数理解析研究所講究録
930巻 1995年 120-127

Generic Oracles と Random Oracles について
(特に, 相対化 BPP の部分クラスたちの分離)

(株) 東芝本社　工藤正史　(Masafumi Kudoh)
法政大・工　田中尚夫　(Hisao Tanaka)

§ 1. 序論. 計算量理論における基本的問題は

(1) $P = NP$?　(2) $P = NP \cap coNP$?

(3) $NP = coNP$?　及びこれらに類似する沢山の問題たち

を解決することであろう. 一まとめにして $P = NP$ 問題 と呼ぶことにする. ((1) が yes なら (2), (3) は yes となる.)

そこで, generic oracles がどうして $P = NP$ 問題に関わるのか説明する.

$\Sigma = \{0,1\}$, $\Sigma^* =$ the set of all finite strings over Σ.

$u, v \in \Sigma^*$ に対し, $u \subseteq v$ は u が v の prefix であること: $\exists z(uz = v)$.

2^{Σ^*} は確率空間及びカントル空間と考える. その要素を A, B, ..., X, Y, ... で表し, set, language, oracle などと呼ぶ. String $u = u_0u_1...u_{n-1}$ は $u(i) = u_i$ $(i < n)$ として, finite function とも考える. Oracle X も characteristic function と同一視する. $X|n = X(0)X(1)...X(n-1)$ は長さ n の initial segment. $[X|n] = \{Y : Y|n = X|n\}$ は basic open set. また, string u とその code 番号とを, 断りなしに, 同一視することもある. $D \subseteq \Sigma^*$ が dense とは, $\forall u \in \Sigma^* \exists v \in D [u \subseteq v]$. D が arithmetic とは, D が first order definable over ω であること.

$\mathbb{D}$ = the set of all dense arithmetic sets of strings とする.

これは明らかに可算集合である: $\mathbb{D} = \{D_0, D_1, D_2, \ldots\}$.

Oracle G が generic とは, $\forall i \exists k [G|k \in D_i]$ が成り立つこと.

$\mathbf{G}$ = the class of all generic oracles , 及び

$\Delta = \{X: P[X] = NP[X] \cap coNP[X]\}$ とおく.

さて, Blum-Impagliazzo (1987) によると,

$$P = NP \quad \text{ならば} \quad \mathbf{G} \subseteq \Delta .$$

$\mathbf{G}$ は comeager であるから,

『 If Δ is meager , then $P \neq NP$ 』

従って, Δ が meager であるかどうか は大きな問題である.

なお, 2^{Σ^*} においては, Kolmogorov Zero-One Law とともに, その Baire Category Version が成立するから, それを利用する :

$\mathbf{A} \subseteq 2^{\Sigma^*}$ が Baire の性質をもち, かつ finite variations の下で閉じていれば, $\mathbf{A}$ は meager or comeager のどちらかである.

これによれば, Blum-Impagliazzo の結果は,

『 If $P = NP$, then Δ is comeager 』

となる.

また, Δ が measure 0 かどうか も big problem である.

ここでは, Δ の代わりに, ある oracle H で相対化して

$$\Delta^H = \{ X: P[X] = NP[H \oplus X] \cap coNP[H \oplus X] \}$$

を考えると,

定理A. Δ^H が meager となる oracle H が存在する

という結果がえられる.

Bennett-Gill [BG 81] の問題 : " $\{X: P[X] \neq BPP[X]\}$ は comeagerであるか ? " も未解決である. これについても 定理A に類似な

定理B. $\{ X: P[X] \neq BPP[H \oplus X] \}$ が comeager となる oracle H が存在する .

