Observations on Measure and Lowness for Δ_2^{P} *

Jack H. Lutz
Department of Computer Science
Iowa State University
Ames, IA 50011

Abstract

Assuming that $k \geq 2$ and Δ_k^P does not have p-measure 0, it is shown that $\mathrm{BP} \cdot \Delta_k^{\mathrm{P}} = \Delta_k^{\mathrm{P}}$. This implies that the following conditions hold if Δ_2^{P} does not have p-measure 0.

(i) $\mathrm{AM} \cap \text{co-AM}$ is low for Δ_2^{P}. (Thus BPP and the graph isomorphism problem are low for Δ_2^{P}.)

(ii) If $\Delta_2^{\mathrm{P}} \neq \mathrm{PH}$, then NP does not have polynomial-size circuits.

*This research was supported in part by National Science Foundation Grant CCR-9157382, with matching funds from Rockwell International, Microware Systems Corporation, and Amoco Foundation.

1 Introduction

Many widely believed conjectures in computational complexity are "strong" in the sense that they are known to imply that $\mathrm{P} \neq \mathrm{NP}$, but are not known to follow from the $\mathrm{P} \neq \mathrm{NP}$ hypothesis. Recent investigations have shown that a number of these conjectures do follow from the (apparently) stronger hypothesis that NP does not have p-measure 0. (This hypothesis, written $\mu_{\mathrm{p}}(\mathrm{NP}) \neq 0$, is defined in terms of resource-bounded measure, a theory developed in [18] and discussed briefly in section 2 below. Intuitively, $\mu_{\mathrm{p}}(\mathrm{NP}) \neq 0$ holds if NP contains a non-negligible subset of the exponential time class $\mathrm{E}_2 = \mathrm{DTIME}(2^{\mathrm{polynomial}})$ – the smallest deterministic time complexity class known to contain NP.) For example, if $\mu_{\mathrm{p}}(\mathrm{NP}) \neq 0$, it is now known that NP contains P-bi-immune languages [25]; there is an NP search problem that is not efficiently reducible to the corresponding decision problem [3, 23]; every $\leq^{\mathrm{P}}_{n^\alpha-\mathrm{tt}}$-complete problem for NP $(\alpha < 1)$ is exponentially dense [22]; every $\leq^{\mathrm{P}}_{\mathrm{m}}$-complete problem for NP has an exponentially dense exponential complexity core [6]; and there are problems that are $\leq^{\mathrm{P}}_{\mathrm{T}}$-complete, but not $\leq^{\mathrm{P}}_{\mathrm{m}}$-complete, for NP [23]. These conclusions, which are not known to follow from $\mathrm{P} \neq \mathrm{NP}$ or other "traditional" complexity-theoretic hypotheses (e.g., the separation of the polynomial-time hierarchy), suggest that $\mu_{\mathrm{p}}(\mathrm{NP}) \neq 0$ is a plausible scientific hypothesis with substantial explanatory power. (See [22, 6, 20] for further discussion of this hypothesis.)

This paper shows that the hypothesis $\mu_{\mathrm{p}}(\mathrm{NP}) \neq 0$ also has consequences involving the complexity classes $\mathrm{BP} \cdot \Delta^{\mathrm{P}}_k$ $(k \geq 2)$ and lowness for Δ^{P}_2. In fact, these consequences all follow from the hypothesis that the class Δ^{P}_2 does not have p-measure 0. Since $\mathrm{NP} \subseteq \Delta^{\mathrm{P}}_2$, the hypothesis $\mu_{\mathrm{p}}(\Delta^{\mathrm{P}}_2) \neq 0$ follows from, and is thus at least as plausible as, the hypothesis $\mu_{\mathrm{p}}(\mathrm{NP}) \neq 0$.

Section 3 contains the main observation of this paper, which concerns the effect of the BP-operator on the classes Δ^{P}_k $(k \geq 2)$ of the polynomial-time hierarchy. The BP-operator, introduced by Schöning [31] and discussed in section 2 below, assigns to each complexity class $\mathcal{C}$ a complexity class $\mathrm{BP} \cdot \mathcal{C}$, which can be regarded as a "feasibly randomized version" of $\mathcal{C}$. Two important special-case values of this operator are the bounded-error probabilistic polynomial-time class $\mathrm{BPP} = \mathrm{BP} \cdot \mathrm{P}$ and the Arthur-Merlin class $\mathrm{AM} = \mathrm{BP} \cdot \mathrm{NP}$. Generalizing the proofs by Lautemann [15] and Sipser and Gács [32] that $\mathrm{BPP} \subseteq \Sigma^{\mathrm{P}}_2 \cap \Pi^{\mathrm{P}}_2$, Schöning [31] showed that, for all $k \geq 1$, $\mathrm{BP} \cdot \Sigma^{\mathrm{P}}_k \subseteq \Pi^{\mathrm{P}}_{k+1}$. This result, in combination with more elementary facts, established the inclusion structure depicted in Figure 1.

