An Observation on Probability versus Randomness with Applications to Complexity Classes

Ronald V. Book [*]
Department of Mathematics
University of California
Santa Barbara, CA 93106, USA

Jack H. Lutz [†]
Department of Computer Science
Iowa State University
Ames, Iowa 50011, USA

Klaus W. Wagner
Institut für Informatik
Universität Würzburg
W-8700 Würzburg, Germany

Abstract

Every class **C** of languages satisfying a simple topological condition is shown to have probability one if and only if it contains some language that is algorithmically random in the sense of Martin-Löf. This result is used to derive separation properties of algorithmically random oracles and to give characterizations of the complexity classes **P**, **BPP**, **AM**, and **PH** in terms of reducibility to such oracles. These characterizations lead to results like:
P = **NP** if and only if there exists an algorithmically random set that is $\leq^{\mathrm{P}}_{btt}$-hard for **NP**.

[*] The work of the first author was supported in part by the Alexander-von-Humboldt-Stiftung and by the National Science Foundation under Grant CCR-8913584 while he visited the Lehrstuhl für Theoretische Informatik, Institut für Informatik, Universität Würzburg, Germany.

[†] The work of the second author was supported in part by the National Science Foundation under Grant CCR-8809238 and in part by DIMACS, where he was a visitor while a portion of his work was done.

1 Introduction

Many results in complexity theory involve conditions that are satisfied by "almost every" oracle. Two of the best-known examples are the following:

(i) For almost every oracle A, $\mathbf{P}(A) \neq \mathbf{NP}(A) \neq \text{co}-\mathbf{NP}(A)$ [BG81].

(ii) For every recursive language B, $B \in \mathbf{BPP}$ if and only if for almost every oracle A, $B \in \mathbf{P}(A)$ [BG81, Amb86].

In such results, the assertion that "almost every oracle A has property θ" means that $\theta(A)$ is true with probability one when the oracle $A \subseteq \{0,1\}^*$ is selected probabilistically by using an independent toss of a fair coin to decide membership of each string in A.

The class **RAND** of *algorithmically random languages*, defined by Martin-Löf [Mar66] (and in Section 3 below) contains almost every oracle. Thus, for every property θ that is satisfied by almost every oracle, there exists an oracle $A \in \mathbf{RAND}$ satisfying $\theta(A)$.

In this paper we prove that the converse holds for a wide variety of properties θ. Specifically, in Section 3 below, we prove the following. Assume that the class of all oracles A satisfying $\theta(A)$ is a union of recursively closed sets (in the Cantor topology on the set of all languages) and is closed under finite variation. Then $\theta(A)$ holds for *some* $A \in \mathbf{RAND}$ if and only if $\theta(A)$ holds for *almost every* oracle A.

To date, most complexity theory results concerning almost every oracle are either oracle separation results, like (i) above, or characterizations of complexity classes, like (ii) above. In Section 4 we illustrate the Main Theorem in both of these contexts. We show how, in many cases, separations for relativized complexity classes for almost every oracle immediately imply separations for *every* algorithmically random oracle. In addition, we show how characterizations of reducibility to *some* algorithmically random oracle yield characterizations of complexity classes in terms of reducibility to almost every oracle.

Applying these results to the facts (i) and (ii) above, we obtain, for example,

(i') For every $A \in \mathbf{RAND}$, $\mathbf{P}(A) \neq \mathbf{NP}(A) \neq \text{co}-\mathbf{NP}(A)$.

(ii') For every recursive language B, $B \in \mathbf{BPP}$ if and only if $B \in \mathbf{P}(\mathbf{RAND})$.

2 Preliminaries

For the most part our notation is standard, following that used by Balcázar, Díaz, and Gabarró [BDG88, BDG90]. We assume that the reader is familiar with the standard recursive reducibilities and the variants obtained by imposing resource bounds such as time or space on the algorithms that compute these reducibilities.

