Research Practice Final Report

A Set Theory Formalization

Alejandro Calle-Saldarriaga

acalles@eafit.edu.co

Mathematical Engineering, Universidad EAFIT
Tutor: Andrés Sicard-Ramírez

June 3, 2017

1 Problem definition

A little preliminary definition: a set is any kind of mental collection of things. Each of the things in a set is called a member of the set. Set theory is the area of mathematics that study sets, and we can construct almost all known mathematics from it [Enderton, 1977]. Sets in set theory are a primitive notion so they are not defined in terms of previously defined concepts (we just appeal to intuition, akin to points and lines in axiomatic geometry), so the general approach is to describe what is it that one can do with sets via some axioms and prove some properties about sets using those axioms.

In this work we will only use pure sets. A set is pure when all of its members are sets, and the members of their members are sets, and so on. Let $\varnothing$ be the set which has no members, called the empty set. Then the sets $\varnothing$; $\{\varnothing\}$; $\{\varnothing, \{\varnothing\}\}$ and $\{\{\varnothing\}\}$ are pure sets. We will restrict our attention to the von Neumann universe [Singh & Singh, 2007] of pure sets, since pure sets gives us many advantages and little generality lost, as most mathematical concepts can be modeled using these sets. You can see that the von Neumann universe in figure (1) has a very particular hierarchy of sets: $V_0 = \varnothing$ is the atom, and $V_{\alpha+1} = \mathcal{P}V_\alpha$, where $\mathcal{P}V_\alpha$ is the power set of V_α, meaning the set of all subsets of V_α.

Here we are trying to formalize[1] set theory using a proof assistant, which is a software tool that verifies the validity of our formalization and automatically checks our proofs [Berendregt & Geuvers, 2001]. We will have to pick a specific axiomatization of set theory in order to translate the axiom to the syntax of the proof assistant we chose. To explain what axiomatization we picked, first a little historical context: Cantor [1955] was specially interested in set theory and made very interesting advances like proving there was more than one kind of infinity. Then some further advances by Frege tried to present the principles of set theory as being principles of logic, but this project failed when Russell informed Frege of a contradiction derivable from the principles (Rusell's paradox). This had tremendous impact in the foundations of mathematics, and new formalizations for set theory were needed. In 1908, Zermelo published his axiomatization of set theory, called the **Z** axioms [Zermelo, 1967]. In 1922 the axiom of replacement was proposed by Fraenkel [Ebbinghaus, 2007], and all these axioms together with the axiom of choice make up what we call the **ZFC** (Zermelo

[1] In this work formalization means that we are translating a mathematical theory into an specific proof assistant, as opposed to classical mathematical formalization which is just an axiomatization of a given theory.

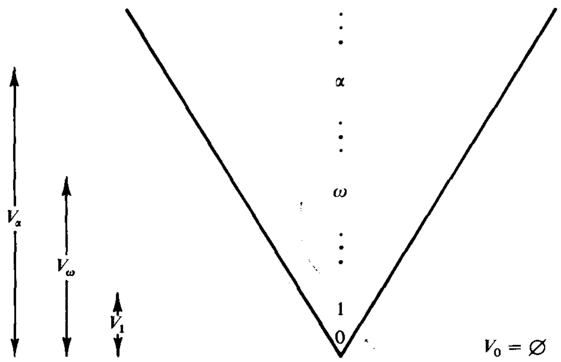

Figure 1: von Neuman universe. Taken from Enderton [1977].

– Fraenkel with Choice) axiomatization – set theory's most popular formalization [Enderton, 1977]. It is important to note that this formalization is written in first-order logic. We will use the **Z** axioms in this work.

Other axiomatizations exist, like for example the **GT** (Grothendieck-Tarski) one, which adds the Tarski axiom [Tarski, 1938] to the **ZFC** axioms.

The proof assistant we are using is AGDA, which is based on constructive type-theory [Bove & Dybjer, 2009; Norell, 2007]. We will also use APIA [Sicard-Ramírez, 2015], a HASKELL program that proves first-order logic theorems.

Strictly formalized proofs that are checked automatically are desirable, and that is why systems such as proof assistants have been created. Set theory's theorems and axioms are translatable into logic, so the process of formalization is possible.

One particular theorem we are interested in is the induction principle for ω (induction for the natural numbers). Most of set theory's texts mention that the induction principle is provable from the **Z** axioms, but they skip the proof, so finding the demonstration for this cornerstone principle in mathematics would be quite interesting.

