アルゴリズム論 1

第 12 回: 計算量理論の基本概念

関川 浩

2016/07/06

第 12 回から第 14 回の目標

計算量理論の紹介

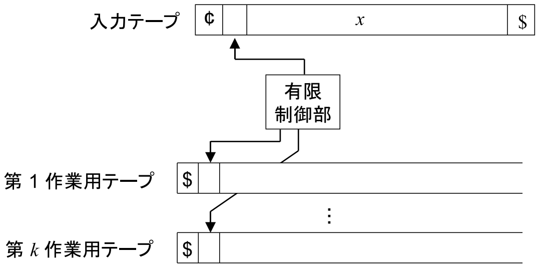
- 第 12 回: 計算量理論の基本概念
- 第 13 回: 計算量クラス, とくに NP について
  NP 完全性について
- 第 14 回: NP 完全問題の例

1. 多テープ Turing 機械の定義
   - k テープ TM (直観的な説明)
   - k テープ非決定性 TM
   - 様相
   - 動作
   - 受理
   - 1 テープ TM の動作例
2. 多テープ Turing 機械と計算量
   - 計算量理論
   - 最小ステップ数
   - 時間限定
   - NTIME, DTIME
   - 正規言語受理の計算量
3. 計算量クラスの概観
   - 計算量クラス P と NP
   - 真偽問題

k テープ TM (直観的な説明) (1/4)

k テープ TM ($k \geq 1$) は, 以下の部分からなる

- 読み取り専用の入力ヘッドを持った入力テープ
- 読み書きのできる作業用ヘッドを持った k 本の作業用テープ
- ヘッドの動きを制御する有限制御部



k テープ TM (直観的な説明) (2/4)

各部の詳細:

- 入力記号列 x は, 両端をエンドマーカとよばれる特別の記号 $\cent$ と $\$$ ではさまれた入力テープ上に与えられる

入力テープ

¢		x	$

- 作業用テープの左端のマス目には $\$$ が書かれている (左端のマス目は書き直しができない)

第 1 作業用テープ

$		

⋮

第 k 作業用テープ

$		

- M の有限制御部は有限種類の状態をとることができる (受理状態とよばれる特別の状態がいくつかある)

k テープ TM (直観的な説明) (3/4)

入力記号列 x が与えられたときの M の計算は以下の状況で開始:

- 入力ヘッドは $x\$$ の左端の記号上 ($x = \varepsilon$ の場合もある)
- 作業用テープの左端以外のマス目には空白記号が書かれており, 作業用ヘッドは \$ の書かれている右隣のマス目
- M は初期状態とよばれる特別の状態にある

k テープ TM (直観的な説明) (4/4)

M の動作は

- 入力ヘッドが見ている記号
- 各作業ヘッドが見ている記号
- 有限制御部の状態

によって決まり，以下の三種類

(1) 有限制御部の状態を変える

(2) 各作業用ヘッドは，今見ているマス目に記号を書き込む

(3) 入力ヘッド，各作業用ヘッドは，それぞれ左または右へ 1 マス動くか，今見ているマス目にとどまって動かない

入力ヘッドが右エンドマーカ \$ 上にあり，有限制御部が受理状態のとき，M は x を受理する，という

入力テープ

定義 1

Σ: アルファベット
$¢, \$ \notin \Sigma$: エンドマーカとよばれる特別な記号

このとき, $x \in \Sigma^*$ を入力とする入力テープを, 組

$$(h, ¢x\$) \qquad (0 \le h \le |x| + 1)$$

で定義

h: 入力ヘッドが見ている入力テープのマス目の番号
(0 番目のマス目には $¢$)

注: $¢x\$ = x_0 x_1 \ldots x_{n+1}$ $(n = |x|)$ のとき,
$(h, ¢x\$)$ を $x_0 x_1 \ldots \underline{x_h} \ldots x_{n+1}$ と表すこともある

作業用テープ

定義 2

Γ: アルファベット
$\Gamma \not\ni \$$, $\Gamma \ni B$ (空白記号とよばれる特別の記号)

Γ をアルファベットとする作業用テープ:

- $h \in \mathbb{N}$ と写像 $\xi : \mathbb{N} \to \Gamma \cup \{\$\}$ の組 (h, ξ)
  ただし, $\xi(0) = \$$, $\xi(n) \in \Gamma$ $(n \geq 1)$
- h: 作業用ヘッドが見ているマス目の番号
- $\xi(i) \in \Gamma \cup \{\$\}$: i 番目のマス目に書き込まれている記号

