La théorie des types, de Russell à de Bruijn

Thierry Coquand

COLLÈGE DE FRANCE
1530

Plan du cours

Leçon 1 : quelques remarques historiques, première formulation de la théorie des types dépendants,

Leçon 2 : modèles, en particulier recollement de modèles et modèles de préfaisceaux,

Leçon 3 : canonicité et normalisation, par la technique de recollement d'Artin (SGA 4),

Leçon 4 : rapport avec la théorie des ensembles.

La deuxième partie portera sur l'univalence, et présentera des modèles (qui sont des modèles de préfaisceaux), un exemple de formation (espaces d'Eilenberg-MacLane) de types qui ne sont pas des ensembles et une preuve de la conjecture de Voevoedsky (par Rafaël Bocquet).

Je me permettrais d'illustrer des notions par des exemples qui se réfèrent à des faits que l'auditeur peut déjà connaitre par ailleurs, mais qui n'ont pas encore été exposés, précédé du symbole ¶

Système de Church

Alonzo Church 1941 *A Formulation of the Simple Theory of Types*

Types des propositions o et individus N et types de fonctions $A \rightarrow B$

Opérations primitives $\vee : o \rightarrow o \rightarrow o$ and $\neg : o \rightarrow o$ and $\forall_A : (A \rightarrow o) \rightarrow o$

$p \rightarrow q$ est défini comme $\neg p \vee q$

Les axiomes sont essentiellement ceux de *Principia Mathematica*,

$p \rightarrow p \vee q \qquad p \vee q \rightarrow q \vee p \qquad p \vee p \rightarrow p \qquad (q \rightarrow r) \rightarrow (p \vee q \rightarrow p \vee r)$

$(\forall_A f) \rightarrow f\ a \qquad \forall_{x:A}(p \vee f\ x) \rightarrow p \vee \forall_{x:A}(f x)$

Système de Church

Ces axiomes ont un caractère purement formel

Par exemple, il n'est pas clair comment déduire $p \to p$ de ces axiomes

Principia Mathematica avait un axiome supplémentaire

$$p \vee (q \vee r) \to q \vee (p \vee r)$$

qui se déduit des autres axiomes, comme le remarque Bernays dans son ⟪Habilitationsschrift⟫ (1918).

Imprédicativité et Axiome de Réductibilité

Russell avait une version stratifiée du type des propositions $o = o_0, o_1, o_2, \ldots$

On aura $\forall_{f:N \to o} f\ a \to f\ b$ dans o_1 et pas dans o

Russell illustre ces notions avec des exemples concrets

Napoleon was Corsican

est dans o

Napoleon had all the qualities of a great general

est dans o_1

Imprédicativité

Caractère circulaire et donc a priori proche des paradoxes

A typical Englishman is one who possesses all the properties possessed by a majority of Englishmen.

Un anglais typique doit être en fait atypique si on n'introduit pas cette stratification; paradoxe similaire à celui des suites aléatoires : une suite aléatoire de $\{0,1\}^N$ est une suite qui appartient à toutes les sous-parties mesurables de mesure 1 (ensemble qui est vide).

Cette hiérarchie sera une motivation pour Gödel d'introduire la notion d'ensemble *constructible*, (possibilité déjà discutée par Poincaré); on considère $o_\omega = \cup_n o_n$, puis $o_{\omega+1}, \ldots$ On peut montrer que l'on a un ordinal λ dénombrable tel que $o_\lambda = o_{\lambda+1}$, et donc, comme le remarque Gödel, l'axiome de réductibilité est vérifié en ce sens.

Imprédicativité et axiome de réductibilité

Axiome de réductibilité : toute proposition dans o_k est équivalente à une proposition dans o_0

Russell propose de définir l'égalité, en suivant le principe d'indiscernabilité de Leibniz 1686 dans son *Discours de Métaphysique*

$$a \equiv_A b \text{ est } \forall_{f:A\to o} f\ a \to f\ b$$

On a $a \equiv_A b : o_1$ de manière prédicative. L'axiome de réductibilité entraine que cette proposition est équivalente à une proposition dans o, et l'introduction de l'égalité est donc un exemple d'utilisation de l'axiome de réductibilité.

¶ Cette hiérarchie va correspondre à une hierarchie d'univers $U_0, U_1, \ldots$ en théorie des types; on dit qu'un type est U_k-petit s'il est équivalent à un type dans U_k. Voevodsky introduit un axiome (de ⟪redimensionnement⟫) qui dit qu'une *proposition* est U_0-petite. Cet axiome est valide dans le modèle simplicial; en fait, il est une conséquence du tiers-exclu, valide dans ce modèle.

