Dimension Characterizations of Complexity Classes

Xiaoyang Gu [*‡]　　Jack H. Lutz[†‡]

Abstract

We use derandomization to show that sequences of positive pspace-dimension – in fact, even positive Δ^{p}_k-dimension for suitable k – have, for many purposes, the full power of random oracles. For example, we show that, if S is any binary sequence whose Δ^{p}_3-dimension is positive, then $\mathrm{BPP} \subseteq \mathrm{P}^S$ and, moreover, every BPP promise problem is P^S-separable. We prove analogous results at higher levels of the polynomial-time hierarchy.

The *dimension-almost-class* of a complexity class $\mathcal{C}$, denoted by dimalmost-$\mathcal{C}$, is the class consisting of all problems A such that $A \in \mathcal{C}^S$ for all but a Hausdorff dimension 0 set of oracles S. Our results yield several characterizations of complexity classes, such as BPP = dimalmost-P and AM = dimalmost-NP, that refine previously known results on almost-classes. They also yield results, such as Promise-BPP = almost-P-Sep = dimalmost-P-Sep, in which even the almost-class appears to be a new characterization.

1 Introduction

Assessing the computational power of randomness is one of the most fundamental challenges facing computational complexity theory. Concrete questions involving the best algorithms for primality testing, factoring, etc., are instances of this challenge, as are structural questions concerning BPP, AM, and other randomized complexity classes.

One approach to studying the power of a randomized complexity class $\mathcal{C}$ is to address the following question: If $\mathcal{C}_0$ is the nonrandomized version of $\mathcal{C}$, then how weak an assumption can we place on an oracle S and still be assured that $\mathcal{C} \subseteq \mathcal{C}_0^S$? For example, how weak an assumption can we place on an oracle S and still be assured that $\mathrm{BPP} \subseteq \mathrm{P}^S$? For this particular question, it was a result of folklore that $\mathrm{BPP} \subseteq \mathrm{P}^S$ holds for every oracle S that is algorithmically random in the sense of Martin-Löf [22]; it was shown by Lutz [18] that $\mathrm{BPP} \subseteq \mathrm{P}^S$ holds for every oracle S that is pspace-random; and it was shown by Allender and Strauss [3] that $\mathrm{BPP} \subseteq \mathrm{P}^S$ holds for every oracle S that is p-random, or even random relative to a particular sublinear-time complexity class.

In this paper, we extend this line of inquiry by considering oracles S that have *positive dimension* (a complexity-theoretic analog of classical Hausdorff dimension [11, 8]) with respect to various resource bounds. Specifically, we prove that every oracle S that has positive Δ^{p}_3-dimension (hence every oracle S that has positive pspace-dimension) satisfies $\mathrm{BPP} \subseteq \mathrm{P}^S$.

Our main theorem is a generalization of this fact that applies to randomized promise classes at various levels of the polynomial-time hierarchy. (Promise problems were introduced by Grollman and Selman [10]. The randomized promise class Promise-BPP was introduced by Buhrman

[*] Department of Computer Science, Iowa State University, Ames, IA 50011, USA. Email: xiaoyang@cs.iastate.edu

[†] Department of Computer Science, Iowa State University, Ames, IA 50011, USA. Email: lutz@cs.iastate.edu

[‡] Research supported in part by National Science Foundation Grant 0344187.

and Fortnow [6] and shown by Fortnow [9] to characterize a "strength level" of derandomization hypotheses. The randomized promise class Promise-AM was introduced by Moser [25].) For every integer $k \geq 0$, our main theorem says that, for every oracle S with positive $\Delta^{\rm P}_{k+3}$-dimension, every $\mathrm{BP} \cdot \Sigma^{\rm P}_k$ promise problem is $\Sigma^{{\rm P},S}_k$-separable. In particular, if S has positive $\Delta^{\rm P}_3$-dimension, then every BPP promise problem is P^S-separable, and, if S has positive $\Delta^{\rm P}_4$-dimension, then every AM promise problem is NP^S-separable.

We use our results to investigate classes of the form

$$\text{dimalmost-}\mathcal{C} = \left\{ A \,\middle|\, \dim_{\rm H}(\left\{ B \,\middle|\, A \notin \mathcal{C}^B \right\}) = 0 \right\}$$

for various complexity classes $\mathcal{C}$. It is clear that dimalmost-$\mathcal{C}$ is contained in the extensively investigated class

$$\text{almost-}\mathcal{C} = \left\{ A \,\middle|\, \Pr[A \notin \mathcal{C}^B] = 0 \right\},$$

where the probability is computed according to the uniform distribution (Lebesgue measure) on the set of all oracles B. We show that

$$\text{dimalmost-}\Sigma^{\rm P}_k\text{-Sep} = \text{almost-}\Sigma^{\rm P}_k\text{-Sep} = \text{Promise-BP} \cdot \Sigma^{\rm P}_k$$

holds for every integer $k \geq 0$, where $\Sigma^{\rm P}_k$-Sep is the set of all $\Sigma^{\rm P}_k$-separable pairs of languages. This implies that

$$\text{dimalmost-P} = \text{BPP},$$

refining the proof by Bennett and Gill [5] that almost-P = BPP. Also, for all $k \geq 1$,

$$\text{dimalmost-}\Sigma^{\rm P}_k = \text{BP} \cdot \Sigma^{\rm P}_k,$$

refining the proof by Nisan and Wigderson [26] that almost-$\Sigma^{\rm P}_k = \mathrm{BP} \cdot \Sigma^{\rm P}_k$.

