Inspire Create Transform

A Set Theory Formalization

Alejandro Calle-Saldarriaga

Universidad EAFIT
School of Sciences
Departament of Mathematical Sciences
Logic and Computation Research Group

Some basic stuff

- "*Every mathematician agrees that every mathematician must know some set theory*" - Halmos [1974].
- "Set" and "membership" are primitive notions in set theory. Intuitively, set means a mental collection of things (the members of the set). Membership is a relation between sets that asserts whether a set belongs to another set.
- Pure set: A set where all its members are sets, and the members of its members are sets, and so on. Let $\varnothing$ be the set which has no members. Then $\varnothing$ and $\{\varnothing, \{\varnothing\}\}$ are examples of pure sets.

von Neumann universe

The von Nuemann hierarchy of sets [Singh and Singh, 2007] gives us a pure set universe with many advantages and little generality lost. In this universe, $V_0 = \varnothing$ and $V_{\alpha+1} = \mathcal{P} V_\alpha$.

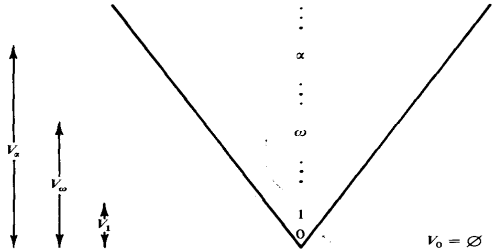

Figure: von Neuman universe. Taken from Enderton [1977].

Justification

- Set theory has been very important for mathematics since Cantor.
- “*...our axioms provide a sufficient collection of assumptions for the development of the whole of mathematics—a remarkable fact.*” - Enderton [1977]
- Formalizing mathematics in computers removes any ambiguities or errors we humans may commit: as you know, to err is human.

Our problem

- A proof assistant is a software tool that verifies the validity of a formalization and automatically checks proofs.
- We want to formalize set theory in a proof assistant.
- One theorem we are specially interested in is the induction principle.
- Two questions arise: What axiomatization of set theory shall we use? What proof assistant?

State of the art

- The MIZAR SYSTEM [Bancerek et al., 2015] uses the Tarski-Grothendieck axioms [Trybulec, 1990] and proves the induction property for ω [Bancerek, 1990].
- In ISABELLE [Nipkow et al., 2016], there are two papers that describe their formalization of the **ZF** axioms [Paulson, 2000a,b].
- There is also a **ZFC** encoding in the proof assistant COQ [Werner, 1996, Coquand and Huet, 1989].
- As far as we know, there are no **ZFC** formalizations in AGDA.

Some historical context

- Cantor [1955] was specially interested in set theory.
- Based on his work, Frege tried to present the principles of set theory as principles of logic.
- Russel derived a contradiction from Frege's principles (Russell's Paradox).
- Zermelo [1967] publishes a new axiomatization avoiding said paradox.
- Fraenkel [Ebbinghaus, 2007] adds the axiom of replacement to Zermelo's axioms .
- The axiom of choice is added to make what we now call the **ZFC** axiomatization of set theory.

Intuitionism

- Intuitionism is one of the main points of view in the philosophy of mathematics.
- Wishes to implement the ideas of constructivism (mathematical objects exists only if they are constructed), due to Brouwer and Heyting [Bezhaishvili and de Jongh, 2005].
- In particular: Existential assertions should be backed up by effective constructions of objects.
- Mathematical truth is created rather than discovered.

Intuitionistic logic

- It is different than classical logic: typically it is not accepted to prove $\exists x \phi(x)$ by deriving a contradiction from the assumption $\forall x \neg \phi(x)$, since such a proof does not create the object supposed to exist.
- A way to characterize intuitionistic logic is by a natural deduction system where logical connectives $\wedge$, $\vee$, and $\rightarrow$ and quantifiers $\forall$ and $\exists$ have some introduction and elimination rules.

Intuitionistic logic

- Negation is usually defined as $\neg\phi := \phi \to \bot$ ($\bot$ is the absurd or falsum).
- Anything can be derived from $\bot$.
- If one wishes to get classical predicate logic, one could add the principle of the excluded middle ($\phi \vee \neg\phi$ is always true).

BHK-interpretation of intuitionistic logic

- In classical logic the meaning of connectives is based on the truth of its parts, e.g. $\phi \wedge \psi$ is true iff ϕ is true and ψ is true, $\neg\phi$ is true iff ϕ is not true, etc.
- The BHK-interpretation of intuitionistic logic is based on the notion of proof, e.g. A proof of $\phi \wedge \psi$ consists of a proof of ϕ and a proof of ψ, plus the conclusion $\phi \wedge \psi$. A proof of $\phi \to \psi$ consists of a method of converting a proof of ϕ into a proof of ψ. No proof of $\bot$ exists. A proof of $\exists x \phi(x)$ consists of an object d and a proof of $\phi(d)$ plus the conclusion that $\exists x \phi(x)$.

