

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) $P = NP \cap \text{coNP}$?

(3) $NP = \text{coNP}$? 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 $A, B, \dots, X, Y, \dots$ で表し, set, language, oracle などと呼ぶ. String $u = u_0 u_1 \dots u_{n-1}$ 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. $X \upharpoonright n = X(0)X(1)\dots X(n-1)$ は長さ n の initial segment. $[X \upharpoonright n] = \{Y : Y \upharpoonright n = X \upharpoonright n\}$ 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.

$\mathbf{D} =$ 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: $\mathbf{D} = \{D_0, D_1, D_2, \dots\}$.

Oracle G が generic とは, $\forall i \exists k (G \upharpoonright k \in D_i)$ が成り立つこと.

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,

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

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 :

$A \subseteq 2^{\Sigma^*}$ が Baire の性質をもち, かつ finite variations の下で閉じていれば, 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 $k = 1, 2, 3, \dots$ 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 $BPP[k] \subseteq BPP[k+1]$ 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 $\forall k \{ BPP[X, k] \neq BPP[X, k+1] \}$ である。

定理 D. $\{X : \forall k \{ BPP[X, k] \neq BPP[X, k+1] \}\}$ 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

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

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 $A \in PP$ ($\in PP[k]$) 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

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

が成り立つこと. また, $A \in \text{BPP}$ ($\in \text{BPP}[k]$) 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

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

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

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

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

問題 ([KV 87]) $\text{BPP}[k] = \text{BPP}[k+1]$ 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

$$\text{BPP}[k] = \text{BPP}[k+1] \quad \text{ならば} \quad \text{BPP}[k+1] = \text{BPP}[k+2].$$

証明. 任意に $A \in \text{BPP}[k+2]$ 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

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

を作る. 但し, $r = 1/(k+1)$, $\lceil \text{正実数 } s \rceil = s \text{ より小さくない最小の整数}$.

これに対し 上記の M を利用して

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

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 $L[A] \in \text{BPP}[k+1]$

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 $|x01^m| = |x| + |x|^r$ 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 $\text{Prob}[M_3(x) = A(x)] \geq (1/2) + e_2$ である. ここで M_3 は $O(|x| + |x|^r + c_2 |x01^m|^k)$ 時間限定である. 或る有限個を除くすべての x に対し

$$|x01^m|^k = |x|^k + |x|^r k^{k+1} \leq |x|^k (|x|^r + 1)^k \leq |x|^{k+1}$$

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, $A = L(M_3, e_3) \in \text{BPP}[k+1]$ となる. $\square$

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, $\{M_1^\sim, M_2^\sim, \dots\}$ 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:

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

証明. 以下, measure を μ で表す. 各 k について, $\mu(\text{SEP}_k) = 1$, $\text{SEP}_k = \{A : \text{BPP}[A, k] \neq \text{BPP}[A, k+1]\}$ 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, $L_k^A \in P[A, k] \subseteq \text{BPP}[A, k]$ である.

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

を導けばよい。何故ならそのとき $\mu(\{A : L_{k+1}^A \notin \text{BPP}[A, k]\}) = 1$ であり、全ての A について $L_{k+1}^A \in \text{BPP}[A, k+1]$ 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。

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

なる正数 ε を見出せばよい。 $M^\sim$ 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 F, G, H を考察する。

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

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

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

ここで、 $\mu(F) = 1/2$ 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、 G と $\neg F$, $\neg G$ と F は互いに独立である。

よって

$$\mu(G \cap \neg F) = \mu(G) \mu(\neg F) = \mu(G) / 2$$

$$\mu(\neg G \cap F) = \mu(\neg G) \mu(F) = \mu(\neg G) / 2$$

$$\therefore \mu(H) = \mu((G \cap \neg F) \cup (\neg G \cap F))$$

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

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：

補題2. 補題1 と同じ条件の下で、次のクラス E は comeager である：

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

証明. E が comeager でない、即ち $\neg E$ が meager でないとする。

$$\neg E = \bigcup_j F_j, \quad F_j = \{ A : L^A = L(M_j^A) \}$$

であるから、或る F_j は nowhere dense でない。よって、或る $[u]$ に対し

$$\forall v ([v] \subseteq [u] \text{ ならば } [v] \cap F_j \neq \emptyset), \text{ i.e.,}$$

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

$$\therefore \mu(\neg E) \geq \mu(F_j) \geq \mu([u]).$$

補題1により $\mu(\neg E) = 0$ であるから、不合理。よって、 E は comeager でない。□

定理 D. クラス SEP は comeager である。

証明. $E_k = \{ A : L_{k+1}^A \in PP[A, k] \}$ とおくと、定理C の証明により、 $\mu(E_k) = 0$ 。従って、補題2により、 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、 $\neg BPP_k \subseteq E_k$ 。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、

$$BPP \neq DSPACE(\text{lin}) \quad BPP \neq NSPACE(\text{lin}),$$

$$BPP \neq DEXT, \quad BPP \neq NEXT$$

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、原問題はなかなか困難な問題である。

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.