One-Way Functions and Balanced NP*

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

Abstract

The existence of cryptographically secure one-way functions is related to the measure of a subclass of NP. This subclass, called βNP ("balanced NP"), contains 3SAT and other standard NP problems. The hypothesis that βNP is not a subset of P is equivalent to the P $\neq$ NP conjecture. A stronger hypothesis, that βNP is not a measure 0 subset of $E_2 = \mathrm{DTIME}(2^{\mathrm{polynomial}})$ is shown to have the following two 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 $\mathrm{DTIME}(2^n)$ "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 $\mathrm{BPP} \subseteq \mathrm{DTIME}(2^{n^\epsilon})$ for all $\epsilon > 0$.)

Such consequences are not known to follow from the weaker hypothesis that P $\neq$ NP.

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

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.

In this paper, we introduce a strong hypothesis concerning the quantitative structure of NP, and prove that this hypothesis implies the existence of cryptographically secure one-way functions. We also prove that this hypothesis implies a partial converse of Yao, Boppana, and Hirschfeld's theorem that BPP $\subseteq \bigcap_{\epsilon>0} \mathrm{DTIME}(2^{n^\epsilon})$ if nonuniformly secure pseudorandom generators exist.

As we use the term here, a cryptographically secure one-way function is a polynomial time computable, honest function $f : \{0,1\}^* \to \{0,1\}^*$ 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 [8], secure pseudorandom generators [16, 15], subexponential time simulations of BPP [33, 5], secure private key encryption protocols [13, 21, 10], bit commitment protocols [28], and zero-knowledge proofs of NP languages [12].

It should be noted that one-way functions with essentially minimum security requirements have also been defined and investigated. (See [31] 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 5 for precise definitions.)

We also emphasize that one-way functions are *not* required to be one-to-one in this paper.

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 4 below, we define the class βNP ("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 too much more than its "fair share" of preimages. We show that βNP is a subclass of NP that contains all efficiently rankable languages in P [9], as well as 3SAT and many other NP languages. The hypotheses P $\neq$ NP and βNP $\not\subseteq$ P are thus equivalent.

In sections 5 and 6, we investigate the consequences of the stronger hypothesis that βNP is not a measure 0 subset of $\mathrm{E}_2 = \mathrm{DTIME}(2^{\mathrm{polynomial}})$. The meaning of this hypothesis requires some explanation.

It is well-known that P $\subseteq$ NP $\subseteq \mathrm{E}_2$. In fact, E_2 is the smallest deterministic time complexity class known to contain NP. The key question is, *how large* are P, NP, and βNP as subsets of E_2? *Resource-bounded measure* [24, 22] is a generalization of classical Lebesgue measure that was developed in order to address questions of this sort in a variety of complexity classes. Here we restrict attention to measure in E_2.

Resource-bounded measure defines the class of *measurable* subsets of E_2 and assigns to each measurable subset X of E_2 a value $\mu(X \mid \mathrm{E}_2)$, called the *measure of* X *in* E_2, satisfying $0 \leq \mu(X \mid \mathrm{E}_2) \leq 1$. Intuitively, the condition $\mu(X \mid \mathrm{E}_2) = 0$ means that X is a *negligibly small* subset of E_2, while the condition $\mu(X \mid \mathrm{E}_2) = 1$ means that X contains *almost every* language in E_2. (A set has measure 1 in E_2 if and only if its complement has measure 0 in E_2.) For a set X that is closed under finite variations (i.e., $A \in X$ and $|A \triangle B| < \infty$ imply that $B \in X$), a resource-bounded extension of the classical Kolmogorov zero-one law [23, 22] tells us that there are only three possibilities: $\mu(X \mid \mathrm{E}_2) = 0$, $\mu(X \mid \mathrm{E}_2) = 1$, or X is not measurable in E_2. Moreover, Regan, Sivakumar, and Cai [29] have recently shown that, if X is closed under finite unions and intersections (or closed under symmetric difference) and $\mu(X \mid \mathrm{E}_2) = 1$, then $\mathrm{E}_2 \subseteq X$. It follows that nearly every subset X of E_2 that is of interest in complexity theory, including each of P, NP, and βNP, is subject to the following trichotomy: X has measure 0 in E_2, X contains all of E_2, or X is not measurable in E_2.

It is easy to see [24] that $\mu(P \mid \mathrm{E}_2) = 0$, i.e., that P is a negligibly small subset of E_2. It is conceivable that P $\neq$ NP, and yet that $\mu(\mathrm{NP} \mid \mathrm{E}_2) = 0$, but we conjecture that this is not the case, i.e., that $\mu(\mathrm{NP} \mid \mathrm{E}_2) \neq 0$. (Note that "$\mu(\mathrm{NP} \mid \mathrm{E}_2) \neq 0$" means that "NP $= \mathrm{E}_2$ or NP is not a measurable subset of E_2.") In fact, we conjecture that NP is a nonmeasurable subset of E_2. In any case, the hypothesis that $\mu(\mathrm{NP} \mid \mathrm{E}_2) \neq 0$ has recently been shown to have a number of plausible consequences: If $\mu(\mathrm{NP} \mid \mathrm{E}_2) \neq 0$, then NP contains E-bi-immune langauges [27]; every $\leq^{\mathrm{P}}_{n^\alpha\text{-}tt}$-

hard language for NP ($\alpha < 1$) is exponentially dense [26]; and every $\leq^{\mathrm{P}}_{m}$-hard language for NP has an exponentially dense, exponentially hard complexity core [17]; there is an NP search problem that is not efficiently reducible to the corresponding decision problem [4, 25]; there are problems that are $\leq^{\mathrm{P}}_{\mathrm{T}}$-complete, but not $\leq^{\mathrm{P}}_{\mathrm{m}}$-complete, for NP[25]; and every $\leq^{\mathrm{P}}_{\mathrm{tt}}$-hard language for NP is p-superterse[3, 32].

Since $\beta\mathrm{NP} \subseteq \mathrm{NP}$, the hypothesis $\mu(\beta\mathrm{NP} \mid \mathrm{E}_2) \neq 0$ implies the hypothesis $\mu(\mathrm{NP} \mid \mathrm{E}_2) \neq 0$. There does not appear to be any *a priori* reason for disbelieving the hypothesis $\mu(\beta\mathrm{NP} \mid \mathrm{E}_2) \neq 0$, but further investigation of the class $\beta\mathrm{NP}$ should precede a conjecture. (It is interesting to note that, if A is an algorithmically random oracle, then $\mu(\mathrm{NP}^A \mid \mathrm{E}_2^A) \neq 0$ [20], while $\mu(\beta\mathrm{NP}^A \mid \mathrm{E}_2^A) = 0$)[19].) In this paper we merely introduce the hypothesis, note that it is not implausible, and prove that it has plausible, interesting consequences.

In section 5, assuming the hypothesis $\mu(\beta\mathrm{NP} \mid \mathrm{E}_2) \neq 0$, we prove that for every k there is a polynomial time computable, honest function f that is "$(2^{n^k}/n^k)$-one-way with exponential security," i.e., 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.

