Théorie des types dépendants et axiome d'univalence

Thierry Coquand

Séminaire Bourbaki, 21 Juin 2014

Fondements des mathématiques

«on sait aujourd'hui qu'il est possible, logiquement parlant, de faire dériver toute la mathématique actuelle d'une source unique, la théorie des ensembles ... Ce faisant, nous ne prétendons pas légiférer pour l'éternité; il se peut qu'un jour les mathématiciens s'accordent à se permettre des modes de raisonnement non formalisables dans le langage exposé ici; suivant certains, l'évolution récente des théories d'homologie dites axiomatiques donnerait à penser que ce jour n'est pas si éloigné. *Il faudrait alors, sinon changer complètement de langage, tout au moins élargir les règles de la syntaxe.* C'est à l'avenir qu'il appartiendra d'en décider.»

Bourbaki, introduction au livre I (théorie des ensembles)

Fondements des mathématiques

Programme de Voevodsky pour exprimer les mathématiques en

théorie des types dépendants

au lieu d'utiliser la

théorie des ensembles

Fondements des mathématiques

Ce programme repose sur les 2 points suivants

(1) description/vision des mathématiques comme analyse des *structures sur les ∞-groupoïdes*

(2) la théorie des types *dépendants* fournit un langage et un système de notations appropriés pour représenter de telles structures sur les ∞-groupoïdes

Description des objets mathématiques

Niveau de ≪base≫ : structures algébriques et structures d'ordre

E.g. groupes, anneaux, treillis

Ensemble muni d'opérations et/ou de relations satisfaisant certaines propriétés

A ce niveau on peut parler de ≪structures initiales≫

Unicité à isomorphisme près

C'est le niveau considéré par Bourbaki dans sa *théorie des structures*

Description des objets mathématiques

Le niveau suivant est décrit d'habitude comme celui des *catégories*

En fait, le niveau suivant est celui des *structures sur les groupoïdes*

(Une catégorie est l'analogue d'une structure d'ordre à ce niveau)

L'égalité ensembliste correspond à la notion d'isomorphisme

La notion d'isomorphisme correspond à la notion d'*équivalence catégorique*

Description des objets mathématiques

Au niveau suivant on a les structures sur les 2-*groupoïdes*

En continuant n-groupoïdes, puis ∞-groupoïdes

« À ce moment apparait l'intuition que les ∞-groupoïdes doivent constituer des modèles, particulièrement adéquats, pour les types d'homotopie, les n-groupoïdes correspondant aux types d'homotopie tronqués (avec $\pi_i = 0$ pour $i > n$) »
(Grothendieck, Esquisses d'un programme)

Les types d'homotopie généralisent les ensembles

La notion d'équivalence (d'homotopie) généralise la notion de bijection

Description des objets mathématiques

Une telle description a été tentée par Makkai (1995)

First Order Logic with Dependent Sorts with Application to Category Theory

Cette description des objets mathématiques a une représentation formelle particulièrement simple en *théorie des types dépendants*

La notion d'∞-groupoïde devient une notion primitive

Les notions d'ensemble, de groupoïde, de 2-groupoïde, $\ldots$ sont dérivées

Théorie des ensembles et théorie des types

1908 Zermelo *Untersuchungen über die Grundlagen der Mengenlehre*

1908 Russell *Mathematical Logic as Based on the Theory of Types*

Théorie des types ⟪simples⟫

1940 Church *A Formulation of the Simple Theory of Types*

Une notion de type extrêmement simple et naturel

Un type $bool$ qui représente le type des ⟪propositions⟫

Un type I qui représente un type des ⟪individus⟫

Un type de fonctions $A \to B$

Par exemple la fonction identique est de type $A \to A$

Sémantique naturelle des *types* comme *ensembles*

Fonctions en théorie des types simples

En théorie des ensembles, une fonction est un *graphe fonctionnel*

En théorie des types, une fonction est donnée par une *définition explicite*

Si $t : B$, on peut introduire la fonction f de type $A \to B$ par la définition

$$f(x) = t$$

$f(a)$ se «réduit» sur $(a/x)t$ si a est de type A

Fonctions en théorie des types

On obtient deux notions de fonction, comme

-*graphe fonctionnel* ou comme

-*fonction définie explicitement* par un terme

Comment relier ces deux notions de fonction ?

