On the Robustness of ALMOST-$\mathcal{R}$

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

Elvira Mayordomo†
Dept. de Informática
C.P.S., Univ. de Zaragoza
María de Luna 3
50015 Zaragoza, Spain
(elvira@prometeo.cps.unizar.es)

Abstract

We study the classes of the form ALMOST-R, for R a reducibility. This includes, among others, the classes BPP, P and PH. We give a characterization of these classes in terms of reductions to n-random languages, a subclass of algorithmically random languages. We also discuss the possibility of characterizing the classes ALMOST-R in terms of resource bounded measure.

*Supported in part by the National Science Foundation under Grant CCR-9302057.
†Supported by a Spanish Government Grant FPI PN90 and by DGICYT project PB94–0564. This work was done while visiting the University of California, Santa Barbara.

1 Introduction

Given a reducibility $\mathcal{R}$, the class $\mathsf{ALMOST}\text{-}\mathcal{R}$ is defined as the class of languages A such that $\mathcal{R}^{-1}(A)$ has Lebesgue probability 1. The "$\mathsf{ALMOST}\text{-}\mathcal{R}$" formalism, studied for instance in [Bo94] and [BLW94], provides characterizations of some interesting complexity classes, among others, $\mathsf{ALMOST}\text{-}\leq_m^{\mathrm{P}} = \mathrm{P}$ [Am86], $\mathrm{P} = \mathsf{ALMOST}\text{-}\leq_{\mathrm{btt}}^{\mathrm{P}}$ [TB91], $\mathrm{BPP} = \mathsf{ALMOST}\text{-}\leq_{\mathrm{T}}^{\mathrm{P}}$ ([Am86], [BG81]), $\mathrm{BPP} = \mathsf{ALMOST}\text{-}\leq_{\mathrm{tt}}^{\mathrm{P}}$ [TB91], $\mathrm{AM} = \mathsf{ALMOST}\text{-}\leq_{\mathrm{T}}^{\mathrm{NP}}$ ([Ca89], [NW88]), and $\mathrm{PH} = \mathsf{ALMOST}\text{-}\leq_{\mathrm{T}}^{\mathrm{PH}}$ ([Ca89], [NW88]).

Book, Lutz, and Wagner [BLW94] characterized these classes in terms of Martin-Löf algorithmically random languages, where Martin-Löf algorithmic randomness is the strongest definition that is regarded as representing randomness of individual infinite sequences. Considering a subset of all reducibilities (that includes all of the standard reducibilities used in structural complexity theory), they showed that $\mathsf{ALMOST}\text{-}\mathcal{R} = \mathcal{R}(\mathrm{RAND}) \cap \mathrm{REC}$, where RAND denotes the class of Martin-Löf algorithmically random languages, and REC denotes the class of recursive languages. This characterization lead to observations about the relationships between complexity classes such as: $\mathrm{P} = \mathrm{NP}$ if and only if some language in RAND is $\leq_{\mathrm{btt}}^{\mathrm{P}}$-hard for NP, and $\mathrm{PH} = \mathrm{PSPACE}$ if and only if some language in RAND is $\leq_{\mathrm{T}}^{\mathrm{PH}}$-hard for PSPACE. Book [Bo94] extended this characterization by showing the *Random Oracle Characterization*, namely that for every $B \in \mathrm{RAND}$, $\mathsf{ALMOST}\text{-}\mathcal{R} = \mathcal{R}(B) \cap \mathrm{REC}$, and the *Independent Pair Characterization*, namely that for every B and C such that $B \oplus C \in \mathrm{RAND}$, $\mathsf{ALMOST}\text{-}\mathcal{R} = \mathcal{R}(B) \cap \mathcal{R}(C)$.

While different classes are obtained in the characterization of $\mathsf{ALMOST}\text{-}\mathcal{R}$ as $\mathcal{R}(\mathrm{RAND}) \cap \mathrm{REC}$ by considering different reducibilities $\mathcal{R}$, here we are concerned with the possibility of obtaining different classes by considering as parameter values the classes RAND and REC. In particular, we investigate the result of substituting specific subclasses of RAND for RAND itself. For each natural n, we find that if we substitute a class based on Kurtz's notion of "n-randomness" (defined in [Ku81]) and simultaneously substitute the class Δ_n^0 (from the arithmetical hierarchy of languages) for the class REC, then once again the result is $\mathsf{ALMOST}\text{-}\mathcal{R}$. That is, $\mathcal{R}(n\text{-RAND}) \cap \Delta_n^0 = \mathsf{ALMOST}\text{-}\mathcal{R}$ (Theorem 3.3 (a) and (c)).

