ALMOST-$\mathcal{R}$: Characterizations using Different Concepts of Randomness

Ronald V. Book
Department of Mathematics
University of California
Santa Barbara, CA 93106 USA
(e-mail: book@math.ucsb.edu)

and

Elvira Mayordomo*
Departament L. S. I.
Universitat Politècnica de Catalunya
Pau Gargallo 5
08028 Barcelona, Spain
(e-mail: mayordomo@lsi.upc.es)

Abstract

We study here the classes of the form ALMOST-R, for R a reducibility. This includes among other the classes BPP, P and PH. We give a characterization of this classes in terms of reducibility to n-random languages, a subclass of algorithmically random languages. We also give a characterization of classes of the form ALMOST-R in terms of resource bounded measure, for R reducibility of a restricted kind.

*supported by a Spanish Government Grant FPI PN90. This work was done while visiting the University of California, supported by this grant.

1 Introduction

The reducibilities normally used in complexity theory are *bounded reducibilities* (the formal definition is given in Section 2). If $\mathcal{R}$ is a bounded reducibility, then the class ALMOST-$\mathcal{R}$ is defined to be the class $\{A \mid \text{Prob}[\mathcal{R}^{-1}(A)] = 1\}$. This concept has proved useful in studying certain complexity classes that are well-studied in structural complexity theory. For example, P = ALMOST- $\leq_m^{\text{P}}$= ALMOST- $\leq_{\text{btt}}^{\text{P}}$, BPP = ALMOST- $\leq_{\text{T}}^{\text{P}}$, AM = ALMOST- $\leq_{\text{T}}^{\text{NP}}$, and PH = ALMOST- $\leq_{\text{T}}^{\text{PH}}$.

Book, Lutz, and Wagner [BLW93] showed that for every bounded reducibility, ALMOST-$\mathcal{R}$ = $\mathcal{R}$(RAND) $\cap$ REC, where RAND denotes the class of languages whose characteristic sequences are algorithmically random in the sense of Martin-Löf [Ma66], and REC denotes the class of recursive languages. This characterization leads to observations about the relationships between complexity classes such as (1) P = NP if and only if some language in RAND is $\leq_{\text{btt}}^{\text{P}}$-hard for NP and (2) PH = PSPACE if and only if some language in RAND is $\leq_{\text{T}}^{\text{PH}}$-hard for PSPACE. Book [Bo93] extended this characterization for certain bounded reducibilities called "appropriate" (all of the standard reducibilities used in structural complexity theory are appropriate) by showing

(1) **The Random Oracle Characterization:** for every $B \in$ RAND, ALMOST-$\mathcal{R}$ = $\mathcal{R}(B) \cap$ REC, and

(2) **The Independent Pair Characterization:** for every B and C such that $B \oplus C \in$ RAND, ALMOST-$\mathcal{R} = \mathcal{R}(B) \cap \mathcal{R}(C)$.

Here we present a new characterization of classes of the form ALMOST-$\mathcal{R}$, a characterization based on the notion of "n-randomness," which is a generalization of Martin-Löf randomness that is due to Kurtz [Ku81]. In addition, for certain reducibilities $\mathcal{R}$, we show that ALMOST-$\mathcal{R}$ can be characterized in terms of "Δ-randomness," a concept defined by Lutz [Lu92] in his study of resource-bounded measure.

2 Preliminaries

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 those reducibilities.

A *word* (string) is an element of $\{0,1\}^*$. The length of a word $w \in \{0,1\}^*$ is denoted by $|w|$. For a set A of strings and an integer $n > 0$, let $A_{\leq n} = \{x \in A \mid |x| \leq n\}$.

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

Let $\mathbf{C}_A$ be the characteristic function of A. The *characteristic sequence* χ_A 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 lexicographical order. We freely identify a language with its characteristic sequence and the class Ω of all languages on the fixed finite alphabet $\{0,1\}$ with the set $\{0,1\}^\omega$ of all such infinite sequences; context should resolve any ambiguity for the reader.

If L is a set of strings (i.e., a language) and $\mathbf{C}$ is a set of sequences (i.e., a class of languages), then $L \cdot \mathbf{C}$ denotes the set $\{w\xi \mid w \in L,\ \xi \in \mathbf{C}\}$. The complement of L is denoted by L^c and the complement of $\mathbf{C}$ is denoted by $\overline{\mathbf{C}}$.

For each string $w, \mathbf{C}_w = \{w\} \cdot \{0,1\}^\omega$ is the *basic open set* determined by w. An *open set* is a (finite or infinite) union of basic open sets, that is, 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.