初期作業用テープ: 組 $(1, \xi_0)$ のこと
ただし, $\xi_0(0) = \$$, $\xi_0(n) = B$ $(n \geq 1)$

注: (h, ξ) を $\xi(0)\xi(1)\ldots\underline{\xi(h)}\ldots\xi(n)\ldots$ と表すこともある

k テープ非決定性 TM (1/3)

定義 3 (1/3)

k テープ非決定性 TM: $M = (K, \Sigma, \Gamma, \delta, q_0, B, F)$

- K, Σ, Γ, F は空ではない有限集合 $F \subseteq K$
- K の要素を状態, F の要素を受理状態という
- $q_0 \in K$ を初期状態という
- Σ: 入力アルファベット
- Γ: 作業用テープのアルファベット
- Γ は空白記号 B を含む

注: 非決定性 TM を NTM と略す

k テープ非決定性 TM (2/3)

定義 3 (2/3)

$\delta \subseteq K \times (\Sigma \cup \{\cancel{c}, \$\}) \times (\Gamma \cup \{\$\})^k \times K \times (\Gamma \cup \{\$\})^k \times \{L, R, N\}^{k+1}$

$(p, a, X_1, \ldots, X_k, q, Y_1, \ldots, Y_k, D_0, \ldots, D_k) \in \delta$ は遷移とよばれ，以下の 4 条件を満たす (ヘッドがテープからはみ出さない条件)

(1) $a = \cancel{c}$ ならば $D_0 = R$ または N

(2) $a = \$$ ならば $D_0 = L$ または N

(3) $X_i = \$$ ならば $Y_i = \$$ であり $D_i = R$ または N $(1 \leq i \leq k)$

(4) $Y_i = \$$ であるのは $X_i = \$$ のときに限る $(1 \leq i \leq k)$

k テープ非決定性 TM (3/3)

定義 3 (3/3)

TM $M = (K, \Sigma, \Gamma, \delta, q_0, B, F)$ に対し

$$Q_1 \stackrel{\text{def}}{=} K \times (\Sigma \cup \{¢, \$\}) \times (\Gamma \cup \{\$\})^k$$
$$Q_2 \stackrel{\text{def}}{=} K \times (\Gamma \cup \{\$\})^k \times \{L, R, N\}^{k+1}$$

このとき各 $u \in Q_1$ に対し

$$\delta(u) \stackrel{\text{def}}{=} \{v \in Q_2 \mid (u, v) \in \delta\}$$

$|\delta(u)| \leq 1$ $(\forall u \in Q_1)$ のとき, M を決定性 TM (DTM) という
$\delta(u) = \{v\}$ のとき, 単純化のため $\delta(u) = v$ と書く

様相

- 入力 x を与えられた TM M の様相とは

  状態 q
  入力テープ $(h, \not{c}x\$)$
  作業用テープ (h_i, ξ_i) ($1 \leq i \leq k$)

  の組

  $$C(x) : (q,\ (h, \not{c}x\$),\ (h_1, \xi_1), \ldots,\ (h_k, \xi_k))$$

  のこと

- 初期作業用テープを $(1, \xi_0)$ として, 様相

  $$(q_0,\ (1, \not{c}x\$),\ (1, \xi_0),\ (1, \xi_0), \ldots,\ (1, \xi_0))$$

  を, x を入力とする M の初期様相とよび $C_0(x)$ と表す

- 受理様相: q が受理状態で $(h, \not{c}x\$) = (|x| + 1, \not{c}x\$)$

動作 (1/2)

x を入力とする M の様相

$$C(x) : (p,\ (h, \not{c}x\$),\ (h_1, \xi_1), \ldots,\ (h_k, \xi_k))$$

が

$$\begin{aligned} x_h &= a & &(\not{c}x\$ = x_0 x_1 \ldots x_{n+1},\ x_i \in \Sigma \cup \{\not{c}, \$\}) \\ \xi_i(h_i) &= X_i & &(1 \leq i \leq k) \end{aligned}$$

を満たしているとき, 遷移

$$(q, Y_1, \ldots, Y_k, D_0, \ldots, D_k) \in \delta(p, a, X_1, \ldots, X_k)$$

によって, 以下で定義される様相 $D(x)$ へ移ることができる

動作 (2/2)

$D(x)$: $(q,\ (h+\tilde{D}_0, \not{c}x\$),\ (h_1+\tilde{D}_1, \tilde{\xi}_1), \ldots,\ (h_k+\tilde{D}_k, \tilde{\xi}_k))$

