One-Way Functions and Balanced NP

Jack H. Lutz
Iowa State University, lutz@iastate.edu

Follow this and additional works at: http://lib.dr.iastate.edu/cs_techreports
Part of the Theory and Algorithms Commons

Recommended Citation
http://lib.dr.iastate.edu/cs_techreports/116

This Article is brought to you for free and open access by the Computer Science at Digital Repository @ Iowa State University. It has been accepted for inclusion in Computer Science Technical Reports by an authorized administrator of Digital Repository @ Iowa State University. For more information, please contact digirep@iastate.edu.
One-Way Functions and Balanced NP*
(Extended Abstract)

Jack H. Lutz
Department of Computer Science
Iowa State University
Ames, IA  50011
lutz@iastate.edu

Note
This extended abstract is followed by an appendix containing proofs of the main results. The appendix is optional, i.e., the extended abstract can be read without consulting the appendix.
1 Introduction

In computational complexity, the existence of cryptographically secure one-way functions is currently a strong hypothesis, in that the existence of such functions is known to imply \( P \neq NP \), but not known to be a consequence of \( P \neq NP \). The question has thus arisen whether the structure of NP is relevant to the investigation of secure one-way functions. This fundamental question can be posed as follows.

\( \star \) Is there a plausible hypothesis concerning the structure of NP that provably implies the existence of cryptographically secure one-way functions?

This paper initiates a new approach to question \( \star \) and suggests a possible affirmative answer. Specifically, we define a subclass of NP called \( \beta \text{NP} \) ("balanced NP"), containing 3SAT and other standard NP problems. The hypothesis that \( \beta \text{NP} \) is not a subset of \( P \) is equivalent to the \( P \neq NP \) conjecture. A stronger hypothesis, that "\( \beta \text{NP} \) is not a measure 0 subset of \( E_2 \)," written

\[ \mu(\beta \text{NP} | E_2) \neq 0, \]

where \( E_2 = \text{DTIME}(2^{\text{polynomial}}) \), is shown to have the following consequences.

1. For every \( k \), there is a polynomial time computable, honest function \( f \) that is \((2^{n^k}/n^k)\)-one-way with exponential security. (That is, no \( 2^{n^k} \)-time-bounded algorithm with \( n^k \) bits of nonuniform advice inverts \( f \) on more than an exponentially small set of inputs.)

2. If \( \text{DTIME}(2^n) \) "separates all BPP pairs," then there is a (polynomial time computable) pseudorandom generator that passes all probabilistic polynomial-time statistical tests. (This result is a partial converse of Yao, Boppana, and Hirschfeld’s theorem, that the existence of pseudorandom generators passing all polynomial-size circuit statistical tests implies that \( \text{BPP} \subseteq \text{DTIME}(2^n) \) for all \( \epsilon > 0 \).)

Such consequences are not known to follow from \( P \neq NP \) or other previously known hypotheses concerning the structure of NP.

In section 1.1 below we describe our results in somewhat more detail. In section 1.2 we discuss the meaning and plausibility of the hypothesis \( \mu(\beta \text{NP} | E_2) \neq 0 \).

1.1 Results

Roughly speaking, as we use the term here, a cryptographically secure one-way function is a polynomial time computable, honest function \( f : \{0,1\}^* \rightarrow \{0,1\}^* \) that is hard to invert in the following sense: For every feasible algorithm \( g \), for all sufficiently large \( n \), if we choose \( x \in \{0,1\}^n \) according to the uniform distribution,
then the probability that \( f(g(f(x))) = f(x) \) (i.e., the probability that \( g \) finds a preimage of \( f(x) \)) is very small. (The reciprocal of this probability can be regarded as the security of \( f \) against inversion by \( g \).) One-way functions of this type have been extensively investigated and can be used to construct secure user authentication schemes [6], secure pseudorandom generators [14, 13], subexponential time simulations of BPP [27, 3], secure private key encryption protocols [11, 17, 8], bit commitment protocols [24], and zero-knowledge proofs of NP languages [10].

It should be noted that one-way functions with essentially minimum security requirements have also been defined and investigated. (See [26] for a survey of such work.) That is, a polynomial time computable, honest function \( f \) is sometimes considered to be one-way if every feasible algorithm \( g \) sometimes fails to invert \( f \). In this paper, we shall refer to such functions as weakly one-way, reserving the term "one-way" for functions that are cryptographically secure in the above sense. (See section 3 for precise definitions.)

It should also be noted that one-way functions are not required to be one-to-one in this paper.

In section 3, assuming the hypothesis \( \mu(\beta \text{NP} \mid E_2) \neq 0 \), we prove that for every \( k \) there is a polynomial time computable, honest function \( f \) that is \((2^{nk}/nk)\)-one-way with exponential security," i.e., no \( 2^{nk} \)-time-bounded algorithm with \( nk \) bits of nonuniform advice inverts \( f \) on more than an exponentially small set of inputs.

Yao [27] and Boppana and Hirschfeld [3] proved that, if nonuniformly secure pseudorandom generators exist, then \( \text{BPP} \subseteq \cap_{k>0} \text{DTIME}(2^{nk}) \). In section 4 below, we show that their argument actually yields an (apparently) stronger conclusion, namely that \( \cap_{k>0} \text{DTIME}(2^{nk}) \) "separates all BPP-pairs." Assuming the hypothesis \( \mu(\beta \text{NP} \mid E_2) \neq 0 \), we then prove a partial converse to this result, namely, that if \( \text{DTIME}(2^{nk}) \) separates all BPP-pairs, then uniformly secure pseudorandom generators exist. Our proof uses the theorem of Håstad [13] (building on work of Impagliazzo, Levin, and Luby [14]), that uniformly secure pseudorandom generators exist if uniformly one-way functions exist.

1.2 Discussion of the Hypothesis

It is well-known that a nonempty language is in NP if and only if it is the range of a polynomial time computable, honest function. In section 2 below, we define the class \( \beta \text{NP} \) ("balanced NP"), consisting of those NP languages that are ranges of polynomial time computable balanced functions. Roughly speaking, a balanced function is an honest function with the additional property that no element of the range has much more than its "fair share" of preimages. We show that \( \beta \text{NP} \) is a subclass of NP that contains all efficiently rankable languages in P [7], as well as 3SAT and other NP languages. The hypotheses \( P \neq \text{NP} \) and \( \beta \text{NP} \not\subseteq \text{P} \) are thus equivalent.

The main results of this paper concern the stronger hypothesis \( \mu(\beta \text{NP} \mid E_2) \neq 0 \).
In the briefest possible terms, this hypothesis says that $\beta NP$ is not a measure 0, i.e., negligibly small, subset of $E_2$ in the sense of resource-bounded measure theory [20, 22]. To fully appreciate the meaning of this hypothesis, we must be a little more precise.

For a class $C$ $\subseteq E_2$ (e.g., $C = P$, $C = NP$, or $C = \beta NP$), the condition $\mu(C \mid E_2) = 0$ means that there exist a fixed polynomial $q$, a fixed positive quantity $q_0$, and a fixed betting strategy (algorithm) $\sigma$ with the following properties:

Given any language $A \in C$, the strategy $\sigma$ bets on the membership or nonmembership of the successive strings $\lambda, 0, 1, 00, 01, \ldots$ in $A$. Before the betting begins, $\sigma$ has capital $q_0$. When betting on a string $w \in \{0, 1\}^*$, the strategy $\sigma$ is given as input the string consisting of the successive bits $[v \in A]$ for all strings $v$ that precede $w$ in the standard ordering of $\{0, 1\}^*$. On this input, the strategy $\sigma$ computes, in $\leq 2^q(|w|)$ steps, a fraction $r \in [-1, 1]$ of its current capital to bet that $w \in A$. If $\sigma$'s capital prior to this bet is $c$, then $\sigma$'s capital after the bet is $c(1 + r)$ if $w \in A$ and $c(1 - r)$ if $w \notin A$. (That is, the betting is fair.) Finally, the strategy $\sigma$ is successful, in the sense that, for all $A \in C$, $\sigma$'s capital diverges to $+\infty$ as the betting progresses through the successive strings $w \in \{0, 1\}^*$.

Thus the condition $\mu(C \mid E_2) = 0$ asserts the existence of a fixed $2^q(|w|)$-time-bounded algorithm for betting successfully on membership in languages in $C$. If $C \subseteq \text{DTIME}(2^q(|w|))$ for some fixed polynomial $r$, it is easy to devise such a strategy, so $\mu(C \mid E_2) = 0$. Conversely, if $\mu(C \mid E_2) = 0$, then $C$ is “nearly in some $\text{DTIME}(2^q(|w|))”, in the sense that there is a fixed $2^q(|w|)$-time-bounded algorithm for successful betting on languages in $C$.

There does not appear to be any a priori reason for believing that such a strategy $\sigma$ exists if $C$ is NP or $\beta NP$. That is, there does not appear to be any a priori reason for believing that $\mu(\text{NP} \mid E_2) = 0$ or $\mu(\beta \text{NP} \mid E_2) = 0$. We summarize this view by saying that the hypotheses $\mu(\text{NP} \mid E_2) \neq 0$ and $\mu(\beta \text{NP} \mid E_2) \neq 0$ are not implausible relative to our current knowledge. (The hypothesis that the polynomial-time hierarchy separates into infinitely many levels enjoys a similar status.)

Result 2 above (i.e., Theorem 3.2 below) thus suggests an affirmative answer to question (★); the remaining issue is whether the hypothesis $\mu(\beta \text{NP} \mid E_2) \neq 0$ is actually plausible. Only further investigation will determine this. Such investigation may indicate that the consequences of $\mu(\beta \text{NP} \mid E_2) \neq 0$ form, en masse, a plausible state of affairs, thereby suggesting an affirmative answer to (★). On the other hand, such investigation may uncover implausible consequences of $\mu(\beta \text{NP} \mid E_2) \neq 0$, or even yield a proof that $\mu(\beta \text{NP} \mid E_2) = 0$. This outcome might suggest either an affirmative answer or a negative answer to (★), depending upon the form it takes.

In any case, (★) is an important question that may be illuminated, directly or indirectly, by studying the class $\beta NP$.