The 1997 derandomization method of Impagliazzo and Wigderson [16] is central to our arguments.

2 Resource-Bounded Dimension and Relativized Circuit Complexity

This section reviews and develops those aspects of resource-bounded dimension and its relationship to relativized circuit-size complexity that are needed in this paper. It is convenient to use entropy rates as an intermediate step in this development.

2.1 Resource-Bounded Dimension

Resource-bounded dimension is an extension of classical Hausdorff dimension that imposes dimension structure on various complexity classes. There are now several equivalent ways to formulate resource-bounded dimension. Here we sketch the elements of the original formulation that are useful in this paper.

We work in the Cantor-space $\mathbf{C}$ of all infinite binary sequences.

Definition. ([19]). Let $s \in [0, \infty)$.

1. An *s-gale* is a function $d : \{0,1\}^* \to [0, \infty)$ satisfying $d(w) = 2^{-s}[d(w0) + d(w1)]$ for all $w \in \{0,1\}^*$.

2. An s-gale *succeeds* on a sequence $S \in \mathbf{C}$ if $\limsup\limits_{n\to\infty} d(S[0..n-1]) = \infty$, where $S[0..n-1]$ denotes the n-bit prefix of S.

3. The *success set* of an s-gale d is $S^\infty[d] = \{S \in \mathbf{C} \mid d \text{ succeeds on } S\}$.

The following *gale characterization of Hausdorff dimension* is the key to resource-bounded dimension. In this paper we will use this characterization *in place* of the original definition of Hausdorff dimension [11, 8], which we refrain from repeating here.

Theorem 2.1. *(Lutz [19]). The Hausdorff dimension of a set $X \subseteq \mathbf{C}$ is*

$$\dim_{\mathrm{H}}(X) = \inf\{s \mid \textit{there is an s-gale d such that } X \subseteq S^\infty[d]\}.$$

To extend Hausdorff dimension to complexity classes, we define a *resource bound* to be one of the following classes of functions.

all $= \{f \mid f : \{0,1\}^* \to \{0,1\}^*\}$
p $= \left\{f \in \text{all} \,\middle|\, f \text{ is computable in } n^{O(1)} \text{ time}\right\}$
$\Delta^{\mathrm{p}}_k = \mathrm{p}^{\Sigma^{\mathrm{P}}_{k-1}}$ for $k \geq 2$
pspace $= \left\{f \in \text{all} \,\middle|\, f \text{ is computable in } n^{O(1)} \text{ space}\right\}$

Each of these resource bounds Δ is associated with a *result class* $R(\Delta)$ defined as follows.

$R(\text{all}) = \mathbf{C}$
$R(\mathrm{p}) = \mathrm{E} = \mathrm{TIME}(2^{\text{linear}})$
$R(\Delta^{\mathrm{p}}_k) = \Delta^{\mathrm{E}}_k = \mathrm{E}^{\Sigma^{\mathrm{P}}_{k-1}}$
$R(\text{pspace}) = \mathrm{ESPACE} = \mathrm{SPACE}(2^{\text{linear}})$

A real-valued function $f : \{0,1\}^* \to [0,\infty)$ is Δ-*computable* if there is a function $\hat{f} : \{0,1\}^* \times \mathbb{N} \to \mathbb{Q}$ such that $\hat{f} \in \Delta$ (where the input $(w,r) \in \{0,1\}^* \times \mathbb{N}$ is suitably encoded with r in unary) and, for all $w \in \{0,1\}^*$ and $r \in \mathbb{N}$, $|\hat{f}(w,r) - f(w)| \leq 2^{-r}$.

We now define resource-bounded dimension by imposing resource bounds on the gale characterization in Theorem 2.1.

Definition. ([19]). Let Δ be a resource bound, and let $X \subseteq \mathbf{C}$. (We identify each $S \in X$ with the language whose characteristic sequence is S.)

