Univalent Foundation and Constructive Mathematics

Thierry Coquand

Oberwolfach, November 21, 2014

Family of sets over a set

Cf. Exercice 3.2 in Bishop's book

In the first edition, only families over discrete sets are considered while the Bishop-Bridges edition presents a more general definition, due to F. Richman

A course in constructive algebra, Mines,Richman and Ruitenburg

Family of sets over a set

We have a dependent type $A(i),\ i : I$

We have transport functions $f_p : A(i) \to A(j)$ for $p : \mathsf{Eq}_I(i, j)$

Since I is a *set* we have $\mathsf{Eq}(f_p, f_q)$ if $q : \mathsf{Eq}_I(i, j)$

We also get the coherence conditions that are part of Richman's definition

Family of sets over a set

Equality in a sigma type

$\mathsf{Eq}_{(\Sigma i:I)A(i)}((i,x),(j,u))$

is equal to

$(\Sigma p : \mathsf{Eq}_I(i,j))\mathsf{Eq}_{A(j)}(f_p(x),y)$

It is essential to have the transport function

Cf. *A course in constructive algebra*, p. 18

« An element of the disjoint union of a family $(A_i)_{i\in I}$ is a pair (i,x) such that $i \in I$ and $x \in A_i$. Two elements (i,x) and (j,y) of the disjoint sum are equal if $i = j$ and $A^i_j(x) = y$ »

Existence

Voevodsky also introduces a new *modal* operation

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

which is a *proposition* expressing that A is inhabited

A is an arbitrary type

Existence

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

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

(3) $\mathsf{inh}(A) \to \mathsf{prop}(X) \to (A \to X) \to X$

Functions and graphs

We define $(\exists x : A)B$ to be $\mathsf{inh}((\Sigma x : A)B)$

This is a *new* operation on types suggested by this approach

We *cannot* in general extract a witness from a proof of $(\exists x : A)B$, contrary to $(\Sigma x : A)B$

However this extraction is possible whenever $(\Sigma x : A)B$ is a *proposition*

Graphs and functions

In particular if $B(x)$ is a proposition and

$B(x_0) \to B(x_1) \to \mathsf{Eq}_A(x_0, x_1)$

In this case $(\Sigma x : A)B(x)$ is a proposition and we have

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

This *justifies* Church's description axiom

But this applies to more general situation

$\mathbb{Z}$-Torsors

A torsor is a set X with a $\mathbb{Z}$-action such that for any u in X the map $n \longmapsto u + n,\ \mathbb{Z} \to X$ is an equivalence

and $\mathsf{inh}(X)$

If X is a torsor we cannot in general exhibit one element of X

cf. D. Grayson Foundations.Ktheory

Torsors

If X is a torsor we have

$(\Pi u_0\ u_1 : X)(\exists! n : \mathbb{Z})\mathsf{Eq}_X(u_0 + n, u_1)$

and so, by *unique choice* we have an application

$X \times X \to \mathbb{Z}$

$(u_0, u_1) \longmapsto u_1 - u_0$

such that $\mathsf{Eq}_X(u_0 + u_1 - u_0, u_1)$

An example in analysis

If we define the type of real numbers R as a quotient of the set of Cauchy sequences of rationals

We can define $x\#y$ as meaning $(\exists r > 0) r \leqslant |x - y|$

We can define the inverse function $(\Pi x : R) x\#0 \to R$

This is because the inverse is *uniquely* determined

An example in algebra

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

An ideal is defined as a subset of R satisfying the usual properties

It is *finitely generated* if *there exists* a list of generators

But we don't have access to this list, we can only use it to define notions that are independent of the choice of this list