A *word* (string) is an element of $\{0,1\}^*$. The length of a word $w \in \{0,1\}^*$ is denoted $|w|$.

The power set of a set A is denoted by $\mathcal{P}(A)$.

Let c_A be the characteristic function of A. The *characteristic sequence* of a language A is the infinite sequence $c_A(x_0)c_A(x_1)c_A(x_2)\ldots$ where $\{x_0, x_1, x_2, \ldots\} = \{0,1\}^*$ in a lexicographical order. We freely identify a language with its characteristic sequence and the class of all languages on the fixed finite alphabet $\{0,1\}$ with the set $\{0,1\}^\omega$ of all such infinite sequences; the usage is based on context so that there should be no ambiguity on the part of the reader.

If X is a set of strings (i. e., a language) and $\mathbf{C}$ is a set of sequences (i. e., a class of languages), then $X\cdot\ \mathbf{C}$ denotes the set $\{w\xi \mid w \in X,\ \xi \in \mathbf{C}\ \}$.

For each string w, $C_w = \{w\} \cdot \{0,1\}^\omega$ is the *basic open set* defined by w. An *open set* is a (finite or infinite) union of basic open sets, i.e. a set $X \cdot \{0,1\}^\omega$ where $X \subseteq \{0,1\}^*$. (This definition gives the usual product topology, also known as the Cantor topology, on $\{0,1\}^\omega$.) A *closed set* is the complement of an open set. A class of languages is *recursively open* if it is of the form $X \cdot \{0,1\}^\omega$ for some recursively enumerable set $X \subseteq \{0,1\}^*$. A class of languages is *recursively closed* if it is the complement of some recursively open set.

We assume an effective enumeration of the recursively enumerable languages as $W_1,\ W_2,\ \ldots$.

For a class $\mathbf{C}$ of languages we write Prob[$\mathbf{C}$] for the probability that $A \in \mathbf{C}$ when A is chosen by a random experiment in which an independent toss of a fair coin is used to decide whether a string is in A. This probability is defined whenever $\mathbf{C}$ is measurable in the usual product topology of $\{0,1\}^\omega$. In particular, if $\mathbf{C}$ is a countable union or intersection of (recursively) open or closed sets, then $\mathbf{C}$ is measurable, so Prob[$\mathbf{C}$] is defined. Note that there are only countably many recursively open sets, so every intersection of recursively open sets is a countable intersection of such sets, and hence is measurable; similarly every union of recursively closed sets is measurable.

A class $\mathbf{C}$ is *closed under finite variation* if $A \in \mathbf{C}$ holds whenever $B \in \mathbf{C}$ and A and B have finite symmetric difference. The Kolmogorov 0-1 Law says that every measurable set $\mathbf{C} \subseteq \{0,1\}^\omega$ that is closed under finite variation has either measure 0 or measure 1.

3 Main Result

The definition of a random language is due to Martin-Löf [Mar66]. A class $\mathbf{C}$ is called a *constructive null set* if there is a total recursive function g with the properties that for every k,

(i) $\mathbf{C} \subseteq W_{g(k)} \cdot \{0,1\}^\omega$, and

(ii) $\text{Prob}[W_{g(k)} \cdot \{0,1\}^\omega] \leq 2^{-k}$.

Hence every constructive null set has measure 0. Let **NULL** be the union of all constructive null sets, and let $\mathbf{RAND} =_{df} \{0,1\}^\omega - \mathbf{NULL}$ be the class of algorithmically random languages. Since **NULL** is a countable union of measure 0 sets we have $\text{Prob}[\mathbf{NULL}] = 0$, and, consequently, $\text{Prob}[\mathbf{RAND}] = 1$.

The following lemma is needed for our main result.

