Making Set Theory Great Again: The Naproche-SAD Project

Steffen Frerix and Peter Koepke
University of Bonn, Germany
AITP 2019, Obergurgl

10th April 2019

Let's make set theory great again!

John Harrison
Amazon Web Services

AITP 2018, Aussois

27th March 2018 (10:45–11:30)

Foundations in theorem proving

Many of the most popular interactive theorem provers are based on type theory

- Simple type theory (HOL family, Isabelle/HOL)
- Constructive type theory (Agda, Coq, Nuprl)
- Other typed formalisms (IMPS, PVS)

Far fewer substantial systems are based on set theory:

- Metamath
- Isabelle/ZF (but much less popular than Isabelle/HOL)
- Mizar (but that layers a type system on top)

Why not types?

My thesis is that types, despite their merits, have significant disadvantages:

- Types can create dilemmas or inflexibility
- Types can clutter proofs
- Subtypes may not work smoothly
- Type systems are complicated

There are simple type theories like HOL but they are the most inflexible.

Set theory as a foundation

We propose in some sense the 'obvious' foundation in set theory, and the only innovations are a few conventions we think make thing smoother or more natural.

- Work in a fairly standard (ZFC...?) universe of sets and construct number systems and mathematical objects in one of the 'usual' ways, probably in fairly standard first-order logic.
- Things you would express as type constraints in typed systems are usually expressed as set membership: $x : \mathbb{R}$ becomes $x \in \mathbb{R}$ etc.
- Constraints that quantify over 'large' collections like $w : \mathrm{ordinal}$ become applications of predicates $\mathrm{ordinal}(w)$, though we could support syntactic sugar like $x \in On$.

Set theory as a machine code

The philosophy is to use set theory act as a simple, well-understood foundation but leave the theorem proving to layers of code, which the foundations don't help but also don't hinder.

- Can do some kind of 'type checking' for catching errors, encouraging a disciplined style, and do some inference more efficiently.
- Wiedijk's paper "Mizar's soft type theory" shows how in principle Mizar's type system can be understood this way, even though in practice it's coded separately.

The Common Foundations of Mathematics

N. Bourbaki, Theory of Sets

> *... it is known to be possible, logically speaking, to derive practically the whole of known mathematics from a single source, the Theory of Sets. Thus it is sufficient for our purposes to describe the principles of a single formalized language, to indicate how the Theory of Sets could be written in this language, and then to show how the various branches of mathematics, to the extent that we are concerned ... fit into this framework.*

The Common Foundations of Mathematics

Space of continuous functions $\equiv$ **set** of functions, such that ...

f is *continuous* iff $\forall\epsilon\exists\delta$...

The Common Language of Mathematics

Theorem (72c)

For every set x there exist an ordinal α and function f such that $f : \alpha \leftrightarrow x$.

Proof.

...

□

SAD: System for Automated Deduction

- Part of the Evidence Algorithm project (Victor M. Glushkov et. al.)
- 2008 Implementation by Andrei Paskevich
- Controlled natural language input in ForTheL
- First-order logic
- Internal reasoner
- External prover like E
- Small system and small formalizations

Naproche-SAD.

- Naproche: Natural Proof Checking since ca. 2005
- Master project on SAD of Steffen Frerix 2017/2018
- Presentation at AITP 2018
- Enhancing SAD
- Interfacing with LaTeX
- Isabelle-like PIDE with Makarius Wenzel

Let A, B stand for sets. Let $x \in A$ denote x is an element of A. Let x is *in* A denote x is an element of A. Let $x \notin A$ denote x is not an element of A.

Signature 1 *The* empty set *is the set that has no elements. Let* $\emptyset$ *denote the empty set.*

Definition 1 A *is* nonempty *iff* A *has an element.*

Definition 2 A *subset of* B *is a set* A *such that every element of* A *is an element of* B*. Let* $A \subseteq B$ *stand for* A *is a subset of* B*. Let* $B \supseteq A$ *stand for* A *is a subset of* B*.*

Definition 3 A proper subset *of* B *is a subset* A *of* B *such that there is an element of* B *that is not in* A*.*

Proposition 1 $A \subseteq A$*.*

Proposition 2 *If* $A \subseteq B$ *and* $B \subseteq A$ *then* $A = B$*.*

Definition 4 $A \cup B = \{x \mid x \in A \text{ or } x \in B\}$.

