A Cubical Type Theory

Cork, August 26, 2015

Boolean algebra and domain theory

In this talk we shall not use Boolean algebras but distributive lattices and another less well-known structure

de Morgan algebra

distributive lattice with a “de Morgan” involution $1-i$

$$1-(1-\psi)=\psi \qquad\qquad 1-(\varphi\wedge\psi)=(1-\varphi)\vee(1-\psi)$$

But we don’t require $\psi\vee(1-\psi)=1$, nor $\psi\wedge(1-\psi)=0$

A compositional semantics using of the notion of *partial* element

George Boole

"The Laws of Thought"

Distinction between primary and secondary propositions

Every assertion that we make may be referred to one or the other of the two following kinds. Either it expresses a relation among things, or it expresses, or is equivalent to the expression of, a relation among propositions. [...] The former class of propositions, relating to things, I call "Primary" the latter class, relating to propositions, I call "Secondary"

(Boole, 1853, p. 37 of Project Gutenberg's digitization)

George Boole

If instead of the proposition, "The sun shines," we say, "It is true that the sun shines," we then speak not directly of things, but of a proposition concerning things [...] Every primary proposition may thus give rise to a secondary proposition, viz., to that secondary proposition which asserts its truth (loc.cit., p. 38)

The equivalence of these two forms is known as *propositional extensionality*

$$p \equiv (p = 1)$$

It is the simplest particular case of the axiom of univalence (Voevodsky)

Alonzo Church and the Axiom of extensionality

A formulation of the simple theory of types (1940)

Two forms of the axiom $10^{\alpha\beta}$, function extensionality, and 10^{o}

10^{o} states that two propositions are logical equivalent if, and only if, they are equal

10^{o} is not taken as an axiom in Church's original paper

We remark, however, on the possibility of introducing the additional axiom of extensionality, $p \equiv q \supset p = q$*, which has the effect of imposing so broad a criterion of identity between propositions that they are in consequence only two propositions, and which, in conjunction with* $10^{\alpha\beta}$*, makes possible the identification of classes with propositional functions*

Voevodsky's generalization

Formulated in the setting of dependent type theory

Grothendieck's notion of *universe* takes the place of the type of propositions

Define a notion of equivalence between types which generalizes uniformly the notion of logical equivalence between propositions, bijections between sets, categorical equivalence between groupoids, $\ldots$

Axiom of univalence (Voevodsky, 2009)

The canonical map $\mathsf{Id}(U, A, B) \to \mathsf{Equiv}(A, B)$ *is an equivalence*

Voevodsky's generalization

Introduces also a natural stratification of types

A is a *proposition* iff two elements of A are always equal

A is a *set* iff $\mathsf{Id}(A, a_0, a_1)$ is always a proposition

A is a *groupoid* iff $\mathsf{Id}(A, a_0, a_1)$ is always a set

One can show (using univalence) that the type of propositions form a set

Alonzo Church and the Axiom of description

A.k.a. axiom of "unique choice"

Addition of an operation $\iota x.P(x)$ with the Axiom 9^α

$$(\exists ! x : A.P(x)) \rightarrow P(\iota x.P(x))$$

Essential to connect the two notions of functions in this system

(1) function as explicit term or

(2) function as a functional graph

In type theory we shall get unique choice "up to isomorphism"

Alonzo Church

We are going to present a *computational justification* of these axioms

For extensionality it can be seen as a generalization of Gandy (1952) and Takeuti (1953)'s work

For the axiom of description we present a *new* kind of interpretation (so far the only known justification was going back to Russell's paper *On denoting* 1905)

Actually we are going to present a justification of the axiom of univalence and a generalization of the axiom of description (unique up to equality is replaced by unique up to isomorphisms, and even unique up to equivalence)

Cf. Gandy's PhD thesis (1952) on an "abstract theory of structures"

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

These spaces form a cartesian closed category
Moore (1955)

Kan simplicial sets form a model of type theory with the axiom of univalence
Voevodsky (2009)

Algebraic topology

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 some basic facts are *not* provable (j.w.w. M. Bezem and E. Parmann, TLCA 2015)

We have lost the computational aspect of dependent type theory!