Considering the Kleene arithmetical hierarchy as a whole, we show that a language A in it is in $\mathsf{ALMOST}\text{-}\mathcal{R}$ if and only if A is $\mathcal{R}$-reducible to an ω-random language. The concept of "ω-randomness" is, in a sense, the "limit" of the n-random sets, and has been introduced in [Ku81].

Notice that since $\mathsf{ALMOST}\text{-}\mathcal{R}$ is a recursive class, these results show that there are no languages from $\Delta_n^0 - \mathrm{REC}$ in $\mathcal{R}(n\text{-RAND})$, that is, oracles in n-RAND are useless for $\Delta_n^0 - \mathrm{REC}$. In the same way, oracles in ω-RAND are useless for $AH - \mathrm{REC}$

Our new characterizations of classes having the form $\mathsf{ALMOST}\text{-}\mathcal{R}$ imply a robustness property of these classes. The parameters $\mathcal{C}$ and $\mathcal{D}$ in $\mathsf{ALMOST}\text{-}\mathcal{R} = \mathcal{R}(\mathcal{C}) \cap \mathcal{D}$ may vary, while the result is always $\mathsf{ALMOST}\text{-}\mathcal{R}$.

All our results hold for bounded reducibilities that are invariant under finite variations of the oracle. This restriction is the same that is used in [BLW94], and is more general than the one in [Bo94] where invariance under finite translation is also required.

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 $n \geq 0$, 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 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 the sequence $\{x_0, x_1, x_2, \ldots\} = \{0,1\}^*$ in lexicographical order. We freely identify a language with its characteristic sequence and the class $\mathcal{P}(\{0,1\}^*)$ 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 $\mathbf{C}^c$. The class of complements $\mathrm{co} - \mathbf{C}$ is defined as $\mathrm{co} - \mathbf{C} = \{L^c \mid L \in \mathbf{C}\}$.

Given an oracle Turing machine M and a language D, $L(M, D)$ stands for the set accepted by machine M with oracle D. Given a string x, $M^D(x)$ represents the output of M on input x and with oracle D.

Assume a fixed effective enumeration $M_1, M_2, \ldots$ of all deterministic oracle Turing machines. For each language D and $i > 0$, $W_i^D = L(M_i, D)$, therefore, $W_1^D, W_2^D \ldots$ is an enumeration of all languages in RE^D.

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. Let D be a language. A class of languages is *recursively open relative to oracle* D if it is of the form $W_i^D \cdot \{0,1\}^\omega$ for some $i > 0$. A class of languages is *recursively closed relative to* D if it is the complement of some relative to D recursively open set.

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 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[$\mathbf{C}$] is defined. Note that for each oracle D, there are only countably many recursively open sets, so every intersection of recursively open sets relative to D is a countable intersection of such sets, and hence is measurable; similarly every union of recursively closed sets relative to D 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 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.

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 $i > 0$, $M^A_{f(i)}(x)$ is halting for every oracle A and input x, and $\mathbf{C}(A) = \{L(M_{f(i)}, A) \mid i > 0\}$. 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 $\mathcal{R}$ 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 $\leq^{\mathrm{P}}_m$, $\leq^{\mathrm{P}}_{\mathrm{btt}}$, $\leq^{\mathrm{P}}_{\mathrm{T}}$, $\leq^{\mathrm{NP}}_{\mathrm{T}}$, $\leq^{\mathrm{SN}}_{\mathrm{T}}$, $\leq^{\mathrm{logspace}}_m$, etc. The relations $\leq_m$ and $\leq_{\mathrm{T}}$ (from recursive function theory) are reducibilities that are not bounded. A reducibility $\mathcal{R}$ will be called *appropriate* if (i) it is bounded, (ii) for any language L, $\mathcal{R}^{-1}(L)$ is closed under finite variation. This definition of appropriate reducibility is less restrictive than the original one presented in [Bo94], but with this new definition all the results in [Bo94] still hold, as Kautz remarked in [Ka94].

