J. Math. Soc. Japan
Vol. 49, No. 1, 1997

On relativized probabilistic polynomial time algorithms

By Hisao TANAKA*) and Masafumi KUDOH

(Received Dec. 16, 1994)

Let $\boldsymbol{SEP}_B=\{X\subseteq\Sigma^*: \boldsymbol{P}[X]\neq\boldsymbol{BPP}[X]\}$. Bennett-Gill [**BG 81**] show that, in the Cantor space 2^{Σ^*}, $\boldsymbol{SEP}_B$ is of measure zero, and conjectured the possibility that it may be comeager. (In complexity theory there is such an example: Dowd [**Do 92**] shows that the class of m-generic oracles is of measure zero and is comeager.) We give partial answer to this possibility. Namely, we show that (i) there is a recursive oracle H such that the class $\{X: \boldsymbol{P}[X]\neq\boldsymbol{BPP}[H\oplus X]\}$ is comeager, and (ii) if we assume the existence of an oracle with an appropriate property, then the class $\boldsymbol{SEP}_B$ is comeager. These two things also hold for the class $\boldsymbol{SEP}_D=\{X: \boldsymbol{P}[X]\neq\boldsymbol{NP}[X]\cap\boldsymbol{coNP}[X]\}$. Proofs use forcing method due to Poizat [**Po 86**] with some modification. However, we do not know whether $\boldsymbol{SEP}_D$ is comeager. If $\boldsymbol{SEP}_D$ contains all generic oracles (thence it is comeager), then we would have $\boldsymbol{P}\neq\boldsymbol{NP}$, by a theorem of Blum-Impagliazzo [**BI 87**]. In the last section we state the *raison d'etre* for the above (i).

§1. Introduction.

For $X\subseteq\Sigma^*$, let $\boldsymbol{C}[X]$ and $\boldsymbol{D}[X]$ be relativized complexity classes, and let $\boldsymbol{E}(\boldsymbol{C}, \boldsymbol{D})=\{X: \boldsymbol{C}[X]\neq\boldsymbol{D}[X]\}$. Then, how large (or small) is $\boldsymbol{E}(\boldsymbol{C}, \boldsymbol{D})$? For example, $\boldsymbol{E}(\boldsymbol{P}, \boldsymbol{NP})$ has measure 1 [**BG 81**] and is comeager (e.g., [**Po 86**]), where $\boldsymbol{P}[X]$ and $\boldsymbol{NP}[X]$ are deterministic and nondeterministic polynomial time complexity classes relativized by oracle X, respectively. Now, consider the class

$$\boldsymbol{SEP}_B=\boldsymbol{E}(\boldsymbol{P}, \boldsymbol{BPP})=\{X: \boldsymbol{P}[X]\neq\boldsymbol{BPP}[X]\},$$

where $\boldsymbol{BPP}[X]$ is the class of sets accepted by probabilistic polynomial time bounded oracle Turing machines with oracle X whose error probability is bounded above by some positive rationals less than 1/2. Bennett-Gill [**BG 81**] showed, among other things, that the class $\boldsymbol{SEP}_B$ has measure zero and conjectured that it may be comeager.

In this paper, we show that it is the case if $\boldsymbol{BPP}[X]$ is relativized by an appropriate oracle H. Namely, let

* This research was partially supported by Grant-in-Aid for Scientific Research (No. 06640084), Ministry of Education, Science and Culture, Japan.

$$\boldsymbol{SEP}_B^H = \{X : \boldsymbol{P}[X] \neq \boldsymbol{BPP}[X \oplus H]\},$$

where $H \oplus X$ is the disjoint union of H and X (for its precise definition, see below). Then, we have

THEOREM 1. *There is a recursive oracle H such that $\boldsymbol{SEP}_B^H$ is comeager.*

Theorem 1 will be proved by applying some relativized form of Poizat's Theorem in [**Po 86**]. Further, we introduce at class $\boldsymbol{BPPU}[X]$ "probabilistically uniformly" relativized by X in some sense. Then we have

THEOREM 2. *The class $\boldsymbol{SEP}_B$ is comeager, provided that there exists an oracle A such that $\boldsymbol{P}[A] \neq \boldsymbol{BPPU}[A]$.*

The proof of this theorem is similar to that of Theorem 1. This two types of theorem are applicable to the following classes:

Let $\boldsymbol{\Delta}[X] = \boldsymbol{NP}[X] \cap \boldsymbol{coNP}[X]$, $\boldsymbol{SEP}_D = \{X : \boldsymbol{P}[X] \neq \boldsymbol{\Delta}[X]\}$, and let $\boldsymbol{SEP}_D^H = \{X : \boldsymbol{P}[X] \neq \boldsymbol{\Delta}[H \oplus X]\}$. Then, we can show that:

(i) there exists a recursive oracle H such that $\boldsymbol{SEP}_D^H$ is comeager, and

(ii) if there exists an oracle A such that $\boldsymbol{P}[A] \neq \boldsymbol{\Delta U}[A]$ then, $\boldsymbol{SEP}_D$ is comeager, where $\boldsymbol{\Delta U}[X]$ is an uniformly relativized class in appropriate sense. However, we do not know whether $\boldsymbol{SEP}_D$ is comeager. Blum-Impagliazzo [**BI 87**] showed that if $\boldsymbol{P} = \boldsymbol{NP}$ then $\boldsymbol{P}[G] = \boldsymbol{\Delta}[G]$ for some generic oracle G. Therefore, if $\boldsymbol{SEP}_D$ is contains all generic oracles (thence it is comeager), then we would have $\boldsymbol{P} \neq \boldsymbol{NP}$. So, it may be difficult to show that $\boldsymbol{SEP}_D$ is comeager.

§ 2. Preliminaries.

Let $\Sigma = \{0, 1\}$, and let Σ^* be the set of all strings over Σ with the empty string λ. The elements of Σ^* can be enumerated as follows:

$$(1) \qquad \lambda, 0, 1, 00, 01, 10, 11, 000, 001, \cdots.$$

We denote the $(n+1)$-st string in (1) by z_n. For $u \in \Sigma^*$, let $u = u(0)u(1) \cdots u(n-1)$, and put $|u| = n$. For $X \subseteq \Sigma^*$, let $X = X(0)X(1) \cdots X(n) \cdots$, where $X(n) = 1$ or 0 according as $z_n \in X$ or not. For $n > 0$, $X|n = X(0)X(1) \cdots X(n-1)$ (the n-segment of X). For $u \in \Sigma^*$, let $[u] = \{X : X|n = u\}$, where $n = |u|$. $\{[u] : u \in \Sigma^*\}$ is an open base for the space 2^{Σ^*}. We mainly use $u, v, w, \cdots$ for strings, $A, B, \cdots, X, Y, \cdots$ for sets (i.e., languages), and $\boldsymbol{C}, \boldsymbol{D}, \boldsymbol{E}, \cdots$ for classes (i.e., sets of sets).