と言う結果が得られる． BPP については次のパラグラフを参照されたい．

第二は，多項式時間確率アルゴリズムの階層問題である．

BPP[k]（ BPP[X,k]） は， n^k 時間で error 確率が一様におさえられるような確率アルゴリズム（ resp. oracle Xをもって）により受理される言語たち全体のクラスであり，BPP （BPP[X]）は k = 1,2,3,... についての和クラスである． 正確な定義は後で述べる．

すべての k について BPP[k] ⊆ BPP[k+1] であることは自明である．しかしこの包含関係が proper かどうかは未解決の難問である． そこで次善の策として，その相対化版を考える．これについて，次の結果が得られた：

定理C． 確率 1 をもって $\forall k$〔 BPP[X,k] ≠ BPP[X,k+1] 〕である．

定理D． {X : $\forall k$〔 BPP[X,k] ≠ BPP[X,k+1] 〕} は topologically large である，即ちそれは comeager クラスである．

本論文では，定理C，D の証明を記述する． 定理A，B の詳細については [TK 95] を参照されたい．

§2． BPP，相対化 BPP，及びそれらの部分クラス．

確率的多項式時間 (oracle) Turing machine（TM，OTM）M とは，或る多項式 p(n) 時間限定非決定性 Turing machine で，各入力 x に対し M の計算過程は深さ p(n)（但し n = |x|）の2進木であり，その各葉に 0 または 1 を指定する． そして

Prob[M(x) = 1] = （値 1 をもつ葉の個数 ）／$2^{p(n)}$

と定める． 言語のクラス PP，PP[k]，BPP，BPP[k] を定義する．PP[X]，PP[X,k]， BPP[X]， BPP[X,k] はそれぞれのXによる相対化版である． 言語 A について A∈PP （∈PP[k]）とは，或る確率的多項式（k 次多項式）時間TM M があって，すべての入力 x に対し

$$x \in A \Leftrightarrow Prob[\, M(x) = 1 \,] > 1/2$$

が成り立つこと．　また，$A \in BPP$ （ $\in$ $BPP[k]$ ）とは，或る確率的多項式（ k 次多項式） 時間TM　M　と $0 < e < 1/2$ があって

(2.1)　　$\forall x :$　$Prob[\, M(x) = A(x) \,] > (1/2) + e$

が成立すること．ここで，Aを特性関数と考えた．　簡単のため，(2.1) が成り立つとき

$$A = L(M, e)$$

と書く．

定義から，任意の k に対し

$$PP[k] \subseteq PP[k+1], \quad BPP[k] \subseteq BPP[k+1]$$

である．　また，　$PP[k] \neq PP[k+1]$ も容易にわかる．　そこで

問題　([KV 87])　$BPP[k] = BPP[k+1]$　なる整数 k があるか　？

この問題は未解決である．　もしかかる k があれば，その上位のクラスはすべて k のクラスに潰れてしまう：

命題 1．　任意の　k について

$BPP[k] = BPP[k+1]$　ならば　$BPP[k+1] = BPP[k+2]$．

証明．　任意に　$A \in BPP[k+2]$ をとる．(2.1) なる cn^{k+2} 時間限定確率的TM　M　と e がある．　この A に対し

$L[A] = \{\, w01^m : w \in A$　かつ　$|w10^m| = |w|\,\lceil |w|^r \rceil \,\}$，

を作る．　但し，$r = 1/(k+1)$，　「正実数 $s\rceil = s$ より小さくない最小の整数．これに対し 上記の M を利用して

$$Prob[M_1(x) = L[A](x)\,] > (1/2) + e$$

となる　$O(|x| + c|w|^{k+2})$ 時間限定確率的TM　M_1 を構成できる．

$$|w|^{k+2} \leq |w|^{k+1}\,\lceil |w|^r \rceil^{k+1} = |w01^m|^{k+1} = |x|^{k+1}$$

であるから，M_1 は $O(n^{k+1})$ 時間限定である．　よって　$L[A] \in BPP[k+1]$ となる．　従って仮定により，$L[A] = L(M_2, e_2)$　なる $c_2 n^k$ 時間限定確率的

TM M_2 と e_2 がある. 次に, TM M_3 は, 入力 x に対し $|x01^m| = |x|\lceil|x|^r\rceil$ なる string $x01^m$ を書き, その上で M_2 の動作を模倣する. M_2 が受理すれば, M_3 は x を受理する. そうでなければ, 拒否する. このとき $Prob[M_3(x) = A(x)] \geqq (1/2) + e_2$ である. ここで M_3 は $O(|x|\lceil|x|^r\rceil + c_2|x01^m|^k)$ 時間限定である. 或る有限個を除くすべての x に対し

$$|x10^m|^k = |x|^k\lceil|x|^r\rceil^{k+1} \leqq |x|^k(|x|^r+1)^k \leqq |x|^{k+1}$$

なる m があるから, M_3 は $O(|x|^{k+1})$ 時間限定である. かくて, $A = L(M_3, e_3) \in BPP[k+1]$ となる. □

以下で, 上の Karpinski-Verbeek の問題の相対化版の否定を強い形で与える. 定理C, D がそれである.