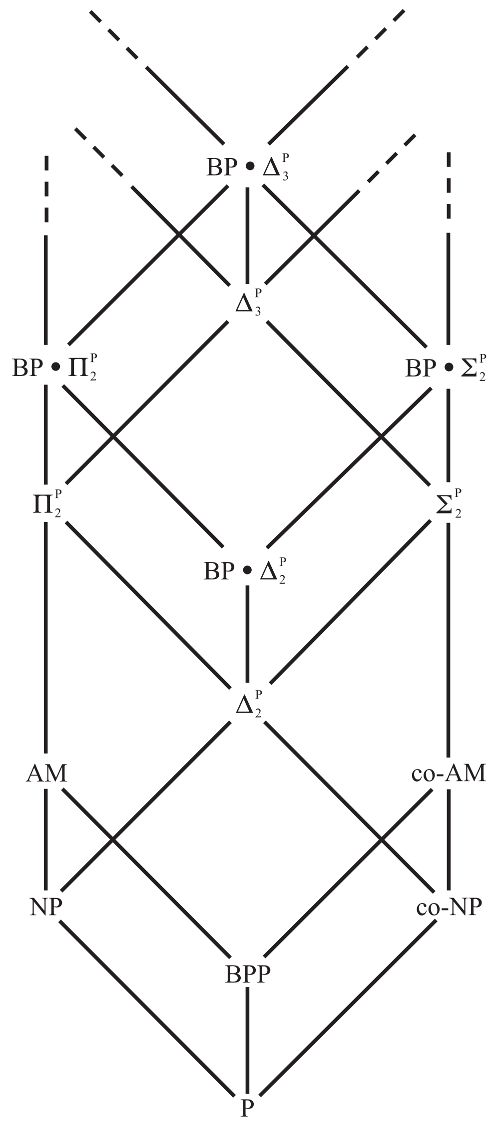

Figure 1: Known inclusion structure

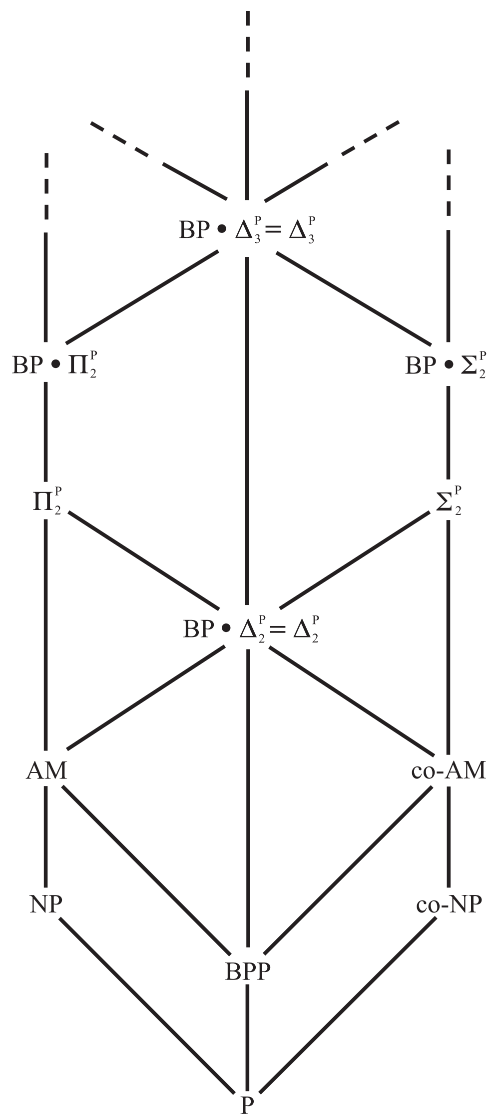

Figure 2: Inclusion structure if $\mu_{\rm P}(\Delta_2^{\rm P}) \neq 0$

The hypothesis $\mu_{\rm p}(\Delta_2^{\rm P}) \neq 0$ simplifies this inclusion structure. Specifically, Theorem 3.3 below shows that, if some class $\Delta_j^{\rm P}$ does not have p-measure 0, then the classes $\Delta_j^{\rm P}, \Delta_{j+1}^{\rm P}, \ldots$ are all fixed points of the BP-operator. That is, if $\mu_{\rm P}(\Delta_j^{\rm P}) \neq 0$, then for all $k \geq j$, $\mathrm{BP} \cdot \Delta_k^{\rm P} = \Delta_k^{\rm P}$. In particular, if $\mu_{\rm p}(\Delta_2^{\rm P}) \neq 0$, then the situation depicted in Figure 2 holds. Intuitively, Theorem 3.3 says that, if $\Delta_2^{\rm P}$ does not have p-measure 0, then it contains a language that is sufficiently random to simmulate a BP-operator. The proof makes essential use of the construction by Nisan and Wigderson [27] of secure pseudorandom generators from languages that are hard to approximate by circuits.

The remaining observations of this paper, presented in sections 4 and 5, involve lowness for $\Delta_2^{\rm P}$ and follow easily from Theorem 3.3 and recent results in computational complexity.

The concept of lowness originated in recursion theory and was introduced to complexity theory by Schöning [29]. A language $A \subseteq \{0,1\}^*$ is *low* for a relativizable complexity class $\mathcal{C}$ if $\mathcal{C}(A) = \mathcal{C}$, i.e., if oracle access to A does not increase the computational power of $\mathcal{C}$. A class $\mathcal{L}$ of languages is then *low* for $\mathcal{C}$ if $\mathcal{C}(\mathcal{L}) = \mathcal{C}$, i.e., if every element of $\mathcal{L}$ is low for $\mathcal{C}$. Köbler [12] has recently provided a useful survey of lowness results in complexity theory.

Section 4 concerns the lowness of probabilistic complexity classes. Zachos and Heller [36] proved that BPP is low for $\Sigma_2^{\rm P}$. Schöning [30] improved this by showing that $\mathrm{NP} \cap \text{co-AM}$ is low for $\Sigma_2^{\rm P}$, whence the graph isomorphism problem is low for $\Sigma_2^{\rm P}$. Klapper [9] strengthed this by establishing that all of $\mathrm{AM} \cap \text{co-AM}$ is low for $\Sigma_2^{\rm P}$. More recently, Köbler, Schöning, and Torán [13] showed that $\mathrm{AM} \cap \text{co-AM}$ is, in fact, low for AM. Theorem 4.2 below notes that, under the hypothesis $\mu_{\rm p}(\Delta_2^{\rm P}) \neq 0$, $\mathrm{AM} \cap \text{co-AM}$ is also low for $\Delta_2^{\rm P}$. Thus if $\mu_{\rm p}(\Delta_2^{\rm P}) \neq 0$ and the polynomial-time hierarchy does not collapse to $\Delta_2^{\rm P}$, then the graph isomorphism problem is not $\leq_{\rm m}^{\rm P}$-complete, $\leq_{\rm T}^{\rm P}$-complete, or $\leq_{\rm T}^{\rm SNP}$-complete for NP.