ただし

$$\tilde{D}_i = \begin{cases} 1, & D_i = R \text{ のとき} \\ -1, & D_i = L \text{ のとき} \\ 0, & D_i = N \text{ のとき} \end{cases} \qquad \tilde{\xi}_i(n) = \begin{cases} Y_i, & n = h_i \text{ のとき} \\ \xi_i(n), & n \neq h_i \text{ のとき} \end{cases}$$

さらに

$$0 \le h+\tilde{D}_0 \le |x|+1,\ \text{かつ},\ h_i+\tilde{D}_i \ge 0\ (1 \le i \le k)$$

が成立するときに限って，この動作は可能であるとする

これを $C(x) \Rightarrow D(x)$ と書く

受理

M は様相 $C(x)$ で停止:
　$C(x) \Rightarrow D(x)$ となる様相 $D(x)$ が存在しないこと

計算: 様相の列 $D_0(x) \Rightarrow D_1(x) \Rightarrow \cdots \Rightarrow D_t(x)$ のこと
　計算ステップ数を明示して $D_0(x) \overset{t}{\Rightarrow} D_t(x)$ と書き，
　$D_0(x)$ から $D_t(x)$ へ t ステップで到達可能という

M は x を受理:
　M の初期様相 $C_0(x)$ から，ある受理様相 $D(x)$ に到達する
　M の計算 (受理計算という) が少なくとも一つあるとき

　M が $D(x)$ で停止のとき，M は x を受理して停止するという

$L(M)$: M によって受理される記号列の集合
　M は $L(M)$ を受理するという

1 テープ TM の動作例 (1/2)

例 1

$M = (K, \Sigma, \Gamma, \delta, q_0, B, F)$ を
1 テープ TM とする
ただし,

$$K = \{q_0, q_1, q_2, q_3\}$$
$$\Sigma = \{0, 1, \#\}$$
$$\Gamma = \{B, 0, 1\}$$
$$F = \{q_3\}$$

かつ, δ は右表

$\Rightarrow M$ は DTM,
$L(M) = \{w\#w \mid w \in \{0,1\}^*\}$

q	a	X	$\delta(q, a, X)$
q_0	0	B	$(q_0, 0, R, R)$
q_0	1	B	$(q_0, 1, R, R)$
q_0	#	B	(q_1, B, N, L)
q_1	#	0	$(q_1, 0, N, L)$
q_1	#	1	$(q_1, 1, N, L)$
q_1	#	\$	$(q_2, \$, R, R)$
q_2	0	0	$(q_2, 0, R, R)$
q_2	1	1	$(q_2, 1, R, R)$
q_2	\$	B	(q_3, B, N, N)

注: $L(M)$ は pda では受理されない (文脈自由言語ではない)

1 テープ TM の動作例 (2/2)

入力 10#10 に対する M の動き

$$
\begin{array}{lll}
(q_0, \not{c}\underline{1}0\#10\$, \$\underline{B}B\ldots) & \left.\begin{array}{l} \Rightarrow (q_0, \not{c}1\underline{0}\#10\$, \$1\underline{B}B\ldots) \\ \Rightarrow (q_0, \not{c}10\underline{\#}10\$, \$10\underline{B}B\ldots) \end{array}\right\} & \text{コピー} \\
 & \left.\begin{array}{l} \Rightarrow (q_1, \not{c}10\underline{\#}10\$, \$1\underline{0}BB\ldots) \\ \Rightarrow (q_1, \not{c}10\underline{\#}10\$, \$\underline{1}0BB\ldots) \\ \Rightarrow (q_1, \not{c}10\underline{\#}10\$, \underline{\$}10BB\ldots) \end{array}\right\} & \begin{array}{l}\text{作業用テープ} \\ \text{のヘッド移動}\end{array} \\
 & \left.\begin{array}{l} \Rightarrow (q_2, \not{c}10\#\underline{1}0\$, \$\underline{1}0BB\ldots) \\ \Rightarrow (q_2, \not{c}10\#1\underline{0}\$, \$1\underline{0}BB\ldots) \\ \Rightarrow (q_2, \not{c}10\#10\underline{\$}, \$10\underline{B}B\ldots) \end{array}\right\} & \text{チェック} \\
 & \left.\begin{array}{l} \Rightarrow (q_3, \not{c}10\#10\underline{\$}, \$10\underline{B}B\ldots) \end{array}\right\} & \text{受理状態へ}
\end{array}
$$

