entre deux ordres partiels $(P, \leq)$ et $(P', \leq')$ est une fonction $h : P \rightarrow P'$ qui préserve les bornes inférieures (c-à-d. $h(\inf\{p,q\}) = \inf'\{h(p),h(q)\}$), donc monotone. On écrit $T \leq T'$ pour le pre-ordre sur les arbres induit par l'immersion.

5.1.2. Théorème (Kruskal, [Kruskal,1960]). *Pour toute suite infinie $\{T_n / n < \omega\}$ d'arbres finis, ils existent i et k tels que $i < k < \omega$ et $T_i \leq T_k$.*

Ce théorème énonce une propriété qui n'est pas du tout évidente: les arbres finis ne peuvent pas être "totalement désordonnés", car toute collection infinie en contient au moins deux "comparables", par immersion et dans l'ordre dans lequel on donne la suite. Mais alors, il ne peut pas y avoir:
(bf) - des suites infinies descendantes d'arbres (c-à-d., $T_{i1} > T_{i2} > T_{i3} > \ldots$),
(comp) - des suites infinies d'arbres tous incomparables,
et, donc, on prouve immédiatement que:

5.1.3 Corollaire. *Tout pre-ordre, qui soit une extension de la relation d'immersion entre arbres finis, est bien-fondé (c-à-d., il ne contient pas des suites infinies descendantes: propriété (bf) dessus).*

L'importance de ce simple corollaire est due aux faits suivants, qui sont difficiles à démontrer. Il faut commencer par donner une fonction qui ait comme domaine les arbres et codomaine les ordinaux et qui soit surjective et monotone: par conséquent, l'ordre sur les ordinaux peut être vu comme une extension de celui sur les arbres. Puisque cela peut être fait sur des arbres finis à valeurs sur des ordinaux "assez grands" (Γ_0, le premier ordinal "imprédicatif", voir 5.3), le théorème de Kruskal, 5.1.2, prouve la bonne fondation de ces ordinaux, en raison du corollaire 5.1.3. Or, les ordinaux forment un ordre total, donc l'absence de suites descendantes démontre qu'il sont un bon ordre. Ceci implique l'induction jusqu'à Γ_0, car tout ensemble bien ordonné

réalise l'induction. En conclusion, 5.1.2 implique la cohérence de l'Arithmétique du I ordre ou de Peano, PA (et de théories bien plus puissantes, en fait), en raison de résultats classiques qui remontent à Gentzen (le bon ordre ou l'induction jusqu'à ε_0, qui est bien plus petit que Γ_0, voir 5.3, suffit à démontrer la cohérence de PA).

L'énoncé en 5.1.2 est clairement infinitaire, dans le sens qu'il concerne des suites infinies (il est Π^1_1 dans la terminologie logique, car il commence par une quantification universelle sur des objets infinis). Toutefois, sa preuve n'est pas particulièrement difficile. Elle se base sur un résultat classique, dû à Higman, concernant les suites finies et infinies, dont on a donné, récemment, aussi une version "constructive"; mais, dans la preuve de 5.1.2, on utilise un argument par absurde pour déduire une formule existentielle; on développe ensuite une méthode simple, mais strictement infinitaire, à savoir des comparaisons et des choix sur des suites infinies; voir [Nash-Williams,1963] ou [Gallier,1991]. Un passage crucial de la preuve, se base sur le choix de suites de moindre longueur (lemme de Higman) et d'arbres de moindre taille (théorème de Kruskal), dans des ensembles de suites ou d'arbres; or, puisque la longueur et la taille sont des fonctions à valeur sur les entiers, l'existence de ces minima se base sur l'existence du plus petit élément pour tout sous-ensemble des entiers.

L'idée de Friedman a été d'obtenir de cet énoncé un autre purement "finitaire", c'est à dire formalisable dans l'Arithmétique de Peano (PA).

