## The Computational Complexity Column

Eric Allender
Rutgers University, Department of Computer Science
Piscataway, NJ 08855 USA
allender@cs.rutgers.edu

A significant segment of the complexity theory community has taken up the study of resource-bounded measure as a tool in understanding complexity classes. For many theoreticians, however, the central problems and accomplishments of this area remain unknown. In this edition of the Column, two leaders in the area of resource-bounded measure map out the frontiers of the field.

# Twelve Problems in Resource-Bounded Measure

Jack H. Lutz [1] and Elvira Mayordomo [2]

## 1 Introduction

Investigation of the measure-theoretic structure of complexity classes began with the development of resource-bounded measure in 1991 [56]. Since that time, a growing body of research by more than forty scientists around the world has shown resource-bounded measure to be a powerful tool that sheds new light on many aspects of computational complexity. Recent survey papers by Lutz [60], Ambos-Spies and Mayordomo [3], and Buhrman and Torenvliet [22] describe many of the achievements of this line of inquiry. In this column, we give a more recent snapshot of resource-bounded measure, focusing not so much on what has been achieved to date as on what we hope will be achieved in the near future.

Section 2 below gives a brief, nontechnical overview of resource-bounded measure in terms of its motivation and principal ideas. Sections 3, 4, and 5 describe twelve specific open problems in the area. We have used the following three criteria in choosing these problems.

1. Their statements are reasonably crisp (not of the form "develop a theory of $x$" or "find applications of $y$ to $z$").

2. We believe that most of them can be solved in the near future.

3. We believe that their solutions will lead to further progress in computational complexity.

Some very important problems have been excluded by criteria 1 and 2. Needless to say, criteria 2 and 3 involve judgments of the uncertain future. We hope that your research helps validate these judgments!

---

[1]Department of Computer Science, Iowa State University, Ames, IA 50011, USA, lutz@cs.iastate.edu. This work was supported in part by National Science Foundation Grant 9610461.

[2]Dept. de Informática e Ingeniería de Sistemas, Universidad de Zaragoza, Zaragoza 50015, Spain, elvira@posta.unizar.es. This work was supported in part by CICYT project (no. TIC 98-0973-C03-02).

## 2 Intractability, Measure, and Betting

Since the early 1970's, the main technique for classifying an apparently intractable problem $A$ has been to identify and study the class of all problems that are efficiently reducible to $A$. Most typically, $A$ is a *decision problem*, i.e., $A \subseteq \{0,1\}^*$, and "efficiently reducible" is taken to mean reducible by a polynomial-time many-one reduction (briefly, a $\leq^{\mathrm{P}}_{\mathrm{m}}$-reduction). In such a case, the set of all problems that are efficiently reducible to $A$ is the *lower* $\leq^{\mathrm{P}}_{\mathrm{m}}$*-span* of $A$, which is the set

$$\mathrm{P_m}(A) = \{B \subseteq \{0,1\}^* \mid B \leq^{\mathrm{P}}_{\mathrm{m}} A\}.$$

For example, if $\mathrm{P_m}(A) = \mathrm{NP}$ (i.e., $A$ is NP-complete), then $A$ is *presumably intractable*, because we believe that $\mathrm{P} \neq \mathrm{NP}$. If $\mathrm{P_m}(A) \supseteq \mathrm{E_2} = \mathrm{DTIME}(2^{poly})$ (i.e., $A$ is hard for exponential time), then $A$ is *provably intractable*, because the time hierarchy theorem of Hartmanis and Stearns [34] implies that $\mathrm{P} \neq \mathrm{E_2}$. Inferences of this kind constitute the primary motivation for studying complexity classes of the form $\mathrm{P_m}(A)$ for various apparently intractable problems $A$. (It is also useful to consider other notions of efficient reducibility here, e.g., to study complexity classes of the form

$$\mathrm{P_T}(A) = \{B \subseteq \{0,1\}^* \mid B \leq^{\mathrm{P}}_{\mathrm{T}} A\},$$

where $\leq^{\mathrm{P}}_{\mathrm{T}}$ denotes polynomial-time Turing reducibility.)

