Set Theory in Type Theory

Gert Smolka

Saarland University

Types 2015, Tallinn, May 19, 2015

How would you teach set theory to students who are familiar with type theory and proof assistants?

- Classical set theory with Zermelo-Fraenkel axioms

- Type theory with XM and impredicative Prop
- Coq as proof assistant

- Perspective very different from mathematical textbooks
- Explore an axiomatization in an expressive, explicit, and familiar logic

Axioms

$$\begin{aligned} \mathbf{S} &: \mathrm{Type} \\ \in &: \mathbf{S} \to \mathbf{S} \to \mathrm{Prop} \end{aligned}$$

$$x = y \leftrightarrow x \equiv y$$

$$\begin{aligned} z \in \emptyset &\leftrightarrow \bot \\ z \in \{x, y\} &\leftrightarrow z = x \lor z = y \\ z \in \bigcup x &\leftrightarrow \exists y \in x.\ z \in y \\ z \in \mathscr{P} x &\leftrightarrow z \subseteq x \\ z \in R @ x &\leftrightarrow \exists y \in x.\ Ryz \land \mathsf{unique}\,(Ry) \end{aligned}$$

- Replacement axiom is higher-order, $R : \mathbf{S} \to \mathbf{S} \to \mathrm{Prop}$
- Infinity and choice are not needed for this talk

Classes

- A **class** is a predicate $p : \mathbf{S} \to \mathrm{Prop}$
- Not every class can be represented as a set, e.g., $\lambda x.\ x \notin x$

- Type theory provides classes and relations on classes
- Classes are not formalized by Zermelo-Fraenkel set theory
- Von-Neumann-Gödel-Bernays set theory accommodates sets and classes in first-order logic

Separation and Description

can be expressed with replacement

$$
\begin{aligned}
z \in x \cap p &\leftrightarrow z \in x \wedge px && \text{separation} \\
p \ulcorner p \urcorner &\leftarrow p \text{ unique and inhabited} && \text{description}
\end{aligned}
$$

An operator that maps relations R on $\mathbf{S}$ to total functions $f : \mathbf{S} \to \mathbf{S}$ such that f agrees with R on unique images can be expressed (i.e., $Rx(fx)$)

Numbers and Ordered Pairs

can be represented as sets

- Functions, numbers, and pairs already exist in type theory
- Can express functions $\overline{\cdot} : \mathbf{N} \to \mathbf{S}$, $\mathrm{succ} : \mathbf{S} \to \mathbf{S}$, and $\mathrm{pred} : \mathbf{S} \to \mathbf{S}$ such that:

$$\begin{aligned} \overline{m} = \overline{m} &\leftrightarrow m = n \\ \mathrm{succ}\ \overline{n} &= \overline{n+1} \\ \mathrm{pred}\ \overline{n+1} &= \overline{n} \end{aligned}$$

- Can express functions $\mathrm{pair} : \mathbf{S} \to \mathbf{S} \to \mathbf{S}$, $\mathrm{fst} : \mathbf{S} \to \mathbf{S}$, and $\mathrm{snd} : \mathbf{S} \to \mathbf{S}$ such that:

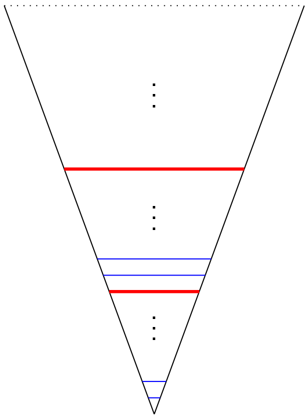
$$\begin{aligned} \mathrm{pair}\ x\ y = \mathrm{pair}\ x'\ y' &\to x = x' \wedge y = y' \\ \mathrm{fst}\ (\mathrm{pair}\ x\ y) &= x \\ \mathrm{snd}\ (\mathrm{pair}\ x\ y) &= y \end{aligned}$$

- [Barras 2010] [von Neumann 1923] [Kuratowski 1921]

Can Construct Models of Axioms

- Without infinity hereditarily finite sets suffice
- Use Ackermann encoding into numbers
- Need strong excluded middle for replacement ($\mathrm{Prop} \simeq \mathrm{bool}$)
- Aczel, Werner, Miquel construct models with infinite sets

Cumulative Hierarchy



- Horizontal lines represent stages (successors and limits)
- Blue lines also represent slices
- Every well-founded set appears in some slice
- Stages are well-ordered
- Every well-ordered set is order-isomorphic to a unique segment

Well-Founded Sets

- Define class $\mathscr{W}$ of **well-founded sets** inductively

$$\frac{x \subseteq \mathscr{W}}{x \in \mathscr{W}}$$

- Well-founded sets are defined as sets that admit ϵ-induction
- Inductive definition unknown in set theory
- Regularity axiom can be expressed as $\forall x.\, x \in \mathscr{W}$
- First-order characterization of $x \in \mathscr{W}$ seems to require infinity (to express transitive closure)
- First-order characterization of $x \in \mathscr{W} \cap \mathscr{T}$ straightforward
- Aczel [1988] studies non-well-founded sets
- $\mathscr{W}$ cannot be represented as a set

