

第13回 2026/7/17 (最終回)

2025年11月27日 20:55

アルゴリズムと計算複雑度, PとNP

計算可能性, Church-Turingの提唱 [1920年代: Turing, Godel, Church] :

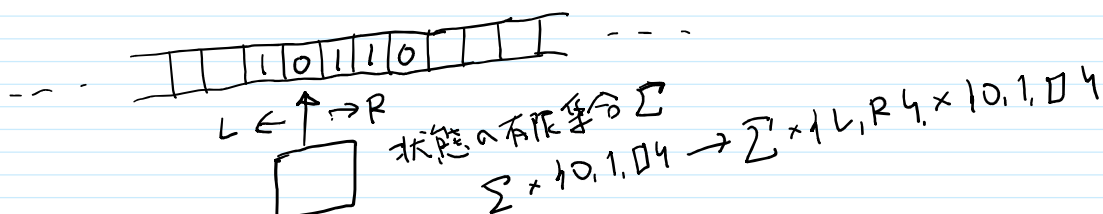
Def: $\phi: \{0,1\}^* \rightarrow \{0,1\}^*$ が計算可能 $\Leftrightarrow$

Φ を「計算する」チューリングマシンが存在

$$\bigcup_{n \geq 0} \{0,1\}^n$$

$\{0,1\}^* := 0 \text{ と } 1 \text{ の有限列の集合}$

0110...01



Φ を「問題例」の集合からその「解」への関数とみて,
それを計算するチューリングマシンのことを「問題 ϕ を解くアルゴリズム」という。

例: 線形計画問題: $\phi: (A, b, c) \mapsto \max. c^T x \text{ s.t. } Ax = b, x \geq 0$ (または最適解)

問題例やその解は, 0-1列としてコーディングされる. その長さのことをサイズという

FACT: 「計算可能でない」関数が存在する. 例: チューリングマシンの停止問題

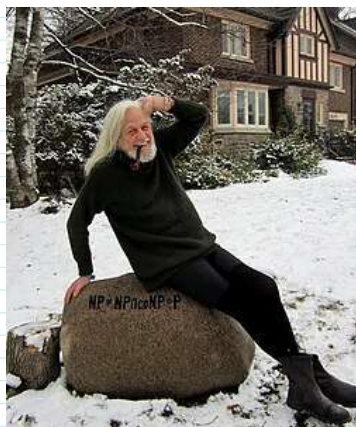
効率的なアルゴリズム, Cobham-Edmonds-伊理の提唱 [1960年代] :

問題 ϕ を解くアルゴリズムが多項式時間アルゴリズム $\Leftrightarrow$

ある多項式 p が存在して, どんな問題例 x に対しても, そのサイズ $|x|$ の $p(|x|)$ の
ステップで解を計算する.

そのようなアルゴリズムのことを「効率がよい」と考えよう.

Jack Edmonds 1934 --



wikipediaより

https://en.wikipedia.org/wiki/Jack_Edmonds

伊理正夫 1933-- 2018

https://orsi.org/wp-content/corsi/or54-6/or54_6_351.pdf

問題クラス **P**: 多項式時間アルゴリズムを持つような問題のクラス

PとNP, NP完全性, co-NP [1970年代 Cook]

問題クラス **NP**: 多項式時間のYES検証アルゴリズムが存在するような

判定問題 $\phi: \{0,1\}^* \rightarrow \{\text{YES}, \text{NO}\}$ のクラス

11.04

多項式時間YES検証アルゴリズム: 答えがYESなら多項式サイズの「証拠」が存在して、それを入力すると多項式時間で受理して終了する(そうでないなら受理しない).

例: $\phi: \text{グラフ } G \mapsto G \text{ がハミルトン閉路を持てば YES そうでなければ NO}$

証拠: ハミルトン閉路,

検証アルゴリズム: 連結であって、すべての頂点を通っていて、各点の次数が2かどうかチェックする.
--> ハミルトン閉路問題はクラスNPに属する.

例: $\phi: A, b \mapsto Ax = b$ に解が存在すれば YES そうでなければ NO

証拠1: 解 x , 検証アルゴリズム: Ax を計算して b になるか確かめる.

証拠2: Gaussの消去法

Thm [Edmonds]: Gaussの消去法は多項式時間アルゴリズムである.

特に、有理数係数の連立一次方程式を解く問題 in P

Proof: $Ax = b$ のサイズ, $A: m \times n$ 有理数行列 --- $O(mn \max_{i,j} \text{size}(a_{ij}))$

$b: m$ 次元有理数ベクトル --- $O(m \max_i \text{size}(b_i))$

where $\text{size}\left(\frac{p}{q}\right) := \log_2 |p| + \log_2 |q| + 1$

Gaussの消去法: 乗算, 除算, 足し算 nm^2 回

ただし、途中にあらわれる有理数のビットサイズが抑えられてなければならない.

