Upward Separations and Weaker Hypotheses in Resource-Bounded Measure*

Ryan C. Harkins † John M. Hitchcock ‡

Abstract

We consider resource-bounded measure in double-exponential-time complexity classes. In contrast to complexity class separation translating downwards, we show that measure separation translates upwards. For example,

$$\mu_{\mathrm{p}}(\mathrm{NP}) \neq 0 \Rightarrow \mu_{\mathrm{e}}(\mathrm{NE}) \neq 0 \Rightarrow \mu_{\mathrm{exp}}(\mathrm{NEXP}) \neq 0.$$

We also show that if NE does not have e-measure 0, then the NP-machine hypothesis holds. We give oracles relative to which the converses of these statements do not hold. Therefore the hypothesis on the e-measure of NE is relativizably weaker than the often-investigated p-measure hypothesis on NP, but it has many of the same consequences.

1 Introduction

The strong hypothesis that NP does not have p-measure 0, written $\mu_{\mathrm{p}}(\mathrm{NP}) \neq 0$, has been often investigated and shown to have many plausible consequences in complexity theory that are not known to follow from more traditional hypotheses such as $\mathrm{P} \neq \mathrm{NP}$. The natural question to ask is whether $\mu_{\mathrm{p}}(\mathrm{NP}) \neq 0$ is the weakest such hypothesis for which these consequences hold. For this we consider resource-bounded measure in double-exponential time.

Book [4] showed that complexity class separations translate downward. For example,

$$\mathrm{E} \neq \mathrm{NE} \Rightarrow \mathrm{P} \neq \mathrm{NP}.$$

In contrast, we show that measure separations translate upward:

$$\mu_{\mathrm{p}}(\mathrm{NP}) \neq 0 \Rightarrow \mu_{\mathrm{e}}(\mathrm{NE}) \neq 0$$

and

$$\mu_{\mathrm{e}}(\mathrm{NE}) \neq 0 \Rightarrow \mu_{\mathrm{exp}}(\mathrm{NEXP}) \neq 0.$$

These upward separations illuminate the often-observed relationship between the measure of NP and exponential-time classes. For example, Lutz [12] showed that $\mu_{\mathrm{p}}(\mathrm{NP}) \neq 0$ implies E^{NP} has high NP-oracle circuit-size complexity, which in turn yields $\mathrm{P}^{\mathrm{NP}} = \mathrm{BPP}^{\mathrm{NP}}$ via Nisan-Wigderson pseudorandom generators [15]. Our result that $\mu_{\mathrm{p}}(\mathrm{NP}) \neq 0$ implies $\mu_{\mathrm{e}}(\mathrm{NE}) \neq 0$ makes it very clear

*This research was supported in part by NSF grant 0515313.
†Department of Computer Science, University of Wyoming. rharkins@cs.uwyo.edu
‡Department of Computer Science, University of Wyoming. jhitchco@cs.uwyo.edu

why this result holds – if $\mu_{\rm e}(\rm NE) \neq 0$, then NE has high circuit-complexity relative to any oracle in E.

Hitchcock and Pavan [5] showed that many of the consequences of $\mu_{\rm p}(\rm NP) \neq 0$ also follow from the NP-machine hypothesis. This hypothesis asserts that there is an NP-machine accepting 0^* such that no subexponential-time algorithm can compute its accepting computations. While at first glance this is a curious statement, the NP-machine hypothesis turns out to capture much of the essential character in nondeterministic hardness assumptions. We show that $\mu_{\rm e}(\rm NE) \neq 0$ also implies the NP-machine hypothesis.

We investigate the relative strength of the $\mu_{\rm e}(\rm NE) \neq 0$ hypothesis by constructing an oracle relative to which $\mu_{\rm e}(\rm NE) \neq 0$ but $\mu_{\rm p}(\rm NP) = 0$. We also construct an oracle where $\mu_{\rm exp}(\rm NEXP) \neq 0$ and the NP-machine hypothesis fails. Taken together, our results suggest that $\mu_{\rm e}(\rm NE) \neq 0$ is the weakest useful measure hypothesis on nondeterministic classes.

For randomized classes the situation is quite different. We use recent work in derandomization [7] and results on zero-one laws for p-measure [19, 8] to show that $\mu_{\rm p}(\rm BPP) = \mu_{\rm e}(\rm BPE)$, and similarly for ZPP, RP, and their exponential variants.

This paper is organized as follows. In section 2 we review resource-bounded measure and explain how it is defined in double-exponential-time classes. The upward measure separations are presented in section 3. In section 4 we consider weaker measure-theoretic hypotheses. We consider randomized classes in Section 5. Section 6 concludes with a discussion of extensions to even larger classes.

2 Resource-Bounded Measure

In this section we review some of the fundamental principles of resource-bounded measure, and show how they extend to the double-exponential-time setting. For more information regarding resource-bounded measure, see [10] and [11].

We identify each language $A \subseteq \{0,1\}^*$ with its infinite binary characteristic sequence

$$\chi_A = [\![s_0 \in L]\!][\![s_1 \in L]\!][\![s_2 \in L]\!] \ldots,$$

where $s_0 = \lambda$, $s_1 = 0$, $s_2 = 1$, $s_3 = 00$, ... is the standard enumeration of $\{0,1\}^*$, and $[\![\Psi]\!]$ is the boolean evaluation of Ψ. The set of all infinite binary sequences is the Cantor space $\mathbf{C}$. With this identification we view complexity classes as subsets of $\mathbf{C}$.

A *martingale* is a function $d : \{0,1\}^* \to [0,\infty)$ satisfying the averaging condition

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

for all $w \in \{0,1\}^*$. We can consider a martingale as a betting scheme that bets on the next bit of the characteristic sequence of a language. The averaging condition says that the betting scheme is fair. When a martingale makes a bet, it places a certain amount of its capital (not to exceed its total capital) on the next bit in the sequence. Then that bit is revealed, and if the martingale has guessed correctly, it receives back twice the amount it bid. Otherwise, it loses all the amount bid. A martingale *succeeds on* a sequence $A \in \mathbf{C}$ if its capital is unbounded while betting on A:

$$\limsup_{n\to\infty} d(A\restriction n) = \infty.$$

Here we write $A \restriction n$ for the first n bits of A. The *success set* of a martingale d, $S^\infty[d]$, is the set of all languages on which d succeeds.

