MyTitle

MyName

October 28, 2024

Contents

Chapter 1

Introduction

The formalization of mathematics using proof assistants such as Isabelle, Coq, and Lean, has been actively conducted, leading to numerous achievements. For instance, the proofs of the four color theorem, Kepler's conjecture, and the Feit-Thompson theorem have been formalized using proof assistants, enhancing the reliability of these proofs. Additionally, various fields of mathematics, such as number theory, algebra, and topology, are also being formalized. However, the formalization related to axiomatic set theory is

The independence of the axiom of choice(AC) from Zermelo-Fraenkel set theory(ZF) is a well-known result in the early history of axiomatic set theory, as well as the independence of the continuum hypothesis(CH) from ZF with AC(ZFC). Cohen invented the forcing method and proved them in 1963. Forcing is a powerful tool for exploring models of set theory and was subsequently further sophisticated by other researchers.

Independence proofs of CH from ZFC has been formalized in Isabelle/ZF by Gunther et al. [1] and in Lean 3 by Han and van Doorn [2]. In these studies, forcing methods were formalized, and the independence of CH was proven by showing the relative consistency of ZFC + CH and ZFC + ¬CH with ZFC.

For AC, the relative consistency of ZFC with ZF has been formalized in Isabelle/ZF by Paulson [3]. However, the relative consistency of ZF + ¬AC with ZF has not been formalized. It can be proven by forcing, but the proof involves complexities that cannot be achieved by simply modifying the proof for CH.

In this work, we formalized the relative consistency proof of ZF + ¬AC with ZF in Isabelle/ZF. This work contributes to the formalization of axiomatic set theory, an area with relatively few prior works. It also serves as a new example of the formalization using forcing, which is a crucial tool in set theory.

This work may provide insights into how the formalization of axiomatic set theory could be advanced.

This work may serve as a basis for considering how the formalization of axiomatic set theory should proceed and what advancements in formalization techniques could be beneficial in the future.

In axiomatic set theory, discussions often shift between meta-level and object-level considerations, such as considering models of set theory within set theory itself. For-

malizing such discussions is considered a challenging task.

Outline

In Chapter 2, we introduce the set-theoretic preliminaries used in this study.

Chapter 2

Set-Theoretic Preliminaries

In this chapter, we introduce the concepts of set theory used in the formalization of this study. We use first-order logic with the language of set theory, which consists only of only two relation symbols $\in$ and $=$. Formulas involving other mathmatical operators that may appear are considered abbreviations for formulas in this language. Parentheses in formulas are omitted where no confusion arises. Unless otherwise stated, "a statement holds" means "the statement holds in ZF".

2.1 ZF Set Theory and the Axiom of Choice

Definition 2.1. *The axioms of ZF are the following statements:*

- *Extensionality:* $\forall x \forall y (\forall z (z \in x \leftrightarrow z \in y) \rightarrow x = y)$
- *Pairing:* $\forall x \forall y \exists z \forall w (w \in z \leftrightarrow w = x \vee w = y)$
- *Union:* $\forall x \exists y \forall z (z \in y \leftrightarrow \exists w (z \in w \wedge w \in x))$
- *Power set:* $\forall x \exists y \forall z (z \in y \leftrightarrow z \subseteq x)$
- *Infinity:* $\exists x (\emptyset \in x \wedge \forall y (y \in x \rightarrow y \cup \{y\} \in x))$
- *Regularity:* $\forall x (x \neq \emptyset \rightarrow \exists y (y \in x \wedge y \cap x = \emptyset))$
- *Infinity:* $\forall x (x \neq \emptyset \rightarrow \exists y (y \in x \wedge \forall z (z \in x \rightarrow z \notin y)))$
- *Separation:* $\forall p \forall x \exists y \forall z (z \in y \leftrightarrow z \in x \wedge \phi(z, p))$
- *Replacement:* $\forall p (\forall x \forall y \forall z (\phi(x, y, p) \wedge \phi(x, z, p) \rightarrow y = z) \rightarrow$
  $\forall X \exists Y \forall y (y \in Y \leftrightarrow \exists x (x \in X \wedge \phi(x, y, p))))$

Where separation and replacement are axiom schemas, representing infinitely many axioms for each formula ϕ with an appropriate arity.

Definition 2.2. The axiom of choice (AC) *is the following statement:*
$\forall x \exists f (\text{"}f \text{ is a function on } x\text{"} \wedge \forall y (y \in x \rightarrow f(y) \in y))$

Where the phrase "f is a function on x" is also considered an abbreviation in the language of set theory. Theory ZF + AC is denoted by ZFC. Next, we introduce the well-ordering theorem, as we treat AC in this form.