Imprédicativité et axiome de réductibilité

¶ L'axiome de redimensionnement est prouvablement faux pour les *ensembles*. Le type des ensembles dans U_0 est un *groupoïde* dans U_1, mais le type des *ordinaux* dans U_0 est un *ensemble* muni d'une structure d'un ordinal qui est prouvablement pas équivalent à un type dans U_0. Pour cela, on a besoin d'utiliser la définition des ordinaux présentée dans le livre *Homotopy Type Theory: Univalent Foundations of Mathematics*, qui provient de la thèse de Robin Grayson (1978).

Imprédicativité et axiome de réductibilité

2 preuves de symmétrie de l'égalité

Une preuve *imprédicative*: $g = \lambda_{x:A} x \equiv_A a$, we have $g\ a$ hence $g\ b$

Pour cette preuve, on a besoin que $g\ x$ soit équivalent à une proposition $h\ x$ dans o

Une preuve *prédicative*: $g = \lambda_{x:A} f\ x \to f\ a$

Logique d'ordre supérieure

Russell, dans la deuxième édition des *Principia Mathematica*, donne beaucoup d'exemples de cette nature, d'énoncés ayant une preuve imprédicative qui peut être réécrite en une preuve prédicative.

¶ En théorie des types avec univalence, on aura une situation analogue avec le *principe de remplacement*, voir le livre *Symmetry* (disponible en ligne). Ce principe est vérifié de manière prédicative, et qui permet de définir des notions ⟪dans le bon univers⟫, par exemple le ⟪déloupage⟫ d'un groupe G dans un univers U_0, qui sera défini comme le type de G-torseurs, est dans U_1, mais il est équivalent à un type dans U_0 par remplacement.

Cette question de mieux comprendre l'imprédicativité va devenir fondamentale en théorie de la démonstration, comme il est expliqué dans le texte de Martin-Löf (2008)

The Hilbert-Brouwer controversy resolved?

Logique d'ordre supérieure

Principes d'extensionnalité

-$(p \leftrightarrow q) \rightarrow p \equiv_o q$, formulée dans Appendix C de *Principia Mathematica*

-$(\forall_{x:A} f(x) \equiv_B g(x)) \rightarrow f \equiv_{A \rightarrow B} g$

-un opérateur $\iota : (A \rightarrow o) \rightarrow A$ tel que $(\exists!_{x:A} P(x)) \rightarrow P(\iota(P))$

-opérateur de choix $\epsilon : (A \rightarrow o) \rightarrow A$ tel que $(\exists_{x:A} P(x)) \rightarrow P(\epsilon(P))$

La première version de Hilbert (1923) était duale : $P(\tau(P)) \rightarrow \forall_{x:A} P(x)$

Logique d'ordre supérieure

L'opérateur de choix *avec* extensionnalité entraine le tiers-exclu

Si $P : B \to B \to o$, $P\ x\ y$ défini comme $\psi \vee x \equiv_B y$ on a

$$\psi \ \leftrightarrow \ \epsilon(P\ 0) \equiv_B \epsilon(P\ 1)$$

Si ψ on a $P\ 0 \equiv_{B \to o} P\ 1$ par *extensionnalité*.

Comme l'égalité sur B est décidable, ψ est aussi décidable.

Description définie

Avoir un opérateur de description définie semble nécessaire pour représenter les mathématiques. Ceci est par exemple remarqué par Henri Cartan *Sur le fondement logique des mathématiques*, 1943, dans lequel il analyse la notion d'《éléments explicites》.

Bourbaki utilise à la place un opérateur de choix (qui est écrit τ comme le symbole ϵ est déjà pris comme symbole de l'appartenance), et il remarque explicitement que cela permet de se dispenser d'avoir un opérateur de description définie.

¶ Si on a un type $\Sigma_{x:A}B$ on peut essayer d'exprimer l'existence 《forte》 avec ce type et on a alors une forme de l'axiome du choix unique en utilisant la deuxième projection. C'est ce que suggère Howard (1969), puis Martin-Löf; mais on a aussi un opérateur de choix général avec cette interprétation.

¶ Avec l'univalence, on utilise le type qui exprime que $\Sigma_{x:A}B$ est contractile pour exprimer l'existence unique, et le principe du choix unique est prouvable, mais avoir un opérateur de choix est incompatible avec l'univalence.