Church introduit un opérateur $\iota x.\varphi$ et l'«axiome de description»

Si $\exists! x : A.\varphi$ alors $\varphi(\iota x.\varphi)$

Fonctions en théorie des types

On peut alors définir une fonction à partir d'un graphe fonctionnel

$\forall x.\exists! y.\psi(x,y) \to \exists f.\forall x.\psi(x,f(x))$

en posant $f(x) = \iota y.\psi(x,y)$

L'opérateur $\epsilon x.\varphi$ de Hilbert, adopté par Bourbaki, vérifie

si $\exists x : A.\varphi$ alors $\varphi(\epsilon x.\varphi)$

Utiliser $\exists! x : A.\varphi$ suppose que l'on a une notion d'égalité sur le type A

Les lois de l'égalité

L'égalité est caractérisée par les lois purement logiques

(1) $a =_A a$

(2) si $a_0 =_A a_1$ et $P(a_0)$ alors $P(a_1)$

Égalité en mathématique

Le premier axiome de la théorie des ensembles est l'axiome d'extensionalité qui dit que deux ensembles qui ont les mêmes éléments sont égaux

Dans le système de Church on a deux formes de l'axiome d'extensionalité

(1) deux propositions logiquement équivalentes sont égales

$$(\varphi \equiv \psi) \;\rightarrow\; \varphi =_{bool} \psi$$

(2) deux fonctions égales en chaque point sont égales

$$(\forall x : A.f(x) =_B g(x)) \quad \rightarrow \quad f =_{A\rightarrow B} g$$

L'axiome d'univalence sera une généralisation de l'axiome (1)

Types dépendants

La notion de base est celle de famille de types $B(x),\ x : A$

On décrit directement certaines opérations *primitives*

$(\Pi x : A)B(x)$	$f \quad \text{avec } f(x) = b$
$(\Sigma x : A)B(x)$	(a, b)
$A + B$	$\mathsf{i}(a), \mathsf{j}(b)$

qui sont des opérations *dérivées* en théorie des ensembles

Types dépendants

Les opérations logiques sont réduites à des constructions sur les types suivant le dictionnaire suivant

$A \wedge B$	$A \times B = (\Sigma x : A)B$
$A \vee B$	$A + B$
$A \to B$	$A \to B = (\Pi x : A)B$
$(\forall x : A)B(x)$	$(\Pi x : A)B(x)$
$(\exists x : A)B(x)$	$(\Sigma x : A)B(x)$

Types dépendants

de Bruijn (1967) reconnait que cette approche est très appropriée pour représenter les preuves mathématiques sur ordinateur (système AUTOMATH)

Prouver une proposition revient à construire un élément d'un type donné

Approche utilisée pour la formalisation du théorème de Feit-Thompson

Le programme de Voevodsky précise cette représentation en caractérisant quels sont les types qui correspondent aux propositions

Univers

Univers : un type dont les éléments sont des types et clos par les opérations

$$(\Pi x : A)B(x) \qquad (\Sigma x : A)B(x) \qquad A + B$$

Le paradoxe de Russell ne s'exprime pas directement car on ne peut *pas* former un *type* exprimant $X : X$

Girard (1971) montre cependant que l'on peut représenter le paradoxe de Burali-Forti si on introduit un type de tous les types

Univers

Martin-Löf, suivant Grothendieck, introduit une hierarchie d'univers

$$U_0 : U_1 : U_2 : \ldots$$

Chaque universe U_n est clos par les opérations

$$(\Pi x : A)B(x) \qquad (\Sigma x : A)B(x) \qquad A + B$$

Univers et sommes dépendantes

Représentation formelle de la notion de structure

$(\Sigma X : U_0)((X \times X \to X) \times X)$

collection des types avec une opération binaire et une constante

$(X \times X \to X) \times X$ définit une famille de types sur $X : U_0$

C'est cette représentation qui est utilisée par Girard pour exprimer le paradoxe de Burali-Forti

Des lois nouvelles pour l'égalité

Martin-Löf introduit (1973) une notion primitive d'égalité en théorie des types dépendants

La « proposition » exprimant que deux éléments a_0 et a_1 d'un type A sont égaux devient une famille de type $\mathsf{Eq}_A(a_0, a_1)$

Comme $\mathsf{Eq}_A(a_0, a_1)$ est lui-même un type, on peut itérer cette construction

$$\mathsf{Eq}_{\mathsf{Eq}_A(a_0,a_1)}(p, q)$$

Cette itération contient en germe la connection avec les ∞-groupoïdes

Des lois nouvelles pour l'égalité

Quelles sont les lois de l'égalité dans ce système ?