Lemma 1 *If* $\mathbf{F}$ *is a recursively closed set of languages with* $\text{Prob}[\mathbf{F}] = 0$*, then* $\mathbf{F}$ *is a constructive null set.*

Proof Let $\mathbf{F}$ be recursively closed with $\text{Prob}[\mathbf{F}] = 0$. By definition there exists a total recursive function g such that $\{0,1\}^\omega - \mathbf{F} = \{g(0), g(1), g(2), \ldots\} \cdot \{0,1\}^\omega$. For $j \geq 0$, let $B_j =_{df} \{g(0), g(1), \ldots, g(j)\}$. Since $B_j \subseteq B_{j+1}$ for $j \geq 0$, the sequence $\text{Prob}[B_j \cdot \{0,1\}^\omega]$ is monotonic increasing and approaches $\text{Prob}[\{0,1\}^\omega - \mathbf{F}] = 1$ with growing j. Hence the function f is total recursive when it is defined by $f(k) =_{df}$ the least j such that $\text{Prob}[B_j \cdot \{0,1\}^\omega] \geq 1 - 2^{-k}$. For each k, let m_k be the length of the longest string in $B_{f(k)}$, and let C_k be the set of all strings of length m_k which have prefixes in $B_{f(k)}$. Hence $C_k \cdot \{0,1\}^\omega = B_{f(k)} \cdot \{0,1\}^\omega$ and $\text{Prob}[C_k \cdot \{0,1\}^\omega] \geq 1 - 2^{-k}$. Obviously, there exists a total recursive function h such that $W_{h(k)} = \{0,1\}^{m_k} - C_k$. Hence $\text{Prob}[W_{h(k)} \cdot \{0,1\}^\omega] \leq 2^{-k}$. Since $\{0,1\}^\omega - \mathbf{F} \supseteq B_{f(k)} \cdot \{0,1\}^\omega$ we have $\mathbf{F} \subseteq W_{h(k)} \cdot \{0,1\}^\omega$ for each k. Hence $\mathbf{F}$ is a constructive null set. □

Now we come to the main result.

Theorem 2 *Let* $\mathbf{C}$ *be a union of recursively closed sets that is closed under finite variation. Then*

$$\text{Prob}[\mathbf{C}] = 1 \Leftrightarrow \mathbf{C} \cap \mathbf{RAND} \neq \emptyset.$$

Proof Since Prob[**RAND**] $= 1$ it is immediate that Prob[**C**] $= 1$ implies $\mathbf{C} \cap \mathbf{RAND} \neq \emptyset$. To see the converse, assume that Prob[**C**] < 1. As a union of recursively closed sets, **C** is measurable. Since **C** is closed under finite variations, the Kolmogorov 0-1 Law yields Prob[**C**] $= 0$. By Lemma 1, each of the recursively closed sets whose union is **C** is a constructive null set. Hence $\mathbf{C} \subseteq \mathbf{NULL}$, and consequently $\mathbf{C} \cap \mathbf{RAND} = \emptyset$. □

The following dual of Theorem 2 is also useful.

Corollary 3 *Let* **C** *be an intersection of recursively open sets that is closed under finite variation. Then*

$$\mathrm{Prob}[\mathbf{C}] = 1 \Leftrightarrow \mathbf{RAND} \subseteq \mathbf{C}.$$

Proof Since Prob[**RAND**] $= 1$ it is clear that $\mathbf{RAND} \subseteq \mathbf{C}$ implies Prob[**C**] $= 1$. To see the converse, assume $\mathbf{RAND} \not\subseteq \mathbf{C}$. Hence $\{0,1\}^\omega - \mathbf{C} \cap \mathbf{RAND} \neq \emptyset$, $\{0,1\}^\omega - \mathbf{C}$ is a union of recursively closed sets, and $\{0,1\}^\omega - \mathbf{C}$ is closed under finite variations. By Theorem 2 we obtain $\mathrm{Prob}[\{0,1\}^\omega - \mathbf{C}] = 1$ and hence Prob[**C**] $= 0$. □

4 Applications

We illustrate the power of the Main Theorem and its corollary with applications of two types, namely, oracle separations and characterizations of complexity classes.

