Type Theory and Constructive Mathematics

Thierry Coquand

Function, Proofs, Constructions, February 21, 2014

This talk

Design of a formal system for representing constructive mathematics

We discuss: existence, equality, unique choice, functions

Motivated by Voevodsky Univalent Foundation project

Strong Existence

Represented in type theory as $(\Sigma x : A)B$

The elements are pair (a, b)

If $w : (\Sigma x : A)B$ we have access to $w.1 : A$ and $w.2 : B[w.1]$

$(a, b).1 = a : A$ $\qquad$ $(a, b).2 = b : B[a]$

We get stronger laws than the usual law for existential quantification

"Strong" existence vs "weak" existence (Howard, 1969)

Strong Existence

Seems to be what "existence" means in constructive mathematics

E.g. Bishop's statement

"A choice function exists in constructive mathematics because a choice is *implied by the very meaning of existence*"

Using only this notion of existence raises however some problem

Strong Existence

(Kreisel, A. Bauer, M. Escardo)

We formulate the continuity principle for functions on Baire space (Brouwer)

$$\mathsf{CP} = (\Pi F : (N \to N) \to N)(\Pi f : N \to N)(\Sigma n : N)\mathsf{MC}(F, f, n)$$

where the modulus relation is defined as

$$\mathsf{MC}(F, f, n) = \\ (\Pi g : N \to N)\ \ ((\forall k \leqslant n)\ f\ k =_N g\ k) \quad \to \quad F\ f =_N F\ g$$

We can *prove* $\neg\mathsf{CP}$ in type theory

Strong Existence

Reminiscent of the situation with Church's Thesis

We can prove the negation of Church's Thesis given function extensionality (which is implied by the equality reflection rule)

One motivation (among others) for not having the equality reflection rule

But here we can prove $\neg$CP without using function extensionality

Strong Existence

A serious problem for representing mathematics in type theory?

Arguable whether Brouwer's continuity principle should be provable or not

But it does not seem suitable to have a formal system for constructive mathematics where we can show the *negation* of Brouwer's continuity principle

What was the notion of existence Brouwer was using when formulating this principle?

The root of the problem seems to be the use of strong existence to express the existence of the modulus of continuity

Existence and Equality

This suggests that a formal system for constructive mathematics should contain a notion of "weak" existence $(\exists x : A)B$ as well

We present one way to formulate this notion

This will also be a constructive notion of existence, but in a more subtle way

Essential use of the identity type $\mathsf{Id}_A\ a_0\ a_1$ introduced by P. Martin-Löf 1973

Propositions

Propositions are types that have at most one element

We define "A is a *proposition*" to mean

$\mathsf{prop}(A) \;=\; (\Pi x_0\ x_1 : A)\mathsf{Id}_A\ x_0\ x_1$

For instance the unit type N_1 and the empty type N_0 are propositions

For N_0 we use N_0 elimination

Any "singleton" type $(\Sigma x : A)\mathsf{Id}_A\ a\ x$ is a proposition

Modality

We add a new modality operation

$\mathsf{inh}(A)$ is a *proposition* stating that A is inhabited

The laws are $\mathsf{prop}(\mathsf{inh}(A))$ and

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

as soon as we have $A \to B$ and $\mathsf{prop}(B)$.

Weak existence

We *define* $(\exists x : A)B$ to mean

$\mathsf{inh}((\Sigma x : A)B)$

We can now formulate without problem

$\mathsf{CP} = (\Pi F : (N \to N) \to N)(\Pi f : N \to N)(\exists n : N)\mathsf{MC}(F, f, n)$

Weak existence

One key point is that we have

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

as soon as $(\Sigma x : A)B$ is a proposition

Indeed we have $\mathsf{inh}(P) \to P$ if P is a proposition

Weak existence

For having

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

it is enough that $B(x),\ x : A$ is a family of propositions and

$B(x_0) \wedge B(x_1) \rightarrow \mathsf{Id}_A\ x_0\ x_1$

In particular we have

$(\exists! x : A)B \rightarrow (\Sigma x : A)B$

Weak existence

The implication

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

does not hold in other previous attempt to introduce a weak existence statement in type theory

E.g. Aczel-Gambino logic-enriched type theory

Intuitively in these previous attempt, a proof of a type which is a proposition had no "computational content"

The notion of proposition is a *defined* notion

A proof of a proposition may have a computational content

Unique Choice

We also have the principle of unique choice

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

Without this principle, we would have *two* notions of functions

Function as term or as functional relation

Compare with Maietti-Sambin approach, where this principle is not present

I believe that having this principle is necessary for mathematics

Stratification of Types

"A is a *set*" means

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

"A is a *groupoid*" means

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

Constructive matematics

If B is a type and $P(y)$ a family of propositions over B then the first projection