1. The Δ-*dimension* of X is

$$\dim_\Delta(X) = \inf\{s \mid \text{there is a } \Delta\text{-computable } s\text{-gale } d \text{ such that } X \subseteq S^\infty[d]\}.$$

2. The *dimension* of X *in* $R(\Delta)$ is $\dim(X|R(\Delta)) = \dim_\Delta(X \cap R(\Delta))$.

As shown in [19], these definitions endow the above-mentioned complexity classes $R(\Delta)$ with dimension structure. In general,

$$0 \leq \dim(X|R(\Delta)) \leq \dim_\Delta(X) \leq 1,$$

and $\dim(R(\Delta)|R(\Delta)) = 1$. Also,

$$\Delta \subseteq \Delta' \implies \dim_{\Delta'}(X) \leq \dim_\Delta(X),$$

e.g., $\dim_{\text{pspace}}(X) \leq \dim_{\Delta^{\mathrm{p}}_3}(X)$. It is clear that $\dim_{\text{all}}(X) = \dim(X|\mathbf{C}) = \dim_{\mathrm{H}}(X)$.

Our main results involve Δ-dimensions of individual sequences S, by which we mean

$$\dim_\Delta(S) = \dim_\Delta(\{S\}).$$

We use the easily verified fact that, if Δ is any of the *countable* resource bounds above, then

$$\dim_{\mathrm{H}}(\{S \mid \dim_\Delta(S) = 0\}) = 0. \tag{2.1}$$

For more discussion, motivation, examples, and results, see [19, 14, 20, 12, 23].

2.2 Entropy Rates

We use a recent result of Hitchcock and Vinodchandran [15] relating entropy rates to dimension. Entropy rates were studied by Chomsky and Miller [7], Kuich [17], Staiger [27, 28], Hitchcock [12], and others.

Definition. The *entropy rate* of a language $A \subseteq \{0,1\}^*$ is

$$H_A = \limsup_{n\to\infty} \frac{\log |A_{=n}|}{n},$$

where $A_{=n} = A \cap \{0,1\}^n$.

Definition. Let $\mathcal{C}$ be a class of languages, and let $X \subseteq \mathbf{C}$. The $\mathcal{C}$-*entropy rate* of X is

$$\mathcal{H}_{\mathcal{C}}(X) = \inf\left\{H_A \;\middle|\; A \in \mathcal{C} \text{ and } X \subseteq A^{\text{i.o.}}\right\},$$

where

$$A^{\text{i.o.}} = \{S \in \mathbf{C} \mid (\exists^\infty n) S[0..n-1] \in A\}.$$

The following result is a routine relativization of Theorem 5.5 of [15].

Theorem 2.2. *(Hitchcock and Vinodchandran [15]). For all $X \subseteq \mathbf{C}$ and $k \in \mathbb{Z}^+$,*

$$\dim_{\Delta^{\mathrm{P}}_{k+2}}(X) \le \mathcal{H}_{\Sigma^{\mathrm{P}}_k}(X).$$

2.3 Relativized Circuit-Size Complexity

Definition.1 [29]. For $f : \{0,1\}^n \to \{0,1\}$ and $A \subseteq \{0,1\}^*$, $\mathrm{size}^A(f)$ is the minimum size of (i.e., number of wires in) an n-input oracle circuit γ such that γ^A computes f.

2. For $x \in \{0,1\}^*$ and $A \subseteq \{0,1\}^*$, $\mathrm{size}^A(x) = \mathrm{size}^A(f_x)$, where $f_x : \{0,1\}^{\lceil \log |x| \rceil} \to \{0,1\}$ is defined by

$$f_x(w_i) = \begin{cases} x[i] & \text{if } 0 \le i < |x| \\ 0 & \text{if } i \ge |x|, \end{cases}$$

$w_0, \ldots, w_{2^{\lceil \log |x| \rceil}-1}$ lexicographically enumerate $\{0,1\}^{\lceil \log |x| \rceil}$, and $x[i]$ is the ith bit of x.

Lemma 2.3. *For all $A, S \in \mathbf{C}$,*

$$\mathcal{H}_{\mathrm{NP}^A}(\{S\}) \le \liminf_{n\to\infty} \frac{\mathrm{size}^A(S[0..n-1]) \log n}{n}.$$

Proof. Assume that

$$\alpha > \beta > \liminf_{n\to\infty} \frac{\mathrm{size}^A(S[0..n-1]) \log n}{n}.$$

It suffices to show that $\mathcal{H}_{\mathrm{NP}^A}(\{S\}) \leq \alpha$.