Let $M^{\sim}$ be a probabilistic polynomial time bounded oracle Turing machine (abbreviated by prob p-time OTM). Assume that each nondeterministic step of $M^{\sim}$ has two possible branches each of which has probability 1/2. For any string u and any oracle X, let $M^X(u)$ be the output of the machine $M^\sim$ on the input u with oracle X. The range of output is $\{0, 1\}$, where 1 denotes the acceptance and 0 the rejection. Let $\mathrm{Prob}[M^X(u)=a]$ be the probability that M^X on u halts in the a-state, where $a\in\{0, 1\}$.

Let $M_k^\sim$ be the k-th prob p-time OTM. Then, a set A is in the class $\boldsymbol{BPP}[X]$ if there is an index k and a binary finite rational e $(0<e<1/2)$ such that for any string u

$$\mathrm{Prob}[M_k{}^X(u) = A(u)] > (1/2)+e.$$

A is in $\boldsymbol{R}[X]$ if there are a k and an e $(0<e<1/2)$ such that for any u

$$u \in A \quad \text{iff } \mathrm{Prob}[M_k{}^X(u) = 1] > (1/2)+e,$$

and

$$u \notin A \quad \text{iff } \mathrm{Prob}[M_k{}^X(u) = 0] = 1.$$

For more information, see [**BGD 88**], [**BGD 90**], [**Pa 94**], and [**Sch 85**].

To show our theorems, we apply Poizat's Theorem and its some relativized form. So we explain part of Poizat's paper [**Po 86**] with some modification.

Let $\boldsymbol{C}$ be a class: $\boldsymbol{C}\subseteq 2^{\Sigma^*}$. $\boldsymbol{C}$ is *dense* if it intersects every basic open set. $\boldsymbol{C}$ is *nowhere dense* if every basic open set contains a basic open set which is disjoint with $\boldsymbol{C}$. $\boldsymbol{C}$ is *meager* if it is a countable union of nowhere dense sets. $\boldsymbol{C}$ is *comeager* if it is the complement of a meager set.

Let u range over Σ^* and X over 2^{Σ^*}, and let $H\subseteq\Sigma^*$ be fixed. Consider arithmetical or arithmetical-in-H predicates of the forms $\phi(X)(u)$, $\phi^H(X)(u)$, $\xi(X)$, and $\xi^H(X)$. For the definition of an arithmetical predicate, see [**Ro 67**]. Examples are given as follows: Consider two machines $M_j^\sim$ and $M_k^\sim$. Let

$$\phi(X)(u) \equiv \mathrm{Prob}[M_j{}^X(u) = 1] > 3/4,$$

and

$$\xi^H(X) \equiv : \forall u[\mathrm{Prob}[M_j{}^X(u) = 1] > 3/4 \longleftrightarrow \mathrm{Prob}[M_k{}^{H\oplus X}(u) = 1] > 3/4]$$

where $H\oplus X=\{y0: y\in H\}\cup\{x1: x\in X\}$ (called the *disjoint union* of H and X). The former is an arithmetical predicate with respect to X and u, and the latter is an arithmetical-in-H predicate with respect to X. For such predicates, let

$$\phi[X] = \{u\in\Sigma^* : \phi(X)(u) \text{ holds}\}, \quad \langle\xi\rangle = \{X\subseteq\Sigma^* : \xi(X) \text{ holds}\},$$

$$\phi^H[X] = \{u : \phi^H(X)(u) \text{ holds}\}, \quad \langle\xi^H\rangle = \{X : \xi^H(X) \text{ holds}\}.$$

The left hands are sets of strings while the right hands are Borel sets of finite order in the space 2^{Σ^*}.

Let G be an oracle, i.e., a subset of Σ^*. G is *H-generic* if, for all arithmetical-in-H predicates of the form $\xi^H(X)$, $\xi^H(G)$ holds whenever $\langle\xi^H\rangle$ is comeager. Such a G exists; in fact, the class $\boldsymbol{G}^H$ of all H-generic oracles is comeager, since G^H is a countable intersection of comeager sets: $G^H = \cap\{\langle\xi^H\rangle : \langle\xi^H\rangle$ is comeager $\wedge$ ξ^H is arithmetical-in-$H\}$. (Clearly there is such an arithmetical-in-H predicate ξ that $\langle\xi^H\rangle$ is comeager.)

Let $u \in \Sigma^*$. We regard u as a *forcing condition.* u *H-forces* $\xi^H(X)$ (denoted by $u \Vdash \xi^H(X)$) if $[u] \cap \langle\neg\xi^H\rangle$ $(=[u]-\langle\xi^H\rangle)$ is meager. So, if $u \Vdash \xi^H(X)$, then $\xi^H(G)$ holds for every H-generic G in $[u]$. Because, letting $\theta^H(X) \equiv (X \notin [u] \vee \xi^H(X))$, $\theta^H(X)$ is an arithmetical-in-H and $\langle\theta^H\rangle$ is comeager. As basic properties for forcing and generic notions we know the following ([**Po 86**; p. 24]):

FACT 1. For every u, there is an H-generic set G such that $G \in [u]$. For, since G^H is comeager, $[u] \cap G^H \neq \phi$.

FACT 2. If G is H-generic and $\xi^H(G)$ is true, where $\xi^H(X)$ is an arithmetical-in-H predicate, then there is a u such that $G \in [u]$ and $u \Vdash \xi^H(X)$. For, put $\zeta^H(Y) = \exists u(Y \in [u] \wedge u \Vdash \xi^H(X))$. Since the relation "$u \Vdash \xi^H(X)$" is arithmetical-in-$H$, so is $\zeta^H(Y)$. Then we have:

$$\forall Y\ (Y : H\text{-generic} \Rightarrow Y \in \langle\zeta^H \vee \neg\xi^H\rangle).$$

So, $G \in \langle\zeta^H \vee \neg\xi^H\rangle$. Since $\xi^H(G)$ holds, we have $\models \zeta^H(G)$. Hence, there is a u such that $G \in [u]$ and $u \Vdash \xi^H(X)$.

We mainly use *continuous* predicates $\phi(X)(u)$, i.e., for ϕ there is a number-theoretic function $\alpha : N \to N$ such that for any u and X

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

holds. Here we temporarily identify finite function $X|n$ with the full function $(X|n)^\frown 000\cdots$. Similarly for ϕ^H. So, we can weaken the notions of forcing and generic oracles by restricting predicates to such ones, though we do not do so here. (Dowd [**Do 92**] uses the notion of machine-generic oracles.)

Hereafter, we sometimes do not distinguish syntactical symbols (i.e., symbols occurred in formulas in forcing relations) with metasymbols.

