Measure, Stochasticity, and the Density of Hard Languages

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

Elvira Mayordomo
Iowa State University

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/108

This Article is brought to you for free and open access by the Computer Science at Iowa State University Digital Repository. It has been accepted for inclusion in Computer Science Technical Reports by an authorized administrator of Iowa State University Digital Repository. For more information, please contact digirep@iastate.edu.
Measure, Stochasticity, and the Density of Hard Languages

TR 92-13
Jack H. Lutz and Elvira Mayordomo

May 1992

Iowa State University of Science and Technology
Department of Computer Science
226 Atanasoff
Ames, IA 50011
Measure, Stochasticity, and the Density of Hard Languages
(Preliminary Version)

Jack H. Lutz
Department of Computer Science
Iowa State University
Ames, Iowa 50011
U.S.A.

Elvira Mayordomo
Dept. Llenguatges i Sistemes Informàtics
Universitat Politècnica de Catalunya
Pau Gargallo 5
08028 Barcelona, Spain

Abstract

Ogiwara and Watanabe have recently shown that the hypothesis
$P \neq NP$ implies that no (polynomially) sparse language is $\leq^P_{tt}$-hard
for NP. Their technique does not appear to allow significant relaxation
of either the query bound or the sparseness criterion. It is shown here
that a stronger hypothesis — namely, that NP does not have measure 0
in exponential time — implies the stronger conclusion that, for every
real $\alpha < 1$, every $\leq^P_{n^\alpha}$-hard language for NP is (exponentially)
dense.

The proof of this fact also yields two absolute results (not involving
unproven hypotheses) concerning the structure of exponential time:
First, almost every language decidable in exponential time has a
stochasticity property, ensuring that it is statistically unpredictable
by feasible deterministic algorithms, even with linear nonuniform ad-
vise. Second, for $\alpha < 1$, only a measure 0 subset of the languages
decidable in exponential time are $\leq^P_{n^\alpha}$-reducible to languages that
are not exponentially dense.

1This author’s research was supported in part by National Science Foundation Grant
CCR-9157382, in part by Rockwell International, and in part by DIMACS, where he was
a visitor during the first phase of this work.

2This author’s research, performed while visiting Iowa State University, was supported
by a Spanish Government grant, FPI PN90.
1 Introduction

How dense must a language $A \subseteq \{0, 1\}^*$ be in order to be hard for a complexity class $C$? The ongoing investigation of this question, especially important when $C = \text{NP}$, has yielded several significant results over the past 15 years.

Any formalization of this question must specify the class $C$ and give precise meanings to “hard” and “how dense.” The results of this paper concern the classes $E = \text{DTIME}(2^\text{linear})$, $E_2 = \text{DTIME}(2^\text{polynomial})$, and all subclasses $C$ of these classes, though we are particularly interested in the case $C = \text{NP}$.

We say that $A$ is $\leq^P_m$-hard for a class $C$ of languages if $C \subseteq P_r(A)$, where $P_r(A) = \{B \subseteq \{0, 1\}^* | B \leq^P A\}$. Here the polynomial time-bounded reducibility $\leq^P_m$ may be $\leq^P_m$ (many-one reducibility), $\leq^P_{T}(Turing$ reducibility), $\leq^P_{btt}(bounded\ truth-table\ reducibility)$, or $\leq^P_{q,tt}(truth\-table\ reducibility\ with\ q(n)\ queries\ on\ inputs\ of\ length\ n)\ where\ q : \mathbb{N} \to \mathbb{Z}^+$.

Two criteria for “how dense” a language $A$ is have been widely used. A language $A$ is (polynomially) sparse, and we write $A \in \text{SPARSE}$, if there is a polynomial $p$ such that $|A| \leq p(n)$ for all $n \in \mathbb{N}$, where $A|_n = A \cap \{0, 1\}^n$. A language $A$ is (exponentially) dense, and we write $A \in \text{DENSE}$, if there is a real number $\epsilon > 0$ such that $|A| \geq 2^n\epsilon$ for all sufficiently large $n \in \mathbb{N}$. It is clear that no sparse language is dense.

For any of the above choices of the reducibility $\leq^P_m$, all known $\leq^P_m$-hard languages for $	ext{NP}$ are dense. Efforts to explain this observation (and similar observations for other classes and reducibilities) have yielded many results. We mention four that are particularly relevant to the work presented here:

1. Meyer [16] proved that every $\leq^P_m$-hard language for $E$ (or any larger class) is dense. That is,

$$E \not\subset P_m(\text{DENSE}^c),$$

where $\text{DENSE}^c$ is the complement of $\text{DENSE}$ and we write $P_r(S) = \bigcup_{A \in S} P_r(A)$.

