確率的多項式時間計算量クラスBPPの内部の時間階層について

KUDOH, Masafumi / TANAKA, Hisao / 田中, 尚夫 / 工藤, 正史

(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)
31
(開始ページ / Start Page)
7
(終了ページ / End Page)
11
(発行年 / Year)
1995-03
(URL)
https://doi.org/10.15002/00003825

確率的多項式時間計算量クラスBPPの内部の時間階層について

工藤正史*，田中尚夫**

On a Time Hierarchy Within The Probabilistic Polynomial − Time Complexity Class BPP

Masafumi KUDOH * and Hisao TANAKA *

Abstract

For any positive integer k, let BPP(k) be the class of languages accepted by $O(n^k)$time bounded probabilistic Turing machines with error probability uniformly bounded below 1/2. It is a well − known open problem whether BPP(k) is properly contained in BPP(k+1) for all k≥1. In this paper, we consider its relativized version. We show that there is an oracle set A such that for all k≥1 $BPP(k)^A$ is properly contained in $BPP(k+1)^A$ Furthermore, we can show that for all k≥1 BPP(k) is properly contained in BPP(k+1) in almost all relativized worlds.

Theorem 3.5.Pr ($\{A| \forall k(BPP(k)^A \subset BPP(k+1)^A)\}$=1.

§1 序　　論

誤り確率を制限した確率的な時間階層に関する研究は，Karpinski-Verbeek [KV87]，Fortnow-Sipser [FS89]，Allender-Beigel-Hertrampf-Homer [ABHH93] によって行われている。誤り確率を制限した確率的階層定理が最初に述べられているのは，[KV87] においてである。現在，最良の誤り確率を制限した確率的階層定理は，[ABHH93, Corollary 3.4] である。しかしBPPの内部階層については，未解決である。すべての正整数k≥1に対してBPP（k）⊂BPP（k＋1）となるか否かという問題を“BPP（k）＝？BPP（k＋1）問題”と呼ぶことにする。ここで，⊂は，真の包含関係（proper inclusion）を表している。Fortnow-Sipser [FS89] は，BPP＝BPP(1)となるようなオラクル集合を構成した。この [FS89] の結果は，誤り確率を制限した“非常に細かい”確率的時

*大学院工学研究科システム工学専攻
**工学部システム制御工学科

問階層定理を相対化可能な技法を用いて証明することが不可能であることを示している。

本稿では，［FS89］の議論を発展させ，BPP（k＋1）＝？BPP（k＋1）問題を相対化して考察する。

§2 準　　備

本稿では，計算量理論の標準的な専門用語と表記法に従う（詳細は［BDG88］を参照されたい）。Σをアルファベットとし，Σ＝｛0，1｝と仮定する。Σ*は，Σの上のすべての記号列の集合を表現している。Σ*の中のxに対して，$|x|$は，xの長さを表している。言語，集合，そしてオラクル集合は，Σ*の部分集合である。

計算モデルは，確率的神託チューリングマシン（probabilistic oracle Turing machine，POTM）である。

kを正整数とする。確率的計算量クラスBPP(k) は，誤り確率が1/2より小さく制限された$O(n^k)$時間限定確率的チューリングマシンによって受理されるすべての言語のクラスである。BPP＝$\cup_{k\geq 1}$BPP(k)．Aをオラクル集合とする。BPP(k) とBPPをオラクル集合Aに対して相対化したクラスをそれぞれBPP(k)^{A}とBPP^{A}とする。PP(k)^{A}は，オラクル集合Aを持つ$O(n^k)$時間限定POTMによって受理されるすべての言語のクラスである。P(k)^{A}は，オラクル集合Aを持つ$O(n^k)$時間限定決定性神託チューリンクマシンによって受理されるすべての言語クラスである。

すべての言語クラスをΩとする。事象C⊆Ωに対して，Pr(C) は，各記号列xが集合Aに属すかどうかを決定するために行うランダム実験（公正なコインの独立したトス）によって集合Aが選択されたとき，$A\in$Cとなる確率である。また，集合のクラスC⊆Ωに対して$\overline{C}=\Omega-C$とする。

§3　BPP（k）＝？BPP（k＋1）問題の相対化

相対化したBPP(k) ＝？BPP(k＋1) 問題を考察する。なお，紙面の都合上，定理3.1と定理3.2の証明は，省略する。

定理3.1　すべての$k\geq 1$に対してBPP(k)$^A\subset$BPP(k＋1)^{A}となるオラクル集合Aが存在する。

パデング技術（padding technique）によって，次の定理を得ることができる。

定理3.2　すべてのオラクル集合Xとすべての$k\geq 1$に対して

$$\mathrm{BPP}(k)^X=\mathrm{BPP}(k+1)^X \Rightarrow \mathrm{BPP}(k+1)^X=\mathrm{BPP}(k+2)^X$$

となる。

ところで，BPPをBPP(1)に崩壊させるようなオラクル集合が存在する。これは，Fortnow-Sipser

[FS89] によつて与えられた結果である。

定理3.3（[FS89]）　$BPP(1)^B = BPP^B$ なるオラクル集合 B が存在する。

定理3.1で，すべての $k \geq 1$ に対して $BPP(k)^A \subset BPP(k+1)^A$ となるオラクル集合 A が存在することを示した。ここでは，この事実がほとんどすべてのオラクル集合 A に対して成り立つことを示す。次のような集合Aに依存する言語 $L_k[A]$ を定義する。

