

相対化された多項式時間計算量クラスの細階層について

田中, 尚夫 / TANAKA, Hisao / 和泉, 正明 / 高橋, 信行 /
Takahashi, Nobuyuki / Izumi, Masa-aki

(出版者 / Publisher)

法政大学工学部

(雑誌名 / Journal or Publication Title)

Bulletin of the Faculty of Engineering, Hosei University / 法政大学工学部
研究集報

(巻 / Volume)

20

(開始ページ / Start Page)

29

(終了ページ / End Page)

41

(発行年 / Year)

1984-03

(URL)

<https://doi.org/10.15002/00004080>

相対化された多項式時間計算量クラスの 細階層について

田中尚夫*・和泉正明**・高橋信行***

On Fine Hierarchies on Relativized Polynomial-Time Complexity Classes

Hisao TANAKA*, Masa-aki IZUMI**, Nobuyuki TAKAHASHI***

Abstract

Let $P(k)^X$ [resp. $NP(k)^X$] be the class of languages accepted by deterministic [resp. nondeterministic] Turing machines with oracle X in k -th order polynomial time. Then the following hold.

- (1) There is an oracle set A such that for all $k \geq 1$
 $P(k)^A \subsetneq NP(k)^A \subsetneq P(k+1)^A$.
- (2) There is an oracle set B such that for all $k \geq 1$ $P(k)^B = NP(k)^B$.
- (3) For all $k \geq 1$, $P(k) = NP(k)$ implies $P(k+1) = NP(k+1)$.
- (4) For each $k \geq 1$, there exists an oracle set D such that $P(k)^D \neq NP(k)^D$
but $P(k+1)^D = NP(k+1)^D$.

And similar results also hold true for exponential-polynomial time.

決定性 (resp. 非決定性) Turing 機械のステップ数を, 入力語の長さの多項式で制限して得られる言語のクラスを P (resp. NP) で表わす。このとき $P=NP$ であるか否かは, 大変困難でしかも重要な未解決問題となっている。この問題は NP -完全なある問題で, 決定性多項式時間アルゴリズムで解けるものがあるかどうかという問題に帰着するのであるが, 今日に至るもそのような問題が一つも発見されていないところから多くの人々によって $P \neq NP$ であろうと予想されている。

ところで, Baker Gill and Solovay[1] ではこの問題の相対化版を論じ, $P(A)=NP(A)$ なる oracle A と $P(B) \neq NP(B)$ なる oracle B の存在を証明している。この結果は, $P=NP$ 問題の本質的な解決が極めて困難であることを証拠だてている。

一方, Kintala and Fischer [2] は Turing 機械の非決定的動作回数 (nondeterminism) を $(\log n)^*$ に制限して, 相対化された言語のクラスの細かな階層を得ている。すなわち, ある oracle

* 電気工学科計測制御専攻

** 工学研究科電気工学専攻 (M2)

*** 横浜商科大学商学部

に対しては $k \geq 2$ をどのようにとっても非決定的動作回数を制限された言語のクラス達が細階層をつくること、あるいは $k \geq 2$ が与えられたとき、制限関数が $(\log n)^1$ から $(\log n)^{k-1}$ までの間では言語のクラスは細階層を構成するのであるが、 $(\log n)^k$ から先はこの階層はなくなり同一のクラスになってしまうように oracle を構成できること、更には補集合をとる演算の下で閉じていないように oracle が構成できるなど、このクラスに関し種々の oracle 達を提示しているのである。

そこで本稿では、正整数 k が与えられたとき、 k 次多項式時間で受理される相対化された言語のクラスを定めることにより、これらのクラスの間色々な階層性を実現する oracle の構成を提示する。すなわち、oracle をうまく構成して決定性の Turing 機械によって k 次多項式時間で受理される言語のクラスと、非決定性の機械による対応する言語のクラスとの間に細かな階層が存在するように出来ることを先ず示す。ところが、Baker, Gill and Solovay [1] 同様 oracle をうまく構成すれば、非決定性機械の動きを決定性の機械でシミュレートできることもまた、可能であることが示せるのである。

一方、計算量クラスの間転移についていくつかの結果が知られている。すなわち一般に階層の下位レベルで決定性機械によって受理される言語のクラスと、非決定性機械によって受理される言語のクラスが一致すれば、上位レベルでも一致することが多い。このことは k 次多項式に関するクラスと $(k+1)$ 次多項式に関するクラスについても同様に成り立つ。そしてこの主張はそのまま相対化されるのであるが、逆は否定的である。すなわち、各 k に対し k 次多項式で計算時間を制限された決定性 Turing 機械の受理する言語のクラスと、その非決定性版とは異なるが、制限関数を $(k+1)$ 次多項式にするとこれら二つのクラスが一致するように oracle を構成できるのである。

更に、これらの結果は指数多項式時間で受理される相対化された言語のクラスについても、そのまま成り立つことが証明できる。

§ 1. 準 備

ω は自然数全体の集合で $\Sigma = \{0, 1\}$ は有限アルファベットとする。0, 1 から成る長さ 0 以上の語の全体を、 Σ^* であらわし、 Σ^* の部分集合を言語という。語 x の長さは $|x|$ で表わす。決定性多テープ Turing 機械を DTM, 非決定性多テープ Turing 機械を NTM であらわす。Turing 機械 T と ω から ω への関数 f が与えられているとき、 $|x| = n$ なる入力 x に対し T の x 上での計算が、高さ $f(n)$ ステップで停止し x を受理するか否かが決まるならば、その Turing 機械 T は f -時間限定であるといわれ、 T が DTM のとき f -時間限定 DTM, NTM ならば f -時間限定 NTM といわれる。正整数 k に対し、 T が k 次多項式時間限定 DTM (resp. NTM) であるとは、 T が n^k -時間限定 DTM (resp. NTM) であることである。 f -時間限定 DTM (resp. NTM) で受理

