Electrical Engineering and Computer Science - Technical Reports

College of Engineering and Computer Science

1-1991

Average Dependence and Random Oracles (Preliminary Report)

Stuart A. Kurtz
University of Chicago

Stephen R. Mahaney
University of Arizona

James S. Royer
Syracuse University

SU-CIS-91-03

Average Dependence and Random Oracles

(Preliminary Report)

Stuart A. Kurtz, Stephen R. Mahaney, and James S. Royer

January 1991

School of Computer and Information Science
Suite 4-116
Center for Science and Technology
Syracuse, New York 13244-4100

(315) 443-2368

Average Dependence and Random Oracles

Preliminary Report

Stuart A. Kurtz[*] Stephen R. Mahaney[†] James S. Royer[‡]

January 29, 1991

[*] Department of Computer Science; University of Chicago; 1100 E. 58th St.; Chicago, Illinois 60637, USA. E-mail: stuart@gargoyle.uchicago.edu.

[†] Department of Computer Science; University of Arizona; Tucson, Arizona; 85721, USA. E-mail: srm@cs.arizona.edu.

[‡] School of Computer and Information Science; Syracuse University; Syracuse, New York 13244, USA. E-mail: royer@top.cis.syr.edu.

1 Introduction

This paper is a technical investigation of issues in computational complexity theory relative to a random oracle. We introduce "average dependence," an alternative method to Bennett and Gill's "measure preserving map" technique and illustrate our technique by the following results.

1. We give a new and simpler proof that, relative to a random oracle R, $\mathrm{NP}^R \neq \mathrm{coNP}^R$;

2. We show that relative to a random oracle R, NP^R is not contained in coNP^R even if coNP^R is allowed subexponentially much advice. That is, $\mathrm{NP}^R \not\subseteq (\mathrm{coNP}/\mathcal{A}_s)^R$, where $\mathcal{A}_s$ is the class of relativized advice functions f such that, for all n, $|f^R(n)| \leq s(n)$ and s is any function such that $\lim_{n\to\infty}(\log s(n))/n = 0$.

3. We show that, relative to a random oracle R, NP^R is not contained in $\mathrm{coNTIME}(n^k)^R$ even if $\mathrm{coNTIME}(n^k)^R$ is allowed an exponential amount of advice. That is, for each $k > 0$, there is a $\gamma_k > 0$ such that, relative to a random oracle R, $\mathrm{NP}^R \not\subseteq (\mathrm{coNTIME}(n^k)/\mathcal{A}_s)^R$, where $\mathcal{A}_s$ is as above, and $s = \lambda n.2^{\gamma_k n}$.

4. We prove that, relative to a random oracle R, there is a NP^R set X^R whose only coNP^R-subsets must be "thin" in the sense that, if A^R is a coNP^R-subset of X^R, then $\mathrm{census}(A^R, n) \in \mathcal{O}(\mathrm{census}(X^R, n)^\beta)$ for each $\beta \in (\frac{1}{2}, 1)$.

Results 2 and 3 are improvements on work of Lutz and Schmidt [LS90] who have analogous results for $\mathrm{P}/\mathcal{A}$ classes in place of $\mathrm{coNP}/\mathcal{A}$ classes. Result 4 complements an earlier result of ours that, relative to a random oracle R, there are NP^R sets whose only P^R subsets are sparse [KMR89]. Also result 1 is an improvement of sorts on Bennett and Gill's original proof that, relative to a random oracle R, $\mathrm{NP}^R \neq \mathrm{coNP}^R$ [BG81]. In that proof Bennett and Gill introduce their measure preserving map technique which has since become one of the stock methods in random oracle work. Their technique, however, is nonintuitive and difficult to use. Our average dependence technique addresses the same sorts of problems as Bennett and Gill's, but from a rather different point of view which we feel is both simpler and more intuitive.

Complexity Relative to a Random Oracle. A relativized statement S *holds relative to a random oracle* if and only if the set $\{\, R \mid S^R \text{ is true} \,\}$ has measure 1 in the standard Lebesgue measure on $\mathcal{P}(N)$.[1] Intuitively, if R is a

[1] See §2 for the formal definition of this measure.

"randomly" chosen oracle, S^R will be true with probability 1. Unlike complexity theory relative to unrestricted oracles, complexity theory relative to a random oracle is consistent and has an *a priori* character as the oracles involved are not constructed. Moreover, it follows from Kolmogorov's 0-1 law that if an arithmetic relativized statement S has the property that the truth value of S^A is unchanged by finite variations made to A, then the measure of $\{ R \mid S^R \}$ is either 0 or 1. Since most relativizable statements of complexity theory have this property, complexity theory relative to a random oracle is thus a "complete" theory.

The study of complexity theory relative to random oracles was begun by Bennett and Gill in [BG81]. In that paper Bennett and Gill established a number of hard, interesting results. For example, they showed that relative to a random oracle,

$$\text{LOGSPACE} \subset \left\{ \begin{array}{c} \text{P} = \text{ZPP} \\ = \\ \text{RP} = \text{BPP} \end{array} \right\} \subset \left\{ \begin{array}{c} \text{NP} \\ \neq \\ \text{coNP} \end{array} \right\}.$$

Note that, other than the collapse of the probabilistic classes into P, the relationships of the above classes match the conventional wisdom as to what the relationships of the unrelativized classes are. Since Bennett and Gill's original paper, random oracle work has become an active subarea of complexity theory with a number of people contributing some very fine results. In this paper we will not attempt to discuss these results except for those directly related to our work.

Why Study Random Oracles? Bennett and Gill provided a bold, controversial motivation for studying complexity theory relative to a random oracle—their ***Random Oracle Hypothesis.*** Informally stated, this hypothesis is: *If a "structural fact" about complexity classes containing* P *holds relative to a random oracle, then that fact also holds in the unrelativized world.* The prime intuition behind the hypothesis was (i) very high quality polynomial-time pseudo-random generators exist, and (ii) when a structural relationship between complexity classes holds relative to a random oracle, then it ought to hold when the random oracle is replaced by one of these pseudo-random generators.

Due to the counterexamples of [Kur83] and [CGH90] the Random Oracle Hypothesis is essentially dead. However, the intuition behind it remains appealing. Complexity theory relative to a random oracle provides a model of a computational world in which extremely strong polynomial-time "pseudo-random functions" exist and their presence implies lots of interesting structural facts. It seems plausible that some sort of polynomial-time pseudo-random functions do exist, but their power is likely nowhere near that of those existing relative to a random oracle. We believe, however, that in working to understand complexity theory relative to a random oracle, we will develop tools and ideas that will be useful in the unrelativized case. Towards this end, our very general aims in this work are (i) to develop as complete a picture as possible of what is true relative to a random oracle and (ii) to put these results on as clear and as simple mathematical basis as possible. The results of this paper are intended as a step towards these goals.

2 Background

General. We shall assume the reader is familiar with the basics of machine based computational complexity as discussed in [HU79].

N denotes the set of natural numbers $\{0,1,2,\ldots\}$. We identify each $x \in N$ with the x-th string over the symbols **0** and **1** in the lexicographic ordering on $\{\mathbf{0},\mathbf{1}\}^*$. We use natural numbers and strings over $\{\mathbf{0},\mathbf{1}\}$ interchangeably. Unless specified otherwise, functions are over N and total and sets are subsets of N. The length of $x \in N$ (i.e., the length of its string representation) is denoted $|x|$. Let $\langle\cdot,\cdot\rangle$ denote a polynomial-time computable pairing function, see [Rog67] for an example.

Suppose $A \subseteq N$. $\overline{A}$ denotes the complement of A, i.e., $N - A$. $\|A\|$ denotes the cardinality of A. $\mathcal{P}(A)$ denotes the power set of A, i.e., $\{B : B \subseteq A\}$. $A \Delta B$ denotes the symmetric difference of A and B, i.e., $(A-B)\cup(B-A)$. For each $n \in N$, $A|_n$ denotes $\{x \in A : |x| = n\}$ and $\text{census}(A,n) = \|A|_n\|$.

Suppose f is a mapping from some set into N. Then, corange(f) denotes $\overline{\text{range}(f)}$.

A *fragment* is a function $\sigma\colon N \to \{0,1\}$ with finite domain. For a fragment σ and an $A \subseteq N$, we say *σ is extended by A* (written: $\sigma \sqsubseteq A$) if and only if the characteristic function of A extends σ, i.e., for all x, $\sigma(x) = 0 \Longrightarrow x \notin A$ and $\sigma(x) = 1 \Longrightarrow x \in A$. For each fragment σ, we define $\langle\!\langle\sigma\rangle\!\rangle$ to be $\{A : \sigma \sqsubseteq A\}$. The $\langle\!\langle\sigma\rangle\!\rangle$ sets form a basis for the standard topology on $\mathcal{P}(N)$ used in computability theory, see [Rog67].

Measure Theory. Below we briefly discuss some results from measure theory used in subsequent sections. For a general introduction to measure theory see any of [Dud89], [Oxt80], [Roy68], and [Rud66].

A *measure space* is a triple $(X,\mathcal{M},m)$ where X is a set, $\mathcal{M}$ is a collection of *measurable* subsets of X and m is the measure for the space which assigns to each $A \in \mathcal{M}$ a nonnegative real, the measure of A. As an example of a measure space, we sketch how to define the standard Lebesgue measure μ on $\mathcal{P}(N)$. In the following let $\mathcal{A}$ range over subsets of $\mathcal{P}(N)$ and let $\overline{\mathcal{A}}$ denote the complement of $\mathcal{A}$ in $\mathcal{P}(N)$, i.e., $(\mathcal{P}(N) - \mathcal{A})$. One can think of μ as a probability measure on $\mathcal{P}(N)$ such that, for each ***fixed*** $x \in N$ we have that "Prob[$A : x \in A$]" $= \mu(\{\, A : x \in A \,\}) = \mu(\{\, A : x \notin A \,\}) =$ "Prob[$A : x \notin A$]" $= \frac{1}{2}$. Moreover, for distinct x's, we require that the sets $\{\, A : x \in A \,\}$ be independent (in the probabilistic sense). These requirements dictate that, for each fragment σ, we have $\mu(\langle\!\langle\sigma\rangle\!\rangle) = 2^{-m}$, where $m = \|\text{domain}(\sigma)\|$. Now, to extend μ to $\mathcal{A} \subseteq \mathcal{P}(N)$ beyond the $\langle\!\langle\sigma\rangle\!\rangle$'s the idea is roughly to define $\mu(\mathcal{A})$ as the limit of measures of approximations to $\mathcal{A}$. Toward this end, define the ***outer measure of $\mathcal{A}$*** (written $\mu^*(\mathcal{A})$) to be the greatest lower bound of $\{\, \sum_{i=0}^{\infty} \mu(\langle\!\langle\sigma_i\rangle\!\rangle) : \mathcal{A} \subseteq \cup_{i=0}^{\infty} \langle\!\langle\sigma_i\rangle\!\rangle \,\}$. We would like to define $\mu(\mathcal{A}) = \mu^*(\mathcal{A})$ for arbitrary $\mathcal{A}$, but there is a problem. Another property we want μ to have is: $\mu(\mathcal{A}) = a \iff \mu(\overline{\mathcal{A}}) = 1 - a$. However, using the axiom of choice one can construct an $\mathcal{A}$ such that $\mu^*(\mathcal{A}) + \mu^*(\overline{\mathcal{A}}) > 1$. On the other hand, all of the sets $\mathcal{A}$ one typically cares about have the property that $\mu^*(\mathcal{A}) + \mu^*(\overline{\mathcal{A}}) = 1$. So we define $\mathcal{A}$ to be ***measurable*** if and only if $\mu^*(\mathcal{A}) + \mu^*(\overline{\mathcal{A}}) = 1$ and then define $\mu(\mathcal{A}) = \mu^*(\mathcal{A})$ for measurable $\mathcal{A}$ and leave $\mu(\mathcal{A})$ undefined for nonmeasurable $\mathcal{A}$. All of the $\mathcal{A}$ we consider below will be first order definable and the first order definable $\mathcal{A}$ can be shown to be μ-measurable.