In typical cases of interest, then, one is investigating the structure of a complexity class $\mathcal{C}$ of the form $\mathcal{C} = \mathrm{P_m}(A)$ (or some similar form like $\mathcal{C} = \mathrm{P_T}(A)$), where $A$ is a scientifically interesting decision problem that appears to be intractable. Most typically, the class $\mathcal{C}$ can be proven to satisfy the inclusions

$$\mathrm{P} \subseteq \mathcal{C} \subseteq \mathrm{E_2}$$

and is *conjectured* to satisfy the conditions

1. $\mathrm{P} \neq \mathcal{C}$;
2. $\mathcal{C} \neq \mathrm{E_2}$;
3. for every *fixed* $k$, $\mathcal{C} \not\subseteq \mathrm{DTIME}(2^{n^k})$.

(For example, these conditions are widely conjectured to hold if $\mathcal{C}$ is any of NP, coNP, $\mathrm{D^P}$, PH, PP, PSPACE, etc.) More concisely, we believe that

$$\mathrm{P} \subsetneqq \mathcal{C} \subsetneqq \mathrm{E_2},$$

and that $\mathrm{E_2}$ is the smallest deterministic time complexity class containing $\mathcal{C}$. A substantial part of current research in computational complexity is devoted to studying those structural properties of such a class $\mathcal{C}$ that might yield useful information about the corresponding problem $A$.

The most natural question to ask about the structure of a class $\mathcal{C} \subseteq \mathrm{E_2}$ is, "How big is it?" The most extensively developed mathematical notion of the size of a class of decision problems is its Lebesgue measure, but as the late Richard Hamming complained in a recent essay, Lesbesgue measure "assigns a measure 0 to each countable set, hence to all of the computable numbers, hence in my opinion, all of reality that you can ever name or talk about!" [33]. Indeed, $\mathrm{E}_2$ is countable, so all the classes $\mathcal{C}$ that we are considering have measure 0, so classical Lesbesgue measure does not offer a useful way to distinguish their sizes.

This situation is remedied by *resource-bounded measure*, a generalization of classical Lesbesgue measure developed by Lutz [56, 52]. This theory contains a parameter $\Delta$ (the resource bound), which is a class of functions from $\{0,1\}^*$ to $\{0,1\}^*$. Various choices of $\Delta$ give measures on corresponding classes $R(\Delta)$ of decision problems. If $\Delta = \mathrm{all}$ contains every function from $\{0,1\}^*$ to $\{0,1\}^*$, then $R(\mathrm{all})$ is the class $\mathcal{P}(\{0,1\}^*)$ of all decision problems, and resource-bounded measure is precisely equivalent to classical Lesbesgue measure on this class. It is useful to think of this measure in probabilistic terms: The Lesbesgue measure of a class $\mathcal{C}$ of decision problems is the probability that $A \in \mathcal{C}$ when the decision problem $A \subseteq \{0,1\}^*$ is chosen by using, for each string $x \in \{0,1\}^*$, an independent toss of a fair coin to decide whether $x \in A$. In complexity theory, this measure has been used extensively for random oracle research (dating from the work of Bennett and Gill [14]), but as Hamming noted, every countable class $\mathcal{C}$, hence every class $\mathcal{C}$ of decidable problems, has Lesbesgue measure 0.