The Field of Real Numbers

Rudin introduces $\mathbb{R}$ in Theorem 1.19 and refers to the ordered field axioms in 1.5, 1.6, 1.12. Our propositions correspond to Rudin's 1.14 - 1.16 on fields.

[number/-s]

Signature 2 *A* real number *is a notion.*

Signature 3 $\mathbb{R}$ *is the set of* real numbers. *Let* x, y, z *denote real numbers.*

Signature 4 $x + y$ *is a real number. Let the* sum *of* x *and* y *denote* $x + y$.

Signature 5 $x \cdot y$ *is a real number. Let the* product *of* x *and* y *denote* $x \cdot y$.

Signature 6 $x < y$ *is an atom. Let* $x > y$ *stand for* $y < x$. *Let* $x \leq y$ *stand for* $x < y \vee x = y$. *Let* $x \geq y$ *stand for* $y \leq x$.

Axiom 1 $x < y \wedge x \neq y \wedge \neg y < x$ *or* $\neg x < y \wedge x = y \wedge \neg y < x$ *or* $\neg x < y \wedge x \neq y \wedge y < x$.

Signature 10 *Assume $x \neq 0$. $1/x$ is a real number such that $x \cdot (1/x) = 1$.*

Axiom 7 (Distributivity) $x \cdot (y + z) = (x \cdot y) + (x \cdot z)$.

Proposition 4 $(y \cdot x) + (z \cdot x) = (y + z) \cdot x$.

Proof

$$(y \cdot x) + (z \cdot x). = (x \cdot y) + (x \cdot z). = x \cdot (y + z). = (y + z) \cdot x$$

. □

Proposition 5 *If $x + y = x + z$ then $y = z$.*

Proof Assume $x + y = x + z$. Then

$$y = (-x + x) + y = -x + (x + y) = -x + (x + z) = (-x + x) + z = z.$$

□

Proposition 6 *If* $x + y = x$ *then* $y = 0$.

Proposition 7 *If* $x + y = 0$ *then* $y = -x$.

Proposition 8 $-(-x) = x$.

Proposition 9 *If* $x \neq 0$ *and* $x \cdot y = x \cdot z$ *then* $y = z$.

Proof Let $x \neq 0$ and $x \cdot y = x \cdot z$.

$$y = 1 \cdot y = ((1/x) \cdot x) \cdot y = (1/x) \cdot (x \cdot y) = (1/x) \cdot (x \cdot z) = ((1/x) \cdot x) \cdot z = 1 \cdot z = z.$$

□

Proposition 10 *If* $x \neq 0$ *and* $x \cdot y = x$ *then* $y = 1$.

Proposition 11 *If* $x \neq 0$ *and* $x \cdot y = 1$ *then* $y = 1/x$.

Proposition 12 *If* $x \neq 0$ *then* $1/(1/x) = x$.

Definition 11 *Let E be a subset of $\mathbb{R}$ such that E is bounded above. A* least upper bound *of E is a real number a such that a is an upper bound of E and for all x if $x < a$ then x is not an upper bound of E.*

Definition 12 *Let E be a subset of $\mathbb{R}$ such that E is bounded below. A* greatest lower bound *of E is a real number a such that a is a lower bound of E and for all x if $x > a$ then x is not a lower bound of E.*

Axiom 10 *Assume that E is a nonempty subset of $\mathbb{R}$ such that E is bounded above. Then E has a least upper bound.*

Definition 13 *Let E be a subset of $\mathbb{R}$. $E^- = \{-x \mid x \in E\}$.*

Lemma 1 *Let E be a subset of $\mathbb{R}$. x is an upper bound of E iff $-x$ is a lower bound of E^-.*

Theorem 1 *Assume that E is a nonempty subset of $\mathbb{R}$ such that E is bounded below. Then E has a greatest lower bound.*

Proof Take a lower bound a of E. $-a$ is an upper bound of E^-. Take a least upper bound b of E^-. Let us show that $-b$ is a greatest lower bound of E. $-b$ is a lower bound of E. Let c be a lower bound of E. Then $-c$ is an upper bound of E^-. end. □

Rational Numbers

Integer and rational numbers are not axiomatized or constructed in Rudin, but simple assumed. We need the following formalizations to make the text self-contained.