BHK-interpretation of intuitionistic logic

- Consequences: Disjunctions and existentials are hard to prove, things based on the two-valuedness of truth are not valid (e.g. $\neg\neg\phi \to \phi$).
- If one would add $(\neg\phi \to \bot) \to \phi$ one would have classical logic.
- AGDA uses intuitionistic logic.

Objectives

General Objective

Formalize some results of set theory using AGDA.

Specific Objectives

- Formalizing **Z**'s axioms using AGDA.
- Proving the induction principle in AGDA.
- Using APIA's automation to prove some more properties.

Methodology

Mostly Suppes [1960] was read while formalizing its major results in AGDA. Weekly meetings were held discussing the work done and the tutor provided help with certain theorems. The order provided in the book is the same we used. The formalization can be found in the repository[1].

[1] https://github.com/acalles1/setform

Methodology

The original idea was to follow the book until the Principle of Mathematical Induction, which is proven by contradiction using the Well-Ordering Principle, but the tutor found a direct proof made by user Git Gud on Mathematics Stack Exchange[2]. We only needed to use the axioms in **Z** for the proofs we made.

[2] https://math.stackexchange.com/questions/490825/prove-the-principle-of-mathematical-induction-in-sf-zfc/490880

Extensionality and the subset relation

The first axiom we introduce is extensionality:

$$\forall x \forall y \forall z (z \in x \leftrightarrow z \in y \rightarrow x = y),$$

and we define the subset relation:

$$x \subseteq y \leftrightarrow \forall t (t \in x \rightarrow t \in y).$$

Some consequences of extensionality

Using the subset relation and the axiom, we get these two theorems:

$$\forall x(x \subseteq x),$$

$$\forall x \forall y(x \subseteq y \land y \subseteq x \rightarrow x = y).$$

The empty set

Some axioms in **Z** allows us to assert the existence of certain sets. The first set we introduce is the set which has no elements:

$$\exists B \forall x (x \notin B).$$

We call the set with this property $\varnothing$. It can be proven that this set is unique.

Algebra of sets

The axiom of union:

$$\forall x \forall y (\exists B [\forall z (z \in B \leftrightarrow z \in x \vee z \in y)]),$$

combined with the subset axiom schema, allows use to define the usual operations of set theory, like union, difference, intersection, etc. The subset axiom schema is:

$$\forall y \exists B \forall z [z \in B \leftrightarrow (z \in y \wedge \phi(z))].$$

Pair axiom

We have only constructed the set $\varnothing$ until now. So, in order to have more sets, we add the pair axiom:

$$\forall x \forall y \exists B \forall z (z \in B \leftrightarrow z = x \vee z = y),$$

from which we can prove (but using the principle of excluded middle):

$$\forall x \forall y \forall u \forall v [\{x, y\} = \{u, v\} \rightarrow (u = x \wedge v = y) \vee (v = x \wedge u = y)].$$

Ordered pairs

With unordered pairs, we can define ordered pairs like this:

$$\langle x, y\rangle = \{\{x\}, \{x, y\}\},$$

and using the last theorem we can prove that:

$$\forall x \forall y \forall u \forall v(\langle x, y\rangle = \langle u, v\rangle \rightarrow x = u \land y = v).$$

Ordered pairs makes the construction of relations and functions possible, which are very prevalent concepts in most mathematics.

Power set

The power set axiom asserts the existence of a power set of a given set:

$$\forall x \exists B \forall y (y \in B \leftrightarrow y \subseteq x),$$

and call the power set of x by $\mathcal{P}x$. We then prove some properties like this:

$$\exists C \forall x (x \in C \leftrightarrow [\exists y \exists z (y \in A \wedge z \in B \wedge x = \langle y, z \rangle)],$$

Power set

The past theorem is proven using this instance of the axiom schema of separation:

$$\exists C \forall x (x \in C \leftrightarrow x \in \mathcal{P}\mathcal{P}(A \cup B) \wedge \exists y \exists z [y \in A \wedge z \in B \wedge x = \langle y, z \rangle]).$$

This properties allows us to define cartesian products like this:

$$\langle x, y \rangle \in A \times B \leftrightarrow x \in A \wedge y \in B.$$

Relations and functions between two sets are subsets of the Cartesian product between those sets. Being able to define this operation is quite important.