2. Watanabe [18, 19] extended Meyer’s result by proving that every $\leq^P_{btt}$-hard language for $E$ is dense. That is,

$$E \not\subset P_{btt}(\text{DENSE}^c).$$
In fact, Watanabe’s argument also works for \( \leq_{O(\log n)}^{P} \)-reducibility, i.e.,

\[ E \not\subseteq P_{O(\log n)}^{\text{tt}}(\text{DENSE}^{c}). \]

3. Mahaney [14], proving a conjecture of Berman and Hartmanis [1], showed that, unless \( P = \text{NP} \), no sparse language is \( \leq_{m}^{P} \)-hard for \( \text{NP} \). That is,

\[ P \neq \text{NP} \Rightarrow \text{NP} \not\subseteq P_{m}(\text{SPARSE}). \]

4. Ogiwara and Watanabe [17] extended Mahaney’s result by proving that, unless \( P = \text{NP} \), no sparse language is \( \leq_{\text{tt}}^{P} \)-hard for \( \text{NP} \). That is,

\[ P \neq \text{NP} \Rightarrow \text{NP} \not\subseteq P_{\text{tt}}(\text{SPARSE}). \]

The main result of this paper, Theorem 4.2, extends results 1 and 2 above by showing that, for every real \( \alpha < 1 \), only a measure 0 subset of the languages in \( E \) are \( \leq_{n^{\alpha}}^{P} \)-reducible to non-dense languages. “Measure 0 subset” here refers to the resource-bounded measure theory of Lutz [10, 11]. In the notation of this theory, our main result says that, for every real \( \alpha < 1 \),

\[ \mu(P_{n^{\alpha}}^{\text{tt}}(\text{DENSE}^{c})|E) = 0. \] (1.1)

This means that \( P_{n^{\alpha}}^{\text{tt}}(\text{DENSE}^{c}) \cap E \) is a negligibly small subset of \( E \) [10, 11]. This result, which requires a completely different technique from Watanabe’s result 2 above, extends result 2, both by imposing the measure 0 condition and by extending the truth table reducibility from \( O(\log n) \) queries to \( n^{\alpha} \) queries (\( \alpha < 1 \)). We also prove that this holds for \( E_{2} \), i.e., for every real \( \alpha < 1 \),

\[ \mu(P_{n^{\alpha}}^{\text{tt}}(\text{DENSE}^{c})|E_{2}) = 0. \] (1.2)

Note that there is an enormous gap between polynomial and \( 2^{n^{\alpha}} \) growth rates. (Consider, for example the \( G_{i} \)-hierarchy of [8].) Thus, a conclusion that every \( \leq_{P}^{P} \)-hard language for \( \mathcal{C} \) is dense is much stronger than a conclusion that no sparse language is \( \leq_{P}^{P} \)-hard for \( \mathcal{C} \).

Much of our interest in (1.1) and (1.2) concerns the class \( \text{NP} \) and results 3 and 4 above. It is well known that \( P \subseteq \text{NP} \subseteq E_{2} \). In fact, \( E_{2} \) is the smallest deterministic time complexity class known to contain \( \text{NP} \). It is easy to see [10] that \( \mu(P|E) = \mu(P|E_{2}) = 0 \), i.e., \( P \) has measure 0 in \( E \) and \( E_{2} \).
Ogiwara and Watanabe’s proof of result 4 above does not appear to allow significant relaxation of either the query bound or the sparseness criterion. However, Lutz has proposed an investigation of the (apparently) stronger hypotheses $\mu(NP|E) \neq 0$ and $\mu(NP|E_2) \neq 0$. (These expressions mean that NP does not have measure 0 in E and that NP does not have measure 0 in $E_2$, respectively. By the resource-bounded generalization of the Kolmogorov zero-one law [11], “$\mu(NP|E_2) \neq 0$” is equivalent to “$\mu(NP|E_2) = 1$ or NP is not measurable in $E_2$”, and similarly for $E$.) It follows immediately from (1.1) and (1.2) above that, for all $\alpha < 1$,

$$\mu(NP|E) \neq 0 \Rightarrow NP \not\subseteq P_{n^\alpha-tt}(DENSE^\ast) \quad (1.3)$$

and

$$\mu(NP|E_2) \neq 0 \Rightarrow NP \not\subseteq P_{n^\alpha-tt}(DENSE^\ast) \quad (1.4)$$

That is, unless NP is negligibly small in exponential time, every $\leq^{P}_{n^\alpha-tt}$-hard language for NP is dense. Comparing (1.3) and (1.4) with Mahaney and Ogiwara and Watanabe’s results 3 and 4 above, we have obtained a stronger conclusion from stronger hypotheses. Note that this stronger conclusion is consistent with our observations to date.

It should be noted that (1.3) and (1.4) follow immediately from (1.1) and (1.2) without using any property of NP. Thus (1.3) and (1.4) hold with NP replaced by PH, PP, PSPACE, or any other class whatsoever.

When proving results of the form

$$\mu(X|C) = 0,$$

where $C$ is a complexity class, it often simplifies matters to have available some general purpose randomness properties of languages in $C$. The term “general purpose randomness property” here is heuristic, meaning a set $Z$ of languages with the following two properties.

(i) Almost every language in $C$ has the property (of membership in) $Z$. (This condition, written $\mu(Z|C) = 1$, means that $\mu(Z^c|C) = 0$.)

(ii) It is often the case that, when one wants to prove a result of the form $\mu(X|C) = 0$, it is easier to prove that $X \cap Z = \emptyset$. For example, in $\text{ESPACE} = \text{DSpace}(2^{\text{linear}})$, it is known [10, 4] that almost every language has very high space-bounded Kolmogorov complexity.
A variety of sets $X$ have been shown to have measure 0 in ESPACE, simply by proving that every element of $X$ has low space-bounded Kolmogorov complexity [10, 4, 13, 9]. Thus high space-bounded Kolmogorov complexity is a “general purpose randomness property” of languages in ESPACE.