Let B be the set of all strings x such that $\mathrm{size}^A(x) < \beta \frac{|x|}{\log |x|}$. By standard circuit-counting arguments (e.g., see [21]), there is a constant $c \in \mathbb{N}$ such that, for all sufficiently large n, if we choose $m \in \mathbb{N}$ with $2^{m-1} \leq n < 2^m$ and write $\gamma = 2^{-m}n$, so that

$$\beta \frac{n}{\log n} = \beta \frac{\gamma 2^m}{\log(\gamma 2^m)} \leq \beta\gamma \frac{2^m}{m-1},$$

then

$$|B_{=n}| \leq c \left(4e\beta\gamma \frac{2^m}{m-1}\right)^{\beta\gamma\frac{2^m}{m-1}},$$

so

$$\begin{aligned} \log |B_{=n}| &\leq \log c + \beta\gamma \frac{2^m}{m-1} \log\left(4e\beta\gamma\frac{2^m}{m-1}\right) \\ &= \log c + \beta\gamma 2^m \left[\frac{m}{m-1} + \frac{\log 4e\beta\gamma - \log(m-1)}{m-1}\right] \\ &\leq \alpha n, \end{aligned}$$

whence

$$H_B = \limsup_{n\to\infty} \frac{\log |B_{=n}|}{n} \leq \alpha.$$

By our choice of β, $S \in B^{\mathrm{i.o.}}$. Since $B \in \mathrm{NP}^A$, it follows that $\mathcal{H}_{\mathrm{NP}^A}(\{S\}) \leq \alpha$. □

Notation. For $k \in \mathbb{N}$ and $x \in \{0,1\}^*$, we write

$$\mathrm{size}^{\Sigma_k^{\mathrm{P}}}(x) = \mathrm{size}^{K^k}(x),$$

where K^k is the canonical Σ_k^{P}-complete language [4].

By Theorem 2.2 and Lemma 2.3, we have the following.

Theorem 2.4. *For all $S \in \mathbf{C}$ and $k \in \mathbb{N}$,*

$$\dim_{\Delta_{k+3}^{\mathrm{P}}}(S) \leq \liminf_{n\to\infty} \frac{\mathrm{size}^{\Sigma_k^{\mathrm{P}}}(S[0..n-1])}{n}$$

3 Positive-Dimension Derandomization

In order to state our main theorem, we review the notion of separability and give a formulation of Promise-BP-classes that is suitable for our purposes.

Definition. Given a class $\mathcal{C}$ of languages, an ordered pair $A = (A^+, A^-)$ of (disjoint) languages is *$\mathcal{C}$-separable* if there exists a language $C \in \mathcal{C}$ such that $A^+ \subseteq C$ and $A^- \cap C = \varnothing$. We write

$$\mathcal{C}\text{-Sep} = \left\{(A^+, A^-) \,\middle|\, (A^+, A^-) \text{ is } \mathcal{C}\text{-separable}\right\}.$$

Definition. Fix a standard paring function $\langle , \rangle : \{0,1\}^* \times \{0,1\}^* \to \{0,1\}^*$.

1. A *witness configuration* is an ordered pair $\mathcal{B} = (B, g)$ where $B \subseteq \{0,1\}^*$ and $g : \mathbb{N} \to \mathbb{N}$.
2. Given a witness configuration $\mathcal{B} = (B, g)$, the $\mathcal{B}$*-critical event* for a string $x \in \{0,1\}^*$ is the set

$$\mathcal{B}_x = \left\{ w \in \{0,1\}^{g(|x|)} \mid \langle x, w \rangle \in B \right\},$$

   interpreted as an event in the sample space $\{0,1\}^{g(|x|)}$ with the uniform probability measure. (That is, the probability of $\mathcal{B}_x$ is $\Pr(\mathcal{B}_x) = 2^{-g(|x|)}|\mathcal{B}_x|$.)

3. Given a class $\mathcal{C}$ of languages, we define the class Promise-BP $\cdot\, \mathcal{C}$ to be the set of all ordered pairs $A = (A^+, A^-)$ of languages for which there is a witness configuration $\mathcal{B} = (B, q)$ with the following four properties.
   (i) $B \in \mathcal{C}$.
   (ii) q is a polynomial.
   (iii) For all $x \in A^+$, $\Pr(\mathcal{B}_x) \geq \frac{2}{3}$.
   (iv) For all $x \in A^-$, $\Pr(\mathcal{B}_x) \leq \frac{1}{3}$.

Note that Promise-BP is an operator that maps a class $\mathcal{C}$ of languages to a class Promise-BP $\cdot\, \mathcal{C}$ of disjoint pairs of languages. In particular,

$$\text{Promise-BP} \cdot \text{P} = \text{Promise-BPP}$$

is the class of *BPP promise problems* investigated by Buhrman and Fortnow [6] and Moser [24], and

$$\text{Promise-BP} \cdot \text{NP} = \text{Promise-AM}$$

is the class of *Arthur-Merlin promise problems* investigated by Moser [25].

The following result is the main theorem of this paper.