される言語のクラスを $\text{DTIME}(f)$ (resp. $\text{NTIME}(f)$) で表わす。従って、

$$P = \bigcup_{i=1}^{\infty} \text{DTIME}(\lambda n[n^i])$$

$$\text{NP} = \bigcup_{i=1}^{\infty} \text{NTIME}(\lambda n[n^i])$$

である。

以下、我々は Oracle Turing 機械を考える。Oracle Turing 機械 (OTM) とは、一本の質問テープと質問状態 $q?$, 肯定状態 q_Y , 否定状態 q_N の三つの特別な内部状態をもつ多テープ Turing 機械であって、OTM M が oracle として $X \subseteq \Sigma^*$ をもつときはその機械を M^X で表わすことにする。 M^X の状態が $q?$ になると機械は oracle X に対して質問テープ上の語が X に属しているか否かを尋ねる。もし、その語が X に属していれば機械は q_Y になり、そうでなければ M^X の状態は q_N になる。このような X に対する問い合わせ (query) を含む計算を X -計算という。

今、 M^X は入力 x 上を何ステップか走って停止するものとする。 M^X の最終状態が受理状態であれば、 M^X は語 x を受理するといひ、受理状態でないとき x を拒否するといひ、 L を言語とする。条件、

$$\forall x \in \Sigma^* [x \in L \iff M^X \text{ は } x \text{ を受理する。}]$$

が成り立つとき、 L は oracle X をもつ OTM M によって受理されるといひ、 $L = R(M^X)$ と書かれる。

§ 2. 多項式時間で受理される相対化された言語のクラス

ω から ω への関数 f を考える。OTM M が f -時間限定であるとは、任意の入力 x と任意の oracle X に対して M の X -計算が $f(|x|)$ ステップ以内で終わって x が受理されるか否かが決定されることである。決定性 [resp. 非決定性] k 次多項式時間限定 OTM 達をエフェクティブに並べたときの e 番目の機械を P_e [resp. NP_e] で表わす。 $\text{DTIME}^X(f)$ [resp. $\text{NTIME}^X(f)$] は oracle に X をもつ決定性 [resp. 非決定性] の f -時間限定 OTM によって受理される言語のクラスとする。

各 $k \geq 1$ と oracle $X \subseteq \Sigma^*$ に対し、次のような言語のクラスを考える。

$$P(k)^X = \bigcup \{ \text{DTIME}^X(\lambda n[c \cdot n^k]) : c > 0 \}$$

$$\text{NP}(k)^X = \bigcup \{ \text{NTIME}^X(\lambda n[c \cdot n^k]) : c > 0 \}$$

このような言語のクラスに関して定理が得られる。

定理 2.1. 次のような oracle A が存在する。すべて $k \geq 1$ のに対し $P(k)^A \not\subseteq \text{NP}(k)^A$ であって、 $\text{NP}(k)^A \subseteq P(k+1)^A$ 。

従って、次の階層が成り立つ。

$$P(1)^A \subseteq \text{NP}(1)^A \subseteq P(2)^A \subseteq \text{NP}(2)^A \subseteq \dots$$

証明 $\lambda k i[\langle k, i \rangle]$ は $(\omega - \{0\}) \times \omega$ から ω の上への 1 対 1 帰納的関数とし, $e = \langle k, i \rangle$ のとき $(e)_0 = k, (e)_1 = i$ と書くことにする。

e 番目の決定性 k 次多項式時間限定 OTM P_e の strict time bound は $p_e(n) = C_e \cdot n^k$ とする。ここで, $k = (e)_0$ であって, $0 < C_0 < C_1 < \dots$ とし, $C_e \frac{k+\frac{1}{2}}{k}$ は偶数になるものとする。

$$L_k(X) = \{0^m \mid \exists u \in X[|u| = m^k]\}$$

とおくと, あきらかに $L_k(X) \in \text{NP}(k)^X$ である。

さて, stage $s \in \omega$ に従って A を構成する。 $A(s)$ は, stage s より前に A に取り込まれた語の集合とし, $A(0) = A(1) = \phi, n_{-1} = 1, p_{-1} \equiv 0$ とおく。構成の途中, 各 index $e = \langle k, i \rangle$ はある stage で cancel される。stage 1 で出発する。

stage $2s+1$. $e = \langle k, i \rangle$ は最初の uncanceled index とし, $b = \max\{(a)_0 \mid a \leq e\}$ とおく。

- (i) $(2s+1) \frac{b}{k(b+\frac{1}{2})} = m$ は奇数
- (ii) $(2s+1) \frac{b}{b+\frac{1}{2}} > p_{e-1} \left((n_{e-1}) \frac{b'}{k(b'+\frac{1}{2})} \right)$