2 State of the art

There are some set theory formalizations checked with proof assistants out there. For example, the MIZAR SYSTEM [Bancerek et al., 2015] uses the Tarski-Grothendieck axioms [Trybulec, 1990] and proves the induction property [Bancerek, 1990] for ω. In ISABELLE [Nipkow, Paulson, & Wenzel, 2016], another proof assistant, there are two papers that describe their formalization of the ZF axioms [Paulson, 2000a, 2000b]. Lastly, we also refer to the **ZFC** encoding in the proof assistant COQ [Coquand & Huet, 1989; Werner, 1996].

3 Justification

"*Every mathematician agrees that every mathematician must know some set theory*" - Halmos [1974].

Set theory has been very important for modern mathematics since Cantor started studying it in the late XIX century. It is often used as a foundation for all mathematics, so it is a very fruitful and interesting area of study.

Formalizing mathematics in computers is very important since it removes any ambiguities or errors we humans may commit while doing mathematics. Particularly, formalizing set theory is a very interesting endeavor, since it is such a central theory for all mathematics.

As far as the authors know, there is no formalization of **Z** on AGDA, so providing one will help the further development of their libraries. Automating reasoning is also one of our concerns, and APIA will help us do that with set theory.

This research project is within the interest of EAFIT's Logic and Computation Group, which is another plus for the university.

4 Methodology

For this work, mostly Suppes [1960] was read while formalizing all the major results in AGDA. Weekly meetings were held then discussing the work done, as well as help provided by the tutor with certain doubts I had while trying to prove difficult theorems. The order provided in Suppes [1960] was followed for theorems, but not proving every one of them (i.e. if the book formalized Theorem 40 and then Theorem 45, then I would follow a similar order, not necessarily proving Theorem 41-44, only when they were necessary results for the proof of Theorem 45).

The original idea was to follow the same book until the Principle of Mathematical Induction (Chapter 5, Theorem Schema 22), which is proven by contradiction based on the Well-Ordering Principle, but the turor found a direct proof by user Git Gud on Mathematics Stack Exchange[2]. He then formalized the proof and an adapted version can be found in our repository[3].

5 Results

The results are backed up by the code in the aforementioned repository. The purpose of this section is not to write out all proofs I made in my code, but to showcase some interesting ones that might shed light to some important ideas in axiomatic set theory.

First of all I would like to mention that as well as sets, the idea of membership (e. g. $x \in A$ means that x is in A, or in other words, that the set x is a member of the set A) is also a primitive notion in set theory. It is quite impressive that using only this simple binary relation and the axioms we are about to present, one can formalize very powerful results. But more on that later. Using this binary relation, we can define then the subset relation, which is:

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

The first axiom we use is extentionality

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

which asserts that two sets that have the same elements are the same set. This gives us some important results. For example, we get the two following theorems:

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

[3] `https://github.com/acalles1/setform/`

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

$$\forall x \forall y(x \subseteq y \wedge y \subseteq x \rightarrow x = y),$$

meaning that every set is subset of itself and if a two sets are each subset of one another, then they are the same set.

Note that we don't really have any sets yet, since the assertion of the existence of a set haven't been done. Some axioms of the **Z** axiomatization will then allows us to introduce sets with certain properties. The first one might by the empty set:

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

The empty set then is the set which has no elements. We might call the set that follows this property $\varnothing$. It can be proven that this set is unique. The next axiom we use is the union axiom, which is stated as:

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

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

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

It is called an axiom schema because it is actually a rule that determines infinite formulas that the theory accepts as axioms. For every different, correctly written formula $\phi(z)$, we get a valid axiom. It is important to note that there must be no mention of B in $\phi(z)$ for the schema to work. If you make $\phi(z) = z \in x$ you can define the intersection between y and x. We can also define things like difference, symmetric difference and all the usual operations between sets using different instances of this axiom schema.

