$\neg$ AC の相対的無矛盾性証明の Isabelle/ZF による形式化

東北大学 大学院情報科学研究科 住井・松田研究室
舟根大喜

October 14, 2024

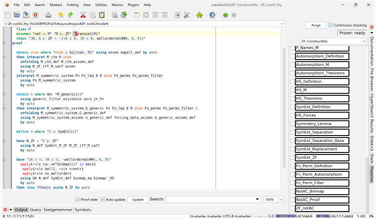
概要

aaaa

Isabelle/ZFについて

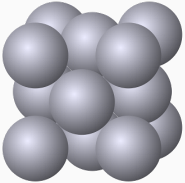
定理証明支援系

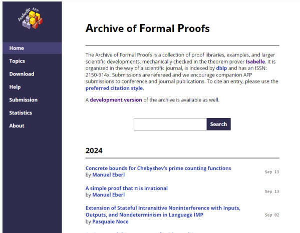
- 数学的証明の形式化や、ソフトウェアの正しさの証明などに用いられるシステム
- プログラムを書くように定義・証明を記述する
- Isabelle はその一種



Isabelle [Paulson 86]

- 実績
  - seL4 カーネルの形式検証 [Klein et al. 14]
  - ALEXANDRIA プロジェクト [Paulson 23]
  - ケプラー予想の形式証明 (の一部)[Hales et al. 15]
- Archive of Formal Proofs





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
  * Higher-Order Logic
  * First-Order Logic
  * . . .
- Isabelle/ZF · · ·
  一階述語論理と ZF(C) 公理系のフレームワーク

Isabelle/ZF における先行研究

- CH の ZFC 上の独立性証明 [Gunther et al. 20,22]
  - 強制法の形式化
  - CH の独立性証明
- AC の ZF 上の相対的無矛盾性証明 [Paulson 02]
  - 構成可能宇宙を形式化

▶ ¬AC の相対的無矛盾性証明は
形式化されていなかったので挑戦

本研究における Isabelle/ZF の利点

- 集合論に関する補題・糖衣構文が豊富
- Gunther らの強制法の形式化が使える
  - ZF の c.t.m. の存在を仮定している
    - c.t.m. $\cdots$ countable transitive model
    - この仮定により証明の形式化にギャップが生じる (後述)

※本研究では相性の良い Karagila(2023) の証明に従う

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 N を構成

- ある poset $\mathbb{P}$ による generic extension $M[G]$ の 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 ($\mathbb{P}$-name)

M を ZF の c.t.m. とする

- 最大元 $1_{\mathbb{P}}$ をもつ疑順序集合 $(\mathbb{P}, \leq_{\mathbb{P}})$ を poset という
- $M^{\mathbb{P}}_{\alpha}$ を再帰的に定義する
  - $M^{\mathbb{P}}_{0} = \emptyset$
  - $M^{\mathbb{P}}_{\alpha+1} = \mathcal{P}^{M}(M^{\mathbb{P}}_{\alpha} \times \mathbb{P})$
  - $M^{\mathbb{P}}_{\alpha} = \bigcup_{\beta<\alpha} M^{\mathbb{P}}_{\beta}$ (α は limit ordinal)
- $M^{\mathbb{P}} = \bigcup_{\alpha \in \mathrm{Ord}} M^{\mathbb{P}}_{\alpha}$ とし、$M^{\mathbb{P}}$ の元を $\mathbb{P}$-name という

symmetric extensionの定義(2)

定義(normal filter / 自己同型の拡張)

$\mathcal{G}$ 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 $\pi H \pi^{-1} \in \mathcal{F}$
- $\mathbb{P}$ の自己同型 π を次のように $M^{\mathbb{P}}$ 上の自己同型に拡張する

$$\pi \dot{x} = \{(\pi \dot{y}, \pi p) | (\dot{y}, p) \in \dot{x}\} \text{ for } \dot{x} \in M^{\mathbb{P}}$$