1. 多テープ Turing 機械の定義
2. 多テープ Turing 機械と計算量
3. 計算量クラスの概観

計算量理論

入力 x を与えたときの,

- TM のステップ数 (時間量),
- 使用される作業用テープの量 (領域量) ,

が入力の長さ $|x|$ に対してどのようにふるまうかを考察

以下では, ステップ数 (時間量) のみ扱う

最小ステップ数 (1/2)

M: TM
$x \in L(M)$ に対して

- x を受理する計算は複数ある場合があり
- 計算のステップ数も異なる場合がある

time$_M(x)$: x を受理する最小ステップ数

$$\text{time}_M(x) \overset{\text{def}}{=} \min \left\{ t \;\middle|\; \begin{array}{c} \text{ある受理様相 } D(x) \text{ に対して} \\ C_0(x) \overset{t}{\Rightarrow} D(x) \end{array} \right\}$$

入力ヘッドは, すべての入力記号を読んで右エンドマーカに到達
$\Longrightarrow$ $\text{time}_M(x) \geq |x|$

最小ステップ数 (2/2)

例 2

M: 例 1 の 1 テープ DTM

$x = w\#w$ に対して, $\mathrm{time}_M(x) = 3|w| + 3$

$$
(q_0, \not{c}\underline{1}0\#10\$, \$\underline{B}B\ldots) \;\Rightarrow\; \left.\begin{array}{l}
(q_0, \not{c}1\underline{0}\#10\$, \$1\underline{B}B\ldots) \\
\Rightarrow\; (q_0, \not{c}10\underline{\#}10\$, \$10\underline{B}B\ldots)
\end{array}\right\}\text{コピー}
$$

$$
\left.\begin{array}{l}
\Rightarrow\; (q_1, \not{c}10\underline{\#}10\$, \$1\underline{0}BB\ldots) \\
\Rightarrow\; (q_1, \not{c}10\underline{\#}10\$, \$\underline{1}0BB\ldots) \\
\Rightarrow\; (q_1, \not{c}10\underline{\#}10\$, \underline{\$}10BB\ldots)
\end{array}\right\}\text{作業用テープのヘッド移動}
$$

$$
\left.\begin{array}{l}
\Rightarrow\; (q_2, \not{c}10\#\underline{1}0\$, \$\underline{1}0BB\ldots) \\
\Rightarrow\; (q_2, \not{c}10\#1\underline{0}\$, \$1\underline{0}BB\ldots) \\
\Rightarrow\; (q_2, \not{c}10\#10\underline{\$}, \$10\underline{B}B\ldots)
\end{array}\right\}\text{チェック}
$$

$$
\Rightarrow\; (q_3, \not{c}10\#10\underline{\$}, \$10\underline{B}B\ldots).\;\}\text{受理状態へ}
$$

時間限定

非負整数から非負整数への関数を単に関数とよぶ

定義 4

$T(n)$: 関数
M: k テープ NTM

言語 L に対して

- $L = L(M)$
- 有限個の例外を除き, 任意の $x \in L$ に対して $\mathrm{time}_M(x) \leq T(|x|)$

が成立するとき, M は L を時間 $T(n)$ で受理するという
そして, M は $T(n)$ 時間限定であるという

NTIME, DTIME

定義 5

$k \geq 1$ とする

$$\mathsf{NTIME}_k(T(n)) \stackrel{\text{def}}{=} \left\{ L \;\middle|\; \begin{array}{c} L \text{ はある } k \text{ テープ NTM によって} \\ \text{時間 } T(n) \text{ で受理される} \end{array} \right\}$$

$$\mathsf{DTIME}_k(T(n)) \stackrel{\text{def}}{=} \left\{ L \;\middle|\; \begin{array}{c} L \text{ はある } k \text{ テープ DTM によって} \\ \text{時間 } T(n) \text{ で受理される} \end{array} \right\}$$

$$\mathsf{NTIME}(T(n)) \stackrel{\text{def}}{=} \bigcup_{k \geq 1} \mathsf{NTIME}_k(T(n))$$

$$\mathsf{DTIME}(T(n)) \stackrel{\text{def}}{=} \bigcup_{k \geq 1} \mathsf{DTIME}_k(T(n))$$

正規言語受理の計算量

命題 1

L を正規言語とすると $L \in \mathsf{DTIME}(n)$

証明

M: L を受理する dfa (L は正規言語だから存在)
　作業用テープを持たない DTM とみなせる

M は長さ n の入力 $x \in L$ を n ステップで受理 ■

計算量クラス P と NP (1/2)

NP (P)

- NTM (DTM) によって多項式時間で受理される言語のクラス
- $P \neq NP$ と信じられており ($P \neq NP$ 予想), 多くの状況証拠があるが, まだ証明されていない