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

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

Given a language D, we will denote with AH^D *the arithmetical hierarchy of languages relative to oracle* D, that is,

(i) $\Sigma_1^D = \mathrm{RE}^D = \{A \subseteq \{0,1\}^* \mid A = L(M,D) \text{ for a Turing Machine } M\}$,

(ii) for every $n > 0$, $\Sigma_{n+1}^D = \mathrm{RE}^{\Sigma_n^D}$,

(iii) for every $n > 0$, $\Pi_n^D = \mathrm{co} - \Sigma_n^D$,

(iv) for every $n > 0$, $\Delta_n^D = \Sigma_n^D \cap \Pi_n^D$,

(v) $AH^D = \bigcup_{n>0}\Sigma_n^D$.

For $D = \emptyset$, we get the unrelativized arithmetical hierarchy, usually denoted with Σ_n^0, Π_n^0, Δ_n^0 and AH. For each $n > 0$, we denote as $K^{(n)}$ the standard many-one complete set for Σ_n^0, that is, $\Sigma_n^0 = \Sigma_1^{K^{(n-1)}}$. For $n = 0$, $K^{(0)} = \emptyset$.

3 Using n-Randomness

In this section we develop our results that relate "n-randomness" with the classes of the form ALMOST-$\mathcal{R}$. We first define the concepts of "D-constructive null set" and "D-random language" in a similar way to the introduction of null sets and random languages in [BLW94].

Let D be a language, a class $\mathbf{X}$ of languages is called a *D-constructive null set* if there is a total recursive function g such that

(i) for every $k \geq 1$, $\mathbf{X} \subseteq W_{g(k)}^D$, and

(ii) for every $k \geq 1$, $\mathrm{Prob}[W_{g(k)}^D] < 2^{-k}$.

Notice that condition (ii) implies that every D-constructive null set has probability 0.

Let NULL^D denote the union of all D-constructive null sets. The class RAND^D of *algorithmically random languages relative to* D is defined as in [Ma66], $\mathrm{RAND}^D = \{0,1\}^\omega - \mathrm{NULL}^D$.

We define n-randomness in terms of $K^{(n-1)}$-constructive null sets, that is, let $\mathrm{NULL}_n = \mathrm{NULL}^{K^{(n-1)}}$ and let $n\text{-RAND} = \{0,1\}^\omega - \mathrm{NULL}_n$.

Notice that $\mathrm{NULL}_n \subseteq \mathrm{NULL}_{n+1}$ and that $n+1\text{-RAND} \subseteq n\text{-RAND}$. In the case of $n = 1$, we use the notation $\mathrm{NULL} = \mathrm{NULL}_1$ and $\mathrm{RAND} =$ 1-RAND.

Omega-randomness is the "limit of" n-randomness, defined as

$$\omega\text{-RAND} = \bigcap_n n\text{-RAND}.$$

From the results in [Bo94], we know that

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

If we have n-RAND in the place of RAND, which languages fulfill $n\text{-RAND} \subseteq \mathcal{R}^{-1}(A)$? This question motivates the next definition.

If $\mathcal{R}$ is a reducibility and $n > 0$, then define the class $\mathsf{ALMOST}_n\text{-}\mathcal{R}$ by

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

and the class $\mathsf{ALMOST}_\omega\text{-}\mathcal{R}$ by

$$\mathsf{ALMOST}_\omega\text{-}\mathcal{R} = \{A \mid \omega\text{-RAND} \subseteq \mathcal{R}^{-1}(A)\}.$$

In [BLW94] Book, Lutz, and Wagner studied the classes $\mathsf{ALMOST}\text{-}\mathcal{R}$ and related them to the class RAND by showing that $\mathsf{ALMOST}\text{-}\mathcal{R} = \mathcal{R}(\mathrm{RAND}) \cap$ REC. The main result of this paper is that each class $\mathsf{ALMOST}_n\text{-}\mathcal{R}$ is related to the class n-RAND in a very similar way, and that $\mathsf{ALMOST}_n\text{-}\mathcal{R} = \mathsf{ALMOST}\text{-}\mathcal{R}$. We also obtain similar results for $\mathsf{ALMOST}_\omega\text{-}\mathcal{R}$ and ω-RAND.