Countable subadditivity refers to the property of μ that, if $\langle \mathcal{A}_i \rangle_{i \in N}$ is a sequence of measurable sets, then

$$\mu\Big(\bigcup_{i \in N} \mathcal{A}_i\Big) \quad \leq \quad \sum_{i \in N} \mu(\mathcal{A}_i).$$

It follows from this that the union of countably many sets of measure 0 is itself a set of measure 0.

Sets A and B are ***finite variants*** if and only if $A \triangle B$ is finite. A collection of sets $\mathcal{A}$ is ***closed under finite variants*** if and only if for each $A \in \mathcal{A}$, every finite variant of A is also in $\mathcal{A}$. ***Kolmogoroff's 0-1 law*** [Oxt80] states that if $\mathcal{A}$ is measurable and closed under finite variants, then $\mu(\mathcal{A})$ is either 0 or 1.

Very roughly, the ***product*** of two measure spaces, $(X_1, \mathcal{M}_1, \mu_1)$ and $(X_2, \mathcal{M}_2, \mu_2)$ is a measure space $(X_1 \times X_2, \mathcal{M}', \mu_1 \times \mu_2)$ in which for each $A_1 \in \mathcal{M}_1$ and $A_2 \in \mathcal{M}_2$ we have $(\mu_1 \times \mu_2)(A_1 \times A_2) = \mu_1(A_1) \cdot \mu_2(A_2)$. (Note: $\mathcal{M}'$ contains more sets than just those of the form $A_1 \times A_2$.) The product of three or more measure spaces is defined analogously. ***Fubini's Theorem*** is a general measure theoretic result about integrating functions over product spaces which, roughly speaking, gives sufficient conditions for when one can "change the order of integration." Below we shall be concerned with integrating 0–1 valued functions over product spaces and for such functions, f, the sufficient conditions for Fubini's Theorem reduce to: both $f^{-1}(0)$ and $f^{-1}(1)$ are measurable subsets of the product space.

3 The Basic Argument

In this section we introduce our average dependence technique by giving a new proof of

Theorem 1 (Bennett and Gill [BG81]). *Relative to a random oracle R, $\mathrm{NP}^R \neq \mathrm{coNP}^R$.*

To state the technical result that implies Theorem 1, we first define the following relativized function. For each $R \subseteq N$ and each $x \in N$, let

$$(1) \qquad \xi^R(x) \stackrel{\text{def}}{=} R(x\mathbf{1})R(x\mathbf{10})\ldots R(x\mathbf{10}^{3|x|}).$$

We prove the following about ξ^R.

Theorem 2. *Relative to a random oracle R,* $\text{range}(\xi^R) \notin \mathrm{coNP}^R$.

Since $\text{range}(\xi^R) \in \mathrm{NP}^R$, Theorem 1 follows immediately. Using a slightly different ξ^R, Bennett and Gill prove the analog of Theorem 2.

To prove Theorem 2, our first task is to reduce the theorem to something a bit more manageable. Let M range over polynomially clocked, nondeterministic TMs. For each M, let

$$\mathcal{B}_M \stackrel{\text{def}}{=} \{ R : L(M^R) = \text{corange}(\xi^R) \},$$

and let $\mathcal{B} \stackrel{\text{def}}{=} \cup_M \mathcal{B}_M$. It is clear that $\mathcal{B} = \{ R : \text{range}(\xi^R) \in \mathrm{coNP}^R \}$. So, Theorem 2 is equivalent to the assertion that $\mu(\mathcal{B}) = 0$ which in turn, by countable subadditivity, is equivalent to the assertion that, for each M, $\mu(\mathcal{B}_M) = 0$. Therefore, to show Theorem 2, we fix an arbitrary M and establish $\mu(\mathcal{B}_M) = 0$. Let p be a polynomial that bounds M's run time (on all oracles).

Now let's reduce the problem still further. For each n, let

$$\mathcal{M}_n \stackrel{\text{def}}{=} \{ R : L(M^R)|_{3n+1} = \text{corange}(\xi^R)|_{3n+1} \},$$

that is, $\mathcal{M}_n$ is the set of all oracles R such that, *on strings of length* $3n+1$, the set accepted by M^R agrees with corange(ξ^R). Note that $\mathcal{B}_M \subseteq \bigcap_{n \in N} \mathcal{M}_n$ and so, for each n, $\mu(\mathcal{M}_n) \geq \mu(\mathcal{B}_M)$. Thus, to establish $\mu(\mathcal{B}_M) = 0$ (and thereby Theorem 2), it suffices to prove

Proposition 3. *For any $\epsilon > 0$, for all but finitely many n, $\mu(\mathcal{M}_n) < \epsilon$.*

Our goal in what follows it to establish this proposition.

3.1 Preliminaries

Before we get on with the proof proper, we introduce three important notions for what follows.

X-Variants

Definition 4. Suppose R and $S \subseteq N$ and $x \in N$. We say that R and S are *x-variants* (written $R \sim_x S$) if and only if $R \bigtriangleup S \subseteq \{\, x\mathbf{1}\mathbf{0}^k : k \leq 3|x| \,\}$, i.e., R and S are identical except perhaps on the strings that determine the value of ξ on argument x.

For each x, the relation $\sim_x$ partitions $\mathcal{P}(N)$ into uncountably many equivalence classes each of cardinality $2^{3|x|+1}$. The next lemma follows easily from Definition 4; its main purpose is to show what is happening in each of these equivalence classes.

Lemma 5. *Suppose $x \in N$ and $R \subseteq N$. For each $y \in N|_{3|x|+1}$, let R_y be the (unique) x-variant of R such that $\xi^{R_y}(x) = y$. Then, $y \mapsto R_y$ is a 1-1 correspondence between the elements of $N_{3|x|+1}$ and the x-variants of R.*

The following lemma is a crucial point in a number of our measure estimation arguments. We omit its proof which essentially consists of factoring $\mathcal{P}(N)$ into the product of two appropriate measure spaces and then applying Fubini's Theorem. This lemma, by the way, was the key observation that lead to the formalization of our proof that the isomorphism conjecture fails relative to a random oracle.

Lemma 6. *Suppose $\mathcal{A}$ is a measurable subset of $\mathcal{P}(N)$, $\epsilon \geq 0$, and $x_0 \in N$. Moreover, suppose that for every $R \in \mathcal{P}(N)$,*

$$\frac{\|\{S : S \sim_{x_0} R\} \cap \mathcal{A}\|}{\|\{S : S \sim_{x_0} R\}\|} \leq \epsilon.$$

Then, $\mu(\mathcal{A}) \leq \epsilon$.

Examination and Dependence

Definition 7. (a) For each $R \subseteq N$ and each x and $y \in N$, we say that a particular computation of M^R on argument y *examines* x if and only if in the course of the computation the oracle R is queried about some string of the form $x\mathbf{1}\mathbf{0}^k$ for $k \leq 3|x|$—intuitively, the computation learns some information about the value of $\xi^R(x)$.

(b) For each $R \subseteq N$ and each x and $y \in N$, we say that *the value of $M^R(y)$ depends on x* if and only if there is an $S \sim_x R$ such that $M^R(y) \neq M^S(y)$.

The notion of "examines" is a direct lift from Bennett and Gill. We note the following without proof.

Lemma 8. *Suppose M^R on input y accepts.*

(a) If the value of $M^R(y)$ depends on x, then every accepting computation of M^R on input y must examine x.

(b) There are no more than $p(|y|)$ many x's on which the value of $M^R(y)$ can depend.

3.2 The Main Argument

To motivate what comes next, let's anthropomorphize M and consider the troubles M would have in trying, with oracle R, to accept precisely corange(ξ^R) on inputs of length $3n+1$. Among poor M's worries are the following two which will turn out to be in conflict.

- Since $(N|_{3n+1} - \text{range}(\xi^R))$ has at least $2^{3n+1} - 2^n$ elements, M^R must accept that many $y \in N|_{3n+1}$.
- At the same time, on inputs $y \in N|_{3n+1}$, M^R (intuitively) must examine essentially every $x \in N|_n$ so that it doesn't erroneously accept y when there is an $x \in N|_n$ such that $\xi^R(x) = y$.

Now there is a difficulty with second item above—mere "examination" isn't good enough. As Lemma 8(a) points out, if M^R accepts a $y \in N|_{3n+1}$, then in order to be sure of a particular x that $\xi^R(x) \neq y$, the value of $M^R(y)$ must *depend* on x, i.e., every accepting computation of M^R on argument y must examine x. Moreover, Lemma 8(b) shows that for each $y \in L(M^R)|_{3n+1}$, M^R on input y can be sure of at most $p(3n+1)$ many x that $\xi^R(x) \neq y$. Since M^R has to accept at least $2^{3n+1} - 2^n$ many $y \in N|_{3n+1}$, one can see that M^R is stretched very thin in its attempts to accept precisely corange$(\xi^R)|_{3n+1}$.

We take advantage of M's difficulties to show $\mathcal{M}_n$ has small measure. We proceed roughly as follows.

