数理解析研究所講究録
833巻 1993年 197-203

確率について或一様性を以って相対化した BPP について

法政大工　田中尚夫（Hisao Tanaka）

梗概　Bennett-Gill は [BG 81] において

$\{X : \mathbf{P}[X] \neq \mathbf{BPP}[X]\}$ は co-meager であるか ？

と問うた．本論文はこの問題への一つのアプローチを試みるのが目的である．問題は未解決のままである．

§1．準備．

$\Sigma = \{0, 1\}$，$\Sigma^* = \Sigma$上の strings 全体の集合 とし，そのメンバーの

(1)　　$\lambda, 0, 1, 00, 01, 10, 11, 000, \ldots$

なる enumeration の n+1 番目の string を z_n で表す．

$X \subseteq \Sigma^*$ は特性関数あるいは（z_n を介して）数論的関数とみる．$\mathbf{P}(\Sigma^*) = 2^{\Sigma^*}$ は Cantor space で，かつ確率測度 μ をもつ．$\mathbf{E} \subseteq 2^{\Sigma^*}$ が nowhere dense（疎）であるとは，（後出の記号法を使用して）どんな basic open set $\langle U \rangle$ についても $\langle V \rangle \subseteq \langle U \rangle$ かつ $\langle V \rangle \cap \mathbf{E} = \phi$ となる basic open set $\langle V \rangle$ が存在すること．$\mathbf{E}$ が 可算個の nowhere dense sets の和集合であるとき，$\mathbf{E}$ は meager set（Baire の第一類集合）であるといい，その補集合を co-meager set という．meager set は字義通り‘痩せた’集合で，測度論の measure 0 に対応する．しかし全面的に対応しているわけではなく，よく知られているように measure 0 かつ comeager という集合が存在する．Complexity theory におけるかかる一例は Dowd の論文 [Do 92] に見られる．

M_i^X は i-th probabilistic polynomial time bounded oracle Turing machine (prob.p.t.b.OTM) で，その非決定ステップは２つの枝分れとする[Sch 85]．

入力 u に対し $M_i^X(u) = a \in \{0,1\}$ とする．

$Prob[\ M_i^X(u) = a\ ]$ = この machine が値 a で停止する確率．

このとき

$\mathbf{BPP}[X]$ =

$$\{\ A : \exists i \exists e\ (0<e<1/2) \forall u\ (\ prob[\ M_i^X(u) = A(u)\ ] > (1/2)+e\ )\ \}.$$

$\mathbf{P}[X]$ はよく知られているクラスである．

Bennett-Gill([BG 81]) は “ $\mathbf{E} = \{X : \mathbf{P}[X] \neq \mathbf{BPP}[X]\}$ は measure 0 である ” ことを証明し，$\mathbf{E}$ が comeager である可能性を述べた． 本論文はこの問題即ち

問題([BG 81])： $\mathbf{E}$ は co-meager であるか？

への一つのアプローチを試みるのが目的である． 結果は

定理 もし $\mathbf{P}[A] \neq \mathbf{BPPU}[A]$ なる oracle A が存在すれば，クラス $\mathbf{E}$ は co-meager である．

ここに現われる $\mathbf{BPPU}[X]$ については後述する．

§２．Poizat の仕事の概略．

[Po 86] の結果を利用するため，Poizat の仕事の概略を説明する． 彼の論文を調べると，forcing の性質のうち使わずにすむものがあり，そういった余計な部分を省き(多少の見過ごしを正し)使い易い形に焼き直したものを述べる．

$u \in \Sigma^*$ ， $X \in 2^{\Sigma^*}$ とし， $\varphi(X)(u)$, $\psi(X)$ は arithmetical predicates ([Ro 67]を参照) とする． 例えば

$\phi_i(X)(u) \Leftrightarrow \mathrm{prob}[\, M_i^X(u) = 1 \,] > 3/4,$

$\psi(X) \Leftrightarrow \forall u\, (\phi_i(X)(u) \longleftrightarrow \phi_k(X)(u))$

は本論文で取り扱う形の arithmetical predicates の例である.

