

相対化された時間計算量のクラスについて

TANAKA, Hisao / 田中, 尚夫

(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)

43

(終了ページ / End Page)

47

(発行年 / Year)

1984-03

(URL)

<https://doi.org/10.15002/00004079>

相対化された時間計算量のクラスについて

田 中 尚 夫*

On Some Relativized Time-Complexity Classes

Hisao TANAKA*

Abstract

It is shown that there is an oracle set A such that $DEXT^A \neq NEXT^A$ but $DEPT^A = NEPT^A$. This result is a higher-level extension of a theorem of Book, Wilson and Mei-Rui [3].

時間計算量のクラスに関し文献 [1], [3], [4] の知識を仮定する。P, NP, DEXT, NEXT およびそれらの相対化クラスの定義もこれらの文献を参照されたい, チューリング計算機 (Turing machine) を TM と略記する。ここでは $\Sigma = \{0, 1\}$ 上の言語のみを考える。0, 1 の有限列全体の集合を Σ^* で表わし, Σ^* の要素を語という。語の集合を言語という。語 x の長さを $|x|$ で表わす。

DEPT [resp. NEPT] は決定性 [resp. 非決定性] の $\lambda n2^{p(n)}$ -時間限定 TM (p は多項式) によって受理される言語全体のクラスである。この定義において, TM を X を oracle としてもつ oracle Turing machine (OTM と略記する) でおきかえて得られるクラスを $DEPT^X$ [resp. $NEPT^X$] で表わす。

P_i は i 番目の決定性多項式時間限定 OTM とし, その時間限定関数を p_i とする。ここに, $p_i(n) = a_i n^{a_i}$, $a_i > 0$ である。 DE_i は i 番目の決定性線形指数時間限定 OTM とし, その時間限定関数を f_i とする。ここに $f_i(n) = 2^{c_i n}$, $c_i > 0$ である。また DEP_i [resp. NEP_i] は i 番目の決定性 [resp. 非決定性] 多項式指数時間限定 OTM とし, その時間限定関数を g_i とする。ここに $g_i(n) = 2^{b_i(n)}$ である。 P_i に oracle X を組合せた計算機を P_i^X で表わす。その他の種類の OTM についても同様である。

Book [2] は, 決定性クラスと非決定性クラスに関し, 色々な場合に下位レベルでのそれらの一致が上位レベルでの一致をもたらすことを示した。例えば (相対化した形で),

命題 1. すべての oracle X について, $P^X = NP^X$ ならば, $DEXT^X = NEXT^X$ である。

命題 2. すべての oracle X について, $DEXT^X = NEXT^X$ ならば, $DEPT^X = NEPT^X$ である。

* 電気工学科計測制御専攻

ここでは命題2について一つの証明を述べる：

$K(X) = \{0^i 1 x 10^n : NEP_i^X \text{ のある計算は } 2^n \text{ ステップ未満で } x \text{ を受理する}\}$

とおく。明らかに $K(X) \in NEXT^X$ であり、 $P^{K(X)}$ は $NEPT^X$ を含む。すなわち、 $K(X)$ は多項式 Turing 還元性に関し $NEPT^X$ -完全である。さて $DEXT^X = NEXT^X$ とせよ。よって $K(X) \in DEXT^X$ である。従って $K(X)$ を受理する DE_i^X がある。 $NEPT^X \subseteq DEPT^X$ を証明するために、任意に言語 $L \in NEPT^X$ をとる。 $L \in P^{K(X)}$ であるから、 L を受理する $P_j^{K(X)}$ がある。 L を受理する決定性多項式時間限定 OTM M with oracle X を次のように作る。任意に与えられた入力 x に対し、先づ M は $P_j^{K(X)}$ をシミュレートする。途中である語 w が $K(X)$ に属するか否かを問われたならば、 M は w 上の DE_j^X の計算をシミュレートする。 $P_j^{K(X)}$ が x を受理すれば、 M は x を受理し、そうでなければ M は x を拒否する。よって M は oracle X を用いて L を受理する。 $|w| \leq p_j(|x|)$ であり、このように質問を受ける w 達の個数も $\leq p_j(|x|)$ であるから、 M の全計算ステップは、

$$|x| \text{ の多項式} \times 2^{c_i p_j(|x|)}$$

でおさえられる。ゆえに M は決定性多項式指数時間限定 OTM である。ゆえに $L \in DEPT^X$ 。これで $NEPT^X \subseteq DEPT^X$ が証明された。□

