A Cubical Type Theory

Nijmegen, June 23, 2015

A Cubical Type Theory

Joint work with Cyril Cohen, Simon Huber and Anders Mörtberg

Thanks to Marcelo Fiore,Georges Gonthier, Andy Pitts, Bas Spitters, Vladimir Voevodsky for many discussions

Thanks to Dan Licata for pointing out an important mistake in a preliminary version of this work

A Cubical Type Theory

(1) constructive mathematics and algebraic topology

(2) nominal extension of type theory, syntax and semantics

(3) internal logic

Algebraic topology and constructive mathematics

"Higher-order" structure

A *set* for Bishop is a collection A with an equivalence relation $R(a, b)$

This is the "equality" on the set

If we have two sets A, R and B, S an "operation" $f : A \to B$ may or not preserve the given equality

If f preserves the equality, it defines a *function*

Algebraic topology and constructive mathematics

Propositions-as-Types: each $R(a, b)$ should itself be considered as a collection with an equality

We should have a relation $R_2(p, q)$ expressing when $p\ q : R(a, b)$ are equal

And then a relation $R_3(s, t)$ on the proofs of these relations

and so on

Constructive mathematics

For expressing the notion of dependent set, one needs to conisder explicitely the proofs of equality

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

It is convenient to consider more generally a relation expressing when a square of equality proofs "commutes"

Algebraic topology

Topology: study of *continuity*, “holding together”

Connected: two points are connected if there is a path between them

Algebraic topology: higher notion of connectedness

Algebraic topology

In the 50s, development of a "combinatorial" notion of higher connectedness

D. Kan: first with cubical sets (1955) then with simplicial sets

Moore (1955): these spaces form a cartesian closed category

However, these structures are not as such suitable for constructive mathematics

Proofs of even basic facts are intrinsically not effective

More precisely: if one expresses the definitions as they are in IZF then the basic facts are *not* provable (j.w.w. M. Bezem and E. Parmann, TLCA 2015)

Univalent Foundations

Goal: to find an effective combinatorial notion of spaces with higher-order notion of connectedness

How do we know if this notion is the right one?

Should form a model of dependent type theory with the axiom of univalence

Type Theory

Dependent type theory: $\Pi, \Sigma, U, N, W(A, B), N_0, N_1, N_2 \ldots$

$(x : A) \to B$ for dependent product

$(x : A)\ (y : B) \to C$ for $(x : A) \to (y : B) \to C$

$(x : A, B)$ for dependent sum

$(x : A, y : B, C)$ for $(x : A, (y : B, C))$

Type Theory

First version (1972) presented without equality types

Non trivial: To have an effective model of dependent product with an higher-order structure on equality

(Usual one-line argument *not* valid effectively)

Type Theory

The axiom of univalence can be seen as the expression of the *axiom of extensionality* for dependent type theory

In HOL, two forms of extensionality (A. Church, 1940)

(1) Function extensionality

(2) Two equivalent propositions are equal

Univalent Foundation

1_a : $\mathsf{Id}_A\ a\ a$

$\mathsf{transp} : C(a) \to \mathsf{Id}\ A\ a\ x \to C(x)$

$\mathsf{Id}\ C(a)\ (\mathsf{transp}\ u\ 1_a)\ u$

$\mathsf{Id}\ (x : A, \mathsf{Id}\ A\ a\ x)\ (a, 1_a)\ (x, p)$ ("singleton are contractible")

Axiom of Univalence

Singleton are contractible

In the setting of algebraic topology, this was the starting point of the PhD work of Jean-Pierre Serre (1951)

"Indeed, to apply Leray's theory I needed to construct fibre spaces which did not exist if one used the standard definition. Namely, for every space X, I needed a fibre space E with base X and with trivial homotopy (for instance contractible). But how to get such a space? One night in 1950, on the train bringing me back from our summer vacation, I saw it in a flash: just take for E the space of paths on X (with fixed origin a), the projection $E \to X$ being the evaluation map: path $\to$ extremity of the path. The fibre is then the loop space of (X, a). I had no doubt: this was it! $\ldots$ It is strange that such a simple construction had so many consequences."