If we instead take $\Delta$ to be the set rec, consisting of all *computable* functions from $\{0,1\}^*$ to $\{0,1\}^*$, then resource-bounded measure induces a measure on the class $R(\mathrm{rec}) = \mathrm{REC}$, consisting of all decidable problems. (This measure was shown by Terwijn [82] to be a technical improvement of the measure on REC developed by Freidzon [31].) This measure assigns to each suitable class $\mathcal{C}$ of decision problems a measure $\mu(\mathcal{C} \mid \mathrm{REC})$ (pronounced "the measure of $\mathcal{C}$ in REC"), which is the *size of* $\mathcal{C} \cap \mathrm{REC}$ *as a subset of* REC. (The class $\mathcal{C}$ is "suitable" here if it is "measurable in REC," a technical condition defined in [52]. We deliberately ignore measurability issues in this column, but it should be kept in mind that classes of interest may fail to be measurable.) In general, $0 \leq \mu(\mathcal{C} \mid \mathrm{REC}) \leq 1$, with $\mu(\mathrm{REC} \mid \mathrm{REC}) = 1$. We say that a class $\mathcal{C}$ is *negligibly small in* REC if $\mu(\mathcal{C} \mid \mathrm{REC}) = 0$. For every *fixed* computable time bound $t : \mathbb{N} \to \mathbb{N}$, the class $\mathrm{DTIME}(t(n))$ is negligible in REC [56], so $\mu(\mathrm{E}_2 \mid \mathrm{REC}) = 0$. Thus measure in REC, like Lesbesgue measure, fails to distinguish the sizes of classes $\mathcal{C} \subseteq \mathrm{E}_2$.

The situation is very different if we take $\Delta$ to be the set $\mathrm{p}_2$ of all functions from $\{0,1\}^*$ to $\{0,1\}^*$ that are computable in *quasipolynomial* time, i.e., $n^{(\log n)^{O(1)}} = n^{\mathrm{polylog}\, n}$ time. In this case, $R(\mathrm{p}_2) = \mathrm{E}_2$ and resource-bounded measure assigns each suitable class $\mathcal{C}$ of decision problems a measure $\mu(\mathcal{C} \mid \mathrm{E}_2)$ ("the measure of $\mathcal{C}$ in $\mathrm{E}_2$"), which is the *size of* $\mathcal{C} \cap \mathrm{E}_2$ *as a subset of* $\mathrm{E}_2$. In general, $0 \leq \mu(\mathcal{C} \mid \mathrm{E}_2) \leq 1$, with $\mu(\mathrm{E}_2 \mid \mathrm{E}_2) = 1$. For every *fixed* $k \in \mathbb{N}$, the class $\mathrm{DTIME}(2^{n^k})$ is negligible in $\mathrm{E}_2$, i.e., $\mu(\mathrm{DTIME}(2^{n^k}) \mid \mathrm{E}_2) = 0$ [56]. In particular, $\mu(\mathrm{P} \mid \mathrm{E}_2) = 0$, so almost every decision problem in $\mathrm{E}_2$ is intractable.

The smaller exponential time-complexity class $\mathrm{E} = \mathrm{DTIME}(2^{\mathrm{linear}})$ has an analogous measure structure induced by the resource bound $\Delta = \mathrm{p}$, consisting of all functions from $\{0,1\}^*$ to $\{0,1\}^*$ that are computable in polynomial time. Here we have $R(\mathrm{p}) = \mathrm{E}$, with $0 \leq \mu(\mathcal{C} \mid \mathrm{E}) \leq 1$ for suitable classes $\mathcal{C}$. The measure of E in E is 1, but for every *fixed* $c \in \mathbb{N}$, $\mu(\mathrm{DTIME}(2^{cn}) \mid \mathrm{E}) = 0$, whence $\mu(\mathrm{P} \mid \mathrm{E}) = 0$. Note also that $\mu(\mathrm{E} \mid \mathrm{E}_2) = 0$.

We conclude this section with a brief discussion of the manner in which these measures are defined. Let $\Delta$ be any one of the above-defined resource bounds $\mathrm{p}, \mathrm{p}_2, \mathrm{rec}, \mathrm{all}$, so that $R(\Delta)$ is one of the classes $\mathrm{E}, \mathrm{E}_2, \mathrm{REC}, \mathcal{P}(\{0,1\}^*)$. In general, the definition of $\mu(\mathcal{C} \mid R(\Delta))$ requires the somewhat involved theory described in [61], which in fact requires us to expand the set $\Delta$ to include type-2 functionals satisfying the appropriate constraint (polynomial time, quasipolynomial time, computable, or unrestricted, corresponding to the four possibilities for $\Delta$ that we have mentioned.) However, for most applications of interest, the resource-bounded Kolmogorov zero-one law [61] implies that it suffices to define the conditions $\mu(\mathcal{C} \mid R(\Delta)) = 0$ and $\mu(\mathcal{C} \mid R(\Delta)) = 1$, and these conditions are easy to define using the resource bound $\Delta$ as we have defined it here, with no type-2 functionals involved. (This conceptual gap is already present, though less explicit, in classical measure theory. It is why most mathematics students learn what a measure 0 set is as undergraduates — typically in the characterization of Riemann integrability — but do not learn general measurability and measure until graduate school.) We thus restrict our discussion to the "zero/one fragment" of resource-bounded measure theory.