Early results of this investigation are encouraging. The hypothesis $\mu(\text{NP} \mid E_2) \neq 0$ has recently been shown to have a number of plausible consequences: If $\mu(\text{NP} \mid E_2) \neq 0$, then NP contains p-random languages [21], NP contains $E$-bi-immune
languages [23], every $\leq_{P}^{m}$-hard language for NP ($\alpha < 1$) is exponentially dense [22], and every $\leq_{m}$-hard language for NP has an exponentially dense, exponentially hard complexity core [15]. Since $\beta$NP $\subseteq$ NP, the hypothesis $\mu(\beta$NP $|$ E$_2$) $\neq$ 0 also has these consequences. In addition, $\mu(\beta$NP $|$ E$_2$) $\neq$ 0 has the consequences proven in sections 3 and 4 below. There is thus some reason to hope that $\mu(\beta$NP $|$ E$_2$) $\neq$ 0 may be a hypothesis with considerably more explanatory power than P $\neq$ NP.

2 The Class $\beta$NP

In this section we introduce the class $\beta$NP ("balanced NP"). In order to motivate our definition, we first discuss a characterization of NP.

**Definition** A function $f$ $\in$ PF is *honest*, and we write $f$ $\in$ PF$_{\text{hon}}$, if there is a polynomial $q$ such that, for all $y$ $\in$ range($f$), $f^{-1}(\{y\})_{\leq q(|y|)} \neq \emptyset$.

It is well-known that nonempty NP languages can be characterized as ranges of honest functions. In fact, the honest functions can be required to have a very special normal form.

**Definition** Let $q$ be a strictly increasing polynomial. A function $f$ $\in$ Partial-PF is *$q$-honest*, and we write $f$ $\in$ PF$_{\text{hon}}^{(q)}$, if there is a fixed string $z_0$ $\in$ $\{0,1\}^*$ such that the following conditions hold.

(i) $\text{dom}(f) = \bigcup_{n=0}^{\infty} \{0,1\}^{q(n)}$.

(ii) For all $n \in \mathbb{N}$, $f(\{0,1\}^{q(n)}) \subseteq \{0,1\}^n \cup \{z_0\}$.

A function $f$ $\in$ Partial-PF is *normal form honest*, and we write $f$ $\in$ PF$_{\text{hon}}^{\text{nf}}$, if $f$ $\in$ PF$_{\text{hon}}^{(q)}$ for some strictly increasing polynomial $q$.

It is easy to see that NP admits the following characterization.

**Theorem 2.1.** For every nonempty language $A \subseteq \{0,1\}^*$, the following conditions are equivalent.

1. $A \in$ NP.
2. $A = \text{range}(f)$ for some $f$ $\in$ PF$_{\text{hon}}$.
3. $A = \text{range}(f)$ for some $f$ $\in$ PF$_{\text{hon}}^{\text{nf}}$.

With this characterization in mind, we define the class $\beta$NP.

**Definition** Let $q$ be a strictly increasing polynomial. A function $f$ $\in$ Partial-PF is *$q$-balanced*, and we write $f$ $\in$ PF$_{\text{bal}}^{(q)}$, if the following conditions hold.
(i) $f \in \text{PF}_{\text{hon}}^{(q)}$.

(ii) For every real number $\alpha < 1$, there exists $n_0 \in \mathbb{N}$ such that, for all $n \geq n_0$ and $x \in \{0, 1\}^{q(n)}$,

$$\left| \left\{ y \in \{0, 1\}^{q(n)} \mid f(y) = f(x) \right\} \right| \leq 2^{q(n) - l^n},$$

where $l = \log |f(\{0, 1\}^{q(n)})|$.

A function $f \in \text{Partial-PF}$ is balanced, and we write $f \in \text{PF}_{\text{bal}}$, if $f \in \text{PF}_{\text{bal}}^{(q)}$ for some strictly increasing polynomial $q$.

Condition (ii), the balancing condition, says that no element of $\text{range}(f)$ has much more than its “fair share” ($= 2^{q(n) - l^n}$) of preimages.

**Definition** The class $\beta \text{NP}$ (“balanced NP”) is defined by

$$\beta \text{NP} = \{ \text{range}(f) \mid f \in \text{PF}_{\text{bal}} \}.$$

It is clear that $\text{PF}_{\text{bal}} \subseteq \text{PF}_{\text{hon}}^{\text{ref}}$, so Theorem 2.1 immediately gives us the following.

**Observation 2.2.** $\beta \text{NP} \subseteq \text{NP}$

It is not clear that $\text{P} \subseteq \beta \text{NP}$. However, it is easy to see that $\beta \text{NP}$ contains all languages that have efficient ranking functions (see [7]). That is, if we let $\rho \text{P}$ be the set of all languages of the form $\text{range}(g)$, where $g \in \text{PF}$ is strictly increasing (with respect to the standard ordering of $\{0, 1\}^*$), then it is clear that $\rho \text{P} \subseteq \text{P}$, and it is easy to see the following.

**Observation 2.3.** $\rho \text{P} \subseteq \beta \text{NP}$

In fact, $\beta \text{NP}$ is a much richer subclass of $\text{NP}$ than Observation 2.3 alone indicates. For example, $\beta \text{NP}$ contains $\text{NP}$-complete languages:

**Proposition 2.4.** $3\text{SAT} \in \beta \text{NP}$

**Corollary 2.5.** The following conditions are equivalent.

1. $\text{P} \neq \text{NP}$.
2. $\beta \text{NP} \not\subseteq \text{P}$.

In the next two sections, we will investigate the consequences of the hypothesis $\mu(\beta \text{NP} \mid E_2) \neq 0$. This is clearly a strong hypothesis in the following sense.

**Observation 2.6.** $\mu(\beta \text{NP} \mid E_2) \neq 0 \implies \mu(\text{NP} \mid E_2) \neq 0 \implies \text{P} \neq \text{NP}$. 

5
3 One-Way Functions With Exponential Security

In this section we define several types of one-way function and prove that, if $\mu(\beta \text{NP} | E_2) \neq 0$, then there exist polynomial time computable functions that are exponentially one-way with exponential security.

One-way functions are functions that are hard to invert. We first define inversion precisely.

**Definition** For $f, g : \{0, 1\}^* \rightarrow \{0, 1\}^*$, $r : \mathbb{N} \rightarrow \mathbb{N}$, and $n \in \mathbb{N}$, we define the following inversion events.

1. $\mathcal{I}[f, g](n) = \{ x \in \{0, 1\}^n \mid f(g(f(x))) = f(x) \}$.
2. $\mathcal{I}_{\text{rand}}[f, g, r](n) = \{ (x, z) \in \Omega_{f, r}(n) \mid f(g(f(x), z)) = f(x) \}$, where $\Omega_{f, r}(n) = \{ (x, z) \mid x \in \{0, 1\}^n \text{ and } z \in \{0, 1\}^{r|f(x)|} \}$.

We interpret $\mathcal{I}[f, g](n)$ and $\mathcal{I}_{\text{rand}}[f, g, r](n)$ as events in the sample spaces $\{0, 1\}^n$ and $\Omega_{f, r}$, respectively, where $\{0, 1\}^n$ has the uniform distribution and each element $(x, z) \in \Omega_{f, r}$ has probability $2^{-|x|-|z|}$. Thus

$$\Pr(\mathcal{I}[f, g](n)) = 2^{-n} : |\mathcal{I}[f, g](n)|$$

and

$$\Pr(\mathcal{I}_{\text{rand}}[f, g, r](n)) = 2^{-n} \sum_{x \in \{0, 1\}^n} 2^{-r|f(x)|} : |\mathcal{I}_{f[x]}|,$$

where each

$$\mathcal{I}_{f[x]} = \{ z \in \{0, 1\}^{r|f(x)|} \mid f(g(f(x), z)) = f(x) \}.$$ 

To clarify the parameters involved, we define the following nine types of one-way function. Note that, in all cases, we require one-way functions to be total, polynomial time computable, and honest.

**Definition** Let $f \in \text{PF}_{\text{hon}}$ and let $t, r : \mathbb{N} \rightarrow \mathbb{N}$.

1. $f$ is *weakly t(n)-one-way* if for every $g \in \text{DTIME}(t)$ there exists $n \in \mathbb{N}$ such that $\Pr(\mathcal{I}[f, g](n)) < 1$.

2. $f$ is *weakly (t(n), r(n))-one-way* if for every $g \in \text{DTIME}(t)$ there exists $n \in \mathbb{N}$ such that $\Pr(\mathcal{I}_{\text{rand}}[f, g, r](n)) < 1$.

3. $f$ is *weakly (t(n)/r(n))-one-way* if for every $g \in \text{DTIME}(t)/\text{ADV}(r)$ there exists $n \in \mathbb{N}$ such that $\Pr(\mathcal{I}[f, g](n)) < 1$.

4. $f$ is *t(n)-one-way with polynomial security* if for all polynomials $q$ and all $g \in \text{DTIME}(t)$, $\Pr(\mathcal{I}[f, g](n)) < \frac{1}{q(n)}$ a.e.
Theorem 3.1. (Allender [1]). \( P \neq NP \) if and only if there exists a weak one-way function.

Using work of Karp and Lipton [16], one can show that the stronger hypothesis \( \Sigma_2^p \neq \Pi_2^p \) implies the existence of functions that are, for all polynomials \( t \) and \( r \), weakly \((t(n)/r(n))\)-one-way (see also [4]), but such functions still do not provide a useful amount of security.
We now come to the main result of this section.

**Theorem 3.2.** If $\mu(\beta \text{NP} | E_2) \neq 0$, then for every polynomial $p$ there is a function that is $(2^{p(n)}/p(n))$-one-way with exponential security.

Immediately from Theorem 3.2, we have:

**Corollary 3.3.** If $\mu(\beta \text{NP} | E_2) \neq 0$, then for every polynomial $p$, there is a function that is $2^{p(n)}$-one-way with exponential security.

Using standard techniques, we can also derive the following from Theorem 3.2.

**Corollary 3.4.** If $\mu(\beta \text{NP} | E_2) \neq 0$, then for every polynomial $p$, there is a function that is $(2^{p(n)}, p(n)\phi)$-one-way with exponential security.

It should be noted that the polynomial $p$ is fixed in Theorem 3.2 and in Corollary 3.4. Thus, for example, Corollary 3.4 tells us that, if $\mu(\beta \text{NP} | E_2) \neq 0$ and $k$ is a large integer, then there is a function $f$ that is $(2^{n^k}, n^k\phi)$-one-way with exponential security, but $f$ depends upon $k$ here. It is conceivable that a polynomial-time adversary, using more than $n^k$ random bits, might invert $f$ with significant probability of success. Note, however, that such an adversary must use more than $n^k$ “truly random” bits. In particular, if the adversary uses a pseudorandom generator, then the seed length must exceed $n^k$.