We begin with a technical lemma stating that for any language A in REC^D, $\mathcal{R}^{-1}(A)$ is a class in Σ_2^D. This will be useful in the proof of our main theorem. We next recall the definition of Σ_n^D, the Kleene's arithmetical hierarchy of classes of languages, that can be found for instance in [Ro67].

Definition. Let D be a language. Let X be a class of languages, let $n > 0$. Then X is in Σ_n^D if and only if there exists a predicate P that is recursive in D and such that

$$X = \{A \mid \exists x_1 \, \forall x_2 \ldots Q_n x_n \; P(A, x_1, \ldots, x_n)\},$$

where Q_n is $\exists$ if n is odd, and $\forall$ otherwise.

Note that classically the same notation is used for both the arithmetical hierarchy of languages defined in the preliminaries (where Σ_n^D denotes a set of languages) and the arithmetical hierarchy of classes of languages we just defined (where Σ_n^D denotes a set of classes). The meaning in each case will be clear from the context.

Lemma 3.1 *If $\mathcal{R}$ is a bounded reducibility and B is a language in* REC^D*, then $\mathcal{R}^{-1}(B)$ is in Σ_2^D.*

Proof Let B be as in the hypothesis. Since $B \in \mathrm{REC}^D$, there exist a Turing Machine M such that $\forall x \in \{0,1\}^*$, $M^D(x) \in \{0,1\}$ and

$$x \in B \text{ if and only if } M^D(x) = 1. \tag{1}$$

Let g be a recursive presentation of $\mathcal{R}$. Then $A \in \mathcal{R}^{-1}(B)$ if and only if there exists $j > 0$ such that $B = L(M_{g(j)}, A)$.

The condition on A, $B = L(M_{g(j)}, A)$ is equivalent to

$$\forall x \; x \in B \Leftrightarrow M^A_{g(j)}(x),$$

which is equivalent to

$$\forall x \; [(x \in B \wedge M^A_{g(j)}(x) = 1) \vee (x \notin B \wedge M^A_{g(j)}(x) = 0)].$$

Using equation 1 we have that $A \in \mathcal{R}^{-1}(B)$ if and only if

$$\exists j \, \forall x \; [(M^D(x) = 1 \wedge M^A_{g(j)}(x) = 1) \vee (M^D(x) = 0 \wedge M^A_{g(j)}(x) = 0)].$$

Since machine M halts on every input, the predicate $P(A, j, x)$ defined as

$$[(M^D(x) = 1 \wedge M^A_{g(j)}(x) = 1) \vee (M^D(x) = 0 \wedge M^A_{g(j)}(x) = 0)].$$

is recursive in D. This proves that $\mathcal{R}^{-1}(B) \in \Sigma_2^D$. □

The proof of our main theorem is based on the following zero-one law for n-RAND that is due to Kautz [Ka94] (see also [Ka91], where a more restrictive version of this lemma is proven).

Lemma 3.2 *Let $\mathbf{X}$ be a class in Σ_2^D that is closed under finite variation. Then either $\mathbf{X} \cap \mathrm{RAND}^D = \emptyset$ or $\mathrm{RAND}^D \subseteq \mathbf{X}$.*

Lemmas 3.1 and 3.2 together imply the following corollary

Corollary 3.3 *For any appropriate reducibility $\mathcal{R}$ and for any language D,*
a) *for every $B \in \mathrm{RAND}^D$, $\mathsf{ALMOST}\text{-}\mathcal{R} = \mathcal{R}(B) \cap \mathrm{REC}^D$;*
b) $\mathsf{ALMOST}\text{-}\mathcal{R} = \mathcal{R}(\mathrm{RAND}^D) \cap \mathrm{REC}^D$.