Constructive mathematics

Similarly we can introduce a new connective

$A \vee B$ defined as $\mathsf{inh}(A + B)$

In general we do not have $A \vee B \to A + B$

If A and B are propositions and $\neg(A \wedge B)$ then $A \vee B \to A + B$

Constructive mathematics

Difference between $\mathsf{inh}(A)$ and $\neg\neg A$

We have $\mathsf{inh}(A) \to \neg\neg A$

Let $P(n)$ be a family of *decidable* propositions over N

Proposition: $\mathsf{inh}((\Sigma n : N)P(n)) \to (\Sigma n : N)P(n)$

This is remarkable since $(\Sigma n : N)P(n)$ needs not be a proposition

Theorem: $\neg\neg((\Sigma n : N)P(n)) \to (\Sigma n : N)P(n)$ *is not provable*

Constructive mathematics

No reason any more why countable choice

$$(\forall n : N)(\exists x : X)R(n, x) \quad \rightarrow \quad (\exists f : N \rightarrow X)(\forall n : N)R(n, f\ n)$$

should hold

Cf. F. Richman "Constructive mathematics without choice" (4 examples in algebra and analysis)

Category Theory

What should be the definition of a category in Bishop's framework?

Intuitively the notion of equality of objects of a category is different than the one for sets

«The collection of binary sequences forms a set because we know what it means for two binary sequences to be equal. Given two groups, or sets, on the other hand, it is generally incorrect to ask if they are equal; the proper question is whether or not they are isomorphic, or, more generally, what are the homomorphisms between them»

A course in constructive algebra

Category theory

The previous definition of category solves some foundational issues that are somewhat disturbing when category theory is formulated in set theory

For instance, what should be a category with binary product?

Should the product of two objects given explicitely as an operation?

We have two notions (if we don't assume choice)

Category theory

In the univalent foundation, there is no problem since the product of two objects is uniquely determined up to isomorphism

And hence *up to equality* by definition of category

Since we have unique choice, we have an explicit product function on objects

Graphs and functions

For instance one can show *without using the axiom of choice* that a fully faithful and essentially surjective functor is an equivalence of categories

If $F : A \to B$ is fully faithful then for each object b of B the groupoid $(\Sigma x : A)\mathsf{Iso}(F(x), b)$ is a *proposition*

If F is also essentially surjective we can define (effectively) its «inverse»

Existence is effective if it is unique up to isomorphism

Complexity of equality

In the definition of category, $\mathsf{Hom}(x_0, x_1)$ has to be a set

This is formally similar to the definition of a *locally small* category

But here what is crucial is the

complexity of equality

of the type $\mathsf{Hom}(x_0, x_1)$ and not its

set theoretic 《size》

Actual formal examples

See

"'Experimental library of univalent formalization of mathematics" V. Voevodsky

Some basic examples

Model

Intended semantics: a type is a "homotopy type"/∞-groupoid

There is a precise definition of ∞-groupoid/homotopy types due to D. Kan

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

Kan simplicial set

Model

This model is non effective

(1) if $E \to B$ Kan fibration and $b_0 \to b_1$ in B then $E(b_0)$ and $E(b_1)$ are homotopy equivalent

Kripke countermodel showing that this cannot be proved effectively (j.w.w. Marc Bezem)

(2) B^A is a Kan simplicial set if B is a Kan simplicial set

Model

In contrast, one important feature of dependent type theory (without the univalence axiom) is that all notions are justified with a direct computational interpretation

I will now present a constructive notion of homotopy types which justifies the axiom of univalence and the modality $\mathsf{inh}(A)$

Model

D. Kan *Abstract Homotopy I*, 1955

uses a simpler notion of cubical set with a Kan filling condition

"Any open box can be filled"

We present an effective presentation of the cubical set model

Cubical set

The basic idea is to describe a topological space by the collection of all continuous maps $[0,1]^n \to X$

If X is a topological space we can consider $X(I)$ set of continuous functions

$$[0,1]^I \to X$$

for I finite set

Elements of I are called symbols/names/dimensions

Cubical sets

We want a "combinatorial" definition, also effective at function types

Goal: to design a system of *notations* for describing the model so that the syntactical description of the model can be seen as an *operational semantics*

Cubical sets

Let $D(I)$ be the free distributive lattice on I

Let $\mathcal{C}$ be the category having for objects finite sets $I, J, \ldots$ and morphisms maps $f : I \to D(J)$

