期末試験のお知らせ

1月27日(金) 13:30 ～ 14:30
(60分試験)

1-101教室 (ここじゃない)

- 最終回(今日)の講義内容まで
- 学生証必携

レポート提出について

- 期日：**2月6日(月)20時頃まで**
- 内容：
  配布プリントのレポート問題の例のような内容
  及び授業に関連する内容で、
  授業内容の理解または発展的な取組みを
  アピールできるようなもの
- 提出方法：
  ⋆ 4-574 室扉のレポートポスト
  ⋆ 電子メイル

本講義最後の話題は、

計算量

について

問題の難しさを如何に計るか？

Church-Turing の提唱 (再掲)

「全てのアルゴリズム (計算手順) は、
チューリングマシンで実装できる」

(アルゴリズムと呼べるのは
チューリングマシンで実装できるものだけ)

$\cdots$ **「アルゴリズム」の定式化**

計算量 (complexity)

- **時間計算量**：計算に掛かるステップ数
  (TM での計算の遷移の回数)
- **空間計算量**：計算に必要なメモリ量
  (TM での計算で使うテープの区画数)

通常は、決まった桁数の四則演算 1 回を
1 ステップと数えることが多い

入力データ長 n に対する
増加のオーダー (Landau の O-記号) で表す

計算量 (complexity)

問題を解くアルゴリズムによって決まる

$\cdots$ アルゴリズムの計算量

$\longrightarrow$ アルゴリズムの効率 の評価

問題の計算量：

その問題を解くアルゴリズムの計算量の下限

最も効率良く解くと、どれ位で解けるか

= どうしてもどれ位必要か

= どれ位難しい問題か

$\longrightarrow$ 問題の難しさ の評価

重要な難しさのクラス

多項式時間 P $\cdots \exists k : O(n^k)$

- **"事実上計算可能" な難しさ**
- **計算モデルの変更に関して頑健 (複数テープ TM などに変更しても不変)**

「しらみつぶし」が入ると大体 $O(2^n)$ **程度以上**

(指数時間 EXP $\cdots \exists k : O(2^{n^k})$**)**

"事実上計算不可能"

非決定性計算モデルでの計算量

計算量にも “非決定性” の概念がある

あてずっぽうを許して、
うまくいけばどの位で解けるか
= 答を知って、その検証にどの位かかるか

非決定性多項式時間 (NP):
非決定性の計算モデルで多項式時間で解ける

例: 素因数分解は NP
··· 素因数を知っていれば割算するだけ

非決定性計算モデルでの計算量

計算量にも “非決定性” の概念がある

あてずっぽうを許して、
うまくいけばどの位で解けるか
＝ 答を知って、その検証にどの位かかるか

非決定性多項式時間 (NP):
非決定性の計算モデルで多項式時間で解ける

例: 素因数分解は NP
… 素因数を知っていれば割算するだけ

非決定性計算モデルでの計算量

計算量にも “非決定性” の概念がある

あてずっぽうを許して、
うまくいけばどの位で解けるか
＝ 答を知って、その検証にどの位かかるか

非決定性多項式時間 (NP):
非決定性の計算モデルで多項式時間で解ける

例: 素因数分解は NP
$\cdots$ 素因数を知っていれば割算するだけ

非決定性計算モデルでの計算量

$$\mathbf{P} \subset \mathbf{NP} \subset \mathbf{EXP}$$

未解決問題 (P vs NP Problem)

$$\mathbf{P} = \mathbf{NP}$$

であるか否か？

“The Millennium Problems”
の 7 つの問題のうちの 1 つ
(賞金 $1M)

非決定性計算モデルでの計算量

$$\mathsf{P} \subset \mathsf{NP} \subset \mathsf{EXP}$$

未解決問題 (P vs NP Problem)

$$\mathsf{P} = \mathsf{NP}$$

であるか否か？

“The Millennium Problems”
の 7 つの問題のうちの 1 つ
(賞金 $1M)

非決定性計算モデルでの計算量

$$\mathsf{P} \subset \mathsf{NP} \subset \mathsf{EXP}$$

未解決問題 (P vs NP Problem)

$$\mathsf{P} = \mathsf{NP}$$

であるか否か？

"The Millennium Problems"
の 7 つの問題のうちの 1 つ
(賞金 $1M)

多項式時間帰着可能性

問題 B が問題 A に多項式時間帰着可能
$\overset{\leftarrow}{\Longleftrightarrow} \exists f : \Sigma^* \longrightarrow \Sigma^*$ **:**