For a class $\mathbf{C}$ of languages we write Prob[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 each string is in A. This probability is defined whenever $\mathbf{C}$ is measurable in the usual product topology on $\{0,1\}^*$. In particular, if $\mathbf{C}$ is a countable union or intersection of (recursively) open or closed sets, then $\mathbf{C}$ is measurable and so Prob[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. A class $\mathbf{C}$ is *closed under finite translation* if for all $w \in \{0,1\}^*$ and all $A \subseteq \{0,1\}^*$, $\{w\} \cdot A \in \mathbf{C}$ implies $A \in \mathbf{C}$.

The Kolmogorov 0–1 Law says that every measurable class $\mathbf{C} \subseteq \{0,1\}^\omega$ that is closed under finite variation has either probability 0 or probability 1.

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 more general setting than reducibilities computed in polynomial time and so we introduce a few definitions.

Assume a fixed enumeration $M_0, M_1, M_2, \ldots$ of deterministic 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 $\mathbf{C}$ of languages is a total recursive function $f : \mathsf{N} \longrightarrow \mathsf{N}$ such that for every language A and every $i \geq 0$, every computation of $M_{f(i)}(A)$ is halting and $\mathbf{C}(A) = \{L(M_{f(i)}, A) \mid i \in \mathsf{N}\}$. A relativized class is *recursively presentable* if it has a recursive presentation.

Notice that if for every A and every i, every computation of $M_{f(i)}(A)$ is halting, then $M_{f(i)}()$ has a running time that is bounded above by a recursive function.

A *reducibility* is a relativized class. A *bounded reducibility* is a relativized class that is recursively presentable. If $\mathcal{R}$ is a reducibility, then we use the notation $A \leq^{\mathcal{R}} B$ to indicate that $A \in \mathcal{R}(B)$, and we write $\mathcal{R}^{-1}(A)$ for $\{B \mid A \leq^{\mathcal{R}} B\}$. Typical bounded reducibilities include $\leq_m^{\mathrm{P}}$, $\leq_{\mathrm{btt}}^{\mathrm{P}}$, $\leq_{\mathrm{T}}^{\mathrm{P}}$, $\leq_{\mathrm{T}}^{\mathrm{NP}}$, $\leq_{\mathrm{T}}^{\mathrm{SN}}$, $\leq_m^{\mathrm{logspace}}$, etc. The relations $\leq_m$ and $\leq_{\mathrm{T}}$ (from recursive function theory) are reducibilities that are not bounded.

If $\mathcal{R}$ is a reducibility and $\mathbf{C}$ is a set of languages, write $\mathcal{R}(\mathbf{C})$ for $\bigcup_{A \in \mathbf{C}} \mathcal{R}(A)$.

A reducibility $\mathcal{R}$ will be called *appropriate* if (i) it is bounded, (ii) for any language A, $\mathcal{R}(A)$ is closed under finite variation, (iii) if B and D have finite symmetric difference and $A \in \mathcal{R}(B)$, then $A \in \mathcal{R}(D)$, and (iv) for any language L, $\mathcal{R}^{-1}(L)$ is closed under finite translation.

The reader should note that the reducibilites commonly used in structural complexity theory meet the conditions for being appropriate.

3 Using n-Randomness

In this section we develop our results about "n-randomness." First we review the concept of the arithmetical hierarchy of classes of languages due to Kleene (see Rogers [Ro67] for background).

Kleene's arithmetical hierarchy is defined as follows.

(i) Let Σ_1^0 be defined as $\{A \mid A \text{ is recursively open}\}$. We fix an enumeration of Σ_1^0 as follows: let $\{M_i\}_{i>0}$ be a recursive enumeration of all Turing machines (so that $\{L(M_i)\}_{i>0}$ is the class of recursively enumerable sets). If $A_i = L(M_i) \cdot \{0,1\}^\omega$, then $\Sigma_1^0 = \{A_i \mid i \in \mathsf{N}\}$.

(ii) We say that $\{C_j \mid j \in \mathsf{N}\}$ is a *uniform sequence in* Σ_1^0 if there exists a total recursive function g such that for every $j \in \mathsf{N}$, $C_j = A_{g(j)}$.

(iii) For every $n \geq 1$, $\Pi_n^0 = \{A \mid A^c \in \Sigma_n^0\}$.

(iv) We say that $\{D_j \mid j \in \mathsf{N}\}$ is a *uniform sequence in* Π_n^0 if there exists a uniform sequence in Σ_n^0, $\{C_j \mid j \in \mathsf{N}\}$, such that for every $j \in \mathsf{N}$, $D_j = C_j^c$.

