Cook versus Karp-Levin: Separating Completeness Notions If NP Is Not Small*

(Preliminary Version—August 14, 1992)

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

Under the hypothesis that NP does not have p-measure 0 (roughly, that NP contains more than a negligible subset of exponential time), it is show n that there is a language that is $\leq_{\mathrm{T}}^{\mathrm{P}}$-complete ("Cook complete"), but not $\leq_{m}^{\mathrm{P}}$-complete ("Karp-Levin complete"), for NP. This conclusion, widely believed to be true, is not known to follow from $\mathrm{P} \neq \mathrm{NP}$ or other traditional complexity-theoretic hypotheses.

Evidence is presented that "NP does not have p-measure 0" is a reasonable hypothesis with many credible consequences. Additional such consequences proven here include the separation of many truth-table reducibilities in NP (e.g., k queries versus $k+1$ queries), the class separation $\mathrm{E} \neq \mathrm{NE}$, and the existence of NP search problems that are not reducible to the corresponding decision problems.

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

1 Introduction

The NP-completeness of decision problems has two principal, well-known formulations. These are the polynomial-time Turing completeness ($\leq_{\mathrm{T}}^{\mathrm{P}}$-completeness) introduced by Cook [5] and the polynomial-time many-one completeness ($\leq_{m}^{\mathrm{P}}$-completeness) introduced by Karp [8] and Levin [11]. These two completeness notions, sometimes called "Cook completeness" and "Karp-Levin completeness," have been widely conjectured, but not proven, to be distinct. The main purpose of this paper is to exhibit a reasonable complexity-theoretic hypothesis that implies the distinctness of these two completeness notions.

In general, given a polynomial-time reducibility $\leq_{r}^{\mathrm{P}}$ (e.g., $\leq_{\mathrm{T}}^{\mathrm{P}}$ or $\leq_{m}^{\mathrm{P}}$), a language (i.e., decision problem) C is *$\leq_{r}^{\mathrm{P}}$-complete for* NP if $C \in \mathrm{NP}$ and, for all $A \in \mathrm{NP}$, $A \leq_{r}^{\mathrm{P}} C$. The difference between $\leq_{\mathrm{T}}^{\mathrm{P}}$-completeness and $\leq_{m}^{\mathrm{P}}$-completeness (if any) arises from the difference between the reducibilities $\leq_{\mathrm{T}}^{\mathrm{P}}$ and $\leq_{m}^{\mathrm{P}}$. If A and B are languages, then A is *polynomial-time Turing reducible to* B, and we write $A \leq_{\mathrm{T}}^{\mathrm{P}} B$, if A is decided in polynomial time by some oracle Turing machine that consults B as an oracle. On the other hand, A is *polynomial-time many-one reducible to* B, and we write $A \leq_{m}^{\mathrm{P}} B$, if every instance x of the decision problem A can be transformed in polynomial time into an instance $f(x)$ of the decision problem B with the same answer, i.e., satisfying $x \in A$ iff $f(x) \in B$.

It is clear that $A \leq_{m}^{\mathrm{P}} B$ implies $A \leq_{\mathrm{T}}^{\mathrm{P}} B$, and hence that every $\leq_{m}^{\mathrm{P}}$-complete language for NP is $\leq_{\mathrm{T}}^{\mathrm{P}}$-complete for NP. Conversely, all known, natural $\leq_{\mathrm{T}}^{\mathrm{P}}$-complete languages for NP are also $\leq_{m}^{\mathrm{P}}$-complete. Nevertheless, it is widely conjectured (e.g., [10, 29, 12, 6]) that Cook completeness is more general than Karp-Levin completeness:

CvKL Conjecture. ("Cook versus Karp-Levin"). There exists a language that is $\leq_{\mathrm{T}}^{\mathrm{P}}$-complete, but not $\leq_{m}^{\mathrm{P}}$-complete, for NP.

The CvKL conjecture immediately implies that $\mathrm{P} \neq \mathrm{NP}$, so it may be very difficult to prove. We mention five items of evidence that the conjecture is reasonable.

1. Selman [24] proved that the widely-believed hypothesis $\mathrm{E} \neq \mathrm{NE}$ implies that the reducibilities $\leq_{\mathrm{T}}^{\mathrm{P}}$ and $\leq_{m}^{\mathrm{P}}$ are distinct in $\mathrm{NP} \cup \mathrm{co-NP}$. That is, if $\mathrm{DTIME}(2^{\mathrm{linear}}) \neq \mathrm{NTIME}(2^{\mathrm{linear}})$, then there exist $A, B \in \mathrm{NP} \cup \mathrm{co-NP}$ such that $A \leq_{\mathrm{T}}^{\mathrm{P}} B$ but $A \not\leq_{m}^{\mathrm{P}} B$. Under the stronger hypothesis $\mathrm{E} \neq \mathrm{NE} \cap \mathrm{co-NE}$, Selman proved that the reducibilities $\leq_{\mathrm{T}}^{\mathrm{P}}$ and $\leq_{m}^{\mathrm{P}}$ are distinct in NP.

2. Ko and Moore [9] constructed a language that is $\leq_{\mathrm{T}}^{\mathrm{P}}$-complete, but not $\leq_{m}^{\mathrm{P}}$-complete, for E. Watanabe [26, 27] refined this by separating a spectrum of completeness notions in E.

3. Watanabe and Tang [28] exhibited reasonable complexity-theoretic hypotheses implying the existence of languages that are $\leq_{\mathrm{T}}^{\mathrm{P}}$-complete, but not $\leq_{m}^{\mathrm{P}}$-complete, for PSPACE.

4. Watanabe [27] and Buhrman, Homer, and Torenvliet [4] constructed languages that are $\leq_{\mathrm{T}}^{\mathrm{P}}$-complete, but not $\leq_{m}^{\mathrm{P}}$-complete, for NE.

5. Longpré and Young [12] showed that, for every polynomial time bound t, there exist languages A and B, both $\leq_{\mathrm{T}}^{\mathrm{P}}$-complete for NP, such that A is $\leq_{\mathrm{T}}^{\mathrm{P}}$-reducible to B in linear time, but A is not $\leq_{m}^{\mathrm{P}}$-reducible to B in $t(n)$ time.

Item 1 above indicates that the reducibilities $\leq_{\mathrm{T}}^{\mathrm{P}}$ and $\leq_{m}^{\mathrm{P}}$ are likely to differ in NP. Item 3 indicates that the CvKL conjecture is likely to hold with NP replaced by PSPACE. Items 2 and 4 indicate that the CvKL Conjecture definitely holds with NP replaced by E or by NE. Item 5 would imply the CvKL Conjecture, were it not for the dependence of A and B upon the polynomial t. Taken together, these five items suggest that the CvKL Conjecture is reasonable.

The CvKL Conjecture is very ambitious, since it implies that $\mathrm{P} \neq \mathrm{NP}$. The question has thus been raised [10, 24, 6, 4] whether the CvKL Conjecture can be derived from some reasonable complexity-theoretic hypothesis, such as $\mathrm{P} \neq \mathrm{NP}$ or the separation of the polynomial-time hierarchy into infinitely many levels. To date, even this more modest objective has not been achieved.

The Main Theorem of this paper, Theorem 4.1 below, says that the CvKL Conjecture follows from the hypothesis that "NP does not have p-measure 0". This hypothesis, whose formulation involves *resource-bounded measure* [14, 13] (a complexity-theoretic generalization of Lebesgue measure), is explained in detail in section 3 below. *Very* roughly speaking, the hypothesis says that "NP is not small," in the sense that NP contains more than a negligible subset of the languages decidable in exponential time.

In section 3 below it is argued that "NP does not have p-measure 0" is a reasonable hypothesis for two reasons: First, its negation would imply the existence of a surprisingly efficient algorithm for betting on all NP languages. Second, the hypothesis has a rapidly growing body of credible consequences. We summarize recently discovered such consequences [16, 7, 15] and prove two new consequences, namely the class separation $\mathrm{E} \neq \mathrm{NE}$ and (building on recent work of Bellare and Goldwasser [1]) the existence of NP search problems that are not reducible to the corresponding decision problems.

In section 4 we prove our Main Theorem. In section 5, we prove that, if NP is not small, then many truth-table reducibilities are distinct in NP.

Taken together, our results suggest that "NP does not have p-measure 0" is a *reasonable scientific hypothesis*, which may have the *explanatory power* to resolve many questions that have not been resolved by traditional complexity-theoretic hypotheses.

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 $A \subseteq \{0,1\}^*$. 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

$$\mathbf{C}_w = \{x \in \{0,1\}^\infty \mid w \sqsubseteq x\} = \{A \subseteq \{0,1\}^* \mid w \sqsubseteq \chi_A\}.$$

Note that $\mathbf{C}_\lambda = \{0,1\}^\infty$, where λ denotes the empty string.

