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 IZF$_R$ (Myhill).

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 $q: \{0, 1\} \rightarrow \{0, 1\}/\sim$ 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 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 $y = 0 \lor y = 1$ and $y = 0 \iff p$. So $p$ is decidable.
IZF\(_R\) and IZF

The set theory IZF\(_R\) is obtained from ZFC by:

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

\[(\forall x) \left( (\forall y \in x) \varphi(y) \rightarrow \varphi(x) \right) \rightarrow (\forall x) \varphi(x).\]

The set theory IZF is obtained from IZF\(_R\) by strengthening replacement to the collection axiom:

\[(\forall x \in a) (\exists y) \varphi(x, y) \rightarrow (\exists b) (\forall x \in a) (\exists y \in b) \varphi(x, y).\]

In ZF this axiom follows from the combination of Replacement and Regularity. Constructively that is not true, and IZF and IZF\(_R\) are different theories.
Models

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

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

<table>
<thead>
<tr>
<th>IZF</th>
<th>IZF&lt;sub&gt;R&lt;/sub&gt;</th>
</tr>
</thead>
<tbody>
<tr>
<td>Good semantics</td>
<td>No good semantics</td>
</tr>
<tr>
<td>Does not have the set existence property (Friedman)</td>
<td>Does have the set existence property (Myhill)</td>
</tr>
<tr>
<td>As strong as ZF</td>
<td>Probably weaker than ZF</td>
</tr>
</tbody>
</table>

**Theorem (Friedman)**

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

**Theorem (Friedman)**

IZF and IZF<sub>R</sub> do not have the same provably recursive functions.

**Conjecture (Friedman)**

IZF proves the consistency of IZF<sub>R</sub>.  

Axioms of **CZF**

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

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

\[(\forall x \in a) (\exists y) \varphi(x, y) \rightarrow (\exists b) ( (\forall x \in a)(\exists y \in b) \varphi(x, y) \land (\forall y \in b) (\exists x \in a) \varphi(x, y) ).\]

- **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 $\text{IZF} \vdash \text{CZF}$.
- $\text{CZF}$ can be interpreted in Martin-Löf theory ($\text{ML}_1 \text{V}$), using a “sets as trees” interpretation (Aczel). In fact, $\text{CZF}$ and $\text{ML}_1 \text{V}$ have the same proof-theoretic strength.
- $\text{CZF} \not\vdash$ Powerset and $\text{CZF} \not\vdash$ Full Separation.
- $\text{CZF}$ is “predicative”.
- $\text{CZF}$ has a good model theory, with realizability and sheaf models formalisable in $\text{CZF}$ itself.
- $\text{CZF} \vdash$ Exponentiation.
Exponentiation vs fullness

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

<table>
<thead>
<tr>
<th></th>
<th>$\text{CZF}$</th>
<th>$\text{CZF}_E$</th>
</tr>
</thead>
<tbody>
<tr>
<td>Good semantics</td>
<td>Good semantics</td>
<td>No good semantics</td>
</tr>
<tr>
<td>Does not have the set existence property (Swan)</td>
<td>Does have the set existence property (Rathjen)</td>
<td></td>
</tr>
<tr>
<td>Dedekind reals form a set (Aczel)</td>
<td>Dedekind reals cannot be shown to be a set (Lubarsky)</td>
<td></td>
</tr>
</tbody>
</table>

$\text{CZF}_E$ and $\text{CZF}$ 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 $\downarrow a = \{ p \in \mathbb{P} : p \leq a \}$ we call a sieve on $a$. 
A coverage Cov on $\mathbb{P}$ is given by assigning to every object $a \in \mathbb{P}$ a collection $\text{Cov}(a)$ of sieves on $a$ such that the following axioms are satisfied:

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

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

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

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

A pair $(\mathbb{P}, \text{Cov})$ 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 \( \textbf{CZF} \) inside \( \textbf{CZF} \), then the formal space has to be set-presented (Grayson, Gambino).

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

\[
S \in \text{Cov}(a) \iff \exists R \in \text{BCov}(a): R \subseteq S.
\]

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

Formal Cantor space: basic opens are finite 01-sequences, with $S \in \text{Cov}(a)$ 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 $\text{CZF}$.

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 \textbf{REA} (Aczel).
- Add \textit{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 $\text{ML}_{1\mathcal{W}}\mathcal{V}$.
- indeed, have the same proof-theoretic strength as $\text{ML}_{1\mathcal{W}}\mathcal{V}$.
- are therefore much stronger theories than \textbf{CZF}, but are still “generalised predicative”.
- have a good model theory.
- are not subsystems of \textbf{IZF} (or even \textbf{ZF}!).
Still, there are results in formal topology which seem to go beyond CZF + REA and CZF + WS + 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.
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.
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)
Friedman has observed that for developing the mathematics in Bishop’s book you only need natural and set induction for bounded formulas.

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

**Theorem (Friedman, Beeson, Gordeev)**

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

But $\text{CZF}_0$ is probably not strong enough to do formal topology!
<table>
<thead>
<tr>
<th>Set theory</th>
<th>Arithmetical theory</th>
<th>Type theory</th>
</tr>
</thead>
<tbody>
<tr>
<td>$B, T_1, CZF_0$</td>
<td>$PA, ACA_0$</td>
<td>$ML_0$</td>
</tr>
<tr>
<td>CST, $T_2$</td>
<td>$\Sigma_1^1 - AC$</td>
<td>$ML_1$</td>
</tr>
<tr>
<td>$CZF, KP_\omega, T_3$</td>
<td>$ID_1$</td>
<td>$ML_1 V$</td>
</tr>
<tr>
<td>$CZF + REA, KPi$</td>
<td>$\Delta^1_2$-CA + BI</td>
<td>$ML_{1W} V$</td>
</tr>
<tr>
<td>$CZF$ + Full Separation, $T_4$</td>
<td>$PA_2$</td>
<td>System $F$</td>
</tr>
</tbody>
</table>
More open questions

- Is CZF conservative for arithmetical sentences over an intuitionistic version of ID₁?
- Is CZF + Full Separation conservative for arithmetical sentences over HA₂?
- Is it possible to give a simple proof of the conservativity of CZF₀ over HA?
- Crosilla and Rathjen have a system CZF⁻ + INAC which has the same strength as ATR₀. Is there a natural constructive set theory having the same strength as Π₁¹ – CA₀?