Constructive set theory – an overview

Benno van den Berg
Utrecht University

Heyting dag, Amsterdam, 7 September 2012

Partial history of constructive set theory

- 1967: Bishop's *Foundations of constructive analysis*.
- 1973: Set theories **IZF** (Friedman) and $\mathbf{IZF}_R$ (Myhill).
- 1975: Myhill, *Constructive set theory*. Set theory **CST**.
- 1977: Friedman, *Set theoretic foundations for constructive analysis*. Set theories $\mathbf{B}, \mathbf{T}_1, \mathbf{T}_2, \mathbf{T}_3, \mathbf{T}_4$.
- 1978: Aczel, *Type-theoretic interpretation of constructive set theory*. Set theory **CZF**.

I will concentrate on **IZF** and **CZF**.

The axioms of **ZFC**

The axioms of **ZFC** are:

- Extensionality
- Pairing
- Union
- Full separation
- Infinity
- Powerset
- Replacement
- Regularity (foundation)
- Choice

Choice

Two axioms in **ZFC** imply **LEM**.

Theorem (Goodman, Myhill, Diaconescu)

The axiom of choice implies **LEM**.

Proof.

We use the axiom of choice in the form: every surjection has a section. Let p be any proposition. Consider the equivalence relation $\sim$ on $\{0, 1\}$ with $0 \sim 1$ iff p. Let $q\colon \{0, 1\} \to \{0, 1\}/\sim$ be the quotient map and s be its section (using choice). Then we have $s([0]) = s([1])$ iff p. But the former statement is decidable. □

Regularity

Regularity says: every non-empty set x has an element disjoint from x.

Theorem

Regularity implies **LEM**.

Proof.

Let p be a proposition and consider $x = \{0 : p\} \cup \{1\}$. Regularity gives us an element $y \in x$ disjoint from x. We have $y = 0 \vee y = 1$ and $y = 0 \leftrightarrow p$. So p is decidable. □

$\mathbf{IZF}_R$ and **IZF**

The set theory $\mathbf{IZF}_R$ is obtained from **ZFC** by:

- replacing classical by constructive logic.
- dropping the axiom of choice.
- reformulating regularity as set induction:

$$(\forall x)\,\big((\forall \in x)\varphi(y) \to \varphi(x)\big) \to (\forall x)\,\varphi(x).$$

The set theory **IZF** is obtained from $\mathbf{IZF}_R$ by strengthening replacement to the collection axiom:

$$(\forall x \in a)\,(\exists y)\,\varphi(x,y) \to (\exists b)\,(\forall x \in a)\,(\exists y \in b)\,\varphi(x,y).$$

In **ZF** this axiom follows from the combination of Replacement and Regularity. Constructively that is not true, and **IZF** and $\mathbf{IZF}_R$ are different theories.

Models

Much work has been done on **IZF** in the seventies and eighties, and as a consequence **IZF** is very well understood. This also due to the fact that **IZF** has a nice model theory, with topological, Heyting-valued, sheaf and realizability models; and this semantics can be formalised inside **IZF** itself.

This is not true for $\mathbf{IZF}_R$! In fact, this theory remains a bit mysterious.

Replacement vs collection

IZF	$\mathbf{IZF}_R$
Good semantics	No good semantics
Does not have the set existence property (Friedman)	Does have the set existence property (Myhill)
As strong as **ZF**	Probably weaker than **ZF**

Theorem (Friedman)

There is a double-negation translation of **ZF** into **IZF**.

Theorem (Friedman)

IZF and $\mathbf{IZF}_R$ do not have the same provably recursive functions.

Conjecture (Friedman)

IZF proves the consistency of $\mathbf{IZF}_R$.

Axioms of **CZF**

Peter Aczel's set theory **CZF** is obtained from **IZF** by:

- Weakening full to bounded separation.
- Strengthening collection to strong collection:

$$(\forall x \in a)\,(\exists y)\,\varphi(x,y) \rightarrow$$
$$(\exists b)\,\big(\,(\forall x \in a)(\exists y \in b)\,\varphi(x,y) \wedge (\forall y \in b)\,(\exists x \in a)\,\varphi(x,y)\,\big).$$

- Weakening powerset axiom to fullness: for any two sets a and b there is a set c of total relations from a to b, such that any total relation from a to b is a superset of an element of c.

