$\neg$ 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 M2
舟根大喜

November 22, 2024

概要

やったこと

¬AC の ZF 上の相対的無矛盾性証明を
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
- 公理的集合論の中でも強制法 (後述) を用いた議論の
  形式化はあまりないので貢献したい

用語

- 公理的集合論
  . . . 何が集合かを公理で厳密に定めて展開する集合論
- ZF . . . Zermelo-Fraenkel 公理系。最も一般的な公理系の一つ
- AC . . . 選択公理 (Axiom of Choice)
  任意の非空集合の族からそれぞれ１つの元を選ぶ関数が存在するという公理

用語

- 命題 φ が公理系 T 上で**相対的無矛盾**
  $\ldots T$ が無矛盾ならば公理系 $T + \varphi$ も無矛盾であること

- φ が T から**独立**
  $\ldots T$ から φ も $\neg\varphi$ も証明できないこと
  (T が無矛盾なら)φ と $\neg\varphi$ の T 上の相対的無矛盾性と同値

相対的無矛盾性を調べることで

公理系の (無矛盾性の) 強さを比較できる

用語

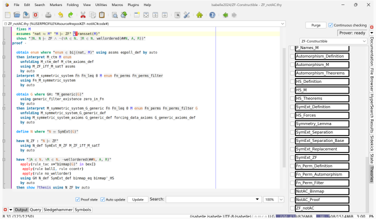
- **強制法** . . .
  集合論のモデルを拡張して新しいモデルを作る技法。
  M を強制法で拡張したモデルを M の generic extension と呼び、$M[G]$ とかく (ここで G は generic filter)

  generic extension 上で何が成り立つかは
  強制関係と呼ばれる関係 $\Vdash$ によって調べることができる

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
  - $\ldots$
- Isabelle/ZF $\cdots$
  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)

▶ ¬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+$\neg$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 は Basic Cohen Model と呼ばれるモデル
  - $N \models$「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

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 ≈ M" "M ⊨ ZF" "Transset(M)"
  shows "∃N. nat ≈ N ∧ N ⊨ ZF ∧ Transset(N) ∧ ¬(∀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 ZF の c.t.m. N があって、N は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 (3K 行)

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

※ Isabelle/ZF での集合論の形式化の各先行研究と同じくらい

困難だった点 (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

困難だった点 (2) 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/ZF 上で、N が $M[G]$ において「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 (2)

- $\mathbf{HS}_{\mathcal{F}}$ に相対化した強制関係 $\Vdash_{\mathbf{HS}_{\mathcal{F}}}$ 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 $\mathbf{HS}_{\mathcal{F}}$ に制限
  - $\Vdash_{\mathbf{HS}_{\mathcal{F}}}$ は、symmetric extension に対し、generic extension に対する $\Vdash$ のように振舞う
- $\Vdash_{\mathbf{HS}_{\mathcal{F}}}$ を用いて ZF のモデルであることを証明

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+¬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、Con(ZF)→Con(ZF+¬AC) だが、
ZF の c.t.m. の存在は、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
        - 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

¬AC の相対無矛盾性証明を Isabelle/ZF で形式化

- ZF の c.t.m. から出発し、
  ZF+¬AC をみたす symmetric extension を構成
- c.t.m. 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

参考文献(1)

- K. Kunen, Set Theory An Introduction To Independence Proofs, North-Holland, 1980
  日本語訳: 藤田 博司 訳, 集合論: 独立性証明への案内, 日本評論社, 2008
- T. Jech, Set Theory: The Third Millennium Edition, Springer, 2002
- T. Jech, The Axiom of Choice, Dover Publications, 2008
- A. Karagila, Lecture Notes: Forcing & Symmetric Extensions, 2023

参考文献(2)

- G. Klein et al., seL4: Formal Verification of an OS Kernel, 2014
- LC. Paulson, The Relative Consistency of the Axiom of Choice Mechanized Using Isabelle/ZF, 2003
- E. Gunther et al., Formalization of Forcing in Isabelle/ZF, 2020
- E. Gunther et al., The Independence of the Continuum Hypothesis in Isabelle/ZF, 2022