LEMMA 2.1. *Let $\phi(X)(u)$ and $\theta^H(X)(u)$ be continuous arithmetical(-in-H) predicates, and let u be a forcing condition. Suppose $u \Vdash \forall y(\theta^H(X)(y) \leftrightarrow \phi(X)(y))$. Then, $\forall y(\theta^H(A)(y) \leftrightarrow \phi(A)(y))$ holds for every $A \in [u]$.*

PROOF. Suppose not. So, there is an $A \in [u]$ and a string y_0 such that $\theta^H(A)(y_0) \not\leftrightarrow \phi(A)(y_0)$. Since θ^H and ϕ are continuous, there are number-theoretic functions α and β such that for all y and X,

$$\forall n \geqq \alpha(|y|)[\theta^H(X)(y) \longleftrightarrow \theta^H(X|n)(y)],$$

and

$$\forall n \geqq \beta(|y|)[\phi(X)(y) \longleftrightarrow \phi(X|n)(y)].$$

Take an m such that $m>\max\{\alpha(|y_0|), \beta(|y_0|)\}$ and $[A|m]\subseteqq[u]$. Then, $\theta^H(A|m)(y_0)\not\leftrightarrow\phi(A|m)(y_0)$. Since $\boldsymbol{G}^H$ is comeager, $[A|m]$ contains an H-generic oracle $G_0\in[u]$. For this G_0 we have

$$(*)\qquad \neg\forall y(\theta^H(G_0)(y)\longleftrightarrow\phi(G_0)(y)).$$

Since $u\Vdash\forall y(\theta^H(X)(y)\leftrightarrow\phi(X)(y))$, $[u]\cap\langle\neg\forall y(\theta^H(X)(y)\leftrightarrow\phi(X)(y))\rangle$ is meager, and hence the union $\neg[u]\cup\langle\forall y(\theta^H(X)(y)\leftrightarrow\phi(X)(y))\rangle$ is comeager. Therefore, if G is an H-generic oracle, then that G belongs to $[u]$ implies $\forall y(\theta^H(G)(y)\leftrightarrow\phi(G)(y))$. This contradicts $(*)$. □

§3. A relativized form of Poizat's Theorem and an oracle *H*.

For any set $\boldsymbol{C}(X)$ (or $\boldsymbol{C}^H(X)$) of continuous arithmetical(-in-H) predicates of the form $\theta(X)(y)$ (or $\theta^H(X)(y)$) we define a class of sets of strings $\boldsymbol{C}[X]$ (or $\boldsymbol{C}^H[X]$) as follows:

$$\boldsymbol{C}[X]=\{A\subseteqq\Sigma^*: A=\theta[X] \text{ for some } \theta(X)(y) \text{ in } \boldsymbol{C}(X)\},$$

where, as defined in the previous section, $\theta[X]=\{y\in\Sigma^*: \theta(X)(y) \text{ holds}\}$. Note that we are severely distinguishing between $\boldsymbol{C}(X)$ and $\boldsymbol{C}[X]$. The former is a set of predicates while the latter is a class of sets of strings. Similarly for $\boldsymbol{C}^H(X)$ and $\boldsymbol{C}^H[X]$.

Let $p_k(n)$ be the time bound function for the OTM $M_k^{\sim}$, and let H be an oracle. We consider the following condition:

$$(2)\qquad \forall X\forall y(\mathrm{Prob}[M_k^{H\oplus X}(y)=1]>(1/2)+e\vee\mathrm{Prob}[M_k^{H\oplus X}(y)=0]=1),$$

and define an index-set I^H by

$$I^H=\{\langle k, e\rangle: (e \text{ is a binary rational such that } 0<e<(1/2))\wedge(2)\}.$$

(Apparently I^H is Π^1_1-in-H, but really, by using continuity of the machines or using $p_k(n)$, it is seen that this set is arithmetical-in-H. However, this observation does not affect the subsequent argument.) For example, suppose $B\in\boldsymbol{R}[H]$ and $M^{\sim}$ is a prob p-time OTM which accepts B with a rational e. Suppose, further, $P^{\sim}$ is a deterministic p-time oracle Turing transducer. Then there is an index k such that $\forall y[M_k^{H\oplus X}(y)=M^H(P^X(y))]$, and thus $\langle k, e\rangle\in I^H$.

Now, for each $\langle k, e\rangle\in I^H$, let $\phi^H_{\langle k,e\rangle}(X)(y)$ be the following arithmetical-in-H predicate:

$$\phi^H_{\langle k,e\rangle}(X)(y)\equiv:\mathrm{Prob}[M_k^{H\oplus X}(y)=1]>(1/2)+e.$$

Then, we define $RU^H(X)$ and $RU^H[X]$ by:

$$\boldsymbol{RU}^H(X)=\{\phi^H_{\langle k,e\rangle}(X)(y): \langle k, e\rangle\in I^H\},$$

and

$$\boldsymbol{RU}^H[X] = \{\theta^H[X] : \theta^H(X)(y) \in \boldsymbol{RU}^H(X)\}.$$

Clearly, $\boldsymbol{R}[H] \subseteq \boldsymbol{RU}^H[X]$ for every X. Since $X \in \boldsymbol{RU}^H[X]$, there is an oracle A such that $\boldsymbol{R}[H] \subset \boldsymbol{RU}^H[A]$. Here, $\subset$ means the proper inclusion.

The class $\boldsymbol{P}[X]$ is well-known (see, e.g., [**BGS 75**] or [**BDG 90**]). However, we must reasonably define its corresponding $\boldsymbol{P}(X)$ as a set of arithmetical predicates, for later usage. Let $P_k^{\sim}$ be the k-th deterministic p-time OTM. Define η_k as follows:

$$\eta_k(X)(y) \equiv : P_k^X \text{ accepts } y \ (\equiv P_k^X(y) = 1).$$

Clearly this predicate is arithmetical, in fact, it is recursive, and hence it is continuous. Define $\boldsymbol{P}(X) = \{\eta_k(X)(y) : k = 0, 1, 2, \cdots\}$. Then $\boldsymbol{P}[X] = \{\theta[X] : \theta(X)(y) \in \boldsymbol{P}(X)\}$.

LEMMA 3.1. (i) $\boldsymbol{RU}^H[X] = \{A : \exists \langle k, e\rangle \in I^H \forall y$
$(y \in A$ *iff* $\text{Prob}[M_k^{H \oplus X}(y) = 1] > (1/2) + e$ *and*
$y \notin A$ *iff* $\text{Prob}[M_k^{H \oplus X}(y) = 0] = 1)\}$.

(ii) $\boldsymbol{P}[X] \subseteq \boldsymbol{RU}^H[X] \subseteq \boldsymbol{R}[H \oplus X] \subseteq \boldsymbol{BPP}[H \oplus X]$. □

Let us define a recursive oracle H such that $L(H) \in \boldsymbol{R}[H] - \boldsymbol{P}[H]$, where $L(H) = \{0^n : \exists y \in H(|y| = n)\}$. Let $n_0 = 0$, and $H(0) = \phi$ (the empty set). This time let $H(s)$ be the set of strings put in H before stage s. (Note that it is not the characteristic function of H.)