Ville [20] proved that a class $\mathcal{C} \subseteq \mathbf{C}$ has Lebesgue measure 0 if and only if there is some martingale d such that $\mathcal{C} \subseteq S^\infty[d]$. Resource-bounded measure is defined by restricting the martingales in Ville's theorem. A *resource bound* is a class Δ of functions. For example, Δ could be functions that are computable in polynomial time. We say that a class $\mathcal{C}$ has Δ-*measure 0* and write $\mu_\Delta(\mathcal{C}) = 0$ if for some martingale $d \in \Delta$, $\mathcal{C} \subseteq S^\infty[d]$. We say that a class $\mathcal{C}$ has Δ-*measure 1* and write $\mu_\Delta(\mathcal{C}) = 1$ if $\mu_\Delta(\mathcal{C}^c) = 0$.

As martingales are real-valued functions, in general we have to work with computable approximations, as the actual values may not be computable. However, Juedes and Lutz [9] proved an exact computation lemma which states that given a martingale with a computable approximation, we can obtain a rational-valued martingale computable within a slightly larger time bound with a success set that subsumes the success set of the original martingale. Because of this, we can assume that all martingales are rational-valued and exactly computable.

Useful in the theory of resource-bounded measure are functions called constructors. A *constructor* $\delta : \{0,1\}^* \to \{0,1\}^*$ maps any string $w \in \{0,1\}^*$ into an extension $\delta(w) = wz$ for some $z \in \{0,1\}^*$, $z \neq \epsilon$. The *result* $R(\delta)$ of a constructor δ is the unique sequence $R(\delta) \sqsupseteq \delta^n(\lambda)$ for all $n \in \mathbb{N}$, i.e. the sequence obtained when δ is applied repeatedly to the empty string. For each resource bound Δ, we define the complexity class

$$R(\Delta) = \{R(\delta) \mid \delta \in \Delta \text{ is a constructor}\}.$$

Let Δ be a standard resource bound. Lutz [10] showed that for each martingale $d \in \Delta$ there is a constructor $\delta \in \Delta$ such that the result $R(\delta) \notin S^\infty[d]$. In particular, this implies that $R(\Delta)$ does not have Δ-measure 0. Furthermore, for every constructor $\delta \in \Delta$, there is a martingale $d \in \Delta$ such that d succeeds on $R(\delta)$. Together these statements justify Δ-measure as the "right" measure for the class $R(\Delta)$ and suggest the following definitions. Let $\mathcal{C}$ be a complexity class.

1. We say that $\mathcal{C}$ *has measure 0 in* $R(\Delta)$ and write $\mu(\mathcal{C} \mid R(\Delta)) = 0$, if $\mu_\Delta(\mathcal{C} \cap R(\Delta)) = 0$.
2. We say that $\mathcal{C}$ *has measure 1 in* $R(\Delta)$ and write $\mu(\mathcal{C} \mid R(\Delta)) = 1$, if $\mu(\mathcal{C}^c \mid R(\Delta)) = 0$.

The two most common instances of Δ are the following time-bounded classes.

$$\begin{aligned} \mathrm{p} = \mathrm{p}_1 &= \{f \mid f \text{ is computable in } n^{O(1)} \text{ time }\} && \text{(polynomial)} \\ \mathrm{p}_2 &= \{f \mid f \text{ is computable in } 2^{(\log n)^{O(1)}} \text{ time}\} && \text{(quasipolynomial).} \end{aligned}$$

Lutz showed that for these resource bounds we have

$$R(\mathrm{p}) = \mathrm{E} = \mathrm{DTIME}(2^{O(n)})$$

and

$$R(\mathrm{p}_2) = \mathrm{EXP} = \mathrm{DTIME}(2^{n^{O(1)}}).$$

Therefore p-measure yields measure in E and p_2-measure yields measure in EXP.

We will work with the following exponential-time resource bounds.

$$\begin{aligned} \mathrm{e} = \mathrm{e}_1 &= \{f \mid f \text{ is computable in } 2^{O(n)} \text{ time}\} && \text{(linear exponential)} \\ \mathrm{exp} = \mathrm{e}_2 &= \{f \mid f \text{ is computable in } 2^{n^{O(1)}} \text{ time}\} && \text{(polynomial exponential)} \\ \mathrm{e}_3 &= \{f \mid f \text{ is computable in } 2^{2^{(\log n)^{O(1)}}} \text{ time}\} && \text{(quasipolynomial exponential)} \end{aligned}$$

It is routine to show the following. Here $\mathrm{EE} = \mathrm{DTIME}(2^{2^{O(n)}})$ and $\mathrm{EEXP} = \mathrm{DTIME}(2^{2^{n^{O(1)}}})$.

Lemma 2.1.

1. $R(\mathrm{e}) = \mathrm{DTIME}(2^{O(2^n)})$.
2. $R(\exp) = \mathrm{EE}$.
3. $R(\mathrm{e}_3) = \mathrm{EEXP}$.

Therefore exp-measure yields measure within EE and e_3-measure gives measure within EEXP. These results also relativize, in that if we allow the martingales access to an oracle A, then $\exp^A$-measure yields measure with EE^A, e_3^A-measure gives measure with EEXP^A, and in general Δ^A-measure yields measure within $R(\Delta^A)$.