Yao [33] and Boppana and Hirschfeld [5] proved that, if nonuniformly secure pseudorandom generators exist, then $\mathrm{BPP} \subseteq \bigcap_{\epsilon>0} \mathrm{DTIME}(2^{n^\epsilon})$. In section 6 below, we show that their argument actually yields an (apparently) stronger conclusion, namely that $\bigcap_{\epsilon>0} \mathrm{DTIME}(2^{n^\epsilon})$ "separates all BPP-pairs." Assuming the hypothesis $\mu(\beta\mathrm{NP} \mid \mathrm{E}_2) \neq 0$, we then prove a partial converse to this result, namely, that if $\mathrm{DTIME}(2^n)$ separates all BPP-pairs, then uniformly secure pseudorandom generators exist. Our proof uses the theorem of Håstad [15] (building on work of Impagliazzo, Levin, and Luby [16]), that uniformly secure pseudorandom generators exist if uniformly one-way functions exist.

Both our main results are proven using the Weak Stochasticity Theorem, which says that, for every fixed k, almost every language in E_2 is statistically unpredictable by 2^{n^k}-time-bounded algorithms, even with n^k bits of nonuniform advice. This result, a small improvement of a result due to Lutz and Mayordomo [26], is presented in section 3.

2 Preliminaries

In this paper, $[\![\psi]\!]$ denotes the *Boolean value* of the condition ψ, 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 $A^c = \{0,1\}^* - A$. 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 $s_0 = \lambda$, $s_1 = 0$, $s_2 = 1$, $s_3 = 00, ...$ 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 $w \sqsubseteq x$, if $x = wy$ for some $y \in \{0,1\}^* \cup \{0,1\}^\infty$. The *cylinder generated by* a string $w \in \{0,1\}^*$ is

$$C_w = \{x \in \{0,1\}^\infty \mid w \sqsubseteq x\}.$$

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

As noted in the introduction, we work with the exponential time complexity class $\mathrm{E}_2 = \mathrm{DTIME}(2^{\mathrm{polynomial}})$. The subscript '2' here distinguishes E_2 from the class $\mathrm{E} = \mathrm{DTIME}(2^{\mathrm{linear}})$. It is well-known that $\mathrm{P} \subsetneqq \mathrm{E} \subsetneqq \mathrm{E}_2$, that $\mathrm{P} \subseteq \mathrm{NP} \subseteq \mathrm{E}_2$ and that $\mathrm{NP} \neq \mathrm{E}$.

We write Partial-PF for the set of all polynomial time computable partial functions $f : \{0,1\}^* \to \{0,1\}^*$. We write PF for the set of all $f \in$ Partial-PF such that 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 $\mathbf{D} = \{m2^{-n} \mid m \in \mathbf{Z}, n \in \mathbf{N}\}$ 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 $d : \mathbf{N}^k \times \{0,1\}^* \to Y$, where Y is $\mathbf{D}$ 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 $d : \mathbf{N}^2 \times \{0,1\}^* \to \mathbf{D}$ is formally interpreted as a function $\tilde{d} : \{0,1\}^* \to \{0,1\}^*$. Under this interpretation, $d(i,j,w) = r$ means that $\tilde{d}(\langle 0^i, \langle 0^j, w\rangle\rangle) = u$, where u is a suitable binary encoding of the dyadic rational r. Similarly, a function $m : \mathbf{N}^k \to \mathbf{N}$ 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 $d : \mathbf{N} \times X \to Y$ and $k \in \mathbf{N}$, 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 $d_0, d_1, d_2, ...$ For a function $d : \mathbf{N}^n \times X \to Y$ $(n \geq 2)$, we write $d_{k,l} = (d_k)_l$, etc.

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

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

Lemma 2.1.[7, 14]. If $X_1, ..., X_N$ are independent 0-1-valued random variables with the uniform distribution, $S = X_1 + ... + X_N$, 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 [14]. □

3 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 5 and 6. We also expect it to be useful in future investigations of the measure structure of E_2.

Resource-bounded measure [24, 22] 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 section 2.

A *constructor* is a function $\delta : \{0,1\}^* \to \{0,1\}^*$ such that $x \sqsubsetneq \delta(x)$ for all $x \in \{0,1\}^*$. The *result* of a constructor δ (i.e., the *language constructed by*

δ) is the unique language $R(\delta)$ such that $\delta^n(\lambda) \sqsubseteq R(\delta)$ for all $n \in \mathbf{N}$. Intuitively, δ constructs $R(\delta)$ by starting with λ 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 $f : \{0,1\}^* \to \{0,1\}^*$, is defined as follows.

$$\mathrm{p}_2 \quad = \quad \{f | f \text{ is computable is } n^{(\log n)^{O(1)}} \text{ time}\}$$

Lemma 3.1.[23]

$$\mathrm{E}_2 = \{\, \mathrm{R}(\delta) \mid \delta \in \mathrm{p}_2 \text{ and } \delta \text{ is a constructor} \,\}.$$

Using Lemma 3.1, the measure structure of E_2 is now developed in terms of the class p_2.

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

$$d(w) \geq \frac{d(w0) + d(w1)}{2} \tag{3.1}$$

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

$$S[d] = \bigcup_{\substack{w \in \{0,1\}^* \\ d(w) \geq 1}} C_w. \tag{3.2}$$

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

For all density functions in this paper, equality actually holds in (3.1) 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, (3.1) and (3.2) 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

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

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

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

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

for all $\vec{k} \in \mathbf{N}^n$, $r \in \mathbf{N}$, and $w \in \{0,1\}^*$. A p_2-*computation* of an n-DS d is a computation $\widehat{d}$ of d such that $\widehat{d} \in \mathrm{p}_2$. An n-DS d is p_2-*computable* if there exists a p_2-computation $\widehat{d}$ of d.

If d is an n-DS such that $d : \mathbf{N}^n \times \{0,1\}^* \to \mathbf{D}$ and $d \in \mathrm{p}_2$, 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 $\widehat{d}$, relying on context and subscripts to distinguish an n-DS d from a computation 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 $k \in \mathbf{N}$, 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 $\mu_{\mathrm{p}_2}(X) = 0$, if there exists a p_2-null cover of X. A set X has p_2-*measure 1*, and we write $\mu_{\mathrm{p}_2}(X) = 1$, if $\mu_{\mathrm{p}_2}(X^c) = 0$.

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 $\mu(X \mid \mathrm{E}_2) = 0$, if $\mu_{\mathrm{p}_2}(X \cap \mathrm{E}_2) = 0$. A set X has *measure 1 in* E_2, and we write $\mu(X \mid \mathrm{E}_2) = 1$, if $\mu(X^c \mid \mathrm{E}_2) = 0$. If $\mu(X \mid \mathrm{E}_2) = 1$, we say that *almost every* language in E_2 is in X.

The following lemma is obvious but useful.