Description définie

Dans le système Coq, une forme ⟪constructive⟫ du principe du choix unique est ajoutée dans le cas d'une propriété décidable sur les entiers. Dans ce cas, on n'a pas besoin de l'unicité, car si $\exists_{x:N} P(x)$ alors on a $\exists!_{x:N} Q(x)$ pour $Q(x)$ qui exprime que x est le *plus petit* x tel que $P(x)$, défini de manière unique. Cet ajout semble être utilisé de manière essentielle dans la preuve du théorème de l'ordre impair. Ce principe est aussi utilisé dans les travaux de Yannick Forster, Dominik Kirst et al. sur la théorie de la calculabilité.

See https://rocq-prover.org/doc/v8.9/stdlib/Coq.Logic.ConstructiveEpsilon.html

Autant que je puisse le juger, la propriété de normalisation pour le système avec cette opération n'a pas été vraiment étudiée.

Le principe du choix unique n'est pas vérifié en général.

Le système Lean ajoute un opérateur de choix, et l'extensionnalité pour les fonctions.

Extensionnalité

Dans le système Coq, l'extensionnalité pour les fonctions est ajoutée, comme convénience, pour la preuve de $BB(5) = 47176870$, qui, a priori, ne considère que des objets ⟪discrets⟫.

```
Axiom functional_extensionality_dep : forall {A} {B : A -> Type},
  forall (f g : forall x : A, B x),
  (forall x, f x = g x) -> f = g.

Definition TM : Type := Q * Sym -> option (Sym * dir * Q).
```

L'extensionnalité est utilisée dans le projet CompCert.

Extensionnalité

Je crois que la preuve du théorème des quatre couleurs est écrite dans un système sans axiomes.

¶ *Avec univalence (et remplacement), le principe de description définie et l'extensionnalité deviennent prouvables.*

¶ On peut construire un modèle effectif et prédicatif qui justifie univalence, remplacement, l'axiome du choix dépendant et LPO $\forall_{x:N}\neg P(x) \vee \exists_{x:N} P(x)$ pour $P(x)$ décidable. Cela utilise le nouveau modèle de Christian Sattler qui capture la notion de types d'homotopie. Ces axiomes sont suffisants pour développer l'analyse. Voir e.g. introduction des *Fondements de l'Analyse Moderne*, par Dieudonné ou *Intégration et Analyse de Fourier* par Cédric Villani, qui écrit

j'ai systématiquement utilisé des hypothèses de séparabilité ou de dénombrabilité, quand le besoin s'en fait sentir, pour éviter l'axiome du choix.

Logique d'ordre supérieure

Dans le système de Russell, sans extensionnalité, on ne peut pas identifier les fonctions propositionnelles et les sous-ensembles (《classes》 pour Russell).

Dans la première version de *Principia Mathematica*, on a besoin de faire une distinction entre un prédicat et le sous-ensemble qu'il définit, car deux prédicats distincts peuvent définir le même sous-ensemble (s'ils sont extensionellement équivalents).

Russell dénote par $\hat{x}\psi(x)$ le sous-ensemble déterminée par la fonction propositionelle $\psi(x)$.

C'est sans doute la source de la notation de l'abstraction en λ-calcul.

Logique d'ordre supérieure

Church étend cette notation pour des fonctions générales, qui ne produisent pas nécessairement des valeurs de vérités, e.g. $N \to N$ ou $(N \to o) \to N$.

Il utilise même cette notation pour représenter des entiers, e.g. $\lambda_x \lambda_f f(f(x))$ représente l'entier 2 *A set of postulates for the foundation of logic* (1932).

Dans son papier de 1941, le type des entiers n'est pas N mais $N \to (N \to N) \to N$.

Cela semble provenir de Wittgenstein qui écrit qu'un entier est un ⟪exposant d'une opération⟫, Tractacus 6.021, et donne des exemples de calcul avec cette représentation.

L'influence semble claire, mais elle n'est pas explicite dans Church, cf. Göran Sundholm *The General Form of the Operation in Wittgenstein's Tractatus* (1992).

Logique d'ordre supérieure

Ramsey note que l'on peut, à la place de l'axiome de réductibilité, introduire $\forall_A : (A \to o) \to o$ même si A contient o.

Il interprête o comme $\{0, 1\}$ et les fonctions $A \to B$ comme des fonctions arbitraires.

C'est la version qui sera décrite par Church, qui introduit aussi un type de fonction général $A \to B$ et pas seulement la formation de fonctions propositionnelles.