ただし, $(e-1)_0 = j, b' = \max\{(a)_0 \mid a \leq e-1\}$

- (iii) $p_e(m) = C_e(2s+1) \frac{b}{b+\frac{1}{2}} < 2s+1 < 2m^k$

が成り立つとする。

このとき, e を cancel し $n_e = 2s+1$ とおく。 $P_e^{A(2s+1)}$ を 0^m 上で走らせる。

Case 1) 拒否するとき, この計算で質問されることのない長さ m^k の語 u をひとつとって, $A(2s+2) = A(2s+1) \cup \{u\}$ とする。かかる u が存在することと, u は $2s+1$ 未満の stage で質問され得ないことが Claim 1 で証明される。

Case 2) 受理するとき, $A(2s+2) = A(2s+1)$ とする。

(i) \wedge (ii) \wedge (iii) が成立しないなら e は cancel せず, $A(2s+2) = A(2s+1)$ とする。

stage $2s+2$ e は $2s+1$ 以前の奇数 stage で cancel された最大の index とする。 $e = -1$ ならば, この stage はスキップする。 $e \geq 0$ ならば $d = \max\{(a)_0 \mid a \leq e\}$ とする。 $k, i, n \in \omega, x \in \Sigma^*$ を適当に選んで,

$$(1) \quad y = 0^k 10^i 1x10^n \wedge k \leq d \wedge \\ 2s+2 = |y| = C_{\langle k, i \rangle} \frac{k+\frac{1}{2}}{k} \cdot |x|^k \cdot \lceil |x|^{\frac{1}{2}} \rceil$$

なる y 達を考える。

$\text{NP}_{\langle k, i \rangle}^{A(2s+2)}$ をこの x の上で走らせる。このとき,

$$\begin{aligned} \text{質問される語の長さ} &< p_{\langle k, i \rangle}(|x|) = C_{\langle k, i \rangle} |x|^k \\ &\leq (2s+2) \frac{k}{k+\frac{1}{2}} \\ &\leq (2s+2) \frac{d}{d+\frac{1}{2}} \quad \because d \geq k \\ &< 2s+2 = |y| \end{aligned}$$

が成り立つ。

Case 1) 受理するとき, \mathcal{Y} を A に取り込む。

Case 2) 拒否するとき, 何もしない。

(1)なるすべての \mathcal{Y} について, この手続きを実行し A へ取り込んだ語の集合を $A'(2s+3)$ とし, $A(2s+3) = A(2s+2) \cup A'(2s+3)$ とする。(1)なる \mathcal{Y} が存在しなければ, $A(2s+3) = A(2s+2)$ とする。この stage で取り込まれる語 \mathcal{Y} が $2s+2$ 未満の stage で質問されることはないことが, Claim 2 で証明される。

$$A = \bigcup_{s=1}^{\infty} A(s) \text{ とおく。}$$

Claim 1. 1°) stage $2s+1$ で質問されない長さ m^k の語 u は存在する。

2°) u が $2s+1$ 未満の stage で質問されることはない。

[証明 1°) $2s+1$ で質問される語の個数 $< p_e(m) = C_e(2s+1)^{\frac{b}{b+\frac{1}{2}}} < 2^{m^k}$ により 1°) は明らかである。

$$2°) |u| = m^k = (2s+1)^{\frac{b}{b+\frac{1}{2}}} \text{ である。}$$

i) $2s' < 2s+1$ で質問される語の長さ $< (2s')^{\frac{d'}{d'+\frac{1}{2}}}$ である。ただし, $2s'$ よりも前の奇 stage で cancel された最後の index を e' とするとき $d' = \max\{(a)_0 | a \leq e'\}$ 。 $e' < e$ であるから $d' \leq b$ が成り立っている。従って, $(2s')^{\frac{d'}{d'+\frac{1}{2}}} < (2s+1)^{\frac{b}{b+\frac{1}{2}}} = |u|$ 。よって u が $2s+1$ 未満の偶数 stage で質問されることはない。

ii) e' は stage $2s'+1 < 2s+1$ で cancel された index とする。よって $e' \leq e-1$, 従って $n_{e'+1} \leq n_e = 2s+1$ 。

$$\begin{aligned} 2s'+1 \text{ で質問される語の長さ} &< p_{e'}(n_{e'+1}^{\frac{b'}{b'+\frac{1}{2}}}) \quad \text{ただし } j' = (e')_0 \\ &< n_{e'+1}^{\frac{b'}{b'+\frac{1}{2}}} \quad \text{ただし } b' = \max\{(a)_0 | a \leq e'\} \\ &\leq (2s+1)^{\frac{b'}{b'+\frac{1}{2}}} \quad \text{ただし } b' = \max\{(a)_0 | a \leq e'+1\} \\ &\leq (2s+1)^{\frac{b}{b+\frac{1}{2}}} = |u| \end{aligned}$$

よって, u は $2s+1$ 未満の奇数 stage で質問されない。]

Claim 2. \mathcal{Y} は $2s+2$ 未満の stage で質問されることはない。

[証明 $|\mathcal{Y}| = 2s+2$ である。

i) stage $2s' < 2s+2$ で質問される語の長さ $< 2s'$ 。よって \mathcal{Y} が $2s+2$ 未満の偶数 stage で質問されることはない。

ii) e' は stage $2s'+1 < 2s+2$ で cancel された index とし, $b' = \max\{(a)_0 | a \leq e'\}$ とする。このとき, $2s'+1$ で質問される語の長さ $< C_{e'}(2s'+1)^{\frac{b'}{b'+\frac{1}{2}}} < 2s'+1 < 2s+2 = |\mathcal{Y}|$ 。

