A Note on Independent Random Oracles*

Jack H. Lutz
Department of Computer Science
Iowa State University
Ames, IA 50011

Abstract

It is shown that $\mathrm{P}(A) \cap \mathrm{P}(B) = \mathrm{BPP}$ holds for *every* algorithmically random oracle $A \oplus B$. This result extends the corresponding "probability one" characterization of Ambos-Spies (1986) and Kurtz (1987).

1 Introduction

Most polynomial time complexity classes are now known to admit *probability one oracle characterizations* [2, 1, 7, 14, 20, 19]. The canonical such characterization, due to Bennett and Gill [2] and Ambos-Spies [1], is the fact that

$$\mathrm{BPP} = \{A \mid \Pr_B[A \in \mathrm{P}(B)] = 1\}, \tag{1.1}$$

where BPP is the class of all decision problems solvable in polynomial time by randomized algorithms with bounded error. (See section 2 for notation and terminology used in this introduction.) In this paper, $\Pr_B[\mathcal{E}]$ denotes the probability that event $\mathcal{E}$ occurs when the language $B \subseteq \{0,1\}^*$ is chosen probabilistically according to the uniform distribution, i.e., according to the random experiment in which an independent toss of a fair coin is used to decide whether each string is in B. Thus (1.1) asserts that a language is in BPP if and only if it is $\leq^{\mathrm{P}}_T$-reducible to *almost every* oracle B. (In this paper, the terms *oracle*, *language*, and *decision problem* are used synonymously, denoting subsets of $\{0,1\}^*$.)

Since BPP is countable, (1.1) implies that *almost every* oracle is $\leq^{\mathrm{P}}_T$-hard for BPP. Nevertheless, (1.1) does not say *which* oracles are $\leq^{\mathrm{P}}_T$-hard for BPP. To remedy this, Lutz [12] gave a *pseudorandom oracle characterization* of BPP, stating that

$$\mathrm{BPP} = \{A \mid (\forall B \in \mathrm{RAND}(\mathrm{pspace}))\ A \in \mathrm{P}(B)\}. \tag{1.2}$$

Here, RAND(pspace) is the class of pspace-*random* oracles, defined by Lutz [10]. (Languages in RAND(pspace) are called *pseudorandom* because (i) they exhibit all pspace-specifiable randomness properties, even though (ii) RAND(pspace) contains many decidable languages, including almost every language in $\mathrm{E_2SPACE} = \mathrm{DSPACE}(2^{\mathrm{polynomial}})$ [10].) In passing from (1.1) to (1.2), the probability condition has been replaced by universal quantification over the set RAND(pspace). In particular, (1.2) implies that *every* pspace-random oracle is $\leq^{\mathrm{P}}_T$-hard for BPP. Since $\Pr_B[B \in \mathrm{RAND}(\mathrm{pspace})] = 1$ [10], this implies and explains the above-noted fact that almost every oracle is $\leq^{\mathrm{P}}_T$-hard for BPP.

Let RAND be the set of all languages which are (*algorithmically*) *random* in the equivalent senses of Martin-Löf [13], Levin [8], Schnorr [16], Chaitin [3, 4], Solovay [18], and Shen′ [17].

*This research was supported in part by National Science Foundation Grant CCR-8809238.

Then RAND $\subseteq$ RAND(pspace), so (1.1) and (1.2) together immediately give the *random oracle characterization*

$$\mathrm{BPP} = \{A \mid (\forall B \in \mathrm{RAND})\, A \in \mathrm{P}(B)\}. \tag{1.3}$$

Since $\Pr_B[B \in \mathrm{RAND} = 1$ [13] and RAND $\subsetneqq$ RAND(pspace) [10], (1.3) is in a sense more informative than (1.1) but less informative than (1.2).

Following (1.1), Ambos-Spies [1] and Kurtz [7] gave the *probability one independent oracle characterization*

$$\Pr_{A,B}[\mathrm{P}(A) \cap \mathrm{P}(B) = \mathrm{BPP}] = 1, \tag{1.4}$$

where $\Pr_{A,B}[\mathcal{E}]$ denotes the probability that event $\mathcal{E}$ occurs when the languages $A, B \subseteq \{0,1\}^*$ are chosen independently according to the uniform distribution. This is an intriguing characterization. It is immediate from (1.1) and the countability of BPP that $\Pr_B[\mathrm{BPP} \subsetneqq \mathrm{P}(B)] = 1$. However, (1.4) tells us that, if we choose A and B independently, then intersecting $\mathrm{P}(A)$ with $\mathrm{P}(B)$ will almost always give precisely the class BPP.