Théorie des types simples

Gödel dans son papier sur l'incomplétude, présente une version encore plus minimale

$$T_0 = N \qquad\qquad T_{n+1} = T_n \to o$$

Norbert Wiener (1914) avait montré comment définir la paire uniquement avec ces types (en théorie des ensembles on utilise souvent le codage de Kuratowski, codant (a, b) comme $\{\{a\}, \{a, b\}\}$)

L'extensionnalité devient alors

$$(\forall_{x:T_n} y(x) \leftrightarrow z(x)) \to y \equiv_{T_{n+1}} z$$

On voit l'analogie avec le premier axiome de la théorie des ensembles qui énonce qu'un ensemble est déterminé par ses éléments.

Théorie des types simples

The simple theory of types provides a straightforward ... foundation for the greater part of classical mathematics. That is why a number of authors (Carnap, Gödel, Tarski, Church, Turing) gave a precise formulation of it, and used it as a basis for metamathematical investigations. The theory is straightforward because it embodies two principles which (at least before the advent of modern abstract concepts) were part of the mathematicians normal code of practice. Namely that a variable always has a precisely delimited range, and that a distinction must always be made between a function and its arguments. In this sense one might claim that all good mathematicians had anticipated simple type theory. [Indeed Turing made this claim for primitive man].

Robin Gandy *The simple theory of types*, Logic Colloquium, 1976

Zermelo-Fraenkel

It is a pity that a system such as Zermelo-Fraenkel set theory is usually presented in a purely formal way, because the conception *behind it is quite straightforwardly based on type theory. One has the concept of an arbitrary* subset of a given domain *and that the collection of* all subsets *of the given domain can form a new domain (of the next type!). Starting with a domain of individuals (possibly empty), this process of forming subsets is then iterated into the* transfinite. *Thus, each set has a type (or* rank*), given by the ordinal number of the stage at which it is first to be found in the iteration.*

Dana Scott, *A type-theoretical alternative to ISWIM, CUCH, OWHY*, 1969

Logique d'ordre supérieure

L'axiome $(p \leftrightarrow q) \rightarrow p \equiv_o q$, n'est pas un axiome dans le papier de Church, qui mentionne seulement

We remark, however, the possibility of introducing the additional axiom of extensionality

$$(p \leftrightarrow q) \rightarrow p \equiv_o q,$$

which has the effect of imposing so broad a criterion of identity between propositions that there are in consequence only two propositions, and which $\ldots$ *makes possible the identification of classes with propositional functions.*

Ceci fait echo à ce qu'écrivait Russell en 1925

We should have $(p \leftrightarrow q) \rightarrow \forall_{f:o\rightarrow o} f(p) \leftrightarrow f(q)$. *Consequently,* $(p \leftrightarrow q) \rightarrow p \equiv_o q$. *There will thus be only two propositions, one true and one false.*

Logique d'ordre supérieure

Il est possible de justifier l'axiome d'extensionnalité par la technique des ⟪relations logiques⟫ que Gandy invente dans sa thèse 1953 (Takeuti indépendamment a la même idée aussi en 1953).

Il est plus difficile d'expliquer l'axiome de description définie; une tentative d'explication est dans *On Denoting*, 1905, mais elle n'est pas ⟪compositionnelle⟫.

¶ *Les modèles de l'univalence vont donner une nouvelle justification de cette opération.*

On peut justifier la logique classique par la technique de ⟪traduction de double négation⟫.

L'axiome du choix général est justifié par la technique des ensembles constructibles de Gödel, mais on a besoin d'ordinaux non dénombrables.

Logique minimale

Une version en logique minimale apparait dans les travaux de Girard et Martin-Löf 1971

S'il y un seul type de base o, donc les types peuvent être aussi décrit par la grammaire

$$A \ ::= \ (A_1, \ldots, A_n)$$

Pour $n = 0$, let type $()$ représente le type des propositions o

En fait, Girard et Martin-Löf ont aussi un type des individus N, mais les types sont

$$A \ ::= \ N \mid (A_1, \ldots, A_n)$$

Version minimale

X contexte de la forme $x_1 : A_1, \ldots, x_n : A_n$

$$\frac{\Gamma, p \vdash_X q}{\Gamma \vdash_X p \to q} \qquad \frac{\Gamma \vdash_X p \to q \qquad \Gamma \vdash_X p}{\Gamma \vdash_X q}$$

$$\frac{\Gamma \vdash_{X,x:A} p}{\Gamma \vdash_X \forall_{x:A} p} \qquad \frac{\Gamma \vdash_X \forall_{x:A} p \qquad X \vdash a : A}{\Gamma \vdash_X p(a/x)}$$