As noted in section 1, we work with the exponential time complexity classes $\mathrm{E} = \mathrm{DTIME}(2^{\text{linear}})$ and $\mathrm{E}_2 = \mathrm{DTIME}(2^{\text{polynomial}})$. 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 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.

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 $d_0, d_1, d_2, \ldots$. For a function $d : \mathbf{N}^n \times X \to Y$ ($n \geq 2$), we write $d_{k,l} = (d_k)_l$, etc.

In general, complexity classes of functions from $\{0,1\}^*$ into $\{0,1\}^*$ will be denoted by appending an 'F' to the notation for the corresponding complexity classes of languages. Thus, for $t : \mathbf{N} \to \mathbf{N}$, DTIMEF$(t)$ is the set of all functions $f : \{0,1\}^* \to \{0,1\}^*$ such that $f(x)$ is computable in $O(t(|x|))$ time. Similarly, $\mathrm{PF} = \bigcup_{k=0}^{\infty} \mathrm{DTIMEF}(n^k)$. (For technical reasons [13], when discussing resource bounds for measure, we will deviate from this practice, writing p for PF, etc., as in section 3 below).

We will discuss a variety of specialized polynomial-time reducibilities, in addition to the well-known reducibilities $\leq_{\mathrm{T}}^{\mathrm{P}}$ and $\leq_m^{\mathrm{P}}$, mentioned in the introduction. These include $\leq_{\mathrm{pos-T}}^{\mathrm{P}}$ (*positive Turing* reducibility), $\leq_{q\text{-}\mathrm{T}}^{\mathrm{P}}$ (*Turing reducibility with $q(n)$ queries* on inputs of length n), $\leq_{q-tt}^{\mathrm{P}}$ (*truth-table reducibility with $q(n)$ queries* on inputs of length n, where $q : \mathbf{N} \to \mathbf{Z}^+$ is a query-counting function), $\leq_{tt}^{\mathrm{P}}$ (*truth-table* reducibility), $\leq_{btt}^{\mathrm{P}}$ (*bounded truth-table* reducibility), and $\leq_{\mathrm{pos}-tt}^{\mathrm{P}}$ (*positive truth-table* reducibility). We now indicate the meanings of these specialized reducibilities.

Let $A, B \subseteq \{0,1\}^*$. The condition $A \leq_{\mathrm{T}}^{\mathrm{P}} B$ means that there is a polynomial time-bounded oracle Turing machine M such that $A = L(M^B)$, i.e., M decides A with oracle B. The condition $A \leq_{\mathrm{pos-T}}^{\mathrm{P}} B$ means that there is a polynomial time-bounded oracle Turing machine M such that $A = L(M^B)$ and, for all $C, D \subseteq \{0,1\}^*$, $C \subseteq D$ implies $L(M^C) \subseteq L(M^D)$. For $q : \mathbf{N} \to \mathbf{Z}^+$, the condition $A \leq_{q\text{-}\mathrm{T}}^{\mathrm{P}} B$ means that there is a polynomial time-bounded Turing machine M such that $A = L(M^B)$ and M makes $\leq q(|x|)$ oracle queries on each input $x \in \{0,1\}^*$.

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

$$f(x) = (f_1(x), \ldots, f_{q(|x|)}(x)) \in (\{0,1\}^*)^{q(|x|)}.$$

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 $w \in \{0,1\}^{q(|x|)}$. A $\leq^{\mathrm{P}}_{q-tt}$-*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 $\leq^{\mathrm{P}}_{q-tt}$-*reduction of* A *to* B is a $\leq^{\mathrm{P}}_{q-tt}$-reduction (f, g) such that, for all $x \in \{0,1\}^*$,

$$[\![x \in A]\!] = g(x)([\![f_1(x) \in B]\!] ... [\![f_{q(|x|)}(x) \in B]\!]).$$

(Recall that $[\![\psi]\!]$ denotes the Boolean value of the condition ψ). In this case we say that $A \leq^{\mathrm{P}}_{q-tt} B$ via g. We say that A is $\leq^{\mathrm{P}}_{q-tt}$-*reducible to* B, and write $A \leq^{\mathrm{P}}_{q-tt} B$, if there exists (f, g) such that $A \leq^{\mathrm{P}}_{q-tt} B$ via (f, g).

The condition $A \leq^{\mathrm{P}}_{tt} B$ means that there exists a polynomial q such that $A \leq^{\mathrm{P}}_{q-tt} B$. The condition $A \leq^{\mathrm{P}}_{btt} B$ means that there exists a constant k such that $A \leq^{\mathrm{P}}_{k-tt} B$. (This is equivalent to saying that there exists a constant k such that $A \leq^{\mathrm{P}}_{k\text{-T}} B$). Finally, the condition $A \leq^{\mathrm{P}}_{\mathrm{pos}-tt} B$ means that there exist a polynomial q such that $A \leq^{\mathrm{P}}_{q-tt} B$ via (f, g) and, for all x, the Boolean function $g(x) : \{0,1\}^{q(|x|)} \to \{0,1\}$ is *monotone*, i.e., satisfies $g(x)(u) \leq g(x)(v)$ whenever each bit of u is less than or equal to the corresponding bit of v.

For more details on these reducibilities, see [10, 24, 25, 26, 27, 6, 4].

3 If NP Is Not Small

In this section we discuss the meaning and reasonableness of the hypothesis that NP is not small. Inevitably, our discussion begins with a review of measure in complexity classes.

Resource-bounded measure [14, 13] 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 E_2, so our discussion of measure is specific to these classes. The interested reader may consult section 3 of [14] for more discussion and examples.

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.

Notation The classes $\mathrm{p}_1 = \mathrm{p}$ and p_2, both consisting of functions $f : \{0,1\}^* \to \{0,1\}^*$, are defined as follows.

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

The measure structures of E and E_2 are developed in terms of the classes p_i, for $i = 1, 2$.

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

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

(Recall that $\mathbf{C}_w = \{A \subseteq \{0,1\}^* \mid w \sqsubseteq \chi_A\}$ 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 language $A \subseteq \{0,1\}^*$ is chosen by using an independent toss of a fair coin to decide whether each string $x \in \{0,1\}^*$ is in A. Taken together, parts (3.1) and (3.2) of the above definition imply that $\Pr[A \in S[d]] \leq d(\lambda)$ in this experiment. Intuitively, we regard a density function d as a "detailed verification" that $\Pr[A \in X] \leq d(\lambda)$ 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 $w \in \{0,1\}^*$. For $i = 1, 2$, a p_i-*computation* of an n-DS d is a computation $\widehat{d}$ of d such that $\widehat{d} \in p_i$. An n-DS d is p_i-*computable* if there exists a p_i-computation $\widehat{d}$ of d.

If d is an n-DS such that $d : \mathbf{N}^n \times \{0,1\}^* \to \mathbf{D}$ and $d \in \mathrm{p}_i$, then d is trivially p_i-computable. This fortunate circumstance, in which there is no need to compute approximations, occurs frequently in practice. (Such applications typically do involve approximations, but these are "hidden" by invoking fundamental theorems whose proofs involve approximations).

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 $d_k(\lambda) \le 2^{-k}$. 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 $\mu_{\mathrm{p}_i}(X) = 0$, if there exists a p_i-null cover of X. A set X has p_i-*measure 1*, and we write $\mu_{\mathrm{p}_i}(X) = 1$, if $\mu_{\mathrm{p}_i}(X^c) = 0$.

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 the classes $\mathrm{E} = \mathrm{E}_1 = \mathrm{DTIME}(2^{\mathrm{linear}})$ and $\mathrm{E}_2 = \mathrm{DTIME}(2^{\mathrm{polynomial}})$.

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

We write $\mu(X \mid \mathrm{E}_i) \neq 0$ to indicate that X does *not* have measure 0 in E_i. Note that this does *not* assert that "$\mu(X \mid \mathrm{E}_i)$" has some nonzero value.

The following is obvious but useful.

Fact 3.1. For every set $X \subseteq \{0,1\}^\infty$,

$$\begin{array}{ccccc}
\mu_{\mathrm{p}}(X) = 0 & \Longrightarrow & \mu_{\mathrm{p}_2}(X) = 0 & \Longrightarrow & \Pr[A \in X] = 0 \\
\Downarrow & & \Downarrow & & \\
\mu(X|\mathrm{E}) = 0 & & \mu(X|\mathrm{E}_2) = 0, & &
\end{array}$$

where the probability $\Pr[A \in X]$ is 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 whether each string $x \in \{0,1\}^*$ is in A.

It is shown in [14] that these definitions endow E and E_2 with internal measure structure. This structure justifies the intuition that, if $\mu(X \mid \mathrm{E}) = 0$, then $X \cap \mathrm{E}$ is a *negligibly small* subset of E (and similarly for E_2). The next two results state aspects of this structure that are especially relevant to the present work.