In this paper we extend (1.4) in a manner analogous to the extension of (1.1) to (1.3). We say that languages A and B are *independent random* if their disjoint union $A \oplus B$ is a random language. (This can easily be proven equivalent to the condition that (A, B) is not an element of any constructive null set in the product space $\Omega \times \Omega$, where Ω is the set of all languages with the uniform probability distribution.) Intuitively, this requires A and B to be individually random and completely uncorrelated. We then prove an *independent random oracle characterization* of BPP, stating that

$$(\forall A \oplus B \in \mathrm{RAND})\, \mathrm{P}(A) \cap \mathrm{P}(B) = \mathrm{BPP}. \tag{1.5}$$

Since $\Pr_{A,B}[A \oplus B \in \mathrm{RAND}] = 1$, (1.5) immediately implies (1.4). Moreover, (1.5) explains (1.4) by identifying a specific probability one event which implies that $\mathrm{P}(A) \cap \mathrm{P}(B) = \mathrm{BPP}$.

A constructive version of Fubini's theorem (see [15], for example) can be used to show that (1.5) implies (1.3). In fact, the comparison here is striking. The random oracle characterization (1.3) says that

$$\mathrm{BPP} = \bigcap_{B \in \mathrm{RAND}} \mathrm{P}(B). \tag{1.3$'$}$$

The independent random oracle characterization (1.5) says that (1.3′) holds even if we only intersect over *two* of the languages $B \in \mathrm{RAND}$, provided that the languages we choose are uncorrelated.

2 Preliminaries

All *languages*, *oracles*, and *decision problems* here are sets $A \subseteq \{0,1\}^*$. We write $A_{=n} = A \cap \{0,1\}^n$ and $A_{\leq n} = A \cap \{0,1\}^{\leq n}$. The *disjoint union* of languages A and B is $A \oplus B = \{x0 \mid x \in A\} \cup \{x1 \mid x \in B\}$.

The *characteristic sequence* of a language A is the infinite binary sequence $\chi_A = [\![s_0 \in A]\!][\![s_1 \in A]\!] \cdots$, where $s_0, s_1, s_2, \ldots$ is the standard enumeration of $\{0,1\}^*$ and $[\![\varphi]\!]$ is the truth value of φ (i.e., $[\![\varphi]\!] = \textbf{if } \varphi \textbf{ then } 1 \textbf{ else } 0$). The *characteristic string* of $A_{\leq n}$ is the $(2^{n+1}-1)$-bit prefix of χ_A. A *prefix* of a language A is a string $x \in \{0,1\}^*$ which is a prefix of χ_A; in this case we write $x \sqsubseteq \chi_A$ or $x \sqsubseteq A$.

We write Ω for the set of all languages and consider Ω as a probability space with the uniform distribution. Thus, for an event $\mathcal{E} \subseteq \Omega$, $\Pr(\mathcal{E}) = \Pr_A[A \in \mathcal{E}]$ is the probability that $A \in \mathcal{E}$ when A is chosen by a random experiment in which an independent toss of a fair coin is used to decide whether each string $x \in \{0,1\}^*$ is in A. The *cylinder generated by* a string $x \in \{0,1\}^*$ is the set

$$C_x = \{A \in \Omega \mid x \sqsubseteq A\}.$$

For convenience, we use the special symbol $\top$ to specify the empty set, $C_\top = \emptyset$. Note that $\Pr(C_\top) = 0$ and $\Pr(C_x) = 2^{-|x|}$ for each $x \in \{0,1\}^*$.

We say that *almost every* language has a property θ if $\Pr_A[A \text{ has property } \theta] = 1$.

<u>Definition</u> (Martin-Löf [13]). A *constructive null cover* of a set X of languages is a total recursive function

$$G : \mathbf{N} \times \mathbf{N} \to \{0,1\}^* \cup \{\top\}$$

such that, for each $k \in \mathbf{N}$,

(i) $X \subseteq \bigcup_{l=0}^{\infty} C_{G(k,l)}$ (the *covering condition*), and

(ii) $\sum_{l=0}^{\infty} \Pr(C_{G(k,l)}) \leq 2^{-k}$ (the *measure condition*).