Results from measure within E and EXP typically carry up to EE and EEXP. For example, for all $c \in \mathbb{N}$, $\mathrm{DTIME}(2^{2^{cn}})$ has measure 0 in EE and $\mathrm{DTIME}(2^{2^{n^c}})$ has measure 0 in EEXP. Mayordomo's result [14] about bi-immunity extends to show that

$$\{A \mid A \text{ is } \mathrm{DTIME}(2^{2^{cn}})\text{-bi-immune}\}$$

has measure 1 in EE. Lutz [10] showed that for all $\alpha < 1$, the circuit-size complexity class

$$\mathrm{SIZE}\left(\frac{2^n}{n}\left(1 + \frac{\alpha \log n}{n}\right)\right)$$

has pspace-measure 0. Here pspace denotes the class of functions computable in polynomial space. Since pspace $\subseteq$ exp, it follows immediately that these classes also have exp-measure 0. In fact, if we instead consider A-oracle circuits for any oracle $A \in \mathrm{E}$, the SIZE^A versions of the above classes can be shown to have e-measure 0.

We remark that the p_i's and e_i's in this section are the first few classes in a general hierarchy that we discuss in section 6.

3 Upward Measure Separations

For a class $\mathcal{C}$ of languages, let $\mathrm{P_m}(\mathcal{C}) = \{A \mid (\exists B \in \mathcal{C}) A \leq^{\mathrm{p}}_{\mathrm{m}} B\}$ be the $\leq^{\mathrm{p}}_{\mathrm{m}}$-*closure of* $\mathcal{C}$. The following result is often useful.

Theorem 3.1. (Juedes and Lutz [9]) *For any class* $\mathcal{C}$*, if* $\mu_{\mathrm{p}_2}(\mathrm{P_m}(\mathcal{C})) = 0$*, then* $\mu_{\mathrm{p}}(\mathcal{C}) = 0$.

In particular, if $\mathcal{C}$ is closed under $\leq^{\mathrm{p}}_{\mathrm{m}}$-reductions, then $\mathcal{C}$ has p-measure 0 if and only if it has p_2-measure 0.

The proof of Theorem 3.1 used the martingale dilation technique of Ambos-Spies, Terwijn, and Zheng [2], which involves the following definitions.

1. For a string $w \in \{0,1\}^*$ and a language $A \subseteq \{0,1\}^*$, the *restriction of* w *to* A is the string $w \restriction A$ defined by successively concatenating the bits $w[n]$ for which $s_n \in A$. (Recall that s_n is the n^{th} string in the enumeration of $\{0,1\}^*$.)
2. Let $f : \{0,1\}^* \to \{0,1\}^*$.

(a) The *range of* f is the language $\mathrm{range}(f) = \{f(x) \mid x \in \{0,1\}^*\}$.

(b) We say that f is *strictly increasing* if $x < y$ implies $f(x) < f(y)$ for all strings x and y.

(c) For any language A, the *preimage of* A *under* f is $f^{-1}(A) = \{x \mid f(x) \in A\}$.

3. Given a function $f : \{0,1\}^* \to \{0,1\}^*$ and a martingale d, the f*-dilation of* d is the function $f\hat{\ }d : \{0,1\}^* \to [0,\infty)$ defined by

$$f\hat{\ }d(w) = d(w \restriction \mathrm{range}(f)).$$

Lemma 3.2. (Ambos-Spies, Terwijn, and Zheng [2]) *If* $f : \{0,1\}^* \to \{0,1\}^*$ *is strictly increasing and* d *is a martingale, then* $f\hat{\ }d$ *is also a martingale. Moreover, for every language* $A \subseteq \{0,1\}^*$*, if* d *succeeds on* $f^{-1}(A)$*, then* $f\hat{\ }d$ *succeeds on* A.

Theorem 3.1 extends to exponential-time measures as follows. Here we let $\mathrm{Lin}_m(\mathcal{C})$ be the closure of $\mathcal{C}$ under linear-time many-one reductions, in analogy with $\mathrm{P_m}(\mathcal{C})$.

Theorem 3.3. *Let* $\mathcal{C}$ *be a complexity class.*

1. *If* $\mu_{\mathrm{e}_2}(\mathrm{Lin}_m(\mathcal{C})) = 0$*, then* $\mu_{\mathrm{e}}(\mathcal{C}) = 0$.
2. *If* $\mu_{\mathrm{e}_3}(\mathrm{P_m}(\mathcal{C})) = 0$*, then* $\mu_{\mathrm{e}}(\mathcal{C}) = 0$.

Proof. We prove (1). The proof of (2) is similar.

Assume that $\mu_{\mathrm{e}_2}(\mathrm{Lin}_m(\mathcal{C})) = 0$. By the exact computation lemma, there exists an exact e_2-martingale d such that $\mathrm{Lin}_m(\mathcal{C}) \subseteq S^\infty[d]$. Fix $k \geq 1$ such that d is a $2^{n^{k+1}}$-martingale and define $f : \{0,1\}^* \to \{0,1\}^*$ such that

$$f(x) = 0^{k|x|}1x.$$

Since f is strictly increasing, then the f-dilation of d, $f\hat{\ }d$, is a martingale. Let $w' = w \restriction \mathrm{range}(f)$. Note that the time required to compute w' is $O(|w|^2)$, and to compute $d(w')$ is $O(2^{|w'|^{k+1}})$. But $|w'|$ is bounded by the number of x such that $(k+1)|x| + 1 \leq |s_{|w|}| \leq \log(1+|w|)$. Thus

$$|w'| \leq 2^{(\log(1+|w|)-1)\frac{1}{k+1}+1}.$$

The time required to compute $f\hat{\ }d(w)$ is

$$O\left(|w|^2 + 2^{|w'|^{k+1}}\right),$$

which simplifies to $O\left(2^{c(1+|w|)}\right)$ for some constant c. Therefore $f\hat{\ }d$ is an e-martingale.

Now let $A \in \mathcal{C}$. Then $f^{-1}(A) \in \mathrm{Lin}_m(A) \subseteq S^\infty[d]$, so $A \in S^\infty[f\hat{\ }d]$. This shows that $\mathcal{C} \subseteq S^\infty[f\hat{\ }d]$, and $\mu_{\mathrm{e}}(\mathcal{C}) = 0$. □

The closure of NE under linear-time reductions and NEXP under polynomial-time reductions allows us to conclude the following.