Theorem 3.2 ([14]). For all cylinders $\mathbf{C}_w$, $\mu(\mathbf{C}_w \mid \mathrm{E}) \neq 0$ and $\mu(\mathbf{C}_w \mid \mathrm{E}_2) \neq 0$. In particular, $\mu(\mathrm{E} \mid \mathrm{E}) \neq 0$ and $\mu(\mathrm{E}_2 \mid \mathrm{E}_2) \neq 0$.

The next lemma, which will be used in proving our main results, involves the following computational restriction of the notion of "countable union."

Definition. Let $i \in \{1,2\}$ and let $Z, Z_0, Z_1, Z_2, \cdots \subseteq \{0,1\}^\infty$. Then Z is a p_i*-union of the* p_i*-measure 0 sets* $Z_0, Z_1, Z_2, \cdots$ if $Z = \bigcup_{j=0}^{\infty} Z_j$ and there exists a p_i-computable 2-DS d such that each d_j is a p_i-null cover of Z_j.

Lemma 3.3 ([14]). Let $i \in \{1,2\}$ and let $Z, Z_0, Z_1, Z_2, \cdots \subseteq \{0,1\}^\infty$. If Z is a p_i-union of the p_i-measure 0 sets $Z_0, Z_1, Z_2, \cdots$, then Z has p_i-measure 0. □

Regarding deterministic time complexity classes, the following fact is an easy exercise. (It also follows immediately from Theorem 4.16 of [14]).

Fact 3.4. For every fixed $c \in \mathbf{N}$,

$$\mu(\mathrm{DTIME}(2^{cn}) \mid \mathrm{E}) = \mu_{\mathrm{p}}(\mathrm{DTIME}(2^{cn})) = 0$$

and

$$\mu(\mathrm{DTIME}(2^{n^c}) \mid \mathrm{E}_2) = \mu_{\mathrm{p}_2}(\mathrm{DTIME}(2^{n^c})) = 0.$$

□

Figure 1 summarizes known implications among various conditions asserting the smallness of NP. (These implications follow from Facts 3.1 and 3.4). Figure 2, the contrapositive of Figure 1, then gives the implications among various conditions asserting the non-smallness of NP. Lutz has con-

$$
\begin{array}{ccc}
\mathrm{P} = \mathrm{NP} & & \\
\Downarrow & & \\
(\exists c)\, \mathrm{NP} \subseteq \mathrm{DTIME}(2^{cn}) & \Longrightarrow & (\exists k)\, \mathrm{NP} \subseteq \mathrm{DTIME}(2^{n^k}) \\
\Downarrow & & \Downarrow \\
\mu_{\mathrm{p}}(\mathrm{NP}) = 0 & \Longrightarrow & \mu_{\mathrm{p}_2}(\mathrm{NP}) = 0 \\
\Downarrow & & \Updownarrow \\
\mu(\mathrm{NP} \mid \mathrm{E}) = 0 & & \mu(\mathrm{NP} \mid \mathrm{E}_2) = 0
\end{array}
$$

Figure 1: Smallness conditions

$$
\begin{array}{ccc}
\mu(\mathrm{NP} \mid \mathrm{E}_2) \neq 0 & & \mu(\mathrm{NP} \mid \mathrm{E}) \neq 0 \\
\Updownarrow & & \Downarrow \\
\mu_{\mathrm{p}_2}(\mathrm{NP}) \neq 0 & \Longrightarrow & \mu_{\mathrm{p}}(\mathrm{NP}) \neq 0 \\
\Downarrow & & \Downarrow \\
(\forall k)\, \mathrm{NP} \not\subseteq \mathrm{DTIME}(2^{n^k}) & \Longrightarrow & (\forall c)\, \mathrm{NP} \not\subseteq \mathrm{DTIME}(2^{cn}) \\
 & & \Downarrow \\
 & & \mathrm{P} \neq \mathrm{NP}
\end{array}
$$

Figure 2: Non-smallness conditions

jectured that the strongest conditions in Figure 2, namely, $\mu(\mathrm{NP} \mid \mathrm{E}_2) \neq 0$ and $\mu(\mathrm{NP} \mid \mathrm{E}) \neq 0$, are true. Most of the results of the present paper involve the weakest measure-theoretic hypothesis in Figure 2, namely the hypothesis that NP does not have p-measure 0. The rest of this section discusses the reasonableness and consequences of this particular hypothesis.

The hypothesis that $\mu_{\mathrm{p}}(\mathrm{NP}) \neq 0$ is best understood by considering the meaning of its negation, that NP has p-measure 0. A particularly intuitive interpretation of this latter condition is in terms of certain algorithmic betting strategies, called martingales.

Definition. A *martingale* is a density function d that satisfies condition (3.1) with equality, i.e., a function $d : \{0,1\}^* \to [0,\infty]$ such that

$$d(w) = \frac{d(w0) + d(w1)}{2} \tag{3.3}$$

for all $w \in \{0,1\}^*$. A martingale d *succeeds* on a language $A \subseteq \{0,1\}^*$ if

$$\limsup_{n \to \infty} d(\chi_A[0..n-1]) = \infty.$$

Intuitively, a martingale d is a betting strategy that, given a language A, starts with capital (amount of money) $d(\lambda)$ and bets on the membership or nonmembership of the successive strings $s_0, s_1, s_2, \cdots$ (the standard enumeration of $\{0,1\}^*$) in A. Prior to betting on a string s_n, the strategy has capital $d(w)$, where

$$w = [\![s_0 \in A]\!] \cdots [\![s_{n-1} \in A]\!].$$

After betting on the string s_n, the strategy has capital $d(wb)$, where $b = [\![s_n \in A]\!]$. Condition (3.3) ensures that the betting is fair. The strategy succeeds on A if its capital is unbounded as the betting progresses.

Martingales were used extensively by Schnorr [20, 21, 22, 23] in his investigation of random and pseudorandom sequences. Recently, martingales have been shown to characterize p-measure 0 sets:

Theorem 3.5 ([14, 13]). A set X of languages has p-measure 0 if and only if there exists a p-computable martingale d such that, for all $A \in X$, d succeeds on A. □

In the case $X = \mathrm{NP}$, Theorem 3.5 says that NP has p-measure 0 if and only if there is a single p-computable strategy d that succeeds (bets successfully) on every language $A \in \mathrm{NP}$. The fact that the strategy d is p-computable means that, when betting on the condition "$x \in A$", d requires only $2^{c|x|}$ time for some fixed constant c. (This is because the running time of d for this bet is polynomial in the number of predecessors of x in the standard ordering of $\{0,1\}^*$). On the other hand, for all $k \in \mathbf{N}$, there exist languages $A \in \mathrm{NP}$ with the property that the apparent search space (space of witnesses) for each input x has $2^{|x|^k}$ elements. Since c is fixed, we have $x^{cn} \ll x^{n^k}$ for large values of k. Such a martingale d would thus be a very remarkable algorithm! It would bet succesfully on *all* NP languages, using far less than enough time to examine the search spaces of most such languages. It is reasonable to conjecture that no such martingale exists, i.e., that NP does not have p-measure 0.

Since $\mu_{\mathrm{p}}(\mathrm{NP}) \neq 0$ implies $\mathrm{P} \neq \mathrm{NP}$, and $\mu_{\mathrm{p}}(\mathrm{NP}) = 0$ implies $\mathrm{NP} \neq \mathrm{E}_2$, we are unable to prove or disprove the $\mu_{\mathrm{p}}(\mathrm{NP}) \neq 0$ conjecture at this time. Until such a mathematical resolution is available, the condition $\mu_{\mathrm{p}}(\mathrm{NP}) \neq 0$ is best investigated as a *scientific hypothesis*, to be evaluated in terms of the extent and credibility of its consequences.

We now mention three recently discovered consequences of the hypothesis that NP does not have p-measure 0. The first concerns P-bi-immunity.

Definition. A language $A \subseteq \{0,1\}^*$ is P-*immune* if, for all $B \in \mathrm{P}$, $B \subseteq A$ implies that B is finite. A language $A \subseteq \{0,1\}^*$ is P-*bi-immune* if A and A^c are both P-immune.

Theorem 3.6 (Mayordomo [16]). The set of P-bi-immune languages has p-measure 1. Thus, if NP does not have p-measure 0, then NP contains a P-bi-immune language. □

The next known consequence of $\mu_{\mathrm{p}}(\mathrm{NP}) \neq 0$ involves complexity cores of NP-complete languages.

Definition. A language $A \subseteq \{0,1\}^*$ is *dense* if there is a real number $\epsilon > 0$ such that $|A_{\leq n}| \geq 2^{n^\epsilon}$ for all sufficiently large n.