Properties of **CZF**

- Note **IZF** $\vdash$ **CZF**.
- **CZF** can be interpreted in Martin-Löf theory (**ML$_1$V**), using a "sets as trees" interpretation (Aczel). In fact, **CZF** and **ML$_1$V** have the same proof-theoretic strength.
- **CZF** $\nvdash$ Powerset and **CZF** $\nvdash$ Full Separation.
- **CZF** is "predicative".
- **CZF** has a good model theory, with realizability and sheaf models formalisable in **CZF** itself.
- **CZF** $\vdash$ Exponentiation.

Exponentiation vs fullness

Let $\mathbf{CZF}_E$ be **CZF** with exponentiation instead of fullness.

CZF	$\mathbf{CZF}_E$
Good semantics	No good semantics
Does not have the set existence property (Swan)	Does have the set existence property (Rathjen)
Dedekind reals form a set (Aczel)	Dedekind reals cannot be shown to be a set (Lubarsky)

$\mathbf{CZF}_E$ and **CZF** do have the same strength.

Formal topology

Formal topology: "predicative locale theory".

Formal space: essentially Grothendieck site on a preorder.

Idea: notion of basis as primitive, other notions (like that of a point) are derived.

Basis elements: preordered set $\mathbb{P}$.

A downwards closed subset of $\downarrow a = \{p \in \mathbb{P} \colon p \leq a\}$ we call a *sieve* on a.

Formal space

A *coverage* Cov on $\mathbb{P}$ is given by assigning to every object $a \in \mathbb{P}$ a collection Cov(a) of sieves on a such that the following axioms are satisfied:

(Maximality) The maximal sieve $\downarrow a$ belongs to Cov(a).

(Stability) If S belongs to Cov(a) and $b \leq a$, then b^*S belongs to Cov(b).

(Local character) Suppose S is a sieve on a. If $R \in$Cov(a) and all restrictions b^*S to elements $b \in R$ belong to Cov(b), then $S \in$ Cov(a).

Here $b^*S = S \cap \downarrow b$.

A pair ($\mathbb{P}$,Cov) consisting of a poset $\mathbb{P}$ and a coverage Cov on it is called a *formal topology* or a *formal space*.

Set-presentation

The well-behaved formal spaces are those that are *set-presented*.

For example, if you want to take sheaves over a formal space and get a model of **CZF** inside **CZF**, then the formal space has to be set-presented (Grayson, Gambino).

A formal topology $(\mathbb{P}, \mathrm{Cov})$ is called *set-presented*, if there is a function BCov which yields, for every $a \in \mathbb{P}$, a *small* collection of sieves $\mathrm{BCov}(a)$ such that:

$$S \in \mathrm{Cov}(a) \Leftrightarrow \exists R \in \mathrm{BCov}(a) \colon R \subseteq S.$$

(Btw, note this is an empty condition impredicatively!)

Examples

Formal Cantor space: basic opens are finite 01-sequences, with $S \in \mathrm{Cov}(a)$ iff there is an $n \in \mathbb{N}$ such that all extensions of a of length n belong to S.

This formal space is set-presented, by construction.

Formal Baire space: basic opens are finite sequences of natural numbers and the topology is inductively generated by:

$$\{u * \langle n \rangle : n \in \mathbb{N}\} \text{ covers } u.$$

This defines a formal space in **CZF**.

But is it also set-presented?

A dilemma

One would hope that **CZF** would be a nice foundation for formal topology.

But **CZF** is unable to show that many formal spaces are set-presented. Indeed:

Theorem (BvdB-Moerdijk)

CZF cannot show that formal Baire space is set-presented.

The proof shows that "formal Baire space is set-presented" implies the consistency of **CZF**.

Solution

As far as I am aware, there are two solutions:

- Add the Regular Extension Axiom **REA** (Aczel).
- Add W-types and the Axiom of Multiple Choice (Moerdijk, Palmgren, BvdB).

Both extensions

- imply the Set Compactness Theorem which implies that all "inductively generated formal topologies" (like formal Baire space) are set-presented.
- can be interpreted in $\mathbf{ML}_{1W}\mathbf{V}$.
- indeed, have the same proof-theoretic strength as $\mathbf{ML}_{1W}\mathbf{V}$.
- are therefore much stronger theories than **CZF**, but are still "generalised predicative".
- have a good model theory.
- are not subsystems of **IZF** (or even **ZF**!).