よって, \mathcal{Y} は $2s+2$ 未満の奇数 stage で質問されることはない。]

Claim 3. stage $2s+1, 2s+2$ が実行されたとき,

(a) $P_e^{A(2s+1)}$ は 0^m を拒否する。 $\iff P_e^A$ は 0^m を拒否する。

(b) $NP_{\langle k, i \rangle}^{A(2s+2)}$ は x を受理する。 $\iff NP_{\langle k, i \rangle}^A$ は x を受理する。

[証明 (a) $A(2s+1)$ に対し、ある語が否定的に返答されたとすると $2s+1$ 以前の stage においてもその語は否定的に返答されるはずである。Claim 1, 2 の対偶により、かかる語は A に取り込まれない。よって、(a) が成り立つ。(b) も同様である。]

Claim 4. すべての $k \geq 1$ に対して $L_k(A) \in P(k)^A$

[証明 任意の i に対して $L_k(A) \in R(P_{\langle k, i \rangle}^A)$ であることを言えばよい。 $e = \langle k, i \rangle$ とおくと、この e もついいは cancel されるから $n_e = 2s+1$ が定まる。このとき P_e^A が 0^m を拒否する $\iff P_e^{A(2s+1)}$ は 0^m を拒否する $\iff \exists u \in A[|u| = m^k] \iff 0^m \in L_k(A)$ 。よって $R(P_e^A) = L_k(A)$ 。 i は任意であったから $L_k(A) \in P(k)^A$]

Claim 5. すべての $k \geq 1$ に対して $NP(k)^A \subseteq P(k + \frac{1}{2})^A$

[証明 任意に $L \in NP(k)^A$ をとると $L = R(NP_{\langle k, i \rangle}^A)$ なる i が存在する。そこで $e_1 = \langle k, i \rangle$ とおく。oracle A をもつ $O(n^{k+\frac{1}{2}})$ 時間限定の DOTM $M = M^A$ を次のように構成する。

与えられた任意の x に対して、 M は、

$$(2) \quad y = 0^k 10^{e_1} x 0^n \wedge |y| = C_{\langle k, i \rangle} \frac{k+\frac{1}{2}}{k} \cdot |x|^{k \cdot \lceil |x|^{\frac{1}{2}} \rceil} > n_{e_1}$$

なる語 y を質問テープ上にかき、 $y \in A$ か? と oracle A にたずねる。もし、yes ならば x を受理し、no ならば拒否する。(2) なる y を与えない x は有限個しかないから、かかる x のうち L の元となっているものだけを finite table で処理することにより M はかかる元だけを受理することができる。(2) なる y が与えられるとき $|y| = 2s+2$ とおける。stage $2s+2$ よりも前の奇数 stage で cancel された最大の index を e とおき $d = \max\{(a)_0 \mid a \leq e\}$ とおくと $n_{e_1} < 2s+2$ ゆえ、 $e_1 \leq e$ である。よって $k \leq d$ が成り立つ。すなわち $y = 0^k 10^{e_1} x 0^n \wedge k \leq d \wedge 2s+2 = |y| = C_{\langle k, i \rangle} \frac{k+\frac{1}{2}}{k} \cdot |x|^{k \cdot \lceil |x|^{\frac{1}{2}} \rceil}$ なる y がとれる。このとき、任意の x に対して

M が x を受理する $\iff y \in A \iff NP_{\langle k, i \rangle}^{A(2s+2)}$ は x を受理する $\iff NP_{\langle k, i \rangle}^A$ は x を受理する $\iff x \in L$ 。よって $L = R(M^A)$ 。

M は与えられた入力 x に対して、 x を受理するか否かを $O(|x|^{k+\frac{1}{2}})$ ステップ以内で決定できる。よって $L \in P^A(k + \frac{1}{2})$ 。従って $PN^A(k) \subseteq P^A(k + \frac{1}{2})$]

時間階層定理により $P(k + \frac{1}{2}) \subsetneq P(k+1)$ であるから、この oracle A に関して $k \geq 1$ をどのようにとっても $P(k)^A \subsetneq NP(k)^A \subsetneq P(k+1)^A$ がなりたつ。□

このように細分化された $P = NP$ 問題に対して否定的な結果を主張する oracle が存在する一方、次のように肯定的な結果を主張する oracle も存在する。

定理 2.2. 次のような oracle B が存在する。すべての $k \geq 1$ に対し $P(k)^B = NP(k)^B$ 。

従って、次の階層がなりたつ。 $P(1)^B = NP(1)^B \subsetneq P(2)^B = NP(2)^B \subsetneq \dots$

証明 $B(0) = \phi$ として stage 0 で出発する。

stage s . $k, i, n \in \omega, x \in \Sigma^*$ を適当に選んで、

$$(1) \quad y = 0^k 10^i 1x10^n \wedge s = |y| = C_{\langle k, i \rangle} \cdot |x|^k$$