1. We choose an $x_n \in N|_n$ such that for "most" of the $R \in \mathcal{M}_n$, the number of $y \in N|_{3n+1}$ such that the value of $M^R(y)$ depends on x_n is small.
2. Then, for each such $R \in \mathcal{M}_n$ with "low dependence" on x_n, we show that among R's x_n-variants, the number of x_n-variants in $\mathcal{M}_n$ is far outnumbered by the x_n-variants of R, S, such that M^S erroneously accepts $\xi^S(x_n)$. Thus, using Lemma 6, we obtain an upper bound on the measure of the set of $R \in \mathcal{M}_n$ with "low dependence" on x_n.

There are a number of difficulties with this sketch. Among them is that it isn't clear that there is any x_n with the properties required by 1. An arbitrary member of $N|_n$ will not do for x_n because there may be certain $x \in N|_n$ on which M has "high dependence." To help make this precise, for each R and each $x \in N$, define

$$(2) \qquad D(R,x) \quad = \quad \left\{ y \in L(M^R)|_{3|x|+1} : \begin{array}{l} \text{the value of } M^R(y) \\ \text{depends on } x \end{array} \right\}.$$

For each R and x, we clearly have $\|D(R,x)\| \leq 2^{3|x|+1}$. It is easy to construct an M for which there are infinitely many x such that for *every* R, $\|D(R,x)\| = \|L(M^R)|_{3|x|+1}\|$. One can think of such x's as "hot spots" of M and if one wants to find an x_n as required above, one cannot look among the hot spots. Therefore, we look for "cold spots." For each $\epsilon \in (0,1]$ and each x, define

$$(3) \qquad \mathcal{C}(\epsilon,x) \quad = \quad \left\{ R \in \mathcal{M}_{|x|} : \|D(R,x)\| < \epsilon \cdot 2^{3|x|+1} \right\}.$$

That is, $\mathcal{C}(\epsilon,x)$ is the set of oracles R such that

- on strings of length $3n+1$, the set accepted by M^R agrees with corange(ξ^R) and
- there are fewer than $\epsilon \cdot 2^{3|x|+1}$ many y in $L(M^R)|_{3|x|+1}$ such that $M^R(y)$ depends on x, i.e., relative to R, x is no more than ϵ "hot."

We establish the following two lemmas about the $\mathcal{C}(\epsilon,x)$'s.

Lemma 9. *Suppose ϵ and n are such that $2^{-2n-1} \leq \epsilon$. Then, for each $x \in N|_n$, we have $\mu(\mathcal{C}(\epsilon,x)) \leq 2\epsilon$.*

Lemma 10 (The cold spot lemma). *Suppose ϵ and n are such that $p(3n+1) \cdot 2^{-n+1} < \epsilon$. Then, there is an $x_n \in N|_n$ such that $\mu(\mathcal{C}(\epsilon,x_n)) \geq \mu(\mathcal{M}_n)/2$.*

Lemmas 9 and 10 respectively correspond to items 2 and 1 in our sketch above. These two lemmas together imply Proposition 3 (and thereby Theorem 2) as follows.

Proof of Proposition 3. Fix an $\epsilon \in (0,1]$ and let $\epsilon_0 = \epsilon/4$. For all but finitely many n we have that $2^{-2n-1} \leq \epsilon_0$ and $p(3n+1) \cdot 2^{-n+1} < \epsilon_0$. Pick an n satisfying these two inequalities. Then, by Lemma 10 there is an $x_n \in N|_n$ such that $\mu(\mathcal{C}(\epsilon_0,x_n)) \geq \mu(\mathcal{M}_n)/2$. By Lemma 9 we have that $\mu(\mathcal{C}(\epsilon_0,x_n)) \leq 2\epsilon_0$. Hence,

$$\mu(\mathcal{M}_n)/2 \quad \leq \quad \mu(\mathcal{C}(\epsilon_0,x_n)) \leq 2\epsilon_0.$$

Therefore, $\mu(\mathcal{M}_n) \leq 4\epsilon_0 = \epsilon$ as required. □

Now we establish the two lemmas.

Proof of Lemma 9. Fix an $x \in N|_n$. Fix an arbitrary oracle $R \in \mathcal{C}(\epsilon, x)$. This R has exactly 2^{3n+1} x-variants. By Lemma 6, to show the present lemma it suffices to show that at least $(1-2\epsilon)\cdot 2^{3n+1}$ many of these x-variants are outside $\mathcal{C}(\epsilon, x)$. Let

$$(4) \qquad I \stackrel{\text{def}}{=} N|_{3n+1} - \left(D(R,x) \cup \operatorname{range}(\xi^R)\right).$$

("I" for independent.) Since $R \in \mathcal{C}(\epsilon,x) \subseteq \mathcal{M}_n$, we have that $L(M^R)|_{3n+1} = \operatorname{corange}(\xi^R)|_{3n+1}$, and, hence, $I \subseteq L(M^R)|_{3n+1}$. Also, by the definitions of I and $D(R,x)$,

$$I = \left\{ y \in L(M^R)|_{3n+1} : \begin{array}{c}\text{the value of } M^R(y) \\ \text{does not depend on } x\end{array} \right\}.$$

Hence,

$$(5) \qquad \text{for } \textit{every } S \sim_x R,\ I \subseteq L^S_M|_{3n+1},$$

because if there is an accepting computation of $M^R(y)$ that does not examine x, then, for every $S \sim_x R$, the same accepting computation works for $M^S(y)$.

Suppose S is an x-variant of R such that $\xi^S(x) \in I$. Then by (5), $\xi^S(x) \in L^S_M|_{3n+1}$. Hence, $L^S_M|_{3n+1} \neq \operatorname{corange}(\xi^S)|_{3n+1}$. So, $S \notin \mathcal{M}_n$, and, hence, $S \notin \mathcal{C}(\epsilon,x)$ (since $\mathcal{C}(\epsilon,x) \subseteq \mathcal{M}_n$). By Lemma 5, for each $y \in I$, there is a distinct x-variant of R, S_y, such that $\xi^{S_y}(x) = y \in I$. Therefore, there are at least $||I||$ many x-variants of R which are not in $\mathcal{C}(\epsilon,x)$. Thus, to establish the lemma it suffices to show that $||I|| \geq (1-2\epsilon)2^{3n+1}$.

By (4) we have

$$(6) \qquad ||I|| \geq ||N|_{3n+1}|| - ||D(R,x)|| - ||\operatorname{range}(\xi^R)|_{3n+1}||.$$

Since $R \in \mathcal{C}(\epsilon,x)$, by (3) we have $||D(R,x)|| \leq \epsilon \cdot 2^{3n+1}$. Since $(\xi^R)^{-1}(N|_{3n+1}) = N|_n$, we have $||\operatorname{range}(\xi^R|_{3n+1})|| \leq 2^n$. By assumption $2^{-2n-1} \leq \epsilon$, and so, $2^n = 2^{-2n-1} \cdot 2^{3n+1} \leq \epsilon \cdot 2^{3n+1}$. Hence, by (6) it follows that $||I|| \geq (1-2\epsilon)2^{3n+1}$ as required. □ **Lemma 9**

Proof of Lemma 10. We want to show that there is an $x_n \in N|_n$ such that $\mu(\mathcal{C}(\epsilon,x_n)) > \mu(\mathcal{M}_n)/2$. For each $x \in N|_n$, let

$$(7) \qquad \begin{aligned} \mathcal{H}(\epsilon,x) &\stackrel{\text{def}}{=} \left\{ R \in \mathcal{M}_{|x|} : ||D(R,x)|| \geq \epsilon \cdot 2^{3|x|+1} \right\} \\ &= \left(\mathcal{M}_n - \mathcal{C}(\epsilon,x)\right). \end{aligned}$$

To establish the lemma, then, it suffices to show the existence of an $x_n \in N|_n$ such that $\mu(\mathcal{H}(\epsilon,x_n)) < \mu(\mathcal{M}_n)/2$. We do this by proving

$$(8) \qquad \operatorname*{avg}_{x \in N|_n} \mu(\mathcal{H}(\epsilon,x)) < \mu(\mathcal{M}_n)/2.$$

The existence of such an x_n then falls out immediately.

So, we now estimate some averages.

For each m, we view $N|_m$ as a measure space under the uniform, normalized counting measure—in plain language, each $x \in N|_m$ has weight 2^{-m}. Thus, $\mathcal{P}(N) \times N|_n \times N|_{3n+1}$ is a measure space under the product of Lebesgue measure on $\mathcal{P}(N)$ and the normalized counting measures on $N|_n$ and $N|_{3n+1}$. For each $R \subseteq N$ and each x and $y \in N$, define

$$dep_M(R, x, y) \;=\; \begin{cases} 1, & \text{if } y \in L(M^R) \text{ and the value} \\ & \quad \text{of } M^R(y) \text{ depends on } x; \\ 0, & \text{otherwise.} \end{cases}$$

Consider the integral $\int_{\mathcal{M}_n \times N|_n \times N|_{3n+1}} dep_M$. It is the average, over $R \in \mathcal{M}_n$ and $x \in N|_n$ and $y \in N|_{3n+1}$, of dep_M and, roughly, describes the amount of information flow in $\lambda R \in \mathcal{M}_n, y \in L(M^R)|_{3n+1} . M^R(y)$ about the behavior of ξ^R on $N|_n$. It is easily seen—honest, it is—that dep_M satisfies the sufficient conditions of Fubini's Theorem. So, we can integrate dep_M over $\mathcal{M}_n \times N|_n \times N|_{3n+1}$ as follows.

$$\begin{aligned}
\int_{\mathcal{M}_n \times N|_n \times N|_{3n+1}} dep_M \;&=\; \int_{\mathcal{M}_n} \int_{N|_{3n+1}} \int_{N|_n} dep_M(R, x, y)\, dx\, dy\, dR \\
&\le\; \int_{\mathcal{M}_n} \int_{N|_{3n+1}} p(3n+1) \cdot 2^{-n}\, dy\, dR \\
&\qquad \text{(since, by Lemma 8(b), for each } R \text{ and } y \in \\
&\qquad L(M^R) \text{, the value of } M^R(y) \text{ depends on no} \\
&\qquad \text{more that } p(|y|) = p(3n+1) \text{ many } x\text{'s)} \\
&=\; p(3n+1) \cdot 2^{-n} \int_{\mathcal{M}_n} \int_{N|_{3n+1}} 1\, dy\, dR \\
&=\; p(3n+1) \cdot 2^{-n} \int_{\mathcal{M}_n} 1\, dR \\
&=\; p(3n+1) \cdot 2^{-n} \cdot \mu(\mathcal{M}_n).
\end{aligned}$$