5.1.4 Théorème FFF (Friedman, [Friedman,1981; Harrington&al.,1985]) *Pour tout n, il existe un m tel que pour toute suite finie d'arbres finis $T_1, T_2, ..., T_m$, telle que chaque T_i ait au plus $n(i+1)$ éléments, ils existent j et k tels que $j < k \leq m$ et $T_j \leq T_k$.*

L'énoncé, cette fois, a la structure logique suivante: "pour tout n, il existe m" suivi d'un prédicat décidable en n et m (KF(n,m), disons), car on sait compter les éléments d'un arbre fini et contrôler, dans une suite finie d'arbre, si il y en a deux qui sont comparable (il est donc un énoncé Π^0_2 de PA). Informellement, il affirme que, sous une petite condition sur les nombres d'éléments des arbres, même les suites finies d'arbres ne peuvent pas être totalement désordonnées. Sa preuve est une conséquence facile du théorème de Kruskal 5.1.2 et du Lemme de Kœnig[3]. En bref, on procède par l'absurde : si "il existe un n tel qui pour aucun m on a KF(n,m)", alors l'argument de compacité à la Kœnig donne un contre-exemple à 5.1.2. Il faut enfin remarquer que ces énoncés (Kruskal, Kœnig) sont des théorèmes important de la "combinatoire infinie", car ils ont un nombre important d'applications, en particulier en Logique et Informatique Théorique. En particulier le

[3] Ce lemme dit: "considérons un arbre, dont chaque élément a un nombre fini de successeurs: si tout branche est finie, il existe alors une borne uniforme pour la profondeur de l'arbre"; ainsi énoncé, de façon duale de ce que nous avons déjà fait, ce lemme est une propriété de compacité. Il reste tout aussi évident, quoique non-constructif.

théorème de Kruskal a des nombreuses applications aux problèmes de la terminaison pour les systèmes de réécriture (voila donc un résultat, relié à l'imprédicativité d'une façon essentielle - le bon ordre jusqu'à Γ_0 - et qui fait partie des mathématiques applicables; voir aussi §.6).

Ce qui est surprenant et difficile à démontrer est que 5.1.4, FFF, n'est pas démontrable dans PA (en fait, il n'est même pas démontrable dans des fragments très expressifs de l'Arithmétique du second ordre, appelée par les logiciens "Analyse", voir l'article de Simpson dans [Harrington&al.,1985]). Friedman a en effet démontré que FFF suffit a donner les mêmes conséquences que 5.1.3, à savoir le bon ordre des ordinaux jusqu'à Γ_0, car il implique qu'il n'y a pas de sous séquences descendantes "primitives récursives", que le langage de l'Arithmétique permet de représenter et que l'on pourrait extraire de toute suite descendante. En raison du deuxième théorème d'incomplétude de Gödel (c-à-d. l'indémontrabilité de la cohérence de PA, dans PA), FFF, qui est un énoncé de PA, n'est pas démontrable par les principes de preuve de PA, tout en étant une propriété démontrablement vraie des nombres entiers. Et tout cela passe par la grande puissance d'un bon-ordre qui s'étend jusqu'au premier ordinal imprédicatif.

5.2 Remarques

Deux curiosités techniques. Primo, FFF est un énoncé avec la structure syntactique suivante : $\forall x \exists y.KF(x,y)$. Or, pour tout n, l'énoncé $\exists y.KF(n,y)$ est démontrable dans PA (!): puisqu'il est vrai, il suffit d'essayer 1, 2, 3 ... tôt ou tard un trouvera m tel que KF(n,m), et cette procédure est une preuve, dans PA, de $\exists y.KF(n,y)$. C'est à dire, si on fixe n, PA démontre $\exists y.KF(n,y)$. Cette preuve est un "schema de preuve" ou une preuve "prototype" par rapport à un entier n générique (voir la §.4.2 pour la notion de preuve prototype). Mais on a vu qu'on ne peut pas en trouver une preuve prototype dans le langage de PA, c-à-d. il n'y a pas de preuve de "pour tout x, il existe y tels que KF(x,y)" dans PA, où x serait générique par rapport à *tout modèle* de PA. En fait, la preuve de $\exists y.KF(n,y)$ dépend strictement du "type" de n, c-à-d. du fait que n soit un entier standard : si la quantification universelle était donnée dans PA, x pourrait être interprété aussi par des entiers non standards, tandis que, dans la preuve, on utilise explicitement n comme entier standard (dans le branchement fini de l'arbre de Kœnig).