(v) For every $n \geq 1$, $B \in \Sigma_{n+1}^0$ if there exists a uniform sequence in Π_n^0, $\{D_j \mid j \in \mathsf{N}\}$, such that $B = \bigcup_{k\in\mathsf{N}} D_k$.

(vi) We say that $\{C_j \mid j \in \mathsf{N}\}$ is a *uniform sequence in* Σ_{n+1}^0 if there exists a uniform sequence in Π_n^0, $\{D_{\langle j,k\rangle} \mid j,k \in \mathsf{N}\}$, such that for every $j \in \mathsf{N}$, $C_j = \bigcup_{k\in\mathsf{N}} D_{\langle j,k\rangle}$.

Now we define the concepts of "n-constructive null cover" and "n-random language" in a similar way to the introduction of null covers and random languages in [BLW93].

For $n \in \mathbb{N}$, a class $\mathbf{X}$ of languages has an *n-constructive null cover* if there exists a uniform sequence in Σ^0_n, $\{C_k \mid k \in \mathbb{N}\}$, such that

(i) for every $k \geq 1$, $\mathbf{X} \subseteq C_k$, and

(ii) for every $k \geq 1$, $\text{Prob}[C_k] < 2^{-k}$.

Notice that condition (ii) implies that every class with an n-constructive null cover has probability 0.

Let NULL_n denote the union of all classes that have an n-constructive null cover, that is, $\text{NULL}_n = \bigcup_{\mathbf{X} \text{ has an } n\text{-null cover}} \mathbf{X}$.

Notice that $\text{NULL}_n \subseteq \text{NULL}_{n+1}$. In the case of $n = 1$, we refer to the class as NULL, that is, $\text{NULL}_1 = \text{NULL}$.

The class RAND of *algorithmically random sequences* was defined by Martin-Löf [Ma66] as $\text{RAND} = \{0,1\}^\omega - \text{NULL}$.

The class of *algorithmically random languages*, also denoted by RAND, is the class of languages whose characteristic sequences are algorithmically random.

Book, Lutz, and Wagner [BLW93] studied the class RAND in the context of the classes ALMOST-$\mathcal{R}$ for appropriate reducibilties $\mathcal{R}$. Here we define, for each $n > 0$, the class "n-RAND" analogous to the definition of RAND.

If $n \in \mathbb{N}$, then define the class n-RAND by $n\text{-RAND} = \{0,1\}^\omega - \text{NULL}_n$.

Since $\text{NULL}_n \subseteq \text{NULL}_{n+1}$, $n{+}1\text{-RAND} \subseteq n\text{-RAND}$. Since $\text{NULL}_1 = \text{NULL}$, 1-RAND = RAND.

The class ALMOST-$\mathcal{R}$ studied in [BLW93] has the property that it is equal to $\{A \mid \text{RAND} \subseteq \mathcal{R}^{-1}(A)\}$ and so we define the class "ALMOST$_n$-$\mathcal{R}$" analogously.

If $\mathcal{R}$ is a bounded reducibility and $n \in \mathbb{N}$, then define the class ALMOST$_n$-$\mathcal{R}$ by

$$\text{ALMOST}_n\text{-}\mathcal{R} = \{A \mid n\text{-RAND} \subseteq \mathcal{R}^{-1}(A)\}.$$

Book, Lutz, and Wagner related each class ALMOST-R to the class RAND by showing that ALMOST-$\mathcal{R} = \mathcal{R}(\text{RAND}) \cap \text{REC}$. The main result of this paper is that each class

ALMOST$_n$-$\mathcal{R}$ is related to the class n-RAND in a similar way, and that ALMOST$_n$-$\mathcal{R}$ = ALMOST-$\mathcal{R}$.

We start with a technical lemma stating that for any language B in Δ^0_n, $\mathcal{R}^{-1}(B)$ is a class in Σ^0_{n+1}. This will be useful in the proof of our main theorem.

Lemma 3.1 *If $\mathcal{R}$ is a bounded reducibility and B is a language in Δ^0_n, then $\mathcal{R}^{-1}(B)$ is in Σ^0_{n+1}.*

Proof We consider only the case where n is odd, the other case being analogous.

Let g be a recursive presentation of $\mathcal{R}$. For every $j \geq 0$, let $\mathcal{R}_j^{-1}(B) = \{A \mid L(M_{g(j)}, A) = B\}$. Then $\mathcal{R}^{-1}(B) = \bigcup_{j\geq 0} \mathcal{R}_j^{-1}(B)$, and it suffices to show that if $B \in \Delta^0_n$, then $\{\mathcal{R}_j^{-1}(B) \mid j \geq 0\}$ is a uniform sequence in Π^0_n, or equivalently, $\{\overline{\mathcal{R}_j^{-1}(B)} \mid j \geq 0\}$ is a uniform sequence in Σ^0_n.