Corollary 3.4.

1. $\mu_{\mathrm{e}}(\mathrm{NE}) \neq 0 \Leftrightarrow \mu_{\mathrm{e}_2}(\mathrm{NE}) \neq 0$.

2. $\mu_{\mathrm{e}}(\mathrm{NEXP}) \neq 0 \Leftrightarrow \mu_{\mathrm{e}_2}(\mathrm{NEXP}) \neq 0 \Leftrightarrow \mu_{\mathrm{e}_3}(\mathrm{NEXP}) \neq 0.$

Additionally, since $\mathrm{NEXP} = \mathrm{P_m}(\mathrm{NE})$, we have our first instance of upward measure separation:

Theorem 3.5. *If $\mu_{\mathrm{e}}(\mathrm{NE}) \neq 0$, then $\mu_{\mathrm{exp}}(\mathrm{NEXP}) \neq 0$.*

Book [4] showed that complexity class equality propagates upwards. For example:

$$\mathrm{P} = \mathrm{NP} \Rightarrow \mathrm{E} = \mathrm{NE},$$

$$\mathrm{E} = \mathrm{NE} \Rightarrow \mathrm{EE} = \mathrm{NEE}.$$

However, there are oracles against upward separations for complexity classes. For example, there is an oracle relative to which $\mathrm{P}^A \neq \mathrm{NP}^A$ and $\mathrm{E}^A = \mathrm{NE}^A$ (see [1]). Despite this, we now show that measure separations for these classes translate upward.

For a language A, let

$$\mathrm{Tally}(A) = \{0^n \mid s_n \in A\}$$

and

$$\mathrm{Tally}^{-1}(A) = \{s_n \mid 0^n \in A\}.$$

For a class $\mathcal{C}$, let $\mathrm{Tally}^{-1}(\mathcal{C}) = \{\mathrm{Tally}^{-1}(A) \mid A \in \mathcal{C}\}$.

Theorem 3.6. *If $\mu_{\mathrm{e}}(\mathrm{Tally}^{-1}(\mathcal{C})) = 0$, then $\mu_{\mathrm{p}}(\mathcal{C}) = 0$.*

Proof. By the exact computation lemma, let d be an exact 2^{cn}-time martingale that succeeds on $\mathrm{Tally}^{-1}(\mathcal{C})$. Define $f : \{0,1\}^* \to \{0,1\}^*$ by $f(s_n) = 0^n$. Then for all A, $f^{-1}(A) = \mathrm{Tally}^{-1}(A)$. By Lemma 3.2, it follows that $f\,\hat{}\,d$ succeeds on $\mathcal{C}$. The running time of $f\,\hat{}\,d$ is $O(n^c)$, so $\mathcal{C}$ has p-measure 0. $\square$

Theorem 3.7. *If $\mu_{\mathrm{p}}(\mathrm{NP}) \neq 0$, then $\mu_{\mathrm{e}}(\mathrm{NE}) \neq 0$.*

Proof. Since $\mathrm{Tally}^{-1}(\mathrm{NP}) = \mathrm{NE}$, this is immediate from Theorem 3.6. $\square$

Theorem 3.7 also holds for many other classes. For example, if $\mu_{\mathrm{p}}(\mathrm{BPP}) \neq 0$, then $\mu_{\mathrm{e}}(\mathrm{BPE}) \neq 0$. We will discuss randomized classes in more detail later in the paper.

4 Weaker Hypotheses

Recently, Hitchcock and Pavan [5] showed that if $\mu_{\mathrm{p}}(\mathrm{NP}) \neq 0$, then the following hypothesis holds.

NP-**Machine Hypothesis**: *There is an* NP *machine M that accepts 0^* and an $\epsilon > 0$ such that no 2^{n^ϵ}-time machine computes infinitely many accepting computations of M.*

We now show that the NP-machine hypothesis holds under a hypothesis on the measure of NE, which is weaker by Theorem 3.7.

Theorem 4.1. *If $\mu_{\mathrm{e}}(\mathrm{NE}) \neq 0$, then the* NP-*machine hypothesis holds.*

Proof. Let LLN be the set of all A that satisfy

$$\lim_{n\to\infty} \frac{\#(1, A\restriction n)}{n} = \frac{1}{2},$$

where $\#(1, w)$ denotes the number of 1's in the string w. Then $\mu_{\mathrm{e}}(\mathrm{LLN}) = 1$ (in fact, it is well-known that $\mu_{\mathrm{p}}(\mathrm{LLN}^c) = 0$). Let X be the set all languages A that are 2^{2^n}-immune. Then we also have $\mu_{\mathrm{e}}(X) = 1$.

Our assumption $\mu_{\mathrm{e}}(\mathrm{NE}) \neq 0$ implies that there exists a language $A \in \mathrm{NE} \cap \mathrm{LLN} \cap X$. Let N be an $\mathrm{NTIME}(2^{cn})$ machine that accepts A. Since $A \in \mathrm{LLN}$, there is some n_0 such that for all $n \geq n_0$, $A[n..2n]$ contains a 1.

We define an NP machine M as follows. On input 0^n, M chooses a value $m \in [n, 2n]$ and simulates N on input s_m. If $n < n_0$, M accepts immediately. Otherwise, M accepts if N accepts s_m. If $n \geq n_0$, there will always be $m \in [n, 2n]$ such that N accepts s_m, so M will accept 0^n. Thus M accepts 0^* and the computation time on input 0^n is bounded by $O(n^c)$.