### 4 BPP-Pairs and Pseudorandom Generators

Yao [27] proved that, if nonuniformly secure pseudorandom generators exist, then $\text{R} \subseteq \bigcap_{c>0} \text{DTIME}(2^{cn})$. Boppana and Hirschfeld [3] subsequently refined Yao’s argument to get the (apparently) stronger conclusion that $\text{BPP} \subseteq \bigcap_{c>0} \text{DTIME}(2^{cn})$. In this section we prove that the hypothesis $\mu(\beta \text{NP} | E_2) \neq 0$ implies a partial converse of this result.

In order to state this converse, we will use Yao, Boppana, and Hirschfeld’s argument to obtain the (apparently) stronger conclusion that the class $\bigcap_{c>0} \text{DTIME}(2^{cn})$ “separates all BPP-pairs.” We first define the relevant notions.

**Definition** A BPP-configuration is an ordered 4-tuple $B = (B, q, \alpha, \beta)$, where $B \in \text{P}$, $q$ is a polynomial, and $0 \leq \alpha < \beta \leq 1$. Given such a configuration $B$, the critical event for a string $x \in \{0, 1\}^*$ is the set

$$B_x = \left\{ y \in \{0, 1\}^{q(|x|)} \mid \langle x, y \rangle \in B \right\},$$

interpreted as an event in the sample space $\{0, 1\}^{q(|x|)}$ with the uniform distribution. (That is, the probability of $B_x$ is $\text{Pr}(B_x) = 2^{-q(|x|)|B_x|}$.) The positive and negative
languages of a BPP-configuration $B = (B, q, \alpha, \beta)$ are the languages

$$B^+ = \{ x \in \{0,1\}^* \mid \Pr(B_x) \geq \beta \},$$

$$B^- = \{ x \in \{0,1\}^* \mid \Pr(B_x) \leq \alpha \},$$

respectively. A BPP-pair is a pair $(A^+, A^-)$ of languages for which there exists a BPP-configuration $B$ such that $A^+ = B^+$ and $A^- = B^-$. The complexity class BPP ("bounded-error probabilistic polynomial time") is defined by

$$\text{BPP} = \{ A \subseteq \{0,1\}^* \mid (A, A^c) \text{ is a BPP-pair} \}.$$

Note: if $(A^+, A^-)$ is a BPP-pair, then $A^+ \cap A^- = \emptyset$. If, in addition, $A^+ \cup A^- = \{0,1\}^*$, then $A^+, A^- \in \text{BPP}$. Using standard techniques [2, 25], it is easy to see that the above definition of BPP is equivalent to standard definitions of BPP.

The class R can be defined similarly.

**Definition** An R-pair is a pair $(B^+, B^-)$ of languages, where $B = (B, q, \alpha, \beta)$ is a BPP-configuration in which $\alpha = 0$. The complexity class R ("randomized polynomial time with one-sided error") is defined by

$$\text{R} = \{ A \subseteq \{0,1\}^* \mid (A, A^c) \text{ is an R-pair} \}.$$

**Definition** A language $C$ separates an ordered pair $(A^+, A^-)$ of languages if $A^+ \subseteq C$ and $A^- \cap C = \emptyset$. A class $C$ of languages separates a pair $(A^+, A^-)$ of languages if there exists $C \in C$ such that $C$ separates $(A^+, A^-)$.

If $C$ is a class of languages that separates every BPP-pair (respectively, every R-pair), then it is clear that $\text{BPP} \subseteq C$ (respectively, $\text{R} \subseteq C$).

We now turn to pseudorandom generators.

**Definition** Let $p$ be a polynomial. A $p(n)$-generator is a function $g \in \text{PF}$ such that $|g(x)| = p(|x|)$ for all $x \in \{0,1\}^*$.

Typically, the polynomial $p(n)$ is much larger than $n$, so that the generator $g$, given a short seed $x$, outputs a long, hopefully pseudorandom, string $g(x)$. The desired notion of pseudorandomness is given by the following definitions, due to Yao [27].

**Definition** A nonuniform test is a language $T \in \text{P/Poly}$. A $p(n)$-generator $g$ passes a nonuniform test $T$ if, for every polynomial $q$,

$$\left| \Pr(g^{-1}(T) = n) - \Pr(T_{=p(n)}) \right| < \frac{1}{q(n)} \text{ a.e.},$$
where the two probabilities are computed according to the uniform distributions on $\{0, 1\}^n$ and $\{0, 1\}^{p(n)}$, respectively.

**Definition.** A *uniform test* is an ordered pair $T = (T, r)$, where $T \in \mathbb{P}$ and $r$ is a polynomial. A $p(n)$-generator $g$ passes a uniform test $T = (T, r)$ if, for every polynomial $q$,

$$\left| \Pr[g(x), z) \in T] - \Pr[(y, z) \in T] \right| < \frac{1}{q(n)} \text{ a.e.}$$

The first probability here is computed according to the uniform distribution on $(x, z) \in \{0, 1\}^n \times \{0, 1\}^{r(p(n))}$. The second probability is computed according to the uniform distribution on $(y, z) \in \{0, 1\}^{p(n)} \times \{0, 1\}^{r(p(n))}$.

**Definition.** A $p(n)$-generator $g$ is *nonuniformly secure* if it passes all nonuniform tests. A $p(n)$-generator $g$ is *uniformly secure* if it passes all uniform tests.

**Definition.** A *nonuniformly secure pseudorandom generator* is a function that is a nonuniformly secure $p(n)$-generator for some polynomial $p(n) \geq n + 1$. A *uniformly secure pseudorandom generator* is a function that is a nonuniformly secure $p(n)$-generator for some polynomial $p(n) \geq n + 1$.

The following well-known result relates pseudorandom generators to the deterministic time complexity of BPP.

**Theorem 4.1.** (Yao[27], Boppana and Hirschfeld[3]). If nonuniformly secure pseudorandom generators exist, then $\text{BPP} \subseteq \bigcap_{k>0} \text{DTIME}(2^{nk})$. \(\square\)

In fact, Yao, Boppana, and Hirschfeld essentially proved the following, perhaps stronger, result. We include the proof for completeness, but emphasize that it is a minor modification of the proof of Theorem 4.1.

**Theorem 4.2.** If nonuniformly secure pseudorandom generators exist, then for all $\epsilon > 0$, $\text{DTIME}(2^n) \text{ separates all BPP-pairs}$. \(\square\)

We now show that the hypothesis $\mu(\beta \text{NP} \mid E_2) \neq 0$ implies a partial converse of Theorem 4.2.

**Theorem 4.3.** If $\mu(\beta \text{NP} \mid E_2) \neq 0$ and $\text{DTIME}(2^n)$ separates all BPP-pairs, then uniformly secure pseudorandom generators exist.

Minor modification of the proof of Theorem 4.3 yields a somewhat stronger result:

**Theorem 4.4.** If $\mu(\beta \text{NP} \mid E_2) \neq 0$ and there is a constant $k$ such that $\text{DTIME}(2^{nk})/\text{ADV}(n^k)$ separates every R-pair, then uniformly secure pseudorandom generators exist.
Acknowledgements

I thank Yaser Abu-Mostafa for his hospitality during a brief visit at Caltech, where part of this paper was written. I also thank Giora Slutzki for helpful discussions.

References


[9] O. Goldreich and S. Micali, reported in [3].


[24] M. Naor. reported in [14].


Optional Appendix

A. Notation and Terminology (for this appendix)
B. Measure and Weak Stochasticity
C. Proofs of Results
A Notation and Terminology

In this paper, \([\psi]\) denotes the Boolean value of the condition \(\psi\), i.e.,

\[
[\psi] = \begin{cases} 
1 & \text{if } \psi \\
0 & \text{if not } \psi 
\end{cases}
\]

All languages here are sets of binary strings, i.e., sets \(A \subseteq \{0,1\}^*\). The complement of a language \(A\) is \(A^c = \{0,1\}^* \setminus A\). We identify each language \(A\) with its characteristic sequence \(\chi_A \in \{0,1\}^\infty\), defined by

\[
\chi_A = [s_0 \in A][s_1 \in A][s_2 \in A]..., 
\]

where \(s_0 = \lambda, s_1 = 0, s_2 = 1, s_3 = 00,\ldots\) is the standard enumeration of \(\{0,1\}^*\). Relying on this identification, the set \(\{0,1\}^\infty\), consisting of all infinite binary sequences, will be regarded as the set of all languages.

If \(w \in \{0,1\}^*\) and \(x \in \{0,1\}^* \cup \{0,1\}^\infty\), we say that \(w\) is a prefix of \(x\), and write \(w \subseteq x\), if \(x = wy\) for some \(y \in \{0,1\}^* \cup \{0,1\}^\infty\). The cylinder generated by a string \(w \in \{0,1\}^*\) is

\[
C_w = \{x \in \{0,1\}^\infty \mid w \subseteq x\}.
\]

Note that \(C_w\) is a set of languages. Note also that \(C_\lambda = \{0,1\}^\infty\), where \(\lambda\) denotes the empty string.

As noted in the introduction, we work with the exponential time complexity class \(E_2 = \text{DTIME}(2^{\text{polynomial}})\). The subscript ‘2’ here distinguishes \(E_2\) from the class \(E = \text{DTIME}(2^{\text{linear}})\). It is well-known that \(P \subseteq E \subsetneq E_2\), that \(P \subseteq \text{NP} \subseteq E_2\) and that \(\text{NP} \neq E\).

We write \(\text{Partial-PF}\) for the set of all polynomial time computable partial functions \(f : \{0,1\}^* \to \{0,1\}^*\). We write \(\text{PF}\) for the set of all \(f \in \text{Partial-PF}\) such that \(\text{dom } (f) = \{0,1\}^*\).

A property \(\Theta(n)\) of natural numbers \(n\) holds almost everywhere (a.e.) if \(\Theta(n)\) is true for all but finitely many \(n\). A property \(\Theta(n)\) holds infinitely often (i.o.) if \(\Theta(n)\) is true for infinitely many \(n\).

We let \(\mathbf{D} = \{m2^{-n} \mid m \in \mathbb{Z}, n \in \mathbb{N}\}\) be the set of dyadic rationals. We also fix a one-to-one pairing function \(\langle, \rangle\) from \(\{0,1\}^* \times \{0,1\}^*\) onto \(\{0,1\}^*\) such that the pairing function and its associated projections, \(\langle x, y \rangle \mapsto x\) and \(\langle x, y \rangle \mapsto y\), are computable in polynomial time.