Lemma 3.2. For every set $X \subseteq \{0,1\}^\infty$,

$$\begin{array}{ccc} \mu_{\mathrm{p}_2}(X) = 0 & \Longrightarrow & \Pr[x \in X] = 0 \\ \Downarrow & & \\ \mu(X \mid \mathrm{E}_2) = 0 & & \end{array}$$

and

$$\begin{array}{ccc} \mu_{\mathrm{p}_2}(X) = 1 & \Longrightarrow & \Pr[x \in X] = 1 \\ \Downarrow & & \\ \mu(X \mid \mathrm{E}_2) = 1, & & \end{array}$$

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 [24] that these definitions endow E_2 with internal measure structure. Specifically, if $\mathcal{I}$ is either the collection $\mathcal{I}_{\mathrm{p}_2}$ of all p_2-measure 0 sets or the collection $\mathcal{I}_{\mathrm{E}_2}$ 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 $\mathcal{I}_{\mathrm{E}_2}$ 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 $\mu(X \mid \mathrm{E}_2) = 0$, then $X \cap \mathrm{E}_2$ 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 [24], 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 $m : \mathbf{N} \to \mathbf{N}$ such that

$$\sum_{n=m(j)}^{\infty} a_n \leq 2^{-j}$$

for all $j \in \mathbf{N}$. A series is p_2-*convergent* if it has a modulus $m \in \mathrm{p}_2$. A sequence

$$\sum_{k=0}^{\infty} a_{j,k} \qquad (j = 0, 1, 2, \ldots)$$

of series is *uniformly* p-*convergent* if there exists a function $m : \mathbf{N}^2 \to \mathbf{N}$ such that $m \in \mathrm{p}_2$ and, for each $j \in \mathbf{N}$, 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 3.3. Let $a_{j,k} \in [0, \infty)$ for all $j, k \in \mathbf{N}$. If there exist a real $\varepsilon > 0$ and a function $h : \mathbf{N} \to \mathbf{N}$ such that $h \in \mathrm{p}_2$ and $a_{j,k} \leq e^{-e^{(\ln k)^{\epsilon}}}$ for all $j, k \in \mathbf{N}$ with $k \geq h(j)$, then the series

$$\sum_{k=0}^{\infty} a_{j,k} \qquad (j = 0, 1, 2, \ldots)$$

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 3.4.[24]. If d is a p_2-computable 2-DS such that the series

$$\sum_{k=0}^{\infty} d_{j,k}(\lambda) \qquad (j = 0, 1, 2, \ldots)$$

are uniformly p_2-convergent, then

$$\mu_{\mathrm{p}_2}\left(\bigcup_{j=0}^{\infty}\bigcap_{t=0}^{\infty}\bigcup_{k=t}^{\infty} S[d_{j,k}]\right) = 0.$$

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 3.5 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 [18]. An *advice*

function is a function $h : \mathbf{N} \to \{0,1\}^*$. Given a function $q : \mathbf{N} \to \mathbf{N}$, we write $\mathrm{ADV}(q)$ for the set of all advice functions h such that $|h(n)| \leq q(n)$ for all $n \in \mathbf{N}$. 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 $t, q : \mathbf{N} \to \mathbf{N}$, we define the *advice class*

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

We now define our notion of weak stochasticity. Let $t, q, \nu : \mathbf{N} \to \mathbf{N}$ and let $A \subseteq \{0,1\}^*$. Then A is *weakly (t,q,ν)-stochastic* if, for all $B, C \in \mathrm{DTIME}(t)/\mathrm{ADV}(q)$ 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,ν)-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 [26], in that the language C is allowed advice here.)

Let $\mathrm{WS}(t,q,\nu)$ denote the set of all languages that are weakly (t,q,ν)-stochastic. The following theorem is a minor variation of a result of [26] on the weak stochasticity of almost every language in E. We include a proof for completeness of exposition.

Theorem 3.5. (Weak Stochasticity Theorem [26]). For every fixed polynomial p and every fixed real number $\gamma > 0$,

$$\mu(\mathrm{WS}(2^{p(n)}, p(n), 2^{n^\gamma}) \mid \mathrm{E}_2) = 1.$$

Proof. Let $\mathrm{WS} = \mathrm{WS}(2^{p(n)}, p(n), 2^{n^\gamma})$, where p is a polynomial and γ is a positive real. It suffices to prove that $\mu_{\mathrm{p}_2}(\mathrm{WS}^c) = 0$, where WS^c is the complement of WS.

Let $U \in \mathrm{DTIME}(2^{n \cdot p(n)})$ be a language that is universal for $\mathrm{DTIME}(2^{p(n)}) \times \mathrm{DTIME}(2^{p(n)})$ in the following sense: for each $i \in \mathbf{N}$, 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 $\mathrm{DTIME}(2^{p(n)}) \times \mathrm{DTIME}(2^{p(n)}) = \{ (C_i, D_i) \mid i \in \mathbf{N} \}$.

For all $i, j, k \in \mathbf{N}$, 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 $n \in \mathbf{N}$, then

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

where each

$$Y_{i,j,k,y,z} = \left\{ A \subseteq \{0,1\}^* \middle| |(C_i/y)_{=n}| \geq 2^{n^\gamma} \right.$$
$$\left. \text{and } \left| \frac{|(A \triangle (D_i/z)) \cap (C_i/y)_{=n}|}{|(C_i/y)_{=n}|} - \frac{1}{2} \right| \geq \frac{1}{j+1} \right\} .$$

It is immediate from the definition of weak stochasticity that

$$\mathrm{WS}^c \subseteq \bigcup_{i=0}^{\infty} \bigcup_{j=0}^{\infty} \bigcap_{m=0}^{\infty} \bigcup_{k=m}^{\infty} Y_{i,j,k}.$$

Thus, by Lemma 3.4, it suffices to exhibit a p_2-computable 3-DS d with the following two properties.

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

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

Define the function $d : \mathbf{N}^3 \times \{0,1\}^* \to [0, \infty)$ as follows. If k is not a power of 2, then $d_{i,j,k}(w) = 0$. Otherwise, if $k = 2^n$, where $n \in \mathbf{N}$, then

$$d_{i,j,k}(w) = \Sigma_{y,z \in \{0,1\}^{\leq p(n)}} \Pr(Y_{i,j,k,y,z} | C_w),$$

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 $U \in \mathrm{DTIME}(2^{n \cdot p(n)})$ and γ 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 $2^{n \cdot p(n)} = k^{(\log k)^{O(1)}}$.) Thus d is p_2-computable.

To see that d has property (I), note first that Lemma 2.1, the Chernoff bound, tells us that, for all $i, j, n \in \mathbf{N}$ and $y, z \in \{0,1\}^{\leq p(n)}$ (writing $k = 2^n$, $N = 2^{n^\gamma} = 2^{(\log k)^\gamma}$, and $\epsilon = \frac{2}{j+1}$),

$$\Pr(Y_{i,j,k,y,z}) \leq 2e^{-\frac{\epsilon^2 N}{6}} < 2e^{-\frac{N}{2(j+1)^2}},$$

whence

$$\begin{aligned} d_{i,j,k}(\lambda) &= \Sigma_{y,z \in \{0,1\}^{\leq p(n)}} \Pr(Y_{i,j,k,y,z}) \\ &< \left(2^{p(n)+1}\right)^2 \cdot 2e^{-\frac{N}{2(j+1)^2}} \\ &< e^{2p(n)+3-\frac{N}{2(j+1)^2}}. \end{aligned}$$

Let $\delta = \frac{\gamma}{3}$, $a = \lceil \frac{1}{\delta} \rceil$, and fix $n_0 \in \mathbf{N}$ 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 $h : \mathbf{N} \to \mathbf{N}$ by

$$h(j) = 2^{n_0} + 2^{(1+2\log(j+1))^a}.$$

It is clear that $h \in \mathrm{p}_2$. For all $i, j, k, n \in \mathbf{N}$ with $k = 2^n$ (still writing $N = 2^{n^\gamma} = 2^{n^{3\delta}}$), we have

$$k \geq 2^{n_0} \Longrightarrow 2^{n^{2\delta}} \geq e^{(\ln k)^\delta} + 2p(n) + 3$$

and

$$\begin{aligned} k \geq 2^{(1+2\log(j+1))^a} &\Longrightarrow n^\delta \geq 1 + 2\log(j+1) \\ &\Longrightarrow 2^{n^\delta} \geq 2(j+1)^2, \end{aligned}$$

so

$$\begin{aligned} k \geq h(j) &\Longrightarrow N = 2^{n^{3\delta}} \geq 2^{n^\delta} \cdot 2^{n^{2\delta}} \geq 2(j+1)^2 \left[e^{(\ln k)^\delta} + 2p(n) + 3\right] \\ &\Longrightarrow 2p(n) + 3 - \frac{N}{2(j+1)^2} \leq -e^{(\ln k)^\delta} \\ &\Longrightarrow d_{i,j,k}(\lambda) \leq e^{-e^{(\ln k)^\gamma}}. \end{aligned}$$

Since $\delta > 0$, it follows by Lemma 3.3 that (I) holds.