Deuxième remarque: grâce à la décidabilité de KF(n,m) en n et m, on peut définir une fonction récursive totale qui associe (choisit) un m pour tout n. Le point est que cette fonction croît plus rapidement que n'importe quelle fonction démontrablement totale en PA (en fait, elle est une des - ou la - plus "rapides" que l'on ait jamais définie, voir [Harrington&al.,1985]).

5.3 L'imprédicativité et les Ordinaux

Il est évident que l'énoncé FFF n'a rien d'imprédicatif, il appartient au langage de PA. Toutefois sa preuve fait intervenir l'imprédicativité profondément, en raison de la construction ordinale associé. On va l'esquisser très brièvement, tout juste au delà de l'infini.

Comptez: 0, 1, 2, 3 ... . Appelez ω la limite de cette suite.
Continuez: $\omega+1, \omega+2, \ldots \omega+\omega = \omega 2$. Et encore: $\omega 2, \omega 3, \ldots \omega\omega = \omega^2$.
La règle du jeu est claire, continuez à la jouer sur les puissances:

$$\omega^2, \omega^3, \ldots \omega^\omega.$$

Donc, ω puissance ω, puissance ω ... à la limite ce sera simplement ω puissance ω, ω fois. Cet ordinal s'appelle ε_0. Considérons maintenant la fonction

$$\phi(0, x) = \omega^x$$

alors ε_0 est un point fixe de $\phi(0, x)$, car $\varepsilon_0 = \omega^{\varepsilon 0} = \phi(0, \varepsilon_0)$; en fait, ε_0 est le plus petit point fixe de $\phi(0, x)$.

Mais continuons et appelons $\phi(1, x)$ la fonction qui énumère les points fixes de $\phi(0, x)$, c-à-d. $\varepsilon_0 = \phi(1, 0)$, $\varepsilon_1 = \phi(1, 1), \ldots, \varepsilon_\omega = \phi(1, \omega), \ldots$. Aussi la fonction $\phi(1, x)$ a des points fixes; appelons $\phi(2, x)$ la fonction qui les dénombre ... . Et ainsi de suite: $\phi(a+1, x)$ dénombre tout les points fixes de $\phi(a, x)$; si b est une limite, comme $\omega, \omega^2, \omega^\omega, \varepsilon_0 = \phi(1, 0)$ ou $\phi(2, 0)$, alors $\phi(b, x)$ dénombre les points fixes de $\phi(a, x)$ pour tout $a < b$.

On pourrait dire que cette construction de la suite ordinal n'est qu'un "jeu de symboles". Ce jeu toutefois n'est pas dépourvu de signification. A chaque niveau nous avons détecté une itération et nous avons *décidé* de "passer à la limite". C'est la *structure d'ordre des entiers* que nous avons étendu en une structure mathématique, celle des ordinaux, par la double opération, d'itération et de limite et ... d'itération des limites. Attention, sa signification n'est que structurelle, car il n'y a pas d'ensemble sous-jacents: ces symboles ne sont pas des cardinaux, en générale, car il n'existe aucun ensemble x qui satisfait, par exemple, l'équation $x = \omega^x$, dont ε_0 est la plus petite solution. On a construit, selon des principes "élémentaires", un ordre dans "l'espace mental", comme extension de celui qui va de 0 à ω.

La fonction binaire $\phi(y, x)$ est totale, c-à-d. elle est définie pour chaque a, b énuméré de la façon que l'on vient de décrire. ϕ croît très rapidement: les points fixes de $\phi(\omega, x), \phi(\varepsilon_0, x), \ldots \phi(\phi(\varepsilon_0, 0), x)$ ... sont des "monstres". On obtient une croissance encore plus forte, si on considère une suite qui nous intéresse particulièrement:

$$\gamma_0 = \phi(0,0), \quad \gamma_{n+1} = \phi(\gamma_n, 0)$$

Leur limite s'appelle Γ_0 et satisfait l'équation $\Gamma_0 = \phi(\Gamma_0, 0)$. Le corollaire 5.1.3 implique le bon ordre des ordinaux (donc l'induction) jusqu'à Γ_0 par une immersion, relativement simple et qui utilise la fonction ϕ, des arbres finis dans l'ensemble des ordinaux qui précèdent Γ_0.