Since we are concerned with the use of oracles, we consider complexity classes that can be specified so as to "relativize." But we want to do this in a general setting and so we introduce a few definitions.

We assume a fixed enumeration M_0, M_1, M_2, $\ldots$ of nondeterministic oracle Turing machines.

A *relativized class* is a function $\mathbf{C} : \mathcal{P}(\{0,1\}^*) \longrightarrow \mathcal{P}(\mathcal{P}(\{0,1\}^*))$. A *recursive presentation* of a relativized class **C** of languages is a total recursive function $f : \mathsf{N} \longrightarrow \mathsf{N}$ such that for every language A and every $i \geq 0$, $M^A_{f(i)}$ halts on every computation and $\mathbf{C}(A) = \{L(M^A_{f(i)}) \mid i \in \mathsf{N}\}$. A relativized class is *recursively presentable* if it has a recursive presentation.

A *reducibility* is a relativized class. A *bounded reducibility* is a relativized class that is recursively presentable. If **R** is a reducibility, then we use the notation

$A \leq^{\mathrm{R}} B$ to indicate that $A \in \mathbf{R}(B)$. In addition we write $\mathbf{R}^{-1}(A)$ for $\{B \mid A \leq^{\mathrm{R}} B\}$. Typical bounded reducibilities include $\leq_m^{\mathrm{P}}$, $\leq_{btt}^{\mathrm{P}}$, $\leq_T^{\mathrm{P}}$, $\leq_T^{\mathrm{NP}}$, $\leq_T^{\mathrm{SN}}$, $\leq_m^{\mathrm{logspace}}$, etc. The relations $\leq_m$ and $\leq_T$ are reducibilities that are not bounded. In many contexts it is useful to restrict attention to reducibilities that are reflexive and transitive, but we do not need such restrictions here.

If $\mathbf{R}$ is a reducibility and $\mathbf{C}$ is a set of languages, then a language A is $\leq^{\mathrm{R}}$-*complete* for $\mathbf{C}$ if $A \in \mathbf{C} \subseteq \mathbf{R}(A)$. A relativized class $\mathbf{C}$ is *recursively presentable with an* $\leq^{\mathrm{R}}$*-complete language* if there exist a recursive presentation f of $\mathbf{C}$ and a constant $c \in \mathsf{N}$ such that for every language A, $L(M_{f(c)}^A)$ is $\leq^{\mathrm{R}}$-complete for $\mathbf{C}(A)$. If $\mathbf{R}$ is a reducibility and $\mathbf{C}$ is a set of languages, write $\mathbf{R}(\mathbf{C})$ for $\bigcup_{A \in \mathrm{C}} \mathbf{R}(A)$. A relativized class $\mathbf{C}$ is *closed* under a reducibility $\mathbf{R}$ if $\mathbf{R}(\mathbf{C}(A)) \subseteq \mathbf{C}(A)$ for every language A.

While the next result is quite general, it does apply to a number of specific situations that are of interest in complexity theory.

Theorem 4 *Let* $\mathbf{C}$ *and* $\mathbf{D}$ *be relativized complexity classes and let* $\mathbf{R}$ *be a reducibility. Suppose that each of the following holds:*

(i) $\mathbf{C}$ *is recursively presentable with an* $\leq^{\mathrm{R}}$*-complete language.*

(ii) $\mathbf{D}$ *is recursively presentable and is closed under* $\mathbf{R}$.

(iii) $\mathbf{C}$ *and* $\mathbf{D}$ *are invariant under finite variations of the oracle.*

Then the following statements hold.

(a) $\mathbf{C}(A) \not\subseteq \mathbf{D}(A)$ *for almost every* A *if and only if* $\mathbf{C}(A) \not\subseteq \mathbf{D}(A)$ *for every* $A \in \mathbf{RAND}$.

(b) $\mathbf{C}(A) \subseteq \mathbf{D}(A)$ *for almost every* A *if and only if* $\mathbf{C}(A) \subseteq \mathbf{D}(A)$ *for some* $A \in \mathbf{RAND}$.

