$\neg$ 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

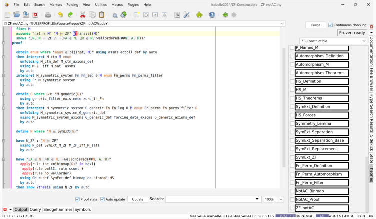
概要

aaaa

Isabelle/ZFについて

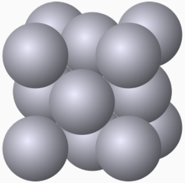
定理証明支援系

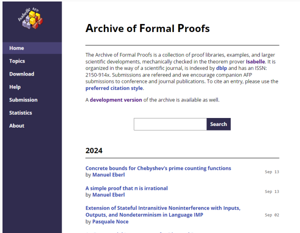
- 数学的証明の形式化や、ソフトウェアの正しさの証明などに用いられるシステム
- プログラムを書くように定義・証明を記述する
- Isabelle はその一種



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 (13K 行)
  - CH の独立性証明 (16K 行)
- 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 (12K 行)

▶ ¬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
- 強制法の形式化 [Gunther et al. 20] が使える
  - ZFのc.t.m.の存在を仮定している
    - c.t.m. ··· 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証明 [Karagila 23] 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
    - $N \vDash$「単射 $\omega \to A$ が存在しない無限集合 A が存在」
        - N ではこの A が整列できない
        - N では A は Dedekind 有限な無限集合

generic extension の定義 (1)

定義 (c.t.m.)

- M が推移的であるとは
  任意の $x \in M$, $y \in x$ に対して $y \in M$ であること
- M が ZF の c.t.m. であるとは
  M が可算で推移的な ZF のモデルであること

定義 (poset)

最大元 $1_{\mathbb{P}}$ をもつ疑順序集合 $(\mathbb{P}, \leq_{\mathbb{P}})$ を poset という

generic extension の定義 (2)

定義 ($\mathbb{P}$-name)

M を ZF の c.t.m., $\mathbb{P} \in M$ を poset とする

- $M^{\mathbb{P}}_\alpha$ 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
- $\mathbb{P}$-name は $\dot{x}, \dot{y}, \dot{z}, \ldots$ で表す

generic extensionの定義(3)

定義 (generic extension)

- $D \subset \mathbb{P}$ が dense:⇔ $p \in \mathbb{P}$ に対し $q \leq_{\mathbb{P}} p$ なる $q \in D$ が存在
- $G \subset \mathbb{P}$ が M-generic filter であるとは、以下を満たすこと
  - $p \in \mathbb{P}$, $q \in G$ に対し、$q \leq_{\mathbb{P}} p$ ならば $p \in G$
  - $p, q \in G$ に対し、$r \in G$ が存在して $r \leq_{\mathbb{P}} p, q$
  - $D \subset \mathbb{P}$ に対し、$D \in M$ かつ dense ならば $D \cap G \neq \emptyset$
- $\dot{x} \in M^{\mathbb{P}}$ に対し、$\dot{x}_G := \{\dot{y}_G \mid \dot{y} \in \mathbf{dom}(\dot{x}), \exists p \in G.(\dot{y}, p) \in \dot{x}\}$
- $M[G] := \{\dot{x}_G \mid \dot{x} \in M^{\mathbb{P}}\}$ を generic extension という

symmetric extension の定義 (1)

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 (2)

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 (3)

定義 (symmetric extension)

M-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
- $\mathbb{P}$, $\mathcal{G}$, $\mathcal{F}$ をうまく選ぶと $\neg$AC も満たす
    - 今回は $\mathbb{P} = (\omega \times \omega \to \{0, 1\}$ の有限部分関数全体)

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、あるモデル 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 ¬AC を満たすことの証明 (2 千行)

※ Isabelle/ZF での集合論の形式化の各先行研究と同じくらい

苦労した点 (1)　自明なことの確認が大変

- クラスに「それを表す論理式が存在すること」
- 定義した関数が「本当に関数であること」
  - 特に「帰納的に定義された M 内の関数」の場合
    - 仮定と ZF 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

苦労した点　1. 自明なことの確認

苦労した点 (2) 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 [Gunther et al. 20] の定義

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

※この定義でうまくいくように修正されている

▶ 帰納法に $\mathbb{P}$-name でないものが混入する...

解決策 (2)

先行研究 [Gunther et al. 20] の x_G の定義

$x \in M$ に対し

$$x_G := \{y_G \mid y \in \mathbf{dom}(x), \exists p \in G.(y, p) \in x\}$$

- $x \in M$ に対し、ある $\dot{z} \in M^{\mathbb{P}}$ があって $x_G = \dot{z}_G$
  - この事実を形式化
  - 帰納法中で x の代わりに $\dot{z}$ を使うことで一度は解決
  - 最終的には解決策 (3) で問題の帰納法自体不要に

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