Dimension Characterizations of Complexity Classes

Xiaoyang Gu †‡ Jack H. Lutz †‡

Abstract

We use derandomization to show that sequences of positive p-space-dimension — in fact, even
positive $\Delta^p_k$-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 $\Delta^p_3$-dimension is positive, then
BPP $\subseteq$ 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 $C$, denoted by dimalmost-$C$, is the class
consisting of all problems $A$ such that $A \in C^S$ 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 challenge, as are structural questions concerning BPP, AM, and other randomized complexity classes.

One approach to studying the power of a randomized complexity class $C$ is to address the
following question: If $C_0$ is the nonrandomized version of $C$, then how weak an assumption can we
place on an oracle $S$ and still be assured that $C \subseteq C_0^S$? For example, how weak an assumption can
we place on an oracle $S$ and still be assured that BPP $\subseteq$ P$^S$? For this particular question, it was
a result of folklore that BPP $\subseteq$ 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 BPP $\subseteq$ P$^S$ holds for every oracle $S$ that
is p-space-random; and it was shown by Allender and Strauss [3] that BPP $\subseteq$ 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 $\Delta^p_3$-dimension (hence
every oracle $S$ that has positive p-space-dimension) satisfies BPP $\subseteq$ 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 $\Delta^p_{k+3}$-dimension, every $\text{BP} \cdot \Sigma^p_k$ promise problem is $\Sigma^p_k \cdot S$-separable. In particular, if $S$ has positive $\Delta^p_0$-dimension, then every $\text{BPP}$ promise problem is $\text{P}^S$-separable, and, if $S$ has positive $\Delta^p_1$-dimension, then every $\text{AM}$ promise problem is $\text{NP}^S$-separable.

We use our results to investigate classes of the form
\[ \text{dimalmost-C} = \{ A \mid \dim_H(\{ B \mid A \notin C^B \}) = 0 \} \]
for various complexity classes $C$. It is clear that dimalmost-$C$ is contained in the extensively investigated class
\[ \text{almost-C} = \{ A \mid \Pr[A \notin C^B] = 0 \} , \]
where the probability is computed according to the uniform distribution (Lebesgue measure) on the set of all oracles $B$. We show that
\[ \text{dimalmost-} \Sigma^p_k \cdot \text{Sep} = \text{almost-} \Sigma^p_k \cdot \text{Sep} = \text{Promise-BP} \cdot \Sigma^p_k \]
holds for every integer $k \geq 0$, where $\Sigma^p_k \cdot \text{Sep}$ is the set of all $\Sigma^p_k$-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 $k \geq 1$,
\[ \text{dimalmost-} \Sigma^p_k = \text{BP} \cdot \Sigma^p_k , \]
refining the proof by Nisan and Wigderson [26] that almost-$\Sigma^p_k = \text{BP} \cdot \Sigma^p_k$.

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

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

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 \(X \subseteq \mathcal{C}\) is

\[
\dim_H(X) = \inf \{s \mid \text{there is an } s\text{-gale } d \text{ such that } X \subseteq S^\infty[d]\}.
\]

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

- \(\text{all} = \{f \mid f : \{0, 1\}^* \to \{0, 1\}^*\}\)
- \(p = \{f \in \text{all} \mid f \text{ is computable in } n^{O(1)} \text{ time}\}\)
- \(\Delta_k^p = p^{\Sigma_k^p} \text{ for } k \geq 2\)
- \(\text{pspace} = \{f \in \text{all} \mid f \text{ is computable in } n^{O(1)} \text{ space}\}\)

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

\[
R(\text{all}) = \mathcal{C}
\]
\[
R(p) = E = \text{TIME}(2^{\text{linear}})
\]
\[
R(\Delta_k^p) = \Delta_k^E = \Sigma_k^{p^E}
\]
\[
R(\text{pspace}) = \text{ESPACE} = \text{SPACE}(2^{\text{linear}})
\]

A real-valued function \(f : \{0, 1\}^* \to [0, \infty)\) is \(\Delta\)-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 \(\Delta\) be a resource bound, and let \(X \subseteq \mathcal{C}\). (We identify each \(S \in X\) with the language whose characteristic sequence is \(S\).)