Version minimale

Avec un traitement uniforme des termes et des preuves, on obtient le système $F\omega$

$$\frac{\Gamma, x : p \vdash_X t : q}{\Gamma \vdash_X \lambda_{x:p} t : p \to q} \qquad \frac{\Gamma \vdash_X t : p \to q \qquad \Gamma \vdash_X u : p}{\Gamma \vdash_X t\ u : q}$$

$$\frac{}{\Gamma, x : A, \Delta \vdash x : A} \qquad \frac{\Gamma \vdash_{X, x:A} t : p}{\Gamma \vdash_X \lambda_{x:A} t : \forall_{x:A} p} \qquad \frac{\Gamma \vdash_X t : \forall_{x:A} p \qquad X \vdash a : A}{\Gamma \vdash_X t\ a : p(a/x)}$$

Girard a une notation différente pour les termes et les preuves, e.g. $DT\alpha\lambda_{x:\alpha}x$ pour $\lambda_{\alpha:o}\lambda_{x:\alpha}x$ et $\delta\alpha(\alpha \to \alpha)$ pour $\Pi_{\alpha:o}\alpha \to \alpha$.

Version minimale

Il prouve la *normalisation* : tous les termes construits ainsi terminent, et la preuve ne peut pas se faire dans l'arithmétique d'ordre supérieur, théorie où l'on a aussi un type des individus et un axiome d'infinité.

La *cohérence* de ce système est élémentaire : il y a un modèle où o devient $\{0, 1\}$.

La normalisation, par contre, n'est pas élémentaire : elle entraine la cohérence de l'axiome de l'infini.

On peut ajouter l'axiome d'infini, par exemple constantes 0 et $S(x)$ et axiomes $\neg(0 \equiv_N x)$ et $S(x) \equiv_N S(y) \to x \equiv_N y$.

¶ Si on a un univers U_0 l'axiome d'infini devient prouvable en utilisant $\Pi_{X:U_0} X \to (X \to X) \to X$. Donc on peut considérer que l'axiome d'infini est justifié de manière purement logique.

Impact des travaux de Girard

Le problème de l'imprédicativité, sous la forme d'une preuve de normalisation de ce système, était étudié systématiquement dans les années 60 par Prawitz et Martin-Löf.

L'espoir était de mieux comprendre quand la hiérarchie L_α modèle l'analyse, voir D. Prawitz (1970) *On the proof theory of mathematical analysis*.

Le résultat de Girard était a donc été étudié en détail par Prawitz et Martin-Löf (juin 1970).

Naissance de la théorie des types dépendants

Fin des années 60, période très riche avec des travaux indépendants

-Howard 1968 et Girard 1971 qui inspirent Martin-Löf 1971

-de Bruijn 1967 qui inspire Scott *Constructive Validity* (1970)

En suivant les idées d'Howard (analogie entre types et propositions, et entre objets et preuves) et la preuve de normalisation de Girard, Martin-Löf a l'idée de formuler un système pour représenter les mathématiques constructives.

Naissance de la théorie des types dépendants

Martin-Löf liste les 3 points suivants comme motivation :

(1) quantification sur les propositions, ce qui était motivé par le travail de Girard

(2) les domaines de quantification forment des types (《doctrine》 des types de Russell)

(3) identification des propositions et types, que Martin-Löf venait d'apprendre via Howard

Ceci conduit à prendre un type de tous les types comme le type des propositions.

Naissance de la théorie des types dépendants

On ne peut pas former le paradoxe de Russell en théorie des types, car on ne peut pas former $a : A$ comme un élément de type o, et donc on ne peut pas former $\neg(a : A)$

$a : A$ est une assertion qui n'est pas représentée par une proposition. Il n'est donc pas absurde d'essayer un système avec type : type.

Une autre motivation était de palier aux limitations du calcul de Church : on ne peut pas quantifier sur des types quelconques, et on ne peut pas former de types de structures mathématiques

On peut définir le type $N = \Pi_{X:\mathsf{type}} X \to (X \to X) \to X$ avec $0 : N$ et $S : N \to N$, et montrer l'axiome de l'infini.

Comment garantir la *cohérence* ? Il n'y a pas de moèle clair en théorie des ensembles, et comme le remarque Martin-Löf, le système est plus fort que celui de Zermelo.