Signature 11 *A* rational number *is a real number. Let* p, q, r *stand for rational numbers.*

Definition 14 $\mathbb{Q}$ *is the set of rational numbers.*

Lemma 2 $\mathbb{Q} \subseteq \mathbb{R}$.

Theorem 5 (120a) *If $x \in \mathbb{R}$ and $y \in \mathbb{R}$ and $x > 0$ then there is a positive integer n such that*

$$n \cdot x > y.$$

Proof Define $X = \{n \cdot x \mid n \text{ is a positive integer}\}$. Assume the contrary. Then y is an upper bound of X. Take a least upper bound α of X. $\alpha - x < \alpha$ and $\alpha - x$ is not an upper bound of X. Take an element z of X such that not $z \leq \alpha - x$. Take a positive integer m such that $z = m \cdot x$. Then $\alpha - x < m \cdot x$ (by 15b).

$\alpha = (\alpha - x) + x <$

$(m \cdot x) + x = (m + 1) \cdot x.$

$(m+1) \cdot x$ is an element of X. Contradiction. Indeed α is an upper bound of X. □

Theorem 6 *(a) If $x \in \mathbb{R}$, $y \in \mathbb{R}$, and $x > 0$, then there is a positive integer n such that*

$$nx > y.$$

Proof Let A be the set of all nx, where n runs through the positive integers. If (a) were false, then y would be an upper bound of A. But then A has a *least* upper bound in $\mathbb{R}$. Put $\alpha = \sup A$. Since $x > 0$, $\alpha - x < \alpha$, and $\alpha - x$ is not an upper bound of A. Hence $\alpha - x < mx$ for some positive integer m. But then $\alpha < (m + 1)x \in A$, which is impossible, since α is an upper bound of A. □

Theorem 7 (120b) *If $x \in \mathbb{R}$ and $y \in \mathbb{R}$ and $x < y$ then there exists a rational number p such that $x < p < y$.*

Proof Assume $x < y$. We have $y - x > 0$. Take a positive integer n such that $n \cdot (y - x) > 1$ (by 120a). Take an integer m such that $m - 1 \leq n \cdot x < m$. Then

$$n \cdot x < m = (m - 1) + 1$$

$$\leq (n \cdot x) + 1 < (n \cdot x) + (n \cdot (y - x))$$

$$= n \cdot (x + (y - x)) = n \cdot y.$$

$m \leq (n \cdot x) + 1 < n \cdot y$. $\frac{m}{n} < \frac{n \cdot y}{n}$. Indeed $m < n \cdot y$ and $1/n > 0$. Then

$$x = \frac{n \cdot x}{n} < \frac{m}{n} < \frac{n \cdot y}{n} = y.$$

Let $p = \frac{m}{n}$. Then $p \in \mathbb{Q}$ and $x < p < y$. □

Theorem 8 *If $x \in \mathbb{R}$, $y \in \mathbb{R}$, and $x < y$, then there exists a $p \in \mathbb{Q}$ such that $x < p < y$.*

Proof Since $x < y$, we have $y - x > 0$, and (a) furnishes a positive integer n such that

$$m(y - x) > 1.$$

Apply (a) again, to obtain positive integers m_1 and m_2 such that $m_1 > nx$, $m_2 > -nx$. Then

$$-m_2 < nx < m_1.$$

Hence there is an integer m (with $-m_2 \leq m \leq m_1$) such that

$$m - 1 \leq nx < m.$$

If we combine these inequalities, we obtain

$$nx < m \leq 1 + nx < ny.$$

Since $n > 0$, it follows that

$$x < \frac{m}{n} < y.$$

This proves (b), with $p = m/n$. □

Naproche-SAD.

- Formal mathematics with first-order logic and set theory is feasible (and great!)
- FOL and set theory support doing formal mathematics naturally
- This may help with the wider acceptance of formal mathematics

Further plans

- Linked libraries of formalizations
- Language extensions, with LaTeX
- Correctness certificates
- Interfacing with other systems
- Automatically translating common mathematical language into ForTheL?
- Checking of free mathematical texts?

Thank You!