MyTitle

MyName

November 1, 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.

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. [**gunther_independence**] and in Lean 3 by Han and van Doorn [**flypitch**]. In these studies, forcing methods were formalized, and the independence of CH was proven by showing the relative consistency of CH and ¬CH with ZFC.

For AC, the relative consistency of AC with ZF has been formalized in Isabelle/ZF by Paulson [**paulson_AC_consistency**]. However, the relative consistency of ¬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 ¬AC with ZF in Isabelle/ZF. This work contributes to the formalization of axiomatic set theory and serves as a new example of the formalization using forcing, which is a crucial tool in set theory. It also may provide insights into how the formalization of axiomatic set theory could be advanced.

Our Approach

The primary reason we chose Isabelle/ZF for this formalization is that Isabelle/ZF is a mature proof assistant for ZF set theory, in particular, the formalization by Gunther et al. [**gunther_forcing**] is a major advantage for this study. Although there is also a formalization of forcing in Lean 3 by Han and van Doorn [**flypitch**], development for

Lean 3 has already ended.

To use Gunther et al.'s formalization, we adopted the c.t.m. approach for our proof, as in their independence proof of CH. Specifically, we assumed the existence of a c.t.m. of ZF and constructed a model of ZF + ¬AC by forcing. This model is known as the basic Cohen model, which is a symmetric extension of assumed c.t.m. Our proof largely follows karagila's lecture note [**karagila**], with some parts also referencing Jech's books [**jech_set_theory**, **jech_AC**] as these resources align well with this approach.

The c.t.m. approach is a well-established method for relative consistency proofs in axiomatic set theory. The relative consistency of ¬AC with ZF means that if ZF is consistent, then ZF + ¬AC is also consistent. Assuming the consistency of ZF implies that a model of ZF exists, but strictly speaking, the existence of a c.t.m. cannot be derived from this assumption in ZF. However, as explained in section **??**, we can prove the relative consistency of ¬AC with ZF if we can construct a model of ZF + ¬AC from a c.t.m. of ZF. This kind of reasoning always arises in the c.t.m. approach, and ideally, we would like to formalize it as well, but this has not been achieved.

Related works

Paulson et al. formalized an extensive part of ZF set theory [**paulson_datatype_impl**, **paulson_reflection**, **paulson_AC_consistency**, **paulson_cardinal_AC**, **paulson_datatype**] , including cardinal arithmetic, relativization, the reflection theorem, features for handling inductive definitions, and the relative consistency of AC with ZF. The proof of the relative consistency was achieved by constructing constructing Gödel's constructible universe.

Building on these results, Gunther et al. formalized forcing and a proof of the independence of CH [**gunther_forcing**, **gunther_independence**] in Isabelle/ZF. In these formalizations, the countable transitive model (c.t.m.) approach was used, following Kunen's book [**kunen2011**].

In Lean, Han and van Doorn also formalized forcing and the independence of CH [**flypitch**] in Lean 3. using the Boolean-valued model approach, which is another approach to forcing. Additionally, in Lean 4, Holmes and Wilshaw formalized the complex parts of the consistency proof of Quine's New Foundations [**NF_consistency**], ensuring the correctness of the proof.

Repository

Our source code is available at:

Chapter 2

Preliminaries

2.1 Set-Theoretic Preliminaries

In this section, we introduce the concepts of set theory used in the formalization of this study. Our meta-theory is ZF, within which we explore ZF itself. Basically, our definition and theorems combine Kunen[**kunen2011**] and karagila's lecture note[**karagila**], adapted to the formalized form in Isabelle/ZF.

2.1.1 ZF Set Theory and the Axiom of Choice

We introduce the axioms of ZF set theory and the axiom of choice(AC). 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.

Definition 2.1.1. *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 2.1.2. 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. Additionally, we introduce the well-ordering theorem, as we treat AC in this form.

Definition 2.1.3. *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 2.1.4. *The axiom of choice is equivalent to the well-ordering theorem, which states that every set can be well-ordered.*

2.1.2 Forcing

Forcing is a tequnique used in proving relative consistency and Independence. We introduce basic concepts of forcing in the context of the 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 2.1.5. *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. $M^{\mathbb{P}} = \bigcup_{\alpha \in \mathrm{Ord}} M_\alpha^{\mathbb{P}}$

Where $\mathcal{P}^M$ denotes the power set operation in M. We often write a $\mathbb{P}$-name with a dot, e.g., $\dot{x}$. The least α such that $\dot{x} \in M_{\alpha+1}^{\mathbb{P}}$ is called the $\mathbb{P}$-*rank* of $\dot{x}$. This allows us to define functions and relations by recursion on $\mathbb{P}$-names.