Computational Interpretation

Our model *does not* justify all the rules of Martin-Löf type theory with intensional equality

The computation rule for identity elimination is only justified as a *propositional* equality

This is expected when equality is defined by induction on the type

The justification of the rules for equality is *different*

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

Constructive models

For dependent type theory, the computations are done in λ-calculus

For univalence, *nominal* extension of λ-calculus

In particular, we get a justification of *function extensionality* without using function extensionality in the metalogic

Reminiscent of the work on Observational Type Theory, but without proof irrelevance

Nominal λ-calculus

$$\Gamma \ ::= \ () \mid \Gamma, x : A \mid \Gamma, i : \mathbb{I}$$

$$t, A \ ::= \ x \mid \lambda x : A.t \mid t\ t \mid \langle i \rangle t \mid t\ \varphi \mid (x : A) \to A$$

φ is a lattice formula on names

Intuitively, names represent in a formal way element in $[0, 1]$

$\mathsf{max}(i, j),\ \mathsf{min}(i, j),\ 1 - i$

As for Kan cubical sets, use of a *presheaf* model

Nominal λ-calculus

Base category $\mathcal{C}$ cartesian category with a distinguished object $[1]$

A *cubical set* is a presheaf (contravariant functor) on $\mathcal{C}$

The interval $\mathbb{I}$ is the presheaf represented by $[1]$

A line in X is an element of the set $X([1])$

$X^{\mathbb{I}}$ defines the cubical set of paths in X

$(X^{\mathbb{I}})(I) = X(I \times [1])$

We can form the diagonal of any square in $X([1] \times [1])$

Presheaf model

N is modelled as the constant functor

Any function $\mathbb{I} \to N$ is constant

In general any map from a representable to a constant functor is constant

Two natural numbers are connected by a path only if they are equal

Presheaf model

We write $u \longmapsto uf$ the restriction map $X(I) \to X(J)$ if $f : J \to I$

This notation is motivated by the fact that $X(I)$ can be seen as $I \to X$

A context Γ is interpreted as a presheaf

$\Gamma \vdash A$ can be defined as a family of sets $A\rho$ for ρ in $\Gamma(I)$ with restriction maps

$$A\rho \to A\rho f, \quad u \longmapsto uf$$

satisfying $u1_I = u \in A\rho$ and $(uf)g = u(fg) \in A\rho fg$ if $g : K \to J$

Presheaf model

If $\Gamma \vdash A$ we define $\Gamma, x : A$

$(\rho, x = u) \in (\Gamma, x : A)(I)$ if $\rho \in \Gamma(I)$ and $u \in A\rho$

$(\rho, x = u)f = (\rho f, x = uf)$

$\Gamma \vdash a : A$ is given by a family of element $a\rho \in A\rho$ such that

$(a\rho)f = a\rho f \in A\rho f$ if $f : J \to I$

Function extensionality

$$\frac{\Gamma \vdash A \qquad \Gamma, i : \mathbb{I} \vdash t : A}{\Gamma \vdash \langle i \rangle t : \mathsf{Id}\ A\ t(i0)\ t(i1)} \qquad \frac{\Gamma \vdash p : \mathsf{Id}\ A\ a\ b}{\Gamma \vdash p\ 0 = a : A} \qquad \frac{\Gamma \vdash p : \mathsf{Id}\ A\ a\ b}{\Gamma \vdash p\ 1 = b : A}$$

$$\frac{\Gamma \vdash t : (x : A) \to B \quad \Gamma \vdash u : (x : A) \to B \quad \Gamma \vdash p : (x : A) \to \mathsf{Id}\ B\ (t\ x)\ (u\ x)}{\Gamma \vdash \langle i \rangle \lambda x : A.\ p\ x\ i : \mathsf{Id}\ ((x : A) \to B)\ t\ u}$$

$$\lambda x : A.\ p\ x\ 0 \quad = \quad \lambda x : A.\ t\ x \quad = \quad t$$

$$\lambda x : A.\ p\ x\ 1 \quad = \quad \lambda x : A.\ u\ x \quad = \quad u$$

Function extensionality

```
funExt (A : U) (B : A -> U) (f g : (x : A) -> B x)
       (p : (x : A) -> Id (B x) (f x) (g x)) :
       Id ((y : A) -> B y) f g = <i> \(a : A) -> (p a) @ i
```

Example

```
mapOnPath (A B : U) (f : A -> B) (a b : A)
          (p : Id A a b) : Id B (f a) (f b) = <i> f (p @ i)
```

Example

```
add (a : nat) : nat -> nat = split
  zero  -> a
  suc n -> suc (add a n)

addZero : (n : nat) -> Id nat (add zero n) n = split
  zero  -> <i> zero
  suc n -> <i> suc (addZero n @ i)
```