To see that M satisfies the NP-machine hypothesis, suppose to the contrary that there is some algorithm D that computes infinitely many accepting computations of M that runs in time less than 2^{n^ϵ} for all $\epsilon > 0$. We construct an algorithm D' as follows. For any string s_n, D' simulates D on $0^{\lceil n/2\rceil}, 0^{\lceil n/2\rceil+1}, \ldots, 0^n$. If D produces a witness for $s_n \in A$, D' accepts. The running time of D' is less than $O(2^{2^{\epsilon|s_n|}})$ and $|L(D')| = \infty$, contradicting our assumption that A is 2^{2^n}-immune. Therefore, the NP-machine hypothesis holds. $\square$

Combining Theorem 4.1 with results of [5] and [17], we have the following. Let CvKL (for Cook versus Karp-Levin) be the assertion that there is a Turing-complete problem for NP that is not many-one complete.

Corollary 4.2. *If* $\mu_{\mathrm{e}}(\mathrm{NE}) \neq 0$, *then* $\mathrm{NP} = \mathrm{AM}$, $\mathrm{P}^{\mathrm{NP}} = \mathrm{BPP}^{\mathrm{NP}}$, P^{NP} *does not have n^k-size circuits for any fixed k, and CvKL holds.*

There are additional consequences from [5] that we could list in Corollary 4.2.

We now have the following picture.

$\mu(\mathrm{NP} \mid \mathrm{EXP}) \neq 0$
$\Leftrightarrow \mu_{\mathrm{p}_2}(\mathrm{NP}) \neq 0$
$\Leftrightarrow \mu_{\mathrm{p}}(\mathrm{NP}) \neq 0$

$\Downarrow$

$\mu(\mathrm{NE} \mid \mathrm{EE}) \neq 0$
$\Leftrightarrow \mu_{\mathrm{e}_2}(\mathrm{NE}) \neq 0$
$\Leftrightarrow \mu_{\mathrm{e}}(\mathrm{NE}) \neq 0$

$\Rightarrow$ NP-Machine Hypothesis $\Rightarrow$

$\mathrm{NP} = \mathrm{AM}$
$\mathrm{P}^{\mathrm{NP}} = \mathrm{BPP}^{\mathrm{NP}}$
$\mathrm{P}^{\mathrm{NP}} \not\subseteq \mathrm{SIZE}(n^k)$
CvKL

$\Downarrow$

$\mu(\mathrm{NEXP} \mid \mathrm{EEXP}) \neq 0$
$\Leftrightarrow \mu_{\mathrm{e}_3}(\mathrm{NEXP}) \neq 0$
$\Leftrightarrow \mu_{\mathrm{exp}}(\mathrm{NEXP}) \neq 0$
$\Leftrightarrow \mu_{\mathrm{e}}(\mathrm{NEXP}) \neq 0$

Is it possible that $\mu_{\mathrm{e}}(\mathrm{NE}) = \mu_{\mathrm{p}}(\mathrm{NP})$? That $\mu_{\mathrm{e}}(\mathrm{NE}) = \mu_{\mathrm{exp}}(\mathrm{NEXP})$? Does $\mu_{\mathrm{exp}}(\mathrm{NEXP}) \neq 0$ also imply the NP-machine hypothesis? The answers to these questions are probably no. We finish this section by constructing oracles that demonstrate the above picture is likely the best possible.

Theorem 4.3. *There is an oracle A relative to which $\mu_{\mathrm{p}^A}(\mathrm{NP}^A) = 0$ but $\mu_{\mathrm{e}^A}(\mathrm{NE}^A) \neq 0$.*

Proof. We will construct our oracle A so that $\mathrm{NE}^A = \mathrm{EE}^A$ while $\mu_{\mathrm{p}^A}(\mathrm{NP}^A) = 0$. In the construction we will use two bijections $\langle \cdot, \cdot \rangle : \mathbb{N}^2 \to \mathbb{N}$ and $\langle \cdot, \cdot, \cdot \rangle : \mathbb{N}^3 \to \mathbb{N}$.

Let $\{M_i^?\}$ be an enumeration of all deterministic oracle machines and define

$$K^A = \left\{ 0^{\langle i,m,t \rangle} \;\middle|\; M_i^A \text{ accepts } 0^m \text{ in } < 2^{t/5} \text{ steps} \right\}.$$

This set is complete for $\mathrm{E}^A \cap \mathrm{TALLY}$ under linear-time reductions. If we construct A so that $K^A \in \mathrm{NP}^A$, then by padding we have $\mathrm{NE}^A = \mathrm{EE}^A$, which implies $\mu_{\mathrm{e}^A}(\mathrm{NE}^A) \neq 0$.

To obtain $\mu_{\mathrm{p}^A}(\mathrm{NP}^A) = 0$, we will ensure that each NP^A set either violates the law of large numbers or has an infinite subset in P. For this, let $\{N_i^?\}$ be an enumeration of all NP oracle machines, where N_i is clocked to run in time $n^i + i$.

Initially we let $A = \emptyset$. The construction proceeds in stages. In stage n, $n \geq 0$, we do the following:

step 1 Let i, m, and t be such that $\langle i, m, t \rangle = n$, and run M_i^A on 0^m for $2^{t/5}$ steps. Reserve for A^c all strings not in A queried by this computation. If M_i^A accepts, find the least y, $|y| = 3n$, such that $\langle 0^n, y \rangle$ is not reserved for A^c and add $\langle 0^n, y \rangle$ to A.

step 2 Now let i and j be such that $\langle i, j \rangle = n$, and consider N_i^A on all strings x of size n. Let x and p be minimal such that N_i^A accepts x with computation path p and there exists s, $|s| = (i+1)\log n$, such that $\langle x, s, i \rangle$ is neither reserved for A^c nor queried by $N_i^A(x)$ on path p. Then we reserve for A^c all strings queried by path p of $N_i^A(x)$ and add $\langle x, s, i \rangle$ to A for the minimal such s. If such an x and p do not exist, do nothing.

In each stage n, we reserve at most $2^{n/5} + n^i + i$ strings for A^c. Therefore at the beginning of stage n there are fewer than $2^{n/4}$ strings reserved for A^c, so we can find a y among the 2^{3n} possible candidates to add to A in step 1. An NP^A machine can decide K^A on input 0^n by guessing a string y of length $3n$ and accepting if $\langle 0^n, y \rangle \in A$.