- f **: 多項式時間で計算可能**
  (多項式時間で計算する TM が存在)
- $w \in B \Longleftrightarrow f(w) \in A$

- **問題 B が問題 A に多項式時間帰着可能のとき、**
  $\mathbf{A} \in \mathbf{P} \Longrightarrow \mathbf{B} \in \mathbf{P}$

多項式時間帰着可能性

問題 B が問題 A に多項式時間帰着可能
$\overset{\leftarrow}{\Longleftrightarrow} \exists f : \Sigma^* \longrightarrow \Sigma^*$ **:**

- f **: 多項式時間で計算可能**
  (多項式時間で計算する TM が存在)
- $w \in B \Longleftrightarrow f(w) \in A$

- **問題 B が問題 A に多項式時間帰着可能のとき、**
  $\mathbf{A} \in \mathbf{P} \Longrightarrow \mathbf{B} \in \mathbf{P}$

NP 完全・NP 困難

- 問題 A が **NP 困難** (**NP-hard**)
  $\overset{\leftarrow}{\Longleftrightarrow}$ 全ての NP 問題 B が
  問題 A に多項式時間帰着可能
- 問題 A が **NP 完全** (**NP-complete**)
  $\overset{\leftarrow}{\Longleftrightarrow}$ 問題 A が NP かつ NP 困難

或る NP 完全な問題 A が P $\Longleftrightarrow$ P = NP

NP 完全・NP 困難

- 問題 A が NP 困難 (NP-hard)
  $\stackrel{\leftarrow}{\Longleftrightarrow}$ 全ての NP 問題 B が
  問題 A に多項式時間帰着可能
- 問題 A が NP 完全 (NP-complete)
  $\stackrel{\leftarrow}{\Longleftrightarrow}$ 問題 A が NP かつ NP 困難

或る NP 完全な問題 A が P $\Longleftrightarrow$ P $=$ NP

充足可能性問題 (SAT)

NOT, OR, AND からなる論理式

$$f(A_1, \ldots, A_n)$$ に対し、

$f(a_1, \ldots, a_n) = 1$ となる変数 A_i の真理値の組

$$(a_1, \ldots, a_n) \in \{0, 1\}^n$$

が存在するか？

定理 (Cook-Levin)

SAT は NP 完全

充足可能性問題 (SAT)

NOT, OR, AND からなる論理式

$$f(A_1, \ldots, A_n)$$ に対し、

$f(a_1, \ldots, a_n) = 1$ となる変数 A_i の真理値の組

$$(a_1, \ldots, a_n) \in \{0, 1\}^n$$

が存在するか？

定理 (Cook-Levin)

SAT は NP 完全

論理積標準形

NOT, OR, AND **からなる全ての論理式は次の形で表せる：**

$$
\begin{aligned}
f(A_1, \ldots, A_n) = (X_{11} \vee \cdots \vee X_{1t_1}) \\
\wedge \cdots \\
\wedge (X_{s1} \vee \cdots \vee X_{st_s})
\end{aligned}
$$

(各 X_{ij} **は** A_k **または** $\neg A_k$**)**

$\cdots$ **論理積標準形・連言標準形**
(conjunctive normal form, CNF)

特に、$\forall i : t_i = 3$ **となる論理式** $\cdots$ 3-**CNF**

3-充足可能性問題 (3-SAT)

3-**CNF** $f(A_1, \ldots, A_n)$ **に対し、**
$f(a_1, \ldots, a_n) = 1$ **となる変数** A_i **の真理値の組**

$$(a_1, \ldots, a_n) \in \{0, 1\}^n$$

が存在するか？

定理

- **SAT は** 3-**SAT に多項式時間帰着可能**
- **従って、**3-**SAT も NP 完全**

3-充足可能性問題 (3-SAT)

3-**CNF** $f(A_1, \ldots, A_n)$ **に対し、**
$f(a_1, \ldots, a_n) = 1$ **となる変数** A_i **の真理値の組**

$$(a_1, \ldots, a_n) \in \{0, 1\}^n$$

が存在するか？

定理

- **SAT は** 3-**SAT に多項式時間帰着可能**
- **従って、**3-**SAT も NP 完全**

他にも沢山の NP 完全問題が知られている

例えば、次のパズルの解の存在判定は全て NP 完全

- **数独**
- **カックロ**
- **ののぐらむ**
- **スリザーリンク**
- **ナンバーリンク**
- **ぬりかべ**
- **美術館**
- **ましゅ**
- **天体ショー**
- **フィルオミノ**　　　　　　**など**