さて命題1に対比して、Book, Wilson and Mei-Rui [3] は、 $P^W \neq NP^W$ であるが、 $DEXT^W = NEYT^W$ である oracle W の存在を証明した。ここでは命題2に対比して類似な結果を示す：

定理 $DEXT^A \neq NEXT^A$ であるが、 $DEPT^A = NEPT^A$ である oracle A が存在する。

証明 oracle A はステージで構成される。 $A(s)$ はステージ s より前に A に取り込まれた語全体の集合で、 $A(0) = \phi$ とする。構成中、 A の補集合のためにいくつかの語を順にリザーブする。ステージ $2s$ より前にリザーブされた語の集合を $F(2s)$ とし、禁止リストと呼ぶ。また各 OTM DE_e の index e は、 DE_e^A が言語

$$L(A) = \{0^n : \exists u \in A[|u| = 2^n]\}$$

を受理しないとわかった時点 n_e で消去される。明らかに $L(A) \in NEXT^A$ である。 $F(0) = \phi$, $n_{-1} = 1$, $f_{-1}(1) = 0$ とする。

ステージ $2s$ 。次の条件(1)をみたす語 y を考える：

(1) ある $x \in \Sigma^*$, i, n に対し、 $y = 0^i 1 x 10^n$ かつ $2s = |y| = 2^{p_i(|x|)}$ 。

x 上で $NEP_i^{A(2s)}$ を走らせる。この非決定的計算中に oracle に質問される語の長さは $2s$ より小さい。もし $NEP_i^{A(2s)}$ が x を受理するならば、次の条件(2)-(4)をみたす語 w を一つとる：

(2) $|w| = p_i(|x|)^2 + \epsilon$, ϵ は 0 か 1,

(3) $|yw|$ は奇数,

(4) yw は禁止リスト $F(2s)$ に入っていない。

かかる w は存在する (Claim 2)。 yw を作ってそれを A へ取り込む。もし $NEP_i^{A(2s)}$ が x を受理しないならば何もしない。(i) が成り立つような (有限個の) すべての語 y に対し上の手続きを行ない、 A へ取り込んだ語全体の集合を $B(2s+1)$ とし、 $A(2s+1) = A(2s) \cup B(2s+1)$ とする。もし (i) なる y が存在しないなら、このステージを飛ばし、 $A(2s+1) = A(2s)$ とする。

ステージ $2s+1$. e をこのステージの始まるまでに消去されなかった最初の index とする。

次の 4 条件が成立すると仮定しよう：

- (i) $2s+1 > f_{e-1}(\log n_{e-1})$,
- (ii) $\log(2s+2)$ は偶数である ($> \log n_{e-1}$ が成り立つ),
- (iii) 禁止リスト $F(2s)$ には $2s+1$ より長い語が含まれない,
- (iv) $f_e(\log(2s+2)) < 2^{(\log(2s+2))^2} < 2^{2s+2}$.