By changing the order of integration we obtain

$$\begin{aligned}
\int_{\mathcal{M}_n \times N|_n \times N|_{3n+1}} dep_M \;&=\; \int_{N|_n} \int_{\mathcal{M}_n} \int_{N|_{3n+1}} dep_M(R, x, y)\, dy\, dR\, dx \\
&\ge\; \int_{N|_n} \int_{\mathcal{H}(\epsilon, x)} \int_{N|_{3n+1}} dep_M(R, x, y)\, dy\, dR\, dx
\end{aligned}$$

$$
\begin{aligned}
& \qquad \text{(since, for each } x,\ \mathcal{H}(\epsilon, x) \subseteq \mathcal{M}_n) \\
> \quad & \int_{N|_n} \int_{\mathcal{H}(\epsilon,x)} (\epsilon \cdot 2^{3n+1}) 2^{-3n-1}\, dR\, dx \\
& \qquad \text{(by the definition of the } \mathcal{H}(\epsilon, x)\text{'s)} \\
= \quad & \epsilon \int_{N|_n} \int_{\mathcal{H}(\epsilon,x)} 1\, dR\, dx \\
= \quad & \epsilon \int_{N|_n} \mu(\mathcal{H}(\epsilon, x))\, dx \\
= \quad & \epsilon \cdot \operatorname*{avg}_{x \in N|_n} \mu(\mathcal{H}(\epsilon, x)).
\end{aligned}
$$

Therefore, we have

$$
\epsilon \cdot \operatorname*{avg}_{x \in N|_n} \mu(\mathcal{H}(\epsilon, x)) \quad < \quad p(3n+1) \cdot 2^{-n} \cdot \mu(\mathcal{M}_n).
$$

Thus,

$$
\begin{aligned}
\operatorname*{avg}_{x \in N|_n} \mu(\mathcal{H}(\epsilon, x)) \quad < \quad & \frac{1}{\epsilon} \cdot \frac{p(3n+1)}{2^n} \cdot \mu(\mathcal{M}_n) \\
< \quad & \frac{2^{n-1}}{p(3n+1)} \cdot \frac{p(3n+1)}{2^n} \cdot \mu(\mathcal{M}_n) \\
& \quad \text{(since by assumption } \frac{p(3n+1)}{2^{n-1}} < \epsilon) \\
= \quad & \tfrac{1}{2} \cdot \mu(\mathcal{M}_n).
\end{aligned}
$$

Therefore, we've shown (8) as required. □ **Lemma 10**

Scholium 11. For each $R \subseteq N$ and each x and $y \in N$, define

$$
dep'_M(R, x, y) \quad = \quad \begin{cases} 1, & \text{if the value of } M^R(y) \\ & \quad \text{depends on } x; \\ 0, & \text{otherwise.} \end{cases}
$$

The function dep'_M is the characteristic function of the dependence relation. It is clear that

$$
\begin{aligned}
\int_{\mathcal{M}_n \times N|_n \times N|_{3n+1}} dep_M \quad = \quad & \int_{\mathcal{M}_n \times N|_n \times L(M^R)|_{3n+1}} dep'_M \\
\leq \quad & \int_{\mathcal{M}_n \times N|_n \times N|_{3n+1}} dep'_M.
\end{aligned}
$$

The function dep'_M is a more natural to consider than dep_M and the integral

$$\int_{\mathcal{M}_n \times N|_n \times N|_{3n+1}} dep'_M$$

is the average of the dependence relation (over $\mathcal{M}_n$, $N|_n$, and $N|_{3n+1}$). The apparent problem with this integral is that when M^R rejects y, the value of $M^R(y)$ can depend on *every* $x \in N|_n$; hence, the upper bound on this integral has to be larger than the one we derived for the dep_M integral. However, if $R \in \mathcal{M}_n$, then M^R rejects at most 2^n of the 2^{3n+1} many $y \in N|_{3n+1}$. A few calculations show

$$\int_{\mathcal{M}_n \times N|_n \times N|_{3n+1}} dep'_M \quad \leq \quad \left(\frac{p(3n+1)}{2^n} + \frac{1}{2^{2n+1}}\right) \mu(\mathcal{M}_n).$$

We could have used dep'_M and the above upper bound in Lemma 10 at the price of a few complications in the lemma's statement and proof. We chose to use dep_M to keep Lemma 10 as simple as possible.

The key property of M used in proofs of this section is that for each y that M^R accepts, the value of $M^R(y)$ depends on at most $p(|y|)$ many x's. So long as M satisfies this property, it does not have to be polynomial-time bounded, it doesn't even have to be computable!

Another key element of the above arguments is that

$$(9) \qquad \liminf_{n\to\infty} \int_{\mathcal{M}_n \times N|_n \times N|_{3n+1}} dep_M \quad = \quad 0.$$

Our technique of finding cold spots is *a* method of taking advantage of (9), but if (9) did not hold, we could not do much of anything. Roughly speaking, we can modify the hypotheses on M and the definition of dep_M and so long as (9) holds, we can expect some version of Proposition 3 to go through.

4 Advice and Circuit Classes

We've shown that relative to a random oracle R, range(ξ^R) isn't contained in coNP^R. In this section we'll do a bit better and show that range(ξ^R) isn't contained in nonuniform, superpolynomial-time versions coNP^R. To make this precise we introduce some terminology.

Let $\mathcal{A}$ be a collection of functions from N to N which we shall call *advice functions* and let $\mathcal{C}$ be a collection of sets. Informally, $\mathcal{C}/\mathcal{A}$ is the collection of sets B which are decided using (i) some machine M for deciding a $\mathcal{C}$ set together with (ii) "advice" from some $f \in \mathcal{A}$, so that to decide whether an x of length n is in B one presents M with input $\langle x, f(n)\rangle$ and accepts x if and only if M accepts $\langle x, f(n)\rangle$; $f(n)$ is the advice offered by f for inputs of length n. Formally, $\mathcal{C}/\mathcal{A}$ is the collection of sets B such that for some $C \in \mathcal{C}$ and $f \in \mathcal{A}$, $B = \{\, x : \langle x, f(|x|)\rangle \in C \,\}$. $\mathcal{A}$ is typically taken to be a class of all functions that grow no faster than a certain rate. For example, let

$$\text{Poly} \overset{\text{def}}{=} \{\, f : (\exists \text{ polynomial } p)(\forall n)[\, |f(n)| \leq p(n) \,] \,\}.$$

P/Poly is then the class of sets decidable using polynomial-time and polynomial advice and NP/Poly is the class of sets accepted by nondeterministic, polynomial-time machines using polynomial advice. To relativized an advice class $\mathcal{C}/\mathcal{A}$ one merely uses relativized versions of $\mathcal{C}$ *and* $\mathcal{A}$. Advice classes were introduced by Karp and Lipton [KL82] although similar formalisms were introduced earlier by Plaisted [Pla77] and Pippenger [Pip79].

Now, suppose $s: N \rightarrow N$ and define

$$\mathcal{A}_s = \left\{ f : \begin{array}{l} f: \mathcal{P}(N) \times N \rightarrow N \text{ and, for all } R \\ \text{and } x, \ |f(R,x)| \leq s(|x|) \end{array} \right\}.$$

That is, $\mathcal{A}_s$ is the class of relativized advice functions "of size s." Below we show

Theorem 12. *Suppose* $s: N \rightarrow N$ *is such that*

$$\lim_{n\rightarrow\infty} \frac{\log s(n)}{n} = 0, \tag{10}$$

i.e., s *is "subexponential." Then, relative to a random oracle* R, range$(\xi^R) \notin (\text{coNP}/\mathcal{A}_s)^R$.

So, for example, it follows from this that relative to a random oracle R, range$(\xi^R) \notin (\text{coNP/Poly})^R$.

Theorem 12 concerns subexponential advice. We can also deal with exponential advice. For each $\gamma \in (0,1)$, define $s_\gamma = \lambda n.2^{\gamma \cdot n}$. It is easily shown that for each $R \subseteq N$ and each $\gamma > 0$, $\text{DTIME}(2^{\mathcal{O}(n)})^R \subseteq (\text{coNP}/\mathcal{A}_{s_\gamma})^R$, and hence, range$(\xi^R) \in (\text{coNP}/\mathcal{A}_{s_\gamma})^R$. However, it is "almost" the case that, relative to a random oracle R, range$(\xi^R) \notin (\text{coNP}/\mathcal{A}_{s_\gamma})^R$ as shown by the next theorem. For each k, define NP_k to be the class of languages accepted by $\mathcal{O}(n^k)$-nondeterministic time TMs.

Theorem 13. *Suppose* $k > 0$ *and* $\gamma \in (0, \frac{1}{3k+6})$. *Then, relative to a random oracle* R, range$(\xi^R) \notin (\text{coNP}_k/\mathcal{A}_{s_\gamma})^R$.

Advice classes are closely related to families of Boolean circuits.[2] For example, Pippenger [Pip79] essentially showed that P/Poly is the class of sets accepted by families of polynomial-sized Boolean circuits. His argument can easily be extended to show that NP/Poly is the class of sets accepted by families of polynomial-sized, nondeterministic Boolean circuits and also that there

[2] In the interests of space we are omitting a background discussion of Boolean circuits. For a good basic discussion see [BDG88]. Wilson [Wil85] introduced the standard model of relativized Boolean circuits.

is a constant c_0 such that for all $\gamma > 0$, if A is accepted by a family of $2^{\gamma n}$-sized Boolean circuits, then $A \in \mathrm{NP}_2/\mathcal{A}$, where $\mathcal{A} = \{\, f : \text{for all } n,\ |f(n)| \leq 2^{c_0 \gamma n} \,\}$. All of this relativizes using Wilson's [Wil85] model of relativized circuits. Hence, we can obtain as a corollary of Theorem 13 that there is a $\gamma > 0$ such that, relative to a random oracle R, corange(ξ^R) is not accepted by any family of $2^{\gamma n}$-sized, nondeterministic Boolean circuits. However, if we look more closely at the proof of Theorem 13 below we can obtain the following stronger result. (Recall that for all R, range$(\xi^R) \subseteq \cup_{n \in N} N|_{3n+1}$.)

Theorem 14. *There exist $\gamma > 0$ such relative to a random oracle R, for each family $(C_i)_{i \in N}$ of $2^{\gamma n}$-sized, relativized, nondeterministic, Boolean circuits, for all but finitely many n, C_{3n+1} fails to accept* corange$(\xi^R)|_{3n+1}$.

As we mentioned in §1, Lutz and Schmidt [LS90] have have results analogous to Theorem 14 for $\mathrm{P}/\mathcal{A}$ classes in place of $\mathrm{coNP}/\mathcal{A}$ classes.

