# $\neg$ ACの相対的無矛盾性のIsabelle/ZFによる形式的証明

東北大学情報科学研究科 住井・松田研究室
舟根大喜

September 16, 2024

# 参考文献


- Kenneth Kunen 著, 藤田 博司 訳 (2008)
  「集合論: 独立性証明への案内」
- Thomas Jech 著 (2008)「the Axiom of Choice」
- Thomas Jech 著 (2002)「Set Theory」
- Asaf Karagila 著 (2023)
  「Lecture Notes: Forcing & Symmetric Extensions」

# Isabelle/ZF について

# 定理証明支援系

- 数学的証明の形式化や、
  ソフトウェアの正しさの証明
  などに用いられるシステム
- プログラムを書くように定義・証明を記述する

# Isabelle

- 定理証明支援系の一つ
- 初版は 1986 年
  - Lawrence Paulson らによる
- 現在も開発・利用が続けられている

# Isabelle

- 論理体系「Pure」上で定理証明を行う
- 「Pure」上に他の論理体系が構築されている
  - Heigher-Order Logic
  - First-Order Logic
  - . . .

# Isabelle/ZF

- Isabelle 上で一階述語論理と ZF(C) 公理系を用いて証明を行うためのフレームワーク

# 集合論の形式化に関する
# 先行研究

# 先行研究 (Isabelle/ZF)

- 構成可能集合の形式化
  - Lawrence C. Paulson(2002)
  - AC が ZF 上相対的無矛盾であることの証明
- 強制法の形式化 & CH の ZFC 上の独立性証明
  - Emmanuel Gunther ら (2020,2022)
  - Kunen の強制法の章を形式化
  - c.t.m. の存在を仮定しその上の preorder を用いる

# 先行研究 (Lean)

- 強制法の形式化 & CH の ZFC 上の独立性証明
  - Jesse Michael Han, Floris van Doorn(2020)
  - flypitch プロジェクト
  - ブール値モデルを用いた証明
- Quine の NF の ZFC 上の相対的無矛盾性証明
  - Sky Wilshaw(2024)

# 本研究

# 本研究

**やったこと**

¬AC が ZF 上相対的無矛盾であることを
Isabelle/ZF で証明

## 背景

- コーエンは CH と AC が ZF から独立であることを示した
- CH の独立性は形式化されている
- AC も形式化したい

# 本研究のアプローチ

- Isabelle/ZF を用いる
  - ZF に関する定義・補題・糖衣構文が多い
- 証明の基本方針は Asaf Karagila の講義ノート
  - Lecture Notes: Forcing & Symmetric Extensions (2023)
  - c.t.m. と preorder を用いた証明
  - すでにある強制法の形式化と相性が良い

# 証明概略

# 証明概略

ZF の c.t.m.$M$ から出発し、ZF+¬AC のモデルを構成

- ある poset $\mathbb{P}$ による generic 拡大 $M[G]$ について
  symmetric extension と呼ばれる
  部分モデル $N \subseteq M[G]$ を構成
- $N$ は ZF を満たすが、整列可能定理を満たさない

# symmetric extensionの定義(1)

**定義 (自己同型)**

$(\mathbb{P}, \leq_{\mathbb{P}})$ は半順序で、最大元 $1_{\mathbb{P}}$ をもつとする
$\pi : \mathbb{P} \to \mathbb{P}$ が自己同型であるとは次を満たすこと

- $\pi$ は全単射
- $p, q \in \mathbb{P}$ に対して、$p \leq_{\mathbb{P}} q \Leftrightarrow \pi p \leq_{\mathbb{P}} \pi q$

$\pi$ は以下のように $M^{\mathbb{P}}$ 上の自己同型に拡張される

$$\pi \dot{x} = \{(\pi \dot{y}, \pi p) | (\dot{y}, p) \in \dot{x}\}$$

# symmetric extension の定義 (2)

**定義 (normal filter)**

$\mathcal{G}$ を $\mathbb{P}$ の自己同型群とする
$\mathcal{G}$ の部分群の族 $\mathcal{F}$ が normal filter であるとは次を満たすこと

- $H_1, H_2 \in \mathcal{F}$ に対して $H_1 \cap H_2 \in \mathcal{F}$
- super group をとる操作で閉じている
- $H \in \mathcal{F}, \pi \in \mathcal{G}$ に対して $\pi H \pi^{-1} \in \mathcal{F}$

# symmetric extension の定義 (3)

**定義 (hereditarily symmetric)**

$\mathcal{F}$ を $\mathcal{G}$ の normal filter とする

- $\dot{x} \in M^{\mathbb{P}}$ が $\mathcal{F}$-symmetric $\Leftrightarrow \{\pi \in \mathcal{G} | \pi\dot{x} = \dot{x}\} \in \mathcal{F}$
- $\dot{x}$ が hereditarily $\mathcal{F}$-symmetric とは以下を満たすこと
  - $\dot{x}$ は $\mathcal{F}$-symmetric
  - $\mathbf{dom}(\dot{x})$ の全ての要素は hereditarily $\mathcal{F}$-symmetric
- hereditarily $\mathcal{F}$-symmetric な $\dot{x}$ の集合を $\mathbf{HS}_{\mathcal{F}}$ とかく

# symmetric extension の定義 (4)

**定義 (symmetric extension)**

$\mathbb{P}$-generic filter $G$ に対し、

$\{\dot{x}_G | \dot{x} \in \mathbf{HS}_{\mathcal{F}}\}$ を symmetric extension という

# Isabelle/ZFによる形式化

# 成果

## 本研究で証明した主定理

```
theorem ZF_notAC_main_theorem :
  fixes M
  assumes "nat ≈ M" "M ⊨ ZF" "Transset(M)"
  shows "∃N. N ⊨ ZF ∧ ¬(∀A ∈ N. ∃R ∈ N. wellordered(##N, A, R))"
```

## 意味

$M$ を ZF の c.t.m. とする。このとき、ある $N$ があって、

$N$ は ZF を満たすが、整列可能定理を満たさない

# 作業工程

以下の工程に分けられる

- symmetric extension の定義
- ZF のモデルであることの証明
- 特定の symmetric extension の構成
- それが $\neg$AC を満たすことの証明

# 作業量

約 1 万 5 千行のコード　　　　　補題など (3 千行)

- symmetric extension の定義 (3 千行)
- ZF のモデルであることの証明 (5 千行)
- 特定の symmetric extension の構成 (2 千行)
- それが $\neg$AC を満たすことの証明 (2 千行)

# 苦労した点(1)

「自明なこと」の証明が非常に大変な場合がある
例えば…

- 定義した関数が「本当に関数であること」
- クラスに対し「本当にそれを表す論理式が存在すること」

# 苦労した点(2)

先行研究の強制関係の定義が少し特殊

# 苦労した点 (3)

ZF のモデルであることの証明

# まとめ

# まとめ