計算理論　第 8 回
前半のまとめ

岡本 吉央
okamotoy@uec.ac.jp

電気通信大学

2020 年 11 月 26 日

最終更新：2020 年 11 月 28 日　14:35

概要

この講義の主題

計算理論 (Theory of Computation)

- 計算可能性理論　(Computability Theory)
- 計算複雑性理論 (計算量理論)　(Complexity Theory)

講義の進め方

- 前半：計算可能性理論 (担当：岡本)
- 後半：計算複雑性理論 (担当：垂井先生)

スケジュール 前半 (予定)

1. 計算とは何か？　(10/1)
2. 計算モデル　(10/8)
3. チャーチ・チューリングの定立　(10/15)
- ⋆ 休み (体育祭)　(10/22)
4. コード化　(10/29)
5. 計算可能性　(11/5)
6. 停止性問題　(11/12)
7. 再帰定理　(11/19)
8. 前半のまとめ　(11/26)

注意：予定の変更もありうる

目次

計算理論 ≠ 計算機理論

重要ポイント

「計算理論」は「計算機の理論」ではない

注：「Computer Science」の訳語として「計算機科学」，
「Theoretical Computer Science」の訳語として「理論計算機科学」を
充てることがあるけれども，それらが「計算機の科学」であると
誤解されることがあるため，この訳語を嫌う専門家もいる

疑問

では，「計算理論」は何を扱うのか？

⇝ つまり，「計算機」ではない「計算」とは何なのか？

何が計算を行なうのか？

- 計算機は計算を行なう
- 人間は計算を行なう
- 生命は計算を行なう
- 電気回路・電子回路は計算を行なう
- ビリヤードは計算を行なう
- ゲームは計算を行なう
- ...

計算を理解するために必要な理論

つまり

- 計算機だけが計算を行なうわけではない
- 様々な対象が計算を行なえる

求められるのは？

- 結局「計算」とは何なのか？ はっきりさせること
- 「計算」について抽象的に語るための理論体系を作ること

⇝ 計算理論

計算が行なっていること

計算が行なっていること (直感的な説明)

- 何か入力 (初期状態) が与えられる
- 入力 (初期状態) が時間とともに処理される (変化する)
- 最終的に，出力 (終了状態) が得られる

時間とともに処理される (変化する) = 計算する

入力 ⟶ 処理 ⟶ 出力

アルゴリズムとは？ (直感的な定義)

処理の手順のこと

「どのような手順が許されるのか」ということは重要

「計算」と「計算機」の理解 — カリキュラムにおける位置づけ

抽象度	講義名
高	プログラミング言語論，計算理論
	アルゴリズム論第一，アルゴリズム論第二
	形式言語理論，プログラミング通論
	オペレーティング・システム論，言語処理系論
	計算機通論，コンピュータ設計論
	論理設計学
低	電気・電子回路

位置づけに異論はあるかもしれない

講義『計算理論』の概要

よく議論される計算モデル

- 「万能」な計算モデル　(← 普通の「計算理論」の対象)
- 「具体的」な計算モデル

- 「万能」= 万能関数が計算できる
- 「万能 $\neq$ なんでもできる」なので，注意

「万能」な計算モデルに対する 2 つの主な理論

計算可能性理論

- 「万能」な計算モデルで原理的にできることは何か？
- 「万能」な計算モデルで原理的にできないことは何か？

計算複雑性理論 (計算量理論)

- 「万能」な計算モデルで実用的にできることは何か？
- 「万能」な計算モデルで実用的にできないことは何か？

計算可能性理論 (Computability Theory)

計算可能性理論

- 「万能」な計算モデルで原理的にできることは何か？
- 「万能」な計算モデルで原理的にできないことは何か？

ここで「原理的にできる」とは？

- アルゴリズムが存在する

重要な事実

原理的にできないことが存在する

前半の目標

- 何が原理的にできないのか，理解する
- なぜ原理的にできないのか，理解する

計算複雑性理論 (計算量理論，computational complexity theory) (1)

計算複雑性理論 (計算量理論)

- 「万能」な計算モデルで実用的にできることは何か？
- 「万能」な計算モデルで実用的にできないことは何か？

ここで「実用的にできる」とは？

- 文脈に依存する ($\rightsquigarrow$ 計算における資源の概念)
- 多くの場合,「多項式時間で」できる

後半の目標 (1)

- 計算における「資源」の概念を理解する

計算複雑性理論 (計算量理論，computational complexity theory) (2)

計算複雑性理論 (計算量理論)