Finally, to see that (II) holds, fix $i, j, k \in \mathbf{N}$. If k is not a power of 2, then (II) is trivially affirmed, so assume that $k = 2^n$, where $n \in \mathbf{N}$. Let $A \in Y_{i,j,k}$. Fix $y, z \in \{0,1\}^{\leq p(n)}$ 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

$$d_{i,j,k}(w) \geq \Pr(Y_{i,j,k,y,z} | C_w) = 1,$$

so $A \in C_w \subseteq S[d_{i,j,k}]$. This completes the proof. □

4 The Class βNP

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

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

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 $f \in \mathrm{PF}_{\mathrm{hon}}^{(q)}$, if there is a fixed string $z_0 \in \{0,1\}^*$ such that the following conditions hold.

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

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

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

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

Theorem 4.1. For every nonempty language $A \subseteq \{0,1\}^*$, the following conditions are equivalent.

(1) $A \in \mathrm{NP}$.

(2) $A = \mathrm{range}(f)$ for some $f \in \mathrm{PF}_{\mathrm{hon}}$.

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

Proof.

(3)$\Longrightarrow$(2). Assume (3). Fix a strictly increasing polynomial q and string z_0 testifying that $f \in \mathrm{PF}^{\mathrm{nf}}_{\mathrm{hon}}$. Define $g : \{0,1\}^* \to \{0,1\}^*$ by

$$g(x) = \begin{cases} f(x) & \text{if } |x| \in \mathrm{range}(q) \\ z_0 & \text{if } |x| \notin \mathrm{range}(q). \end{cases}$$

Then $g \in \mathrm{PF}_{\mathrm{hon}}$ and $\mathrm{range}(g) = range(f) = A$, so (2) holds.

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

(1)$\Longrightarrow$(3). Assume that $A = \exists^p B \in \mathrm{NP}$, where $B \in \mathrm{P}$ 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 $|u| = n$ and $|v| + i = p(n)$, then $|\langle u, v10^i\rangle| = q(n)$.) 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 $x = \left\langle u, v10^{p(n)-|v|}\right\rangle$, where $|u| = n$ and $\langle u, v\rangle \in B$, then $f(x) = u$; otherwise, $f(x) = z_0$. It is clear that $f \in \mathrm{PF}^{(q)}_{\mathrm{hon}}$ and $\mathrm{range}(f) = A$, so (3) holds.

□

With this characterization in mind, we define the class βNP.

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

(i) $f \in \mathrm{PF}^{(q)}_{\mathrm{hon}}$.

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

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

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

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

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

Definition The class βNP ("balanced NP") is defined by

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

It is clear that $\mathrm{PF}_{\mathrm{bal}} \subseteq \mathrm{PF}^{\mathrm{nf}}_{\mathrm{hon}}$, so Theorem 4.1 immediately gives us the following.

Observation 4.2. $\beta\mathrm{NP} \subseteq \mathrm{NP}$

It is not clear that $\mathrm{P} \subseteq \beta\mathrm{NP}$. However, it is easy to see that βNP contains all languages that have efficient ranking functions (see [9]). That is, if we let $\rho\mathrm{P}$ be the set of all languages of the form range(g), where $g \in \mathrm{PF}$ is strictly increasing (with respect to the standard ordering of $\{0,1\}^*$), then it is clear that $\rho\mathrm{P} \subseteq \mathrm{P}$, and it is easy to see the following.

Observation 4.3. $\rho\mathrm{P} \subseteq \beta\mathrm{NP}$

In fact, βNP is a much richer subclass of NP than Observation 4.3 alone indicates. For example, βNP contains NP-complete languages:

Proposition 4.4. $3\mathrm{SAT} \in \beta\mathrm{NP}$

Proof. Fix a sequence $v_1, v_2, \cdots$ of Boolean variables. For each positive integer m, let $V_m = \{v_1, \cdots, v_m\}$, let $\mathcal{A}_m$ be the set of all truth assignments $a : V_m \to \{0,1\}$, and let $3\mathrm{CNF}_m$ 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 $|3\mathrm{CNF}_m| = 8^m\binom{m}{3}^m$.) Extend each $a \in \mathcal{A}_m$ to a function $a : 3\mathrm{CNF}_m \to \{0,1\}$ in the obvious way and let

$$3\mathrm{SAT}_m = \{\, \psi \in 3\mathrm{CNF}_m \mid (\exists a \in \mathcal{A}_m)\, a(\psi) = 1 \,\}.$$

For simplicity, we consider 3SAT as having the form

$$3\mathrm{SAT} = \bigcup_{m=1}^{\infty} 3\mathrm{SAT}_m.$$

For each positive integer m and each $a \in \mathcal{A}_m$, define the set

$$T_m(a) = \{\, \psi \in 3\mathrm{CNF}_m \mid a(\psi) = 1 \,\},$$

consisting of all 3CNF_m formulas that are true under the assignment a. Then define the sets

$$\begin{aligned} T_m &= \bigcup_{a \in \mathcal{A}_m} (\{a\} \times T_m(a)), \\ T &= \bigcup_{m=1}^{\infty} T_m, \end{aligned}$$

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, ψ) such that a is a truth assignment, ψ is a 3CNF formula, and ψ is true under a. Note also that, for each m and a, we have

$$|T_m(a)| = 7^m \binom{m}{3}^m,$$

so

$$|T_m| = 7^m \binom{m}{3}^m |\mathcal{A}_m| = 14^m \binom{m}{3}^m.$$

For each positive integer m, let $w_1^{(m)}, \cdots, w_t^{(m)}$ be the lexicographic enumeration of $\{0,1\}^{q(p(m))}$ and let $y_1^{(m)}, \cdots, y_d^{(m)}$ be the lexicographic enumeration of T_m. (The elements (a, ψ) of T_m are enumerated first in order of a, then in order of ψ. Note that $t = 2^{q(p(m))}$ and $d = 14^m \binom{m}{3}^m \leq t$.) Then define the finite function $g_m : \{0,1\}^{q(p(m))} \xrightarrow{onto} T_m$ 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 $h : T \xrightarrow{onto} 3\text{SAT}$ 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 $f : D \to 3\text{SAT}$ by

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

Since the elements (a, ψ) of T_m can easily be counted and enumerated (first in order of a, then in order of ψ), it is clear that f is computable in

polynomial time. In fact, it is clear that $f \in \mathrm{PF}^{(q)}_{\mathrm{hon}}$ and $\mathrm{range}(f) = 3\mathrm{SAT}$. To finish the proof that $3\mathrm{SAT} \in \beta\mathrm{NP}$, then, it suffices to show that f satisfies the balancing condition, so that $f \in \mathrm{PF}^{(q)}_{\mathrm{bal}}$.