To see that NP^A has p^A-measure 0, consider a language B decided by N_i^A. We look at two cases:

- For infinitely many n, $|B_{=n}| < 2^{n/3}$.
- For all but finitely many n, $|B_{=n}| \geq 2^{n/3}$.

In the first case, B fails the law of large numbers. There is a p-martingale that succeeds on all such B. In the second case, we claim that B has an infinite subset in P^A. Consider the set

$$Q_i = \left\{ x \;\middle|\; \langle x, s, i \rangle \in A \text{ for some } s \in \{0,1\}^{(i+1)\log |x|} \right\}.$$

Then $Q_i \in \mathrm{P}^A$ as we can check all possible s's in $O(n^{i+1})$ time. By construction of A, we have $Q_i \subseteq L(N_i^A)$.

Finally, we claim that Q_i is infinite. Let n such that $|B_{=n}| \geq 2^{n/3}$ and $n = \langle i, j\rangle$ for some j. Since N_i^A runs in time $n^i + i$, each computation of N_i^A on an input x of length n can query at most n^i strings. In particular, for each $x \in B_{=n}$ every accepting path p does not query some string of the form $\langle x, s, i\rangle$. Therefore there are at least $2^{n/3}$ candidates $\langle x, s, i\rangle$ to add to A in step 2. Since this is more than the number of strings reserved for A^c, Q_i will have some element of length n. □

Theorem 4.4. *There is an oracle A relative to which $\mu_{\exp^A}(\mathrm{NEXP}^A) \neq 0$ and the* NP^A*-machine hypothesis fails.*

Proof. Let $\{M_i^?\}$ be an enumeration of all deterministic oracle machines, let $\{N_i^?\}$ be an enumeration of all NP oracle machines, and define

$$K^A = \left\{ 0^{\langle i,m,t\rangle} \;\middle|\; M_i^A \text{ accepts } 0^m \text{ in } < 2^{2^{(\log t)^{1/3}}} \text{ steps} \right\}.$$

This is set is complete for $\mathrm{EXP}^A \cap \mathrm{TALLY}$ under quasipolynomial-time reductions. We will construct A so that $K^A \in \mathrm{NTIME}^A(2^{(\log n)^2})$. This implies that $\mathrm{NEXP}^A = \mathrm{EEXP}^A$, which yields $\mu_{\exp^A}(\mathrm{NEXP}^A) \neq 0$.

Initially we let $A = \emptyset$. The construction proceeds in stages. In each stage n, $n \geq 0$, we do the following.

step 1 Let i, m, and t be such that $\langle i, m, t\rangle = n$, and run M_i^A on 0^m for $2^{2^{(\log t)^{1/3}}}$ steps. Reserve for A^c each string not in A queried by $M_i^A(0^m)$. If M_i^A accepts, find a y such that $|y| = 2^{(\log n)^2}$ and $\langle 0^n, y\rangle$ is not reserved for A^c. Add $\langle 0^n, y\rangle$ to A.

step 2 Let i and j be such that $\langle i, j\rangle = n$, and run N_i^A on 0^j. If N_i^A accepts, let w be some accepting computation path. Reserve for A^c all strings not in A queried by N_i^A along w. Find an r (if one exists) such that $|r| = 2^{(\log n)^{1/2}}$ and for all $k \in [0, \ldots, |w|]$, $\langle i, r, k\rangle$ has not been reserved for A^c. For each $k \in [0, \ldots, |w|]$, if $w[k] = 1$, add $\langle i, r, k\rangle$ to A. Otherwise reserve $\langle i, r, k\rangle$ for A^c

By stage n, step one has reserved no more than $n2^{2^{(\log n)^{1/3}}}$ strings, and step two has reserved $n2^{(\log(n+1))^2}$ strings. Altogether at most $n2^{2^{(\log n)^{1/3}}} + n2^{(\log n)^2}$ strings have been reserved, which is less than the $2^{2^{(\log n)^2}}$ strings of size $2^{(\log n)^2}$. Thus y exists at each stage. By construction, we have $0^n \in K^A \Leftrightarrow \langle 0^n, y\rangle \in A$ for some y of length $2^{(\log n)^2}$. This implies $K^A \in \mathrm{NTIME}(2^{(\log n)^2})$.

To see that the NP-machine hypothesis fails, consider the following algorithm. To find an accepting computation of N_i^A on 0^n, the algorithm loops over each r of size $2^{(\log n)^{1/2}}$ and constructs a candidate string w by querying A for each $\langle i, r, k\rangle$, with $k \in [0, \ldots, n^i + i]$. Then the algorithm checks if w is an accepting computation of N_i. If so, it outputs w.

We claim that if N_i^A accepts 0^*, then by our construction infinitely many w will be encoded in A, and the algorithm will be able to output those w. Thus there is a machine that will output infinitely many accepting computations of N_i^A.

The algorithm loops over each r, requiring $2^{2^{(\log n)^{1/2}}}$ iterations. Constructing each w and checking if w is an accepting computation path of N_i^A requires $p(n)$ time for some polynomial p. Thus it requires $p(n)2^{2^{(\log n)^{1/2}}}$ time. Since $2^{(\log n)^{1/2}}$ is asymptotically less than n^δ for all $\delta > 0$, our running time is at most $p(n)2^{n^\delta} = 2^{n^{\delta'}}$, which is less than 2^{n^ϵ} for all ϵ. Therefore the NP^A-machine hypothesis fails.

