$\neg$AC の相対的無矛盾性の Isabelle/ZF による形式的証明

東北大学情報科学研究科 住井・松田研究室
舟根大喜

September 14, 2024

参考文献

- Kenneth Kunen 著, 藤田 博司 訳 (2008)
「集合論: 独立性証明への案内」
- Thomas Jech 著 (2008) 「the Axiom of Choice」
- Thomas Jech 著 (2002) 「Set Theory」
- Asaf Karagila 著 (2023)
「Lecture Notes: Forcing & Symmetric Extensions」

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

- 定理証明支援系の一つ
- 初版は1986年
  - Lawrence Paulson らによる
- 現在も開発・利用が続けられている

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
  - Heigher-Order Logic
  - First-Order Logic
  - …

Isabelle/ZF

- Isabelle 上で一階述語論理と ZF(C) 公理系を用いて証明を行うためのフレームワーク

集合論の形式化に関する先行研究

先行研究 (Isabelle/ZF)

- 構成可能宇宙 L の形式化
  - ⋆ Lawrence C. Paulson(2002)
  - ⋆ ZF 上 AC が相対的無矛盾であることの証明
- 強制法の形式化と CH の ZFC 上の独立性証明
  - ⋆ Emmanuel Gunther ら (2020,2022)
  - ⋆ Kunen の本のアプローチ

先行研究 (Lean)

- 強制法の形式化と CH の ZFC 上の独立性証明
  - ⋆ Jesse Michael Han, Floris van Doorn(2020)
  - ⋆ flypitch プロジェクト
  - ⋆ ブール値モデルを用いた証明
- Quine の NF の ZFC 上の相対的無矛盾性証明
  - ⋆ Sky Wilshaw(2024)

ZFC 公理系

- Zermelo と Fraenkel による、集合論の公理系
- 選択公理を除いたものを ZF 公理系と呼ぶ
- (等号を含む) 一階述語論理を用いる
- 述語記号は、$\in$ のみ
- 関数・定数記号は無い

略記

- 論理式の括弧は適宜省略する
- $\forall x \in y(\phi)$ は $\forall x(x \in y \to \phi)$ の略記
- $\exists x \in y(\phi)$ は $\exists x(x \in y \land \phi)$ の略記

略記

- 普段用いている$\emptyset, \subset, \bigcup$等の記号を含む論理式は$=$と$\in$のみを用いた論理式の略記とする
- 例：$x = \emptyset$は$\forall y \neg (y \in x)$と書ける
- 例：$x \subset y$は$\forall z (z \in x \to z \in y)$と書ける

ZFC 公理系

ZFC 公理系

ZFC 公理系

ZFC 公理系

ZFC 公理系

ZFC 公理系

ZFC 公理系

ZFC 公理系

ZFC 公理系

ZFC 公理系

ZFC 公理系の上で

- ZFC 公理系の上で、
(それを集合論の言葉に書き直すことで)
ほとんどの数学的対象を扱える

- 自然数、整数、有理数、実数、複素数、位相空間、
ベクトル空間 . . .

例：自然数

- 例えば、自然数は次のように定義できる
- $0 = \emptyset$
- $1 = \{0\} = \{\emptyset\}$
- $2 = \{0, 1\} = \{\emptyset, \{\emptyset\}\}$
- $3 = \{0, 1, 2\} = \{\emptyset, \{\emptyset\}, \{\emptyset, \{\emptyset\}\}\}$

例：自然数

- $n = \{0, 1, \ldots, n-1\}$ と定義する
- このとき、自然数の間の順序 $m < n$ を $m \in n$ で定義できる
- $\mathbb{N} = \{0, 1, 2, \ldots\}$ の存在を証明できる

選択公理

- 選択公理に関する疑問
  - 他の公理から矛盾しないのか？
  - 他の公理から導くことは不可能か？

- 選択公理が ZF の下で独立であることが証明され、どちらの疑問の答えも「Yes」と分かった

Isabelle/ZF

- 定理証明支援系 Isaeblle のバリエーションの一つ
- 他には Isabelle/HOL, Isabelle/FOL などがある
- Isabelle/ZF は、Isabelle 上で ZF 公理系を扱える
- 集合論的な糖衣構文が多数使える
- Isabelle/ZF で証明できる命題は、

独立性証明と研究について

研究の背景

- ZF 公理系における選択公理の独立性証明を Isabelle/ZF を用いて形式化したい

独立性

独立性の例

- $\mathcal{L} = \{\cdot, e\}$ とする (· は 2 変数関数記号、e は定数記号)
- $T =$(群の公理) とする
- このとき、可換性 $\forall x \forall y (x \cdot y = y \cdot x)$ は T において独立

独立性の例

- 実際、$(\mathbb{Z}, +, 0)$ は可換な群 (アーベル群) であり、
- n 次実正則行列全体の集合とその乗法からなる群 $(GL_n(\mathbb{R}), \cdot, I_n)$ は非可換な群である
- 可換な群と非可換な群が存在するため、
  群の公理から可換性を導くことも、
  非可換性を導くこともできない

独立性を証明するには？

研究の背景

- ZF 公理系における選択公理の独立性証明を Isabelle/ZF を用いて形式化したい
- ZF + AC (つまり ZFC) と、ZF + ¬AC が ともに無矛盾であることが Isabelle/ZF 上で示せればよい
- が、ゲーデルの不完全性定理より これは ZF 公理系からは証明できない