A *cubical set* is a presheaf over the category $\mathcal{C}^{opp}$

Concretely a cubical X set is given by a family of sets $X(I)$ together with restriction maps $u \longmapsto uf$ for $f : I \to J$

If $f : I \to J$ and $g : J \to K$ I write $fg : I \to K$

We have $(uf)g = u(fg)$

Cubical sets

Intuitively an element u in $X(I)$ is a cube in the dimensions in I and uf is a substitution

For instance if u is in $X(i,j,k)$

$f(i) = 0,\ f(j) = j,\ f(k) = 1$ then uf is $u(0,j,1)$

$g(i) = j \wedge k,\ g(j) = j,\ g(k) = 1$ then ug is $u(j \wedge k, j, 1)$

$X(I)$ can be seen as a formal representation of $[0,1]^I \to X$

$i \wedge j$ corresponds to $\min(i,j)$ and $i \vee j$ to $\max(i,j)$

Face maps and strict maps

If we have $f(i) = i$ or $0, 1$ for all i then f represents a *face map*

If f never takes the values $0, 1$ then f is a *strict* map

Strict maps correspond to degeneracies

Any map is a unique composition of a face map and a strict map

Face maps and strict maps

We write $\alpha, \beta, \ldots$ for face maps $\alpha : I \to I_\alpha$

I_α subset of i in I such that $\alpha(i) \neq 0, 1$

The face maps form a partial meet semi-lattice

Whenever $\alpha f = \beta g$ then α and β are compatible

The simplest face maps are of the form $(i0) : I \to I - i,\ (i1) : I \to (i1)$

Connections

If $u = u(i)$ is in $X(i)$ we can consider $u(i \wedge j)$ in $X(i, j)$

This is a square which connects the constant path $u(0)$ to the path $u(i)$

This interprets the law that in the type

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

any element is (path) equal to $(a, 1_a)$

Diagonals

If $u = u(i, j)$ is in $X(i, j)$ we can consider $u(k, k)$ in $X(k)$

This represents the diagonal of the square $u(i, j)$

Cubical sets

A closed type $\vdash A$ will be interpreted as a presheaf over $\mathcal{C}^{opp}$

A closed type $\vdash_I A$ which may depend on the dimension in I will be interpreted as a presheaf over $\mathcal{C}^{opp}/I$

We can write $A(i_1, \ldots, i_n)$ if $I = i_1, \ldots, i_n$

We have $\vdash_J Af$ if $\vdash_I A$ and $f : I \to J$

E.g. if we have $A(i, j)$ we can consider its face $A(0, j)$

Cubical sets

We want a syntax for describing the presheaf model

We introduce judgement $\vdash_I T$ and $\vdash_I a : T$ with the *restriction rule*

$$\frac{\vdash_I T}{\vdash_J Tf} \qquad \frac{\vdash_I a : T}{\vdash_J af : Tf} \qquad f : I \to J$$

More generally we have judgement of the form $\Gamma \vdash_I a : T$ and we have e.g.

$$\frac{\Gamma, x : A \vdash_I t : B}{\Gamma \vdash_I \lambda x.t : (\Pi x : A)B}$$

Cubical sets

Similar categories have been considered in the theory of *nominal sets*

Staton (2010), exercise 9.7 in Andy Pitts' book

Nominal Sets. Names and Symmetry in Computer Science

The interval $\mathbf{I}$ is defined as the presheaf

$\mathbf{I}(L) = D(L)$

We also have a natural operation $\mathsf{Path}(X) = X^{\mathbf{I}}$ which can be described directly

$\mathsf{Path}(X)(L) = X(L, i)$ where i is fresh

Cubical sets

$$x_1 : A_1, \ldots, x_m : A_m \vdash_{i_1,\ldots,i_n} A$$

can also be written

$$i_1 : \mathbf{I}, \ldots, i_n : \mathbf{I}, x_1 : A_1, \ldots, x_m : A_m \vdash A$$