Foundations of formal topology

Still, there are results in formal topology which seem to go beyond $\mathbf{CZF} + \mathbf{REA}$ and $\mathbf{CZF} + \mathbf{WS} + \mathbf{AMC}$. Several axioms have been proposed to remedy this:

- strengthenings of **REA** (Aczel).
- the set-generatedness axiom **SGA** (Aczel, Ishihara).
- the principle for non-deterministic inductive definitions **NID** (BvdB).

A lot remains to be clarified!

CZF vs **IZF** 1

It is interesting to find differences between predicative **CZF** and impredicative **IZF**.

One difference is:

- **CZF** + **LEM** = **ZF**, which is much stronger than **CZF**.
- **IZF** + **LEM** = **ZF**, which is as strong as **IZF**.

Therefore:

- there can be no double-negation translation of **CZF** + **LEM** inside **CZF** (problem: fullness, or exponentiation).
- **CZF** cannot prove the existence of *set-presented* boolean formal spaces.

CZF vs **IZF** 2

Theorem (Friedman, Lubarsky, Streicher, BvdB)

There is a model of **CZF** in which the following principles hold:

- Full separation.
- The regular extension axiom **REA**.
- **WS** and **AMC**.
- The presentation axiom **PAx** (existence of enough projectives).
- All sets are subcountable (the surjective image of a subset of the natural numbers).
- The general uniformity principle **GUP**:

$$(\forall x)\,(\exists y \in a)\,\varphi(x, y) \rightarrow (\exists y \in a)\,(\forall x)\,\varphi(x, y).$$

The last two principles are incompatible with the power set axiom.

This model appears as the hereditarily subcountable sets in McCarty's realizability model of **IZF**.

CZF vs **IZF** 3

Especially **GUP**

$$(\forall x)\,(\exists y \in a)\,\varphi(x,y) \rightarrow (\exists y \in a)\,(\forall x)\,\varphi(x,y)$$

is interesting.

- Curi has shown it contradicts certain locale-theoretic results concerning Stone-Čech compactification, valid in **IZF** (or topos theory). Therefore these results fail in formal topology in **CZF** + **REA**.
- I have shown it implies that the only singletons are injective in the category of sets and functions.

Open problems

- Is a general uniformity *rule* a derived rule of **CZF**? (Jaap van Oosten)
- **CZF** + **PAx** proves the same arithmetical sentences as **CZF**. Is the same true for **IZF** + **PAx** and **IZF**? (Rathjen)
- Idem dito but for **DC** or **RDC** instead of **PAx**? (Beeson)

Even weaker

Friedman has observed that for developing the mathematics in Bishop's book you only need natural and set induction for bounded formulas.

Let $\mathbf{CZF}_0$ be **CZF** with natural and set induction restricted to bounded formulas. It is related to Friedman's set theory **B**.

Theorem (Friedman, Beeson, Gordeev)

$\mathbf{CZF}_0$ is a conservative extension of **HA**.

But $\mathbf{CZF}_0$ is probably not strong enough to do formal topology!

Table

Set theory	Arithmetical theory	Type theory
B, $\mathbf{T}_1$, $\mathbf{CZF}_0$	**PA**, $\mathbf{ACA}_0$	$\mathbf{ML}_0$
CST, $\mathbf{T}_2$	$\Sigma^1_1 - \mathbf{AC}$	$\mathbf{ML}_1$
CZF, **KP**ω, $\mathbf{T}_3$	$\mathbf{ID}_1$	$\mathbf{ML}_1\mathbf{V}$
CZF + **REA**, **KP**i	Δ^1_2-**CA** + **BI**	$\mathbf{ML}_{1W}\mathbf{V}$
CZF + Full Separation, $\mathbf{T}_4$	$\mathbf{PA}_2$	System F

More open questions

- Is **CZF** conservative for arithmetical sentences over an intuitionistic version of $\mathbf{ID}_1$?
- Is **CZF** + Full Separation conservative for arithmetical sentences over $\mathbf{HA}_2$?
- Is it possible to give a *simple* proof of the conservativity of $\mathbf{CZF}_0$ over **HA**?
- Crosilla and Rathjen have a system $\mathbf{CZF}^- + \mathbf{INAC}$ which has the same strength as $\mathbf{ATR}_0$. Is there a natural constructive set theory having the same strength as $\mathbf{\Pi}^1_1 - \mathbf{CA}_0$?