1. The \(\Delta\)-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 \(\dim_{R(\Delta)}(X) = \dim_{\Delta}(X \cap R(\Delta))\).

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

\[
0 \leq \dim_{R(\Delta)}(X) \leq \dim_{\Delta}(X) \leq 1,
\]

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

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

e.g., \(\dim_{\text{pspace}}(X) \leq \dim_{\Delta_k^p}(X)\). It is clear that \(\dim_{\text{all}}(X) = \dim(X|\mathcal{C}) = \dim_H(X)\).
Our main results involve $\Delta$-dimensions of individual sequences $S$, by which we mean
\[ \dim_{\Delta}(S) = \dim_{\Delta}([S]). \]
We use the easily verified fact that, if $\Delta$ is any of the countable resource bounds above, then
\[ \dim_{H}([S \mid \dim_{\Delta}(S) = 0]) = 0. \]
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 $C$ be a class of languages, and let $X \subseteq C$. The *$C$-entropy rate* of $X$ is
\[ H_C(X) = \inf \{ H_A \mid A \in C \text{ and } X \subseteq A^{i.o.} \}, \]
where
\[ A^{i.o.} = \{ S \in C \mid (\exists \infty n)S[0..n - 1] \in A \}. \]
The following result is a routine relativization of Theorem 5.5 of [15].

**Theorem 2.2.** *(Hitchcock and Vinodchandran [15]).* For all $X \subseteq C$ and $k \in \mathbb{Z}^+$,
\[ \dim_{\Delta_{k+2}}(X) \leq H_{\Sigma^P_k}(X). \]

2.3 Relativized Circuit-Size Complexity

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

1. For $x \in \{0, 1\}^*$ and $A \subseteq \{0, 1\}^*$, size$_A^f(x) = \text{size}_A^f(f_x)$, where $f_x : \{0, 1\}^{\lfloor \log |x| \rfloor} \to \{0, 1\}$ is defined by
\[ f_x(w_i) = \begin{cases} x[i] & \text{if } 0 \leq i < |x| \\ 0 & \text{if } i \geq |x|, \end{cases} \]
for $w_0, \ldots, w_{\lfloor \log |x| \rfloor - 1}$ lexicographically enumerate $\{0, 1\}^{\lfloor \log |x| \rfloor}$, and $x[i]$ is the $i$th bit of $x$.

2. For $x \in \{0, 1\}^*$ and $A \subseteq \{0, 1\}^*$, size$_A^f(x) = \text{size}_A^f(f_x)$, where $f_x : \{0, 1\}^{\lfloor \log |x| \rfloor} \to \{0, 1\}$ is defined by
\[ f_x(w_i) = \begin{cases} x[i] & \text{if } 0 \leq i < |x| \\ 0 & \text{if } i \geq |x|, \end{cases} \]
for $w_0, \ldots, w_{\lfloor \log |x| \rfloor - 1}$ lexicographically enumerate $\{0, 1\}^{\lfloor \log |x| \rfloor}$, and $x[i]$ is the $i$th bit of $x$.

**Lemma 2.3.** For all $A, S \in C$,
\[ H_{\Sigma^P_n}(\{S\}) \leq \liminf_{n \to \infty} \frac{\text{size}_A^f(S[0..n - 1]) \log n}{n}. \]
Proof. Assume that
\[ \alpha > \beta > \liminf_{n \to \infty} \frac{\text{size}^A(S[0..n-1]) \log n}{n} . \]
It suffices to show that \( \mathcal{H}_{\text{NP}^A}(\{S\}) \leq \alpha \).

Let \( B \) be the set of all strings \( x \) such that \( \text{size}^A(x) < \beta \frac{|x|}{\log |x|} \). 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
\[ \beta \frac{n}{\log n} = \beta \frac{2^m}{\log(2^m)} \leq \beta \gamma \frac{2^m}{m-1} , \]
then
\[ |B_{=n}| \leq c \left( 4e\beta \gamma \frac{2^m}{m-1} \right)^{\beta \gamma \frac{2^m}{m-1}} , \]
so
\[ \log |B_{=n}| \leq \log c + \beta \gamma \frac{2^m}{m-1} \log \left( 4e\beta \gamma \frac{2^m}{m-1} \right) \]
\[ = \log c + \beta \gamma 2^m \left[ \frac{m}{m-1} + \frac{\log 4e\beta \gamma - \log(m-1)}{m-1} \right] \]
\[ \leq \alpha n , \]
whence
\[ H_B = \limsup_{n \to \infty} \frac{\log |B_{=n}|}{n} \leq \alpha . \]
By our choice of \( \beta, S \in B^{i.o.} \). Since \( B \in \text{NP}^A \), it follows that \( \mathcal{H}_{\text{NP}}(\{S\}) \leq \alpha \).