研究の背景

- そこで、「ZF が無矛盾である」という仮定のもとで、
  ZFC と ZF + ¬AC がともに無矛盾であることを示すことになる

- このように、公理系 T の無矛盾性を仮定したうえで、
  公理系 S の無矛盾性を示すことを

無矛盾性を証明するには？

ドルの完全性定理

モデル

- モデルとは、公理系 T を満たす数学的構造のこと

  (「数学的構造」や「満たす」は厳密に定義する必要がある)

- $(\mathbb{Z}, +, 0)$ は、群の公理+(可換性) のモデル
- $(GL_n(\mathbb{R}), \cdot, I_n)$ は、群の公理+($\neg$ 可換性) のモデル

研究の背景

- ZF 公理系における選択公理の独立性証明を Isabelle/ZF を用いて形式化したい
- 「ZF が無矛盾である」という仮定の下では、ZF のモデルの存在する
- このモデルを用いて、ZFC と ZF + ¬AC のモデルを構成することで、相対的無矛盾性を示すことが

研究の背景

- ZFC の ZF からの相対的無矛盾性証明は、
  ゲーデルの証明をもとに Lawrence C. Paulson により
  Isabelle 上ですでに形式化されている
- 構成可能宇宙 L を用いている
- https://www.cl.cam.ac.uk/techreports/UCAM-CL-TR-551.pdf

研究

- ZF からの ZF + ¬AC の相対的無矛盾性は、コーエンによって forcing を用いて証明された
- 定理証明支援系で形式化されていないと思われるので Isabelle/ZF 上で形式化したい
- 議論の中で forcing という数学的手法を用いるが、これはすでに Isabelle/ZF のパッケージがあるのでそれを用いる

Forcing パッケージ

- Emmanuel Gunther らによる
- https://arxiv.org/abs/2001.09715
- Kunen の教科書の内容を形式化している
- 連続体仮説の独立性証明も形式化されている

Forcingパッケージ

- このパッケージを用いると、こちらが指定した「ZFの可算推移$\in$モデル(以下c.t.m.)M」について、それに関するforcingを議論できる

c.t.m. を用いた議論の正当性

- 本来示したいことは、(ZF 上で)
  ZF のモデルが存在 $\Rightarrow$ ZF + $\neg$AC のモデルが存在

- Forcing パッケージを利用する場合は、
  ZF の c.t.m. を用意する必要がある

- だが、ZF のモデルが存在 $\Rightarrow$ ZF の c.t.m. が存在
  は (ZF 上で) 成立しない

c.t.m. を用いた議論の正当性

- この問題は回避できる
- (一般の S について)
  ZF の c.t.m M から ZF + S のモデルを構成できる
  を (ZF 上で) 示せるとき、その証明を修正して
  ZF のモデルが存在 $\Rightarrow$ ZF + S のモデルが存在
  を (ZF 上で) 示せる

c.t.m. を用いた議論の正当性

- つまり、
  ZF の c.t.m. から ZF + ¬AC のモデルを構成できる
  ことの (ZF 上での) 証明は、実質的に
  ZF のモデルが存在 ⇒ ZF + ¬AC のモデルが存在
  ことの (ZF 上での) 証明となる
- ただし、「実質的」でない具体的な証明を Isabelle 上で形式化するのは (労力的に) 難しいかもしれない

Forcing パッケージ

- c.t.m. を利用するのは、
  forcing により相対的無矛盾性証明を行う際の
  メジャーなアプローチのひとつ

- 形式化の側面から見ると、前述のような
  形式化が難しい (かもしれない) 議論が残ってしまう？

ZF + ¬ACのモデルの構成とIsabelle/Z

Forcing

- 集合論のモデル M に元を加えて、
  新たな集合論のモデル $M[G]$ を構成する技法
- この $M[G]$ を M のジェネリック拡大という
- $M \cup \{G\}$ のように単に元を加えただけでは、
  集合論のモデルにはならない
- G と M の元を用いた集合演算で

Forcingの例(ZFCの下で議論する)

連続体仮説,CH)

Forcingの例(ZFCの下で議論する)

- Forcingを用いて、ZFC+¬CHのモデルを構成できる
- Forcingで、ZFCのモデルMに単射$f : \aleph_2 \to \mathcal{P}(\mathbb{N})$を加えたZFCのモデル$M[G]$を構成できる
- この$M[G]$では、少なくとも$\aleph_2$個の$\mathbb{N}$の部分集合が

ZF+¬AC のモデルの構成

- ZF の c.t.m.M から出発して
  あるジェネリック拡大 $M[G]$ をとり、
  その部分モデル N であって ZF+¬AC が
  成り立つようなものを構成する

- この N は、M の symmetric extension と呼ばれる
  もの

- 基本的にこの資料の 10 章の議論に従っている

形式化の現在の進捗

- symmetric extension の定義が完了
- 証明のカギとなる補題 (symmetric lemma) の証明が完了
- 現在は symmetric extension が ZF の公理を満たすことを証明中 (まだ 0 個)
- その後、symmetric extension の中で議論して、

最近の進歩

- symmetric extension が ZF の公理を満たすことを証明中
- Δ_0-formula に関する分出公理図式の証明が完了
- Δ_0-分出公理と almost universal から分出公理を証明

  する流れがよくあるが、なんだかうまくいかない

形式化をしてみて

- 教科書の議論を丸写しにはできない
- パッケージの都合や作業量を考えて、
議論を修正するべきことがよくある
- 教科書等で自明だとされる議論の形式化が
非常に大変になることよくある
- 「ZF のモデルの中で〜ような集合を構成する」