

¬ 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 M2
舟根大喜

October 14, 2024

概要

やったこと

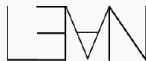
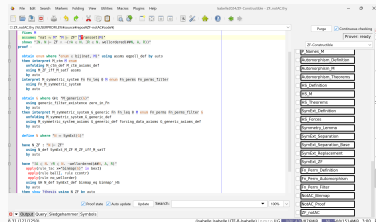
→AC の ZF 上の相対的無矛盾性証明 (の一部) を
Isabelle/ZF で形式化

- 定理証明支援系を用いて
数学の形式化をする試みが行われている
- 集合論の形式化はまだまだ未開拓なので貢献したい

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, Lean, Coq, ...



Isabelle [Paulson 86]

- 実績の例：

seL4 カーネルの形式検証 [Klein et al. 14]

* 130 万行の証明

- 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) ※ Lean にも形式化がある
 - 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)
- ▶ \neg AC の相対的無矛盾性証明は
形式化されていなかったもので挑戦

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 $ZF + \neg AC$ 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
 - * $N \models$ 「単射 $\omega \rightarrow A$ 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 (\mathbb{P} -name)

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

- $M_{\alpha}^{\mathbb{P}}$ を再帰的に定義する
 - * $M_0^{\mathbb{P}} = \emptyset$
 - * $M_{\alpha+1}^{\mathbb{P}} = \mathcal{P}^M(M_{\alpha}^{\mathbb{P}} \times \mathbb{P})$
 - * $M_{\alpha}^{\mathbb{P}} = \bigcup_{\beta < \alpha} M_{\beta}^{\mathbb{P}}$ (α は limit ordinal)
- $M^{\mathbb{P}} = \bigcup_{\alpha \in \text{Ord}} M_{\alpha}^{\mathbb{P}}$ とし、 $M^{\mathbb{P}}$ の元を \mathbb{P} -name という
- \mathbb{P} -name は $\dot{x}, \dot{y}, \dot{z}, \dots$ で表す

generic extension の定義 (2)

定義 (generic extension)

- $D \subset \mathbb{P}$ が dense: $\Leftrightarrow p \in \mathbb{P}$ 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、 $\dot{x}_G := \{\dot{y}_G \mid \dot{y} \in \text{dom}(\dot{x}), \exists p \in G. (\dot{y}, p) \in \dot{x}\}$
- $M[G] := \{\dot{x}_G \mid \dot{x} \in M^{\mathbb{P}}\}$ 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

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

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

symmetric extension の定義 (3)

定義 (symmetric extension)

M -generic filter G に対し、

$\{\dot{x}_G \mid \dot{x} \in \mathbf{HS}_{\mathcal{F}}\}$ 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 $\neg\text{AC}$ も満たす
 - * 今回は $\mathbb{P} = (\omega \times \omega \rightarrow \{0, 1\})$ の有限部分関数全体)

Isabelle/ZF による形式化

成果

本研究で形式証明した命題

```
theorem ZF_notAC_main_theorem :  
  fixes M  
  assumes "nat  $\approx$  M" "M  $\models$  ZF" "Transset(M)"  
  shows " $\exists N. N \models \text{ZF} \wedge \neg(\forall A \in N. \exists R \in N. \text{wellordered}(\#\#N, A, R))$ "
```

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 $\neg AC$ 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

苦勞した点 (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

苦勞した点 (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

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

- 先行研究 [Gunther et al. 20] の定義

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

※この定義でうまくいくように修正されている

- ▶ 強制関係の帰納法に \mathbb{P} -name 以外が混入する...

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_G が M 上の関数になっている
- $x \in M$ に対し、ある $\dot{z} \in M^{\mathbb{P}}$ があって $x_G = \dot{z}_G$
 - * この事実を形式化し帰納法中で x の代わりに \dot{z} を使う
 - * 最終的には解決策 (3) で問題の帰納法自体不要に

苦勞した点 (3) 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

- 参考文献 [Karagila 23] では、symmetric extension が ZF のモデルであることの証明にこの命題を使用
- Isabelle 上で、前提条件は証明できたが「命題自体」が証明できなかった

苦勞した点 (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

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

- 前頁の命題の証明中、この命題の証明で行き詰った
- symmetric extension が、generic extension で definable なクラスであることが証明できなかった
 - * 論理式を具体的に構成するのが大変すぎる？

解決策 (3)

- $\text{HS}_{\mathcal{F}}$ に相対化した強制関係 $\Vdash_{\text{HS}_{\mathcal{F}}}$ を形式化
 - * 参考資料 [Karagila 23] 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 $\text{HS}_{\mathcal{F}}$ に制限
 - * $\Vdash_{\text{HS}_{\mathcal{F}}}$ は、symmetric extension に対し、generic extension に対する \Vdash のように振舞う
- $\Vdash_{\text{HS}_{\mathcal{F}}}$ 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

考察

考察(1) c.t.m. アプローチについて

- 本研究で形式化したのは、
「ZF の c.t.m. が存在すれば $ZF + \neg AC$ のモデルが存在する」
 - * 強制法の形式化 [Gunther et al. 20] を使うため仮定
- 証明したいことは、 $\text{Con}(ZF) \rightarrow \text{Con}(ZF + \neg AC)$ だが、
ZF の c.t.m. の存在は、 $\text{Con}(ZF)$ から証明できない
 - * このギャップを埋める部分が形式化できていない
 - 紙の上では十分かもしれないが、
本当は形式化したい

形式化できていない部分

以下の形式化ができれば、ZF の c.t.m. の存在の仮定をなくせる

- 「任意の ZF の有限部分 Δ に対し、ZF の有限部分 Γ があって Γ の c.t.m. が存在すれば $\Delta + \neg AC$ のモデルが存在する」

- * 今回の形式化を修正すれば可能 (ほぼできている)

- 与えられた ZF の有限部分 Γ に対し、 Γ の c.t.m. が存在する

- * ZF モデルの中で ZF のモデルを考える必要がある？

- (労力的に) 形式化が厳しそう...

考察(2) メタ/対象レベル

今回、ZF のモデルの中の性質の証明が大変だった

- コード化された論理式を扱う必要があった
- メタレベルで成り立つことを
もう一度証明しなければいけないのもきつい
- ▶ メタ/対象レベルの証明を同時に書ける or
他方に変換できるような機能があると嬉しい
- ▶ 今回のテーマに限らず、数学基礎論の形式化には便利そう

まとめ

\neg AC の相対無矛盾性証明の一部を 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
- ctm の存在の仮定に関する形式化できていない部分がある
- 参考資料の通りにいかず試行錯誤した部分も
- メタ/対象レベルの形式的証明を「つなげる」機能がほしい