Notation. For \( k \in \mathbb{N} \) and \( x \in \{0,1\}^* \), we write
\[ \text{size}^{\Sigma_k^P}(x) = \text{size}^{K_k}(x) , \]
where \( K_k \) is the canonical \( \Sigma_k^P \)-complete language [4].

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

Theorem 2.4. For all \( S \in \mathcal{C} \) and \( k \in \mathbb{N} \),
\[ \dim_{\Delta_{k+3}}(S) \leq \liminf_{n \to \infty} \frac{\text{size}_{\Sigma_k^P}(S[0..n-1])}{n} \]

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 \( C \) of languages, an ordered pair \( A = (A^+, A^-) \) of (disjoint) languages is \( C \)-separable if there exists a language \( C \in C \) such that \( A^+ \subseteq C \) and \( A^- \cap C = \varnothing \). We write
\[ C\text{-Sep} = \{(A^+, A^-) \mid (A^+, A^-) \text{ is } C \text{-separable}\} . \]
**Definition.** Fix a standard paring function $\langle , \rangle : \{0, 1\}^* \times \{0, 1\}^* \rightarrow \{0, 1\}^*$.

1. A *witness configuration* is an ordered pair $B = (B, g)$ where $B \subseteq \{0, 1\}^*$ and $g : \mathbb{N} \rightarrow \mathbb{N}$.

2. Given a witness configuration $B = (B, g)$, the $B$-critical event for a string $x \in \{0, 1\}^*$ is the set
   \[
   B_x = \left\{ w \in \{0, 1\}^{g(|x|)} | \langle x, w \rangle \in B \right\},
   \]
   interpreted as an event in the sample space $\{0, 1\}^{g(|x|)}$ with the uniform probability measure.
   (That is, the probability of $B_x$ is $\Pr(B_x) = 2^{-g(|x|)|B_x|}$.)

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 $B = (B, q)$ with the following four properties.
   (i) $B \in \mathcal{C}$.
   (ii) $q$ is a polynomial.
   (iii) For all $x \in A^+$, $\Pr(B_x) \geq \frac{2}{3}$.
   (iv) For all $x \in A^-$, $\Pr(B_x) \leq \frac{1}{3}$.

   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,
   
   \[
   \text{Promise-BP} \cdot \mathcal{P} = \text{Promise-BPP}
   \]
   is the class of *BPP promise problems* investigated by Buhrman and Fortnow [6] and Moser [24], and
   
   \[
   \text{Promise-BP} \cdot \mathcal{NP} = \text{Promise-AM}
   \]
   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 $S \in \mathcal{C}$ and $k \in \mathbb{Z}^+$,
\[
\dim_{\Sigma_k}^{\Delta_{k+3}}(S) > 0 \implies \text{Promise-BP} \cdot \Sigma_k^P \subseteq \Sigma_k^{\Delta_k^P,S} - \text{Sep}.
\]

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 $S \in \mathcal{C}$,
\[
\dim_{\Delta_0^P}(S) > 0 \implies \text{Promise-BPP} \subseteq \text{P}^S - \text{Sep}
\]
and
\[
\dim_{\Delta_1^P}(S) > 0 \implies \text{Promise-AM} \subseteq \text{NP}^S - \text{Sep}.
\]

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 $S \in C$ and $k \in \mathbb{N}$,
\[
\dim_{\Delta_{k+4}^p}(S) > 0 \implies \text{BP} \cdot \Sigma_k^p \subseteq \Sigma_k^{p,S}.
\]
In particular,
\[
\dim_{\Delta_k^p}(S) > 0 \implies \text{BPP} \subseteq P^S
\] (3.1)
and
\[
\dim_{\Delta_4^p}(S) > 0 \implies \text{AM} \subseteq \text{NP}^S.
\] (3.2)

Intuitively, (3.1) says that even an oracle $S$ with $\Delta_{3/4}^p$-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 $\text{P} = \text{BPP}$, we need “only” show how to dispense with such an oracle $S$.