Definition. Given a machine M and an input $x \in \{0,1\}^*$, we write $M(x) = 1$ if M accepts x, $M(x) = 0$ if M rejects x, and $M(x) = \perp$ in any other case. If $M(x) \in \{0,1\}$, we write $\mathrm{time}_M(x)$ for the number of steps used in the computation of $M(x)$. If $M(x) = \perp$, we define $\mathrm{time}_M(x) = \infty$. We partially order the set $\{0,1,\perp\}$ by $\perp < 0$ and $\perp < 1$, with 0 and 1 incomparable. A machine M is *consistent with* a language $A \subseteq \{0,1\}^*$ if $M(x) \le [\![x \in A]\!]$ for all $x \in \{0,1\}^*$.

Definition. Let $K, A \subseteq \{0,1\}^*$. Then K is an *exponential complexity core* of A if there is a real number $\epsilon > 0$ such that, for every machine M that is consistent with A, the "fast set"

$$F = \left\{ x \,\middle|\, \mathrm{time}_m(x) \le 2^{|x|^\epsilon} \right\}$$

satisfies $|F \cap K| < \infty$.

Theorem 3.7 (Juedes and Lutz [7]). If NP does not have p-measure 0, then every $\le_m^{\mathrm{P}}$-complete language A for NP has a dense exponential complexity core. □

Thus, for example, if NP is not small, then there is a dense set K of Boolean formulas in conjunctive normal form such that every machine that is consistent with SAT performs exponentially badly (either by running for more than $2^{|x|^\epsilon}$ steps or by failing to decide) on all but finitely many inputs $x \in K$. (The weaker hypothesis $\mathrm{P} \ne \mathrm{NP}$ was already known [19] to imply the weaker conclusion that every $\le_m^{\mathrm{P}}$-complete language for NP has a nonsparse polynomial complexity core).

The third consequence of $\mu_{\mathrm{p}}(\mathrm{NP}) \ne 0$ to be mentioned here concerns the density of hard languages for NP. Ogiwara and Watanabe [18] recently showed that $\mathrm{P} \ne \mathrm{NP}$ implies that every $\le_{btt}^{\mathrm{P}}$-hard language for NP is nonsparse (i.e., is not polynomially sparse). More recently, it has been proven that the $\mu_{\mathrm{p}}(\mathrm{NP}) \ne 0$ hypothesis yields a stronger conclusion:

Theorem 3.8 (Lutz and Mayordomo [15]). If NP does not have p-measure 0, then for every real number $\alpha < 1$ (e.g., $\alpha = 0.99$), every $\le_{n^\alpha-tt}^{\mathrm{P}}$-hard language for NP is dense.

We conclude this section by noting some new consequences of the hypothesis that $\mu_{\mathrm{p}}(\mathrm{NP}) \ne 0$. The following lemma involves the exponential complexity classes $\mathrm{E} = \mathrm{DTIME}(2^{\mathrm{linear}})$ and $\mathrm{NE} = \mathrm{NTIME}(2^{\mathrm{linear}})$, and also the doubly exponential complexity classes, $\mathrm{EE} = \bigcup_{c=0}^\infty \mathrm{DTIME}(2^{2^{n+c}})$ and $\mathrm{NEE} = \bigcup_{c=0}^\infty \mathrm{NTIME}(2^{2^{n+c}})$.

Lemma 3.9.

1. If NP contains a P-bi-immune language, then $\mathrm{E} \ne \mathrm{NE}$ and $\mathrm{EE} \ne \mathrm{NEE}$.

2. If $\mathrm{NP} \cap \mathrm{co-NP}$ contains a P-bi-immune language, then $\mathrm{E} \neq \mathrm{NE} \cap \mathrm{co-NE}$ and $\mathrm{EE} \neq \mathrm{NEE} \cap \mathrm{co-NEE}$.

Proof. Let $T = \{ 0^{2^n} \mid n \in \mathbf{N}\}$. For each $A \subseteq \{0,1\}^*$, let

$$\sigma(A) = \left\{ s_n \,\middle|\, 0^{2^n} \in A \right\},$$

where $s_0, s_1, s_2, \cdots$ is the standard enumeration of $\{0,1\}^*$. It is routine to show that, for all $A \subseteq \{0,1\}^*$,

$$\sigma(A) \in \mathrm{EE} \text{ iff } A \cap T \in \mathrm{P},$$

$$\sigma(A) \in \mathrm{NEE} \text{ iff } A \cap T \in \mathrm{NP},$$

and

$$\sigma(A) \in \mathrm{co-NEE} \text{ iff } A \cap T \in \mathrm{co-NP}.$$

1. Let $A \in \mathrm{NP}$ be P-bi-immune. Then $A \cap T \in \mathrm{NP}$, so $\sigma(A) \in \mathrm{NEE}$. Since A^c is P-immune, $A \cap T$ is infinite. Since A is P-immune, it follows that $A \cap T \notin \mathrm{P}$, whence $\sigma(A) \notin \mathrm{EE}$. Thus $\sigma(A) \in \mathrm{NEE} - \mathrm{EE}$, so $\mathrm{EE} \neq \mathrm{NEE}$. Note also that $A \cap T$ is a tally language in $\mathrm{NP} - \mathrm{P}$. The existence of such a language is known [3] to be equivalent to $\mathrm{E} \neq \mathrm{NE}$.

The proof of 2 is similar.

□

Theorem 3.10.

1. If NP does not have p-measure 0, then $\mathrm{E} \neq \mathrm{NE}$ and $\mathrm{EE} \neq \mathrm{NEE}$.

2. If $\mathrm{NP} \cap \mathrm{co-NP}$ does not have p-measure 0, then $\mathrm{E} \neq \mathrm{NE} \cap \mathrm{co-NE}$ and $\mathrm{EE} \neq \mathrm{NEE} \cap \mathrm{co-NEE}$.

Proof. This follows immediately from Theorem 3.6 and Lemma 3.9. □

Corollary 3.11. If NP does not have p-measure 0, then there is an NP search problem that does not reduce to the corresponding decision problem.

Proof. Bellare and Goldwasser [1] have shown that, if $\mathrm{EE} \neq \mathrm{NEE}$, then there is an NP search problem that does not reduce to the corresponding decision problem. The present corollary follows immediately from this and Theorem 3.10. □

4 Separating Completeness Notions in NP

In this section we prove our main result, that the CvKL Conjecture holds if NP is not small:

Theorem 4.1 (Main Theorem). If NP does not have p-measure 0, then there is a language C that is $\leq^{\mathrm{P}}_{\mathrm{T}}$-complete, but not $\leq^{\mathrm{P}}_{m}$-complete, for NP.

In fact, the language C exhibited will be $\leq^{\mathrm{P}}_{2\text{-}\mathrm{T}}$-complete, hence also $\leq^{\mathrm{P}}_{3-tt}$-complete, for NP.

Our proof of Theorem 4.1 uses the following definitions and lemma.

Definition. The *tagged union* of languages $A_0, \cdots, A_{k-1} \subseteq \{0,1\}^*$ is the language

$$A_0 \oplus \cdots \oplus A_{k-1} = \left\{ x10^i \,|\, 0 \leq i < k \text{ and } x \in A_i \right\}.$$

Definition. For $j \in \mathbf{N}$, the j^{th} *strand* of a language $A \subseteq \{0,1\}^*$ is

$$A_{(j)} = \left\{ x \,\middle|\, x10^j \in A \right\}.$$

Lemma 4.2 (Main Lemma). For any language $S \subseteq \{0,1\}^*$, the set

$$X = \left\{ A \subseteq \{0,1\}^* \,\middle|\, A_{(0)} \leq^{\mathrm{P}}_{m} A_{(4)} \oplus (A_{(4)} \cap S) \oplus (A_{(4)} \cup S) \right\}$$

has p-measure 0.

Before proving the Main Lemma, we use it to prove the Main Theorem.

Proof of Theorem 4.1 Assume that NP does not have p-measure 0. Let

$$X = \left\{ A \,\middle|\, A_{(0)} \leq^{\mathrm{P}}_{m} A_{(4)} \oplus (A_{(4)} \cap \mathrm{SAT}) \oplus (A_{(4)} \cup \mathrm{SAT}) \right\}.$$

By the Main Lemma, X has p-measure 0, so there exists a language $A \in \mathrm{NP} - X$. Fix such a language A and let

$$C = A_{(4)} \oplus (A_{(4)} \cap \mathrm{SAT}) \oplus (A_{(4)} \cup \mathrm{SAT}).$$

Since $A \in \mathrm{NP}$, we have $A_{(0)}, A_{(4)} \in \mathrm{NP}$. Since $A_{(4)}, \mathrm{SAT} \in \mathrm{NP}$ and NP is closed under $\cap$, $\cup$, and $\oplus$, we have $C \in \mathrm{NP}$. Also, the algorithm

```
begin
input x;
if x1 ∈ C
then if x10 ∈ C then accept
                 else reject
else if x100 ∈ C then accept
                  else reject
end
```

clearly decides SAT using just two (adaptive) queries to C, so SAT $\leq^{\mathrm{P}}_{2\text{-T}} C$. Thus C is $\leq^{\mathrm{P}}_{2\text{-T}}$-complete, hence certainly $\leq^{\mathrm{P}}_{\mathrm{T}}$-complete, for NP. On the other hand, $A \notin X$, so $A_{(0)} \not\leq^{\mathrm{P}}_{m} C$. Since $A_{(0)} \in \mathrm{NP}$, it follows that C is not $\leq^{\mathrm{P}}_{m}$-complete for NP. □

The rest of this section is devoted to proving the Main Lemma. For this we need the following definitions, lemma, and corollary.