4.1 Analysis of the Problem

In this subsection we reduce the problem of showing that

$$\mu(\{\, R : \mathrm{range}(\xi^R) \in (\mathrm{coNP}/\mathcal{A}_s)^R \,\}) = 0, \tag{11}$$

for some fixed $s \colon N \longrightarrow N$, to something more directly amenable to our techniques. Let M range over polynomially-clocked, nondeterministic TMs. For each M define $\mathcal{B}_M =$

$$\left\{ R : \begin{array}{l} (\forall n)\, (\exists a \in N|_{s(3n+1)}) \\ \quad [\, L(M^R(\cdot, a))|_{3n+1} = \mathrm{corange}(\xi^R)|_{3n+1} \,] \end{array} \right\}.$$

In words, $\mathcal{B}_M$ is the set of oracles R such that, for each length $3n+1$, there is some advice string, a, of length $s(3n+1)$ for which, on strings of length $3n+1$, $M^R(\cdot, a)$ accepts precisely corange(ξ^R). Note that a depends on n *and* R. Let $\mathcal{B} = \cup_M \mathcal{B}_M$. Clearly, $\mathcal{B} \supseteq \{\, R : \mathrm{range}(\xi^R) \in (\mathrm{coNP}/\mathcal{A}_s)^R \,\}$. So, to show (11), it suffices to show $\mu(\mathcal{B}) = 0$. It is easy to see that $\mathcal{B}$ is closed under finite variations, hence, by Kolmogoroff's 0-1 law, $\mu(\mathcal{B})$ is either 0 or 1. We note the following.

Lemma 15. *If $\mu(\mathcal{B}) = 1$, then for each $\epsilon > 0$, there is an $M_\star$ such that $\mu(\mathcal{B}_{M_\star}) > 1 - \epsilon$.*

Proof Sketch. Fix an $\epsilon > 0$. Suppose that $\mu(\mathcal{B}) = 1$. Then, by countable subadditivity it follows that there exist $M_0, \ldots, M_{k-1}$ such that $\mu(\cup_{i<k} \mathcal{B}_{M_i}) >$

$1 - \frac{\epsilon}{2}$. Now, some elementary measure theory shows that for each $i < k$, there is a fragment σ_i such that $\mu(\langle\!\langle \sigma_i \rangle\!\rangle \cap \mathcal{B}_{M_i}) > \mu(\mathcal{B}_{M_i}) - \frac{\epsilon}{2k}$. Let $M_\star$ be a TM that on input $\langle x, a \rangle$ and oracle R, $M_\star$ first searches for the least $i < k$ (if any) such that $\sigma_i \sqsubseteq R$; if the search succeeds, then $M_\star$ behaves like $M_i^R(\langle x, a \rangle)$; otherwise, $M_\star$ rejects. It is straightforward to argue that for all oracles R, $M_\star$'s run time is bounded by some polynomial. Therefore, without loss of generality we may assume $M_\star$ is polynomially-clocked. It is also straightforward to argue that $\mu(\mathcal{B}_{M_\star}) > 1 - \epsilon$. So, we are done. □

By the lemma, to show (11) it suffices to prove that, for each M, $\mu(\mathcal{B}_M) \leq \frac{1}{2}$. Arbitrarily fix M for the rest of this subsection and let p be a polynomial that bounds M's run time. Now, for each n, let $\mathcal{G}_n =$

$$\left\{ R : \begin{array}{l} (\exists a \in N|_{s(3n+1)}) \\ \quad [\, L(M^R(\cdot, a))|_{3n+1} = \text{corange}(\xi^R)|_{3n+1} \,] \end{array} \right\}.$$

Clearly, $\mathcal{B}_M = \bigcap_{n \in N} \mathcal{G}_n$. Thus, if, for some n, $\mu(\mathcal{G}_n) \leq \frac{1}{2}$, then $\mu(\mathcal{B}_M) \leq \frac{1}{2}$, and, hence, (11) follows. To show the existence of an n such that $\mu(\mathcal{G}_n) \leq \frac{1}{2}$, it suffices to prove:

(12) There is an n such that for *all* $a \in N|_{s(n)}$,

$$\mu(\{\, R : L(M^R(\cdot, a))|_n = \text{corange}(\xi^R)|_n \,\}) \quad < \quad \tfrac{1}{2} \cdot 2^{-s(n)}.$$

Suppose, without loss of generality, that, for each n, $s(n) \geq n$ and $p(n) > 0$. Then, by an appropriate version of the s-m-n theorem, there is a constant c_0 (independent of p and s) such that for each n and each $a \in N|_{s(n)}$, $M^R(\cdot, a)$ on inputs of length n corresponds to a $c_0 \cdot p(s(n))$ time bounded nondeterministic TM. Thus, to show (12) it suffices to prove:

(13) Suppose $\widehat{M}$ is relativized, nondeterministic TM with $c_0 \cdot p(s(n))$ as its time bound for all oracles. Then, there exists an n such that

$$\mu(\left\{ R : L(\widehat{M}^R)|_{3n+1} = \text{corange}(\xi^R)|_{3n+1} \right\}) \quad < \quad 2^{-s(3n+1)-1}.$$

In Theorem 16 we'll obtain a measure bound which will imply (13) (and, hence, (11)) for the s functions of Theorems 12 and 13.

4.2 The Key Bound

Here is the key technical result of §4—homely though it may be.

Theorem 16. *Suppose M is a relativized, nondeterministic TM such that, for all oracles X and all inputs x, M runs in $t(|x|)$ time. For each n, let*

$$\mathcal{M}_n \quad \overset{\text{def}}{=} \quad \{\, R : L^R_M|_{3n+1} = \text{corange}(\xi^R)|_{3n+1} \,\}\,.$$

Finally, suppose $\alpha \in (0,1)$ and $n \in N$ are such that $n - 2\alpha n - 4 - \log t(3n+1) \geq 0$. Then, $\mu(\mathcal{M}_n) \leq 2^{-2^{\alpha n}}$.

We prove this theorem in §4.3. Here we show how use it to obtain Theorems 12 and 13.

Proof of Theorem 12. Let c_0 be the "s-m-n constant" from §4.1. Let p be a polynomial and let be $\widehat{M}$ be a relativized, $c_0 \cdot p(s(n))$-nondeterministic-time TM. Define

$$\widehat{\mathcal{M}}_n \quad = \quad \left\{ R : L(\widehat{M}^R)|_{3n+1} = \text{corange}(\xi^R)|_{3n+1} \right\}.$$

By the analysis of §4.1, to establish the theorem it suffices to show that there is an n such that,

$$\text{(14)} \qquad \mu(\widehat{\mathcal{M}}_n) \quad < \quad 2^{-s(3n+1)-1}.$$

It follows from (10) that

$$\lim_{n\to\infty} \frac{\log(c_0 \cdot p(s(3n+1)))}{n} \quad = \quad 0.$$

Hence, for any $\alpha \in (0, \frac{1}{2})$, we have, for all but finitely many n, that $n - 2\alpha n - 4 - \log(c_0 \cdot p(s(3n+1))) \geq 0$. Fix such an α. Then by Theorem 16, for all sufficiently large n, $\mu(\widehat{\mathcal{M}}_n) < 2^{-2^{\alpha n}}$. It also follows from (10) that for all sufficiently large n, $2^{-2^{\alpha n}} < 2^{-s(3n+1)-1}$. Thus, (14) and the theorem follow. □ **Theorem 12**

Proof of Theorem 13. Let c_0 be the "s-m-n constant" from §4.1. Let p be a degree k polynomial and let $\widehat{M}$ be an arbitrary relativized, $c_0 \cdot p(s_\gamma(n))$ nondeterministic-time TM. Define

$$\widehat{\mathcal{M}}_n \quad = \quad \left\{ R : L(\widehat{M}^R)|_{3n+1} = \text{corange}(\xi^R)|_{3n+1} \right\}.$$

As before, our goal is to establish that there is an n such that

$$\text{(15)} \qquad \mu(\widehat{\mathcal{M}}_n) \; < \; 2^{-s_\gamma(3n+1)-1} \; = \; 2^{-2^{\gamma\cdot(3n+1)}-1}.$$

A bit of messy algebra shows that if $0 < \alpha < \frac{1}{2}(1 - 3k\gamma)$, then for all but finitely many n, $n - 2\alpha n - 4 - \log(c_0 \cdot p(s_\gamma(3n+1))) \geq 0$, and hence by Theorem 16,

$\mu(\mathcal{M}_n) < 2^{-2^{\alpha n}}$. Now, if $\alpha > 3\gamma$, it follows that, for all but finitely many n, $2^{-2^{\alpha n}} < 2^{-2^{\gamma\cdot(3n+1)}-1}$. Therefore, (15) follows, ***provided*** there is an α such that $3\gamma < \alpha < \frac{1}{2}(1-3k\gamma)$. Well, a bit more algebra shows that $0 < \gamma < \frac{1}{3k+6}$ implies $3\gamma < \frac{1}{2}(1-3k\gamma)$. So, we are done. □ **Theorem 13**

Scholium 17. Since in this draft we are omitting details about Boolean circuits, we also have to omit the proof of Theorem 14. However, the key point in the proof of Theorem 14 is simply to note that in the proof of Theorem 13 we obtain an "almost all n" bound on $\mu(\widehat{\mathcal{M}_n})$ and from this we can obtain the "almost everywhere" result of Theorem 14. The fact that the proofs of Theorems 12 and 13 establish "almost all n" bounds on their respective $\mu(\widehat{\mathcal{M}_n})$'s can also be used to strengthen these results. For example, in Theorem 12 we can replace (10) with $\liminf_{n\to\infty}(\log s(n))/n = 0$. We hope to provide more details on this in later drafts of this paper.

4.3 Proof of the Key Bound: Cold Fronts

The proof of Theorem 2 introduced the notion of a cold spot. The proof of Theorem 16 extends this device to (big) collections of "simultaneously cold" spots, which we'll call *cold fronts.*

Notation. $\mathcal{P}_k(A) \overset{\text{def}}{=} \{\, B \subseteq A : \|B\| = k \,\}$, i.e., the collection of all cardinality k subsets of A.

Definition 18. Suppose R, S, and $X \subseteq N$. We say that R and S are *X-variants* (written $R \sim_X S$) if and only if $R \,\triangle\, S \subseteq \left\{\, x\mathbf{10}^k : x \in X \ \&\ k \leq 3|x| \,\right\}$.