Definition 2.3. *We say that a linear ordering $<$ on a set P is a* well-ordering *if, every non-empty subset of P, it has a least element.*

Lemma 2.4. *The axiom of choice is equivalent to the well-ordering theorem, which states that every set can be well-ordered.*

2.2 Forcing

Forcing is a tequnique used in proving relative consistency and Independence. We introduce basic concepts of forcing in the context of the transitive countable model (c.t.m.) approach. In this approach, the relative consistency proof is achieved by using forcing to construct a extended model by adding new sets to an assumed c.t.m. Let M be a c.t.m. of ZF and $(\mathbb{P}, \leq_{\mathbb{P}})$ be a notion of forcing, which is a pre-ordered set in M with a maximum element $1_{\mathbb{P}}$.

Definition 2.5. *We define $M^{\mathbb{P}}$, the set of* $\mathbb{P}$-names*, by transfinite recursion on ordinals:*

1. $M_0^{\mathbb{P}} = \emptyset$
2. $M_{\alpha+1}^{\mathbb{P}} = \mathcal{P}^M(M_\alpha^{\mathbb{P}} \times \mathbb{P})$
3. $M_\alpha^{\mathbb{P}} = \bigcup_{\beta<\alpha} M_\beta^{\mathbb{P}}$ *for a limit ordinal* α
4. $M^{\mathbb{P}} = \bigcup_{\alpha \in Ord} M_\alpha^{\mathbb{P}}$

Where $\mathcal{P}^M$ denotes the power set operation in M. We often write a $\mathbb{P}$-name with a dot, e.g., $\dot{x}$.

Definition 2.6.

1. *We say that $D \subseteq \mathbb{P}$ is* dense *if, for every $p \in \mathbb{P}$, there exists $q \in D$ such that $q \leq_{\mathbb{P}} p$.*
2. *We say that $G \subseteq \mathbb{P}$ is a* filter *if following conditions hold:*
   - *If $p \in G$, $q \in \mathbb{P}$, and $p \leq_{\mathbb{P}} q$, then $q \in G$*
   - *If $p, q \in G$, there exists $r \in G$ such that $r \leq_{\mathbb{P}} p$ and $r \leq_{\mathbb{P}} q$*
3. *We say that $G \subseteq$ is* generic filter *on $\mathbb{P}$ if G is a filter and for any dense $D \subseteq \mathbb{P}$, $D \cap G \neq \emptyset$.*

The following lemma shows that a generic filter actually exists.

Lemma 2.7. *For any $p \in \mathbb{P}$, there exists a generic filter G on $\mathbb{P}$ such that $p \in G$.*

Definition 2.8. *Let G be a generic filter on $\mathbb{P}$ and $\dot{x} \in M^{\mathbb{P}}$. We define the* interpretation *of $\dot{x}$ denoted by $\dot{x}_G$ recursively, $\dot{x}_G = \{\dot{y}_G \mid \exists p \in G(\langle \dot{y}, p \rangle \in \dot{x})\}$.*

We call a Pbb-name whose interpretation is a set x a name of x and denote it by $\dot{x}$. Note that a single set may have multiple names.

Definition 2.9. *Let G be a generic filter on $\mathbb{P}$. We define a* generic extension $M[G]$ *as* $\{x_G \mid \dot{x} \in M^{\mathbb{P}}\}$.

Theorem 2.10. *Let G be a generic filter on $\mathbb{P}$. Then, $M[G]$ is the smallest c.t.m. of ZF extending M and containing G.*

By choosing $\mathbb{P}$ appropriately, we can construct $M[G]$ with various properties. What holds or does not hold in $M[G]$ can be identified using the forcing relation.

Definition 2.11 (Forcing relation)**.** *ATODE*

Theorem 2.12 (Forcing relation and generic extensions)**.** *ATODE*

2.3 Symmetric Extensions

Symmetric extensions are substructures of generic extensions of a given c.t.m. of ZF and are formed by interpreting only the hereditarily symmetric names. Let M be a c.t.m. of ZF, $(\mathbb{P}, \leq_{\mathbb{P}})$ be a pre-ordered set in M with the maximum element $1_{\mathbb{P}}$.