Definition. The *collision set* of a function $f : \{0,1\}^* \to \{0,1\}^*$ is

$$C_f = \{\, x \in \{0,1\}^* \,|\, (\exists y < x)\, f(y) = f(x) \,\}.$$

Here, we are using the standard ordering $s_0 < s_1 < s_2 < \cdots$ of $\{0,1\}^*$.

Note that f is one-to-one if and only if $C_f = \emptyset$.

Definition. A function $f : \{0,1\}^* \to \{0,1\}^*$ is *one-to-one almost everywhere* (or, briefly, *one-to-one a.e.*) if its collision set C_f is finite.

Definition. Let $A, B \subseteq \{0,1\}^*$ and let $t : \mathbf{N} \to \mathbf{N}$. A *$\leq^{\mathrm{DTIME}(t)}_{m}$-reduction of A to B* is a function $f \in \mathrm{DTIMEF}(t)$ such that $A = f^{-1}(B)$, i.e., such that, for all $x \in \{0,1\}^*$, $x \in A$ iff $f(x) \in B$. A *$\leq^{\mathrm{DTIME}(t)}_{m}$-reduction of A* is a function f that is a $\leq^{\mathrm{DTIME}(t)}_{m}$-reduction of A to $f(A)$.

It is easy to see that f is a $\leq^{\mathrm{DTIME}(t)}_{m}$-reduction of A if and only if there exists a language B such that f is a $\leq^{\mathrm{DTIME}(t)}_{m}$-reduction of A to B.

Definition. Let $t : \mathbf{N} \to \mathbf{N}$. A language $A \subseteq \{0,1\}^*$ is *incompressible by $\leq^{\mathrm{DTIME}(t)}_{m}$-reductions* if every $\leq^{\mathrm{DTIME}(t)}_{m}$-reduction of A is one-to-one a.e. A language $A \subseteq \{0,1\}^*$ is *incompressible by $\leq^{\mathrm{P}}_{m}$-reductions* if it is incompressible by $\leq^{\mathrm{DTIME}(q)}_{m}$-reductions for all polynomials q.

Meyer [17] has shown that there is a language $A \in \mathrm{E}$ that is incompressible by $\leq_m^{\mathrm{P}}$-reductions. Recently, the following stronger result has been proven.

<u>Lemma 4.3</u> (Juedes and Lutz [7]). For every fixed $c \in \mathbf{N}$, the set

$$W = \left\{ A \subseteq \{0,1\}^* \,\middle|\, A \text{ is incompressible by } \leq_m^{\mathrm{DTIME}(2^{cn})} -\text{reductions} \right\}$$

has p-measure 1. □

<u>Corollary 4.4.</u> For every fixed $c \in \mathbf{N}$, the set

$$Y = \left\{ A \subseteq \{0,1\}^* \,\middle|\, A_{(0)} \text{ is incompressible by } \leq_m^{\mathrm{DTIME}(2^{cn})} \text{-reductions} \right\}$$

has p-measure 1. □

<u>Proof.</u> Fix $c \in \mathbf{N}$ and let W and Y be as in Lemma 4.3 and Corollary 4.4. By Lemma 4.3, it suffices to show that $W \subseteq Y$.

Let $A \in W$. To see that $A \in Y$, let f be a $\leq_m^{\mathrm{DTIME}(2^{cn})}$-reduction of $A_{(0)}$. Define $g : \{0,1\}^* \to \{0,1\}^*$ by

$$g(x) = \begin{cases} f(y)1 & \text{if } x = y1 \\ x10 & \text{if } x \text{ is not of the form } y1. \end{cases}$$

It is easily checked that g is a $\leq_m^{\mathrm{DTIME}(2^{cn})}$-reduction of A to $f(A_{(0)}) \oplus A$. Since $A \in W$, it follows that the collision set C_g is finite. Now the function $y \mapsto y1$ is one-to-one and maps C_f into C_g, so the collision set C_f is also finite. Thus $A \in Y$ and the proof is complete. □

We now prove the Main Lemma.

<u>Proof of Lemma 4.2</u> Assume the hypothesis. Let $f \in \mathrm{DTIMEF}(n^{\log n})$ be a function that is universal for PF, in the sense that

$$\mathrm{PF} = \{ f_i \mid i \in \mathbf{N} \}.$$

Let Y be as in Corollary 4.4, with $c = 2$. Define the sets

$$Z = X \cap Y$$

and

$$Z_i = \left\{ A \in Y \,\middle|\, A_{(0)} \leq_m^{\mathrm{P}} A_{(4)} \oplus (A_{(4)} \cap S) \oplus (A_{(4)} \cup S) \text{ via } f_i \right\}$$

for all $i \in \mathbf{N}$. Note that $Z = \bigcup_{i=0}^{\infty} Z_i$.

Our objective is to prove that $\mu_{\mathrm{p}}(X) = 0$. Since $X \subseteq Z \cup Y^c$ and Corollary 4.4 tells us that $\mu_{\mathrm{p}}(Y^c) = 0$, it suffices to prove that $\mu_{\mathrm{p}}(Z) = 0$.

For each $i \in \mathbf{N}$, we define a special partial "inverse" function, $f_i^{\#}$, of f_i as follows. (This definition is technical, designed specifically for this proof). Let $y \in \{0,1\}^*$. Let

$$U_{i,y} = \{\, x \mid f_i(x) \in \{y1, y10, y100\} \text{ and } |x| \leq |f_i(x)| \,\}.$$

If $U_{i,y} = \emptyset$, then $f_i^{\#}(y)$ is not defined. If $U_{i,y} \neq \emptyset$, then $f_i^{\#}(y)$ is the first element of $U_{i,y}$ in the standard ordering of $\{0,1\}^*$. (Intuitively, if $A \in Z_i$, $f_i^{\#}(y)$ is defined, and $f_i(f_i^{\#}(y)) = y10^j$, then the reduction f_i transforms the question "$f_i^{\#}(y) \in A_{(0)}$?" into one of the questions "$y \in A_{(4)}$?," "$y \in A_{(4)} \cap S$?," or "$y \in A_{(4)} \cup S$?," according to whether $j = 0$, 1, or 2, respectively).

For $i \in N$, $j \in \{0,1,2\}$, and $A \subseteq \{0,1\}^*$, define the languages

$$\begin{aligned}
R_{i,j} &= \left\{ y10000 \,\middle|\, f_i(f_i^{\#}(y)) = y10^j \right\}, \\
R_{i,j}^{+}(A) &= \left\{ y10000 \in R_{i,j} \,\middle|\, f_i^{\#}(y) \in A_{(0)} \right\} \\
&= \left\{ y10000 \in R_{i,j} \,\middle|\, f_i^{\#}(y)1 \in A \right\}, \\
R_{i,j}^{-}(A) &= \left\{ y10000 \in R_{i,j} \,\middle|\, f_i^{\#}(y) \notin A_{(0)} \right\} \\
&= \left\{ y10000 \in R_{i,j} \,\middle|\, f_i^{\#}(y)1 \notin A \right\}.
\end{aligned}$$

(It is implicit that $f_i^{\#}(y)$ must be defined in order for $y10000$ to be an element of $R_{i,j}$).

Observation. For all $y10000 \in R_{i,j}$, the string $f_i^{\#}(y)1$ precedes $y10000$ in the standard ordering of $\{0,1\}^*$. (This holds because $\left|f_i^{\#}(y)1\right| = \left|f_i^{\#}(y)\right| + 1 \leq \left|f_i(f_i^{\#}(y))\right| + 1 \leq |y100| + 1 < |y10000|$).

The following claim will be verified at the end of this proof.

Main Claim. For all $i \in \mathbf{N}$, if $A \in Z_i$, then $R_{i,0} \cup R_{i,1}^{+}(A) \cup R_{i,2}^{-}(A)$ is infinite.