A *constructive null set* is a set of languages which has a constructive null cover.

<u>Definition</u> (Martin-Löf [13]). A language A is (*algorithmically*) *random*, and we write $A \in \mathrm{RAND}$, if A is not an element of any constructive null set.

It is easy to see that each constructive null set X has probability $\Pr(X) = 0$. However, Martin-Löf [13] proved that $\Pr_A[A \in \mathrm{RAND}] = 1$, so the converse is not true: For each $A \in \mathrm{RAND}$, $\Pr(\{A\}) = 0$ but $\{A\}$ is not a constructive null set.

Choosing languages A and B independently from Ω is equivalent to choosing the pair (A, B) from the product space $\Omega \times \Omega$ with the probability distribution given by $\Pr(X \times Y) = \Pr(X)\Pr(Y)$ for all events $X, Y \subseteq \Omega$. Formally, one can then define cylinders and constructive null sets in $\Omega \times \Omega$ as we did for Ω above. A pair of *independent random oracles* is then a pair (A, B) which is not an element of any constructive null set in $\Omega \times \Omega$. However, it is easily shown that this is exactly equivalent to the following.

<u>Definition</u>. A and B are *independent random languages* if $A \oplus B \in \mathrm{RAND}$.

If A and B are independent random languages, it is easy to see that $A, B \in \mathrm{RAND}$. However, the converse does not hold. For example, $A \oplus A$ is not random, even if A is random.

The class BPP, first defined by Gill [5], consists of those decision problems A for which there exist a polynomial time-bounded probabilistic Turing machine M and a constant $\alpha > \frac{1}{2}$ such that $\Pr[M \text{ accepts } x] > \alpha$ for all $x \in A$ and $\Pr[M \text{ rejects } x] > \alpha$ for all $x \notin A$. This definition is not used in this paper, so it may be best to regard (1.1) as a definition of BPP.

With the exception of the above definition, all *machines* in this paper are deterministic oracle Turing machines. Such a machine is *polynomial time-bounded* if there is a polynomial q such that, for every input $x \in \{0,1\}^*$ and every oracle B, $M^B(x)$ accepts or rejects x in $\leq q(|x|)$ steps. We write $L(M^B) = \{x \mid M^B(x) \text{ accepts } x\}$. A language A is *polynomial time Turing reducible* to a language B, and we write $A \leq_T^{\mathrm{P}} B$, if $A = L(M^B)$ for some polynomial time-bounded machine M. We write $\mathrm{P}(A) = \{B \mid A \leq_T^{\mathrm{P}} B\}$.

The class RAND(pspace) is discussed only in sections 1 and 4 and will not be defined here. Details may be found in [9, 10, 11, 12].

3 Result

We now prove the independent random oracle characterization of BPP.

Theorem. For *every* pair A, B of independent random oracles,

$$\mathrm{P}(A) \cap \mathrm{P}(B) = \mathrm{BPP}.$$

Proof. The right-to-left inclusion follows immediately from (1.3). For the left-to-right inclusion, assume that

$$D \in \mathrm{P}(A) \cap \mathrm{P}(B) \setminus \mathrm{BPP}.$$

It suffices to prove that $A \oplus B$ is not random.

Fix machines M_a, M_b testifying that $D \in \mathrm{P}(A)$, $D \in \mathrm{P}(B)$, respectively, and fix a strictly increasing polynomial q such that $|y| < q(|x|)$ for all x and all queries y of M_a or M_b on input x. For each $n \in \mathbf{N}$, let $K(n) = 2^{q(n)} - 1$ and $N(n) = 2K(n) + 1 = 2^{q(n)+1} - 1$. Throughout this proof, let $u, v \in \{0,1\}^{K(n)}$ denote the characteristic strings of sets $U, V \subseteq \{0,1\}^{<q(n)}$, respectively, and let $u \oplus v \in \{0,1\}^{N(n)}$ denote the characteristic string of $U \oplus V$.

For each $n \in \mathbf{N}$ and $u \in \{0,1\}^{K(n)}$, let

$$\mathcal{V}(u) = \{v \in \{0,1\}^{K(n)} \mid L(M_a^U)_{\leq n} = L(M_b^V)_{\leq n}\}.$$

For each $k, n \in \mathbf{N}$, then, let $\mathcal{U}_{k,n}$ be the set of all strings $u \in \{0,1\}^{K(n)}$ with the following two properties.