For each $\epsilon > 0$, $R \subseteq N$, and $x \in N$, define $D(R,x)$ and $\mathcal{C}(\epsilon,x)$ as in (2) and (3) respectively, Also, for each $\epsilon \in (0,1]$ and $X \subseteq N$, define

$$\mathcal{C}(\epsilon,X) \;=\; \bigcap_{x\in X} \mathcal{C}(\epsilon,x),$$

that is, $\mathcal{C}(\epsilon,X)$ is the set of oracles R such that:

- on strings of length $3n+1$, the set accepted by M^R agrees with corange(ξ^R), *and*

- for *every* $x \in X$, there are no more than $\epsilon\cdot 2^{3n+1}$ many y in L^R_M such that $M^R(y)$ depends on x.

We establish the following two lemmas about the $\mathcal{C}_n(\epsilon,X)$'s.

Lemma 19. *Suppose $\epsilon \in (0,1]$ and $n \in N$ are such that $2^{-2n-1} \leq \epsilon$. Suppose $X \in \mathcal{P}_k(N|_n)$. Then, $\mu(\mathcal{C}_n(\epsilon,X)) \leq (k+1)^k \cdot \epsilon^k$.*

Lemma 20 (The cold front lemma). *Suppose $\epsilon \in (0,1)$ and k and $n \in N$ are such that $k \leq 2^n$ and $k \cdot t(3n+1) \cdot 2^{-n+1} \leq \epsilon$. Then, there is an $X \in \mathcal{P}_k(N|_n)$ such that $\mu(\mathcal{C}_n(\epsilon, X)) \geq \mu(\mathcal{M}_n)/2$.*

Before proving these lemmas, we show how to establish Theorem 16.

Proof of Theorem 16. For the moment we leave $n \in N$ and $k \leq 2^n$ as unspecified. Let

$$\epsilon_0 \;=\; k \cdot t(3n+1) \cdot 2^{-n+1}.$$

Then by Lemma 20 there is a set X_0 of cardinality k such that $\mu(\mathcal{M}_n)/2 \leq \mu(\mathcal{C}_n(\epsilon_0, X_0))$. Clearly, $2^{-2n-1} \leq \epsilon_0$. Hence, by Lemma 19, $\mu(\mathcal{C}_n(\epsilon_0, X_0)) \leq (k+1)^k \cdot \epsilon_0^k$. Combining the two inequalities, we obtain

$$\mu(\mathcal{M}_n)/2 \;\leq\; \mu(\mathcal{C}_n(\epsilon_0, X_0)) \;\leq\; (k+1)^k \cdot \epsilon_0^k.$$

Getting rid of $\mu(\mathcal{C}_n(\epsilon_0, X_0))$ and filling in the definition of ϵ_0 results in the following messy thing.

$$\begin{aligned} \mu(\mathcal{M}_n) \;&\leq\; \frac{2 \cdot ((k+1) \cdot k \cdot t(3n+1))^k}{2^{k(n-1)}} \\ &\leq\; 2^{-k(n-1-\log(k+1)-\log k-\log t(3n+1))+1} \\ &<\; 2^{-k(n-2-2\log k-\log t(3n+1))+1}. \end{aligned}$$

Replacing k in the above with $2^{\alpha n}$, we have

$$\mu(\mathcal{M}_n) \;<\; 2^{-2^{\alpha n}(n-2-2\alpha n-\log t(3n+1))+1}.$$

It is easy to verify that if $n - 2\alpha n - 2 - \log t(3n+1) \geq 2$, then

$$2^{-2^{\alpha n}(n-2\alpha n-\log t(3n+1)-2)+1} \;\leq\; 2^{-2^{\alpha n}}.$$

Therefore, the theorem follows. □ **Theorem 16**

We now prove the two lemmas.

Proof of Lemma 19. Fix an arbitrary oracle $R \in \mathcal{C}(\epsilon, X)$. This R has exactly $2^{k \cdot (3n+1)}$ X-variants. To prove the lemma it suffices, by Lemma 6, to show that at most $(k+1)^k \cdot \epsilon^k \cdot 2^{k \cdot (3n+1)}$ many of these X-variants can be in $\mathcal{C}_n(\epsilon, X)$. Let

$$(16) \qquad I \;\overset{\text{def}}{=}\; N|_{3n+1} - \left(\text{range}(\xi^R) \cup \bigcup_{x \in X} D(R, x) \right).$$

Since $R \in \mathcal{C}(\epsilon, X) \subseteq \mathcal{M}_n$, we have $L^R_M|_{3n+1} = \mathrm{corange}(\xi^R)|_{3n+1}$, and, hence, that $I \subseteq L^R_M|_{3n+1}$. Also, by the definitions of I and $D(R,x)$, we have

$$I \quad = \quad \left\{ y \in L^R_M|_{3n+1} : \begin{array}{r} \text{the value of } M^R(y) \\ \text{does not depend on} \\ \textit{any } x \in X \end{array} \right\}.$$

Hence,

(17) $\qquad$ for *every* $S \sim_X R$, $\; I \subseteq L^S_M|_{3n+1}$.

Suppose S is an X-variant of R such that, for some $x \in X$, $\xi^S(x) \in I$. Then, by (17), $\xi^S(x) \in L^S_M|_{3n+1}$. Hence, $L^S_M|_{3n+1} \neq \mathrm{corange}(\xi^S)|_{3n+1}$. So, $S \notin \mathcal{M}_n$, and, hence, $S \notin \mathcal{C}(\epsilon, X)$ (since $\mathcal{C}(\epsilon, X) \subseteq \mathcal{M}_n$). Therefore, in order for S to be an element of $\mathcal{C}(\epsilon, X)$, it must be the case that for *every* $x \in X$, $\xi^S(x) \in \overline{I}|_{3n+1}$. The number of X-variants of R for which this is the case is easily seen to be $(\|\overline{I}|_{3n+1}\|)^k$. Thus, to establish the lemma it suffices to show that $\|\overline{I}|_{3n+1}\| \leq (k+1) \cdot \epsilon \cdot 2^{3n+1}$.

By (16),

(18) $$\|\overline{I}|_{3n+1}\| \quad \leq \quad \|\bigcup_{x \in X} D(R,x)\| + \|\mathrm{range}(\xi^R|_{3n+1})\|.$$

Since $R \in \mathcal{C}_n(\epsilon, X)$, we have by the definition of $\mathcal{C}_n(\epsilon, X)$ that, for every $x \in X$, $\|D(R,x)\| < \epsilon \cdot 2^{3n+1}$. Therefore,

$$\|\bigcup_{x \in X} D(R,x)\| \quad < \quad \|X\| \cdot \epsilon \cdot 2^{3n+1} \quad = \quad k \cdot \epsilon \cdot 2^{3n+1}.$$

Since $(\xi^R)^{-1}(N|_{3n+1}) = N|_n$, we have that $\|\mathrm{range}(\xi^R)|_{3n+1}\| \leq 2^n$. By assumption $2^{-2n-1} \leq \epsilon$, hence, $2^n = 2^{-2n-1} \cdot 2^{3n+1} \leq \epsilon \cdot 2^{3n+1}$. Thus, by (18) it follows that $\|\overline{I}|_{3n+1}\| \leq (k+1) \cdot \epsilon \cdot 2^{3n+1}$ as required. □ **Lemma 19**

Proof of Lemma 20. We have to show that there is an $X \in \mathcal{P}_k(N|_n)$ such that $\mu(\mathcal{C}(\epsilon, X)) > \frac{1}{2}\mu(\mathcal{M}_n)$. As in the proof of Lemma 10, for each $x \in N$, let $\mathcal{H}(\epsilon, x) \overset{\text{def}}{=} \mathcal{M}_n - \mathcal{C}_n(\epsilon, x)$. Also, for each $X \subseteq N$, let

(19) $$\begin{aligned} \mathcal{H}(\epsilon, X) \quad & \overset{\text{def}}{=} \quad \bigcup_{x \in X} \mathcal{H}(\epsilon, x) \\ & = \quad (\mathcal{M}_n - \mathcal{C}_n(\epsilon, X)) \end{aligned}$$

So, to establish the lemma, it suffices to show,

(20) $\quad$ there exists an $X \in \mathcal{P}_k(N|_n)$ such that $\mu(\mathcal{H}(\epsilon, X)) < \frac{1}{2}\mu(\mathcal{M}_n)$,

which is what we do in the following.

Let $x_0, \ldots, x_{2^n-1}$ be an indexing of $N|_n$ such that

$$\mu(\mathcal{H}(\epsilon, x_0)) \leq \mu(\mathcal{H}(\epsilon, x_1)) \leq \ldots \leq \mu(\mathcal{H}(\epsilon, x_{2^n-1})). \tag{21}$$

Consider $X = \{ x_0, \ldots, x_{k-1} \}$. We have,

$$\begin{array}{rcll} \mu(\mathcal{H}(\epsilon, X)) & = & \mu(\bigcup_{i<k} \mathcal{H}(\epsilon, x_i)) & \text{(by (19))} \\ & \leq & \sum_{i<k} \mu(\mathcal{H}(\epsilon, x_i)) & \text{(by subadditivity).} \end{array}$$

Now, it is a trivial fact about averages that if $v_0 \leq v_1 \leq \cdots \leq v_{n-1}$, then, for each $j \leq n$, $\operatorname{avg}_{i<j} v_i \leq \operatorname{avg}_{i<n} v_i$, and, hence, $\sum_{i<j} v_i \leq j \cdot \operatorname{avg}_{i<n} v_i$. Thus, we have

$$\mu(\mathcal{H}(\epsilon, X)) \quad \leq \quad k \cdot \operatorname*{avg}_{x \in N|_n} \mu(\mathcal{H}(\epsilon, x)). \tag{22}$$

By a simple modification of the proof of Lemma 10 we can show

$$\operatorname*{avg}_{x \in N|_n} \mu(\mathcal{H}(\epsilon, x)) \quad < \quad \frac{1}{\epsilon} \cdot \frac{t(3n+1)}{2^n} \cdot \mu(\mathcal{M}_n).$$

Since, by hypothesis, $k \cdot t(3n+1) \cdot 2^{-n+1} \leq \epsilon$, the above inequality implies that

$$\operatorname*{avg}_{x \in N|_n} \mu(\mathcal{H}(\epsilon, x)) \quad < \quad \frac{\mu(\mathcal{M}_n)}{2 \cdot k}. \tag{23}$$

Together (22) and (23) imply (20). □ **Lemma 20**

5 Immunity Properties

In [KMR89] we showed that, relative to a random oracle R, the only P^R subsets of range(ξ^R) are sparse. Using this result we were able to show that, relative to a random oracle, the Berman-Hartmanis isomorphism conjecture fails. It's a natural question to ask how big the coNP^R subsets of range(ξ^R) can be, relative to a random oracle R. Here is our current best answer.