In §3 below, after reviewing some fundamentals of measure in complexity classes, we prove a Weak Stochasticity Theorem, stating that almost every language in $E$, and almost every language in $E_2$, is statistically unpredictable by feasible deterministic algorithms, even with linear nonuniform advice. Specifically, for every $c \in \mathbb{N}$ and every real number $\gamma > 0$, almost every language in $E$ has the following property: For all languages $C, D \in \text{DTIME}(2^m)$ and for all advice functions $h : \mathbb{N} \rightarrow \{0, 1\}^*$ satisfying $|h(n)| \leq cn$, suppose that we try to use $B = D/h = \{x | (x, h(x)) \in D\}$ to predict $A$ on the set $C$. If $|C_n| \geq 2^m$ for all sufficiently large $n$, then our prediction scheme will be asymptotically no better than random coin-tossing, i.e.,

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

Following the terminology of Kolmogorov [7], we call such a property a stochasticity property of the language $A$. To be precise, the above result says that almost every language $A \in E$ is weakly $(2^m, cn, 2^m)$-stochastic. The adverb “weakly” here defers to a stronger stochasticity property to be proven in [12], but weak stochasticity is a powerful and convenient tool. For example, in §4 below we prove (1.1) by a combinatorial construction showing that no language in $\text{P}_{\text{non-un}}(\text{DENSE}^c)$ is weakly $(2^{2n}, 3n, 2^{\frac{n}{2}})$-stochastic. We then appeal directly to the Weak Stochasticity Theorem of §3. It appears likely that the Weak Stochasticity Theorem will be useful for a variety of such applications in the future.

## 2 Preliminaries

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 $A \subseteq \{0, 1\}^*$. We
identify each language $A$ with its characteristic sequence $\chi_A \in \{0,1\}^\infty$ defined by
\[
\chi_A = \llbracket s_0 \in A \rrbracket \llbracket s_1 \in A \rrbracket \llbracket s_2 \in A \rrbracket,\]
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 $w \sqsubseteq x$, 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 $\lambda$ denotes the empty string.

As noted in §1, we work with the exponential time complexity classes $E = \text{DTIME}(2^{\text{linear}})$ and $E_2 = \text{DTIME}(2^{\text{polynomial}})$. It is well-known that $P \nsubseteq E \nsubseteq E_2$, that $P \subseteq \text{NP} \subseteq E_2$ and that $\text{NP} \neq E$.

We let $D = \{m2^{-n} \mid m \in \mathbb{Z}, n \in \mathbb{N}\}$ 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 $Y$ is $D$ 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 $Y = D$.

For example, a function $d : \mathbb{N}^2 \times \{0,1\}^* \to D$ is formally interpreted as a function $\hat{d} : \{0,1\}^* \to \{0,1\}^*$. Under this interpretation, $\hat{d}(i, j, w) = r$ means that $\hat{d}((0^i, 0^j, w)) = u$, where $u$ is a suitable binary encoding of the dyadic rational $r$.

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 $d_k(x) = d(k, x) = d(0^k, x)$. 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 $d_{k,i} = (d_k)_i$, 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 uses the following form of the Chernoff bound.
Lemma 2.1 [2, 3]. 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

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

In particular, taking $\epsilon = \frac{2}{j+1}$, where $j \in \mathbb{N}$,

$$\Pr[|S - \frac{N}{2}| \geq \frac{N}{j+1}] \leq 2e^{-\frac{N}{2(j+1)^2}}.$$ 

Proof. See [3]. \qed

3 Measure and Weak Stochasticity

In this section, after reviewing some fundamentals of measure in exponential time complexity classes, we prove the Weak Stochasticity Theorem. This theorem will be useful in the proof of our main result in §4. We also expect it to be useful in future investigations of the measure structure of E and E2.

Resource-bounded measure [10, 11] 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 and E2, so our discussion of measure is specific to these classes.

Throughout this section, we identify every language $A \subseteq \{0, 1\}^*$ with its characteristic sequence $\chi_A \in \{0, 1\}^\infty$, defined as in §2.

A constructor is a function $\delta : \{0, 1\}^* \to \{0, 1\}^*$ 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 $R(\delta)$. Given a set $\Delta$ of functions from $\{0, 1\}^*$ into $\{0, 1\}^*$, we write $R(\Delta)$ for the set of all languages $R(\delta)$ such that $\delta \in \Delta$ and $\delta$ is a constructor.

We first note that the exponential time complexity classes E and E2 can be characterized in terms of constructors.
Notation. The classes \( p_1 = p \) and \( p_2 \), both consisting of functions \( f : \{0,1\}^* \rightarrow \{0,1\}^* \), are defined as follows.

\[
\begin{align*}
\text{p}_1 &= p = \{ f | f \text{ is computable is polynomial time} \} \\
\text{p}_2 &= \{ f | f \text{ is computable is } n^{O(1)} \text{ time} \}
\end{align*}
\]

**Lemma 3.1.** [8]

1. \( R(p) = E \).
2. \( R(p_2) = E_2 \).