Stage $s \geqq 0$. Let m_s be the least $m > n_s$ such that $p_s(m) < 2^{m-2}$. Run $P_s^{H(s)}$ on 0^{m_s}. If it rejects the string, then we choose $2^{m_s - 1} + 2^{m_s - 2} + 1$ strings of length m_s which are not queried during the computation, and add these strings to $H(s)$ to make $H(s+1)$. Such strings exist. If it accepts the string, then let $H(s+1) = H(s)$. Put $n_{s+1} = 2^{m_s}$. Then, the set $H = \cup \{H(s) : s = 0, 1, 2, \cdots\}$ is the desired oracle.

For this oracle H, we have: $L(H) \in \boldsymbol{RU}^H[X]$ for all X. For, let $M_k^{H \oplus X}$ be a prob OTM such that: on 0^n it randomly writes a string of length n on its oracle tape and suffixies 0 to it; then it enters the query state; if the queried string is in $H \oplus X$, then the machine accepts the input, otherwise it rejects. This machine is p-time bounded and its probability is independent of the oracle X. So, the index $\langle k, 1/4\rangle$ is in I^H, and hence we have the following lemma:

LEMMA 3.2. *There is a recursive oracle H such that*

$$L(H) \in \boldsymbol{RU}^H[X] - \boldsymbol{P}[H] \quad \textit{for all } X. \qquad \square$$

Later we shall use this H.

Now, let $\boldsymbol{C}(X)$ $(\boldsymbol{C}^H(X))$ be a set of arithmetical(-in-H) predicates of the form $\phi(X)(y)(\phi^H(X)(y))$ and let $\boldsymbol{C}[X]$ $(\boldsymbol{C}^H[X])$ be its corresponding class of sets. For $X, Y \subseteqq \Sigma^*$, $X \doteqdot Y$ means that X and Y are identical but finitely many members. The following conditions are Poizat's four hypotheses for $\boldsymbol{C}(X)$ (here we add ones for relativized classes also):

HYPOTHESIS 1. Each predicate in $\boldsymbol{C}(X)$ $(\boldsymbol{C}^H(X))$ is continuous.

HYPOTHESIS 2. If $X \doteqdot Y$, then $\boldsymbol{C}[X]=\boldsymbol{C}[Y]$ $(\boldsymbol{C}^H[X]=\boldsymbol{C}^H[Y])$.

HYPOTHESIS 3. If $A \in \boldsymbol{C}[X]$ $(\in \boldsymbol{C}^H[X])$ and if $B \doteqdot A$, then $B \in \boldsymbol{C}[X]$ $(\in \boldsymbol{C}^H[X])$.

HYPOTHESIS 4. There is a mapping $\# : 2^{\Sigma^*} \to 2^{\Sigma^*}$ such that (a) $\boldsymbol{C}[X]=\boldsymbol{C}[\#X]$ $(\boldsymbol{C}^H[X]=\boldsymbol{C}^H[\#X])$, and (b) for any $A \in \boldsymbol{C}[X]$ $(\in \boldsymbol{C}^H[X])$ there is a predicate θ in $\boldsymbol{C}(X)$ $(\theta^H$ in $\boldsymbol{C}^H(X))$ such that $A=\theta[\#X]$ $(=\theta^H[\#X])$ and it has the following property: if $Y \doteqdot \#Z$, then $\theta[Y] \doteqdot \theta[\#Z]$ $(\theta^H[Y] \doteqdot \theta^H[\#Z])$. (We slightly modify Poizat's Hypothesis 4.)

Then,

A relativized version of Poizat's Theorem.

Let H be an oracle. Let $\boldsymbol{C}(X)$ $(\boldsymbol{D}^H(X))$ be a set of arithmetical(-in-H) predicates of the form $\phi(X)(y)$ $(\theta^H(X)(y))$ which satisfies the Hypotheses 1~4 with the same mapping: $X \to \#X$. $\boldsymbol{C}[X]$ $(\boldsymbol{D}^H[X])$ is its corresponding class of sets. Suppose that there exists an oracle A such that $\boldsymbol{D}^H[A]-\boldsymbol{C}[A] \neq \phi$. Then, $\boldsymbol{C}[G] \neq \boldsymbol{D}^H[G]$ for every H-generic oracle G, and hence

$$\boldsymbol{E}(\boldsymbol{C}, \boldsymbol{D}^H) = \{X : \boldsymbol{C}[X] \neq \boldsymbol{D}^H[X]\}$$

is comeager.

PROOF. Take a $B \in \boldsymbol{D}^H[A]-\boldsymbol{C}[A]$. Then, by Hypothesis 4, there is a predicate θ^H in $\boldsymbol{D}^H(X)$ such that $B=\theta^H[\#A]$ and such that

$$(3) \qquad Y \doteqdot \#Z \Longrightarrow \theta^H[Y] \doteqdot \theta^H[\#Z].$$

CLAIM. For any predicate $\phi(X)(y)$ in $\boldsymbol{C}(X)$, if G is H-generic, then $\neg \forall y$ $(\theta^H(G)(y) \leftrightarrow \phi(G)(y))$ holds.

PROOF. Suppose not. Then, there is a predicate $\phi(X)(y)$ in $\boldsymbol{C}(X)$ and an H-generic G_0 such that $\forall y$ $(\theta^H(G_0)(y) \leftrightarrow \phi(G_0)(y))$ holds. Put $\xi^H(X) \equiv \forall y$ $(\theta^H(X)(y) \leftrightarrow \phi(X)(y))$. Then, $\xi^H(G_0)$ holds. By H-genericity of G_0, $\langle \xi^H \rangle$ is not meager. So, by the Baire property for $\langle \xi^H \rangle$, for some forcing condition u, $[u] \cap \langle \neg \xi^H \rangle$ is meager. Hence, $u \Vdash \xi^H(X)$, i.e., $u \Vdash \forall y$ $(\theta^H(X)(y) \leftrightarrow \phi(X)(y))$. So, by Lemma 2.1, we have

(4) $\forall Y\ (Y \in [u] \longrightarrow \forall y\ (\theta^H(Y)(y) \longleftrightarrow \phi(Y)(y)))$.

For the above A, we consider its image $\#A$ and take an $S \in [u]$ such that $S \doteq \#A$. Then, $\theta^H[S] \doteq \theta^H[\#A]$. Since $S \in [u]$, by (4) we have $\forall y\ (\theta^H(S)(y) \leftrightarrow \phi(S)(y))$. Let $Z = \theta^H[S]$. Then, $Z = \phi[S]$. So, $Z \in \boldsymbol{C}[S] = \boldsymbol{C}[\#A]$ (by Hyp. 2). As seeing above we have $\theta^H[S] \doteq \theta^H[\#A]$, and hence $Z \doteq B$. Since $Z \in \boldsymbol{C}[\#A]$, by Hyp. 3 we have $B \in \boldsymbol{C}[\#A]$. Since by Hyp. 4, $\boldsymbol{C}[\#A] = \boldsymbol{C}[A]$, we have $B \in \boldsymbol{C}[A]$. This contradicts the assumption $B \notin \boldsymbol{C}[A]$. So, the proof of the claim completes.