Since $B \in \Delta^0_n$, there exist recursive languages C and D such that $\forall x \in \{0,1\}^*$,

(i) $x \in B$ if and only if $\exists m_1 \forall m_2 \ldots \exists m_n(\langle x, m_1, \ldots, m_n\rangle \in C)$,

(ii) $x \notin B$ if and only if $\exists m_1 \forall m_2 \ldots \exists m_n(\langle x, m_1, \ldots, m_n\rangle \in D))$.

Consider a language A. Fix $j \geq 0$. Notice that $A \in \overline{\mathcal{R}_j^{-1}(B)}$ if and only if

(iii) $\exists x([x \in B] \neq [L(M_{g(j)}, A)(x)])$ if and only if

(iv) $\exists x[(x \in B \ \underline{\text{and}}\ [L(M_{g(j)}, A)(x)] = 0) \ \underline{\text{or}}\ (x \notin B \ \underline{\text{and}}\ [L(M_{g(j)}, A)(x)] = 1)]$.

Thus, combining (i)-(iv), we see that $A \in \overline{\mathcal{R}_j^{-1}(B)}$ if and only if

(v) $\exists x[(\exists m_1 \forall m_2 \ldots \exists m_n(\langle x, m_1, \ldots, m_n\rangle \in C) \ \underline{\text{and}}\ [L(M_{g(j)}, A)(x)] = 0) \ \underline{\text{or}}$
$(\exists m_1 \forall m_2 \ldots \exists m_n(\langle x, m_1, \ldots, m_n\rangle \in D) \ \underline{\text{and}}\ [L(M_{g(j)}, A)(x)] = 1)]$.

Using (v), we can express $\overline{\mathcal{R}_j^{-1}(B)}$ as follows:

$$\overline{\mathcal{R}_j^{-1}(B)} = \bigcup_x \bigcup_{m_1} \bigcap_{m_2} \cdots \bigcap_{m_{n-1}} (Y^j_{x,m_1,m_2\ldots,m_{n-1}} \cup Z^j_{x,m_1,m_2\ldots,m_{n-1}}) \tag{1}$$

where for fixed $x, m_1, m_2, \ldots, m_{n-1} \in \{0,1\}^*$,

$$Y^j_{x,m_1,m_2\ldots,m_{n-1}} = \{A \mid \exists m_n \langle x, m_1, \ldots, m_n\rangle \in C \text{ and } [L(M_{g(j)}, A)(x)] = 0\},$$

and

$$Z^j_{x,m_1,m_2\ldots,m_{n-1}} = \{A \mid \exists m_n \langle x, m_1, \ldots, m_n\rangle \in D \text{ and } [L(M_{g(j)}, A)(x)] = 1\}.$$

First we show that for fixed $x, m_1, m_2 \ldots, m_{n-1} \in \{0,1\}^*$, $Y^j_{x,m_1,m_2\ldots,m_{n-1}}$ is recursively open. To do this we define a partial recursive function $h^j_{x,m_1,m_2\ldots,m_{n-1}}$ as follows. For $m_n, z \in \{0,1\}^*$, if $\langle x, m_1, \ldots, m_n\rangle \in C$, $[L(M_{g(j)}, z0^\omega)(x)] = 0$ and $L(M_{g(j)}, z0^\omega)(x)$ needs only the initial part z of $z0^\omega$, then $h^j_{x,m_1,m_2\ldots,m_{n-1}}(z, m_n) = z$. Otherwise, $h^j_{x,m_1,m_2\ldots,m_{n-1}}(z, m_n)$ is undefined.

From the definition of $Y^j_{x,m_1,m_2\ldots,m_{n-1}}$ we know that $A \in Y^j_{x,m_1,m_2\ldots,m_{n-1}}$ if and only if there exists a prefix z of A such that $\langle x, m_1, \ldots, m_n\rangle \in C$, $[L(M_{g(j)}, z0^\omega)(x)] = 0$ and $L(M_{g(j)}, z0^\omega)(x)$ needs only the initial part z of $z0^\omega$. But this is exactly the definition of z being in the range of $h^j_{x,m_1,m_2\ldots,m_{n-1}}$. Thus $Y^j_{x,m_1,m_2\ldots,m_{n-1}} = \text{range}(h^j_{x,m_1,m_2\ldots,m_{n-1}}) \cdot \{0,1\}^\omega$, and $Y^j_{x,m_1,m_2\ldots,m_{n-1}}$ is recursively open. By a similar argument $Z^j_{x,m_1,m_2\ldots,m_{n-1}}$ is recursively open, using functions $f^j_{x,m_1,m_2\ldots,m_{n-1}}$.