なる γ 達を考える。

$NP_{\langle k, i \rangle}^{B(s)}$ を x 上で走らせる。この間に質問される語の長さは $\langle C_{\langle k, i \rangle} \cdot |x|^k = s = |y|$ である。

x を受理するなら、この γ を B へ取り込む。拒否すれば何もしない。

(1) なるすべての γ についてこの手続きを行ない、 B へ取り込んだ語全体の集合を $B'(s+1)$ とし

$B(s+1) = B(s) \cup B'(s+1)$ とする。もし(1)なる γ が存在しないなら $B(s+1) = B(s)$ とする。

$$B = \bigcup_{s=0}^{\infty} B(s) \text{ とおく。}$$

Claim 1. stage s で $B(s)$ に対し否定的に返答された語は、 s 以降の stage で B に取り込まれない。

[証明 質問される語の長さ $\langle |y|$ により、あきらか。]

Claim 1 により、次の Claim 2 が言える。

Claim 2. (1) の k, i, x に対し

$$NP_{\langle k, i \rangle}^{B(s)} \text{ が } x \text{ を受理する} \iff NP_{\langle k, i \rangle}^B \text{ が } x \text{ を受理する。}$$

Claim 3. すべての $k \geq 1$ に対し $NP(k)^B \subseteq P(k)^B$

[証明 $L \in NP(k)^B$ を任意にとると $L = R(NP_{\langle k, i \rangle}^B)$ なる i がとれる。oracle B をもつ $O(n^k)$ の DOTM $M = M^B$ を次のようにつくる。

任意に与えられた $x \in \Sigma^*$ に対し、 M はその質問テープ上に、

$$(2) \quad y = 0^k 10^i 1x0^n \wedge |y| = C_{\langle k, i \rangle} \cdot |x|^k$$

なる語を書き込み $y \in B$ かと oracle B にたずねる。もしも yes ならば x を受理し、no ならば拒否する。

(2) なる γ がとれないときの x の処理は、定理 2.1 のそれと同様である。

(2) なる形の γ がとれるとき $|y| = s$ とおく。このとき、 M が x を受理する $\iff y \in B \iff$

$$NP_{\langle k, i \rangle}^{B(s)} \text{ は } x \text{ を受理する} \iff NP_{\langle k, i \rangle}^B \text{ は } x \text{ を受理する} \iff x \in L。$$

よって $L = R(M)$ 。従って $L \in P(k)^B$ 。以上により $NP(k)^B \subseteq P(k)^B$ 。]

よって定理はなりたつ。□

前節でも述べたように、complexity hierarchy の下位レベルで等号が成り立てば上位レベルでも等号は成り立つことが多い。たとえば、 $P = NP$ を仮定すれば $DEXT = NEXT$ である。しかしこの逆はあきらかでない。相対化された計算量のクラス間では、否定が可能であることが判っている (Cf Book, Wilson and Mei-Rui[3])。我々の k 次多項式時間計算量クラスにおいても、これらの事実と同様のことがなりたっている。

定理 2.3. すべての $k \geq 1$ に対して

$$P(k) = NP(k) \text{ ならば } P(k+1) = NP(k+1)$$

従って, $P(1) = NP(1)$ ならば $P = NP$ である。

証明 証明のアイデアは Book [4] に負う。 $P_{\langle a, i \rangle}$ の strict time bound $p_{\langle a, i \rangle}$ は,

$$p_{\langle a, i \rangle}(n) = C_{\langle a, i \rangle} \lceil n^a \rceil$$

であるとする。特に $C_{\langle a, i \rangle}^{1/a}$ は整数であるとしておく。

$k \geq 1$ を固定する。明らかに, $P(k+1) \subseteq NP(k+1)$ 。

任意の $L_1 \in NP(k+1)$ に対して, $L_1 = R(NP_{\langle k+1, i \rangle})$ なる index i がある。

いま, $M_1 = NP_{\langle k+1, i \rangle}$ とする。さらに,

$$L_2 = \{w10^m \mid w \in L_1 \wedge |w10^m| = C_{\langle k+1, i \rangle}^{1/k} |w| \cdot \lceil |w|^{1/k} \rceil\}$$

と定義する。 M_1 から, 入力 $w10^m$ 上で $|w10^m|^k$ ステップで L_2 を受理する NTM M_2 を構成できる。 $\therefore L_2 \in NP(k)$ 。

仮定により $P(k) = NP(k)$ であるから, $L_2 = R(P_{\langle k, j \rangle})$ なる index j がある。 $M_3 = P_{\langle k, j \rangle}$ とする。

しかし, M_3 から次のような DTM M_4 を構成できる:

M_4 は入力 w 上で L_1 を受理する。 そのとき, M_4 は入力 $w10^m$ ($|w10^m| \geq C_{\langle k+1, i \rangle}^{1/k} |w|^{(k+1)/k}$) 上での M_3 のステップ数と同じステップ数を使用する。 すなわち, M_4 は,

$$O(|w10^m|^k) = O(|C_{\langle k+1, i \rangle}^{1/k} |w| \cdot \lceil |w|^{1/k} \rceil^k) = O(C_{\langle k+1, i \rangle} |w|^{k+1}) = O(|w|^{k+1})$$

ステップ使用する。

よって, $L_1 = R(M_4) \in P(k+1)$ 。

従って, $NP(k+1) \subseteq P(k+1)$ 。

ゆえに, $P(k+1) = NP(k+1)$ 。 \square

この結果は容易に一様に相対化できる。 すなわち,

系 2.4. すべての $k \geq 1$ とすべての oracle X に対して,

$$P(k)^X = NP(k)^X \text{ ならば } P(k+1)^X = NP(k+1)^X。$$

果してこの逆は成り立つであろうか。 この問いに対して否定的な結果が得られる。

定理 2.5. 各 $k \geq 1$ に対し, $P(k)^D \neq NP(k)^D$ であるが $P(k+1)^D = NP(k+1)^D$ なる oracle D が存在する。