Theorem 3.1. *For every $S \in \mathbf{C}$ and $k \in \mathbb{N}$,*

$$\dim_{\Delta^{\text{P}}_{k+3}}(S) > 0 \implies \text{Promise-BP} \cdot \Sigma^{\text{P}}_k \subseteq \Sigma^{\text{P},S}_k\text{-Sep}.$$

Before proving Theorem 3.1, we derive some of its consequences. First, the cases $k = 0$ and $k = 1$ are of particular interest:

Corollary 3.2. *For every $S \in \mathbf{C}$,*

$$\dim_{\Delta^{\text{P}}_3}(S) > 0 \implies \text{Promise-BPP} \subseteq \text{P}^S\text{-Sep}$$

and

$$\dim_{\Delta^{\text{P}}_4}(S) > 0 \implies \text{Promise-AM} \subseteq \text{NP}^S\text{-Sep}.$$

We next note that our results for promise problems imply the corresponding results for decision problems. (Note, however, that the results of Fortnow [9] suggest that the results on promise problems are in some sense stronger.)

Corollary 3.3. *For every $S \in \mathbf{C}$ and $k \in \mathbb{N}$,*

$$\dim_{\Delta^{\mathrm{P}}_{k+3}}(S) > 0 \implies \mathrm{BP} \cdot \Sigma^{\mathrm{P}}_k \subseteq \Sigma^{\mathrm{P},S}_k.$$

In particular,

$$\dim_{\Delta^{\mathrm{P}}_3}(S) > 0 \implies \mathrm{BPP} \subseteq \mathrm{P}^S \tag{3.1}$$

and

$$\dim_{\Delta^{\mathrm{P}}_4}(S) > 0 \implies \mathrm{AM} \subseteq \mathrm{NP}^S. \tag{3.2}$$

Intuitively, (3.1) says that even an oracle S with Δ^{P}_3-dimension 0.001 – which need not be random relative to any reasonable distribution – "contains enough randomness" to carry out a deterministic simulation of BPP. To put the matter differently, to prove that P = BPP, we need "only" show how to dispense with such an oracle S.

As in section 1, for each relativizable complexity class $\mathcal{C}$ (of languages or pairs of languages), define the *dimension-almost-class*

$$\text{dimalmost-}\mathcal{C} = \left\{ A \mid \dim_{\mathrm{H}}(\left\{ S \mid A \notin \mathcal{C}^S \right\}) = 0 \right\},$$

noting that this is contained in the previously studied *almost-class*

$$\text{almost-}\mathcal{C} = \left\{ A \mid \Pr[A \in \mathcal{C}^S] = 1 \right\},$$

where the probability is computed according to the uniform distribution (Lebesgue measure) on the set of all oracles S.

Theorem 3.4. *For every $k \in \mathbb{N}$,*

$$\text{dimalmost-}\Sigma^{\mathrm{P}}_k\text{-Sep} = \text{almost-}\Sigma^{\mathrm{P}}_k\text{-Sep} = \text{Promise-BP} \cdot \Sigma^{\mathrm{P}}_k.$$

Nisan and Wigderson's unconditional pseudorandom generator for constant depth circuit is used in the proof for Theorem 3.4. We state it here.

Theorem 3.5 (Nisan and Wigderson [26]). *Let $d \in \mathbb{Z}^+$. There exists a function $G^{NW} : \{0,1\}^* \to \{0,1\}^*$ defined by a collection $\{G_n : \{0,1\}^{l_n} \to \{0,1\}^n\}$ such that $l_n = O((\log n)^{2d+6})$, G_n is computable by a logspace uniform family of circuits of polynomial size and depth $d+4$, and for any circuit family $\{C_n : \{0,1\}^n \to \{0,1\}\}$ of polynomial size and depth d,*

$$|\Pr[C_n(x) = 1] - \Pr[C_n(G_n(y))]| \leq 1/n.$$

Proof of Theorem 3.4. We only prove for $k > 0$, since when $k = 0$, the proof is easier. Since every set of Hausdorff dimension less than 1 has Lebesgue measure 0, it is clear that dimalmost-Σ^{P}_k-Sep $\subseteq$ almost-Σ^{P}_k-Sep.

To see that almost-Σ^{P}_k-Sep $\subseteq$ Promise-BP $\cdot\ \Sigma^{\mathrm{P}}_k$, we use Nisan and Wigderson's proof. Let $A = (A^+, A^-) \in$ almost-Σ^{P}_k-Sep. Then by the Lebesgue density theorem, there exists Σ^{P}_k oracle machine N' with time bound n^m such that

$$\Pr_R[N'^R \text{ separates A}] \geq 3/4.$$

Note that when input x is fixed and $|x| = n$, the computation of $N'(x)$ may be represented as a depth $k+2$ circuit of size $2^{(k+1)n^m}$ with $2^{(k+1)n^m}$ oracle queries as input. This is a linear size (with respect to oracle input length) depth $k+2$ circuit. We can use Theorem 3.5 to derandomize the exponential number of queries on random oracle to $n^{(2k+10)m}$ random oracle queries.

