A univalent approach to constructive mathematics

Chuangjie Xu

Ludwig-Maximilians-Universität München

Second Workshop on Mathematical Logic and its Applications

5-7,**8**,9 March 2018, Kanazawa, Japan

This talk is

1. to give a very brief introduction to univalent type theory (UTT),
2. to demonstrate some experiments of doing mathematics in UTT, and
3. to collect your valuable advices of interesting concrete mathematics that could be suitable to carry out within such foundation.

Constructive mathematics and Martin-Löf type theory

A central tenet of constructive mathematics is that the logical symbols carry computational content.

Constructive mathematics and Martin-Löf type theory

A central tenet of constructive mathematics is that the logical symbols carry computational content.

Curry–Howard logic in Martin-Löf type theory (MLTT)

Propositions	Types
$P \wedge Q$	$P \times Q$
$P \vee Q$	$P + Q$
$P \to Q$	$P \to Q$
$\forall (x : A). P(x)$	$\Pi (x : A). P(x)$
$\exists (x : A). P(x)$	$\Sigma (x : A). P(x)$

Constructive mathematics and Martin-Löf type theory

A central tenet of constructive mathematics is that the logical symbols carry computational content.

Curry–Howard logic in Martin-Löf type theory (MLTT)

Propositions	Types
$P \wedge Q$	$P \times Q$
$P \vee Q$	$P + Q$
$P \to Q$	$P \to Q$
$\forall (x : A). P(x)$	$\Pi (x : A). P(x)$
$\exists (x : A). P(x)$	$\Sigma (x : A). P(x)$

Computer proof assistants based on (variants of) MLTT include Agda, Coq, Lean, Nuprl, ...

Martin-Löf type theory for constructive mathematics?

Nonaxiom of choice

$$\Pi(x:A).\Sigma(y:B).P(x,y) \to \Sigma(f:A\to B).\Pi(x:A).P(x,f(x))$$

Martin-Löf type theory for constructive mathematics?

Nonaxiom of choice

$$\Pi(x:A).\Sigma(y:B).P(x,y) \to \Sigma(f:A\to B).\Pi(x:A).P(x,f(x))$$

Trouble of defining the image of a function $f : A \to B$

$$(\Sigma(y:B).\Sigma(x:A).f(x)=y) \;\simeq\; A$$

Martin-Löf type theory for constructive mathematics?

Nonaxiom of choice

$$\Pi(x : A).\Sigma(y : B).P(x, y) \to \Sigma(f : A \to B).\Pi(x : A).P(x, f(x))$$

Trouble of defining the image of a function $f : A \to B$

$$(\Sigma(y : B).\Sigma(x : A).f(x) = y) \;\simeq\; A$$

Failure of Brouwer's continuity principle (Escardó and X, 2015)

$$\Big(\Pi(f : \mathbb{N}^{\mathbb{N}} \to \mathbb{N}).\Pi(\alpha : \mathbb{N}^{\mathbb{N}}).\Sigma(n : \mathbb{N}).\Pi(\beta : \mathbb{N}^{\mathbb{N}}).\,(\alpha =_n \beta \to f(\alpha) = f(\beta))\Big) \to 0 = 1$$

Martin-Löf type theory for constructive mathematics?

Nonaxiom of choice

$$\Pi(x:A).\Sigma(y:B).P(x,y) \to \Sigma(f:A\to B).\Pi(x:A).P(x,f(x))$$

Trouble of defining the image of a function $f : A \to B$

$$(\Sigma(y:B).\Sigma(x:A).f(x)=y) \;\simeq\; A$$

Failure of Brouwer's continuity principle (Escardó and X, 2015)

$$\Big(\Pi(f:\mathbb{N}^{\mathbb{N}}\to\mathbb{N}).\Pi(\alpha:\mathbb{N}^{\mathbb{N}}).\Sigma(n:\mathbb{N}).\Pi(\beta:\mathbb{N}^{\mathbb{N}}).\,(\alpha =_n \beta \to f(\alpha)=f(\beta))\Big) \to 0=1$$

Is this theory of construction too computationally informative?

Voevodsky's Univalent Foundations

A univalent type theory is a mathematical language for expressing definitions, theorems and proofs that is invariant under equivalences, i.e.

$$P(X) \times (X \simeq Y) \to P(Y)$$

Examples: UniMath, HoTT book, cubical type theory.

Voevodsky's Univalent Foundations

A univalent type theory is a mathematical language for expressing definitions, theorems and proofs that is invariant under equivalences, i.e.

$$P(X) \times (X \simeq Y) \to P(Y)$$

Examples: UniMath, HoTT book, cubical type theory.