Singleton are contractible

We also can justify the fact that any element in $(x : A, \mathsf{Id}\ A\ a\ x)$ is equal to $(a, 1_a)$

$$\frac{\Gamma \vdash a : A \qquad \Gamma \vdash b : A \qquad\qquad \Gamma \vdash p : \mathsf{Id}\ A\ a\ b}{\Gamma \vdash \langle i \rangle (p\ i, \langle j \rangle p\ (i \wedge j)) : \mathsf{Id}\ (x : A, \mathsf{Id}\ A\ a\ x)\ (a, 1_a)\ (b, p)}$$

Base category

Direct description of $\mathcal{C}^{op}$

Objects: finite sets $I, J, \ldots$

Maps: $I \to \mathsf{dM}(J)$ where $\mathsf{dM}(J)$ is the free de Morgan algebra on J

de Morgan algebra: bounded distributive lattice with a reverse operation

Example: $[0,1]$ with $\mathsf{max}(i,j),\ \mathsf{min}(i,j),\ 1-i$

$I+J$ is the product of I and J in $\mathcal{C}$

Nominal sets

$\mathbb{I}(I) = dM(I)$

We have a de Morgan algebra structure on $\mathbb{I}$

Subobject classifier

$\Omega(I)$ set of sieves on I

where a sieve L on I is a set of maps of codomain I such that

$fg : K \to I$ in L if $f : J \to I$ in L and $g : K \to J$

Ω is the suboject classifier

Example: if $I = i, j$ then we can consider the *boundary* of I which is the sieve generated by all faces $i = 0, i = 1, j = 0, j = 1$ of I

A sieve on I can be seen as a subpresheaf of the presheaf represented by I

Shapes

We define $\mathbb{S}$ subpresheaf of Ω

$\mathbb{S}$ is the sublattice of Ω generated by $i = 1$ for i in $\mathbb{I}$

$i = 0$ is defined as $1 - i = 1$

A *shape* is an element of $\mathbb{S}$, thus defined as a special kind of truth-value

Shapes

For this base category, we have

$[i = 0] \wedge [i = 1] = \perp$

$[\mathsf{max}(i, j) = 1] = [i = 1] \vee [j = 1] \qquad [\mathsf{min}(i, j) = 1] = [i = 1] \wedge [j = 1]$

This defines a de Morgan algebra map

$$\mathbb{I} \to \Omega \times \Omega$$

$$i \longmapsto ([i = 0], [i = 1])$$

Internal logic

Any element L of $\mathbb{S}$ can be seen as a subobject of the terminal object

In particular for any presheaf X we can consider X^L

If $\vec{u}$ in X^L we can consider the presheaf $X|\vec{u}$

a is in $X|\vec{u}$ if $(\lambda\alpha : L)a$ and $\vec{u}$ coincides on L

External interpretation

$(L : \mathbb{S}, X^L)$

An element of $(L : \mathbb{S}, X^L)(I)$ is a sieve L on I together with a family of element $u_f \in X(J)$ for $f : J \to I$ in L such that $(u_f)g = u_{fg} \in X(K)$ if $g : K \to J$

$L : \mathbb{S}, u : X^L \vdash X|u$

If we have L sieve on I and such a family $\vec{u} = (u_f)$ then $(X|u)(L = L, u = \vec{u})$ is the set of elements a in $X(I)$ such that $af = u_f$ for $f : J \to I$ in L

This gives a(n internal) notion of connectedness: such an element a is a witness of the fact that the elements defined by the system $\vec{u}$ are *connected*

External interpretation

For instance if $I = \{i\}$ an element of

$(L : \mathbb{S}, X^L)(I)$

is given by a sieve L in $\mathbb{S}(\{i\})$ and a family of elements $u_f \in X(J)$ for $f : J \rightarrow I$ in L

If we take $L = [i = 0] \vee [i = 1]$ such a family is completely characterized by a system

$(i = 0) \mapsto u_0,\ (i = 1) \mapsto u_1$

with u_0 in $X()$ and u_1 in $X()$ are points of X

An element in $(X|\vec{u})(I)$ is a line connecting u_0 and u_1

System of elements

$X \longmapsto (L : \mathbb{S}, X^L)$

is a polynomial functor on the category of cubical sets

Equality

If we have $\Gamma \vdash a : A$ and $\Gamma \vdash b : A$ and $\Gamma \vdash L : \mathbb{S}$

Then $\Gamma, \alpha : L \vdash a = b : A$ means

$$a\rho = b\rho \in A\rho$$

whenever $\rho \in \Gamma(I)$ such that $1_I \in L\rho$

$\Gamma \vdash a = b : A$ means

$$a\rho = b\rho \in A\rho$$

for all $\rho \in \Gamma(I)$

Internal logic

We can now express *internally* when a presheaf (=cubical set) X is “fibrant” by the fact that we have one constant