Axiom of Regularity

The axiom of regularity gives sets some properties we want sets to have. It can be stated like this:

$$\forall A(A \neq \varnothing \to \exists x[x \in A \wedge \forall y(y \in x \to y \notin A)]).$$

It says that given a non-empty set A, there is an $x \in A$ such that $A \cap x = \varnothing$

Regularity's consequences

Regularity has two intuitive consequence

$$\forall A (A \notin A),$$

$$\forall A \forall B [\neg (A \in B \land B \in A)].$$

The Axiom of Infinity

The last axiom we formalize is the axiom of infinity:

$$\exists I(\varnothing \in I \wedge \forall x[x \in I \rightarrow x \cup \{x\} \in I]).$$

We define the succesor of a set x (called x^+) as $x \cup \{x\}$. A set A is said to be inductive if:

$$ind(A) = \varnothing \in A \wedge \forall x(x \in A \rightarrow x^+ \in A).$$

Induction

Then, by instantiating the formula $\phi(x) = \forall A(ind(A) \to x \in A)$ on the subset axiom we get that:

$$\exists B \forall x (x \in B \leftrightarrow x \in I \land \forall A[ind(A) \to x \in A]),$$

which tells us that a set x belongs to B if it is a natural number. Lets call the set of natural numbers $\mathbb{N}$, and can formulate this version of Mathematical induction:

$$\forall A[A \subseteq \mathbb{N} \land \varnothing \in A \land \forall n(n \in A \to n^{+} \in A)) \to A = \mathbb{N}].$$

Natural Numbers

Then we can define naturals like this:

$$
\begin{aligned}
0 &= \varnothing \\
1 &= 0^{+} = \{\varnothing\} \\
2 &= 1^{+} = \{\varnothing, \{\varnothing\}\},
\end{aligned}
$$

and so on. In general, they can be defined recursively as:

$$
\begin{aligned}
0 &= \varnothing \\
n + 1 &= n^{+}.
\end{aligned}
$$

Properties of Naturals

This set-theoretic construction gives these two interesting properties to numbers:

$$0 \in 1 \in 2 \in 3 \in \ldots$$

$$0 \subseteq 1 \subseteq 2 \subseteq 3 \subseteq \ldots$$

Conclusions

- It is possible to prove the Principle of Mathematical Induction on ω just using the axioms in **Z**.
- Most of the theorems here were proven using only intuitionistic logic.
- Set theory is formalized by just using a handful of axioms and a simple binary relation called membership and this can lead us to interesting results despite using such 'rudimentary' tools.

Future Work

- In future work, a set-theoretic formalization of rational numbers and subsequently of real numbers may be possible, since we were able to formalize natural numbers.
- The consequences of the axioms included in **ZFC** but not on **Z** may also be studied in later projects.

References I

Grzegorz Bancerek. The Fundamental Properties of Natural Numbers. *Formalized Mathematics*, 1(1):41–46, 1990.

Grzegorz Bancerek, Czesław Byliński, Adam Grabowski, Arthur Korniłowicz, Roman Matuszewski, Adam Naumowicz, Karol Pąk, and Josef Urban. Mizar: State-of-the-art and Beyond. *Conferences on Intelligent Computer Mathematics. CICM 2015*, 9150:261–279, 2015.

Nick Bezhaishvili and Dick de Jongh. Intuitionisic Logic. Technical report, Universitet van Amsterdam, 2005.

References II

Georg Cantor. *Contributions to the Founding of the Theory of Transfinite Numbers, translated by P. Jourdain*. Dover, New York, 1 edition, 1955.

Thierry Coquand and Gérard Huet. The coq proof assistant, 1989. URL `https://coq.inria.fr/`.

Heinz-Dieter Ebbinghaus. *Ernst Zermelo: An Approach to His Life and Work*. Springer, 2007.

Herbert B. Enderton. *Elements of Set Theory*. Academic Press, 1 edition, 1977.

Paul R. Halmos. *Naive Set Theory*. Springer, 1974.

References III

Tobias Nipkow, Lawrence C. Paulson, and Markus Wenzel. *Isabelle/HOL: A Proof Assistant for Higher-Order Logic*, volume 2283 of *Lecture Notes in Computer Science*. Springer-Verlag, December 2016.

Lawrence C. Paulson. Set Theory for Verification: I. From Foundations to Functions. Technical report, Cambridge University, 2000a.

Lawrence C. Paulson. Set Theory for Verification: II. Induction and Recursion. Technical report, Cambridge University, 2000b.

References IV

D. Singh and J. N. Singh. von neumann universe: A perspective. *International Journal of Contemporary Mathematical Sciences*, 2:475–478, 2007.

Patrick Suppes. *Axiomatic Set Theory*. The University Series in Undergraduate Mathematics. D. Van Nostrand Company, 1960.

Andrzej Trybulec. Tarski Grothendieck Set Theory. *Formalized Mathematics*, 1(1):9–11, 1990.

Benjamin Werner. An encoding of Zermelo-Fraenkel set theory in Coq, 1996. URL `https://github.com/coq-contribs/zfc/`.

References V

Ernst Zermelo. Investigations in the foundations of set theory I. In Jean van Heijenoort, editor, *From Frege to Gödel: A Source Book in Mathematical Logic, 1879 - 1931*. Harvard University Press, 1967.

Thanks!