The claim states: If G is an H-generic oracle, then

$$\theta^H[G] \neq \phi[G] \quad \text{for any predicate } \phi(X)(y) \text{ in } \boldsymbol{C}(X).$$

So, $\theta^H[G]$ does not belong to $\boldsymbol{C}[G]$ for any H-generic G. Therefore, for all H-generic G $\boldsymbol{D}^H[G] \neq \boldsymbol{C}[G]$. Since the class $\boldsymbol{G}^H$ of all H-generic oracles is comeager, so is $\boldsymbol{E}(\boldsymbol{C}, \boldsymbol{D}^H) = \{X : \boldsymbol{C}[X] \neq \boldsymbol{D}^H[X]\}$. □

§4. Proof of Theorem 1.

Consider the class $\boldsymbol{E}(\boldsymbol{P}, \boldsymbol{RU}^H)$ $(= \{X : \boldsymbol{P}[X] \neq \boldsymbol{RU}^H[X]\})$, then $\boldsymbol{E}(\boldsymbol{P}, \boldsymbol{RU}^H) \subseteq \{X : \boldsymbol{P}[X] \neq \boldsymbol{R}[H \oplus X]\} \subseteq \boldsymbol{SEP}_B{}^H$ $(= \{X : \boldsymbol{P}[X] \neq \boldsymbol{BPP}[H \oplus X]\})$. Therefore, if it is shown that $\boldsymbol{E}(\boldsymbol{P}, \boldsymbol{RU}^H)$ is comeager for some recursive H, then so is $\boldsymbol{SEP}_B{}^H$ for the same H, and hence we obtain Theorem 1. So, for our purpose, by the relativized Poizat's Theorem, it suffices to show that $\boldsymbol{P}(X)$ and $\boldsymbol{RU}^H(X)$ satisfy Hypotheses 1~4 for the H in Lemma 3.2 with the same mapping $\#$ defined below, since $\boldsymbol{E}(\boldsymbol{P}, \boldsymbol{RU}^H)$ is not empty for this H (in fact, it contains the H as an element).

Here we show this for $\boldsymbol{RU}^H(X)$ with the mapping $\# : X \to \#X$, where $\#X = \pi(\Sigma^*, X)$ and π is an *one-to-one* pairing function from $\Sigma^* \times \Sigma^*$ *onto* Σ^* which is polynomial time computable and is polynomial time invertible. The proof for $\boldsymbol{P}(X)$ can be understood in the course of the following argument.

HYPOTHESIS 1. For $\phi^H_{\langle k, e \rangle}$, where $\langle k, e \rangle \in I^H$, we can take $\alpha(n) = 2^{p_k(n)+1} - 1$ in the definition of continuity, since the maximal number of strings of length m in the enumeration (1) is $2^{m+1} - 2$.

HYPOTHESIS 2. Suppose $X \doteq Y$, and let $A \in \boldsymbol{RU}^H[X]$. So, there is an index $\langle k, e \rangle \in I^H$ such that for all y and Z $\text{Prob}[M_k{}^{H \oplus Z}(y) = 1] > (1/2) + e$ or $\text{Prob}[M_k{}^{H \oplus Z}(y) = 0] = 1$ holds, and $y \in A$ iff $\text{Prob}[M_k{}^{H \oplus X}(y) = 1] > (1/2) + e$. Since $X \doteq Y$, there is a linear time bound OTM $P^{\sim}$ such that $X = P^Y$. Then, we can construct a prob p-time OTM $M_j{}^{\sim}$ preserving the probability, i.e., such that for any Z $\text{Prob}[M_k{}^{H \oplus P^Z}(y) = a] = \text{Prob}[M_j{}^{H \oplus Z}(y) = a]$ for all $a \in \{0, 1\}$ and y. So, we have $\langle j, e \rangle \in I^H$ and hence $A \in \boldsymbol{RU}^H[Y]$. Thus, $\boldsymbol{RU}^H[X] \subseteq \boldsymbol{RU}^H[Y]$.

The proof of the reverse inclusion is similar.

HYPOTHESIS 3. Suppose $A \in \boldsymbol{RU}^H[X]$ and $B \doteq A$. We show $B \in \boldsymbol{RU}^H[X]$. By the supposition, there are an index $\langle k, e\rangle \in I^H$ and a number m such that for any input y

$$(5) \qquad y \in A \text{ iff } \mathrm{Prob}[M_k^{H \oplus X}(y) = 1] > (1/2) + e,$$

$$(6) \qquad y \notin A \text{ iff } \mathrm{Prob}[M_k^{H \oplus X}(y) = 0] = 1,$$

and

$$(7) \qquad \forall n \geqq m \ (B(n) = A(n)).$$

Recall $A(n)=1$ if $z_n \in A$, $A(n)=0$ otherwise. We shall define a p-time OTM $M_j^{\sim}$ such that $\langle j, e\rangle \in I^H$ and such that for all y

$$(8) \qquad y \in B \text{ iff } \mathrm{Prob}[M_j^{H \oplus X}(y) = 1] > (1/2) + e,$$

$$(9) \qquad y \notin B \text{ iff } \mathrm{Prob}[M_j^{H \oplus X}(y) = 0] = 1.$$

We use the notation ' ' defined by 'z_n'$=n$. First of all, we define a segment of the OTM $M_j^{\sim}$ by a finite table so that for every y with 'y'$<m$ the segment satisfies (8) and (9) as well as the following condition: for every oracle Z

$$(10) \qquad \text{either } \mathrm{Prob}[M_j^{H \oplus Z}(y) = 1] > (1/2) + e \text{ or } \mathrm{Prob}[M_j^{H \oplus Z}(y) = 0] = 1.$$

On any input y with 'y'$\geqq m$, $M_j^{H \oplus Z}$ simulates $M_k^{H \oplus Z}$ so that $M_j^{H \oplus Z}(y) = M_k^{H \oplus Z}(y)$ holds. Then, by (5) and (6) we have (8) and (9) for these y and the X. Such an index j exists and $\langle j, e\rangle \in I^H$. Thus, $B \in \boldsymbol{RU}^H[X]$.

HYPOTHESIS 4. We must show that the same mapping $X \to \# X$, where $\# X = \pi(\Sigma^*, X)$, satisfies the following conditions (a) and (b):

(a) $\boldsymbol{RU}^H[X] = \boldsymbol{RU}^H[\# X]$.