Proof (a): Let $\mathbf{SEP} = \{A \mid \mathbf{C}(A) \not\subseteq \mathbf{D}(A)\}$. By Corollary 3 it suffices to show that $\mathbf{SEP}$ is a countable intersection of recursively open sets and that $\mathbf{SEP}$ is closed under finite variation. The latter is immediate by (iii).

Let f, g be recursive presentations of $\mathbf{C}$, $\mathbf{D}$ respectively, and fix $c \in \mathsf{N}$ such that, for all $A \in \{0,1\}^\omega$, $L(M_{f(c)}^A)$ is $\leq^{\mathrm{R}}$-complete for $\mathbf{C}(A)$. Since $\mathbf{D}$ is closed under $\mathbf{R}$, we have $\mathbf{C}(A) \not\subseteq \mathbf{D}(A) \Leftrightarrow L(M_{f(c)}^A) \notin \mathbf{D}(A)$. For each j let $\mathbf{SEP}_j = \{A \mid L(M_{g(j)}^A) \neq$

$L(M^A_{f(c)})\}$. Then $\mathbf{SEP} = \bigcap_{j \geq 0} \mathbf{SEP}_j$, so it suffices to show that each $\mathbf{SEP}_j$ is a recursively open set of languages.

Fix j. Define a partial recursive function $h : \{0,1\}^* \times \{0,1\}^* \longrightarrow \{0,1\}^*$ as follows. For $x, z \in \{0,1\}^*$, if $M^{z0^\omega}_{g(j)}(x)$ and $M^{z0^\omega}_{f(c)}(x)$ differ and need only the initial part z of $z0^\omega$, then $h(z,x) = z$. Otherwise, let $h(z,x)$ be undefined. For every A

$$\begin{aligned}
A \in \mathbf{SEP}_j \quad &\Leftrightarrow \quad \exists x \; (M^A_{g(j)}(x) \text{ and } M^A_{f(c)}(x) \text{ differ }) \\
&\Leftrightarrow \quad \exists x \; \exists z \;\; (M^A_{g(j)}(x) \text{ and } M^A_{f(c)}(x) \text{ differ} \\
&\qquad\qquad \text{and need only the initial part } z \text{ of } A) \\
&\Leftrightarrow \quad \exists x \; \exists z \; (M^{z0^\omega}_{g(j)}(x) \text{ and } M^{z0^\omega}_{f(c)}(x) \text{ differ} \\
&\qquad\qquad \text{and need only the initial part } z \text{ of } z0^\omega, \text{ and } A \in \mathbf{C}_z) \\
&\Leftrightarrow \quad \exists z \; (z \in \text{range}(h) \text{ and } A \in \mathbf{C}_z) \\
&\Leftrightarrow \quad A \in \text{range}(h) \cdot \{0,1\}^\omega.
\end{aligned}$$

Since range(h) is an r. e. set, the set A is recursively open.

(b): Statement (a) yields that $\mathbf{C}(A) \subseteq \mathbf{D}(A)$ for some $A \in \mathbf{RAND}$ if and only if Prob$[\{A \neq \mathbf{C}(A) \subseteq \mathbf{D}(A)\}] > 0$. By the Kolmogorov 0-1 Law the latter is equivalent to Prob$[\{A \neq \mathbf{C}(A) \subseteq \mathbf{D}(A)\}] = 1$. □

¿From Theorem 4 and known probability one oracle separations, it follows immediately that *every* algorithmically random set A satisfies

- $\mathbf{P}(A) \neq \mathbf{NP}(A) \neq \text{co}-\mathbf{NP}(A)$ [BG81],
- $\mathbf{BH}(A)$ has infinitely many levels [Cai87],
- $\mathbf{PH}(A) \neq \mathbf{PSPACE}(A)$ [Cai89],

etc. Similarly, if with probability one, the relativized polynomial-time hierarchy has infinitely many levels, then this separation is achieved relative to *every* algorithmically random set.