Univalent Foundations

I will now present a possible 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

Constructive model

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

In this approach, *nominal* extension of λ-calculus

Similarity with works on semantical justification of higher-order abstract syntax

Constructive *presheaf* model

Objects: finite sets of symbols/names/directions/atoms $I, J, K, \dots$

Morphisms: a map $I \to J$ is a set-theoretic map $J \to \mathsf{dM}(I)$

$\mathsf{dM}(I)$ is the free de Morgan algebra on I

For usual higher-order abstract syntax we look at maps $J \to I$

Constructive *presheaf* model

A *cubical set* is a presheaf on this base category

We write $u \longmapsto uf,\ X(I) \to X(J)$ the transition map for $f : J \to I$

$X(I)$ can be identified to $I \to X$

If X is a cubical set, we think of $X(I)$ as the set of I-cubes of X

$X()$ set of points of X

$X(i)$ set of lines of X in the direction i

$X(i, j)$ set of squares of X in the directions i and j

The interval

We take $\mathbb{I}(I) = \mathsf{dM}(I)$

A cubical set which can be thought of as a formal representation of $[0,1]$

$\mathbb{I}$ has the structure of a de Morgan algebra

The object I itself can be seen as a formal representation of $[0,1]^I$

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

Paths

If X is a cubical set, simple description of $X^{\mathbb{I}}$

"path space" of X

An element of $X^{\mathbb{I}}(I)$ is an element of $X(I,j)$ with j not in I

And this, up to "α"-conversion

u in $X(I,j)$ is the same as v in $X(I,k)$ iff $v = u(j=k)$

$(j=k) : I,k \rightarrow I,j$

An element of $X^{\mathbb{I}}(I)$ is a "path" connecting two I-cubes of X

Partial objects

$\Omega(I)$ is the set of *sieves* on I

A sieve on I is a set of maps of codomain I closed by composition

Special sieves are defined by union of faces of I

A "direct" face $(k0)$ of $\{i, j, k\}$ is given by $\{i, j\} \rightarrow \{i, j, k\}$ sending k to 0

A face is obtained by composing these maps, e.g. $(i1)(k0)$

Partial objects

We write $\mathbb{F}(I)$ the sieves that are union of faces of I

This itself defines a cubical set $\mathbb{F}$, sublattice of Ω

A special element of $\mathbb{F}(I)$ is the boundary of I (union of all direct faces)

Partial objects

In general a partial object of X at level I is given by

(1) a sieve L on I

(2) a family u_f in $X(J)$ for $f : J \to I$ in L, such that $u_f g = u_{fg}$ if $g : K \to J$

We consider only partial elements where L is in $\mathbb{F}(I)$

L, seen as an element of $\Omega(I)$, is called the *extent* of the partial element

For $I = \{i\}$ two points a_0, a_1 in $X()$ define a partial element of X at level I

Partial objects

Any total element defines by restriction a partial element on a given extent

In general a partial element may not be the restriction of a total element

If it is we say that this partial element is *connected*

A special case: two points path-connected

We obtain in this way a “higher-order” notion of connectedness

“Fibrant” cubical sets

We can now adapt the notion of *Kan* cubical set (1955)

“Any open box can be filled” (in particular we can find the missing lid)

We say that X is *fibrant* iff it satisfies

Any partial path in X *connected at* 0 *is connected at* 1

(If the extent of this partial path is a boundary, we retrieve Kan’s condition)

"Fibrant" cubical sets

Given $\psi : \mathbb{F},\ \psi \vdash u : A^{\mathbb{I}},\ a_0 : A$ such that $\psi \vdash a_0 = u\ 0$

$$\mathsf{comp}(\psi, u, a_0) : A \qquad\qquad \psi \vdash \mathsf{comp}(\psi, u, a_0) = u\ 1$$

We can then define $\mathsf{fill}(\psi, u, a_0) : A^{\mathbb{I}}$

$$\mathsf{fill}(\psi, u, a_0) = \langle i \rangle \mathsf{comp}(\psi \vee (i = 0), v, a_0)$$

-$v = \langle j \rangle u\ (i \wedge j)$ on ψ

-$v = \langle j \rangle a_0$ on $(i = 0)$

We have $\mathsf{fill}(\psi, u, a_0)\ 0 = a_0$ and $\mathsf{fill}(\psi, u, a_0)\ 1 = \mathsf{comp}(\psi, u, a_0)$

George Boole

As 1 *denotes the whole duration of time, and* x *that portion of it for which the proposition* X *is true,* $1 - x$ *will denote that portion of time for which the proposition* X *is false.*