Naissance de la théorie des types dépendants

Martin-Löf trouve plus naturel d'ajouter un type *primitif* des entiers

Aussi type $\Sigma_{x:A}B(x)$ ⟪dual⟫ du type $\Pi_{x:A}B(x)$

Il montre aussi comment représenter des types inductifs plus complexes comme le type des ordinaux, avec lois de calcul.

¶ Ceci sera généralisé dans le papier *Inductively Defined Types*, Th. C. et Christine Paulin, 1989, qui donne un schéma général de définition de types inductifs. Le papier *Observational Equality Meets CIC* par Tabareau et Pujet (2024) montre comment étendre ces définitions à celle des ⟪familles inductives⟫ dès que l'on a un type d'égalité avec les lois de calcul de Martin-Löf.

Naissance de la théorie des types dépendants

En fait, Martin-Löf prouve la *normalisation* de ce système, en suivant l'idée de Girard pour la normalisation de Fω d'utiliser des candidats de réductibilité.

Sa preuve est *formellement* correcte.

¶ On reprendra cette preuve dans la troisième leçon, preuve qui peut être vue comme une application de la technique de recollement d'Artin (SGA 4).

Cela ne contredit pas le théorème de Gödel car l'argument se fait dans un calcul plus fort, avec un principe de reflexion (si on montrer $P(n)$ pour chaque entier donné n et $P(x)$ est décidable, alors on a $\forall_{x:N} P(x)$).

Il est alors vraiment surprenant que Girard obtient un paradoxe dans ce système, car la preuve est formellement une généralisation naturelle de la preuve de normalisation de Girard.

Naissance de la théorie des types dépendants

$$\frac{\Gamma \vdash}{\Gamma \vdash \mathsf{type} : \mathsf{type}} \qquad \frac{\Gamma \vdash A : \mathsf{type}}{\Gamma, x : A \vdash} \qquad \frac{\Gamma, x : A \vdash B : \mathsf{type}}{\Gamma \vdash \Pi_{x:A} B : \mathsf{type}}$$

$$\frac{\Gamma, x : A, \Delta \vdash}{\Gamma, x : A, \Delta \vdash x : A} \qquad \frac{\Gamma, x : A \vdash t : B}{\Gamma \vdash \lambda_{x:A} t : \Pi_{x:A} B} \qquad \frac{\Gamma \vdash t : \Pi_{x:A} B \qquad \Gamma \vdash u : A}{\Gamma \vdash t\ u : B(u/x)}$$

$$\frac{\Gamma \vdash t : A \qquad \Gamma \vdash B : \mathsf{type} \qquad A = B}{\Gamma \vdash t : B}$$

Naissance de la théorie des types dépendants

Martin-Löf *A Theory of Types* (1971) disponible sur le net.

La propriété de confluence est utilisée pour montrer la préservation des types par β-réduction.

Martin-Löf présente une preuve de confluence qui utilise une *relation* définie inductivement, qui décrit une version ⟪parallèle⟫ de la β-réduction.

Cette preuve est citée par Plotkin comme une des motivations pour la sémantique opérationnelle *The Origins of Structural Operational Semantics* (2004)

Le papier suivant contient une présentation des types inductifs

On the strength of intuitionistic reasoning, texte d'un exposé 1971

Naissance de la théorie des types dépendants

Martin-Löf n'utilise pas la notion de contexte, que l'on trouve dans AUTOMATH.

J'ai introduit ce style de présentation dans ma thèse pour présenter le calcul des constructions.

Il montre de manière très claire que si l'on a normalisation, alors il y a un algorithme pour décider si une assertion $a : A$ est correcte ou non.

Un tel algorithme était aussi décrit par de Bruijn pour AUTOMATH

The mathematical language AUTOMATH, its usage, and some of its extensions (1970).

Naissance de la théorie des types dépendants

Martin-Löf montre alors comment traduire le système Fω dans ce calcul.

Mais on a une traduction d'un système *plus* fort : on peut quantifier sur des types comme $A = \Pi_{X:\text{type}}(T\ X \rightarrow X) \rightarrow X$ avec $T\ X = (X \rightarrow o) \rightarrow o$

Intuitivement, ces types sont trop ⟪gros⟫ et on doit s'attendre à une contradiction en suivant Burali-Forti.

C'est ce que fait Girard.

Naissance de la théorie des types dépendants

En utilisant les types $\Sigma_{x:A}B(x)$ et le type des entiers, on a une version assez directe du paradoxe, en utilisant le type des relations d'ordre strict bien fondée (qui n'ont pas de suite infinie décroissante).

Sur ce type, on a une relation d'ordre strict bien fondée et on a une contradiction, i.e. on construit un terme de type $\perp = \Pi_{X:\mathsf{type}}X$.