As in section 1, for each relativizable complexity class $C$ (of languages or pairs of languages), define the dimension-almost-class
\[
\dim_{\text{almost}-C} = \{ A \mid \dim_H(\{ S \mid A \notin C^S \}) = 0 \},
\]
noting that this is contained in the previously studied almost-class
\[
\text{almost}-C = \{ A \mid \Pr[A \in C^S] = 1 \},
\]
where the probability is computed according to the uniform distribution (Lebesgue measure) on the set of all oracles $S$.

Theorem 3.4. For every $k \in \mathbb{N}$,
\[
\dim_{\text{almost}-\Sigma_k^p}-\text{Sep} = \text{almost}-\Sigma_k^p-\text{Sep} = \text{Promise-BP} \cdot \Sigma_k^p.
\]

Proof. Since every set of Hausdorff dimension less than 1 has Lebesgue measure 0, it is clear that $\dim_{\text{almost}-\Sigma_k^p}-\text{Sep} \subseteq \text{almost}-\Sigma_k^p-\text{Sep}$.

To see that $\dim_{\text{almost}-\Sigma_k^p}-\text{Sep} \subseteq \text{Promise-BP} \cdot \Sigma_k^p$, let $A = (A^+, A^-) \in \text{almost}-\Sigma_k^p-\text{Sep}$. Then by the Lebesgue density theorem, there exists a deterministic polynomial-time oracle Turing machine $M$ and polynomial $p$ such that
\[
\Pr_R[\exists^{\Sigma_k^p} M_{\Sigma_{k-1}^p}^R \text{ separates } A] \geq 3/4,
\]
where $\exists^p$ means that the Turing machine can make $p(n)$ nondeterministic moves with input of length $n$. Let $n^k$ be the time bound of $M$. Let $G^{NW}$ be the Nisan-Wigderson pseudorandom generator. Let $N$ be the following Turing machine with $\Sigma_{k-1}^p$ oracle.

```
input x
n = |x|
input s \in \{0, 1\}^{2n \cdot 10^k}
input w \in \{0, 1\}^{n^k}
let r = G^{NW}(s)
simulates M_{\Sigma_{k-1}^p}^R((x, w))
output the output of the simulation
```
Note that each bit of \( r \) may be computed in polynomial time and \( M^{\Sigma^P_{k-1}}_{n^k}(x) \) makes at most \( n^k \) queries, therefore the above oracle Turing machine runs in polynomial time.

For all \( x \in A^+ \), \( \Pr_R[\exists y \in \{0,1\}^{p(|x|)}M^{\Sigma^P_{k-1}}_{n^k}(\langle x, y \rangle) = 1] \geq 3/4 \). By the pseudorandomness of \( G^{NW} \),

\[
\Pr_{s \in \{0,1\}^{2n^{10k}}}[(\exists y \in \{0,1\}^{p(|x|)}M^{\Sigma^P_{k-1}}_{n^k}G^{NW}(s)(\langle x, y \rangle) = 1) \geq 2/3. \tag{3.3}
\]

Similarly, for all \( x \in A^- \),

\[
\Pr_{s \in \{0,1\}^{2n^{10k}}}[(\exists y \in \{0,1\}^{p(|x|)}M^{\Sigma^P_{k-1}}_{n^k}G^{NW}(s)(\langle x, y \rangle) = 1] \leq 1/3. \tag{3.4}
\]

Let

\[
B = \left\{ < x, s > \mid (\exists y \in \{0,1\}^{3n^k})N(\langle x, s, y \rangle) = 1 \right\}.
\]

It is clear that \( B \in \text{NP}^{\Sigma^P_{k-1}} = \Sigma^P_k \).

Then 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 \((B, 2n^{10k})\) is a witness configuration for \( A \), hence \( A \in \text{Promise-BP} \cdot \Sigma^P_k \).