Observez que, jusqu'à Γ_0 nous n'étions pas sorti du dénombrable et du prédicatif: le jeu de

symbole n'utilisait, pour une nouvelle définition, que les précédentes. Même les "plus petites solutions" des équations posées peuvent être atteinte par le bas, grâce à la construction basé sur la fonction $\phi(y, x)$, comme, par exemple, les limites ω et ε_0, car $\omega = \phi(0, 1)$ et $\varepsilon_0 = \phi(1, 0)$. Il n'en ait pas ainsi pour Γ_0, car pour tout $a, b < \Gamma_0$, on a $\phi(a,b) < \Gamma_0$.

Γ_0 échappe donc a cette construction par "itération + limite", d'extraordinaire puissance, représentée par la fonction ϕ, une fonction qui est donné dans un langage dénombrable et "stratifié", à partir de la pratique du comptage naturel 1, 2, 3 ... et du premier passage à la limite, ω. En effet, chaque fonction $\phi(a+1, x)$ est une itération "à la limite" de la fonction $\phi(a, x)$. Mais, si on fixe le *deuxième* argument, $\phi(y, b)$, comme dans la hiérarchie qui donne Γ_0, on fait une itération sur les *procès* d'itération eux-mêmes, tels qu'ils sont décrits par *toute la collection* des fonctions $\phi(a, x)$, pour tout $a < \Gamma_0$. On a donc un opérateur ou fonctionnel $\phi(y, b)$, dont la définition est bien donnée seulement quand on connaît son domaine et codomaine. Pour cette raison, Γ_0 ne peut pas être atteint par le bas, grâce aux fonctions $\phi(y, x)$: on ne peut le définir que en utilisant Γ_0 lui-même (ou la collection de tous les ordinaux, qui le contient et que nous sommes en train de définir). La définition de Γ_0 est donc essentiellement imprédicative. Pour résumer en des termes différents, Γ_0 est le plus petit ordinal tel que $\Gamma = \phi(\Gamma,0)$, mais la collection de ces Γ contient Γ_0 lui même, que nous sommes en train de définir; contrairement à ce qu'on a vu pour les $a < \Gamma_0$, on ne peut pas faire mieux, c-à-d. on ne peut pas atteindre Γ_0 par le bas, grâce aux opérations de l'arithmétique ordinale, voir par ϕ (cette esquisse informelle a été inspiré par les articles de Smorynski dans [Harrington&al.,1985]; l'imprédicativité de Γ_0 a été démontré en toute rigueur par Feferman et Schütte).

En conclusion, FFF est un énoncé arithmétique relativement simple et donné d'une façon tout à fait prédicative. Toutefois, sa preuve demande un argument très "raisonnable" mais essentiellement infinitaire, car il n'y a pas de preuve dans PA. En fait, FFF implique la bonne fondation, donc l'induction, jusqu'au premier ordinal imprédicatif, ce qui implique la cohérence de PA. C'est à dire, FFF permets de démontrer que la construction mathématique généralisée, par les fonctions ϕ, de l'itération et des limites, donne une structure mathématique, une structure d'ordre bien-fondée, quoique cette structure, dont la construction arrive jusqu'à Γ_0, soit imprédicative.

6. Théorie de la Mesure

Les définitions imprédicatives ne sont pas un artifice des logiciens : elles massivement partie de la pratique des Mathématiques de ce siècle.

Rappelons, par exemple, que les ensembles de **Borel**, sur un espace topologique, sont définis comme "la plus petite collection B d'ensembles ouverts, fermée par union infinie, intersections et complément".

Il s'agit, encore une fois, d'une définition imprédicative :

la classe C de ces collections, sur lesquelles on prend l'intersection (la plus petite dans C = intersection sur C) contient la collection B que nous sommes en train de définir.

Or, en Théorie de la Mesure, mesurable veut dire borellien. En fait, la mesure de **Lebesgue** μ sur X, est donnée par une fonction des borelliens aux réels:

$\mu: B \rightarrow R$ *telle que* $\mu(\cup A_i) = \Sigma_i \mu(A_i)$ *pour* A_i, $i < \omega$.

Cette mesure est une probabilité, si on a aussi que $\mu(X) = 1$.