Next we wish to develop characterizations of complexity classes in terms of **RAND** via Theorem 2. For this we need the following lemma

Lemma 5 *If* $\mathbf{R}$ *is a bounded reducibility then the inverse-image* $\mathbf{R}^{-1}(B)$ *of a recursive* B *is a union of recursively closed sets.*

Proof Let g be a recursive representation of $\mathbf{R}$. For each $j \geq 0$ let $\mathbf{R}^{-1}_j(B) = \{A : L(M^A_{g(j)}) = B\}$. Then $\mathbf{R}^{-1}(B) = \bigcup_{j \geq 0} \mathbf{R}^{-1}_j(B)$, so it suffices to show that the complement $\mathbf{COM}_j$ of $\mathbf{R}_j^{-1}(B)$ is recursively open for every $j \geq 0$. This is shown exactly as for $\mathbf{SEP}_j$ in the proof of Theorem 4 where we have to replace $M_{f(c)}^A(x)$ by the characteristic function $c_B(x)$. □

Note that the above proof shows: The inverse-image of a recursive set $B \subseteq \{0,1\}^\omega$ with respect to the recursive operator $L(M_{g(j)}^{()})$ is a recursively closed set. Since $\{B\}$ is a recursively closed set, this is a special case of the fact: The inverse-image of a recursively closed set with respect to a recursive operator is a recursively closed set. Since recursive operators are continous mappings in the Cantor topology on $\{0,1\}^\omega$ this is the "recursive analogue" of the well known fact from topology that the inverse-image of a closed set with respect to a continous mapping is a closed set (in fact, continous mappings are defined in this way in general topology).

For each relativized class $\mathbf{C}$, let $\mathbf{ALMOST{-}C} = \{A \mid \text{Prob}[\{B : A \in \mathbf{C}^B\}] = 1\}$. Let further $\mathbf{REC}$ denote the class of recursive languages.

Theorem 6 *If* $\mathbf{R}$ *is a bounded reducibility that is invariant under finite variations of the oracle, then* $\mathbf{ALMOST{-}R} = \mathbf{R}(\mathbf{RAND}) \cap \mathbf{REC}$.

Proof ¿From a result of Sacks (see [Rog67], p.272), we have $A \in \mathbf{ALMOST{-}R}$ if and only if $\text{Prob}[\mathbf{R}^{-1}(A)] = 1$ and $A \in \mathbf{REC}$. By Theorem 2 and Lemma 5, the latter condition is equivalent to $\mathbf{R}^{-1}(A) \cap \mathbf{RAND} \neq \emptyset$ and $A \in \mathbf{REC}$, which in turn is equivalent to $A \in \mathbf{R}(\mathbf{RAND}) \cap \mathbf{REC}$. □

Now we turn to characterizations of complexity classes. For the sake of brevity, we give just four applications, characterizing the classes $\mathbf{P}$, $\mathbf{BPP}$, $\mathbf{AM}$, and $\mathbf{PH}$ in terms of reducibilities to algorithmically random languages.

Theorem 7 (a) $\mathbf{P} = \mathbf{P}_m(\mathbf{RAND}) \cap \mathbf{REC} = \mathbf{P}_{btt}(\mathbf{RAND}) \cap \mathbf{REC}$
$= \mathbf{P}_{\log n - T}(\mathbf{RAND}) \cap \mathbf{REC}$.

(b) $\mathbf{BPP} = \mathbf{P}_{tt}(\mathbf{RAND}) \cap \mathbf{REC} = \mathbf{P}_T(\mathbf{RAND}) \cap \mathbf{REC}$.

(c) $\mathbf{AM} = \mathbf{NP}_T(\mathbf{RAND}) \cap \mathbf{REC}$.

(d) $\mathbf{PH} = \mathbf{PH}(\mathbf{RAND}) \cap \mathbf{REC}$.