Section 5 concerns the lowness of self-reducible languages with polynomial-size circuits. Karp and Lipton [8] used self-reducibility to show that, if the polynomial hierarchy does not collapse to $\Sigma_2^{\rm P}$, then $\mathrm{NP} \not\subseteq \mathrm{P/Poly}$, i.e., NP does not have polynomial-size circuits. Ko and Schöning [11] refined this by showing that every language in NP that has polynomial-size circuits is low for $\Sigma_2^{\rm P}$. Very recently, Köbler and Watanabe [14] have significantly improved upon these results by showing that every self-reducible language with polynomial-size circuits – in fact, every self-reducible language in $(\mathrm{NP} \cap \text{co-NP})/\mathrm{Poly}$ – is low for ZPP(NP). Thus, if the polynomial-time hierarchy does not collapse to ZPP(NP), then NP does not have polynomial-size circuits. In Theorem 5.3 (which follows immediately from Theorem 3.3 and the result of Köbler and Watanabe), it is noted that, if $\mu_{\rm p}(\Delta_2^{\rm P}) \neq 0$, then every self-reducible language in (NP $\cap$ co-NP)/Poly is low for $\Delta_2^{\rm P}$. Thus, if $\mu_{\rm p}(\Delta_2^{\rm P}) \neq 0$ and polynomial-time hierarchy does not collapse to $\Delta_2^{\rm P}$, then NP does not have polynomial-size circuits.

2 Preliminaries

The reader is referred to any of the texts [2, 4, 13, 28] for basic material on complexity classes, relativized complexity classes, the polynomial-time hierarchy, feasible reductions, self-reducibility, polynomial advice, and (Boolean) circuits. Oracle circuits are described in [34, 24]. For each $k \geq 1$, QBF_k is the well-known *k-quantified Boolean formula* problem. Stockmeyer [33] and Wrathall [35] have shown that QBF_k is $\leq_{\rm m}^{\rm P}$-complete for $\Sigma_k^{\rm P}$, and it is clear that $QBF_k \in {\rm E}$, where ${\rm E} = {\rm DTIME}(2^{\rm linear})$. Other specific terminology and notation used here include the following.

For languages $A, B \subseteq \{0,1\}^*$, the *symmetric difference* of A and B is

$$A \bigtriangleup B = (A - B) \cup (B - A),$$

and the *tagged union* of A and B is

$$A \oplus B = \left\{ x0 \;\middle|\; x \in A \right\} \cup \left\{ x1 \;\middle|\; x \in B \right\}.$$

Using the *standard enumeration*

$$s_0 = \lambda, s_1 = 0, s_2 = 1, s_3 = 00, s_4 = 01, \ldots$$

of $\{0,1\}^*$, each language $A \subseteq \{0,1\}^*$ is identified with its *characteristic sequence* $\chi_A \in \{0,1\}^\infty$, whose ith bit ($i \geq 0$) is $\chi_A[i] =$ if $s_i \in A$ then 1 else 0. The *cylinder generated by* a string $w \in \{0,1\}^*$ is the set

$$\mathbf{C}_w = \left\{ A \subseteq \{0,1\}^* \;\middle|\; \chi_A[0..|w|-1] = w \right\}$$

where $\chi_A[0..l-1]$ is the string consisting of the first l bits of χ_A.

Resource-bounded measure was introduced in [18]. Introductions to this subject may be found in the papers [16, 22, 7, 6, 23, 21, 20], and in the theses

[26, 5]. For the purpose of this note, it suffices to indicate the intuition and cite a result that is used in the proof of Lemma 3.2.

Intuitively, a set X of languages has *p-measure* 0 (polynomial-time measure 0) if the following two conditions hold.

(i) If a language $A \subseteq \{0,1\}^*$ is chosen probabilistically according to a random experiment in which an independent toss of a fair coin is used to decide membership of each string in A, then the probability is 0 that $A \in X$.

(ii) Condition (i) holds in a manner that can be computationally verified in polynomial time.

If a set X has p-measure 0, then $X \cap \mathrm{E}$ is, in a precise sense, a *negligibly small* subset of E [18].

More formally, a *supermartingale* is a function $d : \{0,1\}^* \to [0,\infty)$ such that, for all $w \in \{0,1\}^*$,

$$d(w) \geq \frac{d(w0) + d(w1)}{2}.$$

If d is a supermartingale, then the *success set* of d is

$$S^\infty[d] = \left\{ A \;\middle|\; \limsup_{l\to\infty} d(\chi_A[0..l-1]) = \infty \right\},$$

and the *unitary success set* of d is

$$S^1[d] = \bigcup_{d(w)\geq 1} \mathbf{C}_w = \left\{ A \;\middle|\; (\exists l \in \mathbb{N}) d(\chi_A[0..l-1]) \geq 1 \right\}.$$

For any $i \geq 0$, a real-valued function $f : \mathbb{N}^i \times \{0,1\}^* \to \mathbb{R}$ is p-*computable* if there is a function $\hat{f} : \mathbb{N}^{i+1} \times \{0,1\}^* \to \mathbb{Q}$ such that $\hat{f}(r, k_1, \cdots, k_i, w)$ is computable in time polynomial in $r + k_1 + \cdots + k_i + |w|$ and, for all $r, k_1, \cdots, k_i \in \mathbb{N}$ and $w \in \{0,1\}^*$,

$$\left| \hat{f}(r, k_1, \cdots, k_i, w) - f(k_1, \cdots, k_i, w) \right| \leq 2^{-r}.$$

Definition. A set X of languages has p-*measure* 0 if there is a p-computable supermartingale d such that $X \subseteq S^\infty[d]$.

The expression $\mu_{\rm p}(X) = 0$ means that X has p-measure 0. The expression $\mu_{\rm p}(X) \neq 0$ means that X does not have p-measure 0. (This does *not* imply that "$\mu_{\rm p}(X)$" has some nonzero value.)

A series $\sum_{k=0}^{\infty} a_k$ of nonnegative reals is p-*convergent* if there is a polynomial q such that, for all $r \in \mathbb{N}$, $\sum_{k=q(r)}^{\infty} a_k \leq 2^{-r}$. The proof of Lemma 3.2 uses the following polynomial-time version of the classical first Borel-Cantelli lemma.

Theorem 2.1 (Lutz [18]). Assume that $d : \mathbb{N} \times \{0,1\}^* \to [0, \infty)$ is a function with the following properties.

(i) d is p-computable.

(ii) For each $k \in \mathbb{N}$, the function d_k, defined by $d_k(w) = d(k, w)$, is a supermartingale.

(iii) The series $\sum_{k=0}^{\infty} d_k(\lambda)$ is p-convergent.