We define a recursive function F that is the uniform version of all h's and f's as follows. For every $j \geq 0$, $x, m_1, m_2 \ldots, m_{n-1}, m_n, z \in \{0,1\}^*$,

$$F(j, x, m_1, m_2 \ldots, m_{n-1}, m_n, z0) = h^j_{x,m_1,m_2\ldots,m_{n-1}}(m_n, z),$$

$$F(j, x, m_1, m_2 \ldots, m_{n-1}, m_n, z1) = f^j_{x,m_1,m_2\ldots,m_{n-1}}(m_n, z).$$

F witnesses the fact that the sequence of classes

$$\{ \text{range}(h^j_{x,m_1,m_2\ldots,m_{n-1}}) \cdot \{0,1\}^\omega \bigcup \text{range}(f^j_{x,m_1,m_2\ldots,m_{n-1}}) \cdot \{0,1\}^\omega$$

$$\mid j \geq 0,\ x, m_1, m_2, \ldots, m_{n-1} \in \{0,1\}^* \}$$

is a uniform sequence in Σ^0_1.

To complete the proof note that $\{\overline{\mathcal{R}_j^{-1}(B)} \mid j \geq 0\}$ can be seen to be a uniform sequence in Σ_n^0 by using the expresion of $\overline{\mathcal{R}_j^{-1}(B)}$ in Equation 1, and the facts that $Y^j_{x,m_1,m_2\ldots,m_{n-1}} = \text{range}(h^j_{x,m_1,m_2\ldots,m_{n-1}}) \cdot \{0,1\}^\omega$, and $Z^j_{x,m_1,m_2\ldots,m_{n-1}} = \text{range}(f^j_{x,m_1,m_2\ldots,m_{n-1}}) \cdot \{0,1\}^\omega$. □

The proof of our main theorem is based on the following lemma due to Kautz [Ka91]. The proof is a straightforward generalization to $n > 1$ of the proof of Theorem 3.4 in [Bo93], which is itself a simplification of the proof of a result of Kautz.

Lemma 3.2 *Let* X *be a class in* Σ^0_{n+1} *that is closed under finite variation and finite translation. Then either* $\mathrm{X} \cap n$-RAND $= \emptyset$ *or* n-RAND $\subseteq \mathrm{X}$.

Now we have our main result.

Theorem 3.3 *For any bounded reduciblity* $\mathcal{R}$ *and any* $n > 0$,

a) $\mathsf{ALMOST}_n\text{-}\mathcal{R} = \mathcal{R}(n\text{-RAND}) \cap \Delta^0_n = \mathsf{ALMOST}\text{-}\mathcal{R}$;

b) *for every* $B \in n$-RAND, $\mathsf{ALMOST}\text{-}\mathcal{R} = \mathcal{R}(B) \cap \Delta^0_n$.

Proof First, we show that $\mathsf{ALMOST}\text{-}\mathcal{R} \subseteq \mathcal{R}(n\text{-RAND}) \cap \Delta^0_n$. Since NULL_n is a countable union of classes having probability 0, Prob[n-RAND] = 1. If $A \in \mathsf{ALMOST}\text{-}\mathcal{R}$, then $\mathrm{Prob}[\mathcal{R}^{-1}(A)] = 1$ and so $\mathcal{R}^{-1}(A) \cap n\text{-RAND} \neq \emptyset$ and hence, $A \in \mathcal{R}(n\text{-RAND})$. Since $\mathsf{ALMOST}\text{-}\mathcal{R} \subseteq \mathrm{REC}$, $\mathsf{ALMOST}\text{-}\mathcal{R} \subseteq \Delta^0_n$ and so $\mathsf{ALMOST}\text{-}\mathcal{R} \subseteq \mathcal{R}(n\text{-RAND}) \cap \Delta^0_n$.