§3. 定理C, Dの証明.

我々は Bennett-Gill の補題 を利用する.

補題1. [BG 81] $L^{\sim}$ は oracle-dependent 言語, $\{M_1^{\sim}, M_2^{\sim}, \ldots\}$ は [BG 81] に記述された4条件をみたす OTMs の集合とする. このとき, もし或る正数 ε に対し, $\{A : \forall i[T(M_i^A) \neq L^A]\}$ の measure が $> \varepsilon$ ならば, $\{A : \exists i[T(M_i^A) = L^A]\}$ の measure は 0 である.

定理C. 次式で定義されるクラスの measure は 1 である:

$$SEP = \{A : \forall k(BPP[A,k] \neq BPP[A,k+1])\}$$

証明. 以下, measure を μ で表す. 各 k について, $\mu(SEP_k) = 1$, $SEP_k = \{A : BPP[A,k] \neq BPP[A,k+1]\}$ であることを示せばよい. そこで k を固定する. 先ず

$$L_k^A = \{x : 0^m \in A, m = |x|^k\}$$

を作ると, 任意の A について, $L_k^A \in P[A,k] \subseteq BPP[A,k]$ である.

$$\mu(\{A : L_{k+1}^A \in PP[A,k]\}) = 0 \tag{3.1}$$

を導けばよい. 何故ならそのとき $\mu(\{A: L_{k+1}^A \notin BPP[A,k]\}) = 1$ であり，全ての A について $L_{k+1}^A \in BPP[A,k+1]$ だからである. そこで補題1における OTMs の集合として，k 次多項式時間限定確率OTMs 全体の集合をとる. よって，$M^\sim$ を任意の cn^k 時間限定確率OTM（cは正定数）であるとし，$n^{k+1} > cn^k$ なる自然数 n を一つ固定する.

(3.2) $\mu(\{A: T(M^A)(0^n) \neq L_{k+1}^A(0^n)\}) = \varepsilon$

なる正数 ε を見出せればよい. $M^\sim$ は任意だから，そのとき，補題1により (3.1) が言える（補題1の他の条件が満たされていることは明らかである）. これについて，我々は (3.2) の ε として 1/2 を取ることができることを示す： 次の3つのクラス $\mathbf{F}$, $\mathbf{G}$, $\mathbf{H}$ を考察する.

$\mathbf{F} = \{A: 0^n \in L_{k+1}^A\} = \{A: 0^m \in A, m = n^{k+1}\}$,

$\mathbf{G} = \{A: 0^n \in T(M^A)\}$,

$\mathbf{H} = \{A: T(M^A)(0^n) \neq L_{k+1}^A(0^n)\}$ （これが目標のクラス）.

ここで, $\mu(\mathbf{F}) = 1/2$ である. $M^\sim$ は cn^k より長い string を問い合わせることができないから，n の選び方により，$M^\sim$ は 0^m（ただし $m = n^{k+1}$）を問い合わせることができない. 従って，$\mathbf{G}$ と $\neg\mathbf{F}$, $\neg\mathbf{G}$ と $\mathbf{F}$ は互いに独立である.