Define a function $d : \mathbf{N} \times \mathbf{N} \times \{0,1\}^* \to [0,\infty)$ as follows: Let $i, k \in \mathbf{N}$, let $w \in \{0,1\}^*$, let $b \in \{0,1\}$, let

$$B_w = \{\, s_n \mid 0 \leq n < |w| \text{ and } w[n] = 1 \,\},$$

and let $z = s_{|w|}$. (Recall that $s_0, s_1, \cdots$ is the standard enumeration of $\{0,1\}^*$. Thus if wb is a prefix of the characteristic sequence of a language A, then $B_w = A \cap \{s_0, \cdots, s_{|w|-1}\}$ and $b = [\![z \in A]\!]$. Also, by the above observation, for $j \in \{0,1,2\}$, we have

$$z \in R^+_{i,j}(A) \text{ iff } z \in R^+_{i,j}(B_w)$$

and

$$z \in R^-_{i,j}(A) \text{ iff } z \in R^-_{i,j}(B_w)).$$

(i) $d_{i,k}(\lambda) = 2^{-k}$.

(ii) If $z \in R^+_{i,0}(B_w) \cup R^+_{i,1}(B_w)$, then $d_{i,k}(wb) = 2 \cdot d_{i,k}(w) \cdot b$.

(iii) If $z \in R^-_{i,0}(B_w) \cup R^-_{i,2}(B_w)$, then $d_{i,k}(wb) = 2 \cdot d_{i,k}(w) \cdot (1-b)$.

(iv) In any other case, $d_{i,k}(wb) = d_{i,k}(w)$.

It is clear that d is a 2-DS. In fact, since $f \in \mathrm{DTIMEF}(n^{\log n})$ and the computation of $f_i^{\#}(y)$ only involves computing $f_i(x)$ for strings x with $|x| \leq |y| + 3$, it is easily c hecked that $d \in \mathrm{p}$. Thus d is a p-computable 2-DS.

We now show that $Z_i \subseteq S[d_{i,k}]$ for all $i, k \in \mathbf{N}$. To this end, fix $i, k \in \mathbf{N}$ and let $A \in Z_i$. For each $m \in \mathbf{N}$, let $w_m = \chi_A[0..m-1]$ and consider the sequence

$$r_0, r_1, r_2, \cdots$$

of values $r_m = d_{i,k}(w_m)$, computed according to clauses (i)–(iv) above. By clause (i), $r_0 = 2^{-k}$. Also, for all $m \in \mathbf{N}$, $r_{m+1} \in \{0, r_m, 2r_m\}$. Moreover, since f_i is a $\leq^{\mathrm{P}}_m$-reduction of $A_{(0)}$ to $A_{(4)} \oplus (A_{(4)} \cap S) \oplus (A_{(4)} \cup S)$, it is easily checked that r_{m+1} is never set to 0, i.e., that $r_{m+1} \in \{r_m, 2r_m\}$ for all $m \in \mathbf{N}$. This means that $r_{m+1} = 2r_m$ for all m such that $s_m \in R^+_{i,0}(B_{w_m}) \cup R^+_{i,1}(B_{w_m}) \cup R^-_{i,0}(B_{w_m}) \cup R^-_{i,2}(B_{w_m})$, i.e., for all m such that $s_m \in R_{i,0} \cup R^+_{i,1}(A) \cup R^-_{i,2}(A)$. By the Main Claim, th ere are infinitely many such m. In particular, then, there is some m such that $1 \leq r_m = d_{i,k}(w_m)$. Then $A \in \mathbf{C}_{w_m} \subseteq S[d_{i,k}]$. This completes the proof that $Z_i \subseteq S[d_{i,k}]$ for all $i, k \in \mathbf{N}$. It follows that, for each $i \in \mathbf{N}$, d_i is a p-null cover of Z_i. This implies that $Z = \bigcup_{i=0}^{\infty} Z_i$ is a p-union of p-measure 0 sets, whence $\mu_{\mathrm{p}}(Z) = 0$ by Lemma 3.3. This completes the proof of the Main Lemma, using the Main Claim.

To prove the Main Claim, let $i \in \mathbf{N}$ and $A \in Z_i$. Then f_i is a $\leq^{\mathrm{P}}_m$-reduction of $A_{(0)}$ and $A_{(0)} \in Y$, so f is one-to-one a.e . It clearly suffices to prove the following three things.

Claim 1. $R_{i,0} \cup R_{i,1} \cup R_{i,2}$ is infinite.

Claim 2. If $R_{i,1}$ is infinite, then $R^+_{i,1}(A)$ is infinite.

Claim 3. If $R_{i,2}$ is infinite, then $R^-_{i,2}(A)$ is infinite.

Proof of Claim 1. Define the languages

$$Q = \left\{ y10^j \mid y \in \{0,1\}^* \text{ and } j \in \{0,1,2\} \right\},$$
$$C = A_{(4)} \oplus (A_{(4)} \cap S) \oplus (A_{(4)} \cup S)$$

and fix a string $v \notin A_{(0)}$. (Such a string v exists because $A \in Z_i \subseteq Y$). Define a function $g : \{0,1\}^* \to \{0,1\}^*$ by

$$g(x) = \begin{cases} x & \text{if } f_i(x) \in Q \\ v & \text{if } f_i(x) \notin Q. \end{cases}$$

Since $C \subseteq Q$ and $A_{(0)} \leq^{\mathrm{P}}_m C$ via f_i, g is a $\leq^{\mathrm{P}}_m$-reduction of $A_{(0)}$ to itself. Since $A \in Y$, it follows that the set $g^{-1}(\{v\})$ is finite, whence the set $f_i^{-1}(Q)$ is cofinite. Since f_i is one-to-one a.e., it follows that $f_i^{\#}(y)$ is defined for infinitely many y. Since $R_{i,0} \cup R_{i,1} \cup R_{i,2} = \left\{ y10000 \,\middle|\, f_i^{\#}(y) \text{ is defined} \right\}$, this proves Claim 1. □

Proof of Claim 2. Assume that $R^+_{i,1}(A)$ is finite. It suffices to prove that $R^-_{i,1}(A)$ is also finite.

Fix strings $u \in A_{(0)}$ and $v \notin A_{(0)}$. (Such strings exist because $A \in Z_i \subseteq Y$). Define a function $h : \{0,1\}^* \to \{0,1\}^*$ by

$$h(x) = \begin{cases} u & \text{if } f_i(x)000 \in R^+_{i,1}(A) \\ v & \text{if } f_i(x)000 \in R^-_{i,1}(A) \\ x & \text{if } f_i(x)000 \notin R_{i,1}. \end{cases}$$

For all sufficiently large x, the condition "$f_i(x)000 \in R_{i,1}$" can be decided in at most $2^{|x|} \cdot |x|^{\log|x|}$ steps. (If $f_i(x) = y10$, then we need to check predecessors x' of x for the condition $f(x') \in \{y1, y100\}$). Since $R^+_{i,1}(A)$ is finite (this is crucial!), it follows that $h \in \mathrm{DTIMEF}(2^{2n})$. In fact, it is easily checked that h is a $\leq^{\mathrm{DTIME}(2^{2n})}_m$-reduction of $A_{(0)}$ to itself. Since $A \in Y$, it follows that the set $h^{-1}(\{v\})$ is finite. This implies that $R^-_{i,1}(A)$ is finite. □

Proof of Claim 3. This is exactly analogous to the proof of Claim 2. □

The proof of the Main Claim, and hence that of the Main Lemma, is now complete. □

5 Separating Reducibilities in NP

In this section, assuming that NP is not small, we establish the distinctness of many polynomial-time reducibilities in NP.

Our first such result involves known consequences of $\mathrm{E} \neq \mathrm{NE}$.

Theorem 5.1. Assume that NP does not have p-measure 0.

1. There exist $A, B \in \mathrm{NP} \cup \mathrm{co-NP}$ such that $A \leq_{\mathrm{T}}^{\mathrm{P}} B$, but $A \not\leq_{\mathrm{pos-T}}^{\mathrm{P}} B$.

2. There exist $A, B \in \mathrm{NP} \cup \mathrm{co-NP}$ such that $A \leq_{tt}^{\mathrm{P}} B$, but $A \not\leq_{\mathrm{pos-}tt}^{\mathrm{P}} B$.

Proof. Selman [25] has shown that these conclusions follow from $\mathrm{E} \neq \mathrm{NE}$, so the present theorem follows immediately from Theorem 3.10. □

Similarly, we have the following.

Theorem 5.2. Assume that $\mathrm{NP} \cap \mathrm{co-NP}$ does not have p-measure 0.

1. There exist $A, B \in \mathrm{NP}$ such that $A \leq_{\mathrm{T}}^{\mathrm{P}} B$ but $A \not\leq_{\mathrm{pos-T}}^{\mathrm{P}} B$.