証明 $L_k(X) = \{0^m \mid \exists u [u \in X \wedge |u| = m^k]\}$ とおく。

あきらかに, $L_k(X) \in NP(k)^X$ 。 以下 $k \geq 1$ を一つ固定する。 oracle D は stage で構成されるが, 構成中, 有限個の語が D へ取り込まれ, また \bar{D} のために reserve される。 ある stage でまだ D へ取り込まれてもいなく, \bar{D} に reserve もされていない語は unreserved であるという。

$D(s)$ は stage s より前に D に取り込まれた語の集合とする。 また, $P_{\langle k, i \rangle}$ (resp. $NP_{\langle k, i \rangle}$) の strict time bound $p_{\langle k, i \rangle}$ は,

$$p_{\langle k, i \rangle} = C_{\langle k, i \rangle} \cdot n^k$$

であり, $C_{\langle k+1, i \rangle}^{\frac{1}{k+1}}$ は正整数であるとする。

$D(0) = \phi$, $n_{-1} = 0$, $p_{\langle k, -1 \rangle}(n_{-1}) = 0$ として stage 0 で出発する。

Stage $2s$.

(1) $s^{k+1} \cdot 2^s < 2^{2(s-2)}$ (or $(k+1) \log s + s + 4 < 2s$)

とする。そのとき

(2) $\forall s > s_0 [s^{k+1} \cdot 2^s < 2^{2(s-2)}]$

なる s_0 が存在する。(1)が成立しないならこの stage をスキップし $D(2s+1) = D(2s)$ とする。そこで(1)が成り立つとする。

(3) $y = 0^i 1 x 10^n \wedge |y| = s$

なる y 連を考える。これらを適当な順序に枚挙して、

$$y_1, y_2, \dots, y_l$$

$$y_j = 0^{i(j)} 1 x_j 10^{n(j)} \quad (1 \leq j \leq l)$$

とする。(1)によりむしろ $l \geq 1$ である。

$D_0(2s) = D(2s)$ とし, y_j を考える。簡単のため $y = y_j = 0^i 1 x 10^n (|y| = s)$ とおく。

$NP_{\langle k+1, i \rangle}^{D_{j-1}(2s)}$ を x 上で n^{k+1} ステップ走らせる。この間に質問される語の長さは $< s^{k+1}$ 。

この間に受理すれば, $y 0^{|y|^{k+1}}$ を $D_{j-1}(2s)$ へ添加し, $D_j(2s)$ とする。 $|y 0^{|y|^{k+1}}|$ は偶数であることに注意せよ。さらにこのとき, この間に質問されるすべての unreserved な語 (長さは $< n^{k+1} \leq s^{k+1}$) を \bar{D} へ reserve する。

またこの間に受理しなければ $D_{j-1}(2s)$ へのあるいくつかの unreserved な語の添加が受理を惹き起すかどうかを決定する。(これは, 長さ $\leq n^{k+1}$ なる語についての添加のみを考えればよいから, 決定できる。) 2つの場合が生ずる。

Case a) もしそうなら, 一つの受理計算上で質問される unreserved な語を D と \bar{D} に適当に割り振り, 受理されるようにして, $y 0^{|y|^{k+1}}$ を D へとり込む。

Case b) もしそうでなければ, $y 0^{|y|^{k+1}}$ を \bar{D} へ reserve する。

このようにして新しく D へ取り込まれたすべての語を $D_{j-1}(2s)$ へ加え, $D_j(2s)$ とする。

$D(2s+1) = D_i(2s)$ として次の stage へ進む。作り方から,

(*) $y 0^{|y|^{k+1}} \in D \iff NP_{\langle k+1, i \rangle}^{D_j(2s)}$ が n^{k+1} ステップ未満で x を受理する

が成り立つ。

Stage $2s+1$. e は最初の uncancelled index とする。

(i) $p_{\langle k, e-1 \rangle}(n_{e-1}) < s + s^{k+1}$,

(ii) $p_{\langle k, e-1 \rangle}(n_{e-1}) < (2s+1)^k$,

(iii) $p_{\langle k, e \rangle}(2s+1) = C_{\langle k, e \rangle}(2s+1)^k < (s+1) + (s+1)^{k+1} < (2s+1)^{k+1}$,

$$(2s+1)^{k+1} + 2^{2s} < 2^{(2s+1)^k}$$

とする。

このとき e を cancel し, $n_e = 2s + 1$ とおく。 $P_{\langle k, e \rangle}^{D(2s+1)}$ を $x = 0^{2s+1}$ 上で走らせる。この間に質問されるすべての unreserved な語を \bar{D} へ reserve する。

$P_{\langle k, e \rangle}^{D(2s+1)}$ が z を拒否すれば, $|u| = (2s + 1)^k$, かつ, $\{u$ はこの計算中質問されず, より前の stage で reserve されていない} という u を一つとって (存在は Claim 3 をみよ) $D(2s + 2) = D(2s + 1) \cup \{u\}$ とする。 $|u|$ は偶数であることに注意せよ。