Among the significant univalent concepts and techniques, here I present two:

Stratification of types

- A type P is a proposition if
$$\mathsf{isProp}(P) \;:\equiv\; \Pi(x, y : P).x = y$$
- A type A is a set if
$$\mathsf{isSet}(A) \;:\equiv\; \Pi(x, y : A).\mathsf{isProp}(x = y)$$
- groupoids and, more generally, n-types

provides a flexible way to intuitively describe mathematical objects.

Propositional truncation

A propositional truncation of a type X, if it exists, is a proposition $\|X\|$ together with a map $|-| : X \to \|X\|$ such that for any proposition P and $f : X \to P$ we can find $\bar{f} : \|X\| \to P$ with

$$\begin{tikzcd} X \arrow[r, "|-|"] \arrow[dr, "f"'] & \|X\| \arrow[d, dashed, "\bar{f}"] \\ & P \end{tikzcd}$$

Propositional truncation

A propositional truncation of a type X, if it exists, is a proposition $\|X\|$ together with a map $|-| : X \to \|X\|$ such that for any proposition P and $f : X \to P$ we can find $\bar{f} : \|X\| \to P$ with

$$\begin{tikzcd} X \arrow[r, "|-|"] \arrow[dr, "f"'] & \|X\| \arrow[d, dashed, "\bar{f}"] \\ & P \end{tikzcd}$$

- Intuitively, $\|X\|$ is the (type of) truth value of the inhabitedness of X.
- Several kinds of types can be shown to have truncations in MLTT.
- There are different ways to extend MLTT to get truncations for all types.
- $\|X\| \to X$ is not provable in general, and is equivalent to $X + \neg X$.

Univalent logic

Let P, Q be propositions.

$$
\begin{aligned}
\bot &:\equiv \mathbb{0} \\
\top &:\equiv \mathbb{1} \\
P \wedge Q &:\equiv P \times Q \\
P \vee Q &:\equiv \|P + Q\| \\
P \to Q &:\equiv P \to Q \\
\forall(x:A).P(x) &:\equiv \Pi(x:A).P(x) \\
\exists(x:A).P(x) &:\equiv \|\Sigma(x:A).P(x)\|
\end{aligned}
$$

Univalent logic

Let P, Q be propositions.

$$
\begin{aligned}
\bot &:\equiv \mathbb{0} \\
\top &:\equiv \mathbb{1} \\
P \wedge Q &:\equiv P \times Q \\
P \vee Q &:\equiv \|P + Q\| \\
P \to Q &:\equiv P \to Q \\
\forall (x : A). P(x) &:\equiv \Pi (x : A). P(x) \\
\exists (x : A). P(x) &:\equiv \|\Sigma (x : A). P(x)\|
\end{aligned}
$$

Axiom of choice

$$\Pi(x : A). \|\Sigma(y : B). P(x, y)\| \to \|\Sigma(f : A \to B). \Pi(x : A). P(x, f(x))\|$$

Image of $f : A \to B$

$$\mathsf{image}(f) :\equiv \Sigma(y : B). \|\Sigma(x : A). f(x) = y\|$$

Continuity principle

$$\Pi(f : \mathbb{N}^{\mathbb{N}} \to \mathbb{N}). \Pi(\alpha : \mathbb{N}^{\mathbb{N}}). \|\Sigma(n : \mathbb{N}). \Pi(\beta : \mathbb{N}^{\mathbb{N}}). (\alpha =_n \beta \to f(\alpha) = f(\beta))\|$$

From now on, I use logical connectives for properties and type formers for structures.

Example I: Intermediate Value Theorem

Continuity as a structure or a property?

Example I: Intermediate Value Theorem

Continuity as a structure or a property?

Theorem (Bishop,1967)
Let $f : [a, b] \to \mathbb{R}$ be uniformly continuous such that $f(a) \leq 0 \leq f(b)$. For any $\varepsilon > 0$ we can find $c \in [a, b]$ such that $|f(c)| < \varepsilon$.

Theorem (Taylor, 2010)
Let $f : [a, b] \to \mathbb{R}$ be uniformly continuous such that $f(a) \leq 0 \leq f(b)$. If f is locally nonzero (for any $x < y$ there exists $z \in (x, y)$ such that $f(z) \neq 0$), then we can find $c \in [a, b]$ such that $f(c) = 0$.

Example I: Intermediate Value Theorem

Continuity as a structure or a property?

Theorem (Bishop,1967)
Let $f : [a, b] \to \mathbb{R}$ be uniformly continuous such that $f(a) \leq 0 \leq f(b)$. For any $\varepsilon > 0$ we can find $c \in [a, b]$ such that $|f(c)| < \varepsilon$.