Resource-bounded measure is based on *martingales*, which are strategies for betting on the membership or nonmembership of successive strings in a decision problem. Martingales were introduced more than sixty years ago by Ville [84] in connection with early efforts by von Mises [85], Wald [86], and Church [28] to define the randomness of individual sequences. Ville's work proved the inadequacy of these efforts, and it was not until 1966 that Martin-Löf [64] used computability theory to give the first successful definition of random sequences. Soon afterwards, Schnorr [73, 74, 75, 76] made extensive use of martingales in his investigations of Martin-Löf's definition and several variants thereof.

Formally, a *martingale* is a function $d : \{0,1\}^* \longrightarrow [0,\infty)$ with the property that, for all $w \in \{0,1\}^*$, $d(w0)+d(w1) = 2d(w)$, i.e., $d(w)$ is the average of $d(w0)$ and $d(w1)$. Intuitively, $d(\lambda)$ — the value of the martingale $d$ at the empty string $\lambda$ — is the initial capital (amount of money) that the martingale $d$ has prior to betting on the membership or nonmembership of the successive strings $s_0, s_1, s_2, \ldots$ (the standard enumeration of $\{0,1\}^*$) in a decision problem $A$. Prior to betting on a string $s_n$, the martingale has capital $d(A[0..n-1])$, where $A[0..n-1]$ is the binary string representing the membership status of $s_0, \ldots, s_{n-1}$ in $A$. After betting on the string $s_n$, the martingale has capital $d(A[0..n])$. The condition $d(w0) + d(w1) = 2d(w)$ ensures that the betting is "fair."

A martingale $d$ *succeeds* on a decision problem $A$ if its capital is unbounded when it bets on $A$. It was proven by Ville [84] (and it is easy to see) that a set $X$ of decision problems has classical (Lesbesgue) measure 0 if and only if there is a martingale $d$ such that $d$ succeeds on every element of $X$. Generalizing this idea, Lutz [56] made the following definitions. Let $X$ be a set of decision problems.

1. $X$ has *$\Delta$-measure 0*, and we write $\mu_\Delta(X) = 0$, if there is a martingale $d \in \Delta$ such that $d$ succeeds on every element of $X$.

2. $X$ has *$\Delta$-measure 1*, and we write $\mu_\Delta(X) = 1$, if the complement $X^c$ of $X$ has $\Delta$-measure 0.

3. $X$ has *measure 0 in* $R(\Delta)$, and we write $\mu(X \mid R(\Delta)) = 0$, if $\mu_\Delta(X \cap R(\Delta)) = 0$.

4. $X$ has *measure 1 in* $R(\Delta)$, and we write $\mu(X \mid R(\Delta)) = 1$, if $\mu(X^c \mid R(\Delta)) = 0$. In this case, we say that $X$ contains *almost every* element of $R(\Delta)$.

Thus, for example, a set $X$ has measure 0 in $\mathrm{E}_2$ if there is a martingale $d \in \mathrm{p}_2$ — i.e., a martingale computable in quasipolynomial time — such that $d$ succeeds on every element of $X \cap \mathrm{E}_2$.

It was shown in [56] that these definitions endow E, $\mathrm{E}_2$, and other complexity classes with nontrivial measure-theoretic structure.

## 3 Weak Completeness and Derandomization

As noted in section 2, problems that are $\leq^{\mathrm{P}}_{\mathrm{m}}$-hard for exponential time are provably intractable by the time hierarchy theorem of Hartmanis and Stearns [34]. In fact, in the 1980's, such problems were shown to have very strong intractability properties [11, 37, 69, 77]. In order to extend the class of provably intractable problems, Lutz [54] introduced a generalization of hardness, called weak hardness.

