7/3ゼミ

M2 舟根大喜

July 1, 2024

本日の内容

- 現在行っている研究について紹介
- 研究のテーマ：
  ZF+¬AC の ZF からの相対的無矛盾性証明を
  Isabelle/ZF を用いて形式化すること

1. ZFC 公理系と Isabelle/ZF
2. 独立性証明と研究について
3. ZF + ¬AC のモデルの構成と Isabelle/ZF による形式化

1. ZFC 公理系と Isabelle/ZF
2. 独立性証明と研究について
3. ZF + ¬AC のモデルの構成と Isabelle/ZF による形式化

公理的集合論

- 数学基礎論の一分野
- 何が集合であるかを公理で厳密に定義する集合論
- その公理系でなにが証明できるかを調べたり、公理系同士の関係を調べたりする
- 公理系は多数あるが、ZFC 公理系は最も一般的なものの一つ

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

定義

- **外延性公理**
  集合 x と y の要素たちが同じならば、x と y は等しい
- **空集合公理**
  空集合が存在する
- **対の公理**
  集合 x, y に対し、集合 $\{x, y\}$ が存在する

ZFC公理系

定義

- **外延性公理**
  $\forall x \forall y (\forall z (z \in x \leftrightarrow z \in y) \to x = y)$
- **空集合公理**
  $\exists x \forall y \neg (y \in x)$
- **対の公理**
  $\forall x \forall y \exists z \forall u (u \in z \leftrightarrow u = x \vee u = y)$

ZFC公理系

定義

- **和集合の公理**
  集合 x に対し、$\bigcup x$ が存在する
- **べき集合の公理**
  集合 x に対し、$\mathcal{P}(x)$ が存在する
- **無限公理**
  無限集合が存在する※

ZFC公理系

定義

- **和集合の公理**
  $\forall x \exists y \forall z (z \in y \leftrightarrow \exists u (u \in x \land z \in u))$
- **べき集合の公理**
  $\forall x \exists y \forall z (z \in y \leftrightarrow \forall u (u \in z \rightarrow u \in x))$
- **無限公理**
  $\exists x (\emptyset \in x \land \forall y (y \in x \rightarrow y \cup \{y\} \in x))$

ZFC公理系

定義

- **正則性公理**

  $x_0 \ni x_1 \ni x_2 \ni \ldots$ という集合の無限列は存在しない

ZFC公理系

定義

- **正則性公理**

  $\forall x(x \neq \emptyset \to \exists y(y \in x \land x \cap y = \emptyset))$

ZFC公理系

定義

- **分出公理図式**

  $x, v_1, \ldots, v_n$ を集合とし、
  $\phi(u, v_1, \ldots, v_n)$ を論理式とするとき、
  集合$\{\, u \in x | \phi(u, v_1, \ldots, v_n) \,\}$ が存在する

ZFC公理系

定義

- **分出公理図式**
  $\forall x \forall v_1 \ldots \forall v_n \exists y \forall u (u \in y \leftrightarrow u \in x \wedge \phi(u, v_1, \ldots, v_n))$

ZF公理系は各論理式ϕに対してこの形の公理を持つ。

分出公理は、空集合公理と、後述する置換公理から導けるので省かれることもある

ZFC公理系

定義

- **置換公理図式**
  F をクラス関数、x を集合とするとき、
  集合 $\{F(u) | u \in x\}$ が存在する

ZFC公理系

定義

- **選択公理**
  非空集合の族 $\{x_i\}_{i \in I}$ に対し、
  $\prod_{i \in I} x_i \neq \emptyset$ が成り立つ

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、
  ZF 公理系で証明できる命題だと思うことができる

1. ZFC 公理系と Isabelle/ZF
2. 独立性証明と研究について
3. ZF + ¬AC のモデルの構成と Isabelle/ZF による形式化

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

定義

T を言語 $\mathcal{L}$ 上の公理系とする

- T から命題 ϕ も $\neg\phi$ も証明できないとき、
  ϕ は T において独立であるという
- T において、ある命題 ϕ とその否定 $\neg\phi$ が
  ともに証明できるとき、T は矛盾するという
- そのような ϕ がないとき、T は無矛盾であるという

(「証明できる」は厳密に定義する必要がある)

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？

命題

任意の公理系 T, 命題 ϕ に対し、以下は同値

- T において ϕ を証明できない
- $T + \neg\phi$ は無矛盾

従って、$T + \phi$ と $T + \neg\phi$ がともに無矛盾であれば、
ϕ は T において独立である

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 (従って、Isabelle/ZF 上でも証明できないはずである)

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相対的無矛盾性証明という

無矛盾性を証明するには？

ゲーデルの完全性定理

任意の公理系 T に対し、以下は同値

- T は無矛盾
- T はモデルを持つ

従って、$T+\phi$ と $T+\neg\phi$ それぞれのモデルを構成できれば、ϕ は T において独立である

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+(¬ 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できる

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 + ¬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？

1. ZFC 公理系と Isabelle/ZF
2. 独立性証明と研究について
3. ZF + ¬AC のモデルの構成と Isabelle/ZF による形式化

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
  閉じていなければならない

Forcingの例(ZFCの下で議論する)

定義 (連続体仮説,CH)

$|\mathcal{P}(\mathbb{N})| = \aleph_1$ である
ただし、$\aleph_n$ は、n番目に大きい無限濃度 (無限基数) で
特に $\aleph_0 = |\mathbb{N}|$ である

- CHはZFCにおいて独立である
- ゲーデルがZFC + CHの無矛盾性を、
  コーエンがZFC + ¬CHの無矛盾性を示した

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$\mathbb{N}$の部分集合が存在するから、$|\mathcal{P}(\mathbb{N})| > \aleph_1$であり、よって¬CH

(いろいろ不正確な記述あり)

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
  https://karagila.org/files/Forcing-2023.pdf

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、AC が成り立たないことを示す

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
- この問題の回避策を考えた

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」
  といった議論が特に大変 (超限再帰的な構成だとさらに)