Second, we show that $\mathcal{R}(n\text{-RAND}) \cap \Delta^0_n \subseteq \mathsf{ALMOST}\text{-}\mathcal{R}$. It follows from Lemma 3.1 that if $A \in \Delta^0_n$, then $\mathcal{R}^{-1}(A) \in \Sigma^0_{n+1}$. Since R is an appropiate reducibility as defined in the preliminaries, $\mathcal{R}^{-1}(A)$ is closed under finite variation and is closed under under finite translation. By Lemma 3.2, either $n\text{-RAND} \subseteq \mathcal{R}^{-1}(A)$ or $n\text{-RAND} \cap \mathcal{R}^{-1}(A) = \emptyset$. If $A \in \mathcal{R}(n\text{-RAND}) \cap \Delta^0_n$, then $n\text{-RAND} \cap \mathcal{R}^{-1}(A) \neq \emptyset$ and so $n\text{-RAND} \subseteq \mathcal{R}^{-1}(A)$. Thus, $\mathrm{Prob}[\mathcal{R}^{-1}(A)] = 1$ so that $A \in \mathsf{ALMOST}\text{-}\mathcal{R}$.

Third, we show that for every $B \in n$-RAND, $\mathsf{ALMOST}\text{-}\mathcal{R} = \mathcal{R}(B) \cap \Delta^0_n$. From a) it follows that $\mathcal{R}(B) \cap \Delta^0_n \subseteq \mathsf{ALMOST}\text{-}\mathcal{R}$. If $A \in \mathsf{ALMOST}\text{-}\mathcal{R}$, then $\mathcal{R}^{-1}(A) \cap n\text{-RAND} \neq \emptyset$ by the first argument in this proof. It follows from Lemma 3.1 that $n\text{-RAND} \subseteq \mathcal{R}^{-1}(A)$, and $A \in \mathcal{R}(B)$. Hence, ALMOST-$\mathcal{R} \subseteq \mathcal{R}(B)$. Since ALMOST-$\mathcal{R} \subseteq$ REC, this means that ALMOST-$\mathcal{R} \subseteq \Delta_n^0$ and so ALMOST-$\mathcal{R} \subseteq \mathcal{R}(B) \cap \Delta_n^0$.

Finally, the proof that ALMOST-$\mathcal{R}$ = ALMOST$_n$-$\mathcal{R}$ follows from b) and the definition of ALMOST$_n$-$\mathcal{R}$. □

Thus, Theorem 3.3 extends the Random Oracle Characterization to classes having the form ALMOST$_n$-$\mathcal{R}$ by showing that for every $n > 0$ and every $B \in n$-RAND, ALMOST-$\mathcal{R}$ = $\mathcal{R}(B) \cap \Delta_n^0 = \mathcal{R}(n\text{-RAND}) \cap \Delta_n^0$ = ALMOST$_n$-$\mathcal{R}$. As a corollary we see that the Independent Pair Characterization, as stated in the Introduction, can also be extended.

Corollary 3.4 *Let $n \geq 1$. For every B and C such that $B \oplus C \in n$-RAND, ALMOST$_n$-$\mathcal{R}$ = $\mathcal{R}(B) \cap \mathcal{R}(C)$.*

Proof If $B \oplus C \in n$-RAND, then $B \oplus C \in$ RAND since n-RAND $\subseteq$ RAND. Since $B \oplus C \in$ RAND, ALMOST-$\mathcal{R} = \mathcal{R}(B) \cap \mathcal{R}(C)$ by The Independent Pair Characterization. By Theorem 3.3 we have ALMOST$_n$-$\mathcal{R}$ = ALMOST-$\mathcal{R}$ so that ALMOST$_n$-$\mathcal{R} = \mathcal{R}(B) \cap \mathcal{R}(C)$. □

4 Using Δ-measure

In this section we use the concept of "Δ-measure 0" that was introduced by Lutz in his development of resource-bounded measure, a generalization of classical Lebesgue measure, that he used to classify complexity classes by their size. We use this concept to give a different characterization of ALMOST-$\mathcal{R}$. See [Lu92] for a complete introduction to resource-bounded measure.

We consider four classes of functions from $\{0,1\}^*$ to $\{0,1\}^*$, the class *all* of all such functions, the class *rec* of total recursive functions, the class *p* of functions computed in polynomial time, and the class *pspace* of functions computed in polynomial space. Here, Δ is a variable taking only the four classes *all*, *rec*, *p*, and *pspace* as values.

A *martingale* is a function $d : \{0,1\}^* \longrightarrow [0, \infty)$ with the property that for every $w \in \{0,1\}^*$, $d(w) = (d(w0) + d(w1))/2$. For each martingale d, define the class $S[d]$ as $S[d] =$

$\{L \mid \limsup_{n\to\infty} d(\chi_L[0..n]) = \infty\}$, where $\chi_L[0..n]$ is the string consisting of the 0^{th} to n^{th} bits in χ_L.