Theorem 21. *Suppose $\beta \in (\frac{1}{2}, 1)$. Then, relative to a random oracle R, if A^R is a coNP^R subset of* range(ξ^R)*, then, for all but finitely many n,* census($A^R, 3n+1) < 2^{\beta \cdot n}$.

It follows from the proof of Lemma 3.1 in [KMR89] that, relative to a random oracle R, for all but finitely many n, $\mathrm{census}(\mathrm{range}(\xi^R), 3n+1) = 2^n$, and, hence, if A^R is as in the theorem, we have that

$$\mathrm{census}(A^R, n) \quad \in \quad \mathcal{O}(\mathrm{census}(\mathrm{range}(\xi^R), n)^\beta),$$

for each $\beta > \frac{1}{2}$.

We care about this result for a couple different reasons. The first is purely technical. As we shall see below, the proof of Theorem 21 develops the technique of §3 in a rather different direction from that of §4. Our second reason is more strategic in character. Both Theorem 21 and our result on the P^R subsets of $\mathrm{range}(\xi^R)$ establish (complexity theoretic) immunity properties and immunity properties are often key in showing interesting structural properties of classes, e.g., strong separations. Theorem 21 is not strong enough to imply anything too exciting. But, as we discuss in Scholium 25, certain strengthenings of this theorem would have some interesting consequences.

5.1 Preliminaries

Notation. $(\overset{\infty}{\exists} x)Q(x, \vec{y})$ means there are infinitely many $x \in N$ such that $Q(x, \vec{y})$ holds.

Let M be an arbitrary relativized, polynomially-clocked, nondeterministic TM and let p be a polynomial that bounds M's run time. By an analysis similar to that carried out in §3 and §4, it follows that to show Theorem 21 it suffices to prove:

$$\mu(\left\{ R : \begin{array}{c} \overline{L(M^R)} \subseteq \mathrm{range}(\xi^R) \quad \& \\ (\overset{\infty}{\exists} n)[\, \|A^R|_{3n+1}\| \geq 2^{\beta n}\,] \end{array} \right\}) \;=\; 0,$$

for each $\beta \in (\frac{1}{2}, 1)$. It is useful re-express this. For each $\eta \colon N \longrightarrow (0, 1]$, define

$$\mathcal{M}(\eta) \;=\; \left\{ R : \begin{array}{c} \overline{L(M^R)} \subseteq \mathrm{range}(\xi^R) \qquad \& \\ (\overset{\infty}{\exists} n)[\, \|\overline{L(M^R)}|_{3n+1}\| \geq \eta(n) \cdot 2^n\,] \end{array} \right\}.$$

Therefore, to show the theorem, it suffices to show

$$\text{(24)} \qquad \text{for each } \alpha \in (0, \tfrac{1}{2}),\ \mu(\mathcal{M}(\lambda n.2^{-\alpha n})) = 0.$$

Let's further reduce the problem. Define, for each $\gamma \in (0, 1]$ and each $n \in N$,

$$\mathcal{M}_{n,\gamma} \;=\; \left\{ R : \begin{array}{c} \overline{L(M^R)} \subseteq \mathrm{range}(\xi^R) \quad \& \\ \|\overline{L(M^R)}|_{3n+1}\| \geq \gamma \cdot 2^n \end{array} \right\}.$$

Note that, $\mathcal{M}(\eta) = \bigcap_{n=0}^{\infty} \bigcup_{i\geq n} \mathcal{M}_{n,\eta(n)}$. Hence, for all n,

$$\mathcal{M}(\eta) \;\subseteq\; \bigcup_{i\geq n} \mathcal{M}_{n,\eta(n)}. \tag{25}$$

Our goal in what follows is to show

Proposition 22. *Suppose $\alpha \in (0, \frac{1}{2})$. Then, for all sufficiently large n,*

$$\mu(\mathcal{M}_{n,2^{-\alpha n}}) \;\leq\; 1/n^2.$$

It follows from the proposition that, for each $\alpha \in (0, \frac{1}{2})$ and for all sufficiently large n,

$$\begin{array}{rcll} \mu(\mathcal{M}(\lambda n.2^{-\alpha\cdot n})) & \leq & \mu(\cup_{i\geq n}\mathcal{M}_{n,2^{-\alpha n}}) & \text{(by (25))} \\ & \leq & \sum_{i\geq n} \mu(\mathcal{M}_{n,2^{-\alpha n}}) & \text{(by subadditivity)} \\ & \leq & \sum_{i\geq n} \frac{1}{n^2} & \text{(by Proposition 22)} \\ & \leq & \frac{1}{n-1}. & \end{array}$$

Therefore, by the proposition, we have that (24) (and, hence, Theorem 21) follows.

5.2 The Main Argument

For each R and each $x \in N$, define $D(R,x)$ as in (2) and, for each ϵ and $\gamma \in (0,1]$ and each $x \in N$, define

$$\mathcal{C}(\epsilon,\gamma,x) \;=\; \left\{ R \in \mathcal{M}_{|x|,\gamma} : \begin{array}{c} \xi^R(x) \in \overline{L(M^R)} \quad \& \\ \|D(R,x)\| < \epsilon \cdot 2^{3|x|+1} \end{array} \right\}.$$

Note that this is definition of the $\mathcal{C}$ classes differs from than in the proofs Theorems 2 and 16. The introduction of the the "$\xi^R(x) \in \overline{L(M^R)}$" conjunct is necessary since, unlike the NP$^R \neq$ coNP^R argument, we are allowing $\overline{L(M^R)}$ to be a strict subset of range(ξ^R) when $R \in \mathcal{M}_n$. As one might expect this conjunct is the source of the difficulties in the argument below.

We show the following two lemmas about the $\mathcal{C}(\epsilon,\gamma,x)$'s.

Lemma 23. *Suppose $\epsilon \in (0,1]$ and $n \in N$ are such that $2^{-2n-1} \leq \epsilon$. Then, for all $x \in N|_n$ and all $\gamma \in (0,1]$, $\mu(\mathcal{C}(\epsilon,\gamma,x)) \leq 2\epsilon$.*

Lemma 24 (The cold spot lemma). *Suppose ϵ and $\gamma \in (0,1)$ and $n \in N$ are such that $\epsilon = \frac{p(3n+1)}{\gamma\cdot 2^{n-1}}$. Then, there exists an $x_n \in N|_n$ such that*

$$\mu(\mathcal{C}(\epsilon,\gamma,x)) \;>\; \frac{\gamma}{2}\cdot\mu(\mathcal{M}_{n,\gamma}).$$

Before proving these two lemmas, we attend to the proof of the main proposition.

Proof of Proposition 22. Suppose $n \in N$ and γ and $\epsilon \in (0,1)$ are such that $\epsilon = \frac{p(3n+1)}{\gamma \cdot 2^{n-1}}$. Then, by Lemma 24 there is an $x_n \in N|_n$ such that

$$\mu(\mathcal{C}(\epsilon, \gamma, x)) \quad > \quad \frac{\gamma}{2} \cdot \mu(\mathcal{M}_{n,\gamma}).$$

Clearly, $2^{-2n-1} \leq \epsilon$, so by Lemma 23 we have that $\mu(\mathcal{C}(\epsilon,\gamma,x)) < 2\epsilon$. Combining the two inequalities and filling in our choice definition of ϵ, we have that

$$\frac{4 \cdot p(3n+1)}{\gamma^2 \cdot 2^n} > \mu(\mathcal{M}_{n,\gamma}).$$

So, to guarantee that $\mu(\mathcal{M}_{n,\gamma}) \leq 1/n^2$, it suffices to make $4 \cdot p(3n+1)/(\gamma^2 \cdot 2^n) \leq 1/n^2$. Solving for γ we find that we need

$$\gamma \quad \geq \quad \sqrt{\frac{4 \cdot n^2 \cdot p(3n+1)}{2^n}}.$$

If $\gamma = 2^{-\alpha n}$ for $\alpha \in (0, \frac{1}{2})$, this last inequality holds for sufficiently large n. So, we're done. □ **Proposition 22**

The proof of Lemma 23 is essentially the same as the proof of Lemma 9. It is the proof of Lemma 24 where things get interesting.

Proof of Lemma 24. Suppose n, γ, and ϵ are as in the hypothesis. For each $x \in N|_n$, let

$$\begin{aligned}\mathcal{H}(\epsilon,\gamma,x) \quad &\stackrel{\text{def}}{=} \quad \left\{ R \in \mathcal{M}_{n,\gamma} : \begin{array}{c} \xi^R(x) \in L(M^R) \quad \text{or} \\ \|D(R,x)\| > \epsilon \cdot 2^{3n+1} \end{array} \right\} \\ &= (\, \mathcal{M}_{n,\gamma} - \mathcal{C}(\epsilon,\gamma,x)\,).\end{aligned}$$

To show the existence of an $x_n \in N|_n$ such that $\mu(\mathcal{C}(\epsilon,\gamma,x_n)) \geq \frac{\gamma}{2} \cdot \mu(\mathcal{M}_{n,\gamma})$, it suffices to find an $x_n \in N|_n$ such that $\mu(\mathcal{H}(\epsilon,\gamma,x_n)) \leq (1 - \frac{\gamma}{2}) \cdot \mu(\mathcal{M}_{n,\gamma})$. As in the proof of Lemma 10, we show that

$$\operatorname*{avg}_{x \in N|_n} \mu(\mathcal{H}(\epsilon,\gamma,x)) \quad \leq \quad (1 - \frac{\gamma}{2}) \cdot \mu(\mathcal{M}_{n,\gamma}),$$

and, hence, the existence of x_n is immediate.