$(\Sigma y : B)P(y) \ \rightarrow B$

is injective

$(\Sigma y : B)P(y)$ represents the *subset* of elements of B satisfying P

Subsets

If B is a set, a *subset* of B is defined to be a set A with an *injective* map

$f : A \to B$

$Id_B\ (f\ a_0)\ (f\ a_1) \to \mathsf{Id}_A\ a_0\ a_1$

Bishop's definition

Constructive matematics

If $f : A \to B$ we can define the *image* of f

$P_f(y) = (\exists x : A)\mathsf{Id}_B\ (f\ x)\ y$

and $P_f(y)$ is a proposition

If A, f is a subset of B, we can define an *isomorphism* between

$(\Sigma y : B)P_f(y)$ and A

using *unique choice*

Constructive matematics

Thus we have a good correspondance between

subsets

and

properties

which is essential for the development of mathematics

Some example in algebra

A *ring* R will be represented as a *set* with the usual structure

a divides b will be defined as *there exists* x such that $ax = b$

If a is *regular* i.e. $au = 0 \to u = 0$ then this x is *uniquely determined* and we have an explicit division operation

Some example in algebra

An exact sequence $0 \longrightarrow E \xrightarrow{f} F \xrightarrow{g} G$

f is injective and the image of f is equal to the kernel of g

We can show that E is isomorphic to the kernel of g

Some example in algebra

An *ideal* of R will be represented by a *subset* I of R

I *finitely generated* means that *there exists* a finite list of elements of R generating R

$a_1, \ldots, a_n$ generates I means that for all x in I *there exists* $u_1, \ldots, u_n$ such that $x = a_1u_1 + \cdots + a_nu_n$

We can *use* a finite list of generators of I but only for building objects in a canonical way

Some example in algebra

For instance we can define $Gr(I) \geqslant 2$ to mean that if $a_1, \ldots, a_n$ is a system of generators and $b_1, \ldots, b_n$ is proportional to $a_1, \ldots, a_n$ there exists a unique x such that $b_i = xa_i$

This is *because* one can show that this property does not depend on the system of generators and hence that this is a well defined notion

(For this we need that two equivalent propositions are equal)

Some example in algebra

More generally, if we define an element $t(x_1, \ldots, x_n)$ in a set A

and we furthermore have

$\mathsf{Id}_A\ t(x_1, \ldots, x_n)\ t(y_1, \ldots, y_m) : A$

whenever $x_1, \ldots, x_n$ and $y_1, \ldots, y_m$ generate the same ideal

Then we can define $t(I) : A$ given a finitely generated ideal I using that there exists a unique element $u : A$ such that

$u = t(x_1, \ldots, x_n) : A$

for some generating system $x_1, \ldots, x_n$ of I

This approach

In constructive mathematics one works with a given *presentation* of a mathematical object

In this approach the typing system ensures that we only can define other objects in a way which is independent of the chosen presentation

Formal system

What did we need?

-Dependent type theory

-Identity types, with the usual laws

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

Theorem: *This formal system has a constructive (realizability) model*

This gives in particular a constructive explanation of the description operator

This model also validates function extensionality (and Voevodsky's Axiom of Univalence)

New directions for the analysis of paradoxes

In order to avoid paradoxes (Girard) Martin-Löf introduced a hierarchy of universes

$U_0 : U_1 : U_2 : \ldots$

Tempting to introduce the new principle that if A is a proposition then

$A : U_0$

And also that $(\Sigma A : U_0)\mathsf{prop}(A)$ is in U_0

New directions for the analysis of paradoxes

This however is in conflict with the notion of "size"

It is a consequence of the laws of identity in type theory that any type $(\Sigma x : A)\mathsf{Id}_A\ a\ x$ is a proposition

So for instance a type like $(\Sigma X : U_2)\mathsf{Id}_{U_2}\ U_1\ X$ should be in U_0 though it should be in U_3 if we look at its "size"

This appears to be as a very strong form of impredicativity

Is it possible to show that this is contradictory?

Or to prove (impredicatively) normalization of our realizability model?

Some references

S. Awodey and M. Warren *Homotopy theoretic model of identity types*, 2009

M. Hofmann and Th. Streicher *A groupoid model of type theory*, 1993

M.E. Maietti and G. Sambin *A minimalist two-level foundations for constructive mathematics*

V. Voevodsky *Univalent foundation*, home page

HoTT book, 2013

M. Escardo, home page

M. Bezem, Th. C., S Huber
A cubical set model of type theory, preprint, 2013