Definition 2.1.6.

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

Definition 2.1.8. *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 with respect to the $\mathbb{P}$-rank of $\dot{x}$:*

$$\dot{x}^G = \{\dot{y}^G \mid \exists p \in G(\langle \dot{y}, p \rangle \in \dot{x})\}$$

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 2.1.9. *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 2.1.10. *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. The forcing relation is defined recursively on formulas in a forcing language. The forcing language is an extension of tha language of set theory by adding the elements of $M^{\mathbb{P}}$ as constants.

Definition 2.1.11. *We define the* forcing relation $\Vdash$ *for formulas in the forcing language and $p \in \mathbb{P}$ inductively* [1] *as follows:*

1. $p \Vdash \dot{x} = \dot{y} \Leftrightarrow \forall \dot{z} \in \mathrm{dom}(\dot{x}) \cup \mathrm{dom}(\dot{y})\, \forall q \leq_{\mathbb{P}} p\, (q \Vdash \dot{z} \in \dot{x} \leftrightarrow q \Vdash \dot{z} \in \dot{y})$
2. $p \Vdash \dot{x} \in \dot{y} \Leftrightarrow \forall q \leq_{\mathbb{P}} p\, \exists r \leq_{\mathbb{P}} q\, \exists s \in \mathbb{P}\, \exists \dot{z} \in M^{\mathbb{P}}\, (\langle \dot{z}, s \rangle \in \dot{y} \wedge r \leq_{\mathbb{P}} s \wedge r \Vdash \dot{x} = \dot{z})$
3. $p \Vdash \phi \wedge \psi \Leftrightarrow p \Vdash \phi \wedge p \Vdash \psi$
4. $p \Vdash \neg\phi \Leftrightarrow \forall q \leq_{\mathbb{P}} p\, \neg(q \Vdash \phi)$
5. $p \Vdash \exists x \phi(x) \Leftrightarrow \forall q \leq_{\mathbb{P}} p\, \exists r \leq_{\mathbb{P}} q\, \exists \dot{x} \in M^{\mathbb{P}}\, (r \Vdash \phi(\dot{x}))$

Theorem 2.1.12. *Let G be a generic filter on $\mathbb{P}$, φ be a formula, and $\dot{x} \in M^{\mathbb{P}}$, then*

$$M[G] \vDash \varphi(\dot{x}^G) \Leftrightarrow \exists p \in G\, (p \Vdash \varphi(\dot{x}))$$

Corollary 2.1.13. *Let $p \in \mathbb{P}$, φ be a formula and $\dot{x} \in M^{\mathbb{P}}$, then*

$$p \Vdash \varphi(\dot{x}) \Leftrightarrow \textit{for any generic filter } G \textit{ containing } p, M[G] \vDash \varphi(\dot{x}^G)$$

[1] Specifically, the forcing relation is first defined for atomic formulas $\dot{x} = \dot{y}$ and $\dot{x} \in \dot{y}$ by mutual recursion, inductively on the $\mathbb{P}$-rank of $\dot{x}$ and $\dot{y}$. Then, the definition is extended to all formulas in the forcing language by induction on the complexity of formulas.

2.1.3 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 2.1.14. *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 2.1.15. *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 2.1.16. *For every $\mathbb{P}$-name $\dot{x}$, let $\mathrm{sym}_{\mathcal{G}}(\dot{x}) = \{\pi \in \mathcal{G} \mid \pi\dot{x} = \dot{x}\}$. We say that $\mathbb{P}$-name $\dot{x}$ is* hereditarily $\mathcal{F}$-symmetric *if $\mathrm{sym}_{\mathcal{G}}(\dot{x}) \in \mathcal{F}$. $\mathrm{HS}_{\mathcal{F}}$ denotes the set of all hereditarily $\mathcal{F}$-symmetric $\mathbb{P}$-names.*

Definition 2.1.17. *Let G be a generic filter on $\mathbb{P}$. The set $\mathrm{HS}^G_{\mathcal{F}} = \{\dot{x}^G \mid \dot{x} \in \mathrm{HS}_{\mathcal{F}}\}$ is called a* symmetric extension *of M.*

Theorem 2.1.18. *Let G be a generic filter on $\mathbb{P}$. Then, the symmetric extension $\mathrm{HS}^G_{\mathcal{F}}$ is a c.t.m. of ZF and a substructure of $M[G]$.*

Definition 2.1.19. *The relativized forcing relation $\Vdash_{\mathrm{HS}}$ is defined as the forcing relation $\Vdash$ with $M^{\mathbb{P}}$ in its definition replaced by $\mathrm{HS}_{\mathcal{F}}$.*

The relation $\Vdash_{\mathrm{HS}}$ acts as the forcing relation for symmetric extensions.