$P_{\langle k, e \rangle}^{D(2s+1)}$ が z を受理すれば, 長さ $(2s + 1)^k$ のすべての語を \bar{D} へ reserve し, $D(2s + 2) = D(2s + 1)$ とする。

$$D = \bigcup_{s=0}^{\infty} D(s) \text{ とする。}$$

Claim 1. どの index e も遂には cancel される。

[証明はあきらかである。]

Claim 2. 偶数 stage $2s$ で D または \bar{D} に取り込まれた語 $w = y_0^{|y|^{k+1}}$ は, $2s$ より前の任意の stage で質問されない。(従って stage $2s$ の初めで unreserved である。)

[証明 stage $2s' \leq 2s$ で質問される語の長さは,

$$(s')^{k+1} \leq s^{k+1} < |w|$$

より小さい。そこで, $2s$ より前に実行された最後の奇数 stage $2s' + 1 (< 2s)$ を考え, その stage で cancel される index を e' とする。そのとき,

$$p_{\langle k, e'-1 \rangle}(n_{e'-1}) < s' + (s')^{k+1} < s + s^{k+1} = |w|,$$

$$p_{\langle k, e' \rangle}(2s' + 1) < (s' + 1) + (s' + 1)^{k+1} = |w|$$

であるから, $|w|$ はより前の stage で質問されるどの語よりも長い。ゆえに, w はより前の stage で質問されない。]

Claim 3. 奇数 stage $2s + 1$ であの u が存在する。

[証明 (ii) によってより前の奇数 stage $< 2s + 1$ で質問される語の長さは $< (2s + 1)^k$ であるから, そこは考慮しなくてもよい。偶数 stage $2s' < 2s + 1$ で reserve される語の個数を評価する。 $y_j = 0^i 1 x 10^n$, $|y_j| = s'$ に対し, $NP_{\langle k+1, i \rangle}^{D_{j-1}(2s)}$ の x 上の n^{k+1} ステップの計算で reserve される語の個数は Case a) をも考慮して数えても (Case b) では 1 個だけ) $< n^{k+1} < (s')^{k+1}$ 。よって, stage $2s'$ での reserve される語の個数の合計は,

$$< (s')^{k+1} \cdot (x \text{ 達の個数}) < (s')^{k+1} \cdot 2s' < 2^{2(s'-2)}.$$

ゆえに, より前のすべての偶数 stage ($\leq 2s$) で reserve される語の個数は $< \sum_{s'=0}^s 2^{2(s'-2)} < 2^{2s}$ 。stage $2s + 1$ で質問される語の個数は $< (2s + 1)^{k+1}$ 。従って, (iii) により,

$$2^{2s} + (2s + 1)^{k+1} < 2^{(2s+1)^k} = \text{長さ } (2s + 1)^k \text{ の語の個数。}$$

偶数 stage で D にとり込まれる語の長さは偶数であるから, 長さ $(2s + 1)^k$ の任意の語とは一致しない。ゆえに, stage $2s + 1$ でも質問されず, より前の stage で reserve もされない長さ

$(2s+1)^k$ の語 u が存在する。]

注意：ある stage t で reserve されるある語がより前の偶数 stage $2s < t$ の Case b) の計算で質問されることがあっても、Case b) は stage $2s$ でそのまま保たれている。だからより前の stage で unreserved な語の D, \bar{D} への reservation はより前の stage に影響しないのである。

今までの考察から、

Claim 4.

1°) 偶数 stage $2s$ が実行されているとき、あの $y_j = 0^i 1 x 1 0^n$ に対し、 n^{k+1} ステップ以内では、

(α) $NP_{\langle k+1, i \rangle}^{D_j(2s)}$ の x 上の計算

と、

(β) $NP_{\langle k+1, i \rangle}^D$ の x 上の計算

とは一致する。従って、もし、

$$n^{k+1} \geq p_{\langle k+1, i \rangle}(|x|) = C_{\langle k+1, i \rangle} |x|^{k+1}$$

ならば、(α) と (β) とは全く一致する。

2°) 奇数 stage $2s+1$ が実行されているとき、

(γ) $P_{\langle k, e \rangle}^{D(2s+1)}$ の $z = 0^{2s+1}$ 上の計算

と、

(δ) $P_{\langle k, e \rangle}^D$ の z 上の計算

とは一致する。

[証明 1°) まず $NP_{\langle k+1, i \rangle}^{D_{j-1}(2s)}$ が n^{k+1} ステップ以内で x を受理するときは、 D にとり込んだ $y_0^{|y|^{k+1}}$ はこの計算で質問されないこと、および Claim 2, 3 と注意によって、(α) と (β) は n^{k+1} ステップで一致している。

次に $NP_{\langle k+1, i \rangle}^{D_{j-1}(2s)}$ が x を n^{k+1} ステップでは受理しないとき、Case a) では、 $NP_{\langle k+1, i \rangle}^{D_j(2s)}$ は x を n^{k+1} ステップで受理し、Claim 2, 3 と注意により $NP_{\langle k+1, i \rangle}^D$ も x を n^{k+1} ステップで受理する。Case b) では、 $y_0^{|y|^{k+1}}$ の \bar{D} への reservation はこの stage の計算に影響しないので、Claim 2, 3 と注意により (α) と (β) は一致する。すなわち、両者とも n^{k+1} ステップでは受理しない。

2°) Claim 2, 3 と注意により直ちに従う。]