- 「万能」な計算モデルで実用的にできることは何か？
- 「万能」な計算モデルで実用的にできないことは何か？

重要な事実

- 原理的にできるが，実用的にできないことが存在する
- よく現れる問題が，実用的に解けるかどうか分かっていない
  $\rightsquigarrow$ P vs NP 問題 (P $\neq$ NP 問題，P =? NP 問題)

後半の目標 (2)

- 「P vs NP 問題」とは何なのか，理解する

前半のまとめ

計算モデルとして「WHILE プログラム」を採用

- WHILE プログラムは部分関数を計算する

WHILE プログラムを通して，次を理解

- 計算の模倣 (シミュレーション)： GOTO プログラムと等価
- コード化： プログラムを入力できる
- 万能計算の実現： インタプリタの設計
- 計算不可能問題の存在： 対角線論法
- 多くの重要な問題の計算不可能性： 停止性問題と帰着
- 再帰の実現： 再帰定理

重要な観点

このような理論は，チューリング機械やラムダ計算など，
他の「万能」な計算モデルでも展開できる

目次

世の中の「ほとんど」の問題は計算不可能

次の定理の証明を思い出してみる

定理：計算不可能な部分関数

計算不可能な部分関数 $f\colon \mathbb{N} \nrightarrow \mathbb{N}$ が存在する

証明は 対角線論法 を用いて行った

カントールの対角線論法

集合 A, B に対して

- A が B よりも「圧倒的に大きい」ことを証明する技法

$\therefore$ 部分関数の集合は計算可能部分関数の集合よりも「圧倒的に大きい」

- つまり,「ほとんど」の部分関数は計算不可能

具体的な計算不可能問題

授業の中で扱った 具体的な 計算不可能問題

- 停止性問題
- その他，プログラムの性質を問う問題

いまから 紹介すること

その他の 具体的な 計算不可能問題

- ヒルベルトの第 10 問題に関する問題
- コラッツ予想に関する問題
- 行列の乗算に関する問題

ヒルベルトの第 10 問題：例

例：x, y, z を変数とする次の方程式は整数解を持つか？

$$x^2 - xy + 2yz^3 + 2 = 0$$

解答：持つ (例えば，$x = 1, y = 1, z = -1$ が整数解)

例：x, y, z を変数とする次の方程式は整数解を持つか？

$$x^2 - 2xy - 6xyz + x^2z^2 + 10y^2 + 1 = 0$$

解答：持たない (例えば，左辺 $= (x - y)^2 + (3y - xz)^2 + 1 > 0$)

ヒルベルトの第 10 問題

ヒルベルトの第 10 問題

与えられた整数係数多変数代数方程式 $p(x_1, x_2, \ldots, x_n) = 0$ が整数解を持つか？　　(ディオファントス方程式)

$$p(x_1, x_2, \ldots, x_n) = \sum_{i_1=0}^{d} \sum_{i_2=0}^{d} \cdots \sum_{i_n=0}^{d} a_{i_1,i_2,\ldots,i_n} x_1^{i_1} \cdots x_n^{i_n}$$

入力は n, d, $a_{i_1,i_2,\ldots,i_n}$ $(i_1, i_2, \ldots, i_n \in \{0, \ldots, d\})$

注

整数は適当な方法で自然数にコード化する

WHILE 計算可能性を考えるときは，
「整数解を持つか」という問題を関数 f を計算する問題と見なす

$$f(\text{入力}) = \begin{cases} 1 & (\text{入力に対して } p \text{ が整数解を持つ}) \\ 0 & (\text{入力に対して } p \text{ が整数解を持たない}) \end{cases}$$

ヒルベルトの第 10 問題の計算不可能性

定理

ヒルベルトの第 10 問題は計算不可能
(つまり，ヒルベルトの第 10 問題を解くアルゴリズムは存在しない)

これは深い定理で，証明を構築した研究者の名前の頭文字をとって MRDP 定理と呼ばれることがある (証明されたのは 1970 年)
(Matiyasevich, Robinson, Davis, Putnam)

コラッツ予想

次の数列 $\{a_n\}_{n \geq 0}$ を考える

$$a_0 = c \geq 1,$$
$$a_n = \begin{cases} a_{n-1}/2 & (a_{n-1} \equiv 0 \pmod 2 \text{ のとき}) \\ 3a_{n-1} + 1 & (a_{n-1} \equiv 1 \pmod 2 \text{ のとき}) \end{cases} \quad (n \geq 1)$$

未解決問題 (コラッツ予想)

任意の整数 $c \geq 1$ に対して，ある k が存在して $a_k = 1$ となる

- $c \leq 2^{68}$ のときは正しいと分かっている　　(Barina '20)
  http://www.ericr.nl/wondrous/
- Erdős said "Mathematics is not yet ready for such problems."