2. There exist $A, B \in \mathrm{NP}$ such that $A \leq_{tt}^{\mathrm{P}} B$ but $A \not\leq_{\mathrm{pos-}tt}^{\mathrm{P}} B$.

Proof. Selman [25] has shown that these conclusions follow from $\mathrm{E} \neq \mathrm{NE} \cap \mathrm{co-NE}$, so the present theorem follows immediately from Theorem 3.10. □

The rest of our results concern the separation of various polynomial-time truth-table reducibilities in NP, according to the number of queries. Theorem 5.3 separates $\leq_{(k+1)-tt}^{\mathrm{P}}$ reducibility from $\leq_{k-tt}^{\mathrm{P}}$, for k any constant, while Theorem 5.5 separates $\leq_{q-tt}^{\mathrm{P}}$ reducibilty from $\leq_{r-tt}^{\mathrm{P}}$, for $r(n) \in o(\sqrt{q(n)})$.

Theorem 5.3. If NP does not have p-measure 0, then for all $k \in \mathbf{N}$ there exist $A, B \in \mathrm{NP}$ such that $A \leq_{(k+1)-tt}^{\mathrm{P}} B$ but $A \not\leq_{k-tt}^{\mathrm{P}} B$.

The proof of Theorem 5.3 uses the following notation and lemma.

Notation For $x \in \{0,1\}^*$ and $k \in \mathbf{N}$, let

$$Q_k(x) = \left\{ x10^i \,\middle|\, 0 \leq i < k \right\}.$$

For all $B \subseteq \{0,1\}^*$ and $k \in \mathbf{N}$, then, define the *k-fold disjunction of* B to be the language

$$\vee^{(k)} B = \{\, x \in \{0,1\}^* \,|\, Q_k(x) \cap B \neq \emptyset \,\}\,.$$

Lemma 5.4. For all $k \in \mathbf{N}$, the set

$$X_k = \left\{\, B \subseteq \{0,1\}^* \,\middle|\, \vee^{(k+1)} B \leq^{\mathrm{P}}_{k-tt} B \,\right\}$$

has p-measure 0.

Proof of Theorem 5.3. Assume that NP does not have p-measure 0 and let $k \in \mathbf{N}$. Then Lemma 5.4 tells us that there exists $B \in \mathrm{NP}$ such that $\vee^{(k+1)} B \not\leq^{\mathrm{P}}_{k-tt} B$. Fix such a language B and let $A = \vee^{(k+1)} B$. Then $A \in \mathrm{NP}$ (because $A \leq^{\mathrm{P}}_{\mathrm{pos-T}} B$ and NP is closed under $\leq^{\mathrm{P}}_{\mathrm{pos-T}}$-reducibility [25]), $A \leq^{\mathrm{P}}_{(k+1)-tt} B$ (trivially), and $A \not\leq^{\mathrm{P}}_{k-tt} B$ (by our choice of B). □

Proof of Lemma 5.4 Fix $k \in \mathbf{N}$ and let X_k be as in the statement of the lemma. Let $(f_0, g_0), (f_1, g_1), \cdots$ be an enumeration of all $\leq^{\mathrm{P}}_{k-tt}$-reductions such that $f_i(x)$ and $g_i(x)$ are computable in $\leq 2^{i+|x|}$ steps for all $i \in \mathbf{N}$ and $x \in \{0,1\}^*$. (See section 2 for our notation for $\leq^{\mathrm{P}}_{k-tt}$-reductions.) Define a sequence $z_0, z_1, \cdots$ of strings by the recursion

$$z_0 = \lambda, \quad z_{n+1} = 0^{2^{2^{|z_n|}}}.$$

For $i, n \in \mathbf{N}$, define the set

$$Y_{i,n} = \Big\{ B \subseteq \{0,1\}^* \,|\, [\![z_n \in \vee^{(k+1)} B]\!] \\ = g_i(z_n)([\![f_{i,1}(z_n) \in B]\!] \cdots [\![f_{i,k}(z_n) \in B]\!]) \Big\}.$$

Here, $f_{i,1}(z_n), \cdots, f_{i,k}(z_n)$ denote the k queries of f_i on input z_n, while $g_i(z_n)$ is the (binary encoding of a Boolean circuit computing the) truth-table given by g_i on input z_n. Thus $Y_{i,n}$ is the set of all B such that the $\leq^{\mathrm{P}}_{k-tt}$-reduction (f_i, g_i) correctly reduces the single question "$z_n \in \vee^{(k+1)} B$?" to B. For each $i \in \mathbf{N}$, let

$$Y_i = \bigcap_{n=0}^{\infty} Y_{i,n},$$

and let

$$Y = \bigcup_{i=0}^{\infty} Y_i.$$

It is clear that $X_k \subseteq Y$, so it suffices to prove that $\mu_{\mathrm{p}}(Y) = 0$.

Define a function $d : \mathbf{N} \times \mathbf{N} \times \{0,1\}^* \to [0, \infty)$ as follows: let $i, l \in \mathbf{N}$, let $w \in \{0,1\}^*$, let $b \in \{0,1\}$, and let $y = s_{|w|}$. (Recall that $s_0, s_1, s_2, \cdots$ is the standard enumeration of $\{0,1\}^*$.)

(i) $d_{i,l}(\lambda) = 2^{-l}$

(ii) If $i < |z_n| \leq |y| < |z_{n+1}|$ and $\Pr(Y_{i,n}|\mathbf{C}_w) \neq 0$, then

$$d_{i,l}(wb) = d_{i,l}(w) \cdot \frac{\Pr(Y_{i,n}|\mathbf{C}_{wb})}{\Pr(Y_{i,n}|\mathbf{C}_w)} = 2d_{i,l}(w) \cdot \frac{\Pr(Y_{i,n} \cap \mathbf{C}_{wb})}{\Pr(Y_{i,n} \cap \mathbf{C}_w)}.$$

(iii) In any other case, $d_{i,l}(wb) = d_{i,l}(w)$.

(In clause (ii), the probabilities are computed according to the random experiment in which a language is chosen probabilistically, using an independent toss of a fair coin to decide membership of each string.) Using the definition of conditional probability and the fact that $\Pr(\mathbf{C}_w) = 2 \cdot \Pr(\mathbf{C}_{wb})$, it is easy to check that d is a 2-DS. In fact, since k is a constant and $f_i(x)$ and $g_i(x)$ are computable in $\leq 2^{i+|x|}$ steps, we have $d \in \mathrm{p}$. Thus d is a p-computable 2-DS.

We now show that $Y_i \subseteq S[d_{i,l}]$ for all $i, l \in \mathbf{N}$. Fix $i, l \in \mathbf{N}$ and let $B \in Y_i$. For each $n \in \mathbf{N}$, let

$$w_n = \chi_B[0..m],$$

where $s_m = z_n$. (That is, w_n is the initial segment of the characteristic sequence χ_B of B up to and including the bit that decides whether $z_n \in B$. Consider the sequence

$$r_0, r_1, r_2, \cdots$$

of values $r_n = d_{i,l}(w_n)$, computed according to clauses (i)–(iii) above. By clauses (i) and (iii), $r_n = 2^{-l}$ for all n such that $|z_n| \leq i$. Also, since $B \in Y_i = \bigcap_{i=0}^{\infty} Y_{i,n}$, it is easily checked that $\Pr(Y_{i,n}|\mathbf{C}_w) \neq 0$ for all $w \sqsubseteq \chi_B$, i.e., that

$$r_{n+1} = r_n \cdot \frac{\Pr(Y_{i,n}|\mathbf{C}_{w_{n+1}})}{\Pr(Y_{i,n}|\mathbf{C}_{w_n})}$$

for all n such that $|z_n| > i$. Moreover, for all n such that $|z_n| > i$, all the queries $f_{i,1}(z_n), \cdots, f_{i,k}(z_n)$ and all the strings in $Q_k(z_n)$ are decided by w_{n+1}, so $\Pr(Y_{i,n}|\mathbf{C}_{w_{n+1}}) = 1$ for all such n. That is,

$$r_{n+1} = \frac{r_n}{\Pr(Y_{i,n}|\mathbf{C}_{w_n})}$$

for all n such that $|z_n| > i$. Finally, the definitions of $Y_{i,n}$ and w_n tell us that

$$\Pr(Y_{i,n}|\mathbf{C}_{w_n}) \leq 1 - 2^{-(k+1)}$$

for all n such that $|z_n| > i$. We thus have

$$r_{n+1} \geq \alpha \cdot r_n$$

for all n such that $|z_n| > i$, where $\alpha = 1/(1 - 2^{-(k+1)}) > 1$. This implies that there is some n such that $1 \leq r_n = d_{i,l}(w_n)$. For this n we have $B \in \mathbf{C}_{w_n} \subseteq S[d_{i,l}]$. This completes the proof that $Y_i \subseteq S[d_{i,l}]$ for all $i, l \in \mathbf{N}$.