Let G^{NW} be the Nisan-Wigderson pseudorandom generator. Let $l_n = n^{(2k+10)m}$. Let N be the following oracle Turing machine.

```
input $x$
$n = |x|$
input $s \in \{0,1\}^{l_n}$
let $\tilde{R} = G^{NW}(s)$
simulates $N'^{\tilde{R}}(x)$
output the output of the simulation
```

For all $x \in A^+$, $\Pr_R[N'^R(x) = 1] \geq 3/4$. By the pseudorandomness of G^{NW}, then,

$$\Pr_{s \in \{0,1\}^{l_n}}[N'^{G^{NW}(s)}(x) = 1] \geq 2/3. \tag{3.3}$$

Similarly, for all $x \in A^-$,

$$\Pr_{s \in \{0,1\}^{l_n}}[N'^{G^{NW}(s)}(x) = 1] \leq 1/3. \tag{3.4}$$

Let

$$B = \{\langle x, s \rangle \mid N(\langle x, s \rangle) = 1\}.$$

It is clear that $B \in \Sigma_k^{\mathrm{P}}$. Also by (3.3), for all $x \in A^+$,

$$\Pr(B_x) \geq 2/3,$$

and, by (3.4), for all $x \in A^-$,

$$\Pr(B_x) \leq 1/3.$$

Then $(B, n^{(2k+10)m})$ is a witness configuration for A, hence $A \in \text{Promise-BP} \cdot \Sigma_k^{\mathrm{P}}$.

To see that $\text{Promise-BP} \cdot \Sigma_k^{\mathrm{P}} \subseteq \text{dimalmost-}\Sigma_k^{\mathrm{P}}\text{-Sep}$, let $A \in \text{Promise-BP} \cdot \Sigma_k^{\mathrm{P}}$. Let

$$X = \left\{ S \,\middle|\, A \notin \Sigma_k^{\mathrm{P}^S}\text{-Sep} \right\}.$$

By Theorem 3.1, every element of X has $\Delta_{k+3}^{\mathrm{p}}$-dimension 0. By (2.1), this implies that $\dim_{\mathrm{H}}(X) = 0$, whence $A \in \text{dimalmost-}\Sigma_k^{\mathrm{P}}\text{-Sep}$. □

Corollary 3.6. *For every $k \in \mathbb{N}$,*

$$\text{dimalmost-}\Sigma_k^{\mathrm{P}} = \mathrm{BP} \cdot \Sigma_k^{\mathrm{P}}.$$

In particular,

$$\text{dimalmost-P} = \mathrm{BPP} \tag{3.5}$$

and

$$\text{dimalmost-NP} = \mathrm{AM}. \tag{3.6}$$

We now turn to the proof of Theorem 3.1. We use the following well-known derandomization theorem.

Theorem 3.7 (Impagliazzo and Wigderson [16]). *For each $\epsilon > 0$, there exists constants $c' > c > 0$ such that, for every $A \subseteq \{0,1\}^*$ and integer $n > 1$, the following holds. If $f : \{0,1\}^{\lfloor c \log n \rfloor} \to \{0,1\}$ is a Boolean function that cannot be computed by an oracle circuit of size at most $n^{c\epsilon}$ relative to A,* *then the generator $G_f^{IW97} : \{0,1\}^{\lfloor c' \log n \rfloor} \to \{0,1\}^n$ has the property that, for every oracle circuit γ with size at most n,*

$$\left| \mathrm{Pr}_{r \in U_n}[\gamma^A(r) = 1] - \mathrm{Pr}_{x \in U_{\lfloor c' \log n \rfloor}}[\gamma^A(G_f^{IW97}(x)) = 1] \right| < \tfrac{1}{n},$$

where U_m denotes $\{0,1\}^m$ with the uniform probability measure.

Proof of Theorem 3.1. We prove the theorem for $k > 0$, since when $k = 0$, the proof is easier.

Assume that $\dim_{\Delta^p_{k+3}}(S) = \alpha > 0$. It suffices to show that for every $A \in$ Promise-BP $\cdot\, \Sigma_k^{\mathrm{P}}$, $A \in \Sigma_k^{\mathrm{P},S}$-Sep. Note that Promise-BP $\cdot\, \Sigma_k^{\mathrm{P}}$ does not have oracle access to S. So we actually prove $A \in \mathrm{NP}^{\Sigma_{k-1}^{\mathrm{P}},S}$-Sep.

By Theorem 2.4, we have $\mathrm{size}^{\Sigma_k^{\mathrm{P}}}(S[0..n-1]) > \frac{\alpha n}{2 \log n}$ for all but finitely many n.