一般に arithmetical predicates ψ, ϕ に対して

$\langle\psi\rangle = \{ X : \psi(X) \text{ holds} \},$

$\phi[X] = \{ u : \phi(X)(u) \text{ holds} \}.$

と定義する. 前者は 2^{Σ^*} の部分クラスであり, 後者は Σ^* の部分集合である. ψ が arithmetical だから, $\langle\psi\rangle$ は有限次の Borel 集合である.

$G \subseteq \Sigma^*$ が generic とは, 全ての arith. pred. $\psi(X)$ に対して,

$$\langle\psi\rangle \text{ is co-meager} \Rightarrow \psi(G) \text{ holds}$$

が成り立つこと.

通常 arithmetic においては, 先に forcing relation を定義して, それを用いて generic set を定義する. ここでは, forcing relation とは独立に generic set (oracle) が定義される.

Forcing condition : $U = (U_0, U_1)$. ここに, U_0 と U_1 は Σ^* の disjoint finite subsets. かかる U に対して

$$\langle U\rangle = \{ X : U_0 \subseteq X \text{ and } X \cap U_1 = \phi \}$$

とする. $\langle U\rangle$ たち全体は Cantor space 2^{Σ^*} の 開基をなす.

U forces $\psi(X)$ ($U \Vdash \psi(X)$) とは, $\langle U\rangle \cap \langle \neg\psi\rangle$ が meager であること. 従って

$$U \Vdash \psi(X) \Rightarrow \psi(G) \text{ holds for all generic } G$$

が成り立つ. 容易にわかるように

命題 2.1. Generic oracles の全体は co-meager である.

$\phi(X)(u)$ が finitely testable (f.t.)とは，或 $\alpha: N \to N$ があって，

$$\forall u \forall X \forall n \geqq \alpha(|u|)[\phi(X)(u) \longleftrightarrow \phi(X|n)(u)]$$

が成立すること． ここに，$X|n$ は X の n-initial segment を表す．

ここでは，f.t. predicates のみを取り扱うので，通常のような方法，即ち forcing relation を 帰納的に定義しそれが arithmetize 出来ることを証明するという方法，を必要としない． 我々の議論が簡潔なのはそのためである．

補題 2.2. $\psi(X)(u)$ と $\phi(X)(u)$ は f.t. arith. preds., U は forc. cond. とする． もし $U \Vdash \forall u(\psi(X)(u) \longleftrightarrow \phi(X)(u))$ ならば，すべての $X \in \langle U \rangle$ について

$$\forall u(\psi(X)(u) \longleftrightarrow \phi(X)(u))$$

が成り立つ．

さて一般に，$C(X)$ を arith. pred. たちの任意の集合とし，

$$C[X] = \{ A : A = \phi[X] \text{ for some } \phi \text{ in } C(X) \}$$

とおく．

Poizat の条件：

Hyp.1. $C(X)$ の pred. は f.t. である．

Hyp.2. $X \fallingdotseq Y \Rightarrow C[X] = C[Y]$.

Hyp.3. $A \in C[X] \ \& \ B \fallingdotseq A \Rightarrow B \in C[X]$.

Hyp.4. 次のような写像 $\# : 2^{\Sigma^*} \to 2^{\Sigma^*}$ がある：(a) $C[X] = C[\#X]$, (b) $A \in C[X]$ なる各 A に対し次のような $\psi \in C(X)$ がある：(b1) $A = \psi[\#X]$, (b2) $Y \fallingdotseq \#Z \Rightarrow \psi[Y] \fallingdotseq \psi[\#Z]$.

このとき 補題 2.2 などを使って次の定理が証明される：

THE POIZAT THEOREM. $C(X)$ と $D(X)$ が同じ写像 # を以って Hyp.1 ～

Hyp.4 を満たすとし，更に $C[A] \neq D[A]$ なる A が存在するとする． このとき

$$C[G] \neq D[G] \quad \text{for every generic } G$$

が成り立つ． 従って，$\{ X : C[X] \neq D[X] \}$ は co-meager である．

§3. BPPU[X] の導入.