Using Lemma 3.1, the measure structures of \( E \) and \( E_2 \) are now developed in terms of the classes \( p_i \), for \( i = 1, 2 \).

**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

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

(Recall that \( C_w = \{ x \in \{0,1\}^\infty \mid w \subseteq x \} \) 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

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

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

**Definition** A computation of an $n$-DS $d$ is a function

$$\hat{d} : \mathbb{N}^{n+1} \times \{0, 1\}^* \rightarrow D$$

such that

$$| \hat{d}_{k^r}(w) - d_k(w) | \leq 2^{-r}$$

for all $k \in \mathbb{N}^n$, $r \in \mathbb{N}$, and $w \in \{0, 1\}^*$. For $i = 1, 2$, a $p_i$-computation of an $n$-DS $d$ is a computation $\hat{d}$ of $d$ such that $\hat{d} \in p_i$. An $n$-DS $d$ is $p_i$-computable if there exists a $p_i$-computation $\hat{d}$ of $d$.

If $d$ is an $n$-DS such that $d : \mathbb{N}^n \times \{0, 1\}^* \rightarrow D$ and $d \in p_i$, then $d$ is trivially $p_i$-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 $d_k(\lambda) \leq 2^{-k}$. For $i = 1, 2$, a $p_i$-null cover of $X$ is a null cover of $X$ that is $p_i$-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 $p_i$-measure 0, and we write $\mu_{p_i}(X) = 0$, if there exists a $p_i$-null cover of $X$. A set $X$ has $p_i$-measure 1, and we write $\mu_{p_i}(X) = 1$, if $\mu_{p_i}(X^c) = 0$. Thus a set $X$ has $p_i$-measure 0 if $p_i$ 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 structures of $E = \mathbb{R}(p_1)$ and $E_2 = \mathbb{R}(p_2)$.

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

The following lemma is obvious but useful.

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

\[
\begin{align*}
\mu_p(X) = 0 & \quad \implies \quad \mu_{p_2}(X) = 0 & \quad \implies \quad \Pr[x \in X] = 0 \\
\downarrow & & \downarrow \\
\mu(X|E) = 0 & \quad \mu(X|E_2) = 0,
\end{align*}
\]

where the probability $\Pr[x \in X]$ is computed according to the random experiment in which a sequence $x \in \{0, 1\}^\omega$ 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 $p$-measure 0 gives information about the size of $X$ in $E$, in $E_2$, and in $\{0, 1\}^\omega$.

It was noted in Lemma 3.2 that $\mu_p(X) = 0$ implies $\mu_{p_2}(X) = 0$. In fact, more is true.

**Lemma 3.3.** [12] Let $Z$ be the union of all sets $X$ such that $\mu_p(X) = 0$. Then $\mu_{p_2}(Z) = 0$.

(The proof of Lemma 3.3 makes essential use of the fact that $p_2$ contains a universal function for $p$. It is *not* the case that $\mu_p(Z) = 0$.)

It is shown in [10] that these definitions endow $E$ and $E_2$ with internal measure structure. Specifically, for $i = 1, 2$, if $\mathcal{I}$ is either the collection $\mathcal{I}_{p_i}$ of all $p_i$-measure 0 sets or the collection $\mathcal{I}_{\mathbb{R}(p_i)}$ of all sets of measure 0 in $\mathbb{R}(p_i)$, then $\mathcal{I}$ is a “$p_i$-ideal”, i.e., is closed under subsets, finite unions, and “$p_i$-unions” (countable unions that can be generated with the resources of $p_i$). More importantly, it is shown that the ideal $\mathcal{I}_{\mathbb{R}(p_i)}$ is a *proper* ideal, i.e., that $E$ does *not* have measure 0 in $E$ and $E_2$ does *not* have measure 0 in $E_2$. Taken together, these facts justify the intuition that, if $\mu(X|E) = 0$, then $X \cap E$ is a *negligibly small* subset of $E$ (and similarly for $E_2$).
Our proof of the Weak Stochasticity Theorem does not directly use the above definitions. Instead we use a sufficient condition, proved in [10], for a set to have measure 0. To state this condition we need a polynomial notion of convergence for infinite series. All our series here consist of nonnegative terms. A \textit{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 \textit{p-convergent} if it has a modulus that is a polynomial. A sequence

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

of series is \textit{uniformly p-convergent} if there exists a polynomial $m : \mathbb{N} \to \mathbb{N}$ such that, 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-convergence. (This well-known lemma is easily verified by routine calculus.)