Proof These follow immediately from Theorem 6 and the known facts that $\mathbf{P} = \mathbf{ALMOST{-}P}_m$ [Amb86], $\mathbf{P} = \mathbf{ALMOST{-}P}_{btt} = \mathbf{ALMOST{-}P}_{\log n - T}$ [TB91],

$\mathbf{BPP} = \mathbf{ALMOST}{-}\mathbf{P}_T$ [BG81, Amb86], $\mathbf{BPP} = \mathbf{ALMOST}{-}\mathbf{P}_{tt}$ [Amb86, TB91], $\mathbf{AM} = \mathbf{ALMOST}{-}\mathbf{NP}_T$ [NW88], and $\mathbf{PH} = \mathbf{ALMOST}{-}\mathbf{PH}$ [NW88]. □

Note that $\mathbf{BPP} = \mathbf{P}_T(\mathbf{RAND}) \cap \mathbf{REC}$ has already been proved in [Ben88].

The class **RAND** is considered to be the class of those languages having the greatest possible information content. It is well known that there is a constant c such that for all languages A and all n, the Kolmogorov complexity of the finite language $A_{\leq n} = \{x \in A \mid |x| \leq n\}$ is not greater than $2^{n+1} + c$. (Recall that the Kolmogorov complexity of the finite language $A_{\leq n}$ is the Kolmogorov complexity of its characteristic string, that is, the prefix of length $2^{n+1} - 1$ of the characteristic sequence of A.) Martin-Löf [Mar71] proved that every language A in **RAND** has nearly maximal information content in the sense that the Kolmogorov complexity of $A_{\leq n}$ is strictly greater than $2^{n+1} - 2n$ for all but finitely many n. However, Theorem 8 below shows that in the given context, the power of oracles with such a great information content is similar to those with very small information content.

Recall that a set S is *sparse* if there exists a polynomial q such that $\#S_{\leq n} \leq q(n)$ for all n. Sparse sets S are considered to be sets with small information content since the Kolmogorov complexity of $S_{\leq n}$ is not greater than $n^c + c$ for a suitable constant $c > 0$.

Theorem 8 *The following are equivalent.*

(a) $\mathbf{P} = \mathbf{NP}$.

(b) *There exists a sparse set that is* $\leq^{\mathrm{P}}_{btt}$*-hard for* **NP**.

(c) *There exists an algorithmically random set that is* $\leq^{\mathrm{P}}_{btt}$*-hard for* **NP**.

(d) *Every sparse set is* $\leq^{\mathrm{P}}_{btt}$*-hard for* **NP**.

(e) *Every algorithmically random set is* $\leq^{\mathrm{P}}_{btt}$*-hard for* **NP**.

Proof The equivalence of (a) and (b) is proved in [OW91]. Further, (a) $\Leftrightarrow$ (d), (a) $\Leftrightarrow$ (e), and (e) $\Rightarrow$ (c) are obvious. Finally, (c) $\Rightarrow$ (a) is an immediate consequence of Theorem 7(a). □

Theorem 8 remains true for **P** versus **PSPACE** via a result from [OL91], and similar statements are true for **NP** versus **PH** and **PH** versus **PSPACE** (cf. [KL82], [BBS86] and [LS86]).

The similarity between the results for sparse sets and algorithmically random sets, resp., in Theorem 8 is striking. When the sets having the greatest possible information content, algorithmically random sets, and when the sets having very small information content, sparse sets, serve as oracle sets, the conclusions are the same. One can interpret this result as indicating that the information in algorithmically random sets is encoded in such a way that little of it is computationally useful from the standpoint of structural complexity theory, since one may as well use a sparse set. This suggests that a theory that relates the information content of oracle sets to the computational power of reducibilities needs to be developed; the results presented here should be viewed as only first steps.