コラッツ予想に関連する問題

「コラッツ予想が難しい」ことを計算理論的に考察するために，
コラッツ予想に関連する次の数列 $\{a_n\}_{n \geq 0}$ を考える

$$a_0 = c \geq 1,$$
$$a_n = \begin{cases} \alpha_0 a_{n-1} + \beta_0 & (a_{n-1} \equiv 0 \pmod P \text{ のとき}) \\ \alpha_1 a_{n-1} + \beta_1 & (a_{n-1} \equiv 1 \pmod P \text{ のとき}) \\ \vdots & \\ \alpha_{P-1} a_{n-1} + \beta_{P-1} & (a_{n-1} \equiv P - 1 \pmod P \text{ のとき}) \end{cases} \quad (n \geq 1)$$

ただし，α_i, β_i $(i \in \{0, 1, \ldots, P-1\})$ は数列のすべての項が整数になるものとする

- コラッツ予想に現れる数列は
  $P = 2$，$\alpha_0 = 1/2$，$\beta_0 = 0$，$\alpha_1 = 3$，$\beta_1 = 1$ として得られる

コラッツ予想に関連する問題 (続き)

「コラッツ予想が難しい」ことを計算理論的に考察するために，
コラッツ予想に関連する次の数列 $\{a_n\}_{n \geq 0}$ を考える

$$a_0 = c \geq 1,$$
$$a_n = \begin{cases} \alpha_0 a_{n-1} + \beta_0 & (a_{n-1} \equiv 0 \pmod P \text{ のとき}) \\ \alpha_1 a_{n-1} + \beta_1 & (a_{n-1} \equiv 1 \pmod P \text{ のとき}) \\ \vdots & \\ \alpha_{P-1} a_{n-1} + \beta_{P-1} & (a_{n-1} \equiv P - 1 \pmod P \text{ のとき}) \end{cases} \quad (n \geq 1)$$

一般化コラッツ問題

$c, P, \alpha_0, \ldots, \alpha_{P-1}, \beta_0, \ldots, \beta_{P-1}$ が与えられたとき，
上の数列 $\{a_n\}_{n \geq 0}$ において，ある k が存在して $a_k = 1$ となるか？

この問題を解こうと思ったら，アルゴリズムを作りたくなるかもしれないが $\cdots$

コラッツ予想に関連する問題の計算不可能性

定理 (Conway '72)

一般化コラッツ問題は計算不可能

つまり，一般化コラッツ問題を解くアルゴリズム (プログラム) を作ることで，コラッツ予想を解くことは (どう頑張っても) できない

注意

- コラッツ予想そのものをアルゴリズム的に解けないとはいっていない
- 次の 0 変数関数は計算可能！

$$f() = \begin{cases} 1 & (\text{コラッツ予想は正しい}) \\ 0 & (\text{コラッツ予想は正しくない}) \end{cases}$$

行列の乗算に関する問題 (1)

次のような行列の集合を考える

$$\left\{ M_1 = \begin{pmatrix} 1 & -1 \\ -1 & 1 \end{pmatrix}, \quad M_2 = \begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix}, \quad M_3 = \begin{pmatrix} 2 & 2 \\ 3 & 4 \end{pmatrix} \right\}$$

これらを使って，零行列 O を作ることができる

$$M_1 M_2 M_1 M_2 = O$$

行列の乗算に関する問題 (2)

次のような行列の集合を考える

$$\left\{ M_1 = \begin{pmatrix} 1 & 0 \\ -1 & 1 \end{pmatrix}, \quad M_2 = \begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix}, \quad M_3 = \begin{pmatrix} 2 & 2 \\ 3 & 4 \end{pmatrix} \right\}$$

これらを掛け合わせることで，零行列 O を作れない (なぜ？)

行列のモータリティ問題

行列のモータリティ問題

d 次正方整数行列が m 個与えられたとき $(M_1, M_2, \ldots, M_m)$
これらを掛け合わせることで，零行列を作れるか？

知られていること

- $d = 3$ であっても，計算不可能 (Paterson '70)
- $d = 3$, $m = 7$ であっても，計算不可能 (Halava, Harju, Hirvensalo '07)
- $d = 13$, $m = 3$ であっても，計算不可能 (Halava, Hirvensalo '07)
- $d = 21$, $m = 2$ であっても，計算不可能 (Halava, Harju, Hirvensalo '07)
- $d = 2$, $m = 2$ のときは，計算可能 (Bournez, Branicky '02)

未解決問題

$d = 2$ のとき，行列のモータリティ問題は計算不可能か？