PROOF. Let X be fixed, and suppose $A \in \boldsymbol{RU}^H[X]$. Then, we must show $A \in \boldsymbol{RU}^H[\# X]$. By the supposition, there is an index $\langle k, e\rangle \in I^H$ such that for any y (5) and (6) hold. Then, we will find an index j such that $\langle j, e\rangle \in I^H$ and such that for any y

$$(11) \qquad y \in A \text{ iff } \mathrm{Prob}[M_j^{H \oplus \# X}(y) = 1] > (1/2) + e,$$

and

$$(12) \qquad y \notin A \text{ iff } \mathrm{Prob}[M_j^{H \oplus \# X}(y) = 0] = 1$$

hold. For this purpose, we define an OTM $M_j^{\sim}$ (call it j-machine) as follows: Let $Y \subseteq \Sigma^*$ be arbitrary and let $\rho(Y) = \{v : \exists y, w[w \in Y \wedge w = \pi(y, v)]\}$. Then

$\rho(Y)=X$ if $Y=\#X$. Now, given input y, the j-machine begins to simulate the computation of $M_k^{H\oplus\sim}(y)$. Suppose $M_k^{H\oplus\sim}$ enters the query state. Let x be the queried string. Then, the j-machine checks the tail end letter of x. If the letter is 0, then the j-machine enters yes-state or no-state according as $x'\in H$ or not, where x' is the string obtained from x by deleting the tail letter. If it is 1, then the j-machine writes $\pi(y, x')$ on its oracle tape (this work can be done in time $O(p_k(|y|))$), and queries whether $\pi(y, x')1\in H\oplus Y$. If the answer is yes, then $x'\in\rho(Y)$ and so the j-machine simulates the yes-branch of the computation of $M_k^{H\oplus\sim}(y)$. Otherwise, it simulates the no-branch. After the whole simulation ends, the j-machine outputs the value of this simulation for $M_k^{H\oplus\sim}(y)$. This is a *quasi*-simulation for $M_k^{H\oplus\rho(Y)}(y)$ (it may not be the exact one, because there can be a case that $\pi(y, x')\notin Y$ but for some other u $\pi(u, x')\in Y\wedge x'\in\rho(Y)$). If $Y=\#Z$ for some Z, then the output of j-machine is the same as that of $M_k^{H\oplus Z}(y)$, since for any u $\pi(u, x')\in Y$ iff $x'\in Z$. The j-machine is a prob p-time OTM, so certainly such an index j exists, and it has the additional uniformity property (2). Hence $\langle j, e\rangle\in I^H$. For this j-machine, we have

$$\text{Prob}[M_j^{H\oplus\#X}(y)=a]=\text{Prob}[M_k^{H\oplus X}(y)=a]$$

for any input y and $a\in\{0, 1\}$. (Since the j-machine must be probabilistic OTM, at any time it must be binarily branching, for example, even during the calculation of $\pi(y, x')$. During such period, the machine does the same computation on each branch. So, though $M_j^{H\oplus\#X}$'s computation is longer than that of $M_k^{H\oplus X}$, the probabilities of both machines are the same.) Thus, we have $A\in\boldsymbol{RU}^H[\#X]$.

Conversely, let $A\in\boldsymbol{RU}^H[\#X]$. Then, there is an index $\langle j, e\rangle\in I^H$ such that for all y (11) and (12) hold. We define a prob p-time OTM $M_k^{\sim}$ as follows: on an input y, $M_k^{H\oplus X}$ simulates the computation of $M_j^{H\oplus\sim}$ on y. Suppose the latter machine enters the query state. Let x be the queried string. $M_k^{H\oplus X}$ checks its tail end letter. If the letter is 0, then the machine enters yes-state or no-state according as $x'\in H$ or not, where, as before, x' is the string obtained from x by deleting the tail end letter. If that letter is 1, then the machine calculates v such that $\pi(y, v)=x'$. Recall that v is uniquely determined and can be computed in polynomial time of $|x|$. Then, the machine queries whether $v\in X$ (i.e., whether $v1\in H\oplus X$). After it enters yes-state or no-state, it resumes simulating. Finally, it outputs the same value as $M_j^{\sim}$. This $M_k^{\sim}$ satisfies the desired condition. Namely, such an index k exists and $\langle k, e\rangle\in I^H$. Clearly, for any $a\in\{0, 1\}$

$$\text{Prob}[M_k^{H\oplus X}(y)=a]=\text{Prob}[M_j^{H\oplus\#X}(y)=a].$$

Thus we have $A\in\boldsymbol{RU}^H[X]$.

(b) For each $A \in \boldsymbol{RU}^H[X]$ there is a predicate $\theta^H(X)(y)$ in $\boldsymbol{RU}^H(X)$ such that (b1) $A \in \theta^H[\#X]$ and (b2) if $Y \doteq \#Z$ then $\theta^H[Y] \doteq \theta^H[\#Z]$.

PROOF. By the assumption, there is an index $\langle k, e\rangle \in I^H$ such that (5) and (6) hold. Then we take the OTM $M_j^{\sim}$ described in the proof of (a). As was shown above, we have (11) and (12). Let $\theta^H(X)(y)$ be the predicate "$\text{Prob}[M_j^{H\oplus X}(y)=1]>(1/2)+e$". Then, $\theta^H(X)(y)$ is in $\boldsymbol{RU}^H(X)$, and we have $A=\theta^H[\#X]$. Thus, (b1) is shown. To show (b2), suppose $Y \doteq \#Z$. Then, there is a number m (depending on Y and Z) such that

$$\forall y \forall v[(|y| \geqq m \text{ or } |v| \geqq m) \longrightarrow (\pi(y, v) \in Y \text{ iff } \pi(y, v) \in \#Z \text{ iff } v \in Z)].$$

So, both $M_j^{H\oplus Y}(y)$ and $M_j^{H\oplus \#Z}(y)$ are identical with $M_k^{H\oplus Z}(y)$ for any y with $|y| \geqq m$. Therefore we have $\theta^H[Y] \doteq \theta^H[\#Z]$.

Thus, we have shown that $\boldsymbol{RU}^H(X)$ satisfies Hypotheses 1~4. Similarly for $\boldsymbol{P}(X)$.

Consequently we have the following theorem:

THEOREM 1. *There is a recursive oracle H such that the class $\{X : \boldsymbol{P}[X] \neq \boldsymbol{RU}^H[X]\}$ is comeager, a fortiori so is $\boldsymbol{SEP}_B^H$.*

§ 5. Proof of Theorem 2.

As in the preceding argument, we can define $\boldsymbol{RU}(X)$ and $\boldsymbol{RU}[X]$ deleting the oracle H. Also we have the H-unrelativized versions of Lemmas 2.1, 3.1, and Poizat's Theorem. However we do not have any H-unrelativized version of Lemma 3.2. So, we must assume the following assumption:

(A) There exists an oracle A such that $\boldsymbol{RU}[A]-\boldsymbol{P}[A] \neq \phi$.

Under this assumption, we can prove that the class $\{X : \boldsymbol{P}[X] \neq \boldsymbol{RU}[X]\}$ is comeager. However, in order to obtain our Theorem 2, we must modify (A).

Let $I' = \{\langle k, e\rangle : (e \text{ is a binary rational such that } 0<e<1/2) \wedge (2')\}$, where

(2′) $\forall X \forall y(\text{Prob}[M_k^X(y)=1] > (1/2)+e \vee \text{Prob}[M_k^X(y)=0] > (1/2)+e)$.