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 $s = \lceil \frac{2^{q(n)}}{|T_m|} \rceil$. If n is sufficiently large, then

$$\begin{aligned}
\left| \left\{ y \in \{0,1\}^{q(n)} \mid f(y) = f(x) \right\} \right| \cdot 2^{l^\alpha - q(n)} &\leq s \cdot |h^{-1}(\{\psi\})| \cdot 2^{l^\alpha - q(n)} \\
&\leq s \cdot |\mathcal{A}_m| \cdot |3\mathrm{CNF}_m|^\alpha \cdot 2^{-q(n)} \\
&< \frac{2}{|T_m|} \cdot |\mathcal{A}_m| \cdot |3\mathrm{CNF}_m|^\alpha \\
&= 2 \cdot \left(\frac{8^\alpha}{7} \binom{m}{3}^{\alpha - 1} \right)^m .
\end{aligned}$$

Since $\frac{8^\alpha}{7} \cdot \binom{m}{3}^{\alpha-1} \to 0$ as $m \to \infty$, it follows that

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

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

Case II. $n \notin \mathrm{range}(p)$. Then

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

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

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

again affirming the balancing condition.

We have now shown that $f \in \mathrm{PF}^{(q)}_{\mathrm{bal}}$, whence $3\mathrm{SAT} = \mathrm{range}(f) \in \beta\mathrm{NP}$. □

Corollary 4.5. The following conditions are equivalent.

(1) $\mathrm{P} \neq \mathrm{NP}$.

(2) $\beta\mathrm{NP} \not\subseteq \mathrm{P}$.

In the next two sections, we will investigate the consequences of the hypothesis $\mu(\beta\mathrm{NP} \mid \mathrm{E}_2) \neq 0$. This is clearly a strong hypothesis in the following sense.

Observation 4.6. $\mu(\beta\mathrm{NP} \mid \mathrm{E}_2) \neq 0 \Longrightarrow \mu(\mathrm{NP} \mid \mathrm{E}_2) \neq 0 \Longrightarrow \mathrm{P} \neq \mathrm{NP}$.

5 One-Way Functions With Exponential Security

In this section we define several types of one-way function and prove that, if $\mu(\beta\mathrm{NP} \mid \mathrm{E}_2) \neq 0$, 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 $f, g : \{0,1\}^* \to \{0,1\}^*$, $r : \mathbf{N} \to \mathbf{N}$, and $n \in \mathbf{N}$, 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) $\mathcal{I}_{\mathrm{rand}}[f,g,r](n) = \{\, (x,z) \in \Omega_{f,r}(n) \mid f(g(\langle f(x), z\rangle)) = f(x) \,\}$, where $\Omega_{f,r}(n) = \left\{\, (x,z) \mid x \in \{0,1\}^n \text{ and } z \in \{0,1\}^{r(|f(x)|)} \,\right\}$.

We interpret $\mathcal{I}[f,g](n)$ and $\mathcal{I}_{\mathrm{rand}}[f,g,r](n)$ 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

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

and

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

where each

$$\mathcal{I}_{f(x)} = \left\{\, z \in \{0,1\}^{r(|f(x)|)} \mid f(g(\langle f(x), z\rangle)) = f(x) \,\right\}.$$

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 $f \in \mathrm{PF}_{\mathrm{hon}}$ and let $t, r : \mathbf{N} \to \mathbf{N}$.

(1) f is *weakly $t(n)$-one-way* if for every $g \in \mathrm{DTIMEF}(t)$ there exists $n \in \mathbf{N}$ such that

$$\Pr(\mathcal{I}[f,g](n)) < 1.$$

(2) f is *weakly $(t(n), r(n)\not\in)$-one-way* if for every $g \in \mathrm{DTIMEF}(t)$ there exists $n \in \mathbf{N}$ such that

$$\Pr(\mathcal{I}_{\mathrm{rand}}[f,g,r](n)) < 1.$$

(3) f is *weakly $(t(n)/r(n))$-one-way* if for every $g \in \mathrm{DTIMEF}(t)/\mathrm{ADV}(r)$ there exists $n \in \mathbf{N}$ 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 $g \in \mathrm{DTIMEF}(t)$,

$$\Pr(\mathcal{I}[f,g](n)) < \frac{1}{q(n)} \text{ a.e.}$$

(5) f is *$(t(n), r(n)\not\in)$-one-way with polynomial security* if for all polynomials q and all $g \in \mathrm{DTIMEF}(t)$,

$$\Pr(\mathcal{I}_{\mathrm{rand}}[f,g,r](n)) < \frac{1}{q(n)} \text{ a.e.}$$

(6) f is *$(t(n)/r(n))$-one-way with polynomial security* if for all polynomials q and all $g \in \mathrm{DTIMEF}(t)/\mathrm{ADV}(r)$,

$$\Pr(\mathcal{I}[f,g](n)) < \frac{1}{q(n)} \text{ a.e.}$$

(7) f is *$t(n)$-one-way with exponential security* if for every $g \in \mathrm{DTIMEF}(t)$ there exists a real number $\epsilon > 0$ such that

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

(8) f is *$(t(n), r(n)\not\in)$-one-way with exponential security* if for every $g \in \mathrm{DTIMEF}(t)$ there exists a real number $\epsilon > 0$ such that

$$\Pr(\mathcal{I}_{\mathrm{rand}}[f,g,r](n)) < 2^{-n^{\epsilon}} \text{ a.e.}$$

(9) f is $(t(n)/r(n))$-*one-way with exponential security* if for every $g \in$ DTIMEF(t)/ADV(r) there exists a real number $\epsilon > 0$ such that

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

We briefly discuss these nine definitions. Intuitively, the function g is an *adversary* that we want to be unsuccessful in inverting f. In (1), (4), and (7), the adversaries are $t(n)$-time-bounded deterministic algorithms. In (2), (5), and (8), the adversaries are $t(n)$-time-bounded randomized algorithms that can use at most $r(n)$ coin tosses. In (3), (6), and (9), the adversaries are $t(n)$-time-bounded algorithms, augmented by at most $r(n)$ bits of nonuniform advice. Thus the adversary may be deterministic, randomized, or nonuniform, with computational power quantified by the functions t and r.

Whatever the power of the adversary, the nine definitions provide three levels of *security* against inversion. Definitions (1), (2), and (3) provide essentially no security, stipulating only that the adversary sometimes fails to find a preimage. Definitions (4), (5), and (6) provide *polynomial security*, a level of security that has been extensively investigated in the past 10 years. Definitions (7), (8), and (9) provide *exponential security*, a very high level of security that may be preferable to polynomial security in some contexts.

Note that our terminology requires every one-way function to be in PF_{hon}, but does *not* require one-way functions to be one-to-one.

Only the following very weak type of one-way function is known to exist under the hypothesis that P $\neq$ NP.

Definition A *weak one-way function* is a function that is, for every polynomial t, weakly $t(n)$-one-way.

Theorem 5.1.(Allender [1]). P $\neq$ NP if and only if there exists a weak one-way function.

Using work of Karp and Lipton [18], 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 [6]), but such functions still do not provide a useful amount of security.

In Theorem 5.3 below, we will show that the hypothesis $\mu(\beta\text{NP} \mid \text{E}_2) \neq 0$ implies the existence of one-way functions with exponential security. The following lemma will simplify our proof.