We need only to check that r exists infinitely often for each N_i^A. Our construction visits each NP^A machine an infinite number of times. The number of strings reserved by stage n is $O(2^{(\log n)^2} + n2^{2^{(\log n)^{1/3}}})$. This is $o(2^{2^{(\log n)^{1/2}}})$, the number of candidate strings for r. Thus for sufficiently large n, r exists. $\square$

As the proofs of Theorems 3.7 and 4.1 relativize, we also have the following for the oracle of Theorem 4.4:

Corollary 4.5. *There is an oracle A relative to which $\mu_{\mathrm{exp}^A}(\mathrm{NEXP}^A) \neq 0$ but $\mu_{\mathrm{e}^A}(\mathrm{NE}^A) = \mu_{\mathrm{p}^A}(\mathrm{NP}^A) = 0$.*

5 Randomized Classes

In this section we show that the situation is dramatically different for randomized classes. The resource-bounded measure of BPP, RP, and ZPP is very well understood. Each of these classes has zero-one law [18, 19, 8], that is, their measure within EXP is either 0 or 1.

Recently, Impagliazzo, Kabanets, and Wigderson [7] showed that these randomized classes are equal to EXP if and only if their exponential variant is equal to EE. We will combine this and other results in [7] with the above zero-one laws to derive equivalences for the measures of these classes. First, we need a simple result in e-measure.

Proposition 5.1. *For every $c \in \mathbb{N}$, io-$[\mathrm{DTIME}(2^{2^{cn}})/cn]$ has e-measure 0.*

The proof of Proposition 5.1 is analogous to the known result that io-$[\mathrm{DTIME}(2^{cn})/cn]$ has p-measure 0 [10, 6]. (In fact, because we are working at the exponential-time level we could prove something much stronger than this, pushing the advice up from linear to nearly 2^n.)

Theorem 5.2. *The following are equivalent.*

(1) $\mu(\mathrm{BPP} \mid \mathrm{EXP}) = 0$.

(2) $\mu(\mathrm{BPE} \mid \mathrm{EE}) = 0$.

(3) $\mathrm{BPP} \neq \mathrm{EXP}$.

(4) $\mathrm{BPE} \neq \mathrm{EE}$.

Proof. By the measure conservation theorem we have (2) implies (4). The equivalence of (1) and (3) was proved by van Melkebeek [19]. Impagliazzo, Kabanets, and Wigderson [7] showed that (3) and (4) are equivalent. Finally, another result in [7] is that (4) implies $\mathrm{BPE} \subseteq$ io-$[\mathrm{DTIME}(2^{2^n})/n]$, which implies (2) by Proposition 5.1. $\square$

Theorem 5.3. *The following are equivalent.*

(1) $\mu(\mathrm{ZPP} \mid \mathrm{EXP}) = 0$.

(2) $\mu(\mathrm{RP} \mid \mathrm{EXP}) = 0$.

(3) $\mu(\mathrm{ZPE} \mid \mathrm{EE}) = 0$.

(4) $\mu(\mathrm{RE} \mid \mathrm{EE}) = 0$.

(5) $\mathrm{RP} \neq \mathrm{EXP}$.

(6) $\mathrm{ZPP} \neq \mathrm{EXP}$.

(7) RE $\neq$ EE. (8) ZPE $\neq$ EE.

Proof. Impagliazzo and Moser [8] showed that (1), (2), (5), and (6) are equivalent. The equivalence of (5), (6), (7), and (8) follows from the work of Impagliazzo, Kabanets, and Wigderson [7]. Additionally, in [7] it was shown that (8) implies ZPE $\subseteq$ io-DTIME(2^{2^n}), which implies (3) by Proposition 5.1. The converse (3) implies (8) follows from the measure conservation theorem. As (4) immediately implies (3), it remains to show that (3) implies (4).

Suppose that (4) does not hold, i.e., $\mu(\mathrm{RE} \mid \mathrm{EE}) \neq 0$. Then using an argument similar to one in [8], we can show that ZPP = BPP. This implies that ZPE = RE and therefore that (3) does not hold. □

Therefore

$$\mu(\mathrm{BPP} \mid \mathrm{EXP}) = \mu(\mathrm{BPE} \mid \mathrm{EE})$$

and

$$\mu(\mathrm{RP} \mid \mathrm{EXP}) = \mu(\mathrm{ZPP} \mid \mathrm{EXP}) = \mu(\mathrm{RE} \mid \mathrm{EE}) = \mu(\mathrm{ZPE} \mid \mathrm{EE}),$$

each of these quantities is either 0 or 1.

6 Further Upward

The p_i and e_i hierarchies are the first two slices of a much larger hierarchy, which we now briefly discuss. Let $\Gamma_{0,0}$ be the class of all functions $f : \mathbb{N} \to \mathbb{N}$ such that $(\exists c)(\forall^\infty n) f(n) \leq cn$. For each $i, j \geq 0$, we let

$$\Gamma_{i+1,0} = \{f \mid (\exists g \in \Gamma_{i,0})(\forall^\infty n) f(n) \leq 2^{g(n)}\}$$

and

$$\Gamma_{i,j+1} = \{f \mid (\exists g \in \Gamma_{i,j})(\forall^\infty n) f(n) \leq 2^{g(\log n)}\}.$$

We note that the classes $(\Gamma_{0,i})_{i\in\mathbb{N}}$ are the same as Lutz's $(G_i)_{i\in\mathbb{N}}$ classes [10].

For each $i, j \geq 0$, we define the complexity class

$$\mathcal{T}_{i,j} = \bigcup_{f \in \Gamma_{i,j}} \mathrm{DTIME}(f)$$

and similarly we let $\Delta_{i,j}$ be the class of all functions that are computable in time $f(n)$ for some $f \in \Gamma_{i,j}$. The union of all the $\mathcal{T}_{i,j}$'s gives the class ELEMENTARY [16]. Lutz's hierarchies are the slices $\mathrm{p}_i = \Delta_{0,i}$ and $\mathrm{E}_i = \mathcal{T}_{1,i-1}$ for all $i \geq 1$. The exponential resource bounds we defined earlier are $\mathrm{e}_i = \Delta_{1,i-1}$. The double-exponential time classes fit in as $\mathrm{EE} = \mathcal{T}_{2,0}$ and $\mathrm{EEXP} = \mathcal{T}_{2,1}$. Lutz's result that $R(\mathrm{p}_i) = \mathrm{E}_i$ and our Lemma 2.1 can be extended to show that for all $i \geq 0$ and $j \geq 1$,