But if you have noticed, we have only asserted the existence of one set until now: the empty set. Well, we have union, intersection and difference, but if you only have the empty set, then you can't define other sets (Recall that $\varnothing \cup \varnothing = \varnothing$, $\varnothing \cap \varnothing = \varnothing$ and $\varnothing - \varnothing = \varnothing$), so we need to introduce another axiom that help us create other sets from the empty set, and that those sets are different than the empty set. And the pair axiom helps us do just that:

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

This axiom assert that for any sets x and y, there is a set with just x and y as elements. Then, using $x = y = \varnothing$, we can construct the set $\{\varnothing, \varnothing\}$, which is the same as the set $\{\varnothing\}$. Now, finally, we have a set that is different than the empty set! We can use then the union axiom, or the pair axiom again to construct other sets like $\{\{\varnothing\}, \varnothing\}$; $\{\{\varnothing\}\}$ or $\{\{\varnothing\}, \varnothing, \{\{\varnothing\}\}\}$

One interesting consequence of the pair axiom is:

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

The proof is not as easy at it may look (it was partially done by the tutor), and we have to add the principle of excluded middle as an axiom (the principle asserts that $A \vee \neg A$ is always true for any proposition A) in order to prove it. We had to add this property as an axiom since AGDA uses intuitionistic logic [Norell, 2007], which does not accept this principle in general [Moschovakis, 2015].

Keep in mind the pairs we are talking about until now are unordered pairs. But with this unordered pairs, we can define ordered pairs like this:

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

then using, the previous theorem we can prove this property:

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

Having ordered pairs make us have all sorts of interesting sets and makes the constructions of relations and functions possible. Another interesting set is the power set of any set, meaning a set which contains all the subsets of a given set. Its existence is justified using the subset axiom:

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

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

$$\exists C \forall x(x \in C \leftrightarrow [\exists y \exists z(y \in A \land z \in B \land x = \langle y, z\rangle)], \tag{1}$$

which is proven using this instance of the axiom schema of separation:

$$\exists C \forall x(x \in C \leftrightarrow x \in \mathcal{P}\mathcal{P}(A \cup B) \land \exists y \exists z[y \in A \land z \in B \land x = \langle y, z\rangle]). \tag{2}$$

Then, Theorem (1) is just Theorem (2) but without the clause '$x \in \mathcal{P}\mathcal{P}(A \cup B)$', so we just show that the equivalence still holds when the clause is eliminated. This property es very interesting, since it allows us to assert the existence of a set which is the cartesian product of two sets. This property allows us to define cartesian products like this:

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

Relations and functions between two sets, two of the most important concepts in mathematics, are subsets of the cartesian products between those sets [Hamilton, 1983], so being able to define this operation on the few axioms we've mentioned is a remarkable result.

The next axiom we formalize is regularity, which can be stated as:

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

Intuitively, it says that given any non-empty set A, there is a $x \in A$ such that $A \cap x = \varnothing$. This has a very intuitive consequence:

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

which means that a set can not be an element of itself.

At last, for proving the induction principle, we have to introduce our last axiom: the axiom of infinity. The proof we present here was made by user Git Gud on Mathematics Stack Exchange, formalized by the tutor in AGDA and adapted to fit in the code that already existed in this work. The axiom of infinity reads like this:

$$\exists I(\varnothing \in I \land \forall x[x \in I \to x \cup \{x\} \in I]). \tag{3}$$

Also, we can define the "successor" of a set x (let's call it x^+) as $x \cup \{x\}$. A set A is said to be inductive when it follows this property:

$$ind(A) = \varnothing \in A \land \forall x(x \in A \to x^+ \in A).$$

Lets I be the set that exists because of axiom (3). Lets also consider the formula

$$\varnothing(x) = \forall A(ind(A) \to x \in A).$$

By instantiating the subset axiom schema on I and on $\phi(x)$, we obtain the following property:

$$\exists B \forall x(x \in B \leftrightarrow x \in I \land \forall A[ind(A) \to x \in A]). \tag{4}$$

This statement asserts that a set x belongs to the set B if x is a natural number. We shall call the set of natural numbers $\mathbb{N}$, and formulate this version of the principle of Mathematical induction [Iborra, n.d.]:

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

To prove this, we need to prove that $x \in A \to x \in \mathbb{N}$ and $x \in \mathbb{N} \to x \in A$. The first part is trivial since A $\subseteq \mathbb{N}$. Now, from the second and third hypothesis, and Theorem (4), we know that A is an inductive set and a natural number belongs to every inductive set. This finishes the proof of the principle of mathematical induction.