Let μ_* the product measure on $\mathcal{P}(N) \times N|_n$. Let:

$$\begin{aligned}
\mathcal{D} \quad &\stackrel{\text{def}}{=} \quad \{\, (R,x) : R \in \mathcal{M}_{n,\gamma} \;\&\; \xi^R(x) \in L(M^R) \,\}. \\
\mathcal{E} \quad &\stackrel{\text{def}}{=} \quad \left\{ (R,x) : \begin{array}{c} R \in \mathcal{M}_{n,\gamma} \quad \& \\ \|D(R,x)\| > \epsilon \cdot 2^{3n+1} \end{array} \right\}. \\
\mathcal{F} \quad &\stackrel{\text{def}}{=} \quad \{\, (R,x) : x \in \mathcal{H}(\epsilon,\gamma,x) \,\} \\
&= \quad \mathcal{D} \cup \mathcal{E}.
\end{aligned}$$

Clearly,

$$\begin{aligned}
\operatorname{avg}_{x\in N|_n} \mu(\mathcal{H}(\epsilon,\gamma,x)) &= \mu_*(\mathcal{F}) \\
&= \mu_*(\mathcal{D}) + \mu_*(\mathcal{E}) - \mu_*(\mathcal{D}\cap\mathcal{E}) \qquad (26)\\
&\leq \mu_*(\mathcal{D}) + \mu_*(\mathcal{E}).
\end{aligned}$$

Thus, in order to obtain an upper bound on $\operatorname{avg}_{x\in N|_n} \mu(\mathcal{H}(\epsilon,\gamma,x)$, we find upper bounds on $\mu_*(\mathcal{D})$ and $\mu_*(\mathcal{E})$.

First consider $\mu_*(\mathcal{D})$. *Notation.* If $R(\vec{x})$ is a relation, then $[\![R(\vec{x})]\!]$ is the "characteristic function" of the relation. E.g., $[\![x < y]\!](a,b)$ is 1 if $a < b$ and 0 otherwise. (This notation is due to Iverson.) Now,

$$\begin{aligned}
\mu_*(\mathcal{D}) &= \int_{\mathcal{M}_{n,\gamma}\times N|_n} [\![\xi^R(x) \in L(M^R)]\!] \\
&= \int_{\mathcal{M}_{n,\gamma}} \int_{N|_n} [\![\xi^R(x) \in L(M^R)]\!]\, dx\, dR \\
&\leq \int_{\mathcal{M}_{n,\gamma}} (1-\gamma)\, dR \\
&\qquad \text{(by the definition of } \mathcal{M}_{n,\gamma}) \\
&= (1-\gamma)\cdot\mu(\mathcal{M}_{n,\gamma}).
\end{aligned}$$

Next consider $\mu_*(\mathcal{E})$. By our choice of ϵ we have $\epsilon \geq p(3n+1)\cdot 2^{-n+1}$. So, by a direct lift of the proof of Lemma 10 it follows that

$$\mu_*(\mathcal{E}) \;<\; \frac{p(3n+1)}{\epsilon\cdot 2^n}\cdot\mu(\mathcal{M}_{n,\gamma}).$$

Therefore, by (26) and the bounds on $\mu_*(\mathcal{D})$ and $\mu_*(\mathcal{E})$ we have

$$\operatorname*{avg}_{x\in N|_n} \mu(\mathcal{H}(\epsilon,\gamma,x) \;<\; (1-\gamma+\frac{p(3n+1)}{\epsilon\cdot 2^n})\cdot\mu(\mathcal{M}_{n,\gamma}).$$

Since $\epsilon = \frac{p(3n+1)}{\gamma\cdot 2^{n-1}}$, the above inequality becomes

$$\operatorname*{avg}_{x\in N|_n} \mu(\mathcal{H}(\epsilon,\gamma,x) \;<\; (1-\frac{\gamma}{2})\cdot\mu(\mathcal{M}_{n,\gamma})$$

as required. □ **Lemma 24**

Scholium 25. We doubt the upper bound of Theorem 21 is tight. Let's briefly consider how one might improve this bound. An analysis of the proof shows that the key bound is

$$\begin{aligned}
\operatorname*{avg}_{x\in N|_n} \mu(\mathcal{H}(\epsilon,\gamma,x)) &= \mu_*(\mathcal{D}) + \mu_*(\mathcal{E}) - \mu_*(\mathcal{D}\cap\mathcal{E}) \qquad (27)\\
&\leq \mu_*(\mathcal{D}) + \mu_*(\mathcal{E}).
\end{aligned}$$

Our bounds on $\mu_*(\mathcal{D})$ and $\mu_*(\mathcal{E})$ are tight, but in the proof we use the trivial lower bound of 0 on $\mu_*(\mathcal{D}\cap\mathcal{E})$ and it is here that there is room for improvement.

We do not yet have a good lower bound on $\mu_*(\mathcal{D}\cap\mathcal{E})$. In the best of all possible worlds, $\mathcal{D}$ and $\mathcal{E}$ would be independent and then we would have

$$\operatorname*{avg}_{x\in N|_n} \mu(\mathcal{H}(\epsilon,\gamma,x)) \quad = \quad \mu_*(\mathcal{D}) + \mu_*(\mathcal{E}) - \mu_*(\mathcal{D})\cdot\mu_*(\mathcal{E}).$$

Now, if $0 \leq a, b \leq 1$, then in the region $[0,a]\times[0,b]$ the function $\lambda x, y \,.\, (x+y-x\cdot y)$ achieves is maximal value at the point (a,b). Hence, from our upper bounds on $\mu_*(\mathcal{D})$ and $\mu_*(\mathcal{E})$ and some algebra it follows that

$$\mu_*(\mathcal{D}) + \mu_*(\mathcal{E}) - \mu_*(\mathcal{D}\cap\mathcal{E}) \quad \leq \quad \gamma(1-\frac{p(3n+1)}{\epsilon\cdot 2^n}),$$

provided, $\epsilon \geq p(3n+1)\cdot 2^{-n+1}$. Well, choosing $\epsilon = p(3n+1)\cdot 2^{-n+1}$ and going through some more calculations, the lower bound on γ becomes $\gamma \geq 4\cdot n^2\cdot p(3n+1)\cdot 2^{-n}$. Hence, we could conclude from this that, relative to a random oracle R, the only coNP^R subsets of range(ξ^R) are sparse. We doubt that $\mathcal{D}$ and $\mathcal{E}$ are really independent, but their covariance may well be low.

We mention another possible improvement of Theorem 21. It follows from our work in [KMR89] that if, relative to a random oracle, A^R is a P^R set with census$(A^R, 3n+1) \leq 2^n$ (for all but finitely many n), then $A^R\cap$range(ξ^R) is sparse. If in Theorem 21 we could replace the hypothesis that "A^R is a coNP^R subset of range(ξ^R)" with "census$(A^R, 3n+1) \leq 2^n$," then we believe we could use this result to obtain strong separation results about the extended Boolean Hierarchy (see the survey [Wag88]) relative to a random oracle. We do not have the space here to go into the details of this.

6 Conclusions and Directions

We believe the above results have shown that our average dependence technique to be a powerful and simple method for addressing certain random oracle questions. But it is clear that there is still much room for improvement. We mentioned a number of specific technical open problems in prior sections. Here we briefly discuss some broader (and wilder) open questions that interest us.

1. By Cai's [Cai89] and Babai's [Bab87] we know that, relative to a random oracle, PH $\subset$ PSPACE. Both [Cai89] and [Bab87] depend heavily on the Furst, Saxe, and Sisper analysis [FSS84] and Yao's circuit size bounds [Yao85]. Is there a proof which by-passes [FSS84] and [Yao85] and shows PH $\subset$ PSPACE relative to a random oracle? The motivation here is to find an alternative analysis of this problem that may develop some interesting new insights.

2. Is PH strict relative to a random oracle? This is one of the best known open problems on random oracles. If one can answer the previous question, then this might fall.

3. Can one rid random oracle results of random oracles? By this we mean the following. We claimed in the introduction that random oracles modeled very strong polynomial-time, pseudo-random functions. Can one formalize these functions so that from their existence one can deduce most of the structural facts known to be true relative to a random oracle. Our work on annihilating and the isomorphism conjecture is a small example of what we have in mind.

We have no idea if average dependence will be useful in solving any of the above. But, we feel strongly that the general methodology of striving for simplicity and clarity of underlying ideas will be important in obtaining any solution of these very hard problems.

Acknowledgments. We wish to thank Jack Lutz for his very helpful comments on an earlier version of this paper. The third author's research was supported in part by NSF grant number CCR-89011154.

References

[Bab87] L. Babai. Random oracles separate PSPACE from the polynomial-time hierarchy. *Information Processing Letters*, 26:51–53, 1987.

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

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

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

[CGH90] B. Chor, O. Goldreich, and J. Hastad. The random oracle hypothesis is false. Technical Report TR 631, Dept. of Computer Science, Technion Institute, 1990.

[Dud89] R. Dudley. *Real Analysis.* Wadsworth & Brooks/Cole, 1989.

[FSS84] M. Furst, J. Saxe, and M. Sipser. Parity, circuits, and the polynomial-time hierarchy. *Math. Syst. Theory*, pages 13–27, 1984.

[HU79] J. Hopcroft and J. Ullman. *Introduction to Automata Theory, Languages, and Computation.* Addison-Wesley, 1979.

[KL82] R. Karp and R. Lipton. Turing machines that take advice. *L'Enseignement Mathématique*, 20:191–209, 1982.

[KMR89] S. Kurtz, S. Mahaney, and J. Royer. The isomorphism conjecture fails relative to a random oracle. In *Proceedings of the 21st annual ACM Symposium on Theory of Computing*, pages 157–166, 1989.

[Kur83] S. Kurtz. On the random oracle hypothesis. *Information and Control*, 57:40–47, 1983.

[LS90] J. Lutz and W. Schmidt. Circuit size relative to pseudorandom oracles. A revision of a paper of the same title in the *Proceedings of the 5th Annual IEEE Structure in Complexity Theory Conference*, 1990.

[Oxt80] J. Oxtoby. *Measure and Category.* Springer-Verlag, 1980.

[Pip79] N. Pippenger. On simultaneous resource bounds. In *Proceedings of the 18th Annual IEEE Symposium on Foundations of Computer Science*, pages 307–311. IEEE Computer Society, 1979.

[Pla77] D. Plaisted. New NP-hard and NP-complete polynomial and integer divisibility problems. In *Proceedings of the 18th Annual IEEE Symposium on Foundations of Computer Science*, pages 241–253, 1977.

[Rog67] H. Rogers. *Theory of Recursive Functions and Effective Computability.* McGraw-Hill, 1967. Reprinted. MIT Press. 1987.

[Roy68] H. Royden. *Real Analysis.* Macmillan, 1968.

[Rud66] W. Rudin. *Real and Complex Analysis.* McGraw-Hill, 1966.

[Wag88] K. Wagner. Bounded query computations. In *Proceedings of the 3rd Annual IEEE Structure in Complexity Theory Conference*, pages 260–277, 1988.

[Wil85] C. Wilson. Relativized circuit complexity. *J. Comput. Syst. Sci.*, 31:169–181, 1985.

[Yao85] A. Yao. Separating the polynomial-time hierarchy by oracles. In *Proceedings of the 26th Annual IEEE Symposium on Foundations of Computer Science*, pages 1–10, 1985.