Then

$$\mu_{\rm p}\left(\bigcap_{j=0}^{\infty} \bigcup_{k=j}^{\infty} S^1[d_k]\right) = 0.$$

The BP-operator, introduced by Schöning [31], is defined as follows. If $\mathcal{C}$ is a class of languages, then $\mathrm{BP} \cdot \mathcal{C}$ is the class of languages $A \subseteq \{0,1\}^*$ for which there exist a polynomial q and a language $B \in \mathcal{C}$ such that, for all $x \in \{0,1\}^*$,

$$\Pr_{y \in \{0,1\}^{q(|x|)}} [x \in A \iff < x, y > \in B] > \frac{2}{3}. \tag{2.1}$$

(The probability here is computed according to the uniform distribution on $\{0,1\}^{q(|x|)}$, using the string-pairing function $< x, y > = bd(x)01y$, where $bd(x)$ is x with each bit doubled, e.g., $bd(110) = 111100$.) It is clear that the BP-operator is monotone ($\mathcal{C} \subseteq \mathcal{D} \Rightarrow \mathrm{BP} \cdot \mathcal{C} \subseteq \mathrm{BP} \cdot \mathcal{D}$) and commutes with complementation ($\mathrm{BP} \cdot \mathrm{co} - \mathcal{C} = \mathrm{co} - \mathrm{BP} \cdot \mathcal{C}$). For all "reasonable" classes $\mathcal{C}$ – including all complexity classes discussed in this note – Schöning [31] has shown that $\mathcal{C} \subseteq \mathrm{BP} \cdot \mathcal{C}$ and that, in inequality (2.1), any real number $\beta \in (\frac{1}{2}, 1)$ can be used in place of $\frac{2}{3}$ without changing the resulting class $\mathrm{BP} \cdot \mathcal{C}$.

3 The classes $\mathrm{BP} \cdot \Delta_k^{\mathrm{P}}$

This section shows that, if Δ_2^{P} does not have p-measure 0, then at all levels $k \geq 2$ of the polynomial-time hierarchy, $\mathrm{BP} \cdot \Delta_k^{\mathrm{P}} = \Delta_k^{\mathrm{P}}$. The proof uses the idea of languages that are hard to approximate by circuits. The key definitions, which were introduced by Nisan and Wigderson [27], are as follows.

Definition. Let $B, C \subseteq \{0,1\}^*$.

1. For $n, s \in \mathbb{N}$, C is *s^B-hard at n* if, for every n-input oracle circuit γ with $size(\gamma) \leq s$,

$$\left| L(\gamma^B) \bigtriangleup C_{=n} \right| > 2^{n-1} \left(1 - \frac{1}{s} \right),$$

   where $L(\gamma^B)$ is the set of inputs on which γ with oracle B outputs 1 and $C_{=n} = C \cap \{0,1\}^n$. (If $s = 0$, this holds trivially because the right-hand side is $-\infty$)

2. The *hardness of C at n relative to B* is

$$H_C^B(n) = \max \left\{ s \in \mathbb{N} \middle| C \text{ is } s^B\text{-hard at } n \right\}.$$

Definition. For $0 < \alpha < 1$ and $B \subseteq \{0,1\}^*$, the *relativized hardness class* H_α^B is defined by

$$\mathrm{H}_\alpha^B = \left\{ C \subseteq \{0,1\}^* \;\middle|\; H_C^B(n) > 2^{\alpha n} \text{ a.e.} \right\}$$

where "a.e." ("almost everywhere") means that the condition holds for all but finitely many $n \in \mathbb{N}$.

The following result was proven via explicit construction of a pseudorandom generator.

Theorem 3.1 (Nisan and Wigderson [27]). For all $0 < \alpha < 1$ and all $A \subseteq \{0,1\}^*$, if $\mathrm{E}^A \cap \mathrm{H}_\alpha^A \neq \emptyset$, then $\mathrm{P}^A = \mathrm{BPP}^A$.

Theorem 3.1 has been useful in several recent investigations, and has focused some attention on the condition $\mathrm{E}^A \cap \mathrm{H}_\alpha^A \neq \emptyset$. Lutz [17] showed that, for $0 < \alpha < \frac{1}{3}$, the (nonrelativized) class H_α has pspace-measure 1, so if $\mathrm{E} \cap \mathrm{H}_\alpha = \emptyset$, then E has measure 0 in ESPACE. Lutz [19] showed that, for $0 < \alpha < \frac{1}{3}$, the set of all A satisfying $\mathrm{E}^A \cap \mathrm{H}_\alpha^A = \emptyset$ has pspace-measure 0. This result was recently improved by Allender and Strauss [1], who proved that, for $0 < \alpha < \frac{1}{3}$, the set of all A satisfying $\mathrm{E}^A \cap \mathrm{H}_\alpha^A = \emptyset$ has p-measure 0. The following lemma is a small, but useful, extension of this fact.

Lemma 3.2. For all $0 < \alpha < \frac{1}{3}$ and all $S \in \mathrm{E}$,

$$\mu_{\mathrm{p}}\left(\left\{A \;\middle|\; \mathrm{E}^A \cap \mathrm{H}_\alpha^{A \oplus S} = \emptyset\right\}\right) = 0.$$

Proof. For brevity, the notation and calculations of [19] are followed, while using the test language of [1].

Let $0 < \alpha < \frac{1}{3}$ and $S \in \mathrm{E}$. Without loss of generality, assume that α is rational. For each $A \subseteq \{0,1\}^*$, define the test language

$$C(A) = \left\{x \;\middle|\; pad(x) \in A\right\},$$

where

$$pad(x) = x10^{2^{|x|}}.$$

Let

$$X = \left\{A \;\middle|\; C(A) \notin \mathrm{H}_\alpha^{A \oplus S}\right\}.$$

Since $C(A) \in \mathrm{E}^A$ for all $A \subseteq \{0,1\}^*$, it suffices to show that $\mu_{\mathrm{p}}(X) = 0$.