NP 完全な言語

- NP に属し, かつ, NP に属するすべての言語の複雑さを代表する言語. S. A. Cook が存在することを示した
- NP 完全な言語が P に属するなら $P = NP$

NP 完全性の意義

- 多項式時間で解けそうにないという漠然とした感覚が NP 完全性という概念によりはっきりと位置づけられた点
- 多項式時間アルゴリズムがなさそうだと思われていた非常に多くの重要な問題が NP 完全であることが示された点

計算量クラス P と NP (2/2)

定義 6 (計算量クラス P と NP)

$$\mathsf{P} \stackrel{\text{def}}{=} \bigcup_{d \geq 1} \mathsf{DTIME}(n^d), \qquad \mathsf{NP} \stackrel{\text{def}}{=} \bigcup_{d \geq 1} \mathsf{NTIME}(n^d)$$

定義 6 からすぐに分かる結果:

定理 1

$\mathsf{P} \subseteq \mathsf{NP}$

O 記号

$f(n)$, $g(n)$: 関数

ある定数 $c > 0$ と整数 $n_0 \geq 0$ が存在して

$$\text{すべての } n \geq n_0 \text{ に対して } f(n) \leq cg(n)$$

となるとき, $f(n) = O(g(n))$ と書く

例

- $n = O(n^2)$
- 任意の $d > 0$ に対し, $2^n \neq O(n^d)$, $n^d = O(2^n)$

P と NP の定義のいいかえ

命題 2

$\lim_{n\to\infty} T_2(n)/n = \infty$, $T_1(n) = O(T_2(n))$ とする

このとき, すべての $k \geq 1$ に対して以下が成り立つ

(1) $\mathrm{DTIME}_k(T_1(n)) \subseteq \mathrm{DTIME}_{k+1}(T_2(n))$

(2) $\mathrm{NTIME}_k(T_1(n)) \subseteq \mathrm{NTIME}_{k+1}(T_2(n))$

最高次の係数が正である任意の多項式 $p(n)$ に対して,
$d > 1$ を十分大きくとれば $\lim_{n\to\infty} n^d/n = \infty$ かつ $p(n) = O(n^d)$

$\Longrightarrow$ 命題 2 より, $\mathrm{DTIME}(p(n)) \subseteq \mathrm{DTIME}(n^d)$
$\mathrm{NTIME}(p(n)) \subseteq \mathrm{NTIME}(n^d)$

$\Longrightarrow$ P は DTM によって多項式時間で受理される言語のクラス
NP は NTM によって多項式時間で受理される言語のクラス

k テープ TM と 1 テープ TM の関係

命題 3

任意の整数 $k \geq 1$ に対して, 以下の (1), (2) が成立

(1) $\mathsf{DTIME}(n^k) \subseteq \mathsf{DTIME}_1(n^{2k})$

(2) $\mathsf{NTIME}(n^k) \subseteq \mathsf{NTIME}_1(n^{2k})$

$\Longrightarrow$ 多項式時間で受理するか否か (次数は問わない) を問題にするときは 1 テープ TM のみで考えてよい

真偽問題

- 写像 $A : \Sigma^* \to \{0, 1\}$ をアルファベット Σ で表現された**真偽問題**, または, 単に**問題**という
- A は $\{x \in \Sigma^* \mid A(x) = 1\} \subseteq \Sigma^*$ と同一視可能
  $\Longrightarrow$ A は Σ 上の言語とみなせる
  $\Longrightarrow$ **写像 A の複雑さ**は言語 $\{x \in \Sigma^* \mid A(x) = 1\}$ を受理する TM の時間量などではかることができる

以後, 整数は 2 進数で表現されているものとする

真偽問題の例

COMPOSITE NUMBERS
$= \{x \in \{0,1\}^* \mid x$ は合成数の 2 進表現 $\} \in$ NP

COMPOSITE NUMBERS を受理する 3 テープ NTM M の動作:

1. 入力 w が与えられると, 非決定的に動いて第 1 作業テープと第 2 作業テープにそれぞれ x と y を書き出す
2. x, y が 2 以上の 2 進数であることを確認後, xy を第 3 作業テープに書き出し, これが w と一致すれば w を受理

w が受理される場合, $|x|$, $|y| \leq |w|$ より, 多項式時間で受理される

注: PRIMES $= \{x \in \{0,1\}^* \mid x$ は素数の 2 進表現 $\} \in$ P が 2002 年に証明されたので, COMPOSITE NUMBERS $\in$ P