Lemma 5.2. Assume that there exist a stricly increasing polynomial q and a function $f \in \mathrm{PF}_{\mathrm{hon}}^{(q)}$ with the following property.

(*) For every $g \in \mathrm{DTIMEF}(t)/\mathrm{ADV}(r)$ satisfying $|g(y)| = q(|y|)$ for all $y \in \{0,1\}^*$, there is a real number $\epsilon > 0$ such that

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

Then there exists a function that is $(t(n)/r(n))$-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 $\tilde{f} \in \mathrm{PF}_{\mathrm{hon}}$. To see that $\tilde{f}$ is $(t(n)/r(n))$-one-way with exponential security, let $\tilde{g} \in \mathrm{DTIMEF}(t)/\mathrm{ADV}(r)$. Define $g : \{0,1\}^* \to \{0,1\}^*$ by

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

Then $g \in \mathrm{DTIMEF}(t)/\mathrm{ADV}(r)$ 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

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

Now assume for a moment that $x \in \mathcal{I}[\tilde{f},\tilde{g}](m)$, 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 $|\tilde{g}(\tilde{f}(x))| \geq q(|\tilde{f}(x)|)$, so $g(\tilde{f}(x)) = \tilde{g}(\tilde{f}(x))[0..q(|\tilde{f}(x)|)-1] = \tilde{g}(\tilde{f}(x))[0..q(n_x)-1]$, so

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

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

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

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

$$\begin{aligned} \Pr(\mathcal{I}[\tilde{f}, \tilde{g}](m)) &\leq \Pr(\mathcal{I}[f, g](q(n_m))) \\ &< 2^{-q(n_m)^\epsilon} \\ &< 2^{-m^{\epsilon/2}}. \end{aligned}$$

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

□

We now come to the main result of this section.

Theorem 5.3. If $\mu(\beta\mathrm{NP} \mid \mathrm{E}_2) \neq 0$, then for every polynomial p there is a function that is $(2^{p(n)}/p(n))$-one-way with exponential security.

Proof. 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 $\mu(\beta\mathrm{NP} \mid \mathrm{E}_2) = 0$.

Let $A \in \beta\mathrm{NP}$. Fix a strictly increasing polynomial q and a function $f \in \mathrm{PF}_{\mathrm{bal}}^{(q)}$ such that $A = \mathrm{range}(f)$. Let $\epsilon = \frac{1}{2 \cdot deg(q)}$. Since there is no function that is $(2^{p(n)}/p(n))$-one-way with exponential security, Lemma 5.2 tells us that there is a function $g \in \mathrm{DTIMEF}(2^{p(n)})/\mathrm{ADV}(p(n))$ such that the set

$$I = \left\{ n \in \mathbf{N} \mid \Pr(\mathcal{I}[f, g](q(n))) \geq 2^{-q(n)^\epsilon} \right\}$$

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

We now have two cases.

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

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

(ii) $q(n)^\epsilon \leq n^{5/8}$.

(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 $f \in \mathrm{PF}_{\mathrm{bal}}^{(q)}$ 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 $n \in \mathbf{N}$, if $|f(\mathcal{I}[f,g](q(n)))| \geq 2^{\sqrt{n}}$, then $C_{=n} = f(\mathcal{I}[f,g](q(n)))$. Otherwise, $C_{=n} = \{0,1\}^n$. Note that $|C_{=n}| \geq 2^{\sqrt{n}}$ for all $n \in \mathbf{N}$. Also, since $f \in \mathrm{PF}_{\mathrm{bal}}^{(q)}$ and $g \in \mathrm{DTIMEF}(2^{p(n)})/\mathrm{ADV}(p(n))$, it is clear that $C \in \mathrm{DTIME}(2^{p(n)+2n})/\mathrm{ADV}(p(n))$. (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

$$\begin{aligned}
|f(\mathcal{I}[f,g](q(n)))| &\geq \frac{|I[f,g](q(n))|}{\max\limits_{y \in A_{=n}} |f^{-1}(\{y\})|} \\
&\geq \frac{2^{q(n)-q(n)^\epsilon}}{2^{q(n)-l^{3/4}}} \\
&= 2^{l^{3/4}-q(n)^\epsilon} \\
&\geq 2^{(n-2)^{3/4}-n^{5/8}} \\
&\geq 2^{\sqrt{n}}.
\end{aligned}$$

Thus, for all $n \in J$,

$$C_{=n} = f(\mathcal{I}[f,g](q(n))) \subseteq \mathrm{range}(f) = A,$$

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

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

as $n \to \infty$. Thus $\{0,1\}^*$ and C testify that $A \notin \mathrm{WS}(2^{p(n)+2n}, p(n), 2^{\sqrt{n}})$.

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 $A \notin \mathrm{WS}(2^{p(n)+2n}, p(n), 2^{\sqrt{n}})$.

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

$$\beta\mathrm{NP} \cap \mathrm{WS}(2^{p(n)+2n}, p(n), 2^{\sqrt{n}}) = \emptyset.$$

It follows by the Weak Stochasticity Theorem that $\mu(\beta\mathrm{NP} \mid \mathrm{E}_2) = 0$, completing the proof of Theorem 5.3.

□

Immediately from Theorem 5.3, we have:

Corollary 5.4. If $\mu(\beta\mathrm{NP} \mid \mathrm{E}_2) \neq 0$, 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 5.3.

Corollary 5.5. If $\mu(\beta\mathrm{NP} \mid \mathrm{E}_2) \neq 0$, then for every polynomial p, there is a function that is $(2^{p(n)}, p(n)\not!)$-one-way with exponential security.

It should be noted that the polynomial p is fixed in Theorem 5.3 and in Corollary 5.5. Thus, for example, Corollary 5.5 tells us that, if $\mu(\beta\mathrm{NP} \mid \mathrm{E}_2) \neq 0$ and k is a large integer, then there is a function f that is $(2^{n^k}, n^k\not!)$-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.

6 BPP-Pairs and Pseudorandom Generators

Yao [33] proved that, if nonuniformly secure pseudorandom generators exist, then $\mathrm{R} \subseteq \bigcap_{\epsilon>0} \mathrm{DTIME}(2^{n^\epsilon})$. Boppana and Hirschfeld [5] subsequently

refined Yao's argument to get the (apparently) stronger conclusion that $\mathrm{BPP} \subseteq \bigcap_{\epsilon>0} \mathrm{DTIME}(2^{n^\epsilon})$. In this section we prove that the hypothesis $\mu(\beta\mathrm{NP} \mid \mathrm{E}_2) \neq 0$ 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 $\bigcap_{\epsilon>0} \mathrm{DTIME}(2^{n^\epsilon})$ "separates all BPP-pairs." We first define the relevant notions.

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

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

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

$$\begin{aligned} \mathcal{B}^+ &= \{ x \in \{0,1\}^* \mid \Pr(\mathcal{B}_x) \geq \beta \}, \\ \mathcal{B}^- &= \{ x \in \{0,1\}^* \mid \Pr(\mathcal{B}_x) \leq \alpha \}, \end{aligned}$$

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

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

Note: if (A^+, A^-) is a BPP-pair, then $A^+ \cap A^- = \emptyset$. If, in addition, $A^+ \cup A^- = \{0,1\}^*$, then $A^+, A^- \in \mathrm{BPP}$. Using standard techniques [2, 30], 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 $(\mathcal{B}^+, \mathcal{B}^-)$ of languages, where $\mathcal{B} = (B, q, \alpha, \beta)$ is a BPP-configuration in which $\alpha = 0$. The complexity class R ("randomized polynomial time with one-sided error") is defined by

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

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

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

We now turn to pseudorandom generators.