解のサイズの評価: $\text{size}(A^{-1}b)_i = \text{size} \frac{\det(a_1 \dots b \dots a_n)}{\det A} \leq O((n \log n) + \text{size } A + \text{size } b)$

Lem: $P \subseteq NP$

Proof: 多項式時間アルゴリズムはYES検証アルゴリズムでもある.

Def: NP完全問題 := NPの問題であって、その問題を解くアルゴリズムをサブルーチン(オラクル)として用いることができればNPのすべての問題に多項式時間アルゴリズムが存在する.

Thm (Cook, Levin): SATはNP完全, 特に, NP完全問題は存在する.

SAT: 充足可能性判定問題

λ カ CNF形

論理式

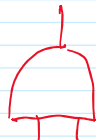
$$\varphi = (x_1 \vee \bar{x}_2 \vee x_3) \wedge (x_2 \vee x_4) \wedge (\bar{x}_1 \vee \bar{x}_4)$$

$x_i: 0, 1$ 変数

$$x \wedge y = \begin{cases} 1 & (x=y=1) \\ 0 & \text{o.w.} \end{cases}$$

$$x \vee y = \begin{cases} 0 & (x=y=0) \\ 1 & \text{o.w.} \end{cases}$$

$$\bar{x} = \begin{cases} 0 & x=1 \\ 1 & x=0 \end{cases}$$



CNFが充足 $\iff$ $x_i \in \{0, 1\}$ の割り当て $\exists$ があ $\exists$ x
 $\varphi = 1$

SAT = λ カ CNF φ

出力 YES φ が充足

NO 充足しない

Lem SAT $\in$ NP

⊙ 証拠: 充足可能性

polynomial - 代入して計算する

SAT $\in$ NP-complete の証明

⌋ 同値不十分 X

NPの問題を1つ与える

SAT から与える x の問題に与える

$x = X$ の λ カ

x が YES $\iff$ ある $\gamma: |x| \leq p(|x|)$, $B(x, \gamma) = \text{YES}$

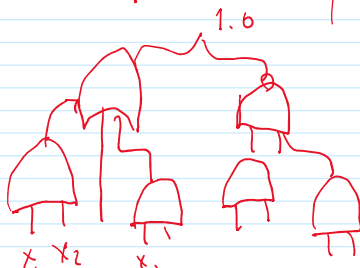
多項式時間
17M 証明可能

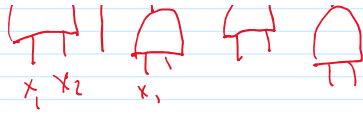
$B: |x| + p(|x|)$ の $0, 1$ 変数から

$0, 1$ を与える内政

$\rightarrow$ B は多項式時間
で計算可能 $\rightarrow$ CNFで表現可能

$(|x| + p(|x|))$
の多項式で与える





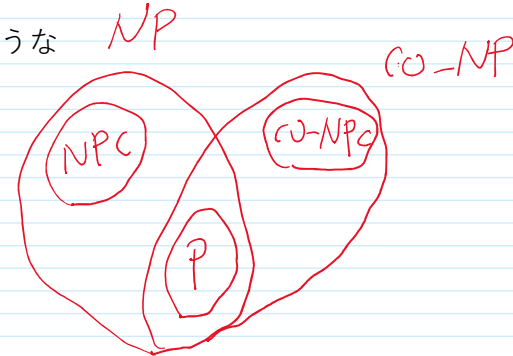
未解決問題： $P=NP$ か？

問題クラス **co-NP**: 多項式時間のNO検証アルゴリズムが存在するような

判定問題 $\phi: \{0,1\}^* \rightarrow \{YES, NO\}$ のクラス

Lem: $P \subseteq NP \cap co-NP$

Proof: 多項式時間アルゴリズムはNO検証アルゴリズムでもある。



未解決問題： $P = NP \cap co-NP$ か？

Lem: 線形不等式系 $Ax \leq b$ の解の存在判定問題 $\in NP \cap co-NP$

Good characterization

Proof: Farkasの補題

YESの証拠: $Ax \leq b$ をみたす x

NOの証拠: $y^T A = 0, y^T b < 0$ となる $y \geq 0$

Lem: フーリエ・モツキンの消去法は多項式時間アルゴリズムではない。

Proof: 1つ変数を消去すごとに不等式の個数が2倍になる。

線形不等式系や線形計画問題を解く多項式時間アルゴリズムは存在するか？

--> 楕円体法により肯定的に解決 (Khachian 1979)

FACT: 「いまのところ」単体法は多項式時間アルゴリズムではない。

未解決問題：

単体法が多項式時間アルゴリズムになるようなピボットルールは存在するか？