Un terme de type $\perp$ ne peut pas avoir une forme normale.

Naissance de la théorie des types dépendants

On peut en fait suivre une autre route pour avoir une contradiction : on peut suivre la preuve de Reynolds 1984 qu'il n'y a pas de modèle ensembliste du polymorphisme. C'est ce que j'ai remarqué en 1989.

Cette version a une preuve très courte par Hurkens *A Simplification of Girard's Paradox* (1995) dont j'ai donné récemment une version encore plus courte dans *A Variation of Reynolds-Hurkens* (2024).

Voir aussi les papiers *Polymorphism is Set Theoretic, Constructively* (1987) et *Non-trivial Power Types Can't Be Subtypes of Polymorphic Types* (1989) par Andy Pitts, pour une version dans une théorie des types ⟪extensionnelle (théorie des topos).

Alexandre Miquel, dans sa thèse (2001), montre comment exprimer le paradoxe de Russell en précisant les rapports avec la théorie des ensembles.

Naissance de la théorie des types dépendants

Girard donne un paradoxe pour la version sans types $\Sigma_{x:A} B(x)$ et types des entiers.

Il présente une variation du paradoxe de Burali-Forti, avec des ordres ⟪sans torsions⟫, relations d'ordre strict qui sont *extensionnels* : deux éléments qui définissent des segments *isomorphes* sont *égaux*. C'est la condition cruciale de la notion d'ordinal de Robin Grayson.

Il n'y a pas de condition demandant que l'ordre soit bien fondé.

Il peut construire un type des ordres sans torsions en utilisant un codage de $\exists_{x:A} B(x)$

L'argument est subtil car c'est une existence ⟪faible⟫, en utilisant la terminologie d'Howard (1968) qui contraste $\Sigma_{x:A} B(x)$ et $\exists_{x:A} B(x)$.

Naissance de la théorie des types dépendants

Donc on a un terme non normalisable, qui ne se réduit pas sur lui-même. Il est possible de construire à partir de ce terme une famille $Y_n : \Pi_{A:\mathsf{type}}(A \to A) \to A$ telle que $Y_n\ f = f\ (Y_{n+1}\ f)$

On en déduit que *le jugement* $a : A$ *n'est* pas *décidable*, Meyer-Reinholdt LICS 1986

Argument reproduit dans *A-Translation and Looping Combinators in Pure Type* (1994) Th. C. et Hugo Herbelin.

Un problème ouvert est si l'on peut construire un terme de type $\perp$ qui se réduit sur lui-même, auquel cas on pourrait construire un terme Y tel que $Y\ f = f\ (Y\ f)$.

Un tel terme existe si on a $\Sigma_{x:A}B(x)$ ou si on prend une version avec abstraction non typée.

Analyse du paradoxe

Rappel : Martin-Löf liste les trois points suivants comme motivation :

(1) quantification sur les propositions, ce qui était motivé par le travail de Girard

(2) les domaines de quantification forment des types (《doctrine》 des types de Russell)

(3) identification des propositions et types, que Martin-Löf venait d'apprendre via Howard

Ces trois principes ensembles conduisent à une contradiction.

La solution pour Martin-Löf est de ne pas permettre (1), d'avoir un calcul prédicatif.

Une autre possibilité est de modifier (3) : les *propositions* sont des types, mais la notion de type est plus générale

Le calcul prédicatif des univers

On va stratifier type en $U_0, U_1, \ldots$ comme pour le calcul ramifié de Russell *An intuitionistic theory of types* (1972).

Martin-Löf signale l'analogie avec la notion d'univers introduite par Grothendieck en théorie des ensembles.

Chaque univers réalise un principe de réflection : il est clos par les opérations de la théorie des types.

Comme dans le papier 1971, Martin-Löf ajoute les types inductifs et le type $\Sigma_{x:A}B(x)$.

La formulation précise n'est pas simple : dans le calcul 1971, on a inférence des types

Dans un calcul avec $\Sigma_{x:A}B(x)$ on ne peut pas inférer le type de (a, b) qui peut être $\Sigma_{x:A}B(x)$ ou $A \times B(a)$.

Martin-Löf pour raison d'uniformité note alors $\lambda_x b$ au lieu de $\lambda_{x:A} b$.