It follows that, for each $i \in \mathbf{N}$, d_i is a p-null cover of Y_i. This implies that $Y = \bigcup_{i=0}^{\infty} Y_i$ is a p-union of p-measure 0 sets, whence $\mu_{\mathrm{p}}(Y) = 0$ by Lemma 3.3. This completes the proof of Lemma 5.4. □

Our remaining results are stated without proof in this preliminary draft.

Theorem 5.5. If NP does not have p-measure 0 and $q, r : \mathbf{N} \to \mathbf{N}$ are polynomial-time computable query-counting functions satisfying the conditions $q(n) = o(\sqrt{r(n)})$ and $r(n) = O(n)$, then there exist $A, B \in \mathrm{NP}$ such that $A \leq^{\mathrm{P}}_{r-tt} B$ but $A \not\leq^{\mathrm{P}}_{q-tt} B$.

To prove this theorem, we use a technique very similar to that of Theorem 5.3, this time replacing the disjunctive operator by a majority operator. The following notation and lemma are used.

Notation For all $B \subseteq \{0,1\}^*$ and $k \in \mathbf{N}$, define the *q-fold majority of B* to be the language

$$\mathrm{maj}^{(q)} B = \left\{ x \in \{0,1\}^* \middle| \left| Q_{q(|x|)}(x) \cap B \right| \geq \left\lceil \frac{q(|x|)}{2} \right\rceil \right\}.$$

Lemma 5.6. For all $q, r : \mathbf{N} \to \mathbf{N}$ polynomial-time computable functions satisfying the conditions $q(n) = o(\sqrt{r(n)})$ and $r(n) = O(n)$, the set

$$X = \left\{ B \subseteq \{0,1\}^* \middle| \mathrm{maj}^{(q)} B \leq^{\mathrm{P}}_{r-tt} B \right\}$$

has p-measure 0.

The query bounds of Theorems 5.3 and 5.5 can be relaxed if we make the stronger assumption that $\mu(\mathrm{NP} \mid \mathrm{E}_2) \neq 0$.

Theorem 5.7. If $\mu(\mathrm{NP} \mid \mathrm{E}_2) \neq 0$ and q is a polynomial-time computable query-counting function such that $q(n) = O(\log n)$, then there exist $A, B \in$ NP such that $A \leq^{\mathrm{P}}_{(q+1)-tt} B$ but $A \not\leq^{\mathrm{P}}_{q-tt} B$.

Theorem 5.8. If $\mu(\mathrm{NP} \mid \mathrm{E}_2) \neq 0$ and $q, r : \mathbf{N} \to \mathbf{N}$ are polynomial-time computable query-counting functions satisfying $q(n) = o(\sqrt{r(n)})$, then there exist $A, B \in$ NP such that $A \leq^{\mathrm{P}}_{r-tt} B$ but $A \not\leq^{\mathrm{P}}_{q-tt} B$.

6 Conclusion

We have shown that the hyothesis "NP does not have p-measure 0" resolves the CvKL Conjecture affirmatively. We have also shown that this hypothesis resolves other questions in complexity theory, including the class separation E $\neq$ NE, the existence of NP search problems not reducible to the corresponding decision problems, and the separation of various truth-table reducibilities in NP. For each of these questions, the hypothesis gives the answer that seems most likely, relative to our current knowledge. Further investigation of this hypothesis and its power to resolve other questions is clearly indicated.

The most immediate open problem involves the further separation of completeness notions in NP. We have shown that the hypothesis $\mu_{\mathrm{p}}(\mathrm{NP}) \neq 0$ separates $\leq^{\mathrm{P}}_{\mathrm{T}}$-completeness ("Cook completeness") from $\leq^{\mathrm{P}}_{m}$-completeness ("Karp-Levin completeness") in NP. However, there is a large spectrum of completeness notions between $\leq^{\mathrm{P}}_{\mathrm{T}}$ and $\leq^{\mathrm{P}}_{m}$. Watanabe [26, 27] and Buhrman, Homer, and Torenvliet [4] have shown that nearly all these completeness notions are distinct in E and in NE, respectively. In light of the results of sections 4 and 5 above, it is reasonable to conjecture that the hypothesis "NP does not have p-measure 0" yields a similarly detailed separation of completeness notions in NP. Investigation of this conjecture may shed new light on NP-completeness phenomena.

Acknowledgments

We thank Alan Selman, Mitsunori Ogiwara, and Osamu Watanabe for helpful remarks.

References

[1] M. Bellare and S. Goldwasser, The complexity of decision versus search, *SIAM Journal on Computing*, to appear. See also MIT Laboratory for Computer Science Technical Memorandum MIT/LCS/TM 444.

[2] L. Berman and J. Hartmanis, On isomorphism and density of NP and other complete sets, *SIAM Journal on Computing* **6** (1977), pp. 305–322.

[3] R. V. Book, Tally languages and complexity classes, *Information and Control* **26** (1974), pp. 186–193.

[4] H. Buhrman, S. Homer, and L. Torenvliet, Completeness for nondeterministic complexity classes, *Mathematical Systems Theory* **24** (1991), pp. 179–200.

[5] S. A. Cook, The complexity of theorem proving procedures, *Proceedings of the Third ACM Symposium on the Theory of Computing*, 1971, pp. 151–158.

[6] S. Homer, Structural properties of nondeterministic complete sets, *Proceedings of the Fifth Annual Structure in Complexity Theory Conference*, 1990, pp. 3–10.

[7] D. W. Juedes and J. H. Lutz, The complexity and distribution of hard problems, Technical Report 92-23, Department of Computer Science, Iowa State University, 1992.

[8] R. M. Karp, Reducibility among combinatorial problems, In R. E. Miller and J. W. Thatcher, editors, *Complexity of Computer Computations*, pp. 85–104. Plenum Press, 1972.

[9] K. Ko and D. Moore, Completeness, approximation and density, *SIAM Journal on Computing* **10** (1981), pp. 787–796.

[10] R. Ladner, N. Lynch, and A. Selman, A comparison of polynomial-time reducibilities, *Theoretical Computer Science* **1** (1975), pp. 103–123.

[11] L. A. Levin, Universal sequential search problems, *Problems of Information Transmission* **9** (1973), pp. 265–266.

[12] L. Longpré and P. Young, Cook reducibility is faster than Karp reducibility in NP, *Journal of Computer and System Sciences* **41** (1990), pp. 389–401.

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

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

[15] J. H. Lutz and E. Mayordomo, Measure, stochasticity, and the density of hard languages, Technical Report 92–11, Department of Computer Science, Iowa State University, 1992.

[16] E. Mayordomo, Almost every set in exponential time is P-bi-immune, *Seventeenth International Symposium on Mathematical Foundations of Computer Science*, 1992. Springer-Verlag, to appear.

[17] A. R. Meyer, 1977, reported in [2].

[18] M. Ogiwara and O. Watanabe, On polynomial bounded truth-table reducibility of NP sets to sparse sets, *SIAM Journal on Computing* **20** (1991), pp. 471–483.

[19] P. Orponen and U. Schöning, The density and complexity of polynomial cores for intractable sets, *Information and Control* **70** (1986), pp. 54–68.

[20] C. P. Schnorr, Klassifikation der Zufallsgesetze nach Komplexität und Ordnung, *Z. Wahrscheinlichkeitstheorie verw. Geb.* **16** (1970), pp. 1–21.

[21] C. P. Schnorr, A unified approach to the definition of random sequences, *Mathematical Systems Theory* **5** (1971), pp. 246–258.

[22] C. P. Schnorr, Zufälligkeit und Wahrscheinlichkeit, *Lecture Notes in Mathematics* **218** (1971).

[23] C. P. Schnorr, Process complexity and effective random tests, *Journal of Computer and System Sciences* **7** (1973), pp. 376–388.

[24] A. L. Selman, P-selective sets, tally languages, and the behavior of polynomial time reducibilities on NP, *Mathematical Systems Theory* **13** (1979), pp. 55–65.

[25] A. L. Selman, Reductions on NP and P-selective sets, *Theoretical Computer Science* **19** (1982), pp. 287–304.

[26] O. Watanabe, A comparison of polynomial time completeness notions, *Theoretical Computer Science* **54** (1987), pp. 249–265.

[27] O. Watanabe, *On the Structure of Intractable Complexity Classes*, PhD thesis, Tokyo Institute of Technology, 1987.

[28] O. Watanabe and S. Tang, On polynomial time Turing and many-one completeness in PSPACE, *Theoretical Computer Science* **97** (1992), pp. 199–215.

[29] P. Young, Some structural properties of polynomial reducibilities and sets in NP, *Proceedings of the Fifteenth ACM Symposium on Theory of Computing*, 1983, pp. 392–401.