よって

$$\mu(\mathbf{G}\cap\neg\mathbf{F}) = \mu(\mathbf{G})\,\mu(\neg\mathbf{F}) = \mu(\mathbf{G})/2$$

$$\mu(\neg\mathbf{G}\cap\mathbf{F}) = \mu(\neg\mathbf{G})\,\mu(\mathbf{F}) = \mu(\neg\mathbf{G})/2$$

$$\therefore\quad \mu(\mathbf{H}) = \mu((\mathbf{G}\cap\neg\mathbf{F})\cup(\neg\mathbf{G}\cap\mathbf{F}))$$

$$= (\mu(\mathbf{G}) + \mu(\neg\mathbf{G}))/2 = 1/2 .$$

これで，定理C が証明された. □

次に，定理D を証明するために，補題1 を Baire category 用に改変する：

<u>補題2</u>. 補題1 と同じ条件の下で，次のクラス $\mathbf{E}$ は comeager である：

$$\mathbf{E} = \{A: \exists j\,[\,T(M_j^A) \neq L^A\,]\}$$

証明. $\mathbf{E}$ が comeager でない，即ち $\neg\mathbf{E}$ が meager でないとする.

$$\neg \mathbf{E} = \bigcup_j \mathbf{F}_j, \qquad \mathbf{F}_j = \{ A : L^A = L(M_j^A) \}$$

であるから，或る $\mathbf{F}_j$ は nowhere dense でない．よって，或る [u] に対し

$\forall v$ ($[v] \subseteq [u]$ ならば $[v] \cap \mathbf{F}_j \neq \phi$)，i.e.,

$$[u] \subseteq \overline{\mathbf{F}_j} \text{ (closure)} = \mathbf{F}_j \quad (\because \ \mathbf{F}_j \text{は閉集合})$$

$$\therefore \quad \mu(\neg \mathbf{E}) \geq \mu(\mathbf{F}_j) \geq \mu([u]) .$$

補題1により $\mu(\neg \mathbf{E}) = 0$ であるから，不合理．よって，$\mathbf{E}$ は comeger でない．□

定理D． クラス SEP は comeager である．

証明． $\mathbf{E}_k = \{ A : L_{k+1}^A \in PP[A,k] \}$ とおくと，定理C の証明により，$\mu(\mathbf{E}_k) = 0$．従って，補題2 により，$\mathbf{E}_k$ はmeager である．

ところで， $BPP[A,k] = BPP[A,k+1]$ ならば，

$$L_{k+1}^A \in P[A,k+1] \subseteq BPP[A,k+1] = BPP[A,k] \subseteq PP[A,k]$$

であるから， $\neg BPP_k \subseteq \mathbf{E}_k$， 従って，$\neg BPP_k$ は meager である．

k は任意であるから，$\neg BPP = \bigcup_k \neg BPP_k$ は meager， よって BPP は comeagerである．□

§4．その他の問題．

BPP については，§2 で述べた Karpinski-Verbeek の問題の他に，未解決問題として，完全集合の問題がある．即ち

“ BPP- 完全集合は存在するか ？ ”

これに対し，『線形時間多対1還元に関する BPP- 完全集合は存在しない』ことを証明できる．これより，

$$BPP \neq DSPACE(lin) \qquad BPP \neq NSPACE(lin),$$

$$BPP \neq DEXT, \qquad BPP \neq NEXT$$

を導くことができる．今の結果において，BPP を PP で置き換えることができる．しかし，原問題はなかな困難な問題である．

文　　献

[BG 81] Bennett, C.H., Gill, J., Relative to a random oracle A, $P^A \neq NP^A \neq coNP^A$ with probability 1, SIAM J. Comput., 10 (1981), 96-113.

[BI 87] Blum, M., Impagliazzo, R., Generic oracles and oracle classes, Proc. 28th Annual IEEE Symposium on Foundations of Computer Sci., IEEE Computing Soc. Press, Washington D.C., (1987), 118-126.

[KT 95] Kudoh, M., and Tanaka, H., On some oracle results on the bounded error probabilistic polynomial time complexity class BPP (Abstract), to appear in Logic Colloquium '95, Haifa, Israel.

[KV 87] Karpinski, M., Verbeek, R., Randomness, probability, and the separation of monte carlo time and space, Computation and Logic, LN in Computer Science, Springer, Vol.270 (1987), 189-207.

[TA 95] Tanaka, H., and Kudoh, M., On relativized probabilistic polynomial time algorithms, to appear.