\textbf{Lemma 3.4.} Let $a_{j,k} \in [0, \infty)$ for all $j, k \in \mathbb{N}$. If there exist a real $\varepsilon > 0$ and a polynomial $g : \mathbb{N} \to \mathbb{N}$ such that $a_{j,k} \leq e^{-k^\varepsilon}$ for all $j, k \in \mathbb{N}$ with $k \geq g(j)$, then the series

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

are uniformly p-convergent. \hfill \Box

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

\textbf{Lemma 3.5.} [10]. If $d$ is a p-computable 2-DS such that the series

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

are uniformly p-convergent, then

$$\mu^p \left( \bigcup_{j=0}^{\infty} \bigcap_{t=0}^{\infty} \bigcup_{k=t}^{\infty} S[d_{j,k}] \right) = 0. \hfill \Box$$
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-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 [6]. An advice function is a function \( h : \mathbb{N} \rightarrow \{0, 1\}^* \). Given a function \( q : \mathbb{N} \rightarrow \mathbb{N} \), 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 \( t, q : \mathbb{N} \rightarrow \mathbb{N} \), we define the advice class

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

**Definition** Let \( t, q, \nu : \mathbb{N} \rightarrow \mathbb{N} \) and let \( A \subseteq \{0, 1\}^* \). Then \( A \) is weakly \((t, q, \nu)\)-stochastic if, for all \( B \in \text{DTIME}(t)/\text{ADV}(q) \) and all \( C \in \text{DTIME}(t) \) 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.

The following lemma captures the main technical content of the Weak Stochasticity Theorem.

**Lemma 3.6.** Fix \( c \in \mathbb{N} \) and \( 0 < \gamma \in \mathbb{R} \) and let

\[
WS_{c,\gamma} = \{ A \subseteq \{0, 1\}^* \mid A \text{ is weakly } (2^m, cn, 2^m)\text{-stochastic} \}.
\]

Then \( \mu_p(WS_{c,\gamma}) = 1 \).

**Proof.** Assume the hypothesis. Let \( U \in \text{DTIME}(2^{(c+1)m}) \) be a language that is universal for \( \text{DTIME}(2^m) \times \text{DTIME}(2^m) \) in the following sense: For each \( i \in \mathbb{N} \), let

\[
C_i = \{ x \in \{0, 1\}^* \mid (0^i, 0x) \in U \},
\]
Then DTIME(2^n) × DTIME(2^m) = \{(C_i, D_i) | i ∈ N\}.

For all i, j, k ∈ 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} = ∅. Otherwise, if k = 2^n, where n ∈ N, then

\[ Y_{i,j,k} = \bigcup_{z \in \{0,1\}^{\leq cn}} Y_{i,j,k,z}, \]

where each

\[ Y_{i,j,k,z} = \{ A \subseteq \{0,1\}^* \mid |(C_i)_z| \geq 2^m \]

\[ \text{and } \left| \frac{|(A \triangle (D_i/z)) \cap (C_i)_z|}{|(C_i)_z|} - \frac{1}{2} \right| \geq \frac{1}{j+1} \} \right\}. \]

It is immediate from the definition of weak stochasticity that the complement WS_{c,γ} of WS_{c,γ} satisfies

\[ WS_{c,γ}^c \subseteq \bigcup_{i=0}^{∞} \bigcap_{j=0}^{∞} \bigcup_{m=0}^{∞} \bigcup_{k=m}^{∞} Y_{i,j,k}. \]

It follows by Lemma 3.5 that it suffices to exhibit a p-computable 3-DS d with the following two properties.

(I) The series \( \sum_{k=0}^{∞} d_{i,j,k}(\lambda) \), for i, j ∈ N, are uniformly p-convergent.

(II) For all i, j, k ∈ N, Y_{i,j,k} ⊆ S[d_{i,j,k}].

Define the function d : N^3 × {0,1}^* → [0,∞) as follows. If k is not a power of 2, then d_{i,j,k}(w) = 0. Otherwise, if k = 2^n, where n ∈ N, then

\[ d_{i,j,k}(w) = \sum_{z \in \{0,1\}^{\leq cn}} \Pr(Y_{i,j,k,z} \mid C_w), \]

where the conditional probabilities \( \Pr(Y_{i,j,k,z} \mid C_w) = \Pr[A \in Y_{i,j,k,z} \mid A \in C_w] \) are computed according to the random experiment in which the language A ⊆ {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 $U \in \text{DTIME}(2^{(c+1)n})$ and $c$ is fixed, we can use binomial coefficients to (exactly) compute $d_{i,j,k}(w)$ in time polynomial in $i+j+k+|w|$. Thus $d$ is p-computable.

To see that $d$ has property (I), note first that the Chernoff bound, Lemma 2.1, tells us that, for all $i, j, k \in \mathbb{N}$ and $z \in \{0,1\}^c$ (writing $k = 2^n$ and $N = k^\gamma = 2^m$),

$$\Pr(Y_{i,j,k,z}) \leq 2e^{-\frac{k^\gamma N}{2(j+1)^{\delta+1}}} ,$$

whence

$$d_{i,j,k}(\lambda) = \sum_{z \in \{0,1\}^c} \Pr(Y_{i,j,k,z}) \leq 2^{cn+1} \cdot 2e^{-\frac{k^\gamma N}{2(j+1)^{\delta+1}}} < e^{cn+2\frac{k^\gamma N}{2(j+1)^{\delta+1}}} .$$