A decision problem $A \subseteq \{0,1\}^*$ is *weakly* $\leq^{\mathrm{P}}_{\mathrm{m}}$*-hard* for $\mathrm{E}_2$ if $\mathrm{P_m}(A)$ does not have measure 0 in $\mathrm{E}_2$. That is, $A$ is weakly $\leq^{\mathrm{P}}_{\mathrm{m}}$-hard for $\mathrm{E}_2$ if all the decision problems in a nonnegligible subset of $\mathrm{E}_2$ are $\leq^{\mathrm{P}}_{\mathrm{m}}$-reducible to $A$. A decision problem $A$ is *weakly* $\leq^{\mathrm{P}}_{\mathrm{m}}$*-complete* for $\mathrm{E}_2$ if $A \in \mathrm{E}_2$ and $A$ is weakly $\leq^{\mathrm{P}}_{\mathrm{m}}$-hard for $\mathrm{E}_2$.

Elementary properties of measure in $\mathrm{E}_2$ [56] imply immediately that every $\leq^{\mathrm{P}}_{\mathrm{m}}$-hard problem for $\mathrm{E}_2$ is weakly $\leq^{\mathrm{P}}_{\mathrm{m}}$-hard, and that no element of P can be weakly $\leq^{\mathrm{P}}_{\mathrm{m}}$-hard for $\mathrm{E}_2$. Thus weak hardness generalizes hardness, weak completeness generalizes completeness, and weakly hard problems are necessarily intractable. In fact, Juedes and Lutz [41] have shown that weakly $\leq^{\mathrm{P}}_{\mathrm{m}}$-hard problems for $\mathrm{E}_2$ have the strongest intractability properties known to hold for $\leq^{\mathrm{P}}_{\mathrm{m}}$-hard problems for $\mathrm{E}_2$.

The next question to answer was whether weak completeness is a *proper* generalization of completeness. That is, do there exist problems that are weakly $\leq^{\mathrm{P}}_{\mathrm{m}}$-complete, but not $\leq^{\mathrm{P}}_{\mathrm{m}}$-complete, for $\mathrm{E}_2$? This question was answered affirmatively by Lutz [58], who used a "martingale diagonalization" to prove the existence of such problems. Juedes [40] then refined this technique to prove that the weakly $\leq^{\mathrm{P}}_{\mathrm{m}}$-complete problems form a non-measure 0 subset of $\mathrm{E}_2$. Since Mayordomo [65] and Juedes and Lutz [41] had already shown that the $\leq^{\mathrm{P}}_{\mathrm{m}}$-complete problems form a measure 0 subset of $\mathrm{E}_2$, this established that a nonnegligible subset of $\mathrm{E}_2$ consists of problems that are weakly $\leq^{\mathrm{P}}_{\mathrm{m}}$-complete but not $\leq^{\mathrm{P}}_{\mathrm{m}}$-complete.

Much more turned out to be true. Ambos-Spies, Terwijn, and Zheng [5] developed the *martingale dilation* technique and used it to prove that the weakly $\leq^{\mathrm{P}}_{\mathrm{m}}$-complete problems form a measure 1 subset of $\mathrm{E}_2$. That is, *almost every* problem in $\mathrm{E}_2$ is weakly $\leq^{\mathrm{P}}_{\mathrm{m}}$-complete but not $\leq^{\mathrm{P}}_{\mathrm{m}}$-complete. We thus have an *abundance* of problems that are provably strongly intractable but not $\leq^{\mathrm{P}}_{\mathrm{m}}$-hard for exponential time. In contrast, existing proofs of the intractability of natural problems (see, for example [81]) have been proofs that these problems are $\leq^{\mathrm{P}}_{\mathrm{m}}$-hard for exponential time. Since developing techniques for proving the intractability of natural problems is arguably the main objective of computational complexity theory, this leads to the first and most important of our twelve problems.