Several functions in this paper are of the form \(d : \mathbb{N}^k \times \{0,1\}^* \to Y\), where \(Y = \mathbf{D}\) or \([0,\infty)\), the set of nonnegative real numbers. Formally, in order to have uniform criteria for their computational complexities, we regard all such functions as having domain \(\{0,1\}^*\), and codomain \(\{0,1\}^*\) if \(Y = \mathbf{D}\). For example, a function \(d : \mathbb{N}^2 \times \{0,1\}^* \to \mathbf{D}\) is formally interpreted as a function \(\tilde{d} : \{0,1\}^* \to \{0,1\}^*\). Under this interpretation, \(\tilde{d}(i, j, w) = r\) means that \(d((\langle 0^i, 0^j, w \rangle)) = u\), where \(u\) is a suitable binary encoding of the dyadic rational \(r\). Similarly, a function \(m : \mathbb{N}^k \to \mathbb{N}\)
is formally interpreted as a function \( \tilde{m} : \{0,1\}^* \to \{0,1\}^* \), with inputs and outputs represented in unary. Thus \( m(i,j) = n \) means that \( \tilde{m}(\langle 0^i,0^j \rangle) = 0^n \).

For a function \( d : \mathbb{N} \times X \to Y \) and \( k \in \mathbb{N} \), we define the function \( d_k : X \to Y \) by \( d_k(x) = d(k,x) = d(\langle 0^k, x \rangle) \). We then regard \( d \) as a “uniform enumeration” of the functions \( d_0, d_1, d_2, \ldots \). For a function \( d : \mathbb{N}^n \times X \to Y \) \((n \geq 2)\), we write \( d_{k,l} = (d_k)_l \), etc.

For a function \( \delta : \{0,1\}^* \to \{0,1\}^* \) and \( n \in \mathbb{N} \), we write \( \delta^n \) for the \( n \)-fold composition of \( \delta \) with itself.

Our proof of the Weak Stochasticity Theorem in appendix B uses the following form of the Chernoff bound.

**Lemma A.1**[5, 12]. If \( X_1, \ldots, X_N \) are independent 0-1-valued random variables with the uniform distribution, \( S = X_1 + \ldots + X_N \), and \( \epsilon > 0 \), then

\[
\Pr \left[ \left| S - \frac{N}{2} \right| \geq \frac{\epsilon N}{2} \right] \leq 2e^{-\frac{\epsilon^2 N}{6}}.
\]

**Proof.** See [12]. \( \square \)
B Measure and Weak Stochasticity

In this section we review some fundamentals of measure in $E_2$ and prove the Weak Stochasticity Theorem. This theorem will be useful in the proof of our main results in sections 3 and 4. We also expect it to be useful in future investigations of the measure structure of $E_2$.

Resource-bounded measure [19, 20] is a very general theory whose special cases include classical Lebesgue measure, the measure structure of the class REC of all recursive languages, and measure in various complexity classes. In this paper we are interested only in measure in $E_2$, so our discussion of measure is specific to this class.

Throughout this section, we identify every language $A \subseteq \{0, 1\}^*$ with its characteristic sequence $\chi_A \in \{0, 1\}^\infty$, defined as in appendix A.

A constructor is a function $\delta : \{0, 1\}^* \rightarrow \{0, 1\}^*$ such that $x \leq \delta(x)$ for all $x \in \{0, 1\}^*$. The result of a constructor $\delta$ (i.e., the language constructed by $\delta$) is the unique language $R(\delta)$ such that $\delta^n(\lambda) \subseteq R(\delta)$ for all $n \in \mathbb{N}$. Intuitively, $\delta$ constructs $R(\delta)$ by starting with $\lambda$ and then iteratively generating successively longer prefixes of $R(\delta)$.

We first note that $E_2$ can be characterized in terms of constructors.

**Notation.** The class $p_2$, consisting of functions $f : \{0, 1\}^* \rightarrow \{0, 1\}^*$, is defined as follows.

$$p_2 = \{ f | f \text{ is computable is } n(\log n)^{O(1)} \text{ time} \}$$

**Lemma B.1.** [18]

$$E_2 = \{ R(\delta) | \delta \in p_2 \text{ and } \delta \text{ is a constructor} \}.$$  

Using Lemma B.1, the measure structure of $E_2$ is now developed in terms of the class $p_2$.

**Definition** A density function is a function $d : \{0, 1\}^* \rightarrow [0, \infty)$ satisfying

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

for all $w \in \{0, 1\}^*$. The global value of a density function $d$ is $d(\lambda)$. The set covered by a density function $d$ is

$$S[d] = \bigcup_{w \in \{0, 1\}^*} \{ x \mid w \subseteq x \} \text{ where } w \subseteq x \text{ is the cylinder generated by } w.$$  

(Recall that $C_w = \{ x \in \{0, 1\}^\infty \mid w \subseteq x \} \text{ is the cylinder generated by } w$.) A density function $d$ covers a set $X \subseteq \{0, 1\}^\infty$ if $X \subseteq S[d]$.  

B-1
For all density functions in this paper, equality actually holds in (B.1) above, but this is not required.

Consider the random experiment in which a sequence \( x \in \{0, 1\}^\infty \) is chosen by using an independent toss of a fair coin to decide each bit of \( x \). Taken together, (B.1) and (B.2) imply that \( \Pr[x \in S[d]] \leq d(\lambda) \) in this experiment. Intuitively, we regard a density function \( d \) as a “detailed verification” that \( \Pr[x \in X] \leq d(\lambda) \) for all sets \( X \subseteq S[d] \).

More generally, we will be interested in “uniform systems” of density functions that are computable within some resource bound.

**Definition** An \( n \)-dimensional density system (\( n \)-DS) is a function

\[
d : \mathbb{N}^n \times \{0, 1\}^* \to [0, \infty)
\]

such that \( d_{\vec{k}} \) is a density function for every \( \vec{k} \in \mathbb{N}^n \). It is sometimes convenient to regard a density function as a 0-DS.

**Definition** A computation of an \( n \)-DS \( d \) is a function \( \hat{d} : \mathbb{N}^{n+1} \times \{0, 1\}^* \to \mathbb{D} \) such that

\[
\left| \hat{d}_{\vec{k}, r}(w) - d_{\vec{k}}(w) \right| \leq 2^{-r}
\]

for all \( \vec{k} \in \mathbb{N}^n, r \in \mathbb{N}, \) and \( w \in \{0, 1\}^* \). A \( p_2 \)-computation of an \( n \)-DS \( d \) is a computation \( \hat{d} \) of \( d \) such that \( \hat{d} \in p_2 \). An \( n \)-DS \( d \) is \( p_2 \)-computable if there exists a \( p_2 \)-computation \( \hat{d} \) of \( d \).

If \( d \) is an \( n \)-DS such that \( d : \mathbb{N}^n \times \{0, 1\}^* \to \mathbb{D} \) and \( d \in p_2 \), then \( d \) is trivially \( p_2 \)-computable. This fortunate circumstance, in which there is no need to compute approximations, occurs frequently in practice. In any case, we will sometimes abuse notation by writing \( d \) for \( \hat{d} \), relying on context and subscripts to distinguish an \( n \)-DS \( d \) from a computation \( \hat{d} \) of \( d \).

We now come to the key idea of resource-bounded measure theory.

**Definition** A null cover of a set \( X \subseteq \{0, 1\}^\infty \) is a 1-DS \( d \) such that, for all \( k \in \mathbb{N} \), \( d_k \) covers \( X \) with global value \( d_k(\lambda) \leq 2^{-k} \). A \( p_2 \)-null cover of \( X \) is a null cover of \( X \) that is \( p_2 \)-computable.

In other words, a null cover of \( X \) is a uniform system of density functions that cover \( X \) with rapidly vanishing global value. It is easy to show that a set \( X \subseteq \{0, 1\}^\infty \) has classical Lebesgue measure 0 (i.e., probability 0 in the above coin-tossing experiment) if and only if there exists a null cover of \( X \).

**Definition** A set \( X \) has \( p_2 \)-measure 0, and we write \( \mu_{p_2}(X) = 0 \), if there exists a \( p_2 \)-null cover of \( X \). A set \( X \) has \( p_2 \)-measure 1, and we write \( \mu_{p_2}(X) = 1 \), if \( \mu_{p_2}(X^c) = 0 \).
Thus a set $X$ has $p_2$-measure 0 if $p_2$ provides sufficient computational resources to compute uniformly good approximations to a system of density functions that cover $X$ with rapidly vanishing global value.

We now turn to the internal measure structure of $E_2$.

**Definition** A set $X$ has measure 0 in $E_2$, and we write $\mu(X \mid E_2) = 0$, if $\mu_{p_2}(X \cap E_2) = 0$. A set $X$ has measure 1 in $E_2$, and we write $\mu(X \mid E_2) = 1$, if $\mu(X^c \mid E_2) = 0$. If $\mu(X \mid E_2) = 1$, we say that almost every language in $E_2$ is in $X$.

The following lemma is obvious but useful.

**Lemma B.2.** For every set $X \subseteq \{0, 1\}^\infty$,

\[
\mu_{p_2}(X) = 0 \quad \implies \quad \Pr[x \in X] = 0
\]

\[
\mu(X \mid E_2) = 0
\]

and

\[
\mu_{p_2}(X) = 1 \quad \implies \quad \Pr[x \in X] = 1
\]

\[
\mu(X \mid E_2) = 1,
\]

where the probability $\Pr[x \in X]$ is computed according to the random experiment in which a sequence $x \in \{0, 1\}^\infty$ is chosen probabilistically, using an independent toss of a fair coin to decide each bit of $x$.

Thus a proof that a set $X$ has $p_2$-measure 0 gives information about the size of $X$ in $E_2$ and in $\{0, 1\}^\infty$.

It is shown in [19] that these definitions endow $E_2$ with internal measure structure. Specifically, if $\mathcal{I}$ is either the collection $\mathcal{I}_{p_2}$ of all $p_2$-measure 0 sets or the collection $\mathcal{I}_{E_2}$ of all sets of measure 0 in $E_2$, then $\mathcal{I}$ is a “$p_2$-ideal”, i.e., is closed under subsets, finite unions, and “$p_2$-unions” (countable unions that can be generated within the resources of $p_2$). More importantly, it is shown that the ideal $\mathcal{I}_{E_2}$ is a proper ideal, i.e., that $E_2$ does not have measure 0 in $E_2$. Taken together, these facts justify the intuition that, if $\mu(X \mid E_2) = 0$, then $X \cap E_2$ is a negligibly small subset of $E_2$.