(1) Tout élément est égal à lui-même $1_a : \mathsf{Eq}_A(a, a)$

(2) $C(a)$ implique $C(x)$ si on a $p : \mathsf{Eq}_A(a, x)$

Des lois nouvelles pour l'égalité

La loi *nouvelle* mise en évidence par Martin-Löf (1973) est que dans le type

$$(\Sigma x : A)\mathsf{Eq}_A(a, x)$$

qui contient l'élément

$$(a, 1_a) : (\Sigma x : A)\mathsf{Eq}_A(a, x)$$

tout élément (x, ω) est en fait *égal* à cet élément $(a, 1_a)$

Des lois nouvelles pour l'égalité

Il résulte de ces lois que tout type est muni d'une structure d'∞*-groupoïde*

Par exemple, la composition correspond à la transitivité de l'égalité

Le fait que l'égalité est symétrique entraine l'existence d'inverse

Hoffman-Streicher (1995)

S. Awodey, M. Warren (2009), P. Lumsdaine (2010)

Des lois nouvelles pour l'égalité

Martin-Löf a formulé ces lois en 1973

Est-ce que cette égalité doit satisfaire les axiomes d'extensionalité ?

En fait, que deviennent les axiomes d'extensionalité dans ce contexte ?

Une réponse à ces questions a été apportée par Voevodsky (2009)

Stratification des types

Un type A est une *proposition*

$(\Pi x_0 : A)(\Pi x_1 : A)\mathsf{Eq}_A(x_0, x_1)$

Un type est un *ensemble*

$(\Pi x_0 : A)(\Pi x_1 : A)\mathsf{prop}(\mathsf{Eq}_A(x_0, x_1))$

Un type est un *groupoïde*

$(\Pi x_0 : A)(\Pi x_1 : A)\mathsf{set}(\mathsf{Eq}_A(x_0, x_1))$

Stratification des types

Les notions de *propositions*, *ensembles*, *groupoïdes* ont maintenant une signification précise

Elles seront utilisées uniquement en ce sens dans le reste de cet exposé

La théorie des types apparait alors comme une généralisation *de la théorie des ensembles*

Équivalence

Voevodsky donne une définition très simple et uniforme d'une notion d'équivalence pour $f : A \to B$

Si A et B sont des *ensembles* on retrouve la notion de *bijection* entre ensembles

Si A et B sont des *propositions* on retrouve la notion d'équivalence logique entre propositions

Si A et B sont des *groupoïdes* on retrouve la notion d'équivalence catégorique entre groupoïdes

Équivalence

Si $f : A \to B$ la *fibre* de f en $b : B$ est le type

$F(b) = (\Sigma x : A)\mathsf{Eq}_B(b, f(x))$

f est une *équivalence* si cette fibre est *contractile* en chaque point b

$(\Pi b : B)(F(b) \times \mathsf{prop}(F(b)))$

$A \simeq B$ sera $(\Sigma f : A \to B)\mathsf{Equiv}(f)$

Par exemple, l'application identique est une équivalence en utilisant la nouvelle loi de l'égalité découverte par Martin-Löf et donc on a $A \simeq A$

L'Axiome d'Univalence

L'*Axiome d'Univalence* dit en gros que si $f : A \to B$ est une équivalence alors A et B sont égaux

Plus précisément, comme $A \simeq A$ on a une application $\mathsf{Eq}_U(A, B) \to A \simeq B$

cette application canonique $\mathsf{Eq}_U(A, B) \to A \simeq B$ *est une équivalence*

Ceci généralise l'axiome d'extensionalité pour les *propositions* dans le système de Church