We conclude with the following open question which is suggested by Theorem 7. If $\mathbf{C}$ is a relativizable class of languages, under what conditions is it the case that $\mathbf{C}(\mathbf{RAND}) \cap \mathbf{REC} = \mathbf{BP} \cdot \mathbf{C}$? This equation is known to be true for $\mathbf{C} = \mathbf{P}$, $\mathbf{C} = \mathbf{NP}$, and $\mathbf{C} = \mathbf{PH}$ by the results stated above. If $\mathbf{C}$ is a relativizable class of languages, under what conditions is it the case that $\mathbf{BP} \cdot \mathbf{C} = \mathbf{C}$? It is known to be true for $\mathbf{C} = \mathbf{PH}$. It is clear that $\mathbf{BP} \cdot \mathbf{PSPACE} = \mathbf{PSPACE}$. Is $\mathbf{PSPACE}(\mathbf{RAND}) \cap \mathbf{REC}$ equal to $\mathbf{PSPACE}$ (the queries of a $\mathbf{PSPACE}$ oracle machine are poly-length bounded) ?

Acknowledgement The authors thank the anonymous referees for many valuable hints, including a simplified proof of Theorem 2 and a correction to Theorem 4.

References

[Amb86] K. Ambos-Spies. Randomness, relativations, and polynomial reducibilities. In *Lecture Notes in Computer Sci. 223*, pages 23–34. Proc. 1st Conf. Stucture in Complexity Theory, Springer-Verlag, 1986.

[BBS86] J. Balcázar, R. Book, and U. Schöning. The polynomial-time hierarchy and sparse oracles. *J. Assoc. Comput. Mach.*, 33:603–617, 1986.

[BDG88] J. Balcázar, J. Díaz, and J. Gabarró. *Structural Complexity I.* Springer-Verlag, 1988.

[BDG90] J. Balcázar, J. Díaz, and J. Gabarró. *Structural Complexity II.* Springer-Verlag, 1990.

[Ben88] C. Bennett. Logical depth and physical complexity. In R. Herken (ed.), *The Universal Turing Machine: A Half-Century Survey*, pages 227–257. Oxford University Press, 1988.

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

[Cai87] J.-Y. Cai. Probability one separation of the boolean hierarchy. In *Lecture Notes in Computer Sci. 38*, pages 148–158. STACS 87, Springer Verlag, 1987.

[Cai89] J.-Y. Cai. With probability one, a random oracle separates PSPACE from the polynomial-time hierarchy. *J. Comput. Systems Sci.*, 38:68–85, 1989.

[KL82] R. Karp and R. Lipton. Turing machines, that take advice. *L'Enseignement Mathématique*, 28 2nd series:191–209, 1982.

[LS86] T. Long and A. Selman. Relativizing complexity classes with sparse oracles. *J. Assoc. Comput. Mach.*, 33:618–627, 1986.

[Mar66] P. Martin-Löf. On the definition of random sequences. *Info. and Control*, 9:602–619, 1966.

[Mar71] P. Martin-Löf. Complexity oscillations in infinite binary sequences. *Zeitschrift für Wahrscheinlichkeitstheorie und Verwandte Gebiete*, 19:225–230, 1971.

[NW88] N. Nisan and A. Wigderson. Hardness versus randomness. In *Proc. 29th IEEE Symp. Found. of Comput. Sci.*, pages 2–11, 1988.

[OL91] M. Ogiwara and A. Lozano. On one query self-reducible sets. In *Proc. 6th IEEE Conference on Structure in Complexity Theory*, pages 139–151, 1991.

[OW91] M. Ogiwara and O. Watanabe. On polynomial bounded truth table reducibility of NP sets to sparse sets. *SIAM J. Computing*, 20:471–483, 1991.

[Rog67] H. Rogers. *Theory of Recursive Functions and Effective Computability.* McGraw-Hill, 1967.

[TB91] S. Tang and R. Book. Polynomial-time reducibilities and "almost-all" oracle sets. *Theoret. Computer Sci.*, 81:36–47, 1991.