Cubical sets

We introduce the operations, where $\iota_i : J \to J, i$ is the inclusion

$$\frac{\vdash_J T \qquad \vdash_{J,i} a : T\iota_i}{\vdash_J \langle i \rangle a : \mathsf{Path}(T)}$$

$$\frac{\vdash_{J,i} a : T\iota_i}{\vdash_J \langle i \rangle a : \mathsf{Eq}_T\ a(i0)\ a(i1)}$$

$\langle i \rangle a$ can be thought of as ordinary λ-abstraction over names

Name abstraction

If $\vdash a : T$ then $\langle i \rangle (a\iota_i)$ is a constant path

This follows the intuition that symbols can be thought of as elements in $[0, 1]$

$(\langle i \rangle a)g = \langle j \rangle ah$ if $g : J \to K$ and $h = (g, i = j) : J, i \to K, j$

It is simple to show that function extensionality holds in this model

Transport function

What is missing crucially is a rule of the form

$$\frac{\Gamma \vdash_I A : \mathsf{Eq}_U(A_0, A_1)}{\Gamma \vdash_I \mathsf{comp}(A) : A_0 \to A_1}$$

with the regularity condition

$$\mathsf{comp}(A)\ a_0 = a_0 : A_0 = A_1$$

if A is the constant path A_0

Transport function

Bishop's notion of a set

« Each set A will be endowed with a relation $=$ of equality. This relation is a matter of convention, except that it must be an *equivalence relation* »

A cubical set is a higher analog of a collection with a binary relation

We want a way to express that this higher relation is an equivalence relation

This is expressed by the *Kan filling operations*

Kan operations

Let A be a cubical set with Kan operations

It is simple to define directly $\pi_1(A, a)$

An element of this group is a loop at a up to homotopy

Since $\mathsf{Eq}_A(a, a)$ has Kan operations, we can define $\pi_n(A, a)$, e.g.

$\pi_2(A, a) = \pi_1(\mathsf{Eq}_A(a, a), 1_a)$

Cf. D. Kan *Abstract Homotopy I*, 1955

Compare with

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

Transport function

We should have at least the operation

$$\frac{\Gamma \vdash_I A : \mathsf{Eq}_U(A_0, A_1)}{\Gamma \vdash_I \mathsf{comp}(A) : A_0 \to A_1}$$

and we require

$$\mathsf{comp}(A)f = \mathsf{comp}(Af)$$

if $f : I \to J$

Transport function

We need to express that

$$\Gamma \vdash_I \mathsf{Eq}_A(a_0, a_1)$$

has a composition operation as well

This will be expressed by a more general composition operations *on* A similar to the general Kan ⟪composition⟫ operation

Transport function

Using connection, we can reduce the path lifting operation to transport

$$\mathsf{fill}_A(a_0) = \langle i \rangle \mathsf{comp}(\langle j \rangle A(i \wedge j))\ a_0 \iota_i$$

Allows for a simple definition of the composition operations of a product type

We then define the Kan operations by induction on the type A

The most complex case is for a universe

A similar algorithm transforms any equivalence $\sigma : A \to B$ to an equality $A \to B$ (path in the universe)

Implementation

The system is simple enough to be represented in Haskell

j.w.w. Cyril Cohen, Simon Huber and Anders Mörtberg

Experimental version

https://github.com/simhu/cubical

on the branch

connections_hsplit

Implementation

This gives a type theory where types represent homotopy types

In particular, we can *effectively* transport structures along equivalences

Implementation

The system we interpret contains the rules of Martin-Löf type theory with intensional equality

But the justification of the rules for equality is different

In Martin-Löf type theory equality is inductively defined (least reflexive relation)

Here, equality on A is explained by induction on A

The axiom of univalence and function extensionality are justified by this explanation

Implementation

This explanation suggests new operations

Dependent equality

Map on path as a primitive operation with new judgemental equalities

We can implement/justify the modality $\mathsf{inh}(A)$

We can also represent higher inductive types (S^1, pushout, suspension, proof that S^1 is equal to the suspension of Bool)