Proof Let $B \in \mathrm{RAND}^D$. We start by remarking that $\mathrm{RAND}^D \subseteq \mathrm{RAND}$ by definition (since $\mathrm{NULL} \subseteq \mathrm{NULL}^D$). Therefore, by the *Random Oracle Characterization* in [Bo94],

$$\mathsf{ALMOST}\text{-}\mathcal{R} = \mathcal{R}(B) \cap \mathrm{REC} \subseteq \mathcal{R}(B) \cap \mathrm{REC}^D.$$

For the other part, let $A \in \mathcal{R}(B) \cap \mathrm{REC}^D$. By Lemma 3.1, $\mathcal{R}^{-1}(A) \in \Sigma_2^D$, and by Lemma 3.2, either $\mathcal{R}^{-1}(A) \cap \mathrm{RAND}^D = \emptyset$ or $\mathrm{RAND}^D \subseteq \mathcal{R}^{-1}(A)$. Since $B \in \mathcal{R}^{-1}(A) \cap \mathrm{RAND}^D$, $\mathrm{RAND}^D \subseteq \mathcal{R}^{-1}(A)$.

But RAND^D is a countable intersection of measure 1 classes, therefore $\mathrm{Prob}[\mathrm{RAND}^D] = 1 = \mathrm{Prob}[\mathcal{R}^{-1}(A)]$, and $A \in \mathsf{ALMOST}\text{-}\mathcal{R}$. This completes the proof of a).

Part b) follows directly from a). □

Now we have our main result.

Theorem 3.4 *For any appropriate reducibility $\mathcal{R}$ and any $n > 0$,*
a) $\mathsf{ALMOST}_n\text{-}\mathcal{R} = \mathcal{R}(n\text{-RAND}) \cap \Delta_n^0$;
b) *for every $B \in n\text{-RAND}$, $\mathsf{ALMOST}_n\text{-}\mathcal{R} = \mathcal{R}(B) \cap \Delta_n^0$;*
c) $\mathsf{ALMOST}_n\text{-}\mathcal{R} = \mathsf{ALMOST}\text{-}\mathcal{R}$.

Proof From Corollary 3.3, taking $D = K^{(n-1)}$, we know that for each $B \in n\text{-RAND}$,

$$\mathsf{ALMOST}\text{-}\mathcal{R} = \mathcal{R}(B) \cap \Delta_n^0. \tag{2}$$

and that

$$\mathsf{ALMOST}\text{-}\mathcal{R} = \mathcal{R}(n\text{-RAND}) \cap \Delta_n^0.$$

Since equation 2 holds for every $B \in n\text{-RAND}$, we have that for each $A \in \mathsf{ALMOST}\text{-}\mathcal{R}$, $n\text{-RAND} \subseteq \mathcal{R}^{-1}(A)$, therefore $A \in \mathsf{ALMOST}_n\text{-}\mathcal{R}$, and $\mathsf{ALMOST}\text{-}\mathcal{R} \subseteq \mathsf{ALMOST}_n\text{-}\mathcal{R}$.

As remarked below, for each D, $\mathrm{Prob}[\mathrm{RAND}^D] = 1$. This implies that $\mathrm{Prob}[n\text{-RAND}] = 1$ and $\mathsf{ALMOST}_n\text{-}\mathcal{R} \subseteq \mathsf{ALMOST}\text{-}\mathcal{R}$ for every $n > 0$. This completes our proof. □

Theorem 3.4 extends the Random Oracle Characterization to classes having the form $\mathsf{ALMOST}_n\text{-}\mathcal{R}$ by showing that for every $n > 0$ and every $B \in n$-RAND, $\mathsf{ALMOST}\text{-}\mathcal{R} = \mathcal{R}(B) \cap \Delta_n^0 = \mathcal{R}(n\text{-RAND}) \cap \Delta_n^0 = \mathsf{ALMOST}_n\text{-}\mathcal{R}$. As a corollary we see that it can be extended to ω-RAND.

Corollary 3.5 *For any appropriate reducibility $\mathcal{R}$,*

a) $\mathsf{ALMOST}_\omega\text{-}\mathcal{R} = \mathcal{R}(\omega\text{-RAND}) \cap AH$;

b) *for every* $B \in \omega$-RAND, $\mathsf{ALMOST}_\omega\text{-}\mathcal{R} = \mathcal{R}(B) \cap AH$;

c) $\mathsf{ALMOST}_\omega\text{-}\mathcal{R} = \mathsf{ALMOST}\text{-}\mathcal{R}$.