(i) $0 < |\mathcal{V}(u)| \leq 2^{K(n)-k}$.

(ii) No prefix of u is in $\mathcal{U}_{k,n'}$ for any $0 \leq n' < n$. (This condition holds vacuously if $n = 0$.)

For each $k \in \mathbf{N}$, let $\mathcal{U}_k = \bigcup\limits_{n=0}^{\infty} \mathcal{U}_{k,n}$. Note that condition (ii) ensures that each $\mathcal{U}_k$ is an instantaneous code (i.e., no element of $\mathcal{U}_k$ is a prefix of any other) and hence satisfies the Kraft inequality,

$$\sum_{u \in \mathcal{U}_k} 2^{-|u|} \leq 1.$$

For each $k \in \mathbf{N}$ and $u \in \{0,1\}^*$, define a nonempty list $\Gamma_k(u)$ of elements of $\{0,1\}^* \cup \{\top\}$ as follows. If $u \in \mathcal{U}_k$, then $\Gamma_k(u) = (u \oplus v_1, \ldots, u \oplus v_j)$, where $v_1, \ldots, v_j$ enumerate $\mathcal{V}(u)$ lexicographically. If $u \notin \mathcal{U}_k$, then $\Gamma_k(u) = \{\top\}$. Then, for each $k \in \mathbf{N}$, let Γ_k be the infinite list obtained by concatenating the lists $\Gamma_k(u)$ for all $u \in \{0,1\}^*$. (The concatenation is lexicographic in u, i.e., $\Gamma_k = \Gamma_k(\lambda) \cdot \Gamma_k(0) \cdot \Gamma_k(1) \cdot \Gamma_k(00) \cdot \cdots$.) Finally, define a function

$$G : \mathbf{N} \times \mathbf{N} \to \{0,1\}^* \cup \{\top\}$$

by letting $G(k,l)$ be the l^{th} item in the list Γ_k. Since M_a and M_b are time-bounded machines, and since the lists $\Gamma_k(u)$ are all nonempty, it is clear by inspection that G is a total recursive function. We will show that G is a constructive null cover of the singleton set $\{A \oplus B\}$.

To see that G satisfies the covering condition, fix $k \in \mathbf{N}$. Since $D \notin \mathrm{BPP}$, (1.1) and the Kolmogorov [6] zero-one law tell us that $\Pr_E[L(M_b^E) = D] = 0$. It follows that there exists some $n \in \mathbf{N}$ such that the event

$$\mathcal{E}_n = \{E \mid L(M_b^E)_{\leq n} = D_{\leq n}\}$$

has probability $\Pr(\mathcal{E}_n) \leq 2^{-k}$. Let u be the characteristic string of $A_{<q(n)}$ and let v be the characteristic string of $B_{<q(n)}$. Note that $v \in \mathcal{V}(u)$. Also, by our choice of q and n, we have $2^{-k} \geq \Pr(\mathcal{E}_n) = 2^{-K(n)}|\mathcal{V}(u)|$. Thus $0 < |\mathcal{V}(u)| \leq 2^{K(n)-k}$. This implies that $u' \in \mathcal{U}_k$ for some prefix u' of u; say $u' \in \mathcal{U}_{k,n'}$, where $n' \leq n$. Let v' be the characteristic string of $B_{<q(n')}$. Then $v' \in \mathcal{V}(u')$ and $u' \in \mathcal{U}_k$, so $u' \oplus v'$ appears in the list Γ_k, i.e., $G(k,l) = u' \oplus v'$ for some $l \in \mathbf{N}$. We now have $A \oplus B \in C_{u \oplus v} \subseteq C_{u' \oplus v'} = C_{G(k,l)}$, so $\{A \oplus B\} \subseteq \bigcup\limits_{l=0}^{\infty} C_{G(k,l)}$, affirming the covering condition.