Let $a = \left[ \frac{1}{\gamma} \right]$, let $\delta = \frac{\alpha}{\gamma}$, and fix $k_0 \in \mathbb{N}$ such that

$$k^2 \delta \geq k^\delta + c \log k + 2$$

for all $k \geq k_0$. Define $g : \mathbb{N} \to \mathbb{N}$ by

$$g(j) = 4^a(j+1)^{4a} + k_0 .$$

Then $g$ is a polynomial and, for all $i, j, n \in \mathbb{N}$ (writing $k = 2^n$ and $N = k^\gamma = k^{4\delta}$),

$$k \geq g(j) \implies \left\{ \begin{array}{l} N = k^2 \delta k^{2\delta} \\
\geq \left[ 4^a(j+1)^{4a} \right]^{2\delta} (k^\delta + c \log k + 2) \\
\geq 2(j+1)^2 (k^\delta + cn + 2) \end{array} \right. \implies d_{i,j,k}(\lambda) < e^{-k^\delta} .$$

Thus $d_{i,j,k}(\lambda) < e^{-k^\delta}$ for all $i, j, k \in \mathbb{N}$ such that $k \geq g(j)$. Since $\delta > 0$, it follows by Lemma 3.4 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 $z \in \{0,1\}^c$ such that $A \in Y_{i,j,k,z}$ and let $w$ be the $(2^{n+1} - 1)$-bit characteristic string of $A \leq n$. Then

$$d_{i,j,k}(w) \geq \Pr(Y_{i,j,k,z}|C_w) = 1 .$$
so \(A \in C_w \subseteq S[d_{i,j,k}].\) This completes the proof of Lemma 3.6.

We now have the Weak Stochasticity Theorem.

**Theorem 3.7.**

1. For all \(c \in \mathbb{N}\) and \(\gamma > 0,\) almost every language \(A \in E\) is weakly \((2^m, cn, 2^m)\)-stochastic.

2. Almost every language \(A \in E_2\) is, for all \(c \in \mathbb{N}\) and \(\gamma > 0,\) weakly \((2^m, cn, 2^n)\)-stochastic.

**Proof.** Part (1) follows immediately from Lemma 3.6 via Lemma 3.2. Part (2) follows from Lemma 3.6 via Lemmas 3.3 and 3.2.

### 4 The Density of Hard Languages

In this section we prove our main result, that for every real \(\alpha < 1,\) the set \(P_{\alpha}-\text{tt}(\text{DENSE}^c)\) has measure 0 in \(E\) and in \(E_2.\) Some terminology and notation will be useful.

Given a query-counting function \(q : \mathbb{N} \to \mathbb{Z}^+\), a \(q\)-query function is a function \(f\) with domain \(\{0, 1\}^*\) such that, for all \(x \in \{0, 1\}^*,\)

\[
f(x) = (f_1(x), \ldots, f_{\varphi(|x|)}(x)) \in (\{0, 1\}^*)^{\varphi(|x|)}.
\]

Each \(f_i(x)\) is called a query of \(f\) on input \(x.\) A \(q\)-truth table function is a function \(g\) with domain \(\{0, 1\}^*\) such that, for each \(x \in \{0, 1\}^*, g(x)\) is the encoding of a \(q(|x|)\)-input, 1-output Boolean circuit. We write \(g(x)(w)\) for the output of this circuit on input \(w \in \{0, 1\}^{\varphi(|x|)}\). A \(\leq^P_{\psi-\text{tt}}\)-reduction is an ordered pair \((f, g)\) such that \(f\) is a \(q\)-query function, \(g\) is a \(q\)-truth table function, and \(f\) and \(g\) are computable in polynomial time.

Let \(A, B \subseteq \{0, 1\}^*.\) \(A \leq^P_{\psi-\text{tt}}\)-reduction of \(A\) to \(B\) is a \(\leq^P_{\psi-\text{tt}}\)-reduction \((f, g)\) such that, for all \(x \in \{0, 1\}^*,\)

\[
[x \in A] = g(x)([f_1(x) \in B] \cdots [f_{\varphi(|x|)}(x) \in B]).
\]

(Recall that \([\psi]\) denotes the Boolean value of the condition \(\psi.\)) In this case we say that \(A \leq^P_{\psi-\text{tt}} B\) via \(g.\) We say that \(A\) is \(\leq^P_{\psi-\text{tt}}\)-reducible to \(B,\) and write \(A \leq^P_{\psi-\text{tt}} B,\) if there exists \((f, g)\) such that \(A \leq^P_{\psi-\text{tt}} B\) via \((f, g).\)
The proof of our main result makes essential use of the following construction.

Given an $n^\alpha$-query function $f$ and $n \in \mathbb{N}$, the \textit{sequentially most frequent query selection} (smfq selection) for $f$ on inputs of length $n$ is the sequence

$$(S_0, Q_0, y_0), (S_1, Q_1, y_1), \ldots, (S_{n^\alpha}, Q_{n^\alpha}, y_{n^\alpha})$$

defined as follows. Each $S_k \subseteq \{0,1\}^n$. Each $Q_k$ is an $|S_k| \times n^\alpha$ matrix of strings, with each string in $Q_k$ colored either green or red. The rows of $Q_k$ are indexed lexicographically by the elements of $S_k$. For $x \in S_k$, row $x$ of $Q_k$ is the sequence $f_1(x), \ldots, f_{n^\alpha}(x)$ of queries of $f$ on input $x$. If $Q_k$ contains at least one green string, then $y_k$ is the green string occurring in the greatest number of rows of $Q_k$. (Ties are broken lexicographically.) If $Q_k$ is entirely red, then $y_k = \top$ ("top," i.e., undefined). The sets $S_k$ and the coloring are specified recursively. We set $S_0 = \{0,1\}^n$ and color all strings in $Q_0$ green. Assume that $S_k, Q_k,$ and $y_k$ have been defined, where $0 \leq k < n^\alpha$. If $y_k = \top$, then $(S_{k+1}, Q_{k+1}, y_{k+1}) = (S_k, Q_k, y_k)$. If $y_k \neq \top$, then $S_{k+1}$ is the set of all $x \in S_k$ such that $y_k$ appears in row $x$ of $Q_k$. The strings in $Q_{k+1}$ are then colored exactly as they were in $Q_k$, except that all $y_k$'s are now colored red. This completes the definition of the smfq selection.