Our proof of the Weak Stochasticity Theorem does not directly use the above definitions. Instead we use a sufficient condition, proved in [19], for a set to have measure 0. To state this condition we need a $p_2$ notion of convergence for infinite series. All our series here consist of nonnegative terms. A *modulus* for a series $\sum_{n=0}^{\infty} a_n$ is a function $m : \mathbb{N} \to \mathbb{N}$ such that

\[
\sum_{n=m(j)}^{\infty} a_n \leq 2^{-j}
\]
for all $j \in \mathbb{N}$. A series is $p_2$-convergent if it has a modulus $m \in p_2$. A sequence
\[ \sum_{k=0}^{\infty} a_{j,k} \quad (j = 0, 1, 2, \ldots) \]
of series is uniformly $p$-convergent if there exists a function $m : \mathbb{N}^2 \to \mathbb{N}$ such that $m \in p_2$ and, for each $j \in \mathbb{N}$, $m_j$ is a modulus for the series $\sum_{k=0}^{\infty} a_{j,k}$. We will use the following sufficient condition for uniform $p_2$-convergence. (This lemma is verified by routine calculus.)

**Lemma B.3.** Let $a_{j,k} \in [0, \infty)$ for all $j, k \in \mathbb{N}$. If there exist a real $\varepsilon > 0$ and a function $h : \mathbb{N} \to \mathbb{N}$ such that $h \in p_2$ and $a_{j,k} \leq e^{-e^{(lnk)^\varepsilon}}$ for all $j, k \in \mathbb{N}$ with $k \geq h(j)$, then the series
\[ \sum_{k=0}^{\infty} a_{j,k} \quad (j = 0, 1, 2, \ldots) \]
are uniformly $p_2$-convergent.

The proof of the Weak Stochasticity Theorem is greatly simplified by using the following special case (for $p_2$) of a uniform, resource-bounded generalization of the classical first Borel-Cantelli lemma.

**Lemma B.4.***[19]. If $d$ is a $p_2$-computable 2-DS such that the series
\[ \sum_{k=0}^{\infty} d_{j,k}(\lambda) \quad (j = 0, 1, 2, \ldots) \]
are uniformly $p_2$-convergent, then
\[ \mu_{p_2} \left( \bigcup_{t=0}^{\infty} \bigcap_{k=t}^{\infty} S[d_{j,k}] \right) = 0. \]

If we write $S_j = \bigcap_{t=0}^{\infty} \bigcup_{k=t}^{\infty} S[d_{j,k}]$ and $S = \bigcup_{j=0}^{\infty} S_j$, then Lemma B.4 gives a sufficient condition for concluding that $S$ has $p_2$-measure 0. Note that each $S_j$ consists of those languages $A$ that are in infinitely many of the sets $S[d_{j,k}]$.

We now formulate our notion of weak stochasticity. For this we need a few definitions. Our notion of advice classes is standard [16]. An advice function is a function $h : \mathbb{N} \to \{0, 1\}^*$. Given a function $q : \mathbb{N} \to \mathbb{N}$, we write $\text{ADV}(q)$ for the set of all advice functions $h$ such that $|h(n)| \leq q(n)$ for all $n \in \mathbb{N}$. Given a language $A \subseteq \{0, 1\}^*$ and an advice function $h$, we define the language $A/h$ (“$A$ with advice $h$”) by
\[ A/h = \{ x \in \{0, 1\}^* \mid \langle x, h(|x|) \rangle \in A \}. \]
Given functions $t,q : \mathbb{N} \to \mathbb{N}$, we define the advice class

$$\text{DTIME}(t)/\text{ADV}(q) = \{A/h \mid A \in \text{DTIME}(t), h \in \text{ADV}(q)\}.$$ 

We now define our notion of weak stochasticity. Let $t,q,\nu : \mathbb{N} \to \mathbb{N}$ and let $A \subseteq \{0,1\}^*$. Then $A$ is weakly $(t,q,\nu)$-stochastic if, for all $B,C \in \text{DTIME}(t)/\text{ADV}(q)$ such that $|C_n| \geq \nu(n)$ for all sufficiently large $n$,

$$\lim_{n \to \infty} \frac{|(A \triangle B) \cap C_n|}{|C_n|} = \frac{1}{2}.$$ 

Intuitively, $B$ and $C$ together form a “prediction scheme” in which $B$ tries to guess the behavior of $A$ on the set $C$. $A$ is weakly $(t,q,\nu)$-stochastic if no such scheme is better in the limit than guessing by random tosses of a fair coin. (This definition is slightly stronger than the weak stochasticity defined in [22], in that the language $C$ is allowed advice here.)

Let $\text{WS}(t,q,\nu)$ denote the set of all languages that are weakly $(t,q,\nu)$-stochastic.

The following theorem is a minor variation of a result of [22] on the weak stochasticity of almost every language in $E$. We include a proof for completeness of exposition.

**Theorem B.5.** (Weak Stochasticity Theorem [22]). For every fixed polynomial $p$ and every fixed real number $\gamma > 0$,

$$\mu(\text{WS}(2^p, p(n), 2^n\gamma) \mid E_2) = 1.$$ 

**Proof.** Let $\text{WS} = \text{WS}(2^p, p(n), 2^n\gamma)$, where $p$ is a polynomial and $\gamma$ is a positive real. It suffices to prove that $\mu_{p_i}(\text{WS}^c) = 0$, where $\text{WS}^c$ is the complement of $\text{WS}$.

Let $U \in \text{DTIME}(2^{p(n)})$ be a language that is universal for $\text{DTIME}(2^{p(n)}) \times \text{DTIME}(2^{p(n)})$ in the following sense: for each $i \in \mathbb{N}$, let

$$C_i = \{x \in \{0,1\}^* \mid \langle 0^i,0x \rangle \in U \},$$

$$D_i = \{x \in \{0,1\}^* \mid \langle 0^i,1x \rangle \in U \}.$$ 

Then $\text{DTIME}(2^{p(n)}) \times \text{DTIME}(2^{p(n)}) = \{(C_i,D_i) \mid i \in \mathbb{N}\}$.

For all $i,j,k \in \mathbb{N}$, define the set $Y_{i,j,k}$ of languages as follows. If $k$ is not a power of 2, then $Y_{i,j,k} = \emptyset$. Otherwise, if $k = 2^n$, where $n \in \mathbb{N}$, then

$$Y_{i,j,k} = \bigcup_{y,z \in \{0,1\} \leq p(n)} Y_{i,j,k,y,z},$$

where each
It is immediate from the definition of weak stochasticity that
\[ WS^c \subseteq \bigcup_{i=0}^{\infty} \bigcup_{j=0}^{\infty} \bigcap_{m=0}^{\infty} \bigcup_{k=m}^{\infty} Y_{i,j,k}. \]

Thus, by Lemma B.4, it suffices to exhibit a p_2-computable 3-DS \( d \) with the following two properties.

(I) The series \( \sum_{k=0}^{\infty} d_{i,j,k}(\lambda) \), for \( i, j \in \mathbb{N} \), are uniformly p_2-convergent.

(II) For all \( i, j, k \in \mathbb{N} \), \( Y_{i,j,k} \subseteq S[d_{i,j,k}] \).

Define the function \( d : \mathbb{N}^3 \times \{0, 1\}^* \to [0, \infty) \) as follows. If \( k \) is not a power of 2, then \( d_{i,j,k}(w) = 0 \). Otherwise, if \( k = 2^n \), where \( n \in \mathbb{N} \), then
\[ d_{i,j,k}(w) = \sum_{y,z \in \{0, 1\}^{\leq 2^n}} \Pr(Y_{i,j,k,y,z} | C_w), \]
where the conditional probabilities
\[ \Pr(Y_{i,j,k,y,z} | C_w) = \Pr[A \in Y_{i,j,k,y,z} | A \in C_w] \]
are computed according to the random experiment in which a language \( A \subseteq \{0, 1\}^* \) is chosen probabilistically, using an independent toss of a fair coin to decide membership of each string in \( A \).

It follows immediately from the definition of conditional probability that \( d \) is a 3-DS. Since \( U \in \text{DTIME}(2^{n^p(n)}) \) and \( \gamma \) is fixed, we can use binomial coefficients to (exactly) compute \( d_{i,j,k}(w) \) in time that is \( p_2 \) in \( i + j + k + |w| \). (Note that if \( k = 2^n \), then \( 2^{n^p(n)} = k^{(\log k)^{\Theta(1)}} \). Thus \( d \) is \( p_2 \)-computable.

To see that \( d \) has property (I), note first that Lemma A.1, the Chernoff bound, tells us that, for all \( i, j, n \in \mathbb{N} \) and \( y, z \in \{0, 1\}^{\leq p(n)} \) (writing \( k = 2^n \), \( N = 2^{n^\gamma} = 2^{(\log k)^\gamma} \), and \( \epsilon = \frac{2}{j+1} \)),
\[ \Pr(Y_{i,j,k,y,z}) \leq 2e^{-\frac{j^2 N}{6}} < 2e^{-\frac{N}{2(j+1)^2}}, \]
whence
\[ d_{i,j,k}(\lambda) = \sum_{y,z \in \{0, 1\}^{\leq p(n)}} \Pr(Y_{i,j,k,y,z}) \]
\[ < \left( 2^{p(n)+1} \right)^2 \cdot 2e^{-\frac{N}{2(j+1)^2}} \]
\[ < 2^{p(n)+3-\frac{N}{2(j+1)^2}}. \]
Let $\delta = \frac{\gamma}{3}$, $a = \lceil \frac{1}{\delta} \rceil$, and fix $n_0 \in \mathbb{N}$ such that
\[ n^{3\delta} \geq n^{2\delta} + n^\delta \quad \text{and} \quad 2^{n^{2\delta}} \geq e^{(n \ln 2)^\delta} + 2p(n) + 3 \]
for all $n \geq n_0$. Define $h : \mathbb{N} \to \mathbb{N}$ by
\[ h(j) = 2^{n_0} + 2^{(1+2\log(j+1))a}. \]
It is clear that $h \in p_2$. For all $i, j, k, n \in \mathbb{N}$ with $k = 2^n$ (still writing $N = 2^{n^\gamma} = 2^{n^{2\delta}}$), we have
\[ k \geq 2^{n_0} \implies 2^{n^{2\delta}} \geq e^{(\ln k)^\delta} + 2p(n) + 3 \]
and
\[ k \geq 2^{(1+2\log(j+1))a} \implies n^\delta \geq 1 + 2 \log(j + 1) \implies 2^n \geq 2(j + 1)^2, \]
so
\[ k \geq h(j) \implies N = 2^{n^{2\delta}} \geq 2^{n^\delta} \cdot 2^{n^{2\delta}} \geq 2(j + 1)^2 \left[ e^{(\ln k)^\delta} + 2p(n) + 3 \right] \implies 2p(n) + 3 - \frac{N}{2(j + 1)^2} \leq -e^{(\ln k)^\delta} \implies d_{i,j,k}(\lambda) \leq e^{-e^{6n \gamma}}. \]

Since $\delta > 0$, it follows by Lemma B.3 that (I) holds.