For each $n \in \mathbb{N}$, define the sets

$$\mathrm{OCIRC}(n) = \{\gamma | \gamma \text{ is a novel } n\text{-input oracle circuit with } size(\gamma) \leq 2^{\alpha n}\},$$

$$\mathrm{DELTA}(n) = \left\{D \subseteq \{0,1\}^n \;\middle|\; |D| \leq 2^{n-1}(1 - 2^{-\alpha n})\right\}.$$

(An n-input oracle circuit is *novel* if it is functionally distinct from all those preceding it in a standard enumeration.) It was shown in [19] that there is a constant $k_0 \in \mathbb{N}$ such that, for all $k = 2^n \geq k_0$,

$$|\ \mathrm{OCIRC}(n)\ | \cdot |\ \mathrm{DELTA}(n)\ | \cdot 2^{-k} \leq e^{-k^{\frac{1}{4}}}. \tag{3.1}$$

For each $\gamma \in \mathrm{OCIRC}(n)$ and $D \in \mathrm{DELTA}(n)$, define the set

$$Y_{\gamma,D} = \left\{A \;\middle|\; L(\gamma^{A \oplus S}) \bigtriangleup D = C(A)_{=n}\right\},$$

and for each $k \in \mathbb{N}$, let

$$X_k = \begin{cases} \bigcup_{\gamma,D} Y_{\gamma,D} & \text{if } k = 2^n, \\ \emptyset & \text{if } k \text{ is not a power of 2,} \end{cases}$$

where the union is taken over all $\gamma \in \mathrm{OCIRC}(n)$ and $D \in \mathrm{DELTA}(n)$. It is easy to see that

$$X = \bigcap_{j=0}^{\infty} \bigcup_{k=j}^{\infty} X_k, \tag{3.2}$$

so Theorem 2.1 can be used to show that $u_{\mathrm{p}}(X) = 0$.

Define $d : \mathbb{N} \times \{0,1\}^* \to [0,\infty)$ as follows, writing $d_k(w)$ for $d(k,w)$.

(i) If $k < k_0$ or k is not a power of 2, then $d_k(w) = 0$.

(ii) If $k = 2^n \geq k_0$ and $|w| < 2^{k+1}$, then $d_k(w) = e^{-k^{\frac{1}{4}}}$.

(iii) If $k = 2^n > k_0$ and $|w| \geq 2^{k+1}$, then

$$d_k(w) = \sum_{\gamma,D} \Pr(Y_{\gamma,D} \mid \mathbf{C}_w),$$

where the sum is taken over all $\gamma \in \mathrm{OCIRC}(n)$ and $D \in \mathrm{DELTA}(n)$, and the conditional probabilities $\Pr(Y_{\gamma,D} | \mathbf{C}_w)$ are computed according to the random experiment in which a language $B \subseteq \{0,1\}^*$ is chosen probabilistically, using an independent toss of a fair coin to decide membership of each string in B.

The following four claims are verified below.

Claim 1. d is p-computable.

Claim 2. For each $k \in \mathbb{N}$, d_k is a supermartingale with $d_k(\lambda) \leq e^{-k^{\frac{1}{4}}}$.

Claim 3. For all $k \geq k_0$, $X_k \subseteq S^1[d_k]$.

Claim 4. $X \subseteq \bigcap_{j=0}^{\infty} \bigcup_{k=j}^{\infty} S^1[d_k]$.

Assume for a moment that Claims 1-4 are true. By Claim 2, the series $\sum_{k=0}^{\infty} d_k(\lambda)$ is p-convergent. It follows by Claim 1, Claim 4, and Theorem 2.1 that $\mu_p(X) = 0$, completing the proof of Lemma 3.2. Thus it suffices to prove Claims 1-4.

PROOF OF CLAIM 1. In the definition of d, it is clear that cases (i), (ii), and (iii) can be distinguished in time polynomial in $k + |w|$. In case (i), the computation of $d_k(w)$ is then trivial, and in case (ii), standard numerical techniques suffice to compute an approximation of $d_k(w)$ to within 2^{-r} in time polynomial in $r + k + |w|$. Attention is thus focused on case (iii).

In case (iii), for each fixed γ and D, all oracle queries in the computation of $L(\gamma^{A \oplus S}) \triangle D$ concern strings s_i with $|s_i| \leq 2^{\alpha n} \leq k$, whence $i < 2^{k+1} \leq |w|$. If $A \in \mathbf{C}_w$ and such a query concerns membership in A, then the answer is already determined by w. If such a query concerns membership in S, then, since $S \in \mathrm{E}$, the answer can be computed in $2^{\mathrm{O}(|s_i|)} = 2^{\mathrm{O}(k)} = |w|^{\mathrm{O}(1)}$ time. Thus, for each fixed γ and D, the conditional probability $\Pr(Y_{\gamma,D} | \mathbf{C}_w)$ can be exactly computed in time polynomial in $|w|$ as follows: If $Y_{\gamma,D} \cap \mathbf{C}_w = \emptyset$, i.e., the condition $A \in \mathbf{C}_w$ forces $L(\gamma^{A \oplus S}) \triangle D \neq C(A)_{=n}$, then this is determined in time polynomial in $|w|$, and $\Pr(Y_{\gamma,D} | \mathbf{C}_w) = 0$. Otherwise, $\Pr(Y_{\gamma,D} | \mathbf{C}_w) = 2^{-m}$, where m is the number of strings x such that w does not determine membership of $pad(x)$ in A, and this, too, can be determined in time polynomial in $|w|$. Thus $\Pr(Y_{\gamma,D} | \mathbf{C}_w)$ can be computed in $|w|^{\mathrm{O}(1)}$ time for each γ and D. By (3.1), there are fewer than $|w|$ different values of γ and D, so it follows that $d_k(w)$ can be computed in time polynomial in $|w|$ in case (iii). This completes the proof of Claim 1.

PROOF OF CLAIM 2. Let $k \in \mathbb{N}$. If $k < k_0$ or k is not a power of 2, then d_k is trivially a supermartingale, so assume that $k = 2^n \geq k_0$. Let $w \in \{0,1\}^*$. There are three cases.

1. If $|w| < 2^{k+1} - 1$, then $d_k(w) = d_k(w0) = d_k(w1) = e^{-k^{\frac{1}{4}}}$, so $d_k(w) = \frac{1}{2}[d_k(w0) + d_k(w1)]$.