Stages of Cumulative Hierarchy

- Define class $\mathscr{Z}$ of **cumulative sets** inductively

$$\frac{x \subseteq \mathscr{Z}}{\bigcup x \in \mathscr{Z}} \qquad \frac{x \in \mathscr{Z}}{x \cup \mathscr{P}x \in \mathscr{Z}}$$

- $\mathscr{Z}$ well-ordered by $\subseteq$, unbounded, $\emptyset$ least element
- $\mathscr{W} \equiv \bigcup \mathscr{Z}$
- $x \subset y$ iff $x \in y$ for all $x, y \in \mathscr{Z}$
- $x \cup \mathscr{P}x = \mathscr{P}x$ if $x \in \mathscr{Z}$ since $\mathscr{Z} \subseteq \mathscr{T}$
- Definition of $\mathscr{Z}$ is instance of tower construction
- $\mathscr{Z}$ usually defined with transfinite induction on ordinals

Ordinals

- Define class $\mathscr{O}$ of **ordinals** inductively

$$\frac{x \subseteq \mathscr{O}}{\bigcup x \in \mathscr{O}} \qquad \frac{x \in \mathscr{O}}{x \cup \{x\} \in \mathscr{O}}$$

- Every cumulative slice contains exactly one ordinal
- Every ordinal is the set of all smaller ordinals
- Every well-ordered set is order isomorphic to a unique ordinal
- $\mathscr{O}$ order isomorphic with $\mathscr{Z}$
- Definition of $\mathscr{O}$ is instance of tower construction

First-Order Characterization of Ordinals

- Ordinals are hereditarily transitive and well-founded sets [Bernays 1931]

- $x \in \mathscr{O}$ iff $x \in \mathscr{T}$ and $x \subseteq \mathscr{T}$ and $x \in \mathscr{W}$
- $x \in \mathscr{O}$ iff $x \in \mathscr{T}$ and $x \subseteq \mathscr{T}$ and $\mathscr{P}x \subseteq \mathscr{R}$

- $\mathscr{T} := \{\, x \mid \forall y \in x.\ y \subseteq x \,\}$ transtive sets
- $\mathscr{R} := \{\, x \mid \exists y \in x\ \forall z \in x.\ z \notin y \,\}$ regular sets

- If $x \in \mathscr{T}$, then $x \in \mathscr{W}$ iff $\mathscr{P}x \subseteq \mathscr{R}$

- Corresponding inductive characterization:

$$\frac{x \in \mathscr{T} \qquad x \subseteq \mathscr{O}}{x \in \mathscr{O}}$$

Tower Construction for Sets

- Assume $f : \mathbf{S} \to \mathbf{S}$
- Define class T of sets inductively:

$$\frac{x \subseteq T}{\bigcup x \in T} \qquad \frac{x \in T}{x \cup f\,x \in T}$$

- T is well-ordered by $\subseteq$, $\emptyset$ least element
- $x \cup f\,x$ successor of x if $x \in T$ not maximal
- Every segment of T can be represented as a set
- If f preserves transitivity and well-foundedness, and $x \in f\,x$ for all x,
  - T unbounded
  - T cannot be represented as a set
  - Every well-ordered set is isomorphic to a proper segment of T
  - $x \in y$ iff $x \subset y$ for all $x, y \in T$

Tower Construction for Complete Partial Orders

- Assume type X and partial order $\leq$
- Assume $x_0 : X$
- Assume increasing function $f : X \to X$ (i.e., $x \leq f\,x$)
- Assume family $\mathscr{S}$ of classes on X, closed under subclasses
- Assume function $\bigsqcup$ that yields supremum for every $p \in \mathscr{S}$
- Define class T on X inductively:

$$\frac{}{x_0 \in T} \qquad \frac{x \in T}{f\,x \in T} \qquad \frac{p \subseteq T \qquad p \in \mathscr{S} \qquad p \text{ inhabited}}{\bigsqcup p \in T}$$

- T well-ordered by $\leq$ (x_0 least element, f yields successors)
- T unbounded iff f has no fixed point in T
- If $T \in \mathscr{S}$, then $\bigsqcup T$ is unique fixed point of f in T (Bourbaki-Witt theorem)
- See forthcoming paper at ITP 2015

Final Remarks

- Type theory provides expressive language for talking about sets and classes
  - more natural than first-order logic
  - first-order encodings are low-level and tedious; e.g.,
    - well-founded sets
    - von-Neumann-Gödel-Bernays set theory
- Many aspects of set theory can be formulated more generally at the level of type theory:
  - Well-orderings
  - Transfinite recursion
  - Tower construction
  - Well-ordering theorem
- Cumulative hierarchy can be considered before ordinals, transfinite recursion is not needed