Le calcul des constructions

$$\frac{\Gamma \vdash}{\Gamma \vdash o : \textsf{type}} \qquad \frac{\Gamma \vdash A : \tau}{\Gamma, x : A \vdash} \qquad \frac{\Gamma, x : A \vdash B : \tau}{\Gamma \vdash \Pi_{x:A} B : \tau}$$

$$\frac{\Gamma, x : A, \Delta \vdash}{\Gamma, x : A, \Delta \vdash x : A} \qquad \frac{\Gamma, x : A \vdash t : B}{\Gamma \vdash \lambda_{x:A} t : \Pi_{x:A} B} \qquad \frac{\Gamma \vdash t : \Pi_{x:A} B \qquad \Gamma \vdash u : A}{\Gamma \vdash t\ u : B(u/x)}$$

$$\frac{\Gamma \vdash t : A \qquad \Gamma \vdash B : \tau \qquad A = B}{\Gamma \vdash t : B}$$

τ dénote o ou type

Le calcul des constructions

Le système contient la logique d'ordre supérieur.

Il est très proche du système avec type : type; est-il cohérent ?

On a un plongement $F\omega \rightarrow CC$ et Christine Paulin définit un inverse à gauche $E : CC \rightarrow F\omega$ dans *Extracting Fω Programs from Proofs in the Calculus of Constructions*, POPL 89

Par exemple $E(\Pi_{A:o}\Pi_{P:A\rightarrow o}\Pi_{x:A}P\ x \rightarrow P\ x)$ est $\Pi_{A:o}\Pi_{P:o}A \rightarrow P \rightarrow P$

Ceci montre que le plongement est conservatif.

En particulier, on ne peut pas montrer $\perp = \Pi_{X:o}X$ dans CC.

Voir le papier *Inductively defined types in the Calculus of Constructions* (1989), Christine Paulin et Frank Pfenning.

Problèmes

L'étude de ces systèmes semble trop dépendre de choix syntaxiques, qui ne devraient pas conceptuellement jouer un rôle

Par exemple, on utilise la confluence du calcul pour β-réduction, mais la confluence n'est pas valable sur les termes en général si on ajoute η-réduction. C'est le contre-exemple de Nederpelt (1973) $\lambda_{x:A}(\lambda_{y:B}y)\ x$ se réduit en $\lambda_{y:B}y$ et $\lambda_{x:A}x$

Comment formuler les univers ? Avec fonction de décodage ou non ?

Il n'est pas si clair de donner des modèles de ce calcul.

À la place, ⟪jugement⟫ d'égalité, et étude systématique des *modèles*, ce qui va être fait dans la prochaine leçon.

La bibliothèque de Babel : le programme de Ralph Loader

On peut coder les entiers en suivant Wittgenstein/Church $N = \Pi_{X:o} X \to (X \to X) \to X$

On peut aussi coder les ordinaux $Ord = \Pi_{X:o} X \to (X \to X) \to ((N \to X) \to X) \to X$

On peut définir des hiérarchies de fonctions le long des ordinaux, par exemple celle de Hardy (1904)

$$h\ 0\ n = n \qquad h\ (x+1)\ n = h\ x\ (n+1) \qquad h\ (\mathsf{lim}\ u)\ n = h\ (u\ n)\ n$$

Par exemple, $h\ \epsilon_0$ est une fonction qui n'est pas prouvablement totale dans PA

Il y a une définition très simple de ϵ_0 de *manière imprédicative*.

Une définition *prédicative* est possible, mais beaucoup plus complexe.

Ce genre de question est mentionnée par Hilbert (1925,1927)

La bibliothèque de Babel : le programme de Ralph Loader

Ceci montre que l'on peut décrire des entiers très grand de manière concise dans ce système

Mais ceci suppose par exemple la création de hiérarchie de fonctions, ou d'ordinaux.

Peut-on faire mieux?

The Bignum Bakeoff was a programming contest held by David Moews in December 2001. The object of the competition is to write a C program with at most 512 characters (ignoring whitespace) that returns the largest possible number, assuming a computer with infinite resources.

La bibliothèque de Babel : le programme de Ralph Loader

Comment écrire un ⟪très grand nombre⟫ par un programme ayant moins de 512 caractères?

On écrit un programme qui liste *tous* les termes de taille limitée fixée et on prend la somme de toutes les valeurs des termes de type N dans cette liste. Il est essentiel d'avoir un programme de typage.

Loader écrit un tel programme (2001) qui réalise un *parser, proof-checker, interpreter and proof-search implementation* tout ceci en moins de 512 caractères.

On obtient de cette manière un programme qui décrit un entier gigantesque, sans avoir à trouver un système de notation ingénieux (de tels systèmes vont apparaitre dans cette liste).