Proof Since ω-RAND is a countable intersection of classes having probability 1, Prob[ω-RAND] $= 1$ and $\mathsf{ALMOST}_\omega\text{-}\mathcal{R} \subseteq \mathsf{ALMOST}\text{-}\mathcal{R}$. By definition of $\mathsf{ALMOST}_n\text{-}\mathcal{R}$ and $\mathsf{ALMOST}_\omega\text{-}\mathcal{R}$, for every $n > 0$ $\mathsf{ALMOST}_n\text{-}\mathcal{R} \subseteq \mathsf{ALMOST}_\omega\text{-}\mathcal{R}$, because ω-RAND $\subseteq n$-RAND. From Theorem 3.4,

$$\mathsf{ALMOST}_n\text{-}\mathcal{R} = \mathsf{ALMOST}\text{-}\mathcal{R},$$

therefore $\mathsf{ALMOST}_\omega\text{-}\mathcal{R} = \mathsf{ALMOST}\text{-}\mathcal{R}$.

Let $B \in \omega$-RAND, then for every $n > 0$, $B \in n$-RAND, and by Theorem 3.4

$$\mathsf{ALMOST}\text{-}\mathcal{R} = \mathcal{R}(B) \cap \Delta_n^0 = \mathcal{R}(\omega\text{-RAND}) \cap \Delta_n^0.$$

Since this holds for every $n > 0$,

$$\mathsf{ALMOST}\text{-}\mathcal{R} = \mathcal{R}(B) \cap AH = \mathcal{R}(\omega\text{-RAND}) \cap AH.$$

□

Notice that since $\mathsf{ALMOST}\text{-}\mathcal{R}$ is a recursive class, Theorem 3.4 shows that there are no languages from $\Delta_n^0 - \text{REC}$ in $\mathcal{R}(n\text{-RAND})$, that is, oracles in n-RAND are useless for $\Delta_n^0 - \text{REC}$. In the same way, by Corollary 3.5 there are no languages from $AH - \text{REC}$ in $\mathcal{R}(\omega\text{-RAND})$.

Note that the Independent Pair Characterization trivially holds inside n-RAND and ω-RAND, because both classes are included in RAND.

4 Using p-measure

In this section we briefly discuss the characterization of $\mathsf{ALMOST}\text{-}\mathcal{R}$ in terms of "p-measure". This concept was introduced by Lutz in his development of resource-bounded measure, a generalization of classical Lebesgue measure that classifies recursive complexity classes by their size. See [Lu92] for a complete introduction to resource-bounded measure.

Let D be the set of dyadic rationals, that is, $\mathsf{D} = \{2^{-n}m \mid n, m > 0\}$.

A *martingale* is a function $d : \{0,1\}^* \to \mathsf{D}$ 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.

Let p be the class of functions that can be computed in polynomial time. Let p_2 be the class of functions that can be computed in time $2^{\log^k}$, for some k. Let $\Delta \in \{\mathrm{p}, \mathcal{P}_2\}$. A class $\mathbf{X}$ of languages has Δ-*measure* 0 if there exists a martingale $d \in \Delta$ 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 $\mu_\Delta(\mathbf{X}^c) = 0$.

Due to the Kolmogorov 0-1 Law, we need to consider only Δ-measure 0 and Δ-measure 1 when dealing with classes that are closed under finite variations (see [Lu92]).

We define the following classes:

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

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

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

It follows easily from the definitions that for every $n > 0$, $\mathrm{NULL}_\mathrm{p} \subseteq \mathrm{NULL} \subseteq \mathrm{NULL}_n$ and $\text{p-RAND} \supseteq \mathrm{RAND} \supseteq n\text{-RAND}$. From basic results in resource bounded measure [Lu92], NULL_p has p_2 measure 0, and p-RAND has p_2 measure 1.