Voevodsky a montré que cet axiome entraine l'axiome d'extensionalité pour les *fonctions*

L'Axiome d'Univalence

$\mathsf{Eq}_U(A \times B, B \times A)$

$\mathsf{Eq}_U(A \times (B \times C), (A \times B) \times C)$

Toute propriété de $A \times B$, si elle s'exprime en théorie des types, est aussi vérifiée pour $B \times A$

Ceci n'est pas valable en général en théorie des ensembles

$(1, -1) \in \mathbb{N} \times \mathbb{Z}$ $\qquad$ $(1, -1) \notin \mathbb{Z} \times \mathbb{N}$

L'Axiome d'Univalence

Cet axiome entraine aussi

-des ensembles isomorphes sont égaux

-des structures algébriques isomorphes sont égales

-des groupoïdes équivalents (au sens catégorique) sont égaux

-des catégories équivalentes sont égales

L'égalité de a et b entraine que toute propriété de a est aussi valide pour b

Structures algébriques

Les structures algébriques seront éléments d'un type de la forme

$(\Sigma X : U_0)\mathsf{set}(X) \times T(X)$

ensembles munis d'opération et de propriété

Sémantique

Il est naturel d'interpréter un type comme un *type d'homotopie*

D. Kan *A Combinatorial Definition of Homotopy Groups*, 1958

Un type est interprété par un ensemble simplicial vérifiant la condition de Kan

Une famille de type $B(x),\ x : A$ est interprétée par une *fibration* de Kan

Le type $\mathsf{Eq}_A(a_0, a_1)$ est l'espace des *chemins* entre a_0 et a_1

L'axiome d'univalence est justifié dans ce modèle

Sémantique

Que devient la nouvelle loi sur l'égalité découverte par Martin-Löf dans cette interprétation ?

Tout élément de $(\Sigma x : A)\mathsf{Eq}_A(a, x)$ est égal à $(a, 1_a)$

Elle dit que l'espace total de la fibration définie par l'espace des chemins ayant une origine fixée est *contractile*

C'est exactement ce fait qui est à l'origine de la méthode de l'espace des chemins en topologie algébrique (J.P. Serre)

Transport de structures

Soit $\mathsf{Grp}(A)$ le type qui donne une structure de groupe sur A

$\mathsf{Grp}(A) = (\Sigma f : A \to A \to A)(\Sigma a : A) \dots$

La collection des groupes sera $(\Sigma X : U_0)\mathsf{set}(X) \times \mathsf{Grp}(X)$

Ce type est un groupoïde

Transport de structures

Si A et B sont des ensembles isomorphes, on a une preuve de

$$\mathsf{Eq}_U(A, B)$$

par l'axiome d'univalence, et donc une preuve de

$$\mathsf{Grp}(A) \to \mathsf{Grp}(B)$$

Ceci réalise le *transport de structure* (Bourbaki) de groupe le long de l'isomorphisme entre A et B

Différences avec la théorie des ensembles

Toute propriété est transportable

Pas besoin de « critères de transportabilité » comme en théorie des ensembles

« La pratique seule peut enseigner dans quelle mesure l'identification de deux ensembles, munis ou non de structures, présente plus d'avantages que d'inconvénients. Il est nécessaire en tout cas, lorqu'on l'applique, qu'on ne soit pas exposé à décrire des relations non transportables. »

Bourbaki, Théorie des Ensembles, Chapitre 4, Structures (1957)

$0 \in A$ est une propriété non transportable d'un groupe

« être résoluble » est une propriété transportable

Différences avec la théorie des ensembles

La collection des groupes/anneaux/ensembles ordonnés forme un groupoïde

U_0 n'est pas un ensemble (au moins un groupoïde)

U_1 n'est pas un groupoïde (au moins un 2-groupoïde)