Definition 2.13. *We say that $\pi : \mathbb{P} \to \mathbb{P}$ is an* automorphism *if for all $p, q \in \mathbb{P}$, $p \leq_{\mathbb{P}} q \Leftrightarrow \pi p \leq_{\mathbb{P}} \pi q$. π induces an bijection on $\mathbb{P}$-names defined recursively as follows:*

$$\pi\dot{x} = \{\langle \pi\dot{y}, \pi p\rangle \mid \langle \dot{y}, p\rangle \in \dot{x}\}$$

Definition 2.14. *Let $\mathcal{G}$ be a group of automorphisms of $\mathbb{P}$. We say that $\mathcal{F}$ is a* normal filter *on $\mathcal{G}$ if the following conditions hold:*

1. *$\mathcal{F}$ is non-empty family of subgroups of $\mathcal{G}$.*
2. *$\mathcal{F}$ is closed under finite intersections and supergroups.*
3. *For every $H \in \mathcal{F}$ and $\pi \in \mathcal{G}$, $\pi H \pi^{-1} \in \mathcal{F}$.*

We fix a group of automorphisms $\mathcal{G}$ of $\mathbb{P}$ and a normal filter $\mathcal{F}$ on $\mathcal{G}$.

Definition 2.15. *For every $\mathbb{P}$-name $\dot{x}$, let $sym_{\mathcal{G}}(\dot{x}) = \{\pi \in \mathcal{G} \mid \pi\dot{x} = \dot{x}\}$. We say that $\mathbb{P}$-name $\dot{x}$ is* hereditarily $\mathcal{F}$-symmetric *if $sym_{\mathcal{G}}(\dot{x}) \in \mathcal{F}$. $HS_{\mathcal{F}}$ denotes the set of all hereditarily $\mathcal{F}$-symmetric $\mathbb{P}$-names.*

Definition 2.16. *Let G be a generic filter on $\mathbb{P}$. The set $HS^G_{\mathcal{F}} = \{\dot{x}_G \mid \dot{x} \in HS_{\mathcal{F}}\}$ is called a* symmetric extension *of M.*

Theorem 2.17. *Let G be a generic filter on $\mathbb{P}$. Then, the symmetric extension $HS^G_{\mathcal{F}}$ is a c.t.m. of ZF and a substructure of $M[G]$.*

Definition 2.18 (HS forcing relation)**.** *ATODE*

Lemma 2.19 (strengthening)**.** *ATODE*

Theorem 2.20 (relation between HS forcing relations and symmetric extensions)**.** *ATODE*

Lemma 2.21 (Symmetric Lemma)**.** *ATODE*

Chapter 3

Outline of the Formalized Proof

We outline the formalized relative consistency proof of ZF + ¬AC. In this proof, the relative consistency is proved by assuming the existence of a c.t.m. of ZF and constructing a model of ZF + ¬AC by forcing. This model is a symmetric extension called the basic Cohen model.

Let M be a c.t.m. of ZF, $\mathbb{P}$ be the set of all finite partial functions from $\omega \times \omega$ to $\{0, 1\}$, and $\leq_{\mathbb{P}}$ be $\supseteq$. Note that the maximum element $1_{\mathbb{P}}$ is the empty set. Let π be a bijection on ω. π induces an automorphism on $\mathbb{P}$ defined as follows:

$$dom(\pi p) = \{(\pi n, m) \mid (n, m) \in dom(p)\}$$
$$(\pi p)(\pi n, m) = p(n, m)$$

This automorphism further induces an automorphism on $\mathbb{P}$-names. Let $\mathcal{G}$ be the group of all such automorphisms. For every finite $e \subseteq \omega$, let

$$\mathrm{fix}(e) = \{\pi \in \mathcal{G} \mid \forall n \in e(\pi n = n)\}$$

Let $\mathcal{F}$ be the set of all subgroups H of $\mathcal{G}$ such that there exists a finite $e \subseteq \omega$ with $\mathrm{fix}(e) \subseteq H$. Note that $\mathcal{F}$ is a normal filter on $\mathcal{G}$. Let $\mathcal{N} = \mathrm{HS}^{G}_{\mathcal{F}}$. Since $\mathcal{N}$ is a symmetric extension of M, it is a c.t.m. of ZF.