A function $d : \{0,1\}^* \longrightarrow [0,\infty)$ is Δ-*approximable* if there exists $\hat{d} : \{0,1\}^* \times \mathsf{N} \longrightarrow \mathsf{D}$, where $\mathsf{D} = \{2^{-n}m \mid n,m \in \mathsf{N}\}$, such that for all $i \in \mathsf{N}$ and all $w \in \{0,1\}^*$, $|d(w) - \hat{d}(i,w)| \leq 2^{-i}$.

A class $\mathbf{X}$ of languages has Δ-*measure* 0 if there exists a Δ-approximable martingale d such that $\mathbf{X} \subseteq S[d]$; this is denoted by $\mu_\Delta(\mathbf{X}) = 0$. A class $\mathbf{X}$ has Δ-*measure* 1, denoted by $\mu_\Delta(\mathbf{X}) = 1$, if $\mu_\Delta(\overline{\mathbf{X}}) = 0$.

Due to the Kolmogorov 0-1 Law, we only need to consider Δ-measure 0 and Δ-measure 1 (see [Lu92]).

Let Δ be a class of functions. Define the following:

i. $\mathrm{NULL}_\Delta = \bigcup_{\mu_\Delta(\mathbf{X})=0} \mathbf{X}$;

ii. $\Delta\text{-RAND} = \{0,1\}^\omega - \mathrm{NULL}_\Delta$;

iii. $\mathsf{ALMOST}_\Delta\text{-}\mathcal{R} = \{A \mid \mu_\Delta(\mathcal{R}^{-1}(A)) = 1\}$.

It follows easily from the definitions that for every $n > 0$, $\mathrm{NULL}_\Delta \subseteq \mathrm{NULL} \subseteq \mathrm{NULL}_n$ and $\Delta\text{-RAND} \supseteq \mathrm{RAND} \supseteq n\text{-RAND}$.

For reducibilities $\mathcal{R}$, there are two conditions of interest here: (1) $\mathsf{ALMOST}\text{-}\mathcal{R} \subseteq \mathcal{R}(\emptyset)$, and (2) for every A, $\mathcal{R}(\emptyset) \subseteq \mathcal{R}(A)$. Examples of reducibilities meeting both of these conditions are $\leq^{\mathrm{P}}_{\mathrm{btt}}, \leq^{\mathrm{PH}}_{\mathrm{T}}$, and $\leq^{\mathrm{PQH}}_{\mathrm{T}}$, where $\leq^{\mathrm{PQH}}_{\mathrm{T}}$ is defined by $A \leq^{\mathrm{PQH}}_{\mathrm{T}} B$ if and only if $A \leq^{\mathrm{PH}}_{\mathrm{T}} B \oplus \mathrm{QBF}$. Observe that for these examples, the values of $\mathcal{R}(\emptyset)$ are P, PH, and PSPACE, respectively.

We prove that for reducibilities $\mathcal{R}$ satisfying both of conditions (1) and (2), $\mathsf{ALMOST}_\Delta\text{-}\mathcal{R}$ is exactly the class $\mathsf{ALMOST}\text{-}\mathcal{R}$.

Theorem 4.1 *Let $\mathcal{R}$ be a bounded reducibility that satisfies conditions (1) and (2). Then* $\mathsf{ALMOST}\text{-}\mathcal{R} = \mathsf{ALMOST}_\Delta\text{-}\mathcal{R}$ *and for every $B \in \Delta$-RAND,* $\mathsf{ALMOST}_\Delta\text{-}\mathcal{R} \subseteq \mathcal{R}(B) \cap \mathrm{REC}$.

Proof First, we show that $\mathsf{ALMOST}\text{-}\mathcal{R} \subseteq \mathsf{ALMOST}_\Delta\text{-}\mathcal{R}$. For any $A \in \mathsf{ALMOST}\text{-}\mathcal{R}$, $A \in \mathcal{R}(\emptyset)$ by condition (1). It follows from condition (2) that $\mathcal{R}^{-1}(A) = \{0,1\}^\omega$. But $\mu_\Delta(\{0,1\}^\omega) =$

1 so that $A \in \mathsf{ALMOST}_\Delta\text{-}\mathcal{R}$.

Second, we show that $\mathsf{ALMOST}_\Delta\text{-}\mathcal{R} \subseteq \mathsf{ALMOST}\text{-}\mathcal{R}$. For any $A \in \mathsf{ALMOST}_\Delta\text{-}\mathcal{R}$, if $\mu_\Delta(\mathcal{R}^{-1}(A)) = 1$, then $\mu_\Delta(\overline{\mathcal{R}^{-1}(A)}) = 0$ so that $\mathrm{Prob}[\overline{\mathcal{R}^{-1}(A)}] = 0$. Hence, $\mathrm{Prob}[\mathcal{R}^{-1}(A)] = 1$, and so $A \in \mathsf{ALMOST}\text{-}\mathcal{R}$.