Complexité de l'égalité d'un type versus ⟪taille⟫ ensembliste

Ensembles ordonnés et catégorie

Dans cette approche

la notion de groupoïde est plus fondamentale que la notion de catégorie

Un groupoïde est défini comme un type vérifiant une propriété

Ensembles ordonnés et catégorie

Un *préordre* est un *ensemble* A muni d'une relation $R(x, y)$ vérifiant

$$(\Pi x : A)(\Pi y : A)\mathsf{prop}(R(x, y))$$

et qui est transitive, réflexive

Ceci définit un préordre

Un *ensemble ordonné* est un préordre tel que l'implication canonique

$$\mathsf{Eq}_A(x, y) \to R(x, y) \times R(y, x)$$

est une équivalence logique

Ensembles ordonnés et catégorie

Une *catégorie* est un *groupoïde* A muni d'une relation $\mathsf{Hom}(x, y)$ qui vérifie

$$(\Pi x : A)(\Pi y : A)\mathsf{set}(\mathsf{Hom}(x, y))$$

Cette famille d'ensemble est « transitive » (on a une opération de composition associative) et « réflexive » (on a un élément neutre pour la composition)

Ceci correspond à la notion de préordre

Ensembles ordonnés et catégorie

On peut définir $\mathsf{Iso}(x, y)$ qui est un *ensemble* et montrer que l'on a $\mathsf{Iso}(x, x)$

Ceci détermine une application canonique

$$\mathsf{Eq}_A(x, y) \to \mathsf{Iso}(x, y)$$

On demande que cette application soit une équivalence (bijection) entre les deux *ensembles* $\mathsf{Eq}(x, y)$ et $\mathsf{Iso}(x, y)$

L'axiome d'univalence entraine que le groupoïde des anneaux, par exemple, forme une catégorie

Existence

Dans le modèle simplicial on peut définir un opérateur

$$\mathsf{inh}(A)$$

qui est une *proposition* exprimant que A a au moins un élément

Structure au niveau des groupoïdes

Si G est un groupe, on peut considérer le type des G-*torseurs*

Un G-torseur est un *ensemble* A muni d'une G-action telle que

(1) l'application $G \to A,\ g \longmapsto ag$ est une équivalence (i.e. bijection) si $a : A$

(2) $\mathsf{inh}(A)$

Ce type des G-torseurs est un *groupoïde* qui est l'espace classifiant de G

Graphes et fonctions

On définit $(\exists x : A)B$ comme étant $\mathsf{inh}((\Sigma x : A)B)$

C'est une nouvelle opération sur les types suggérée par cette approche

Contrairement à $(\Sigma x : A)B$ on ne *peut pas* en général extraire un témoin d'une preuve de $(\exists x : A)B$

Toutefois cette extraction est possible dès que $(\Sigma x : A)B$ est une *proposition*

Graphes et fonctions

En particulier si $B(x)$ est une proposition et

$B(x_0) \to B(x_1) \to Id_A(x_0, x_1)$

Dans ce cas $(\Sigma x : A)B(x)$ est une proposition et on a

$(\exists x : A)B(x) \to (\Sigma x : A)B(x)$

Ceci *justifie* l'axiome de description de Church

Mais ceci s'applique aussi pour des situations où $B(x)$ est un ensemble

Graphes et fonctions

Par exemple on peut montrer *sans utiliser l'axiome du choix* qu'un foncteur pleinement fidèle et essentiellement surjectif est une équivalence de catégorie

Si $F : A \to B$ est pleinement fidèle, alors pour chaque objet b de B le groupoïde $(\Sigma x : A)\mathsf{Iso}(F(x), b)$ est une *proposition*

Si F est aussi essentiellement surjectif on peut donc définir (effectivement) son ⟪ inverse ⟫

L'existence est effective si elle est unique à isomorphisme près

Complexité de l'égalité

Dans la définition d'une catégorie, $\mathsf{Hom}(x_0, x_1)$ doit être un ensemble

Formellement similaire à la définition de catégorie *localement petite*

Mais ici ce qui est important est crucialement la

complexité de l'égalité

du type $\mathsf{Hom}(x_0, x_1)$ et non sa

《taille》 ensembliste

Directions nouvelles

Un type $(\Sigma X : U_2)\mathsf{Eq}_{U_2}(U_1, X)$ est intuitivement très ≪gros≫ (dans U_3)

Mais c'est une proposition

≪Axiome de redimensionnement≫ (Voevodsky)

si A est un type qui est une proposition alors A est dans U_0

La distinction entre complexité de l'égalité et taille ensembliste sera sans doute fondamentale pour une analyse plus fine des paradoxes