For $0 \leq k \leq n^\alpha$, it is clear that every row of $Q_k$ contains at least $k$ red strings. In particular, the matrix $Q_{n^\alpha}$ is entirely red.

Our main results follow from the following lemma. Recall that $WS_{c, \gamma}$ is the set of all weakly $(2^{cn}, cn, 2^m)$-stochastic languages.

\textbf{Lemma 4.1.} For every real $\alpha < 1$, $P_{n^\alpha-\epsilon}(\text{DENSE}) \cap WS_{3, \frac{\alpha}{2}} = \emptyset$.

\textbf{Proof.} Let $\alpha < 1$ and assume that $A \preceq_{n^\alpha-\epsilon} L$ via $(f, g)$, where $L \not\in \text{DENSE}$. It suffices to show that $A \not\in WS_{3, \frac{\alpha}{2}}$. Fix a polynomial $p$ such that $|f_i(x)| \leq p(|x|)$ for all $x \in \{0,1\}^n$ and $1 \leq i \leq |x|^\alpha$. Let $\epsilon = \frac{1-\epsilon}{4}$ and fix $n_0 \in \mathbb{N}$ such that the following conditions hold for all $n \geq n_0$.

\begin{enumerate}
  \item[(i)] $n \geq 2 \cdot n_1^{1-2\epsilon}$.
  \item[(ii)] $n^{2\epsilon} - n^\epsilon \geq 2$.
\end{enumerate}

Let

$$K = \{ n \in \mathbb{N} | n \geq n_0 \text{ and } |L_{\preceq p(n)}| < 2^{\epsilon n} \}.$$
Note that $K$ is infinite because $L$ is not dense.

Define languages $B$, $C$, $D$ and an advice function $h : \mathbb{N} \to \{0,1\}^*$ as follows. For all $n < n_0$, $C_{=n} = D_{=n} = \{0,1\}^n$ and $h(n) = \lambda$. For all $n \geq n_0$, $C_{=n}$, $D_{=n}$, and $h(n)$ are defined from the smfq selection for $f$ on inputs of length $n$ as follows: Let $k = k(n)$ be the greatest integer such that $0 \leq k \leq n^\alpha$ and $|S_k| \geq 2^{n-kn^2\epsilon}$. (Note that $k$ exists because $|S_0| = 2^n$.) We then define

$$C_{=n} = S_k,$$

$$h(n) = [y_0 \in L]..., [y_{k-1} \in L],$$

and we let $D_{=n}$ be the set of all coded pairs $(x, z)$ such that $x \in S_k$, $z \in \{0,1\}^k$, and $g(x)(b_1...b_{n^\alpha}) = 1$, where each

$$b_i = \begin{cases} z[j] & \text{if } f_i(x) = y_j, 0 \leq j < k, \\ 0 & \text{if } f_i(x) \notin \{y_0, ..., y_{k-1}\}. \end{cases}$$

Finally, we let $B = D/h$. Intuitively here, $B$ tries to predict $A$ on $C$. Specifically, for each $n \geq n_0$ and each $x \in C_{=n} = S_k$, the bit $[x \in B]$ is a “guessed value” of the bit $[x \in A]$. The actual value, given by the reduction $(f, g)$ to $L$, is

$$[x \in A] = g(x)([w_i \in L]..., [w_{n^\alpha} \in L]),$$

where $w_1,...,w_{n^\alpha}$ are the entries in row $x$ of the matrix $Q_k$. The guessed value $[x \in B] = g(x)(b_1...b_{n^\alpha})$ uses the advice function $h$ to get the correct bit $b_i = [w_i \in L]$ when the string $w_i$ is red in $Q_k$, and guesses that $w_i \notin L$ when the string $w_i$ is green in $Q_k$.

It is easy to see that $C, D \in \text{DTIME}(2^{3n})$ and $B \in \text{DTIME}(2^{3n})/\text{ADV}(3n)$. (The bound $3n$ is generous here.) Also, by condition (i) in our choice of $n_0$,

$$|C_{=n}| \geq 2^{n-n^\alpha n^2\epsilon} \geq 2^n$$

for all $n \geq n_0$, whence $|C_{=n}| \geq 2^n$ for all $n \in \mathbb{N}$.

We now show that $B$ does a good job of predicting $A$ on $C_{=n}$, for all $n \in K$. Let $n \in K$. We have two cases.