Third, we show that $\mathsf{ALMOST}_\Delta\text{-}\mathcal{R} \subseteq \mathcal{R}(B) \cap \mathrm{REC}$. If $A \in \mathsf{ALMOST}_\Delta\text{-}\mathcal{R}$, then $\mu_\Delta(\mathcal{R}^{-1}(A)) = 1$ implies that $\Delta\text{-RAND} \subseteq \mathcal{R}^{-1}(A)$, which means that for every $B \in \Delta\text{-RAND}$, $A \in \mathcal{R}(B)$.
□

5 Remarks

For any appropriate reducibility $\mathcal{R}$, the class $\mathsf{ALMOST}\text{-}\mathcal{R}$ is defined to be $\{A \mid \mathrm{Prob}[\mathcal{R}^{-1}(A)] = 1\}$. Book, Lutz, and Wagner gave an alternative (intrinsic) characterization: $\mathsf{ALMOST}\text{-}\mathcal{R} = \mathcal{R}(\mathrm{RAND}) \cap \mathrm{REC}$. Naturally, different classes are obtained by considering different reducibilities $\mathcal{R}$. Other possibilities include substituting other classes for RAND and substituting other classes for REC.

Lutz and Martin (personal communication) have considered the following situation: take a reducibility $\mathcal{R}$ and restrict it so that only a bounded number of queries can be made (making it like a "bounded truth-table" or "bounded Turing" reducibility) while maintaining the bounds on computational complexity. If $\mathcal{R}_b$ denotes the result, then $\mathcal{R}_b(\mathrm{RAND}) \cap \Sigma_1^0 = \mathsf{ALMOST}\text{-}\mathcal{R}_b \subseteq \mathsf{ALMOST}\text{-}\mathcal{R}$.

Kautz and Lutz (personal communication) went in the other direction. If $\mathcal{R}$ is a reducibility that is not bounded truth-table or bounded Turing, then $\mathcal{R}(\mathrm{RAND}) \cap \Sigma_1^0 \neq \mathsf{ALMOST}\text{-}\mathcal{R}$ (but clearly $\mathsf{ALMOST}\text{-}\mathcal{R} \subset \mathcal{R}(\mathrm{RAND}) \cap \Sigma_1^0$).

In the current paper we have not considered any variation in $\mathcal{R}$. Rather, we have considered subclasses of RAND having the form n-RAND and superclasses of REC having the form Δ_n^0. In this case we showed that $\mathcal{R}(n\text{-RAND}) \cap \Delta_n^0 = \mathsf{ALMOST}\text{-}\mathcal{R}$. Thus, as n varies, the subclass of RAND becomes smaller and the superclass of REC becomes larger, but still the bounded reducibility $\mathcal{R}$ forces $\mathcal{R}(n\text{-RAND}) \cap \Delta_n^0$ to be just $\mathsf{ALMOST}\text{-}\mathcal{R}$.

These results show that classes of the form n-RAND (and Δ-RAND) yield the same complexity classes as RAND when studying classes characterized as ALMOST-$\mathcal{R}$. Hence, these classes may be useful in studying the idea of "complexity-theoretic pseudo-randomness" just as RAND is useful in studying "intrinsic randomness." This paper represents only a first step in this investigation.

References

[Bo93] R. Book, On languages reducible to algorithmically random languages, submitted for publication, 1993.

[BLW93] R. Book, J. Lutz, and K. Wagner, An observation on probability versus randomness with applications to complexity classes, *Math. Systems Theory* 26 (1993), to appear.

[Ka91] S. Kautz, *Degrees of Random Sets*, Ph.D. Dissertation, Cornell University, 1991.

[Ku81] S. Kurtz, *Randomness and Genericity in the Degrees of Unsolvability*, Ph.D. Dissertation, University of Illinois at Urbana-Champaign, 1981.

[Lu92] J. Lutz, Almost-everywhere high nonuniform complexity, *J. Comput. System. Sci.* 25 (1992), 130-143.

[Ma66] P. Martin-Löf, On the definition of infinite random sequences, *Info. and Control* 9 (1966), 602-619.

[Ro67] H. Rogers, *Theory of Recursive Functions and Effective Computatibility*, McGraw-Hill, 1967.