For each $\langle k, e\rangle \in I'$, let

$$\phi_{\langle k, e\rangle}(X)(y) \equiv \text{Prob}[M_k^X(y)=1] > (1/2)+e.$$

Then

$$\boldsymbol{BPPU}(X) = \{\phi_{\langle k, e\rangle}(X)(y) : \langle k, e\rangle \in I'\},$$

and

$$\boldsymbol{BPPU}[X] = \{\xi[X] : \xi(X)(y) \in \boldsymbol{BPPU}(X)\}.$$

We can show that $\boldsymbol{BPPU}(X)$ and $\boldsymbol{BPPU}[X]$ satisfy the Hypotheses 1∼4 suppressed H. Since $\boldsymbol{BPPU}[X]\subseteq\boldsymbol{BPP}[X]$, by Poizat's Theorem, we have

THEOREM 2. *Assume*
(A′) *There exists an oracle A such that $\boldsymbol{BPPU}[A]-\boldsymbol{P}[A]\neq\phi$.*
Then, the class $\boldsymbol{SEP}_B=\{X:\boldsymbol{P}[X]\neq\boldsymbol{BPP}[X]\}$ is comeager.

By a similar argument as in the proof of Lemma 3.2, we can get an oracle A such that $L(A)\in\boldsymbol{BPP}[A]-\boldsymbol{P}[A]$. But, the probability of the prob p-time OTM with oracle A that accepts $L(A)$ depends on the oracle A, and the machine does not have the uniformity described in (2′). This is why we assume (A′).

So, Bennett-Gill's problem whether $\boldsymbol{SEP}_B$ is comeager is still open.

§6. On $\boldsymbol{NP}[X]\cap$ $\boldsymbol{coNP}[X]$.

As before, let $\boldsymbol{\Delta}[X]\equiv\boldsymbol{NP}[X]\cap\boldsymbol{coNP}[X]$. Whether the measure of

$$\boldsymbol{SEP}_D=\boldsymbol{E}(\boldsymbol{P},\boldsymbol{\Delta})=\{X:\boldsymbol{P}[X]\neq\boldsymbol{\Delta}[X]\}$$

is one is a well-known open problem. Whether $\boldsymbol{SEP}_D$ is comeager is also open. The assertion that $\boldsymbol{SEP}_D$ is comeager, by the argument in §3, seems to be considerably near the assertion that $\boldsymbol{SEP}_D$ contains all generic oracles. The latter assertion implies $\boldsymbol{P}\neq\boldsymbol{NP}$, by a result of Blum-Impagliazzo [**BI 86**]. So, whether $\boldsymbol{SEP}_D$ is comeager may be a hard problem. By reason of this account, we will take the course of argument developed in §3.

Let F be a fixed oracle. Define an index set J^F as follows:

$$J^F=\{\langle j,k\rangle:\forall X\forall y(NP_j^{F\oplus X}(y)=1\ \text{ iff }\ NP_k^{F\oplus X}(y)\neq 1)\},$$

where $NP_k^{\sim}$ is the k-th nondeterministic p-time OTM. For each $\langle j,k\rangle\in J^F$ we define the formula $\psi^F_{\langle j,k\rangle}(X)(y)$ as follows:

$$\psi^F_{\langle j,k\rangle}(X)(y)\equiv NP_j^{F\oplus X}(y)=1\ (\equiv NP_k^{F\oplus X}(y)\neq 1).$$

Then, let $\boldsymbol{\Delta U}^F(X)=\{\psi^F_{\langle j,k\rangle}(X)(y):\langle j,k\rangle\in J^F\}$, and $\boldsymbol{\Delta U}^F[X]=\{\theta^F[X]:\theta^F(X)(y)\in\boldsymbol{\Delta U}^F(X)\}$. Further, let

$$L_0(F)=\{x:\exists y(0y\in F\wedge|0y|=|x|)\}.$$

After Baker-Gill-Solovay [**BGS 75**; Theorem 7], we can construct a recursive oracle F such that $L_0(F)\notin\boldsymbol{P}[F]$ and

$$\exists y\ (0y\in F\wedge|0y|=n)\ \text{ iff }\ \neg\exists y\ (1y\in F\wedge|1y|=n) \tag{13}$$

for all n, and hence

$$(14) \qquad L_0(F) \in \boldsymbol{NP}[F] \cap \boldsymbol{coNP}[F] - \boldsymbol{P}[F].$$

LEMMA 6.1. *For the above F, we have*

$$L_0(F) \in \boldsymbol{\varDelta U}^F[X] - \boldsymbol{P}[F] \quad \textit{for all } X.$$

PROOF. We define two nondeterministic p-time OTM's $NP_j^{\sim}$ and $NP_k^{\sim}$ as follows:

$NP_j^{F\oplus\sim}$: On input x, it guesses $0y$ such that $|0y|=|x|$, and writes $0y0$ on its query tape and enters the query state. If $0y0 \in F\oplus\sim$, then it accepts x. If $0y0 \notin F\oplus\sim$ for any y such that $|0y|=|x|$, then it rejects x.

$NP_k^{F\oplus\sim}$: On input x, it guesses $1y$ such that $|1y|=|x|$, and writes $1y0$ on its query tape and enters the query state. If $1y0 \in F\oplus\sim$, then it accepts x. If $1y0 \notin F\oplus\sim$ for any y such that $|1y|=|x|$, then it rejects x.

Certainly there exist such indicies j and k. It is easy to show that for these j and k $\langle j, k\rangle \in J^F$ and $L_0(F) \in NP_j^{F\oplus X}$ for all X. Hence we have $L_0(F) \in \boldsymbol{\varDelta U}^F[X]$ for all X. □

This is the counterpart of Lemma 3.2.

By a similar argument, we can show that the $\boldsymbol{\varDelta U}^F(X)$ and $\boldsymbol{\varDelta U}^F[X]$ satisfy Hypotheses 1~4 with F instead of H. Here we show Hypothesis $2F$ only: Let $X \doteq Y$, and suppose $A \in \boldsymbol{\varDelta U}^F[X]$. So, there is $\langle j, k\rangle \in J^F$ such that $\forall y$ ($y \in A$ iff $NP_j^{F\oplus X}(y)=1$ iff $NP_k^{F\oplus X}(y) \neq 1$). For some linear time bounded OTM $T^{\sim}$ $X=T^Y$. For this T we can find indicies r and s such that

$$\forall Z \forall y (NP_j^{F\oplus T^Z}(y) = 1 \quad \text{iff} \quad NP_r^{F\oplus Z}(y) = 1)$$

and the same formula with k and s instead of j and r. So we have

$$\forall Z \forall y (NP_r^{F\oplus Z}(y) = 1 \quad \text{iff} \quad NP_s^{F\oplus Z}(y) \neq 1).$$

Thus, $\langle r, s\rangle \in J^F$ and $\forall y$ ($y \in A$ iff $NP_r^{F\oplus Y}(y)=1$). Hence we have $A \in \boldsymbol{\varDelta U}^F[Y]$. Therefore Hypothesis $2F$ holds.