そのとき、このステージで e を消去し、 $n_e = 2s+1$ とおく。 $DE_e^{A(2s+1)}$ を語 $z_s = 0^{\log(2s+2)}$ 上で走らせる。この計算中否定的に質問された長さ $> 2s+1$ のすべての語を $F(2s)$ へ加え $F(2s+2)$ とする。もし $DE_e^{A(2s+1)}$ が z_s を拒否するならば、その計算中質問されない長さ $2s+2$ の語 u を一つとって $A(2s+1)$ へ加え $A(2s+2)$ とする。かかる語 u は存在する (Claim 3)。もし $DE_e^{A(2s+1)}$ が z_s を受理するならば、 $A(2s+2) = A(2s+1)$ とする。またもし (i)-(iv) の少くとも一つが満足されないならば何もせず (従って e の消去も行なわない)、 $A(2s+2) = A(2s+1)$ とする。

全ステージが終了したとき、

$$A = \bigcup_{s=0}^{\infty} A(s)$$

とする。この A が所要の条件をみたす oracle であることを証明する。初めにいくつかの準備を行なう：

Claim 1. 奇数ステージ $2s+1$ が実行されているとき、次の条件 (v) が成り立つ：

- (v) 任意 $\epsilon (= 0$ または $1)$, $i, n \in \omega$, $y, x \in \Sigma^*$ に対し、もし $y = 0^i 1 x 10^n$ かつ $2s+1 \leq |y| \leq 2^{p_i(|x|)}$ ならば、次のような語 w が存在する： $|w| = p_i(|x|)^2 + \epsilon$ かつ $DE_e^{A(2s+1)}$ は z_s 上の計算で yw を質問しない。

証。 z_s 上の $DE_e^{A(2s+1)}$ の計算で質問される語の個数は $f_e(\log(2s+2))$ より小さく、従って (iv) によりそれは $2^{(\log(2s+2))^2}$ より小さい。 $2s+1 \leq 2^{p_i(|x|)}$ であるから $2^{(\log(2s+2))^2} \leq 2^{p_i(|x|)^2}$ 。後者は $|w| = p_i(|x|)^2 + \epsilon$ なる w に対する yw という形の語の数を超えない。

Claim 2. 偶数ステージ $2s$ が実行されているとき、あのような語 yw が存在し、それは $2s$ 以前のどのステージでも質問されない。

証。 $2s'+1$ を $2s$ より前に実行された最後の奇数ステージとし、 e' をステージ $2s'+1$ で消去された index とする。Claim 1 によって、

- (5) 任意の $\epsilon (= 0$ または $1)$, $j, m \in \omega$, $y', x' \in \Sigma^*$ に対し、もし $y' = 0^j 1 x' 10^m$ かつ $2s'+1$

$\leq |y'| \leq 2^{p_i(|x'|)}$ ならば, $|w| = p_j(|x'|)^2 + \epsilon$, $|y'w|$ は奇数, かつ $DE_{e',A}(2s'+1)$ が $z_{s'}$ 上の計算で $y'w$ を質問しないような w がある。

そこで $y = 0^i 1 x 10^n$ をステージ $2s$ で考えている1つの語とする。ただし $2s = |y| = 2^{p_i(|x|)}$ である。 $2s'+1 < 2s$ であるから (5) によって, $|w| = p_i(|x|)^2 + \epsilon$, $|yw|$ は奇数, かつ $DE_{e',A}(2s'+1)$ が $z_{s'}$ 上の計算で yw を質問しないような w がある。 $2s'+1 > f_{e'-1}(n_{e'-1})$ なので $2s'+1$ より前の奇数ステージで質問される語は長さ $< 2s'+1$ なるものだけである。よって yw はもちろん禁止リスト $F(2s)$ に入っていない。さらに $2s$ 以前の偶数ステージで質問される語は長さが $< 2s$ なるものだけである。よって yw は所要の条件をみたす。

Claim 3. 奇数ステージ $2s+1$ が実行されているとき, あのような語 u が存在し, それは $2s+1$ より前のどのステージでも質問されない。

証。 z_s 上の $DE_{e,A}(2s+1)$ の計算で質問される語の長さは $f_e(\log(2s+2))$ より短かく, 従ってそれは 2^{2s+2} より短い。よって長さ $2s+2$ のかかる語 u が存在する。もちろん $u \in A(2s+1)$ である。 $2s+1$ より前の偶数ステージで質問される語の長さは $< |u|$ 。また (iii) により $u \in F(2s)$ 。ゆえに u は $2s+1$ 以前のどのステージでも質問されない。