(I) If $k = k(n) = n^\alpha$, then all strings in $Q_k$ are red, so all the guesses made by $B$ are correct, so

$$|(A \triangle B) \cap C_{=n}| = 0.$$
(II) If \( k = k(n) < n^\alpha \), let \( r \) be the number of rows in \( Q_k \), i.e., \( r = |S_k| = |C_n| \). By our choice of \( k \), we have
\[
|S_{k+1}| \leq 2^{n-(k+1)n^{2e}} \leq 2^{-n^{2e} r}.
\]
That is, no green string appears in more than \( 2^{-n^{2e}} r \) of the rows of \( Q_k \). Moreover, since \( |L_{\leq p(n)}| \leq 2^{n^e} \), there are at most \( 2^{n^e} \) green strings \( w \) in \( Q_k \) such that \( w \in L \). Thus there are at most \( 2^{n^e} \cdot 2^{-n^{2e} r} = 2^{n^e-n^{2e} r} \) rows of \( Q_k \) in which \( B \) makes an incorrect guess that a green string is not in \( L \); the guesses made by \( B \) are correct in all other rows! By condition (ii) in our choice of \( n_0 \), then, \( B \) is incorrect in at most \( \frac{1}{4} r \) rows of \( Q_k \). That is,
\[
|(A \triangle B) \cap C_n| \leq \frac{1}{4} r.
\]
In either case, (I) or (II), we have
\[
|(A \triangle B) \cap C_n| \leq \frac{1}{4} |C_n|.
\]
Since this holds for all \( n \in K \), and since \( K \) is infinite,
\[
\frac{|(A \triangle B) \cap C_n|}{|C_n|} \neq \frac{1}{2}.
\]
Thus \( B \) and \( C \) testify that \( A \) is not weakly \((2^{3n}, 3n, 2^n)\)-stochastic, i.e., that \( A \not\in WS_{S, \frac{3}{2}} \).

Our main results are now clear.

**Theorem 4.2.** For every real \( \alpha < 1 \),
\[
\mu(P_n^{\alpha-\mu}(DENSE^c)|E) = \mu(P_n^{\alpha-\mu}(DENSE^c)|F_2) = 0.
\]

**Proof.** This follows immediately from Theorem 3.7 and Lemma 4.1. \( \square \)

As noted in §1, Theorem 4.2 extends Watanabe’s result [18, 19] that every \( \leq_P^{\mu} \)-hard language for \( E \) is dense, both by relaxing the query bound and by imposing the measure 0 condition: If a language \( A \) is even weakly \( \leq_P^{\mu} \)-hard for \( E \), in the sense that \( P_n^{\mu}(A) \) does not have measure 0 in \( E \), then Theorem 4.2 tells us that \( A \) must be dense.
Finally, we note the consequence for NP.

**Theorem 4.3.** If $\mu(\text{NP}|E) \neq 0$ or $\mu(\text{NP}|E_2) \neq 0$, then for all $\alpha < 1$, every $\leq_{n^\alpha}^\text{tt}$-hard language for NP is dense, i.e., $\text{NP} \not\subseteq \text{P}_{n^\alpha}^\text{tt}(\text{DENSE}^*)$.

**Proof.** If NP has a $\leq_{n^\alpha}^\text{tt}$-hard language $H$ that is not dense then Theorem 4.2 tells us that $\mu(\text{NP}|E) = \mu(\text{P}_{n^\alpha}^\text{tt}(H)|E) = 0$ and $\mu(\text{NP}|E_2) = \mu(\text{P}_{n^\alpha}^\text{tt}(H)|E_2) = 0$. \hfill $\Box$

Note that the hypothesis and conclusion of Theorem 4.3 are both stronger than their counterparts in Ogiwara and Watanabe’s result that

$$\text{P} \neq \text{NP} \Rightarrow \text{NP} \not\subseteq \text{P}_{\text{tt}}(\text{SPARSE}).$$

Note also that Theorem 4.3 holds with NP replaced by PH, PP, PSPACE, or any other class.

5 Conclusion

The density criterion in Theorem 4.2 cannot be improved, since for every $\epsilon > 0$ there is a language $A \in E$ that is $\leq_{m}^\text{P}$-hard for $E_2$ and satisfies $|A_{\leq n}| < 2^n\epsilon$ for all $n$. It is an open question whether the query bound $n^\alpha$ can be significantly relaxed. A construction of Wilson [20] shows that there is an oracle $B$ such that $E^B \subseteq P_{O(\log n)\text{-tt}}^B(\text{SPARSE})$, so progress in this direction will require nonrelativizable techniques.

The hypothesis that $\mu(\text{NP}|E_2) \neq 0$, i.e., that NP is not a negligibly small subset of $E_2$, has recently been shown to have a number of plausible consequences: If $\mu(\text{NP}|E_2) \neq 0$, then NP contains p-random languages [12]; NP contains E-bi-immune languages [15]; every $\leq_m^\text{P}$-hard language for NP has an exponentially dense, exponentially hard complexity core [5]; and now, by Theorem 4.3 above, every $\leq_{n^\alpha}^\text{tt}$-hard language for NP ($\alpha < 1$) is exponentially dense. Further investigation of the consequences and plausibility of $\mu(\text{NP}|E_2) \neq 0$ and related strong, measure-theoretic hypotheses is clearly indicated.
References