Finally, to see that (II) holds, fix $i, j, k \in \mathbb{N}$. If $k$ is not a power of 2, then (II) is trivially affirmed, so assume that $k = 2^n$, where $n \in \mathbb{N}$. Let $A \in Y_{i,j,k}$. Fix $y, z \in \{0, 1\}^{p(n)}$ such that $A \in Y_{i,j,k,y,z}$ and let $w$ be the $(2^{n+1} - 1)$-bit characteristic string of $A_{\leq n}$. Then
\[ d_{i,j,k}(w) \geq \Pr(Y_{i,j,k,y,z} \mid C_w) = 1, \]
so $A \in C_w \subseteq S[d_{i,j,k}]$. This completes the proof. \qed

B-7
C Proofs of Results

Proof of Theorem 2.1.
(3)$\implies$(2). Assume (3). Fix a strictly increasing polynomial $q$ and string $z_0$ testifying that $f \in \text{PF}_{\text{mon}}$. Define $g : \{0, 1\}^* \to \{0, 1\}^*$ by
\[ g(x) = \begin{cases} f(x) & \text{if } |x| \in \text{range}(q) \\ z_0 & \text{if } |x| \not\in \text{range}(q). \end{cases} \]
Then $g \in \text{PF}_{\text{mon}}$ and range($g$) = range($f$) = $A$, so (2) holds.

(2)$\implies$(1). Assume that $A = \text{range}(f)$, where $f \in \text{PF}$ and the polynomial $q$ testifies that $f$ is honest. Let $B = \{ (y,x) \mid f(x) = y \}$. Then $B \in \text{P}$ and $A = \exists^p B$, so $A \in \text{NP}$.

(1)$\implies$(3). Assume that $A = \exists^p B \in \text{NP}$, where $B \in \text{P}$ and $p$ is a strictly increasing polynomial. Since $A$ is nonempty, we can fix a string $z_0 \in A$. Let $q(n) = 2n + p(n) + 3$. (This polynomial has the property that, if $|a| = n$ and $|v| + i = p(n)$, then $|a, v10^i| = q(n)$.) Let $D = \bigcup_{n=0}^{\infty} \{0, 1\}^q(n)$ and define $f : D \to \{0, 1\}^*$ as follows. Let $x \in \{0, 1\}^q(n)$. If $x$ is of the form $x = \langle u, v10^{|v|} \rangle$, where $|u| = n$ and $\langle u, v \rangle \in B$, then $f(x) = u$; otherwise, $f(x) = z_0$. It is clear that $f \in \text{PF}_{\text{mon}}^q$ and range($f$) = $A$, so (3) holds.

Proof of Proposition 2.4. Fix a sequence $v_1, v_2, \ldots$ of Boolean variables. For each positive integer $m$, let $V_m = \{ v_1, \ldots, v_m \}$, let $A_m$ be the set of all truth assignments $a : V_m \to \{0, 1\}$, and let $3\text{CNF}_m$ be the set of all $m$-fold conjunctions of 3-clauses over $V_m$, encoded as strings in $\{0, 1\}^{p(m)}$, where $p$ is a suitable, strictly increasing polynomial. (There are $8 \binom{m}{3}$ such 3-clauses over $V_m$, so $|3\text{CNF}_m| = 8^m \binom{m}{3}^m$.) Extend each $a \in A_m$ to a function $a : 3\text{CNF}_m \to \{0, 1\}$ in the obvious way and let
\[ 3\text{SAT}_m = \{ \psi \in 3\text{CNF}_m \mid (\exists a \in A_m) a(\psi) = 1 \}. \]
For simplicity, we consider $3\text{SAT}$ as having the form
\[ 3\text{SAT} = \bigcup_{m=1}^{\infty} 3\text{SAT}_m. \]
For each positive integer $m$ and each $a \in A_m$, define the set
\[ T_m(a) = \{ \psi \in 3\text{CNF}_m \mid a(\psi) = 1 \}, \]
consisting of all $3\text{CNF}_m$ formulas that are true under the assignment $a$. Then define the sets
\[ T_m = \bigcup_{a \in A_m} (\{a\} \times T_m(a)), \]
\[ T = \bigcup_{m=1}^{\infty} T_m, \]
where each pair \((a, \psi) \in T_m\) is encoded as a string in \(\{0, 1\}^{q(p(m))}\) for some suitable, strictly increasing polynomial \(q\). Note that \(T\) is the set of all ordered pairs \((a, \psi)\) such that \(a\) is a truth assignment, \(\psi\) is a 3CNF formula, and \(\psi\) is true under \(a\). Note also that, for each \(m\) and \(a\), we have

\[ |T_m(a)| = \tau^m \left( \frac{m}{3} \right)^m, \]

so

\[ |T_m| = \tau^m \left( \frac{m}{3} \right)^m \quad |A_m| = 14^m \left( \frac{m}{3} \right)^m. \]

For each positive integer \(m\), let \(w_1^{(m)}, \ldots, w_t^{(m)}\) be the lexicographic enumeration of \(\{0, 1\}^{q(p(m))}\) and let \(y_1^{(m)}, \ldots, y_d^{(m)}\) be the lexicographic enumeration of \(T_m\). (The elements \((a, \psi)\) of \(T_m\) are enumerated first in order of \(a\), then in order of \(\psi\). Note that \(t = 2q(p(m))\) and \(d = 14^m \left( \frac{m}{3} \right)^m \leq t\).) Then define the finite function \(g_m : \{0, 1\}^{q(p(m))} \xrightarrow{\text{onto}} T_m\) by

\[ g_m(w_k^{(m)}) = y_r^{(m)} \]

for all \(1 \leq k \leq t\), where \(r\) is the remainder obtained when \(k\) is divided by \(d\). Define the function \(h : T \xrightarrow{\text{onto}} 3\text{SAT}\) by

\[ h(a, \psi) = \psi. \]

Finally, let \(D = \cup_{n=0}^{\infty} \{0, 1\}^{q(n)}\), fix a string \(\psi_0 \in 3\text{SAT}\), and define the function \(f : D \rightarrow 3\text{SAT}\) by

\[ f(x) = \begin{cases} h(g_m(x)) & \text{if } |x| = q(p(m)) \\ \psi_0 & \text{if } |x| \in \text{range}(q) \setminus \text{range}(q \circ p). \end{cases} \]

Since the elements \((a, \psi)\) of \(T_m\) can easily be counted and enumerated (first in order of \(a\), then in order of \(\psi\)), it is clear that \(f\) is computable in polynomial time. In fact, it is clear that \(f \in \text{PF}_{\text{lin}}^{\psi(q)}\) and \(\text{range}(f) = 3\text{SAT}\). To finish the proof that \(3\text{SAT} \in \text{\#NP}\), then, it suffices to show that \(f\) satisfies the balancing condition, so that \(f \in \text{PF}_{\text{lin}}^{\psi(q)}\).

To see that \(f\) satisfies the balancing condition, fix a real number \(\alpha < 1\). Given \(n > |\psi_0|, \) let \(l = \log |f(\{0, 1\}^{q(n)})|\). We have two cases.

**Case I.** \(n = p(m)\) for some positive integer \(m\). Let \(x \in \{0, 1\}^{q(n)}, \psi = f(x), \) and \(s = \left\lceil \frac{2^{q(n)}}{|T_m|} \right\rceil\). If \(n\) is sufficiently large, then

\[
\left| \left\{ y \in \{0, 1\}^{q(n)} \mid f(y) = f(x) \right\} \right| \leq s \cdot |h^{-1}(\psi)| \cdot 2^{q(n)} \leq s \cdot |A_m| \cdot |3\text{CNF}_m|^{\alpha} \cdot 2^{q(n)} < \frac{2}{|T_m|} \cdot |A_m| \cdot |3\text{CNF}_m|^{\alpha}
\]

C-2
\[ = 2 \cdot \left( \frac{8^a}{7 \cdot 3} \right)^{a-1} \]

Since \( \frac{8^a}{7 \cdot 3} \to 0 \) as \( m \to \infty \), it follows that

\[
\left| \left\{ y \in \{0, 1\}^{q(n)} \mid f(y) = f(x) \right\} \right| \leq 2^{q(n) - n}
\]

for all \( x \in \{0, 1\}^{q(n)} \), for all sufficiently large \( n \), affirming the balancing condition.

Case II. \( n \not\in \text{range}(p) \). Then

\[ f(\{0, 1\}^{q(n)}) = \{\psi_0\}, \]

so \( l = \log 1 = 0 \), so for all \( x \in \{0, 1\}^{q(n)} \),

\[
\left| \left\{ y \in \{0, 1\}^{q(n)} \mid f(y) = f(x) \right\} \right| \leq 2^{q(n)} = 2^{q(n) - n},
\]

again affirming the balancing condition.

We have now shown that \( f \in \text{PF}^{[q]}_{\text{log1}} \), whence \( 3\text{SAT} = \text{range}(f) \in \beta\text{NP} \).

The following lemma will simplify our proof of Theorem 3.2.

**Lemma C.1.** Assume that there exist a strictly increasing polynomial \( q \) and a function \( f \in \text{PF}^{[q]}_{\text{log1}} \) with the following property.

\( (*) \) For every \( g \in \text{DTIME}(t) / \text{ADV}(r) \) satisfying \( |g(y)| = q(|y|) \) for all \( y \in \{0, 1\}^* \),

there is a real number \( \epsilon > 0 \) such that

\[ \Pr(I[f, g](q(n))) < 2^{-q(n)^\epsilon} \text{ a.e.} \]

Then there exists a function that is \((t(n)/r(n))-\text{one-way with exponential security}.