To see that G satisfies the measure condition, fix $k \in \mathbf{N}$ once again. Then

$$\begin{aligned}
\sum_{l=0}^{\infty} \Pr(C_{G(k,l)}) &= \sum_{u \in \mathcal{U}_k} \sum_{v \in \mathcal{V}(u)} 2^{-|u \oplus v|} \\
&= \sum_{n=0}^{\infty} \sum_{u \in \mathcal{U}_{k,n}} \sum_{v \in \mathcal{V}(u)} 2^{-N(n)} \\
&\leq \sum_{n=0}^{\infty} \sum_{u \in \mathcal{U}_{k,n}} 2^{K(n)-k-N(n)} \\
&= 2^{-k-1} \sum_{n=0}^{\infty} \sum_{u \in \mathcal{U}_{k,n}} 2^{-K(n)} \\
&= 2^{-k-1} \sum_{n=0}^{\infty} \sum_{u \in \mathcal{U}_{k,n}} 2^{-|u|} \\
&= 2^{-k-1} \sum_{u \in \mathcal{U}_k} 2^{-|u|} \\
&\leq 2^{-k-1},
\end{aligned}$$

by the Kraft inequality. We have now shown that G is a constructive null cover of $\{A \oplus B\}$, whence $A \oplus B$ is not random. □

4 Open Question

Our independent random oracle characterization extends the probability one oracle characterization (1.4) of Ambos-Spies [1] and Kurtz [7]. This extension is analogous to that from (1.1) to (1.3). However, our proof is *not* strong enough to give a result analogous to (1.2). We thus ask the following question: Does the *independent pseudorandom oracle characterization*

$$(\forall A \oplus B \in \mathrm{RAND}(\mathrm{pspace}))\ \mathrm{P}(A) \cap \mathrm{P}(B) = \mathrm{BPP}$$

hold?

References

[1] K. Ambos-Spies, Randomness, relativizations, and polynomial reducibilities, *Proceedings of the First Structure in Complexity Theory Conference*, 1986, pp. 23–34.

[2] C. H. Bennett and J. Gill, Relative to a random oracle A, $\mathrm{P}^A \neq \mathrm{NP}^A \neq \text{co-NP}^A$ with probability 1, *SIAM Journal on Computing* **10** (1981), pp. 96–113.

[3] G. J. Chaitin, A theory of program size formally identical to information theory, *Journal of the Association for Computing Machinery* **22** (1975), pp. 329–340.

[4] G. J. Chaitin, Incompleteness theorems for random reals, *Advances in Applied Mathematics* **8** (1987), pp. 119–146.

[5] J. Gill, Computational complexity of probabilistic Turing machines, *SIAM Journal on Computing* **6** (1977), pp. 675–695.

[6] A. N. Kolmogorov, *Grundbegriffe der Wahrscheinlichkeitsrechnung*, Berlin, 1933.

[7] S. Kurtz, A note on randomized polynomial time, *SIAM Journal on Computing* **16** (1987), pp. 852–853.

[8] L. A. Levin, On the notion of a random sequence, *Soviet Mathematics Doklady* **14** (1973), pp. 1413–1416.

[9] J. H. Lutz, Category and measure in complexity classes, *SIAM Journal on Computing* **19** (1990), pp. 1100–1131.

[10] J. H. Lutz, Pseudorandom sources for BPP, *Journal of Computer and System Sciences* **41** (1990), pp. 307–320.

[11] J. H. Lutz, Almost everywhere high nonuniform complexity, *Journal of Computer and System Sciences*, to appear. See also *Proceedings of the Fourth Structure in Complexity Theory Conference*, 1989, pp. 37–53.

[12] J. H. Lutz, A pseudorandom oracle characterization of BPP, *Proceedings of the Sixth Structure in Complexity Theory Conference*, 1991, to appear.

[13] P. Martin-Löf, On the definition of random sequences, *Information and Control* **9** (1966), pp. 602–619.

[14] N. Nisan and A. Wigderson, Hardness vs. randomness, *Proceedings of the 29th IEEE Symposium on Foundations of Computer Science*, 1988, pp. 2–11.

[15] J. C. Oxtoby, *Measure and Category*, Springer-Verlag, 1980, second edition.

[16] C. P. Schnorr, Process complexity and effective random tests, *Journal of Computer and System Sciences* **7** (1973), pp. 376–388.

[17] A. Kh. Shen′, On relations between different algorithmic definitions of randomness, *Soviet Mathematics Doklady* **38** (1989), pp. 316–319.

[18] R. M. Solovay, 1975, reported in [4].

[19] S. Tang and R. Book, Polynomial-time reducibilities and "almost-all" oracle sets, *Theoretical Computer Science* (1991), to appear.

[20] S. Tang and O. Watanabe, On tally relativizations of BP-complexity classes, *SIAM Journal on Computing* **18** (1989), pp. 449–462.