2. If $|w| \geq 2^{k+1}$, then a routine calculation with conditional probabilities shows that $d_k(w) = \frac{1}{2}[d_k(w0) + d_k(w1)]$.

3. If $|w| = 2^{k+1} - 1$, then $d_k(w) = e^{-k^{\frac{1}{4}}}$ and, for $b \in \{0,1\}$,

$$d_k(wb) = \sum_{\gamma,D} \Pr(Y_{\gamma,D} \;\Big|\; \mathbf{C}_{wb}). \tag{3.3}$$

In this case, the length of wb ensures that, for $A \in \mathbf{C}_{wb}$ and each fixed γ and D, the bits of wb completely determine the set $L(\gamma^{A\oplus S}) \bigtriangleup D$, while determining none of the $2^n = k$ bits of $C(A)_{=n}$. Thus, for each γ, D, and $b \in \{0,1\}$, $\Pr(Y_{\gamma,D}|\mathbf{C}_{wb}) = 2^{-k}$. It follows by (3.1) that

$$d_k(w) = e^{-k^{\frac{1}{4}}} \geq \frac{1}{2}[d_k(w0) + d_k(w1)].$$

The above three cases confirm that d_k is a supermartingale. It is clear that $d_k(\lambda) \leq e^{-k^{\frac{1}{4}}}$.

Proof of Claim 3. Let $k \geq k_0$. If k is not a power of 2, then Claim 3 is trivially affirmed, so assume that $k = 2^n$. Let $A \in X_k$, and fix $\gamma' \in \mathrm{OCIRC}(n)$ and $D' \in \mathrm{DELTA}(n)$ such that $A \in Y_{\gamma',D'}$. Fix $l \in \mathbb{N}$ sufficiently large that $L(\gamma^{A\oplus S}) \bigtriangleup D'$ and $C(A)_{=n}$ are completely determined by the string $w_l = \chi_A[0..l-1]$. Then $l \geq 2^{k+1}$, so

$$d_k(w_l) = \sum_{\gamma,D} \Pr(Y_{\gamma,D}|\mathbf{C}_{w_l}) \geq \Pr(Y_{\gamma',D'}|\mathbf{C}_{w_l}) = 1.$$

Thus $A \in S^1[d_k]$.

Proof of Claim 4. Let $A \in X$. Then $A \in X_k$ for infinitely many k. It follows by Claim 3 that $A \in S^1[d_k]$ for infinitely many k, whence $A \in \bigcap_{j=0}^{\infty} \bigcup_{k=j}^{\infty} S^1[d_k]$.

This completes the proof of Lemma 3.2.

□

The following result is the main observation of this paper.

<u>Theorem 3.3.</u> If $2 \leq j \leq k$ and $\mu_p(\Delta_j^{\mathrm{P}}) \neq 0$, then $\mathrm{BP} \cdot \Delta_k^{\mathrm{P}} = \Delta_k^{\mathrm{P}}$.

<u>Proof.</u> Assume the hypothesis, and let

$$X = \left\{ A \;\middle|\; \mathrm{E}^A \cap \mathrm{H}_\alpha^{A\oplus QBF_{k-1}} = \emptyset \right\},$$

where $\alpha = \frac{1}{4}$. By Lemma 3.2 and the hypothesis, $\mu_{\mathrm{p}}(X) = 0$ and $\mu_{\mathrm{p}}(\Delta_j^{\mathrm{P}}) \neq 0$, so there exists a language $A \in \Delta_j^{\mathrm{P}} - X \subseteq \Delta_k^{\mathrm{P}} - X$. Since $A \notin X$,

$$\emptyset \neq \mathrm{E}^A \cap \mathrm{H}_\alpha^{A\oplus QBF_{k-1}} \subseteq \mathrm{E}^{A\oplus QBF_{k-1}} \cap \mathrm{H}_\alpha^{A\oplus \mathrm{QBF}_{k-1}},$$

so by Theorem 3.1,

$$\mathrm{P}^{A\oplus \mathrm{QBF}_{k-1}} = \mathrm{BPP}^{A\oplus QBF_{k-1}}.$$

It follows that

$$\begin{aligned}\Delta_k^{\mathrm{P}} &\subseteq \mathrm{BP}\cdot\Delta_k^{\mathrm{P}} = \mathrm{BPP}^{QBF_{k-1}} \\ &\subseteq \mathrm{BPP}^{A\oplus QBF_{k-1}} = \mathrm{P}^{A\oplus QBF_{k-1}} \\ &= \Delta_k^{\mathrm{P}}\end{aligned}$$

□

Corollary 3.4. If $\mu_{\mathrm{p}}(\Delta_2^{\mathrm{P}}) \neq 0$, then for all $k \geq 2$, $\mathrm{BP}\cdot\Delta_k^{\mathrm{P}} = \Delta_k^{\mathrm{P}}$.

Assuming that $\mu_{\mathrm{p}}(\Delta_2^{\mathrm{P}}) \neq 0$, the inclusion relations depicted in Figure 2 follow from Corollary 3.4 and the inclusion relations in Figure 1. The operators $\mathrm{P}, \exists^{\mathrm{P}}$, and $\forall^{\mathrm{P}}$ also behave as one would expect in Figure 2. That is (still assuming that $\mu_{\mathrm{p}}(\Delta_2^{\mathrm{P}}) \neq 0$), the identities $\mathrm{P}(\mathrm{AM}) = \Delta_2^{\mathrm{P}}$, $\forall^{\mathrm{P}}\cdot\mathrm{AM} = \Pi_2^{\mathrm{P}}$, etc. all hold. It should be noted, however, that Figure 2 cannot be used as "casually" as Figure 1, because Figure 2 does not relativize. For example, even if $\mu_{\mathrm{p}}(\Delta_2^{\mathrm{P}}) \neq 0$ in the unrelativized case, Ko [10] has shown that there is an oracle A such that, for all $k \geq 0$, $\mathrm{BP}\cdot\Sigma_k^{\mathrm{P}}(A) \not\subseteq \Sigma_{k+1}^{\mathrm{P}}(A)$.

4 Lowness of $\mathrm{AM} \cap \mathrm{co} - \mathrm{AM}$

In this section it is shown that, if Δ_2^{P} does not have p-measure 0, then $\mathrm{AM} \cap \mathrm{co} - \mathrm{AM}$ is low for Δ_2^{P}. The demonstration is easy, using Theorem 3.3 and the following known result.