In its proof, uniform continuity is used as a structure on f to construct the approximate root c for each ε.

Theorem (Taylor, 2010)
Let $f : [a, b] \to \mathbb{R}$ be uniformly continuous such that $f(a) \leq 0 \leq f(b)$. If f is locally nonzero (for any $x < y$ there exists $z \in (x, y)$ such that $f(z) \neq 0$), then we can find $c \in [a, b]$ such that $f(c) = 0$.

Example I: Intermediate Value Theorem

Continuity as a structure or a property?

Theorem (Bishop,1967)
Let $f : [a, b] \to \mathbb{R}$ be uniformly continuous such that $f(a) \leq 0 \leq f(b)$. For any $\varepsilon > 0$ we can find $c \in [a, b]$ such that $|f(c)| < \varepsilon$.

In its proof, uniform continuity is used as a structure on f to construct the approximate root c for each ε.

Theorem (Taylor, 2010)
Let $f : [a, b] \to \mathbb{R}$ be uniformly continuous such that $f(a) \leq 0 \leq f(b)$. If f is locally nonzero (for any $x < y$ there exists $z \in (x, y)$ such that $f(z) \neq 0$), then we can find $c \in [a, b]$ such that $f(c) = 0$.

Here the root c is constructed using the local-nonzero structure on f, and uniform continuity is used only as a property of f to prove $f(c) = 0$.

Example I: Intermediate Value Theorem

Continuity as a structure or a property?

Theorem (Bishop,1967)
Let $f : [a, b] \to \mathbb{R}$ be uniformly continuous such that $f(a) \leq 0 \leq f(b)$. For any $\varepsilon > 0$ we can find $c \in [a, b]$ such that $|f(c)| < \varepsilon$.

In its proof, uniform continuity is used as a structure on f to construct the approximate root c for each ε.

Theorem (Taylor, 2010)
Let $f : [a, b] \to \mathbb{R}$ be uniformly continuous such that $f(a) \leq 0 \leq f(b)$. If f is locally nonzero (for any $x < y$ there exists $z \in (x, y)$ such that $f(z) \neq 0$), then we can find $c \in [a, b]$ such that $f(c) = 0$.

Here the root c is constructed using the local-nonzero structure on f, and uniform continuity is used only as a property of f to prove $f(c) = 0$.

So far it seems to be an art to decide if a particular mathematical statement should be formulated as giving structure or as a proposition.

Example II: Fan Theorem

To distinguish principles of structures from those of properties (univalent reverse math?)

Example II: Fan Theorem

To distinguish principles of structures from those of properties (univalent reverse math?)

Given $B : 2^* \to \mathsf{Prop}$ where Prop is the universe of propositions, define

- $\mathsf{decidable}(B) :\equiv \Pi(u : 2^*).B(u) + \neg B(u)$
- $\mathsf{bar}(B) :\equiv \forall(\alpha : 2^{\mathbb{N}}).\exists(n : \mathbb{N}).B(\bar{\alpha}(n))$
- $\mathsf{bar}_\Sigma(B) :\equiv \Pi(\alpha : 2^{\mathbb{N}}).\Sigma(n : \mathbb{N}).B(\bar{\alpha}(n))$
- $\mathsf{uBar}(B) :\equiv \cdots$, $\mathsf{uBar}_\Sigma(B) :\equiv \cdots$
- $\mathsf{FAN} :\equiv \forall(B : 2^* \to \mathsf{Prop}).\,(\mathsf{decidable}(B) \to \mathsf{bar}(B) \to \mathsf{uBar}(B))$
- $\mathsf{FAN}_\Sigma :\equiv \Pi(B : 2^* \to \mathsf{Prop}).\,(\mathsf{decidable}(B) \to \mathsf{bar}_\Sigma(B) \to \mathsf{uBar}_\Sigma(B))$
- $\mathsf{Cont} :\equiv \cdots$, $\mathsf{Cont}_\Sigma :\equiv \cdots$, $\mathsf{UC} :\equiv \cdots$, $\mathsf{UC}_\Sigma :\equiv \cdots$, $\mathsf{MUC} :\equiv \cdots$, $\mathsf{MUC}_\Sigma :\equiv \cdots$

Example II: Fan Theorem

To distinguish principles of structures from those of properties (univalent reverse math?)