Theorem 2.1.20. *Let G be a generic filter on $\mathbb{P}$, $\mathcal{N}$ be a symmetric extension generated by G, φ be a formula, and $\dot{x} \in \mathrm{HS}_{\mathcal{F}}$, then*

$$\mathcal{N} \vDash \varphi(\dot{x}) \Leftrightarrow \exists p \in G\ (p \Vdash_{\mathrm{HS}} \varphi(\dot{x}))$$

Corollary 2.1.21. *Let $p \in \mathbb{P}$, φ be a formula, and $\dot{x} \in \mathrm{HS}_{\mathcal{F}}$, then*

$$p \Vdash_{\mathrm{HS}} \varphi(\dot{x}) \Leftrightarrow \textit{for any generic filter } G \textit{ containing } p, \mathcal{N} \vDash \varphi(\dot{x}^G)$$

Where $\mathcal{N}$ is the symmetric extension generated by G.

The following lemmas also holds for the forcing relation $\Vdash$, but we only state them for $\Vdash_{\mathrm{HS}}$.

Lemma 2.1.22. *Let $p, q \in \mathbb{P}$, φ be a formula. If $q \leq_{\mathbb{P}} p$ and $p \Vdash_{\mathrm{HS}} \varphi$, then $q \Vdash_{\mathrm{HS}} \varphi$.*

Lemma 2.1.23. *Let π be an automorphism of $\mathbb{P}$, $\dot{x}_0, \ldots, \dot{x}_n \in \mathrm{HS}_{\mathcal{F}}$, and φ be a formula, then*

$$p \Vdash_{\mathrm{HS}} \varphi(\dot{x}_0, \ldots, \dot{x}_n) \Leftrightarrow \pi p \Vdash_{\mathrm{HS}} \varphi(\pi\dot{x}_0, \ldots, \pi\dot{x}_n)$$

2.1.4 The c.t.m. Approach

2.2 Outline for the Informal Proof

We outline an informal proof of the relative consistency of ¬AC with ZF which we will formalize in the next chapter. 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:

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

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

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

Let $\mathcal{F}$ be the set of all subgroups H of $\mathcal{G}$ such that there exists a finite $e \subseteq \omega$ with $\operatorname{fix}(e) \subseteq H$. 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 2.2.1. *$\mathcal{N}$ 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 subset of ω):

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

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 $n \in \omega$ with $a_n \in \operatorname{ran}(f)$, 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 a bijection π on ω 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 $q \leq_{\mathbb{P}} \pi p$

Note that some occurence of π in above conditions refer to the induced automorphism on $\mathbb{P}$ or $\mathbb{P}$-names.. 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. □

2.3 Isabelle/ZF and Formalization in Prior Work

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

Chapter 3

Formalization of the Proof

In this chapter, we present the formalization of the relative consistency proof of ¬AC with ZF in Isabelle/ZF. We follow the outline presented in section **??** and use the c.t.m. approach. We reuse the formalizations from prior work, such as first order formulas, satisfaction relation, utilities for inductive definitions by Paulson [**paulson_datatype_impl**, **paulson_reflection**, **paulson_AC_consistency**, **paulson_cardinal_AC**, **paulson_datatype**] and forcing relation by Gunther et al. [**gunther_forcing**].

3.1 Defining Symmetric Extensions

First, we define symmetric extensions in Isabelle/ZF. We define automorphisms on $\mathbb{P}$, the group of automorphisms $\mathcal{G}$, and the normal filter $\mathcal{F}$. Basically, we work within the locale .

1
2
3
4
5

theorem:

fixes
assumes≈⊨()
shows∃ .⊨∧¬(∀ ∈.∃ ∈.(##,,))
proof−

obtainwhere∈(,)**usingby**
theninterpret
unfolding
using
by
interpret
using
by

obtainwhere:()
using
by
theninterpret
unfolding
using
by

definewhere≡()

have:⊨
using
by

have∃ ∈.∀ ∈.¬(##,,)
apply(=()**in**)
apply(,)
apply()
using′
by
thenshowusingby
qed

3.2 Proving that Symmetric Extensions are Models of ZF

3.3 Defining the Basic Cohen Model

3.4 Proving that the Basic Cohen Model satisfies ¬AC

Chapter 4

Conclusion and Future Work

Acknowledgements