Then, the natural numbers can be constructed using sets in this way [Boolos, 1998]:

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

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

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

The fact that we proved induction without using the axiom of Choice nor the axiom of foundation is an important fact, reducing our system of axioms to the one Zermelo published in 1908 [Zermelo, 1967] (The **Z** axiom system). Franekel's axiom of foundation was introduced later after heavy correspondence by him and Zermelo [Ebbinghaus, 2007], making the system in the famous **ZF**, but since we didn't have to formalize Fraenkel's axiom for any result in this work, we can say we solely worked within the axiom system **Z**.

Also, since our proof of induction did not use the Well-Ordering principle, like one usually sees in set theory textbooks, then we did not have to formalize the axiom of choice either, since the well ordering principle and the axiom of choice are equivalent statements [Kuczma, 2009].

6 Conclusions and Future Work

- It is possible to prove the Principle of Mathematical Induction on ω just using the axioms in **Z**, not needing to resort to **ZFC**.
- Many of set theory's theorems can be proved with intuitionistic logic (i.e. without using the principle of the excluded middle), but one of our proofs in this work had to use it.

- 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.
- 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.

Acknowledgments

I would like to thank Andrés Sicard-Ramírez for his patience and help throughout this project.

References

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

Bancerek, G., Byliński, C., Grabowski, A., Korniłowicz, A., Matuszewski, R., Naumowicz, A., … Urban, J. (2015). Mizar: State-of-the-art and Beyond. *Conferences on Intelligent Computer Mathematics. CICM 2015*, *9150*, 261–279.

Berendregt, H., & Geuvers, H. (2001). Proof-assistants using Dependent Type Systems. In A. Robinson & A. Voronokov (Eds.), *Handbook of automated reasoning* (p. 1151-1238).

Boolos, G. (1998). *Logic, Logic, and Logic*. Harvard University Press.

Bove, A., & Dybjer, P. (2009). Dependent Types at Work. *Lecture Notes in Computer Science*, *5520*(1), 57–99.

Cantor, G. (1955). *Contributions to the Founding of the Theory of Transfinite Numbers, translated by P. Jourdain* (1st ed.). Dover, New York.

Coquand, T., & Huet, G. (1989). *The Coq Proof Assistant.* Retrieved 2016-02-10, from `https://coq.inria.fr/`

Ebbinghaus, H.-D. (2007). *Ernst Zermelo: An Approach to His Life and Work.* Springer.

Enderton, H. B. (1977). *Elements of Set Theory.* Academic Press.

Halmos, P. R. (1974). *Naive Set Theory.* Springer.

Hamilton, A. (1983). *Numbers, Sets and Axioms: The Apparatus of Mathematics.* Cambridge University Press.

Iborra, C. (n.d.). *Teoría Descriptiva de Conjuntos I.* Retrieved from `https://www.uv.es/ivorra/Libros/Libros.htm`

Kuczma, M. (2009). *An Introduction to the Theory of Functional Equations and Inequalities: Cauchy's Equation and Jensen's Inequality.* Springer.

Moschovakis, J. (2015). Intuitionistic Logic. In E. N. Zalta (Ed.), *The stanford encyclopedia of philosophy* (Spring 2015 ed.). Metaphysics Research Lab, Stanford University. `https://plato.stanford.edu/archives/spr2015/entries/logic-intuitionistic/.`

Nipkow, T., Paulson, L. C., & Wenzel, M. (2016). *Isabelle/HOL: A Proof Assistant for Higher-Order Logic* (Vol. 2283). Springer-Verlag.

Norell, U. (2007). *Towards a practical programming language based on dependent type theory.* Chalmers University of Technology.

Paulson, L. C. (2000a). *Set Theory for Verification: I. From Foundations to Functions* (Tech. Rep.). Cambridge University.

Paulson, L. C. (2000b). *Set Theory for Verification: II. Induction and Recursion* (Tech. Rep.). Cambridge University.

Sicard-Ramírez, A. (2015). *Reasoning about Functional Programs by Combining Interactive and Automatic Proofs*. Universidad de la República PEDECIBA Informática Uruguay.

Singh, D., & Singh, J. N. (2007). von Neumann Universe: A Perspective. *International Journal of Contemporary Mathematical Sciences*, *2*, 475–478.

Suppes, P. (1960). *Axiomatic Set Theory*. D. Van Nostrand Company.

Tarski, A. (1938). On the well-order subsets of any set. *Fundamenta Mathematicae*, *32*, 68–89.

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

Werner, B. (1996). *An encoding of Zermelo-Fraenkel set theory in Coq.* Retrieved 2016-02-06, from `https://github.com/coq-contribs/zfc/`

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