Given $B : 2^* \to \mathsf{Prop}$ where Prop is the universe of propositions, define

- $\mathsf{decidable}(B) :\equiv \Pi(u : 2^*).B(u) + \neg B(u)$
- $\mathsf{bar}(B) :\equiv \forall(\alpha : 2^{\mathbb{N}}).\exists(n : \mathbb{N}).B(\bar{\alpha}(n))$
- $\mathsf{bar}_\Sigma(B) :\equiv \Pi(\alpha : 2^{\mathbb{N}}).\Sigma(n : \mathbb{N}).B(\bar{\alpha}(n))$
- $\mathsf{uBar}(B) :\equiv \cdots$, $\mathsf{uBar}_\Sigma(B) :\equiv \cdots$
- $\mathsf{FAN} :\equiv \forall(B : 2^* \to \mathsf{Prop}).\,(\mathsf{decidable}(B) \to \mathsf{bar}(B) \to \mathsf{uBar}(B))$
- $\mathsf{FAN}_\Sigma :\equiv \Pi(B : 2^* \to \mathsf{Prop}).\,(\mathsf{decidable}(B) \to \mathsf{bar}_\Sigma(B) \to \mathsf{uBar}_\Sigma(B))$
- $\mathsf{Cont} :\equiv \cdots$, $\mathsf{Cont}_\Sigma :\equiv \cdots$, $\mathsf{UC} :\equiv \cdots$, $\mathsf{UC}_\Sigma :\equiv \cdots$, $\mathsf{MUC} :\equiv \cdots$, $\mathsf{MUC}_\Sigma :\equiv \cdots$

Theorem (in e.g. BISH).

$$\begin{array}{c} \mathsf{FAN} \\ \updownarrow \\ \mathsf{MUC} \end{array} \wedge \quad \mathsf{Cont} \to \quad \mathsf{UC}$$

Example II: Fan Theorem

To distinguish principles of structures from those of properties (univalent reverse math?)

Given $B : 2^* \to \mathsf{Prop}$ where Prop is the universe of propositions, define

- $\mathsf{decidable}(B) :\equiv \Pi(u : 2^*).B(u) + \neg B(u)$
- $\mathsf{bar}(B) :\equiv \forall(\alpha : 2^{\mathbb{N}}).\exists(n : \mathbb{N}).B(\bar{\alpha}(n))$
- $\mathsf{bar}_\Sigma(B) :\equiv \Pi(\alpha : 2^{\mathbb{N}}).\Sigma(n : \mathbb{N}).B(\bar{\alpha}(n))$
- $\mathsf{uBar}(B) :\equiv \cdots$, $\mathsf{uBar}_\Sigma(B) :\equiv \cdots$
- $\mathsf{FAN} :\equiv \forall(B : 2^* \to \mathsf{Prop}).\,(\mathsf{decidable}(B) \to \mathsf{bar}(B) \to \mathsf{uBar}(B))$
- $\mathsf{FAN}_\Sigma :\equiv \Pi(B : 2^* \to \mathsf{Prop}).\,(\mathsf{decidable}(B) \to \mathsf{bar}_\Sigma(B) \to \mathsf{uBar}_\Sigma(B))$
- $\mathsf{Cont} :\equiv \cdots$, $\mathsf{Cont}_\Sigma :\equiv \cdots$, $\mathsf{UC} :\equiv \cdots$, $\mathsf{UC}_\Sigma :\equiv \cdots$, $\mathsf{MUC} :\equiv \cdots$, $\mathsf{MUC}_\Sigma :\equiv \cdots$

Theorem (in MLTT $+ \| - \|$).

$$\begin{array}{ccccccc} \mathsf{FAN}_\Sigma & \leftrightarrow & \mathsf{FAN} & \wedge & \mathsf{Cont} & \to & \mathsf{UC} \\ \updownarrow & & \updownarrow & & \uparrow & & \updownarrow \\ \mathsf{MUC}_\Sigma & \leftrightarrow & \mathsf{MUC} & & \mathsf{Cont}_\Sigma & & \mathsf{UC}_\Sigma \end{array}$$

Summary and ...

Univalent type theory seems a good approach to constructive mathematics, because

- it is constructive, but also compatible with classical and intuitionistic mathematics,
- the stratification of types (e.g. propositions and sets) provides a flexible and informative way to formulate mathematical statements, and
- its implementations such as cubical Agda allow us to verify and execute proofs and constructions.

A constructive proof of the above claim is to do actual mathematics in UTT.

Summary and ...

Univalent type theory seems a good approach to constructive mathematics, because

- it is constructive, but also compatible with classical and intuitionistic mathematics,
- the stratification of types (e.g. propositions and sets) provides a flexible and informative way to formulate mathematical statements, and
- its implementations such as cubical Agda allow us to verify and execute proofs and constructions.

A constructive proof of the above claim is to do actual mathematics in UTT.

Thank you!

And, comments, remarks, suggestions . . . , please!!!