$$R(\Delta_{i,j}) = \mathcal{T}_{i+1,j-1}.$$

Let us briefly consider the resource bound $\mathrm{eexp} = \mathrm{ee}_2 = \Delta_{2,1}$. This is useful for measuring the class NEE which is a subset of the triple-exponential class $\mathrm{EEE} = \mathcal{T}_{3,0}$. We note that a more general version of Theorem 3.6 holds: if $\mu_{\Delta_{i+1,j}}(\mathrm{Tally}^{-1}(\mathcal{C})) = 0$, then $\mu_{\Delta_{i,j+1}}(\mathcal{C}) = 0$. Using this along with an extension of Theorem 3.3, we have

$$\mu_{\mathrm{exp}}(\mathrm{NE}) \neq 0 \Rightarrow \mu_{\mathrm{eexp}}(\mathrm{NEE}) \neq 0.$$

Lutz and Mayordomo [13] used Mayordomo's bi-immunity result [14] to show that $\mu_{\mathrm{p}}(\mathrm{NP}) \neq 0$ implies E $\neq$ NE and EE $\neq$ NEE. They combined this with Bellare and Goldwasser's result that EE $\neq$ NEE implies search does not reduce to decision for all NP problems [3]. We can view Lutz and Mayordomo's result as an easy corollary of upward measure separation:

$$\begin{array}{ccccccc}
\mu_{\mathrm{p}}(\mathrm{NP}) \neq 0 & \Rightarrow & \mu_{\mathrm{exp}}(\mathrm{NE}) \neq 0 & \Rightarrow & \mu_{\mathrm{eexp}}(\mathrm{NEE}) \neq 0 & \Rightarrow & \cdots \\
\Downarrow & & \Downarrow & & \Downarrow & & \\
\mathrm{P} \neq \mathrm{NP} & \Leftarrow & \mathrm{E} \neq \mathrm{NE} & \Leftarrow & \mathrm{EE} \neq \mathrm{NEE} & \Leftarrow & \cdots
\end{array}$$

The upward separations in resource-bounded measure extend all the way through the above hierarchy. This allows making weaker and weaker hypotheses on nondeterministic classes. However, our results suggest that the measure hypothesis on NE is the weakest hypothesis that is generally useful for complexity theory.

It would be interesting to see $\mu_{\mathrm{p}}(\mathrm{NP}) \neq 0$, $\mu_{\mathrm{exp}}(\mathrm{NE}) \neq 0$, and $\mu_{\mathrm{eexp}}(\mathrm{NEE})$ studied further for their relative explanatory power. We have shown the measure hypothesis on NE implies the NP-machine hypothesis, which yields many, but not all the consequences of $\mu_{\mathrm{p}}(\mathrm{NP}) \neq 0$. The measure hypothesis on NEE implies at least one interesting consequence (search versus decision for NP). The question to consider is: which of the consequences of $\mu_{\mathrm{p}}(\mathrm{NP}) \neq 0$ require its full strength, and which can be derived from these weaker hypotheses?

References

[1] E. Allender. Limitations of the upward separation technique. *Mathematical Systems Theory*, 24(1):53–67, 1991.

[2] K. Ambos-Spies, S. A. Terwijn, and X. Zheng. Resource bounded randomness and weakly complete problems. *Theoretical Computer Science*, 172(1–2):195–207, 1997.

[3] M. Bellare and S. Goldwasser. The complexity of decision versus search. *SIAM Journal on Computing*, 23(1):97–119, 1994.

[4] R. V. Book. Tally languages and complexity classes. *Information and Control*, 26:186–193, 1974.

[5] J. M. Hitchcock and A. Pavan. Hardness hypotheses, derandomization, and circuit complexity. *Computational Complexity*. To appear.

[6] J. M. Hitchcock and N. V. Vinodchandran. Dimension, entropy rates, and compression. *Journal of Computer and System Sciences*, 72(4):760–782, 2006.

[7] R. Impagliazzo, V. Kabanets, and A. Wigderson. In search of an easy witness: Exponential time vs. probabilistic polynomial time. *Journal of Computer and System Sciences*, 65(4):672–694, 2002.

[8] R. Impagliazzo and P. Moser. A zero-one law for RP. In *Proceedings of the 18th IEEE Conference on Computational Complexity*, pages 43–47. IEEE Computer Society, 2003.

[9] D. W. Juedes and J. H. Lutz. Weak completeness in E and E_2. *Theoretical Computer Science*, 143(1):149–158, 1995.

[10] J. H. Lutz. Almost everywhere high nonuniform complexity. *Journal of Computer and System Sciences*, 44(2):220–258, 1992.

[11] J. H. Lutz. The quantitative structure of exponential time. In L. A. Hemaspaandra and A. L. Selman, editors, *Complexity Theory Retrospective II*, pages 225–254. Springer-Verlag, 1997.

[12] J. H. Lutz and E. Mayordomo. Measure, stochasticity, and the density of hard languages. *SIAM Journal on Computing*, 23(4):762–779, 1994.

[13] J. H. Lutz and E. Mayordomo. Cook versus Karp-Levin: Separating completeness notions if NP is not small. *Theoretical Computer Science*, 164(1–2):141–163, 1996.

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

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

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

[17] A. Pavan and A. L. Selman. Separation of NP-completeness notions. *SIAM Journal on Computing*, 31(3):906–918, 2002.

[18] K. W. Regan, D. Sivakumar, and J. Cai. Pseudorandom generators, measure theory, and natural proofs. In *Proceedings of the 36th Symposium on Foundations of Computer Science*, pages 26–35. IEEE Computer Society, 1995.

[19] D. van Melkebeek. The zero-one law holds for BPP. *Theoretical Computer Science*, 244(1–2):283–288, 2000.

[20] J. Ville. *Étude Critique de la Notion de Collectif*. Gauthier–Villars, Paris, 1939.