定義3.4　$$L_k[A] = \{x \mid 0^{|x|^k} \in A\}$$

定理3.5　$$Pr(\{A \mid \forall k\ (BPP(k)^A \subset BPP(k+1)^A)\}) = 1$$

証明　すべてのオラクル集合 A に対して，$L_k[A] \in P(k)^A$ すなわち $L_k[A] \in BPP(k)^A$ である。

次のようなクラスBPPS，$BPPS_k$，および $BPPD_k$ を定義する。

$$BPPS = \{A \mid \forall k\ (BPP(k)^A \subset BPP(k+1)^A)\}$$

$$BPPS_k = \{A \mid BPP\ (k)^A \subset BPP\ (k+1)^A\}$$

$$BPPD_k = \{A \mid L_{k+1}[A] \in BPP(k+1)^A - BPP(k)^A\} = \{A \mid L_{k+1}[A] \notin BPP(k)^A\}$$

$BPPS = \cap_{k \geq 1} BPPS_k$ と可算個の測度1のクラスの共通部分もまた測度1になることから，$Pr(BPPS) = 1$ を証明するには，任意の k を固定して，$Pr(BPPS_k) = 1$ を証明すればよい。

任意の k を固定する。$BPPD_k \subseteq BPPS_k$ より，$Pr(BPPD_k) = 1$ を示せば十分である。従って，$Pr(\{A \mid L_{k+1}[A] \in PP(k)^A\}) = 0$ を示せばよい。

ここで，任意の cn^l 時間限定POTM $M^\sim$ と $n^{k+l} > cn^k$ を満たす任意の十分に大きい n を固定する。但し，c は $M^\sim$ に依存する定数である。[BG81，Lemma 1]（この補題の証明の中の "then $L^{s*A}(x)$" は，"then $L^A(x)$)" と修正されるべきである）より，

$$Pr(\{A \mid L\ (M^A)\ (0^n) \neq L_{k+1}[A](0^n)\}) = \varepsilon$$

なる $M^\sim$ に依存しない $\varepsilon > 0$ が存在することを示せば十分である。

ここで次のようなクラス，C，GおよびHを定義する。

$$C = \{A \mid 0^n \in L_{k+1}[A]\} = \{A \mid 0^{n^{k+1}} \in A\}$$

$$G = \{A \mid 0^n \in L(M^A)\}$$

$$H = \{A \mid L(M^A)(0^n) \neq L_{t,1}[A](0^n)\}$$

このとき，

$$H = (G \cap \overline{C}) \cup (\overline{G} \cap C)$$

となる。また，$Pr(C) = 1/2$ である。

$M^{\sim}$は，長さcn^t以上の語をオラクル集合に問い合わせることができない。$n^{t+1} > cn^t$なるnを選んでいるので，任意のオラクル集合Aと長さnの任意の入力に対してM^Aは，$0^{n^{t+1}}$を問い合わせることはできない。従って，$Pr(G \cap \overline{C})$ と$Pr(\overline{G} \cap C)$ は，次のようになる。

$$Pr(G \cap \overline{C}) = Pr(G) \cdot Pr(\overline{C}) = \frac{Pr(G)}{2}$$

$$Pr(\overline{G} \cap C) = Pr(\overline{G}) \cdot Pr(C) = \frac{Pr(\overline{G})}{2}$$

これで$Pr(H)$ を評価する準備ができた。

$$Pr(H) = \frac{1}{2}\,(Pr(G) + Pr(\overline{G})) = \frac{1}{2}$$

$\varepsilon = \frac{1}{2}$ は，条件を満足する定義である。□

§4　結　　論

定理3.1と定理3.3の結果は，相対化可能な証明法でBPP（k）＝？BPP（k＋1）問題を解決することが不可能であることを意味している。Fortnow-Sipser [FS89] は，このような問題を解決することは困難であるが，必ずしも不可能ではないであろうと述べている。定理3.2によれば，次の二つのうちのどちらかが成り立つ。

1．BPP(k) ＝BPPとなるような正整数kが存在する。
2．すべての$k \geq 1$に対してBPP(k) $\subset$ BPP(k＋1) となる。

この事実と定理3.5から，

$$BPP(1) \subset BPP(2) \subset BPP(3) \subset \cdots \subset BPP$$

であると推測される。

参考文献

[ABHH93] E. Allender, R. Beigel, U. Hertrampf, and S. Homer, Almost－everywhere complexity hierarchies for nondeterministic time, *Theoretical Computer Science* 115 (1993) 225－241.

[BDG88] J.L. Blcázar, J. Díaz, and Gabarró, *Structural Complexity I* (Springer, Berlin, 1988).

[BG81] C.H. Bennett and J. Gill, Relative to a random oracle A, $P^A \neq NP^A \neq co\text{-}NP^A$ with probability 1, *SIAM Journal on Computing* 10 (1981) 96－113.

[FS89] L. Fortnow and M. Sipser, Probabilistic computation and linear time, in : *Proceedings of the 21st Annual ACM Symposium on Theory of Computing* (ACM Press, May 1989) 148－156.

[KV87] M. Karpinski and R. Verbeek, Randomness, provability, and the separation of Monte Carlo time and space, in : E. Börger, ed., *Computation Theory and Logic*, Lecture Notes in Computer Science, Vol. 270 (Springer, Berlin, 1987) 189－207.