Definition Let p be a polynomial. A $p(n)$-*generator* is a function $g \in$ 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 [33].

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

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

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.

The following fact is quite useful. A proof appears in [5].

Theorem 6.1. (Goldreich and Micali [11]). Let p and q be polynomials such that $p(n) \geq n + 1$ and $q(n) \geq n + 1$ for all $n \in \mathbf{N}$.

(1) Nonuniformly secure $p(n)$-generators exist if and only if nonuniformly secure $q(n)$-generators exist.

(2) Uniformly secure $p(n)$-generators exist if and only if uniformly secure $q(n)$-generators exist.

In light of Theorem 6.1, the following definition is sufficient.

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 6.2. (Yao[33], Boppana and Hirschfeld[5]). If nonuniformly secure pseudorandom generators exist, then BPP $\subseteq \bigcap_{\epsilon>0} \mathrm{DTIME}(2^{n^\epsilon})$. □

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 6.2.

Theorem 6.3. If nonuniformly secure pseudorandom generators exist, then for all $\epsilon > 0$, $\mathrm{DTIME}(2^{n^\epsilon})$ separates all BPP-pairs.

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

Fix a BPP-configuration $\mathcal{B} = (B, q, \alpha, \beta)$ such that $A^+ = \mathcal{B}^+$ and $A^- = \mathcal{B}^-$. Without loss of generality, assume that q is strictly increasing. Let $p(m) = q(m^{2/\epsilon})$. By our assumption, nonuniformly secure pseudorandom generators exist, so by Theorem 6.1 there exists a nonuniformly secure $p(m)$-generator g. For each $y \in \{0,1\}^*$, letting $n = |y|$ and $m = n^{\epsilon/2}$, define the "pseudo-critical event"

$$\mathcal{B}'_y = \{\, x \in \{0,1\}^m \mid \langle y, g(x)\rangle \in B \,\}.$$

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 $C \in \mathrm{DTIME}(2^{n^\epsilon})$.

Let

$$\begin{aligned} J^+ &= \{\, q(n) \mid (A^+ - C)_{=n} \neq \emptyset \,\}, \\ J^- &= \{\, q(n) \mid q(n) \notin J^+ \text{ and } (A^- \cap C)_{=n} \neq \emptyset \,\}, \\ J &= J^+ \cup J^- = \{\, q(n) \mid (A^+ - C)_{=n} \cup (A^- \cap C)_{=n} \neq \emptyset \,\}. \end{aligned}$$

Define an advice function $h : \mathbf{N} \to \{0,1\}^*$ as follows. For $j = q(n) \in J^+$, fix $h(j) \in (A^+ - C)_{=n}$. 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 $T \in \mathrm{P/Poly}$, i.e., T is a nonuniform test, so g passes T.

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

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

and

$$\begin{aligned} \Pr(T_{=p(m)}) &= \Pr[y \in T] \\ &= \Pr[\langle y, h(j)\rangle \in D] \\ &= \Pr[\langle h(j), y\rangle \in B] \\ &= \Pr(\mathcal{B}_{h(j)}) \\ &\geq \beta, \end{aligned}$$

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

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

and

$$\Pr(T_{=p(m)}) = \Pr(\mathcal{B}_{h(j)}) \leq \alpha,$$

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

$$\left|(A^+ - C) \cup (A^- \cap C)\right| < \infty,$$

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

The main result of this section, Theorem 6.6 below, is a partial converse of Theorem 6.3. In order to prove this result, 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, $(t(n), r(n)\not)$-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 6.4. (Impagliazzo, Levin, and Luby [16]). If nonuniformly one-way functions exist, then nonuniformly secure pseudorandom generators exist. □

Theorem 6.5. (Håstad [15]). If uniformly one-way functions exist, then uniformly secure pseudorandom generators exist. □

We now show that the hypothesis $\mu(\beta\mathrm{NP} \mid \mathrm{E}_2) \neq 0$ implies a partial converse of Theorem 6.3.

Theorem 6.6. If $\mu(\beta\mathrm{NP} \mid \mathrm{E}_2) \neq 0$ and $\mathrm{DTIME}(2^n)$ separates all BPP-pairs, then uniformly secure pseudorandom generators exist.

Proof. Assume that $\mathrm{DTIME}(2^n)$ separates all BPP-pairs and that uniformly secure pseudorandom generators do not exist. It suffices to prove that $\mu(\beta\mathrm{NP} \mid \mathrm{E}_2) = 0$.

Let $A \in \beta\mathrm{NP}$. Fix a strictly increasing polynomial p and a functon $f \in \mathrm{PF}_{\mathrm{bal}}^{(p)}$ such that $A = \mathrm{range}(f)$. By Theorem 6.5, uniformly one-way functions do not exist, so an argument analagous to the proof of Lemma 5.2 shows that there exist polynomials t, r, and q and a function $g \in \mathrm{DTIMEF}(t)$ such that the set

$$I = \left\{ n \in \mathbf{N} \mid \Pr(\mathcal{I}_{\mathrm{rand}}[f, g, r](p(n))) \geq \frac{1}{q(p(n))} \right\}$$

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

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

$$\mathcal{I}_y = \left\{ z \in \{0,1\}^{r(|y|)} \mid f(g(\langle y, z \rangle)) = y \right\},$$

and let

$$V = \left\{ y \in \{0,1\}^* \mid \Pr(\mathcal{I}_y) \geq \frac{1}{2q(p(|y|))} \right\},$$

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

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

$$\begin{aligned}
\frac{1}{q(p(n))} &\leq \Pr(\mathcal{I}_{\mathrm{rand}}[f, g, r](p(n))) \\
&= 2^{-p(n)} \sum_{x \in \{0,1\}^{p(n)}} \Pr(\mathcal{I}_{f(x)}) \\
&= 2^{-p(n)} \left[\sum_{x \in U_{=p(n)}} \Pr(\mathcal{I}_{f(x)}) + \sum_{x \in \{0,1\}^{p(n)} - U} \Pr(\mathcal{I}_{f(x)}) \right] \\
&\leq 2^{-p(n)} \left[\left| U_{=p(n)} \right| + 2^{p(n)} \frac{1}{2q(p(n))} \right].
\end{aligned}$$

Thus,

$$\left| U_{=p(n)} \right| \geq \frac{2^{p(n)}}{2q(p(n))}$$

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 $n_0 \in \mathbf{N}$ 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 $y \in A_{=n}$,

$$\left| f^{-1}(\{y\}) \right| \leq 2^{p(n)-l^{3/4}},$$

where $l = \log |A_{=n}|$.