**Proof.** Assume the hypothesis and define \( \tilde{f} : \{0, 1\}^* \to \{0, 1\}^* \) as follows. Let \( x \in \{0, 1\}^* \). If \( |x| < q(0) \), let \( \tilde{f}(x) = \lambda \). If \( |x| \geq q(0) \), let \( n_x \) be the greatest integer such that \( q(n_x) \leq |x| \), and let \( \tilde{f}(x) = f(x[0..q(n_x) - 1]) \). It is clear that \( \tilde{f} \in \text{PF}_{\text{log1}} \). To see that \( \tilde{f} \) is \((t(n)/r(n))-\text{one-way with exponential security} \), let \( \tilde{g} \in \text{DTIME}(t) / \text{ADV}(r) \). Define \( g : \{0, 1\}^* \to \{0, 1\}^* \) by

\[
g(y) = \begin{cases} 
\tilde{g}(y)[0..q(|y|) - 1] & \text{if } |\tilde{g}(y)| \geq q(|y|) \\
\text{0}^{|y|} & \text{if } |\tilde{g}(y)| < q(|y|).
\end{cases}
\]

Then \( g \in \text{DTIME}(t) / \text{ADV}(r) \) and \( |g(y)| = q(|y|) \) for all \( y \in \{0, 1\}^* \). It follows by assumption \( (*) \) that there is a real number \( \epsilon > 0 \) such that

\[ \Pr(I[f, g](q(n))) < 2^{-q(n)^\epsilon} \text{ a.e.} \]
Now assume for a moment that \( x \in \mathcal{I}[f, \tilde{g}](m) \), where \( m \geq q(0) \). Define \( n_x \) as above and write \( x = uv \), where \( |u| = q(n_x) \). Then \( \tilde{f}(\tilde{g}(\tilde{f}(x))) = \tilde{f}(x) \), so \( |\tilde{g}(\tilde{f}(x))| \geq q(\lfloor \tilde{f}(x) \rfloor) \), so \( \tilde{g}(\tilde{f}(x)) = \tilde{g}(\tilde{f}(x))[0..q(\lfloor \tilde{f}(x) \rfloor) - 1] = \tilde{g}(\tilde{f}(x))[0..q(n_x) - 1] \), so

\[
\begin{align*}
  f(g(f(u))) &= f(g(\tilde{f}(x))) \\
  &= f(\tilde{g}(\tilde{f}(x))[0..q(n_x) - 1]) \\
  &= f(\tilde{g}(\tilde{f}(x))) \\
  &= f(\tilde{f}(x)) \\
  &= f(u),
\end{align*}
\]

so \( u \in \mathcal{I}[f, g](q(n_x)) \). This argument shows that

\[
\Pr(\mathcal{I}[f, \tilde{g}](m)) \leq \Pr(\mathcal{I}[f, g](q(n_m)))
\]

for all \( m \geq q(0) \), where \( n_m \) is the greatest integer such that \( q(n_m) \leq m \). Now \( q \) is a polynomial, so for all sufficiently large \( m \),

\[
q(n_m) \leq m < q(n_m + 1) < q(n_m)^2.
\]

For all sufficiently large \( m \), we now have

\[
\Pr(\mathcal{I}[\tilde{f}, \tilde{g}](m)) \leq \Pr(\mathcal{I}[f, g](q(n_m))) < 2^{-q(n_m)^r} < 2^{-m^{r/2}}.
\]

Thus \( \tilde{f} \) is \((t(n)/r(n))\)-one-way with exponential security.

\[\square\]

**Proof of Theorem 3.2.** Let \( p \) be a polynomial and assume that there is no function that is \((2^{p(n)}/p(n))\)-one-way with exponential security. It suffices to prove that \( \mu(\betaNP \mid \mathcal{E}_2) = 0 \).

Let \( A \in \betaNP \). Fix a strictly increasing polynomial \( q \) and a function \( f \in \mathcal{PF}_{bal}^{[q]} \) such that \( A = \text{range}(f) \). Let \( \epsilon = \frac{1}{2^{\deg(q)}} \). Since there is no function that is \((2^{p(n)}/p(n))\)-one-way with exponential security, Lemma C.1 tells us that there is a function \( g \in \text{DTIME}(2^{p(n)}) \)/ADV \((p(n))\) such that the set

\[
I = \{ n \in \mathbb{N} \mid \Pr(\mathcal{I}[f, g](q(n))) \geq 2^{-q(n)^r} \}
\]

is infinite and \( |g(y)| = q(|y|) \) for all \( y \in \{0, 1\}^* \).

We now have two cases.

**Case I.** \( 2^{-n} |A_{=n}| \rightarrow \frac{1}{2} \) as \( n \rightarrow \infty \). Then fix \( n_0 \in \mathbb{N} \) such that the following conditions hold for all \( n \geq n_0 \).

(i) \( |A_{=n}| \geq 2^{n-2} \).
(ii) \( q(n)^c \leq n^{5/8} \).

(iii) \((n-2)^3/4 \geq n^{5/8} + n^{1/2} \).

(iv) For all \( x \in \{0,1\}^{q(n)} \),

\[
\left| \left\{ y \in \{0,1\}^{q(n)} \mid f(y) = f(x) \right\} \right| \leq 2^{q(n) - l^{3/4}},
\]

where \( l = \log|f(\{0,1\}^{q(n)})| \).

(Note that we are using the fact that \( f \in \mathbb{P}^{(q)} \text{AL} \) here.) Let

\[ J = \{ n \in I \mid n \geq n_0 \} \]

and note that \( J \) is infinite. Define a language \( C \subseteq \{0,1\}^* \) as follows: For \( n \in \mathbb{N} \), if \( |f(\mathbb{I}[f,g](q(n)))| \geq 2^{\sqrt{n}} \), then \( C_n = f(\mathbb{I}[f,g](q(n))) \). Otherwise, \( C_n = \{0,1\}^n \). Note that \( |C_n| \geq 2^{\sqrt{n}} \) for all \( n \in \mathbb{N} \). Also, since \( f \in \mathbb{P}^{(q)} \text{AL} \) and \( g \in \text{DTIME}(2^{p(n)})/\text{ADV}(p(n)) \), it is clear that \( C \in \text{DTIME}(2^{p(n) + 2n})/\text{ADV}(p(n)) \). To decide membership in \( C_n \), we check the condition \( f(g(y)) = y \) for each \( y \in \{0,1\}^n \).

For all \( n \in J \), letting

\[ l = \log|f(\{0,1\}^{q(n)})| = \log|A_n|, \]

we have

\[
|f(\mathbb{I}[f,g](q(n)))| \geq \max_{y \in A_n} |f^{-1}(\{y\})| \geq 2^q(n) - q(n)^c \geq 2^{l^{3/4} - q(n)^c} \geq 2^{(n-2)^{3/4} - n^{5/8}} \geq 2^{\sqrt{n}}.
\]

Thus, for all \( n \in J \),

\[ C_n = f(\mathbb{I}[f,g](q(n))) \subseteq \text{range}(f) = A, \]

so

\[ (A \triangle \{0,1\}^*) \cap C_n = \emptyset, \]

i.e., \( \{0,1\}^* \) does a good job of predicting \( A \) on \( C_n \), for all \( n \in J \). Since \( J \) is infinite, it follows that

\[
\frac{|(A \triangle \{0,1\}^*) \cap C_n|}{|C_n|} \not\rightarrow \frac{1}{2}
\]

as \( n \to \infty \). Thus \( \{0,1\}^* \) and \( C \) testify that \( A \not\in \text{WS}(2^{p(n) + 2n}; p(n), 2\sqrt{n}) \).

C-5
Case II. $2^{-n}|A_{=n}| \not\to \frac{1}{2}$ as $n \to \infty$. Then
\[
\frac{|(A \triangle \emptyset) \cap \{0,1\}^n|}{|\{0,1\}^n|} \not\to \frac{1}{2},
\]
so $\emptyset$ and $\{0,1\}^*$ testify that $A \not\in \text{WS}(2^p(n)+2n, p(n), 2\sqrt{n})$.

Since $A \in \beta\text{NP}$ is arbitrary, Cases I and II together show that
\[
\beta\text{NP} \cap \text{WS}(2^p(n)+2n, p(n), 2\sqrt{n}) = \emptyset.
\]

It follows by the Weak Stochasticity Theorem that $\mu(\beta\text{NP} | E_2) = 0$, completing the proof of Theorem 3.2.

\[\square\]

The following fact is quite useful. A proof appears in [3].

**Theorem C.2.** (Goldreich and Micali [9]). Let $p$ and $q$ be polynomials such that

\begin{enumerate}
\item Nonuniformly secure $p(n)$-generators exist if and only if nonuniformly secure $q(n)$-generators exist.
\item Uniformly secure $p(n)$-generators exist if and only if uniformly secure $q(n)$-generators exist.
\end{enumerate}

**Proof of Theorem 4.2.** Assume the hypothesis, let $\epsilon > 0$, and let $(A^+, A^-)$ be a BPP-pair. It suffices to prove that $\text{DTIME}(2^{n^{1/2}})$ separates $(A^+, A^-)$.

Fix a BPP-configuration $B = (B, q, \alpha, \beta)$ such that $A^+ = B^+$ and $A^- = B^-$. Without loss of generality, assume that $q$ is strictly increasing. Let $p(m) = q(m^{1/2})$.

By our assumption, nonuniformly secure pseudorandom generators exist, so by Theorem C.2 there exists a nonuniformly secure $p(m)$-generator $g$. For each $y \in \{0,1\}^*$, letting $n = |y|$ and $m = n^{1/2}$, define the "pseudo-critical event"
\[
\mathcal{B}_y = \{ x \in \{0,1\}^n \mid \langle y, g(x) \rangle \in B \}.
\]

Then define the language
\[
C = \left\{ y \in \{0,1\}^* \middle| \Pr(\mathcal{B}_y) \geq \frac{\alpha + \beta}{2} \right\},
\]
where $\Pr(\mathcal{B}_y)$ is computed according to the uniform distribution on $\{0,1\}^m$. It is clear that $C \in \text{DTIME}(2^{n^{1/2}})$.

Let
\[
J^+ = \{ q(n) \mid (A^+ \setminus C)_{=n} \neq \emptyset \},
\]
\[
J^- = \{ q(n) \mid q(n) \notin J^+ \text{ and } (A^- \cap C)_{=n} \neq \emptyset \},
\]
\[
J = J^+ \cup J^- = \{ q(n) \mid (A^+ \setminus C)_{=n} \cup (A^- \cap C)_{=n} \neq \emptyset \}.
\]

C-6
Define an advice function $h : \mathbb{N} \rightarrow \{0, 1\}^*$ as follows. For $j = q(n) \in J^+$, fix $h(j) \in (A^+ \setminus C)_n$. For $j = q(n) \in J^-$, fix $h(j) \in (A^- \cap C)_n$. For all other $j$, let $h(j) = \lambda$. Let $$D = \{ \langle z, w \rangle \mid |z| = q(|w|) \text{ and } \langle w, z \rangle \in B \}$$ and let $T = D/h$. Then $T \in \text{P/Poly}$, i.e., $T$ is a nonuniform test, so $g$ passes $T$.