Theorem 4.1 (Köbler, Schöning, and Tóran [13]). AM ∩ co-AM is low for AM.

The following observation is now easily established.

Theorem 4.2. If $\mu_{\mathrm{p}}(\Delta_2^{\mathrm{P}}) \neq 0$, then AM ∩ co-AM is low for Δ_2^{P}.

Proof. Assume the hypothesis. Then, by Theorems 4.1 and 3.3,

$$\begin{aligned}\mathrm{NP}(\mathrm{AM}\cap\text{co-AM}) &\subseteq \mathrm{AM}(\mathrm{AM}\cap\text{co-AM}) = \mathrm{AM} \\ &= \mathrm{BP}\cdot\mathrm{NP} \subseteq \mathrm{BP}\cdot\Delta_2^{\mathrm{P}} = \Delta_2^{\mathrm{P}},\end{aligned}$$

so

$$\begin{aligned} \Delta_2^{\mathrm{P}} &\subseteq \Delta_2^{\mathrm{P}}(\mathrm{AM} \cap \text{co-AM}) = \mathrm{P}(\mathrm{NP}(\mathrm{AM} \cap \text{co-AM})) \\ &\subseteq \mathrm{P}(\Delta_2^{\mathrm{P}}) = \Delta_2^{\mathrm{P}}. \end{aligned}$$

□

It was recently shown by Allender and Strauss [1] that, if $\mu_{\mathrm{p}}(\Delta_2^{\mathrm{P}}) \neq 0$, then $\mathrm{BPP} \subseteq \Delta_2^{\mathrm{P}}$. The following corollary extends this result.

Corollary 4.3. If $\mu_{\mathrm{p}}(\Delta_2^{\mathrm{P}}) \neq 0$, then BPP is low for Δ_2^{P}.

Proof. This follows immediately from Theorem 4.2 and the fact that $\mathrm{BPP} \subseteq \mathrm{AM} \cap \text{co-AM}$. □

The graph isomorphism problem is known to be in $\mathrm{NP} \cap \text{co-AM}$ [13], which is contained in $\mathrm{AM} \cap \text{co-AM}$. This gives the following corollaries.

Corollary 4.4. If $\mu_{\mathrm{p}}(\Delta_2^{\mathrm{P}}) \neq 0$, then the graph isomorphism problem is low for Δ_2^{P}.

Corollary 4.5. If $\mu_{\mathrm{p}}(\Delta_2^{\mathrm{P}}) \neq 0$ and $\Delta_2^{\mathrm{P}} \neq \mathrm{PH}$, then the graph isomorphism problem is not $\leq_{\mathrm{m}}^{\mathrm{P}}$- complete, $\leq_{\mathrm{T}}^{\mathrm{P}}$-complete, or $\leq_{\mathrm{T}}^{\mathrm{SNP}}$-complete for NP.

Note that, in each of Corollaries 4.3, 4.4, and 4.5, the added hypothesis $\mu_{\mathrm{p}}(\Delta_2^{\mathrm{P}}) \neq 0$ has allowed Δ_2^{P} to replace Σ_2^{P} in a previously known result.

5 Lowness and Polynomial Advice

The relationship between uniform and nonuniform complexity is one of the greatest enigmas of computational complexity. A principal component of current understanding of this relationship is the proof by Karp and Lipton [8] that, if $\Sigma_2^{\mathrm{P}} \neq \mathrm{PH}$, then $\mathrm{NP} \not\subseteq \mathrm{P/Poly}$. That is, if the polynomial-time hierarchy does not collapse to Σ_2^{P}, then NP does not have polynomial-size circuits. The following recent result allows a significant weakening of Karp and Lipton's hypothesis.

Theorem 5.1 (Köbler and Watanabe [14]).

1. Every self-reducible language in $(\mathrm{NP} \cap \text{co-NP})/\mathrm{Poly}$ is low for ZPP(NP).

2. If $k \geq 1$, and $\mathrm{ZPP}(\Sigma_k^{\mathrm{P}}) \neq \mathrm{PH}$, then $\Sigma_k^{\mathrm{P}} \not\subseteq (\Sigma_k^{\mathrm{P}} \cap \Pi_k^{\mathrm{P}})/\mathrm{Poly}$.

Corollary 5.2. If ZPP(NP) $\neq$ PH, then NP $\not\subseteq$ (NP $\cap$ co-NP)/Poly.

In this brief section, it is noted that the hypothesis $\mu_{\mathrm{p}}(\Delta_2^{\mathrm{P}}) \neq 0$ allows Δ_2^{P} to replace ZPP(NP) here.

Theorem 5.3.

1. If $\mu_{\mathrm{p}}(\Delta_2^{\mathrm{P}}) \neq 0$, then every self-reducible language in (NP$\cap$co-NP)/Poly is low for Δ_2^{P}.

2. If $k \geq 1$, $\mu_{\mathrm{p}}(\Delta_{k+1}^{\mathrm{P}}) \neq 0$, and $\Delta_{k+1}^{\mathrm{P}} \neq \mathrm{PH}$, then $\Sigma_k^{\mathrm{P}} \not\subseteq (\Sigma_k^{\mathrm{P}} \cap \Pi_k^{\mathrm{P}})/\mathrm{Poly}$.

Proof.

1. Assume the hypothesis, and let $A \in$ (NP$\cap$co-NP)/Poly be self-reducible. Then by Theorems 5.1(1) and 3.3 (in that order), $\Delta_2^{\mathrm{P}}(A) \subseteq \mathrm{ZPP}(\mathrm{NP}(A))$ $= \mathrm{ZPP}(\mathrm{NP}) \subseteq \mathrm{BPP}(\mathrm{NP}) = \mathrm{BP} \cdot \Delta_2^{\mathrm{P}} = \Delta_2^{\mathrm{P}}$.