By Lemma 6.1, there is an oracle A such that $\boldsymbol{\varDelta U}^F[A] \neq \boldsymbol{P}[A]$. So, by the F-relativized Poizat's Theorem, we have

THEOREM 3. *There is a recursive oracle F such that the class* $\boldsymbol{SEP}_D{}^F = \{X : \boldsymbol{P}[X] \neq \boldsymbol{NP}[F\oplus X] \cap \boldsymbol{coNP}[F\oplus X]\}$ *is comeager.*

Next, as in the proof of Theorem 2, we omit the oracle F in the above argument. Then we obtain J, $\psi_{\langle j,k\rangle}$, $\boldsymbol{\varDelta U}(X)$, and $\boldsymbol{\varDelta U}[X]$. But we do not have the F-unrelativized version of Lemma 6.1. So, we must assume the following assumption:

(B) There exists an oracle F such that $\boldsymbol{\Delta U}[F]-\boldsymbol{P}[F]\neq\phi$.

By a similar argument as above we have:

THEOREM 4. *Under the assumption* (B), *the class* $\boldsymbol{SEP}_D=\{X: \boldsymbol{P}[X]\neq\boldsymbol{NP}[X]\cap\boldsymbol{coNP}[X]\}$ *is comeager.* □

§7. Conclusion.

We have shown that there is a recursive oracle H such that the class $\{X: \boldsymbol{P}[X]\neq\boldsymbol{BPP}[H\oplus X]\}$ is comeager, and also have obtained some related results.

Now, consider the following proposition

There is an oracle H such that

(15) $$\forall X(\boldsymbol{P}[X]\neq\boldsymbol{BPP}[H\oplus X]).$$

If this proposition were true, then our Theorem 1 would be entirely trivial. But this proposition is incorrect! Namely:

LEMMA 7.1. *For each oracle H there is an oracle A such that*

$$\boldsymbol{P}[A]=\boldsymbol{BPP}[H\oplus A].$$

PROOF. Let H be given. Then, we construct an oracle A such that

(16) $$H\oplus A\equiv_{PT}A \quad\text{and}\quad \boldsymbol{P}[A]=\boldsymbol{BPP}[A].$$

So, we have: $\boldsymbol{P}[A]=\boldsymbol{BPP}[A]=\boldsymbol{BPP}[H\oplus A]$. (For $\equiv_{PT}$, see [**BDG 88**].)

Construction of an A which satisfies (16): As before, let $M_k^{\sim}$ be the k-th prob p-time OTM with the time bound $p_k(n)$. This time let $A(s)$ be the set consisting of the strings put in A before stage s, and let $A(0)=\phi$.

Stage $2s\geqq 0$. Consider the following strings w:

(17) $$w=0^k1y10^n,\ |w|=s,\ \text{and}\ n=p_k(|y|)\ \text{for some } k \text{ and } y.$$

Run $M_k^{A(2s)}$ on y. If it accepts y, i.e., Prob$[M_k^{A(2s)}(y)=1]>1/2$, then put $w1$ in A. Otherwise, i.e., Prob$[M_k^{A(2s)}(y)=0]\geqq 1/2$, then do nothing. Let A_s be the set of all strings put in A by doing the above procedure for *all such* w's satisfying (17), and let $A(2s+1)=A(2s)\cup A_s$.

If there is no such w, then let $A(2s+1)=A(2s)$.

Stage $2s+1$. If there is a string w such that $|w|=s$ and $w\in H$, then make $A(2s+2)$ by adding to $A(2s+1)$ $w0$ for *all such* w's. Otherwise, let $A(2s+2)=A(2s+1)$.

Let $A=\bigcup_{s=0}^{\infty}A(s)$. When there is a string w such that (17) holds, $M_k^{A(2s)}(y)=M_k^{A}(y)$, since lengths of queried strings in the computation are

$\leqq p_k(|y|)<s$ and lengths of strings put in A after stage $2s$ are $>s$.

CLAIM. $\boldsymbol{PP}[A]\subseteqq \boldsymbol{P}[A]$.

PROOF. Let $L\in \boldsymbol{PP}[A]$. Then there is an index k such that $\forall y$ ($y\in L$ iff Prob$[M_k{}^A(y)=1]>1/2$). (See, e.g., [**BDG 88**] or [**Pa 94**].) Then we define a det p-time OTM $T^{\sim}$ as follows: Given y, $T^{\sim}$ writes the string $w=0^k1y10^n$ on its oracle tape, where $n=p_k(|y|)$, and enters query state. If the answer is yes, then it accepts y; otherwise it rejects y. Clearly $T^{\sim}$ is a deterministic p-time OTM. Now for an arbitrary input y, let $s=|0^k1y10^n|$, where $n=p_k(|y|)$, and consider at stage $2s$. Then, T^A accepts y iff $0^k1y10^n1\in A$ iff Prob$[M_k{}^{A(2s)}(y)=1]>1/2$ iff Prob$[M_k{}^A(y)=1]>1/2$ iff $y\in L$. Thus $L\in \boldsymbol{P}[A]$. Hence $\boldsymbol{PP}[A]\subseteqq \boldsymbol{P}[A]$.

Clearly, $H\leqq_{PT}A$ and hence $H\oplus A\equiv_{PT}A$. By the Claim, $\boldsymbol{P}[A]=\boldsymbol{PP}[A]$, *a fortiori*, we have: $\boldsymbol{P}[A]=\boldsymbol{BPP}[A]$. □

Thus, there is no H satisfying (15).

So, our Theorem 1 has the *raison d'etre*.

ACKNOWLEDGMENT. The authors thank the anonymous referee for his kind advice.

References

[BGS 75] T. Baker, J. Gill and R. Solovay, Relativizations of the $P=?NP$ question, SIAM J. Comput., 4 (1975), 431-442.

[BDG 88] J. Balcázar, J. Díaz and J. Gabarró, Structural Complexity I, Springer-Verlag, Berlin etc., 1988.

[BDG 90] J. Balcázar, J. Díaz and J. Gabarró, Structural Complexity II, Springer-Verlag, Berlin etc., 1990.

[BG 81] C. H. Bennett and J. 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.

[BI 87] M. Blum and R. Impagliazzo, Generic oracles and oracle classes, 19-th Symposium FOCS, 1987, pp. 118-126.

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

[Pa 94] C. H. Papadimitrious, Computational Complexity, Addison-Wesley, 1994.

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

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

[Sch 85] U. Schoning, Complexity and Structure, Lecture Notes in Comput. Sci., 211 1985.

Hisao TANAKA
Division of Mathematical Science
Department of System and Control Engineering
College of Engineering
Hosei University
Koganei, Tokyo 184
Japan

Masafumi KUDOH
Toshiba Corporation
Shibaura, Minato-ku
Tokyo 105-01
Japan