Now for all $j = q(n) = p(m) \in J^+$, we have

$$\Pr(g^{-1}(T) = m) = \Pr[g(x) \in T] = \Pr[(g(x), h(j)) \in D] = \Pr[\langle h(j), g(x) \rangle \in B] = \Pr(B'_{h(j)}) < \frac{\alpha + \beta}{2}$$

and

$$\Pr(T = p(m)) = \Pr[y \in T] = \Pr[(y, h(j)) \in D] = \Pr[\langle h(j), y \rangle \in B] = \Pr(B_{h(j)}) \geq \beta,$$

so

$$\Pr(T = p(m)) - \Pr(g^{-1}(T) = m) > \beta - \frac{\alpha + \beta}{2} = \frac{\beta - \alpha}{2}.$$  

Similarly, for all $j = q(n) = p(m) \in J^-$, we have

$$\Pr(g^{-1}(T) = m) = \Pr(B'_{h(j)}) \geq \frac{\alpha + \beta}{2}$$

and

$$\Pr(T = p(m)) = \Pr(B_{h(j)}) \leq \alpha,$$

so

$$\Pr(g^{-1}(T) = m) - \Pr(T = p(m)) \geq \frac{\alpha + \beta}{2} - \alpha = \frac{\beta - \alpha}{2}. $$

We thus have

$$\left| \Pr(g^{-1}(T) = m) - \Pr(T = p(m)) \right| \geq \frac{\beta - \alpha}{2}$$

for all $j = p(m) \in J$. Since $g$ passes the test $T$, $\frac{\beta - \alpha}{2}$ is a positive constant, and $p$ is strictly increasing, it follows that $J$ is a finite set. We thus have

$$| (A^+ \setminus C) \cup (A^- \cap C) | < \infty,$$
whence there is a language $C'$ such that $|C' \triangle C| < \infty$ and $C'$ separates $(A^+, A^-)$. Since $C \in \text{DTIME}(2^n)$ and $|C' \triangle C| < \infty$, $C' \in \text{DTIME}(2^n)$. Thus $\text{DTIME}(2^n)$ separates $(A^+, A^-)$. 

In order to prove Theorem 4.3, we recall the well-known relationship between pseudorandom generators and one-way functions. For this purpose, we focus on one-way functions with polynomial security.

**Definition** A nonuniformly one-way function is a function that is, for all polynomials $t$ and $r$, $(t(n)/r(n))$-one-way with polynomial security. A uniformly one-way function is a function that is, for all polynomials $t$ and $r$, $(t(n), r(n))$-one-way with polynomial security.

It is easy to see that nonuniformly one-way functions exist if nonuniformly secure pseudorandom generators exist, and that uniformly one-way functions exist if uniformly secure pseudorandom generators exist. The converse implications, though much deeper, are also known to hold:

**Theorem C.3.** (Impagliazzo, Levin, and Luby [14]). If nonuniformly one-way functions exist, then nonuniformly secure pseudorandom generators exist.

**Theorem C.4.** (Hästad [13]). If uniformly one-way functions exist, then uniformly secure pseudorandom generators exist.

**Proof of Theorem 4.3.** Assume that $\text{DTIME}(2^n)$ separates all BPP-pairs and that uniformly secure pseudorandom generators do not exist. It suffices to prove that $\mu(\beta \text{NP} \mid E_2) = 0$.

Let $A \in \beta \text{NP}$. Fix a strictly increasing polynomial $p$ and a function $f \in \text{PF}^{[p]}_{\text{bal}}$ such that $A = \text{range}(f)$. By Theorem C.4, uniformly one-way functions do not exist, so an argument analogous to the proof of Lemma C.1 shows that there exist polynomials $t$, $r$, and $q$ and a function $g \in \text{DTIME}(t)$ such that the set

$$I = \left\{ n \in \mathbb{N} \left| \Pr(I_{\text{rand}}[f, g, r](p(n))) \geq \frac{1}{q(p(n))} \right. \right\}$$

is infinite and $|g((y, z))| = p(|y|)$ for all $y \in \{0, 1\}^*$ and $z \in \{0, 1\}^{r(|y|)}$.

For each $y \in \{0, 1\}^*$, let

$$I_y = \left\{ z \in \{0, 1\}^{r(|y|)} \mid f(g((y, z))) = y \right\},$$

and let

$$V = \left\{ y \in \{0, 1\}^* \left| \Pr(I_y) \geq \frac{1}{2q(|y|)} \right. \right\},$$

$$U = f^{-1}(V),$$

C-8
where $\Pr(I_y)$ is computed according to the uniform distribution on $\{0, 1\}^{|y|}$. Note that, for all $n \in I$, we have

$$
\frac{1}{q(p(n))} \leq \Pr(I_{\text{rand}}[f, g, r](p(n)))
= 2^{-p(n)} \sum_{x \in \{0, 1\}^p(n)} \Pr(I_{f(x)})
= 2^{-p(n)} \left[ \sum_{x \in U=p(n)} \Pr(I_{f(x)}) + \sum_{x \in \{0, 1\}^p(n) \setminus U} \Pr(I_{f(x)}) \right]
\leq 2^{-p(n)} \left[ |U=p(n)| + 2^p(n) \frac{1}{2q(p(n))} \right].
$$

Thus,

$$
|U=p(n)| \geq \frac{2^p(n)}{2q(p(n))}
$$

for all $n \in I$.

We now have two cases.

Case I. $2^{-n} |A_n| \to \frac{1}{2}$ as $n \to \infty$. Then fix $n_0 \in \mathbb{N}$ such that the following conditions hold for all $n \geq n_0$.

(i) $|A_n| \geq 2^{n-2}$.

(ii) $(1 - \frac{1}{2q(p(n))})q(p(n)) < \frac{2}{3}$.

(iii) For all $y \in A_n$,

$$
|f^{-1}(\{y\})| \leq 2^p(n) - \frac{l}{4},
$$

where $l = \log |A_n|$.

(iv) $2^{(n-2)\frac{3}{4}} \geq 2\sqrt{\pi} \cdot 2q(p(n))$.

(In (ii) we are using the fact that the left-hand side converges to $1/\sqrt{\pi}$, which is less than $2/3$, as $n \to \infty$. In (iii) we are using the fact that $f \in Pf_{\text{bar}}^{(p)}$.) Let

$$
J = \{ n \in I \mid n \geq n_0 \}
$$

and note that $J$ is infinite. Note that, for all $n \in J$ (setting $l = \log |A_n|$),

$$
|V_n| \geq \frac{|U=p(n)|}{2^p(n) - \frac{l}{4}}
$$

$$
\geq \frac{2^p(n)}{2q(p(n))}
$$

$$
\geq \frac{2^{(n-2)\frac{3}{4}}}{2q(p(n))}
$$

$$
\geq \frac{2\sqrt{\pi}}{2q(p(n))}
$$

$$
\geq 2\sqrt{\pi}.
$$
Now let $B$ be the set of all $(y,z)$ such that $z = z_1 \cdots z_{q[p(n)]}$, where each $|z_i| = r(|y|)$ and $I_y \cap \{z_1, \cdots, z_{q[p(n)]}\} \neq \emptyset$. Note that $B \in \text{P}$. Define the polynomial

$$s(n) = q(p(n)) \cdot r(n)$$

and consider the BPP-configuration

$$B = (B, s, 0, 1/3).$$

By our assumption, $\text{DTIME}(2^n)$ separates all BPP-pairs, so there is a language $C \in \text{DTIME}(2^n)$ such that $B^+ \subseteq C$ and $B^- \cap C = \emptyset$.

The language $C$ satisfies

$$V_n \subseteq B^+ \subseteq C \subseteq A$$

for all $n \geq n_0$. The second of these three inclusions is clear. Since $B^- \cap C = \emptyset$, every element of $C$ has a preimage under $f$, whence $C \subseteq \text{range}(f) = A$, i.e., the third inclusion holds. To see that the first inclusion holds, fix $n \geq n_0$ and let $y \in V_n$. Then $\Pr(I_y) \geq \frac{1}{2q(p(n))}$, so the complement $B_y'$ of the critical event $B_y$ has probability

$$\Pr(B_y') \leq \left(1 - \frac{1}{2q(p(n))}\right)^{q[n]} < \frac{2}{3},$$

so $\Pr(B_y) > 1/3$, so $y \in B^+$ and the first inclusion is affirmed.

Now define a language $D \in \text{DTIME}(2^n)$ by

$$D_{=n} = \begin{cases} C_{=n} & \text{if } |C_{=n}| \geq 2^{\sqrt{n}} \\ \{0,1\}^n & \text{if } |C_{=n}| < 2^{\sqrt{n}}. \end{cases}$$

Recall that $|V_n| \geq 2^{\sqrt{n}}$ for all $n \in J$. Since $V_n \subseteq C \subseteq A$, it follows that

$$D_{=n} = C_{=n} \subseteq A$$

for all $n \in J$. But then

$$(A \triangle \{0,1\}^*) \cap D_{=n} = \emptyset$$

for all $n \in J$. Because $J$ is infinite, this implies that

$$\frac{|(A \triangle \{0,1\}^*) \cap D_{=n}|}{|D_{=n}|} \not\rightarrow \frac{1}{2}$$

as $n \rightarrow \infty$. Since $\{0,1\}^*$, $D \in \text{DTIME}(2^{2^n})$ and $|D_{=n}| \geq 2^{\sqrt{n}}$ for all $n \in N$, it follows that $A \not\in \text{WS}(2^{2^n}, 0, 2^{\sqrt{n}})$.

Case II. $2^{-n} |A_{=n}| \not\rightarrow \frac{1}{2}$ as $n \rightarrow \infty$. Then we immediately have $A \not\in \text{WS}(2^{2^n}, 0, 2^{\sqrt{n}})$.

Since $A \in \beta\text{NP}$ is arbitrary, Cases I and II together show that

$$\beta\text{NP} \cap \text{WS}(2^{2^n}, 0, 2^{\sqrt{n}}) = \emptyset.$$

It follows by the Weak Stochasticity Theorem that $\mu(\beta\text{NP} \mid E_2) = 0$, completing the proof of Theorem 4.3. 

\[\square\]