2. Assume the hypothesis. Then, by Theorem 3.3, $\mathrm{ZPP}(\Sigma_k^{\mathrm{P}}) \subseteq \mathrm{BPP}(\Sigma_{k+1}^{\mathrm{P}})$ $= \mathrm{BP}\cdot\Delta_{k+1}^{\mathrm{P}} = \Delta_{k+1}^{\mathrm{P}} \subsetneq \mathrm{PH}$, so by Theorem 5.1(2), $\Sigma_k^{\mathrm{P}} \not\subseteq (\Sigma_k^{\mathrm{P}}\cap\Pi_k^{\mathrm{P}})/\mathrm{Poly}$.

□

Corollary 5.4. If $\mu_{\mathrm{p}}(\Delta_2^{\mathrm{P}}) \neq 0$ and $\Delta_2^{\mathrm{P}} \neq \mathrm{PH}$, then NP $\not\subseteq$ (NP$\cap$co-NP)/Poly.

Thus, if $\mu_{\mathrm{p}}(\Delta_2^{\mathrm{P}}) \neq 0$ and the polynomial-time hierarchy does not collapse to Δ_2^{P}, then NP does not have polynomial-size circuits.

6 Conclusion

The following two questions arise immediately from the observations presented here.

1. Assuming that $\mu_{\mathrm{p}}(\mathrm{NP}) \neq 0$, can Δ_2^{P} be replaced by a smaller class, e.g., Θ_2^{P}, in any or all of the above observations?

2. What is the relationship between the hypotheses $\mu_{\mathrm{p}}(\mathrm{NP}) \neq 0$ and $\mu_{\mathrm{p}}(\Delta_2^{\mathrm{P}}) \neq 0$? Are they equivalent, or is the latter in some sense weaker?

It is to be hoped that this paper is a small first step toward a comprehensive understanding of lowness properties under strong, measure-theoretic hypotheses.

Acknowledgement

I thank two referees and the SUNY-Buffalo complexity theory seminar for several remarks that improved this paper.

References

[1] 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. IEEE Computer Society Press, 1994.

[2] J. L. Balcázar, J. Díaz, and J. Gabarró. *Structural Complexity I.* Springer-Verlag, Berlin, 1994.

[3] M. Bellare and S. Goldwasser. The complexity of decision versus search. *SIAM Journal on Computing*, 23:97–119, 1994.

[4] D. P. Bovet and P. Crescenzi. *Introduction to the Theory of Complexity.* Prentice Hall, 1994.

[5] D. W. Juedes. *The Complexity and Distribution of Computationally Useful Problems.* PhD thesis, Iowa State University, 1994.

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

[7] D. W. Juedes and J. H. Lutz. Completeness and weak completeness under polynomial-size circuits. *Information and Computation*, 125:13–31, 1996.

[8] R. Karp and R. Lipton. Some connections between nonuniform and uniform complexity classes. In *Proc. 12th ACM Symp. Theory of Computer Science*, pages 302–309, 1980.

[9] A. Klapper. Generalized lowness and highness and probabilistic classes. *Mathematical Systems Theory*, 22:37–45, 1989.

[10] K. Ko. Separating and collapsing results on the relativized probabilistic polynomial-time hierarchy. *Journal of the Association for Computing Machinery*, 37:415–438, 1990.

[11] K. Ko and U. Schöning. On circuit-size complexity and the low hierarchy in NP. *SIAM J. Comput.*, 14:41–51, 1985.

[12] J. Köbler. On the structure of low sets. In *Proceedings of the Tenth Structure in Complexity Theory Conference*, pages 246–261. IEEE Computer Society Press, 1995.

[13] J. Köbler, U. Schöning, and J. Torán. *The Graph Isomorphism Problem.* Birkhäuser, Berlin, 1993.

[14] J. Köbler and O. Watanabe. New collapse consequences of NP having small circuits. In *Proceedings of the 22nd International Colloquium on Automata, Languages, and Programming.* Springer-Verlag, 1995. to appear.

[15] C. Lautemann. BPP and the polynomial hierarchy. *Information Processing Letters*, 14:215–217, 1983.

[16] J. H. Lutz. Resource-bounded measure. In preparation.

[17] J. H. Lutz. An upward measure separation theorem. *Theoretical Computer Science*, 81:127–135, 1991.

[18] J. H. Lutz. Almost everywhere high nonuniform complexity. *Journal of Computer and System Sciences*, 44:220–258, 1992.

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

[20] J. H. Lutz. The quantitative structure of exponential time. In *Proceedings of the Eighth Structure in Complexity Theory Conference*, pages 158–175. IEEE Computer Society Press, 1993.

[21] J. H. Lutz. Weakly hard problems. *SIAM Journal on Computing*, 24:1170–1189, 1995.

[22] J. H. Lutz and E. Mayordomo. Measure, stochasticity, and the density of hard languages. *SIAM Journal on Computing*, 23:762–779, 1994.

[23] J. H. Lutz and E. Mayordomo. Cook versus Karp-Levin: Separating completeness notions if NP is not small. *Theoretical Computer Science*, 146:141–163, 1996.

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

[25] E. Mayordomo. Almost every set in exponential time is P-bi-immune. *Theoretical Computer Science*, 136(2):487–506, 1994.

[26] E. Mayordomo. *Contributions to the Study of Resource-Bounded Measure*. PhD thesis, Universitat Politècnica de Catalunya, Barcelona, Spain, 1994.

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

[28] Christos H. Papadimitriou. *Computational Complexity*. Addison-Wesley, 1994.

[29] U. Schöning. A low and high hierarchy within NP. *Journal of Computer and System Sciences*, 27:14–28, 1983.

[30] U. Schöning. Graph isomorphism is in the low hierarchy. *Journal of Computer and System Sciences*, 37:312–323, 1988.

[31] U. Schöning. Probabilistic complexity classes and lowness. *Journal of Computer and System Sciences*, 39:84–100, 1989.

[32] M. Sipser. A complexity-theoretic approach to randomness. In *Proceedings of the 15th ACM Symposium on Theory of Computing*, pages 330–335, 1983.

[33] L. J. Stockmeyer. The polynomial-time hierarchy. *Theoretical Computer Science*, 3:1–22, 1977.

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

[35] C. Wrathall. Complete sets and the polynomial-time hierarchy. *Theoretical Computer Science*, 3:23–33, 1977.

[36] S. Zachos and H. Heller. A decisive characterization of BPP. *Information and Control*, 69:125–135, 1986.