¬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

動機

- 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
- 公理的集合論の重要な技法である強制法 (後述)
  を用いた議論の形式化は限られている
- AC の相対的無矛盾性証明は形式化されている
  ので合わせて AC の独立性が形式化されたことに

用語

- **公理的集合論**：
  集合がみたすべき性質を公理として定めた集合論
- ZF：Zermelo-Fraenkel 公理系。一階述語論理上で形式化されたよく採用される公理系
- 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
  - 整列可能定理、Zorn の補題など同値な重要な命題がある

用語

- 命題φが公理系T上で**相対的無矛盾**：
  Tが無矛盾ならば公理系$T+\varphi$も無矛盾なこと

- φがTから**独立**：
  Tからφも$\neg\varphi$も証明できないこと

- φと$\neg\varphi$のT上の相対的無矛盾性を示すことで
  φがTから独立であることが証明できる
  (Tが無矛盾と仮定すれば)

用語

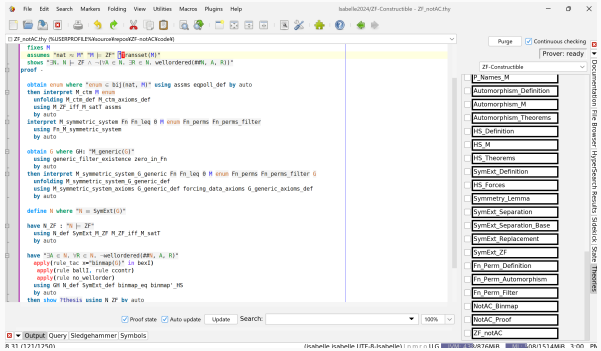
- **強制法**：
  集合論のモデルを拡張し新しいモデルを作る技法
  - M を強制法で拡張したモデルを
    M の generic extension と呼び $M[G]$ と書く
  - $M[G]$ は poset $\mathbb{P}$ と generic filter G に依存しており、$\mathbb{P}$ をうまく選ぶことで、ある程度 $M[G]$ で成り立つことを制御できる
  - $\mathbb{P}$ を決めたうえで、強制関係 $\Vdash$ によって、$M[G]$ で成り立つことを確認できる

※モデルが存在すれば無矛盾であるため、強制法でモデルを構成することで無矛盾性を証明できる

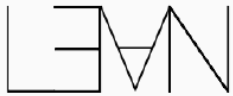
Isabelle/ZFについて

定理証明支援系

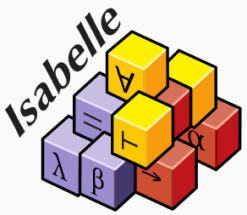
- 数学的証明の形式化や、
  ソフトウェアの正しさの証明
  などに用いられるシステム



- プログラムを書くように
  定義・証明を記述する



- Isabelle, Lean, Coq, . . .



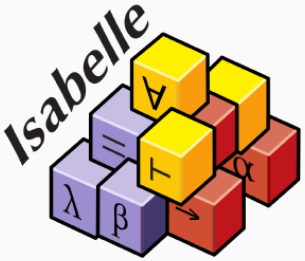
Isabelle [Paulson 86]

- 利用例：

  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

※本研究では Isabelle/ZF 上でさらに形式化された ZF を扱う (形式化された ZF のモデルとなっているような集合を構成する)

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] がすでにある
  - ZF の c.t.m. の存在を仮定している
    - c.t.m. : countable transitive model
  - Lean3 にも強制法の形式化があるが Lean3 は開発終了

※一階述語論理の形式化は [Paulson 02] を利用

証明概略

証明概略 [Karagila 23]

ZF の c.t.m. M から出発して
ZF+¬AC のモデル N を構成する

- N は First Cohen Model と呼ばれるモデル
  - generic extension の部分モデルである
    symmetric extension のひとつ
- 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

1. symmetric extension の構成法の定義
2. ZF のモデルであることの証明
3. First Cohen Model の構成
4. それが ¬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)

1. symmetric extension の定義 (3K 行)
2. ZF のモデルであることの証明 (5K 行)
3. First Cohen Model の構成 (2K 行)
4. 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

面倒だった点 自明なことの確認が大変

- クラスが本当にクラスであること
  - 実際に論理式を構成する必要がある
- 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」
    - 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 N がZFをみたすことの証明

Isabelle/ZF で構成した 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

- 書き下すのが面倒なだけでなく、非自明？
- これは [Karagila 23] で用いられている
  次の命題の証明に必要

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

解決策

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

```
lemma HS_truth_lemma:
  assumes
    "φ∈formula" "M_generic(G)"
  shows
     "⋀env. env∈list(HS) ⟹ arity(φ)≤length(env) ⟹
      (∃p∈G. p ⊩HS φ env) ⟷ SymExt(G), map(val(G),env) ⊨ φ"
```

```
lemma definition_of_forcing_HS:
  assumes
    "p∈P" "φ∈formula" "env∈list(HS)" "arity(φ)≤length(env)"
  shows
    "(p ⊩HS φ env) ⟷
     (∀G. M_generic(G) ∧ p∈G  ⟶  SymExt(G), map(val(G),env) ⊨ φ)"
```

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 $\rightarrow$ ZF+¬AC の c.t.m. が存在」
  - ZF の c.t.m. の存在は、強制法の形式化 [Gunther et al. 20] を使うため仮定
- 証明したいのは Con(ZF)$\rightarrow$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ことができるが、通常 c.t.m. アプローチの紙の上での証明では大まかな議論のみで省略される
    - この部分の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
- 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？
  - 形式化が難しい？

考察(2) メタ/対象レベル

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かった
- 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便利
- 今回のテーマに限らず
  数学基礎論の形式化でも有用

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
- 紙の上では省略される c.t.m. に関する議論の形式化が残っている
- 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