Voici donc les notions de base de la Théorie générale de l'**intégration**: on dit que $f : X \rightarrow R$ est **intégrable** par rapport à μ si

$f(x) = \lim f_n(x)$ *μ–presque partout (partout sauf sur un ensemble de mesure 0),*

où $f_n = r_o 1_{Ao} + ... + r_n 1_{An}$ pour $r_i \in R$, 1_{Ai} fonction caractéristique de A_i .

On connaît l'importance de ces constructions imprédicatives pour les mathématiques modernes, car à partir de là on défini les notions suivantes de mesure.

Mesures dynamiques:

soit $f : X \rightarrow X$ continue, $\mu: B \rightarrow R$ est invariante par rapport à f si

$\mu(f^{-1}(A)) = \mu(A)$ *pour tout ensemble mesurable A.*

Ainsi que, en particulier, les

Mesures érgodiques:

pour tout ensemble mesurable A,

$\mu(f^{-1}(A)) = \mu(A)$ *et , si* $f^{-1}(A) = A$, *alors* $\mu(A) = 0$ *ou* $\mu(X \backslash A) = 0$

(pas de $A \subset X$ invariant, comme X et μ, par rapport à f), dont font partie la mesure de **Dirac** et la mesure de **Bowen-Ruelle-Sinai**.

Or, on parlait du problème des trois corps dans l'introduction de cet article. Quel est-ce le rapport, s'il y a un rapport, entre la circularité apparente de ce problème, dans la description donnée dans le langage ordinaire au moins, et l'"imprédicativité" des outils mathématiques pour son traitement? Où apparaît-elle au niveau des systèmes d'équations différentielles?

L'enjeu est majeur, car il n'est pas possible de faire une liste complète des problèmes physiques, dont la représentation informelle et le traitement mathématique utilisent des formes de circularité, si bien décrites en Logique par les différentes notions rigoureuse de circularité résumées dans cet article. Voilà quelques uns de ces problèmes: les corps dans un champ gravitationnel, les avalanches, les embouteillages routiers, le frottement d'une corde sur un archet de violon, la sédimentation d'une stalactite, les turbulences fluides... .

La force des mathématiques de ce siècle a été de savoir donner des résultats importants sur ces problèmes; un défi de la Logique serait d'essayer de faire une analyse des outils mathématiques employés, en mettant en évidence les définitions et les théories où ces circularités sont essentielles et contribuent à l'expressivité mathématique.

ARGUMENTS DISCUTÉS:

- *Théorie des Ensembles*:

  $x \in x$ (auto-appartenance)

- *Définitions récursives:*

  des fonctions $f = F(f)$, (auto-application)

  des domaines $A = F(A)$

- *Théories imprédicatives*:

  des Ensembles $(\forall X \in Ens.A) \in Ens$

  des Types $(\forall X \in Types.A) \in Types$

  Sémantique mathématique de la Théorie des Types

  Quantification universelle et preuves prototypes

- *Le théorème de Kruskal-Friedman*

  L'imprédicativité et les Ordinaux

- *Mathématiques classiques et Systèmes Dynamiques:*

  Théorie classique des réels (et des entiers!)

  Théorie de la Mesure de Lebesgue

  Théorie générale de l'intégration

  Systèmes dynamiques

... EN TANT QUE SOLUTIONS D'EQUATIONS:

Théorie des Ensembles:

$x = \{y, a\}$

$y = \{x, b\}$

Définitions récursives:

fonctions: $f(n) = n \times f(n-1)$

domaines: $X = X + A \times X$

Définitions imprédicatives:

$$X = \cap \{ Y / X \subseteq Y \ \& \ 0 \in Y \ \& \ \forall z (z \in Y \rightarrow z+1 \in Y)\}$$

Notations ordinales

Γ_0 est le plus petit ordinal tel que $\Gamma = \phi(\Gamma,0)$

Systèmes dynamiques:

Systèmes d'équations différentielles.

Bibliographie

Aczel, **Non-wellfounded sets**, CSLI Lecture-Notes 014, Stanford Univ. 1988.

Amadio R., Curien P.-L., **Domains and lambda-calculi**, Birkhuaser, to appear, 1998.

Asperti A., Longo G., **Categories, Types, and Structures.** MIT Press,1991.

Barendregt H., **The Lambda Calculus; its syntax and semantics**, Revised and expanded edition, North Holland,1984.

