# Applications of Type Theory to Univalent Mathematics

Thierry Coquand

Autumn School, Proof and Computations, September 2019

## Myth: propositional truncation erases information

It doesn't. E.g.:

Theorem of MLTT+$\|-\|$. For any $f : \mathbb{N} \to \mathbb{N}$,

$$\|\Sigma(n : \mathbb{N}), f(n) = 0\| \to \Sigma(n : \mathbb{N}), f(n) = 0.$$

If there is a root of $f$, we can find one.

# Logical strength?

Univalence and propositional truncation does not add logical strength

With a countable hiearchy of universes, equivalent to CZFU$_{<\omega}$

If we add excluded middle, we get a stronger system

# No global choice functions

We cannot have an operation

$$\epsilon : \Pi(A : U)\ \|A\| \to A$$

since such operation would have to be equivariant, and we should have

$$\epsilon\ A\ p\ =_A\ f\ (\epsilon\ A\ p)$$

for any $f : A \cong A$, simply because $\epsilon$ has to preserve equality.

This is not possible e.g. for $A \equiv \mathsf{Bool}$

# Identification of mathematical structures

For all mathematical purposes

(1) two groups are regarded to be the same if they are isomorphic

e.g. one says that the additive integers for "the" free group on one generator

(2) two metric spaces are regarded to be the same if they are isometric

(3) two topological spaces are regarded to be the same if they are homeomorphic

(4) two categories are regarded to be the same if they are equivalent

# Identification of mathematical structures

Do we *choose* the above identifications motivated by particular applications?

Or are these notions of "sameness" imposed upon us, independently of what we want to do with the structures

# Identification of mathematical structures

It may seem that the notion of identification depends on the particular applications

If we consider the lattice of subgroups of a given group (e.g. for proving Jordan-Hölder theorem) then it seems important to consider subgroups as set of elements and not up to isomorphism

On the other hand, in other situations, when reasoning about groups it is considered to be good mathematical practice that all statements should be invariant by isomorphisms

*We seem to be choosing the notion of identifications according to applications*

# Answer in univalent mathematics

We define the collection of structures as a type (for a given universe)

We take as notion of equality the given identity type

then

we can *prove* that equality of groups *is* isomorphism,

that equality of topological spaces *is* homemorphism,

that equality of metric spaces *is* isometry,

that equality of categories *is* equivalence, etc...

# Collection of types

*We seem to be* choosing *the notion of identifications according to applications*

In univalent mathematics we have that

-in the *type of groups*, equality is isomorphism

-in the *type of subgroups* of a given group, equality is "to have the same element" in the ambiant group

This is possible because there is a notion of identification for each given type, but there is no "global" notion of identification

# Collection of types

On the type $U$ we have

$$(X =_U Y) \;=\; (X \cong Y)$$

# Collection of type with operations

What should be the equality on

$T_2 = \Sigma(X : U)\ X \to X \to X$?

We can show (using univalence) that $(X_0, m_0) =_{T_2} (X_1, m_1)$ is equal to

$\Sigma(f : X_0 \to X_1)\ (\mathsf{isEquiv}\ f) \times \Pi(x\ y : X_0)\ m_1\ (f\ x)\ (f\ y) = f\ (m_0\ x\ y)$

# What should be a semi-group?

$\Sigma(X : U)\Sigma(m : X \times X \to X)\ A(X, m)$

where $A(X, m)$ is $\Pi(x_0\ x_1\ x_2 : X)\ m\ x_0\ (m\ x_1\ x_2) =_X m\ (m\ x_0\ x_1)\ x_2$

This is *not* the right type

We should express that $X$ is a *set*

# What should be a semi-group?

How to define isSet $X$?

We should express that the equality types on $X$ are subsingleton

isSet $X = \Pi(x_0\ x_1 : X)$ isProp $(x_0 =_X x_1)$

and the definition of the collection of semigroups $M$ becomes

$\Sigma(X : U)\Sigma(m : X \to X \to X)$ isSet $X\ \times A(X, m)$

An element of type $M$ is a tuple $X, m, i, p$ where $X$ is a (small) type, $m$ a binary operation, $i$ the condition that $X$ is a set and $p$ expresses associativity

# Equality of semigroups

With this definition the type $(X_0, m_0, i_0, p_0) = (X_1, m_1, i_1, p_1)$ is *equal* to the type

$$\Sigma(f : X_0 \to X_1)\ (\mathsf{isEquiv}\ f)\ \times \Pi(x\ y : X_0)\ m_1\ (f\ x)\ (f\ y) = f\ (m_0\ x\ y)$$

Intuitively the conditions that $X$ is a set and that the operation is associative (on a *set*) don't matter since they are proof irrelevant

# Collection of all semigroups

This type $M$ is *not* a set!