Indecies の集合 I を次式で定義する．

$I = \{ \langle i,e \rangle : (\ e$ は $0<e<(1/2)$ なる有理数) & ((2) が成立する) $\}$.

ここで，(2) は次の条件である：

(2) $\forall X \forall u(\mathrm{prob}[M_i^X(u)=1] > (1/2)+e \ \text{ or } \ \mathrm{prob}[M_i^X(u)=0] > (1/2)+e\ )$.

I の複雑さは後の議論に影響しない．

各 $\langle i,e \rangle \in I$ に対し

$$\phi_{\langle i,e \rangle}(X)(u) \quad \Leftrightarrow \quad \mathrm{prob}[M_i^X(u)=1] > (1/2)+e$$

とする． このとき次のように定義する：

$$\mathbf{BPPU}(X) = \{ \phi_{\langle i,e \rangle}(X)(u) : \langle i,e \rangle \in I \},$$

$$\mathbf{BPPU}[X] = \{ \phi_{\langle i,e \rangle}[X] : \langle i,e \rangle \in I \}.$$

前者は arith. preds. の或集合，後者は Σ^* の部分集合たちの或クラスである．
明らかに次の関係が成り立つ：

$$\mathbf{BPP} \subseteq \mathbf{BPPU}[X] \subseteq \mathbf{BPP}[X] \quad \text{for every } X,$$

$$\mathbf{BPP} = \mathbf{BPPU}[\phi],\ \text{ただし } \phi \text{ は空集合.}$$

$\mathbf{P}(X)$ 及び $\mathbf{P}[X]$ も上と同様に定義される． 明らかに任意の X に対して

$\mathbf{P}[X] \subseteq \mathbf{BPPU}[X]$　　である．

[BGS75] の定理３の証明を少し変更すれば $L(A) \in \mathbf{BPP}[A] - \mathbf{P}[A]$ なる oracle A が得られる．　ここに

$$L(A) = \{ u : \exists y \in A \ (|u|=|y|) \}.$$

しかしこのとき $L(A)$ を受理する prob.p.t.b.OTM with oracle A　は この oracle A に強く依存するものであり，(2) における uniformity をもっていない．

定理(再掲)　$\mathbf{P}[A] \neq \mathbf{BPPU}[A]$ なる oraxle A が存在すれば，クラス $\{ X : \mathbf{P}[X] \neq \mathbf{BPPU}[X] \}$ は co-meager であり，従って $\{ X : \mathbf{P}[X] \neq \mathbf{BPP}[X] \}$ も comeagerである．

証明は $\mathbf{P}(X)$ と $\mathbf{BPPU}(X)$ が同一の或写像 # について，Poizat の 条件 Hyp.1～Hyp.4 を満たすことを示すことにある．　Hyp.4 の証明がやや面倒である．

§ 4．結語．

Bennett-Gill の問題への一つのアプローチとして $\mathbf{BPPU}[X]$ を導入し，Poizat の定理を利用した．　その際 Poizat の方法の簡易化を行なった．

予想　：　$\mathbf{P}[A] \neq \mathbf{BPPU}[A]$ なる oracle A　が存在する．

この予想が正しいならば，冒頭の Bennett-Gill の問題は肯定的に解決される．

なお，$\mathbf{P}[B] = \mathbf{BPPU}[B]$ なる oracle B の存在は自明である．

本論文では証明をすべて省略したが，同じ標題をもつ証明付き論文が用意されている．

文　　献

[BGS75] Baker-Gill-Solovay, Relativizations of the P=?NP question, SIAM J. Comput., 4 (1975), 431-442.

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

[Do 92] Dowd,M., Generic oracles, uniform machines, and codes, Inf. and Comput. 96 (1992), 65-76.

[Po 86] Poizat,B., Q=NQ ?, J.Symb.Logic, 51 (1986), 22-32.

[Ro 67] Rogers,H.Jr.,Theory of recursive functions and effective computability, McGraw-Hill, New York (1967).

[Sch85] Schöning,U., Complexity and structure, Springer-Verlag, LN in Comput. Sci. 211 (1985).