Barwise J., Moss L., **Vicious Circles: on the mathematics of non-wellfounded phenomena**, CSLI Lecture-Notes 060, Stanford Univ. 1996.

Cardelli L., Longo G. , "A semantic basis for Quest", **Journal of Functional Programming**, vol.1, n.2, 1991

Coquand T., Huet G. "The Calculus of Constructions" **Information and Computation**, 76, 95 - 120, 1988.

Forti M., Honsell F.. "Set theory with free construction principles, **Ann. Scuola Norm. Sup. Pisa**, Cl. Sci. (4) 10, 493-522, 1983.

Friedman H., "Independence results in finite graph theory", Technical Report, Ohio State University, March 1981.

Fruchart T., Longo G. "Carnap's remarks on Impredicative Definitions and the Genericity Theorem" in **X Conference on Logic, Methodology and Philosophy of Science**, Cantini et al. (eds.), Kluwer, to appear, 1998.

Girard J.-Y., Lafont Y., Taulor P. **Proof and Types**, Cambridge Univ. Press, 1989.

Gallier J., "What is so special about Kruskal's theorem and the ordinal Γ_0?" **Ann. Pure. Appl. Logic**, 53, 1991.

Harrington L. et al. (eds), **H. Friedman's Research on the Foundations of Mathematics**, North-Holland, 1985.

Hindley R., Longo G., "Lambda-calculus models and extensionally", **Zeit. Math. Logik Grund. Math**. n.2, Vol. 26, 1980.

Hyland M., "A small complete category" Lecture delivered at the Conference **Church's Thesis after 50 years**, Zeiss (NL), June 1986 *in* **Ann. Pure Appl. Logic**, 40, 1988.

Kruskal J., "Well-quasi-ordering and the tree theorem" **Trans. Amer. Math. Soc.** 95, 1960.

Lambek J., Scott P.J., **Introduction to higher order Categorical Logic**, Cambridge University Press, 1986.

Longo G., "Set-Theoretical Models of Lambda-Calculus: Theories, Expansions, Isomorphisms", **Annals Pure Applied Logic**, 24, 1983.

Longo G. "Some aspects of impredicativity: notes on Weyl's philosophy of Mathematics and on todays Type Theory" **Logic Colloquium 87**, Studies in Logic (Ebbinghaus et al. eds),

North-Holland, 1989.

Longo G., "The mathematical continuum, from intuition to logic" in **Naturalizing Phenomenology: issues in comtemporary Phenomenology and Cognitive Sciences**, (J. Petitot et al., eds) Stanford U.P., 1999.

Longo G., Milsted K. and Soloviev S., "The genericity theorem and the notion of parametricity in the polymorphic Lambda-calculus" **Theor. Comp. Sci.** vol. 121, 1993.

Longo G., Moggi E., "A category-theoretic characterization of functional completeness" **Theor. Comp. Sci.** vol. 70, 2, 1990.

Longo G., Moggi E., "Constructive Natural Deduction and its omega-Set Interpretation" **Mathematical Structures in Computer Science**,vol.1, n.2, 1991.

Milner R., Toft M., "Co-induction in relational semantics" **Theor. Comp. Sci.**, vol. 87, 1991.

Moschovakis Y.N., **Descriptive Set Theory**, North-Holland, 1980

Nash-Williams C., "On well-quasi-ordering of finite trees" **Proc. Cambridge Phil. Soc.** 59, 1963.

Poincaré H., **La Science et l'Hypothèse**, Flammarion, 1968.

Pitts A., "Polymorphism is Set Theoretic, constructively" **Symposium on Category Theory and Comp. Sci.**, SLNCS 283 (Pitt et al. eds), Edinburgh, 1987.

Scott D., "Outline of a mathematical theory of computation" **4th Ann. Princeton Conf. on Info. Syst. Sci.**, 1970.

Scott D., "Continuous lattices" **Toposes, algebraic Geometry and Logic**, (Lavwere ed.), SLNM 274, (pp.97-136) Springer-Verlag, 1972.

Scott D., "Lambda-calculus, some models, some philosophy," **The Kleene Symposium** (Barwise et al. eds.) North-Holland, 1980.

Smyth M., Plotkin G., "The category-theoretic solution of recursive domain equations" **SIAM Journal of Computing 11**, 1982.