Since Prob[p-RAND] = 1, clearly $\mathsf{ALMOST}_\mathrm{p}\text{-}\mathcal{R} \subseteq \mathsf{ALMOST}\text{-}\mathcal{R}$. But to see the converse, that is, $\mathsf{ALMOST}\text{-}\mathcal{R} \subseteq \mathsf{ALMOST}_\mathrm{p}\text{-}\mathcal{R}$, we need that for each $A \in \mathsf{ALMOST}\text{-}\mathcal{R}$, $\text{p-RAND} \subseteq \mathcal{R}^{-1}(A)$. This would imply that for each $A \in \mathsf{ALMOST}\text{-}\mathcal{R}$, $\mathcal{R}^{-1}(A)$ has p_2 measure 1, but this is not even known for the simplest reducibilities, such as $\leq_m^\mathrm{P}$. In fact the p_2-measurability of $\mathcal{R}^{-1}(A)$ for each language A is an open problem, only solved for trivial cases (such as $A \in \mathrm{P}$) and for very particular examples (see [JL95] and [BM95]).

Let us only remark a first step in this direction. For all natural reducibilities, it trivially holds that for every B, $\mathcal{R}(\emptyset) \subseteq \mathcal{R}(B)$. If, besides, $\mathcal{R}$ is a reducibility such that $\mathsf{ALMOST}\text{-}\mathcal{R} \subseteq \mathcal{R}(\emptyset)$, then $\mathsf{ALMOST}\text{-}\mathcal{R} = \mathsf{ALMOST}_\mathrm{p}\text{-}\mathcal{R}$. Some reducibilities that have this property are $\leq_m^\mathrm{P}, \leq_\mathrm{btt}^\mathrm{P}, \leq_\mathrm{T}^\mathrm{PH}$, and $\leq_\mathrm{T}^\mathrm{PQH}$, where $\leq_\mathrm{T}^\mathrm{PQH}$ is defined by $A \leq_\mathrm{T}^\mathrm{PQH} B$ if and only if $A \leq_\mathrm{T}^\mathrm{PH} B \oplus \mathrm{QBF}$.

5 Remarks

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 $\mathcal{R}_b(\mathrm{RAND}) \cap \Sigma_1^0 = \mathsf{ALMOST}\text{-}\mathcal{R}_b$.

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 $\mathsf{ALMOST}\text{-}\mathcal{R} \subset \mathcal{R}(\mathrm{RAND}) \cap \Sigma_1^0$).

It would be interesting to answer these last two questions in a more general form, that is, does $\mathcal{R}(n\text{-RAND}) \cap \Sigma_{n+1}^0$ equal $\mathsf{ALMOST}\text{-}\mathcal{R}$?

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 p-RAND) yield the same complexity classes as RAND when studying classes characterized as $\mathsf{ALMOST}\text{-}\mathcal{R}$. 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

[Am86] K. Ambos-Spies, Randomness, relativizations, and polynomial reducibilities, *Proc. First Conf. on Structure in Complexity Theory* (1986), 23–34.

[BG81] 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), 96–113.

[Bo94] R. Book, On languages reducible to algorithmically random languages, *SIAM Journal on Computing* 23 (1994), 1275–1282.

[BLW94] R. Book, J. Lutz, and K. Wagner, An observation on probability versus randomness with applications to complexity classes, *Math. Systems Theory* 27 (1994), 201–209.

[BM95] H. Buhrman, and E. Mayordomo, An excursion to the Kolmogorov random strings, *Proc. Tenth Conf. on Structure in Complexity Theory* (1995), 197–203.

[Ca89] J. Cai, With probability one, a random oracle separates PSPACE from the polynomial-time hierarchy, *J. Comput. System. Sci.* 38 (1989), 68–85.

[Hi78] Hinman, *Recursion-Theoretic Hierarchies,* Springer-Verlag, 1978.

[JL95] D.W. Juedes and J.H. Lutz, The complexity and distribution of hard problems, *SIAM Journal on Computing* 24 (1995), 279–295.

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

[Ka94] S. Kautz, An improved zero-one law for algorithmically random sequences, *submitted.*

[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.

[NW88] N. Nisan and A. Wigderson, Hardness versus randomness, *Proc. 29th Symp. on Foundations of Computer Science* (1988), 2–11.

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

[TB91] S. Tang and R.V. Book, Polynomial-time reducibilities and "Almost-all" oracle sets, *Theoretical Computer Science* 81 (1991), 36–47.