Claim 4. 各 index e は遂には消去される。

証。条件 (i)-(iv) の性質から明らか。

以上の準備の下に $DE_{e,A} \neq NEXT^A$ かつ $DE_{e,A} = NEPT^A$ であることを証明する。先づ $L(A) \in DEXT^A$ を示そう。そのため, e を任意の index とする。Claim 4 によって n_e が定まる。 $n_e = 2s+1$ とおく。Claim 3 によって次の対角線論法が成り立つ:

$$\begin{aligned} DE_{e,A} \text{ は } z_s \text{ を拒否する} &\iff DE_{e,A}(2s+1) \text{ は } z_s \text{ を拒否する} \\ &\iff \exists u \in A[|u| = 2s+2] \\ &\iff z_s \in L(A). \end{aligned}$$

よって $DE_{e,A}$ は $L(A)$ を受理しない。 e は任意だから, $L(A) \in DEXT^A$ 。

おしまいに $NEPT^A \subseteq DEPT^A$ を証明するために, 任意に言語 $L \in NEPT^A$ をとる。よってある NEP_i^A が L を受理する。そこで L を受理する決定性多項式指数時間限定 OTM M with oracle A を次のように構成する。与えられた入力 x に対し, M は先づ,

$$(6) \quad y = 0^i 1 x 10^n, \quad |y| = 2^{p_i(|x|)}$$

なる語 y を発生させる。ここに i は上記非決定性 OTM NEP_i^A の index である。もしかかる y が存在しないような x があったとしてもそれらは高々有限個に過ぎない。よってかかる x に対しては有限表を作って,

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

となるようにする。そこでかかる y があるとし, $|y| = 2s$ とおく。 M は, $|w| = p_i(|x|)^2 + \epsilon$, $|yw|$ は奇数という語 w を生成する。そうして $yw \in A$ のときまたそのときに限り M は x を受理

するとする。Claim 3 を用いて、

$$\begin{aligned} M \text{ は } x \text{ を受理する} &\iff yw \in A \\ &\iff NEP_t^{A(2s+1)} \text{ は } x \text{ を受理する} \\ &\iff NEP_t^A \text{ は } x \text{ を受理する} \\ &\iff x \in L. \end{aligned}$$

従って、 M は L を受理する。 $yw \in A$ となるような w を見付けることは、 $2^{p_t(|x|)^2+1}$ の定数倍以下のステップで決定性的に行なうことができる。従って M は決定性の多項式指数時間限定 OTM である。ゆえに $L \in DEPT^A$ 。従って $NEPT^A \subseteq DEPT^A$ である。これで定理の証明が存了した。□

C を言語のクラスとすると、 $Tal(C)$ は C に属する tally 言語達から成る部分クラスとする。ここに tally 言語とは、1文字アルファベット上の言語のことである。tally 言語に関しては例えば「 $DEXT = NEXT$ ならば $Tal(P) = Tal(NP)$ である」ことが知られている。

これと対比して、上の証明から次の系が得られる：

系。 $DEPT^A = NEPT^A$ であるが、 $Tal(DEXT^A) \neq Tal(NEXT^A)$ なる oracle A が存在する。

文 献

- [1] T. Baker, J. Gill and R. Solovay, Relativizations of $P=?NP$ question, SIAM J. Comput., 4 (1975), 431-442.
- [2] R. Book, Comparing complexity classes, J. Comput. Syst. Sci., 9 (1974), 213-229.
- [3] R. Book, C. Wilson and Xu Mei-Rui, Relativizing time, space, and time-space, SIAM J. Comput., 11 (1982), 571-581.
- [4] C. Kintala and P. Fischer, Refining nondeterminism in relativized polynomial-time bounded computation, SIAM J. Comput., 9 (1980), 46-53.