**Problem 1** ([58, 60]) *Prove that some specific, natural decision problem is weakly complete, but not complete, for* $\mathrm{E}_2$*. (The word "natural" here is necessarily informal. It definitely excludes constructions by diagonalization or randomization as in [58, 40, 5]. Ideally, a natural example would be a decision problem of independent interest that has already been studied in some other context.) Alternatively, prove a theorem indicating the nonexistence of such natural examples.*

The investigation of small span theorems has played a key role in several recent developments. The *lower* $\leq_{\mathrm{m}}^{\mathrm{P}}$*-span* of a decision problem $A$ is the set $\mathrm{P_m}(A)$ that we have already discussed, namely, the set of all decision problems that are $\leq_{\mathrm{m}}^{\mathrm{P}}$-reducible to $A$. Similarly, the *upper* $\leq_{\mathrm{m}}^{\mathrm{P}}$*-span* of $A$ is the set ${\mathrm{P_m}}^{-1}(A)$ consisting of those decision problems $B$ to which $A$ is $\leq_{\mathrm{m}}^{\mathrm{P}}$-reducible.

The Small Span Theorem for $\leq_{\mathrm{m}}^{\mathrm{P}}$ in $\mathrm{E_2}$ is the assertion that for every $A \in \mathrm{E_2}$, it must be the case that $\mu(\mathrm{P_m}(A) \mid \mathrm{E_2}) = 0$ or $\mu_{\mathrm{p_2}}({\mathrm{P_m}}^{-1}(A)) = \mu({\mathrm{P_m}}^{-1}(A) \mid \mathrm{E_2}) = 0$. That is, at least one of the upper and lower spans of $A$ is small. Juedes and Lutz [41] proved this result and the corresponding Small Span Theorem for $\leq_{\mathrm{m}}^{\mathrm{P}}$ in E. Since the $\leq_{\mathrm{m}}^{\mathrm{P}}$-degree of $A$ is the intersection of the upper and lower $\leq_{\mathrm{m}}^{\mathrm{P}}$-spans of $A$, it follows easily that every $\leq_{\mathrm{m}}^{\mathrm{P}}$-degree has measure 0 in each of E and $\mathrm{E_2}$. Juedes and Lutz [41] also noted that a Small Span Theorem for $\leq_{\mathrm{T}}^{\mathrm{P}}$ in E or $\mathrm{E_2}$ would (in combination with a result of Bennett and Gill [14]) imply the long-sought separation of BPP from $\mathrm{E_2}$, and thus called for a program of proving Small Span Theorems for reductions of increasing power between $\leq_{\mathrm{m}}^{\mathrm{P}}$-reductions and $\leq_{\mathrm{T}}^{\mathrm{P}}$-reductions. (Ambos-Spies, Neis and Terwijn [4] subsequently pointed out that a Small Span Theorem for $\leq_{\mathrm{tt}}^{\mathrm{P}}$ in E and $\mathrm{E_2}$ would also imply $\mathrm{BPP} \neq \mathrm{E_2}$.) A number of steps have now been taken in this program. Lindner [50] refined the argument in [41] to prove Small Span Theorems for $\leq_{1-\mathrm{tt}}^{\mathrm{P}}$ in E and $\mathrm{E_2}$. Ambos-Spies, Neis, and Terwijn [4] used resource-bounded genericity to prove Small Span Theorems for $\leq_{k-\mathrm{tt}}^{\mathrm{P}}$ in E and $\mathrm{E_2}$ (for each *fixed* positive integer $k$) and, in the same paper, proved that their technique could not be extended to reductions with an unbounded number of queries. Lutz [51, 43] proved a Small Span Theorem for $\leq_{\mathrm{T}}^{\mathrm{P/Poly}}$-reductions (Turing reductions computed by nonuniform polynomial size circuits) in ESPACE. Finally, in a breakthrough result, Buhrman and van Melkebeek [23] used a clever betting argument to prove a Small Span Theorem for $\leq_{n^{o(1)}-\mathrm{tt}}^{\mathrm{P}}$-reductions in $\mathrm{E_2}$. Curiously, their proof does not work in E, where the above-mentioned $\leq_{k-\mathrm{tt}}^{\mathrm{P}}$-result of [4] is still the best that is known.