Claim 5. $P(k)^D \neq NP(k)^D$ 。

[証明 任意に index e をとる。Claim 1 により $n_e = 2s+1$ が定まる。そうしてあの u が存在する。Claim 4 によって、

$$P_{\langle k, e \rangle}^D \text{ は } z = 0^{2s+1} \text{ を拒否する} \iff P_{\langle k, e \rangle}^{D(2s+1)} \text{ は } z = 0^{2s+1} \text{ を拒否する} \\ \iff \exists u [u \in D \wedge |u| = (2s+1)^k] \iff z \in L_k(D)。$$

よって、 $P_{\langle k, e \rangle}^D$ は $L_k(D)$ を受理しない。 e は任意。ゆえに、 $L_k(D) \in NP(k)^D - P(k)^D$ 。

Claim 6. $P(k+1)^D = NP(k+1)^D$ 。

[証明 任意に $L \in NP^{(k+1)^D}$ をとる。よって $L = R(NP_{\langle k+1, i \rangle}^D)$ なる i がある。oracle D をもつ $O(|x|^{k+1})$ 時間限定 DOTM M を次のように構成する。与えられた x に対し, M は,

$$y = 0^i 1 x 1 0, \quad n = C_{\langle k+1, i \rangle}^{\frac{1}{k+1}} \cdot |x|$$

なる γ を生成する。これは, $O(|x|)$ ステップで可能である。 $|y| = s$ とし,

$$(1) \quad s^{k+1} \cdot 2^s < 2^{2^{(s-2)}}$$

が成り立つとする。(1) が成立しないような x 達は高々有限個であるから, かかる x に対し finite table を作って,

$$x \in L \iff M \text{ は } x \text{ を受理する}$$

となるようにする。そこで(1)が成立する場合を考える。

stage $2s$ で, あの γ は枚挙の j 番目とする:

$$y = y_j = 0^i 1 x 1 0^n, \quad n = C_{\langle k+1, i \rangle}^{\frac{1}{k+1}} |x|.$$

M は次に $y 0^{|y|^{k+1}}$ を発生させる。これは $O(|x|^{k+1})$ ステップで可能である。 M は oracle D に $y 0^{|y|^{k+1}} \in D$ かどうかたずねる。yes なら M は x を受理し, no なら x を拒否する。Claim 4 と (*) を用いて,

$$\begin{aligned} x \in L &\iff NP_{\langle k+1, i \rangle}^D \text{ が } x \text{ を受理する} \\ &\iff NP_{\langle k+1, i \rangle}^{D_j(2s)} \text{ が } x \text{ を受理する} \\ &\iff NP_{\langle k+1, i \rangle}^{D_j(2s)} \text{ が } n^{k+1} = C_{\langle k+1, i \rangle} |x|^{k+1} \text{ ステップで } x \text{ を受理する} \\ &\iff y 0^{|y|^{k+1}} \in D \end{aligned}$$

よって, M は L を受理する。あきらかに, M は oracle D をもつ $O(|x|^{k+1})$ 時間限定 DOTM である。 $\therefore L \in P^{(k+1)}$ 。

ゆえに, $NP^{(k+1)^D} \subseteq P^{(k+1)^D}$ 。

よって, 定理は成り立つ。□

§ 3. 指数多項式時間で受理される相対化された言語のクラス

各 $k \geq 1$ と orale $X \subseteq \Sigma^*$ に対し, 次なる言語のクラスを考える。

$$\text{DEXT}(k)^X = \cup \{ \text{DTIME}^X(\lambda n [2^{cn^k}]) : c > 0 \},$$

$$\text{NEXT}(k)^X = \cup \{ \text{NTIME}^X(\lambda n [2^{cn^k}]) : c > 0 \}$$

前節の証明を逐語的に直すことにより, 前節の結果の多くの指数多項式版を得ることができ。すなわち,

定理 3.1. 次のような oracle A が存在する。

すべての $k \geq 1$ に対し $\text{DEXT}(k)^A \neq \text{NEXT}(k)^A$ であって $\text{NEXT}(k)^A \subseteq \text{DEXT}(k+1)^A$ 。

定理 3.2. 次のような oracle B がある:

すべての $k \geq 1$ に対し $\text{DEXT}(k)^B = \text{NEXT}(k)^B$ 。

定理 3.3. すべての $k \geq 1$ に対して

$\text{DEXT}(k) = \text{NEXT}(k)$ ならば $\text{DEXT}(k+1) = \text{NEXT}(k+1)$ 。

定理 3.4. 各 $k \geq 1$ に対し, $\text{DEXT}(k)^D \neq \text{NEXT}(k)^D$ であるが $\text{DEXT}(k+1)^D = \text{NEXT}(k+1)^D$ なる oracle D が存在する。

文 献

- [1] T. Baker, J. Gill and R. Solovay, Relativization of the $P=?NP$ questions, *SIAM J. Computing*, 4 (1975), 431-442.
- [2] C. M. R. Kintala and P. C. Fischer, Refining nondeterminism in relativized polynomial-time bounded computations, *SIAM J. Computing*, 9 (1980), 46-53.
- [3] R. V. Book, C. B. Wilson and Xu Mei-Rui, Relativizing time, space, and time-space, *SIAM J. Computing*, 11 (1982), 571-581.
- [4] R. V. Book, Comparing complexity classes, *J. Computer System Sci*, 9 (1974), 213-229.