Let $A = (A^+, A^-) \in$ Promise-BP $\cdot\, \Sigma_k^{\mathrm{P}}$. There exists $B \in \Sigma_k^{\mathrm{P}}$ and polynomial q such that (B, q) is a witness configuration for A. Therefore, there exists polynomial-time oracle Turing machine M and polynomial p such that, for all $x \in A^+$,

$$\Pr_r[(\exists w \in \{0,1\}^{p(|x|)}) M^{\Sigma_{k-1}^{\mathrm{P}}}(x, r, w) = 1] \geq 2/3$$

and, for all $x \in A^-$,

$$\Pr_r[(\exists w \in \{0,1\}^{p(|x|)}) M^{\Sigma_{k-1}^{\mathrm{P}}}(x, r, w) = 1] \leq 1/3.$$

Let n^d be the upper bound of the running time of M on x of length n with r and w of corresponding lengths.

Let $\epsilon = \alpha/2$ and let c', c be fixed in Theorem 3.7, and let $f : \{0,1\}^{\lfloor cd \log n \rfloor} \to \{0,1\}$ be (the Boolean function whose truth table is) given by the first $2^{\lfloor cd \log n \rfloor}$ bits of S.

By Theorem 3.7, G_f^{IW97} derandomizes linear size circuits with Σ_k^{P} oracle and linear size nondeterministic circuits with $\Sigma_{k-1}^{\mathrm{P}}$ oracle. Let $N^{\Sigma_{k-1}^{\mathrm{P}},S}$ be the following nondeterministic Turing machine with oracles $\Sigma_{k-1}^{\mathrm{P}}$ and S.

```
input $x$
$n = |x|$
guess $w_1, w_2, \ldots, w_{2^{\lfloor c'd \log n \rfloor}} \in \{0,1\}^{p(n)}$
query the first $2^{\lfloor cd \log n \rfloor}$ bits of $S$
Let $f : \{0,1\}^{\lfloor cd \log n \rfloor} \to \{0,1\}$ be given by the first $2^{\lfloor cd \log n \rfloor}$ bits of $S$
for each string $s_i \in \{0,1\}^{\lfloor c'd \log n \rfloor}$ do
    Let $r_i = G_f^{IW97}(s_i)$
end for
Let $r = 0$
for each $r_i$
    if $M^{\Sigma_{k-1}^{\mathrm{P}}}(x, r_i, w_i) = 1$ then $r = r + 1$
end for
if $\frac{r}{2^{\lfloor c'd \log n \rfloor}} \geq 1/2$ then output 1
else output 0.
```

By Theorem 3.7, for all $x \in A^+$, there exists a witness $\langle w_1, w_2, \ldots, w_{2^{\lfloor c'd \log n \rfloor}} \rangle$ such that $N^{\Sigma^{\mathrm{P}}_{k-1},S}(x) =$ 1, and, for all $x \in A^-$, such a witness does not exist. Therefore, the above $\mathrm{NP}^{\Sigma^{\mathrm{P}}_{k-1}}$ machine separates A with oracle S and hence $A \in \Sigma^{\mathrm{P},S}_{k}$-Sep. □

It should be noted that derandomization plays a significantly larger role in the proof of Corollary 3.6 than in the proofs of the analogous results for almost-classes. For example, the proof by Bennett and Gill [5] that almost-P = BPP uses the easily proven fact that the set $X = \left\{ S \mid \mathrm{P}^S \neq \mathrm{BPP}^S \right\}$ has Lebesgue measure 0. Hitchcock [13] has recently proven that this set has Hausdorff dimension 1, so the Bennett-Gill argument does not extend to a proof of (3.5). Instead, our proof of (3.5) relies, via (3.1), on Theorem 3.7 to prove that the set $Y = \left\{ S \mid \mathrm{BPP} \not\subseteq \mathrm{P}^S \right\}$ has Hausdorff dimension 0. Similarly, the proof by Nisan and Wigderson [26] that almost-NP ⊆ AM uses derandomization, but their proof that AM ⊆ almost-NP is elementary. In contrast, *both* directions of the proof of (3.6) use derandomization: The inclusion dimalmost-NP ⊆ AM relies on the fact that almost-NP ⊆ AM (hence on derandomization), and our proof that AM ⊆ dimalmost-NP relies, via (3.2), on Theorem 3.7.

4 Conclusion

We conclude with a brief remark on relativization. Theorem 3.7 relativizes to arbitrary oracles, as to all our arguments here. For example, implication (3.1),

$$\dim_{\Delta^{\mathrm{P}}_{3}}(S) > 0 \implies \mathrm{BPP} \subseteq \mathrm{P}^S,$$

holds relative to every oracle. Note, however, that, if we consider this implication relative to an oracle S of positive Δ^{p}_{3}-dimension, then the *relativized* Δ^{p}_{3}-dimension of this S will be 0, so we cannot use the relativized implication to conclude that $\mathrm{P}^S = \mathrm{BPP}^S$. Indeed, by Hitchcock's just-mentioned result and (2.1), there must exist languages S of positive Δ^{p}_{3}-dimension for which $\mathrm{P}^S \neq \mathrm{BPP}^S$.