Theorem 3.1. *$\mathcal{N}$ does not satisfy the well-ordering theorem.*

Proof. We outline the proof of this theorem as follows. For every $n \in \omega$, let a_n be the following real number:

$$a_n = \{m \in \omega \mid \exists p \in G(p(n, m) = 1)\}$$

Since a_n are pairwise distinct, $A = \{a_n \mid n \in \omega\}$ is an infinity set. A and every a_n are elements of $\mathcal{N}$. A serves as a counterexample to the well-ordering theorem in $\mathcal{N}$. Suppose for contradiction that A is well-ordered in $\mathcal{N}$, there exists a injection f from ω to A in $\mathcal{N}$. Let $\varphi(g, x, y)$ be a formula that represents the relation $g(x) = y$. For

every $n \in \omega$, There exists $i \in \omega$ such that $N \vDash \varphi(f, i, a_n)$. Thus there exists $p \in G$ and hereditarily $\mathcal{F}$-symmetric names $\dot{f}, \dot{i}$ and $\dot{a_n}$ for each of f, i, a_n such that

$$p \Vdash_{\mathrm{HS}} \varphi(\dot{f}, \dot{i}, \dot{a_n})$$

By choosing n and the names appropriately, we can find $\pi \in \mathcal{G}$ such that the following conditions are additionally satisfied:

1. $\pi \dot{f} = \dot{f}$
2. $\pi \dot{i} = \dot{i}$
3. $\pi n \neq n$
4. There exists a hereditarily $\mathcal{F}$-symmetric name $\dot{a_{\pi n}}$ of $a_{\pi n}$ such that $\pi \dot{a_n} = \dot{a_{\pi n}}$
5. There exists $q \in G$ such that $q \leq_{\mathbb{P}} p$ and $q \leq_{\mathbb{P}} \pi p$

By Lemma **??**

$$\pi p \Vdash_{\mathrm{HS}} \varphi(\pi \dot{f}, \pi \dot{i}, \pi \dot{a_n})$$

Thus

$$\pi p \Vdash_{\mathrm{HS}} \varphi(\dot{f}, \dot{i}, \dot{a_{\pi n}})$$

Therefore, by Lemma **??**

$$q \Vdash_{\mathrm{HS}} \varphi(\dot{f}, \dot{i}, \dot{a_n}) \text{ and } q \Vdash_{\mathrm{HS}} \varphi(\dot{f}, \dot{i}, \dot{a_{\pi n}})$$

This means that $\mathcal{N} \vDash \varphi(f, i, a_n)$ and $\mathcal{N} \vDash \varphi(f, i, a_{\pi n})$, which implies that $f(i) = a_n$ and $f(i) = a_{\pi n}$. Since a_n and $a_{\pi n}$ are distinct, this is a contradiction. □

Chapter 4

Isabelle/ZF and Formalization in Prior Work

In this chapter, we introduce Isabelle/ZF, a proof assistant for ZF set theory, and the results from prior work used in the formalization of this study.

4.1 Isabelle/ZF

4.2 Internalized First-Order Formulas

4.3 Forcing

Chapter 5

Formalization of the Proof

5.1 Introduction to the Formalization

In this chapter, we

5.2 Defining Symmetric Extensions

5.2.1 $\mathbb{P}$-names

5.2.2 Automorphisms

5.2.3 Hereditarily Symmetric Names

5.2.4 Symmetric Extensions

5.3 Proving that Symmetric Extensions are Models of ZF

5.3.1 Relativized Forcing Relation $\Vdash_{HS}$

5.3.2 The Symmetric Lemma

5.3.3 Separation

5.3.4 Replacement

5.3.5 Other Axioms

5.4 Defining the Basic Cohen Model

5.4.1 The Notion of Forcing

5.4.2 The Group of Automorphisms

5.4.3 The Normal Filter

5.5 Proving that the Basic Cohen Model satisfies ¬AC

Chapter 6

Conclusion and Future Work

Bibliography

[1] Emmanuel Gunther et al. “The Independence of the Continuum Hypothesis in Isabelle/ZF”. In: *Archive of Formal Proofs* (Mar. 2022). https://isa-afp.org/entries/Independence_CH.html, Formal proof development. ISSN: 2150-914x.

[2] Jesse Michael Han and Floris van Doorn. “A formal proof of the independence of the continuum hypothesis”. In: *Proceedings of the 9th ACM SIGPLAN International Conference on Certified Programs and Proofs, CPP 2020, New Orleans, LA, USA, January 20-21, 2020*. 2020.

[3] Lawrence C. Paulson. “The Relative Consistency of the Axiom of Choice Mechanized Using Isabelle/ZF”. In: (2021). DOI: 10.1112/S1461157000000449. eprint: arXiv:2104.12674.