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

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

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

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

$$\begin{aligned} |V_{=n}| &\geq \frac{\left|U_{=p(n)}\right|}{2^{p(n)-l^{3/4}}} \\ &\geq \frac{2^{l^{3/4}}}{2q(p(n))} \\ &\geq \frac{2^{(n-2)^{3/4}}}{2q(p(n))} \\ &\geq 2^{\sqrt{n}}. \end{aligned}$$

Now let B be the set of all $\langle y, z \rangle$ such that $z = z_1 \cdots z_{q(p(|y|))}$, where each $|z_i| = r(|y|)$ and $\mathcal{I}_y \cap \left\{ z_1, \cdots, z_{q(p(|y|))} \right\} \neq \emptyset$. Note that $B \in \mathrm{P}$. Define the polynomial

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

and consider the BPP-configuration

$$\mathcal{B} = (B, s, 0, 1/3).$$

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

The language C satisfies

$$V_{=n} \subseteq \mathcal{B}^+ \subseteq C \subseteq A$$

for all $n \geq n_0$. The second of these three inclusions is clear. Since $\mathcal{B}^- \cap C = \emptyset$, every element of C has a preimage under f, whence $C \subseteq \mathrm{range}(f) = A$, 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 $\Pr(\mathcal{I}_y) \geq \frac{1}{2q(p(n))}$, so the complement $\mathcal{B}_y^c$ of the critical event $\mathcal{B}_y$ has probability

$$\Pr(\mathcal{B}_y^c) \leq \left(1 - \frac{1}{2q(p(n))}\right)^{q(n)} < \frac{2}{3},$$

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

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

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

as $n \to \infty$. Since $\{0,1\}^*, D \in \mathrm{DTIME}(2^{2n})$ and $|D_{=n}| \geq 2^{\sqrt{n}}$ for all $n \in \mathbf{N}$, it follows that $A \notin \mathrm{WS}(2^{2n}, 0, 2^{\sqrt{n}})$.

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

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

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

It follows by the Weak Stochasticity Theorem that $\mu(\beta\mathrm{NP} \mid \mathrm{E}_2) = 0$, completing the proof of Theorem 6.6. □

Minor modification of the proof of Theorem 6.6 yields a somewhat stronger result:

Theorem 6.7. If $\mu(\beta\mathrm{NP} \mid \mathrm{E}_2) \neq 0$ and there is a constant k such that $\mathrm{DTIME}(2^{n^k})/\mathrm{ADV}(n^k)$ separates every R-pair, then uniformly secure pseudorandom generators exist.

7 Conclusion

We have addressed the following fundamental question.

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

We have shown that the hypothesis $\mu(\beta\mathrm{NP} \mid \mathrm{E}_2) \neq 0$ implies that cryptographically secure one-way functions exist. We have also shown that this hypothesis implies a partial converse to Yao, Boppana, and Hirschfeld's theorem on BPP and pseudorandom generators.

These results constitute a *prima facie* case for investigation of the class $\beta\mathrm{NP}$. It is *not* clear whether the hypothesis $\mu(\beta\mathrm{NP} \mid \mathrm{E}_2) \neq 0$ is plausible. Only further investigation will determine this. Such investigation may indicate that the consequences of $\mu(\beta\mathrm{NP} \mid \mathrm{E}_2) \neq 0$ 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 $\mu(\beta\mathrm{NP} \mid \mathrm{E}_2) \neq 0$, or even yield a proof that $\mu(\beta\mathrm{NP} \mid \mathrm{E}_2) = 0$. 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 $\beta\mathrm{NP}$.

Acknowledgements

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

References

[1] E. W. Allender. *Invertible Functions*. PhD thesis, Georgia Institute of Technology, 1985.

[2] J. L. Balcázar, J. Díaz, and J. Gabarró. *Structural Complexity I*. Springer-Verlag, Berlin, 1988.

[3] R. Beigel, M. Kummer, and F. Stephan. Approximable sets. *Information and Computation*, 20:304–314, 1995.

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

[5] R. B. Boppana and R. Hirschfeld. Pseudorandom generators and complexity classes. In S. Micali, editor, *Advances in Computing Research*, volume 5, pages 1–26. JAI Press Inc, 1989.

[6] R.B. Boppana and J.C. Lagarias. One-way functions and circuit complexity. *Lecture Notes in Computer Science*, 223:51–65, 1986.

[7] H. Chernoff. A measure of asymptotic efficiency for tests of a hypothesis based on the sum of observations. *Annals of Mathematical Statistics*, 23:493–509, 1952.

[8] A. Evans, W. Kantrowitz, and E. Weiss. A user authentication scheme not requiring secrecy in the computer. *Comm. ACM*, 17:437–442, 1974.

[9] A. V. Goldberg and M. Sipser. Compression and ranking. *SIAM Journal on Computing*, 20(3):524–536, June 1991.

[10] O. Goldreich, S. Goldwasser, and S. Micali. How to construct random functions. *Journal of the Association for Computing Machinery*, 33:792–807, 1986.

[11] O. Goldreich and S. Micali. reported in [5].

[12] O. Goldreich, S. Micali, and A. Wigderson. Proofs that yield nothing but their validity or all languages in NP have zero-knowledge proof systems. *Journal of the ACM*, 38(3):691–729, 1991.

[13] S. Goldwasser and S. Micali. Probabilistic encryption. *Journal of Computer and System Sciences*, 28(2):270–299, April 1984.

[14] T. Hagerup and C. Rüb. A guided tour of Chernoff bounds. *Information Processing Letters*, 33:305–308, 1990.

[15] J. Håstad. Pseudo-random generators under uniform assumptions. In *Proceedings of the Twenty-second Annual ACM Symposium on the Theory of Computing*, pages 395–404, 1990.

[16] R. Impagliazzo, L. A. Levin, and M. Luby. Pseudo-random generation from one-way functions. In *Proceedings of the Twenty-first ACM Symposium on the Theory of Computing*, pages 12–24, 1989.

[17] D. W. Juedes and J. H. Lutz. The complexity and distribution of hard problems. *SIAM Journal on Computing*, 24(2):279–295, 1995.

[18] R. M. Karp and R. J. Lipton. Some connections between nonuniform and uniform complexity classes. In *Proceedings of the 12th ACM Symposium on Theory of Computing*, pages 302–309, 1980. also published as Turing machines that take advice, *L'Enseignement Mathematique* **28** (1982), pp. 191–209.

[19] S. M. Kautz, 1993. personal communication.

[20] S. M. Kautz and P. B. Miltersen. Relative to a random oracle, np is not small. In *Proceedings of the Ninth Annual Structure in Complexity Theory Conference*, pages 162–174, 1994.

[21] M. Luby and C. Rackoff. How to construct pseudorandom permutations from pseudorandom functions. *SIAM Journal on Computing*, 17:373–386, 1988.

[22] J. H. Lutz. Resource-bounded measure. in preparation.

[23] J. H. Lutz. Category and measure in complexity classes. *SIAM Journal on Computing*, 19:1100–1131, 1990.

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

[25] J. H. Lutz and E. Mayordomo. Cook versus Karp-Levin: Separating completeness notions if NP is not small. *Theoretical Computer Science*. to appear. See also *Proceedings of the Eleventh Symposium on Theoretical Aspects of Computer Science*, Springer–Verlag, 1994, pp. 415–426.

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

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

[28] M. Naor. reported in [16].

[29] K. Regen, D. Sivakumar, and J. Cai. Pseudo random generators, measure theory, and natural proofs. In *Proceedings of the 1995 IEEE Symposium on Foundations of Computer Science*, 1995. to appear.

[30] U. Schöning. *Complexity and Structure*. Springer-Verlag, Berlin, 1986.

[31] A. L. Selman. One-way functions in complexity theory. In *Proceedings of the Fifteenth International Symposium on Mathematical Foundations of Computer Science*, pages 88–104. Springer-Verlag, 1990.

[32] Y. Wang. P-selective hard sets for exponential time, 1995. manuscript.

[33] A. Yao. Theory and applications of trapdoor functions. In *Proceedings of the 23rd IEEE Symposium on Foundations of Computer Science*, pages 80–91, 1982.