To see that \( \text{Promise-BP} \cdot \Sigma^P_k \subseteq \text{dimalmost-} \Sigma^P_k \text{-Sep} \), let \( A \in \text{Promise-BP} \cdot \Sigma^P_k \). Let

\[
X = \left\{ S \mid A \not\subseteq \Sigma^P_k \text{-Sep} \right\}.
\]

By Theorem 3.1, every element of \( X \) has \( \Delta^P_{k+3} \)-dimension 0. As noted in section 2.1, this implies that \( \text{dim}_H(X) = 0 \), whence \( A \in \text{dimalmost-} \Sigma^P_k \text{-Sep} \).

\[ \square \]

**Corollary 3.5.** For every \( k \in \mathbb{N} \),

\[ \text{dimalmost-} \Sigma^P_k = \text{BP} \cdot \Sigma^P_k. \]

In particular,

\[ \text{dimalmost-} \text{P} = \text{BPP} \tag{3.5} \]

and

\[ \text{dimalmost-} \text{NP} = \text{AM}. \tag{3.6} \]

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

**Theorem 3.6** (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 \( f : \{0,1\}^{[c \log n]} \to \{0,1\} \) 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 \( G^I_{f} : \{0,1\}^{[c' \log n]} \to \{0,1\}^n \) has the property that, for every oracle circuit \( \gamma \) with size at most \( n \),

\[
\left| \Pr_{r \in U_n}[\gamma^A(r) = 1] - \Pr_{x \in U_{[c' \log n]}}[\gamma^A(G^I_{f}(x)) = 1] \right| < \frac{1}{n},
\]

where \( U_m \) denotes \( \{0,1\}^m \) with the uniform probability measure.
Proof of Theorem 3.1. Assume that $\dim_{\Delta^p_{k+3}}(S) = \alpha >0$. It suffices to show that for every $A \in \text{Promise-BP} \cdot \Sigma^p_k, A \in \Sigma^p_k$-Sep.

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

Let $A = (A^+, A^-) \in \text{Promise-BP} \cdot \Sigma^p_k$. There exists $B \in \Sigma^p_k$ 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

$$\forall x \in A^+, \Pr_r[(\exists w \in \{0,1\}^{p(|x|)})M^{\Sigma^p_k-1}(x, r, w) = 1] \geq 2/3$$

and

$$\forall x \in A^+, \Pr_r[(\exists w \in \{0,1\}^{p(|x|)})M^{\Sigma^p_k-1}(x, r, w) = 1] \leq 1/3.$$ 

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 3.6.

Let $f : \{0,1\}^{2\lfloor \log n \rfloor} \rightarrow \{0,1\}$ be given by the first $2^{\lfloor \log n \rfloor}$ bits of $S$.

By Theorem 3.6, $G_f^{IW97}$ derandomizes linear size circuits with $\Sigma^p_k$ oracle and linear size nondeterministic circuits with $\Sigma^p_{k-1}$ oracle.

Let $N^{\Sigma^p_{k-1},S}$ be the following nondeterministic Turing machine with oracles $\Sigma^p_{k-1}$ and $S$:

```
input x
n = |x|

guess $w_1, w_2, \ldots, w_{2^{[c'd \log n]}} \in \{0,1\}^{p(n)}$

query the first $2^{[c'd \log n]}$ bits of $S$

for each string $s_i \in \{0,1\}^{[c'd \log n]}$ do
    Let $r_i = G_f^{IW97}(s_i)$
end for

Let $r = 0$
for each $r_i$
    if $M^{\Sigma^p_{k-1}}(x, r_i, w_i) = 1$ then $r = r + 1$
end for
if $\frac{r}{2^{[c'd \log n]}} \geq 1/2$ then output 1
else output 0.
```

By Theorem 3.6, for all $x \in A^+$, there exists witness $(w_1, w_2, \ldots, w_{2^{[c'd \log n]}})$ such that $N^{\Sigma^p_{k-1},S}(x) = 1$ and for all $x \in A^-$, such witness does not exist.

Therefore, the above NP$_{\Sigma^p_{k-1}}$ machine separates $A$ with oracle $S$ and hence $A \in \Sigma^p_k$-Sep.

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

**Acknowledgment.** We are grateful to Eric Allender, whose discussions of the ideas in [1, 2] were a significant motivation of our work. The first author also thanks John Hitchcock for useful discussions and suggestions.

**References**