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

- symmetric extension は、ZF のモデルとなる

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. 自明なことの確認

「自明なこと」の確認が非常に大変な場合がある

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

苦労した点　1. 自明なことの確認

特に、「帰納的に定義された M 内の関数」の場合

- そもそも「M の元であること」の確認も必要
    - 仮定と ZF の公理からちゃんと構成できるか？

- このような関数を定義するための補題が 2 千行以上

先行研究の強制関係の定義

- よくある for all に対する強制関係の定義

$$p \Vdash \forall x \phi(x, \dot{x}_1, ..., \dot{x}_n) \Leftrightarrow \forall \dot{x} \in M^{\mathbb{P}} (p \Vdash \phi(\dot{x}, \dot{x}_1, ..., \dot{x}_n))$$

- 先行研究の定義

$$p \Vdash \forall x \phi(x, \dot{x}_1, ..., \dot{x}_n) \Leftrightarrow \forall x \in M (p \Vdash \phi(x, \dot{x}_1, ..., \dot{x}_n))$$

※この定義でうまくいくように他の部分も修正されている

苦労した点　2. 先行研究の定義

帰納法に $\mathbb{P}$-name でないものが混入する...

- $\mathrm{val}(G,\cdot)$ を M 上の関数として定義している

$$\mathrm{val}(G,x) := \{\mathrm{val}(G,y) | y \in \mathrm{dom}(x), \exists p \in G.(y,p) \in x\}$$

- $x \in M$ に対しある $\dot{z} \in M^{\mathbb{P}}$ があって $\mathrm{val}(x,G) = \mathrm{val}(\dot{z},G)$
  - この事実を形式化して一度は困難を解決
  - 最終的には別手法で「苦労した点 3.」と同時に解決

苦労した点　3.ZF のモデルであることの証明

symmetric extension が ZF のモデルであることの証明

命題

N が推移的かつ almost universal なクラスで、Δ_0-separation を満たすならば、N は ZF の内部モデルである

- 参考資料ではこの命題を証明に用いている
- 前提条件は証明できたが、「命題自体」が証明できなかった

苦労した点　3.ZF のモデルであることの証明

命題 (Collection Principle, Jech「Set Theory」6.5)

p をパラメータとして

$$\forall X \exists Y (\forall u \in X)[\exists v \phi(u, v, p) \to (\exists v \in Y)\phi(u, v, p)]$$

- 具体的にはこの命題の証明で行き詰った
- symmetric extension が、generic extension で defineble なクラスであることが証明できなかった

苦労した点　3.ZF のモデルであることの証明

代替手段

- HS に相対化した強制関係 $\Vdash_{\mathrm{HS}}$ を形式化
  - 参考資料に書かれている概念
  - 強制関係の定義の量化の動く範囲を HS に制限
  - $\Vdash_{\mathrm{HS}}$ は、symmetric extension に対し、generic extension に対する $\Vdash$ のように振舞う
- $\Vdash_{\mathrm{HS}}$ を用いて ZF のモデルであることを証明
  - 強制関係の帰納法が不要になり「苦労した点 2.」も解決

まとめ

まとめ

$\neg$AC の相対的無矛盾性証明を Isabelle/ZF で形式化

- ZF の c.t.m. から出発し、
  ZF+$\neg$AC をみたす symmetric extension を構成
- 厳密な意味での相対的無矛盾性の証明とはギャップがある
- 参考資料の通りにいかず試行錯誤した部分も
- 先行研究の改善点を発見？

ギャップ

- 既存の Isabelle/ZF での強制法の形式化は
  ZF の c.t.m. の存在を仮定したもの
- これを用いるため、
  本研究でも ZF の c.t.m. を仮定する
- ZF の c.t.m. の存在は、Con(ZF) から証明できない
- 本当の意味での相対的無矛盾性 Con(ZF) $\to$ Con(ZF+$\neg$AC)
  の証明とはギャップがある

ギャップ

c.t.m. を用いた議論の背景

ギャップ

- Boolean-valued model など
  別のアプローチをとれなかったのか？
- 強制法の形式化部分で
  作業量が増えてしまうので断念