It is a *groupoid*, where "to be a groupoid" mean

$\Pi(m_0\ m_1 : M)$ isSet $(m_0 = m_1)$

The type of sets (relative to a given universe)

$\Sigma(X : U)$ isSet $X$

similarly is a *groupoid*

# Discussion

This is quite different from the situation in set theory

In set theory, the collection of small sets is itself a set

In univalent mathematics, the collection of small sets is an object which is "qualitatively" different from sets p Its corresponding notion of equality is more complex

# Discussion

Mathematically this appears in sheaf models

The collection of all sheaves, all groups in a sheaf model is *not* a sheaf

If we have $F_{U_i}$ compatible family of sheaves and we want to patch them together then the patching is possible but not unique

It is only unique up to isomorphisms

This is connected to the introduction of the notion of *stacks*

# Discussion

In this setting the notion of groupoid is a property of a type

Quite different from the traditional view, which defines a groupoid as a special king of *category* where all morphisms are isomorphisms

# Equality for subsemigroups of a given semigroup

What about equality on the collection of *subgroups* of a given group?

A subgroup of a group $A$ is a group $B$ with an embedding $B \to A$

Then the equality will be that the two subgroups have the same element!

# Discussion

(1) The definition of the type of monoids $M$ does not say what a *morphism* should be

Somehow "magically" univalence "knows", without us telling it, what a monoid *isomorphism* should be

(2) We are defining the type of monoids, and then univalence automatically tells us what are their isomorphisms

# Discussion

(3) We are not getting a notion of *morphism* between monoids

In general, for a given collection of structures there might be different notions of morphisms: e.g. topological spaces with continuous functions or with open maps

Univalence automatically determines the *isomorphisms* but not the morphisms

# What happens if we don't have univalence?

We don't have function extensionality

We cannot say very much about the equality of monoids

# Equality for subsemigroups of a given semigroup

Given a semigroup $M$

A subsemigroup is a pair $A, f$ where $f$ is an embedding $A \to N$

Then $(A, f) = (B, g)$ is a subsingleton

Embedding:

-all maps $a_0 =_A a_1 \to f\ a_0 =_B f\ a_1$ are equivalence

-equivalently, all fibers $\Sigma(a : A)\ b =_B (f\ a)$ are subsingleton

# Poswerset of a type

If we define $\Omega_U = \Sigma(X : U)\mathsf{isProp}\ X$ then the powerset of $A : U$ is $A \to \Omega$

$\Omega_U$ is a *set*

Given $P : A \to \Omega_U$ we can form the associated subset of $A$

$\Sigma(x : A)\ \pi_1\ (P\ x)$

If we also have $Q : A \to \Omega_U$ then

$(P = Q)\ =\ \Pi(x : A)\ \pi_1\ (P\ x) = \pi_1\ (Q\ x)$

# Equality of topological spaces

We define topological spaces as in traditional mathematics with a given collection of subsets of a given set

Then we can show that the identifications of spaces are the same as homeomorphisms

# Equality of categories

Similarly one can define the notion of category

A category is best seen as the "groupoid" notion corresponding to the "set" notion of posets

The type of identification of categories will be equal to the type of equivalences between the categories

# Equality of categories

The "data" part of a category is given by the type

$$\Sigma(X : U)(R : X \to X \to U)\ C(X, R)$$

where $C(X, R)$ is the product of

$$\Pi(x : X)\ R\ x\ x$$

$$\Pi(x\ y\ z : X)\ R\ x\ y \to R\ y\ z \to R\ x\ z$$

The rest of the specification of a category is purely propositional

In particular, we write that $X$ is a groupoid and each $R\ x\ y$ is a set

# Another example of a large type which is a set

Take the collection of all finite linear orders

There is at most one proof of equality between two elements

Hence we get a set (wich is large)

So the "size" of a type may not be connected to the complexity of equality of the type