$\mathsf{comp} : (L : \mathbb{S})\ (\vec{u} : (X^L)^{\mathbb{I}}) \to X|\vec{u}0 \to X|\vec{u}1$

$\vec{u} : (X^L)^{\mathbb{I}}$ is a path of system of elements in X^L

If this system is connected at 0, it is connected at 1

A tuple in

$(L : \mathbb{S}, , \vec{u} : (X^L)^{\mathbb{I}}, X|\vec{u})(I)$

is an open box if L in $\mathbb{S}(I)$ is the boundary of I

Main Lemma (internally)

If X is fibrant we have

$\mathsf{fill} : (L : \mathbb{S})\ (\vec{u} : (X^L)^{\mathbb{I}}) \to X|\vec{u}0 \to (i : \mathbb{I}) \to X|\vec{u}i$

This refines the *Kan filling condition* (1955): any open box can be filled

$\vec{u} : (X^L)^{\mathbb{I}}$ is a path of element in X^L

If it is connected at 0, it is always connected

Main Lemma (internally)

$\mathsf{comp} : (L : \mathbb{S})\ (\vec{u} : (X^L)^{\mathbb{I}}) \to X|\vec{u}0 \to X|\vec{u}1$

$\mathsf{fill} : (L : \mathbb{S})\ (\vec{u} : (X^L)^{\mathbb{I}}) \to X|\vec{u}0 \to (i : \mathbb{I}) \to X|\vec{u}i$

We define

$\mathsf{fill}\ L\ \vec{u}\ a_0\ i = \mathsf{comp}\ (L \vee [i = 0])\ \vec{v}\ a_0$

where $\vec{v} : (X^{L \vee [i=0]})^{\mathbb{I}}$ is defined by

$-\vec{v}\ j\ \alpha = \vec{u}\ (i \wedge j)\ \alpha$ if α in L

$-\vec{v}\ j\ \alpha = a_0$ if α in $[i = 0]$

Fibration

$\Gamma \vdash A$

comp : $(\rho : \Gamma^{\mathbb{I}})\ (L : \mathbb{S})\ (\vec{u} : (i : \mathbb{I}) \to A(\rho i)^{L}) \to A(\rho 0)|\vec{u}0 \to A(\rho 1)|\vec{u}1$

fill : $(\rho : \Gamma^{\mathbb{I}})\ (L : \mathbb{S})\ (\vec{u} : (i : \mathbb{I}) \to A(\rho i)^{L}) \to A(\rho 0)|\vec{u}0 \to (i : \mathbb{I}) \to A(\rho i)|\vec{u}i$

We can derive fill from comp

Universe

We have shown externally how to define a universe which is fibrant and univalent

Is there an internal version of this proof?

Uses operations $\mathbb{S}^{\mathbb{I}} \rightarrow \mathbb{S}$ corresponding to natural transformations

$\mathbb{S}(I \times [1]) \rightarrow \mathbb{S}(I)$

Effective model

This model can be represented in Haskell essentially as it is

https://github.com/simhu/cubicaltt

Design choice: programming language with dependent types

Total fragment

In the total fragment conversion and type-checking are terminating

Effective model

We also have experimented with a simple form of higher inductive types

e.g. suspension, spheres, propositional truncation

the circle is equal to the suspension of the Boolean

Effective model

Most complex example so far: define multiplication on the circle

Show that it is an equivalence, using the fact that being an equivalence is a proposition

Deduce that any element in the circle has an inverse for multiplication

Compute the winding number of this inverse applied to some loops

Transport this structure on the suspension of the Boolean

Library of test examples?

Effective model

In particular we get an extension of type theory with function extensionality and with propositional truncation

We can introduce an existential quantification defined as the propositional truncation of the sum types

This existential quantification satisfies unique choice

Suitable formal system for constructive mathematics?

Some references

"A model of type theory in cubical sets"
M. Bezem, T.C. and S. Huber, proceeding of TYPES 2013

Names and Symmetry in Computer Science
A.M. Pitts

"An equivalent presentation of the Bezem-Coquand-Huber category of cubical sets"
A. M. Pitts. Preprint arXiv, December 2013.

Some references

The Univalent Foundation Program
Homotopy Type Theory: Univalent foundation of mathematics

V. Voevodsky Univalent foundation home page and
“Experimental library of univalent foundation of mathematics”