Acknowledgment. We are grateful to Eric Allender, whose discussions of the ideas in [1, 2] were a significant motivation of our work. We thank an anonymous referee for pointing out a flaw in our earlier proof. We thank John Hitchcock for useful discussions and suggestions. We also thank Manindra Agrawal for a useful discussion.

References

[1] E. Allender. When worlds collide: Derandomization, lower bounds, and kolmogorov complexity. In *Proceedings of the 21st annual Conference on Foundations of Software Technology and Theoretical Computer Science*, volume 2245 of *Lecture Notes in Computer Science*, pages 1–15. Springer-Verlag, 2001.

[2] E. Allender, H. Buhrman, M. Koucký, D. van Melkebeek, and D. Ronneburger. Power from random strings. In *Proceedings of the 43rd Annual IEEE Symposium on Foundations of Computer Science*, pages 669–678, 2002. *SIAM Journal on Computing.* To appear.

[3] E. Allender and M. Strauss. Measure on small complexity classes with applications for BPP. In *Proceedings of the 35th Symposium on Foundations of Computer Science*, pages 807–818, 1994.

[4] J. L. Balcázar, J. Díaz, and J. Gabarró. *Structural Complexity I.* Springer-Verlag, Berlin, second edition, 1995.

[5] 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*, 10:96–113, 1981.

[6] H. Buhrman and L. Fortnow. One-sided versus two-sided randomness. In *Proceedings of the sixteenth Symposium on Theoretical Aspects of Computer Science*, pages 100–109, 1999.

[7] N. Chomsky and G. A. Miller. Finite state languages. *Information and Control*, 1(2):91–112, 1958.

[8] K. Falconer. *Fractal Geometry: Mathematical Foundations and Applications.* Wiley, second edition, 2003.

[9] L. Fortnow. Comparing notions of full derandomization. In *Proceedings of the 16th IEEE Conference on Computational Complexity*, pages 28–34, 2001.

[10] J. Grollman and A. Selman. Complexity measures for public-key cryptosystems. *SIAM J. Comput.*, 11:309–335, 1988.

[11] F. Hausdorff. Dimension und äusseres Mass. *Mathematische Annalen*, 79:157–179, 1919.

[12] J. M. Hitchcock. *Effective fractal dimension: foundations and applications.* PhD thesis, Iowa State University, 2003.

[13] J. M. Hitchcock. Hausdorff dimension and oracle constructions. *Theoretical Computer Science*, 355(3):382–388, 2006.

[14] J. M. Hitchcock, J. H. Lutz, and E. Mayordomo. The fractal geometry of complexity classes. *SIGACT News*, 36(3):24–38, 2005.

[15] J. M. Hitchcock and N. V. Vinodchandran. Dimension, entropy rates, and compression. In *Proceedings of the 19th IEEE Conference on Computational Complexity*, pages 174–183, 2004. *Journal of Computer and System Sciences*, to appear.

[16] R. Impagliazzo and A. Wigderson. P = BPP if E requires exponential circuits: Derandomizing the XOR lemma. In *Proceedings of the 29th Symposium on Theory of Computing*, pages 220–229, 1997.

[17] W. Kuich. On the entropy of context-free languages. *Information and Control*, 16(2):173–200, 1970.

[18] J. H. Lutz. A pseudorandom oracle characterization of BPP. *SIAM Journal on Computing*, 22(5):1075–1086, 1993.

[19] J. H. Lutz. Dimension in complexity classes. *SIAM Journal on Computing*, 32:1236–1259, 2003.

[20] J. H. Lutz. Effective fractal dimensions. *Mathematical Logic Quarterly*, 51:62–72, 2005.

[21] J. H. Lutz and W. J. Schmidt. Circuit size relative to pseudorandom oracles. *Theoretical Computer Science*, 107(1):95–120, March 1993.

[22] P. Martin-Löf. The definition of random sequences. *Information and Control*, 9:602–619, 1966.

[23] E. Mayordomo. Effective Hausdorff dimension. In *Proceedings of Foundations of the Formal Sciences III*, pages 171–186. Kluwer Academic Press, 2004.

[24] P. Moser. Relative to P promise-BPP equals APP. Technical Report TR01-68, Electronic Colloquium on Computational Complexity, 2001.

[25] P. Moser. Random nondeterministic real functions and Arthur Merlin games. Technical Report TR02-006, ECCC, 2002.

[26] N. Nisan and A. Wigderson. Hardness vs randomness. *Journal of Computer and System Sciences*, 49:149–167, 1994.

[27] L. Staiger. Kolmogorov complexity and Hausdorff dimension. *Information and Computation*, 103:159–94, 1993.

[28] L. Staiger. A tight upper bound on Kolmogorov complexity and uniformly optimal prediction. *Theory of Computing Systems*, 31:215–29, 1998.

[29] C. B. Wilson. Relativized circuit complexity. *Journal of Computer and System Sciences*, 31:169–181, 1985.