Again, as xy *denotes that portion of time for which the propositions* X *and* Y *are both true, we shall, by combining this and the previous observation, be led to the following interpretations, viz.: The expression* $x(1 - y)$ *will represent the time during which the proposition* X *is true, and the proposition* Y *false. The expression* $(1 - x)(1 - y)$ *will represent the time during which the propositions* X *and* Y *are simultaneously false.*

(loc.cit. page 138)

George Boole

Boole was the considering the "extent" for which a proposition X is true

The situation is similar here, using the notion of propositions as types

We consider a proof/element of a proposition/type which has an extent

The extents form only a distributive lattice

“Fibrant” cubical sets

The fibrant cubical sets form a model of dependent type theory

Uses the fact that we recover filling from composition

Furthermore there is a type of paths $\mathsf{Path}(A, a_0, a_1)$

This interprets all the rules of Martin-Löf identity types

However the computation rule is only validated as a path equality

(More about this later)

Universe

Universe of fibrant cubical sets

Is it itself fibrant?

Does it satisfy the axiom of univalence?

Isomorphisms

An isomorphism bewteen A and B is given by

(1) two maps $f : A \to B$ and $g : B \to A$

(2) two applications

$$u : (x : A) \to \mathsf{Path}(A, g(f(x)), x)$$

$$v : (y : B) \to \mathsf{Path}(B, f(g(y)), y)$$

Corresponds in topology to the notion of homotopy equivalence of two spaces

Partial types

Semantically a partial type at level I is given by a sieve L and a family of sets A_f for f in L with transition maps $A_f \to A_{fg}$

A partial type is "connected" if it is the restriction of a total type

Main result and applications

Main result: *To be connected is preserved by isomorphisms*

Special case: if

(1) A and B are path-connected

(2) A isomorphic to C

(3) B isomorphic to D

then C and D are path-connected

Main result and applications

A direct application is that we can transform an isomorphism between two types into a path between these types.

Indeed, A is connected to A, and A isomorphic to A so if A is isomorphic to B, we get that A is connected to B

Several applications of univalence only use this fact

However this is not enough to show e.g. that the type of propositions form a set, or that the type of sets form a groupoid

Main result and applications

A more subtle application

(Simon Huber and Anders Mörtberg) *The axiom of univalence holds in the sense that the canonical map* Path$(U, A, B) \rightarrow$ Equiv(A, B) *defines an isomorphism*

Another direct application is

The type U is "fibrant" (it has a composition operation)

This is because any path between two types define an isomorphism

Main result and applications

So we get a constructive interpretation of Martin-Löf type theory extended with Voevodsky's axiom of univalence

except that the computation rule for $\mathsf{Path}(A, a, b)$ is only interpreted as a path equality

Recently, A. Swan (Leeds) found a way to recover an identity type $\mathsf{Id}(A, a, b)$ which interprets Martin-Löf's computation rule

Cofibration-trivial fibration Factorization

The main idea is to introduce for any map $f : A \to B$ the following dependent type on B

$T_f(b)$ contains partial element a in A having for image the restriction of b on the extent of a

This type is contractible

The projection $(b : B, T_f(b)) \to B$ defines a trivial fibration on B

The canonical map $a \longmapsto f\ a,\ A \to (b : B, T_f(b))$ has the lifting property w.r.t. any trivial fibration

And f is the composition of this map with the projection $(b : B, T_f(b)) \to B$

A cubical type theory

Both the derivation of univalence and A. Swan's derivation are examples of programming in this "nominal" extension of λ-calculus

A cubical type theory

The model being constructive can be expressed as a type system

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

For instance $x : A$ represents the context of points in A

$i : \mathbb{I}, j : \mathbb{I}$ represented the context a square

$i : \mathbb{I}, j : \mathbb{I}, (i = 0) \vee (i = 1) \vee (j = 0) \vee (j = 1)$ represents the boundary of a square

A cubical type theory

$$t, A \ ::= \ x \mid t\ t \mid \lambda x.t \mid t\ \varphi \mid \langle i \rangle t \mid \psi_1 t_1 \vee \cdots \vee \psi_k t_k$$

$$\varphi, \psi \ ::= \ 0 \mid 1 \mid (i = 0) \mid (i = 1) \mid \varphi \vee \psi \mid \varphi \wedge \psi$$

A cubical type theory

This cubical type theory has been implemented in Haskell

https://github.com/simhu/cubicaltt

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

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

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

It satisfies a strong form of unique choice/axiom of description

Suitable formal system for constructive mathematics?

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 consider 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"