**Problem 2** ([23]) *Prove (or disprove) a Small Span Theorem for unbounded-query reductions in* E.

An explicit pseudorandom generator construction by Nisan and Wigderson [68] has been the basis for several interactions between resource-bounded measure and the BPP question. Using this work, Lutz showed that $\mathrm{P} \neq \mathrm{BPP}$ implies that E has measure 0 in ESPACE [55] (improving the result by Hartmanis and Yesha [35] that $\mathrm{P} \neq \mathrm{BPP}$ implies $\mathrm{E} \neq \mathrm{ESPACE}$) and that the $\leq_{\mathrm{T}}^{\mathrm{P}}$-hard problems for BPP form a set of pspace-measure 1 [57] (improving the result by Bennett and Gill [14] that this set has classical measure 1). More significantly, Allender and Strauss [1] improved this latter result by showing that the $\leq_{\mathrm{T}}^{\mathrm{P}}$-hard problems for BPP form a set of p-measure 1. Thus almost every problem in E is $\leq_{\mathrm{T}}^{\mathrm{P}}$-hard for BPP (and similarly for $\mathrm{E_2}$). It follows easily that, if the $\leq_{\mathrm{T}}^{\mathrm{P}}$-complete degree does not have measure 1 in E (or does not have measure 1 in $\mathrm{E_2}$), then $\mathrm{BPP} \neq \mathrm{E_2}$. This appears to be a considerable improvement over the earlier observation [41] that a Small Span Theorem for $\leq_{\mathrm{T}}^{\mathrm{P}}$ in E or $\mathrm{E_2}$ would imply $\mathrm{BPP} \neq \mathrm{E_2}$. For example, Buhrman, Fortnow, van Melkebeek, and Torenvliet [21] have shown that every $\leq_{\mathrm{T}}^{\mathrm{P}}$-complete problem for $\mathrm{E_2}$ is $\leq_{\mathrm{T}}^{\mathrm{P}}$-autoreducible, and Buhrman, van Melkebeek, Regan, Sivakumar, and Strauss [24] have used this fact (and its $\leq_{\mathrm{tt}}^{\mathrm{P}}$ analog) together with betting games closely related to martingales to give a dozen seemingly plausible conditions, each of which would be sufficient to establish $\mathrm{BPP} \neq \mathrm{E_2}$.

Some natural conditions involving weak completeness also imply $\mathrm{BPP} \neq \mathrm{E}_2$. Juedes and Lutz [42] proved that there are decision problems in E that are weakly $\leq^{\mathrm{P}}_{\mathrm{m}}$-complete for $\mathrm{E}_2$, but not for E. As we have already noted, Lutz [58] proved that there are decision problems that are weakly $\leq^{\mathrm{P}}_{\mathrm{m}}$-complete, but not $\leq^{\mathrm{P}}_{\mathrm{m}}$-complete, for $\mathrm{E}_2$. The $\leq^{\mathrm{P}}_{\mathrm{T}}$-analogs of these results are conditions 2 and 3 of the following problem. (The $\leq^{\mathrm{P}}_{\mathrm{tt}}$ analog of this problem is also of interest.)

**Problem 3** *Consider the following five conditions.*

1. *The Small Span Theorem for* $\leq^{\mathrm{P}}_{\mathrm{T}}$ *in* E.
2. *There is a decision problem in* E *that is weakly* $\leq^{\mathrm{P}}_{\mathrm{T}}$*-complete for* $\mathrm{E}_2$*, but not for* E.
3. *There is a decision problem that is weakly* $\leq^{\mathrm{P}}_{\mathrm{T}}$*-complete, but not* $\leq^{\mathrm{P}}_{\mathrm{T}}$*-complete, for* $\mathrm{E}_2$.
4. *The* $\leq^{\mathrm{P}}_{\mathrm{T}}$*-complete degree does not have measure 1 in* $\mathrm{E}_2$.
5. $\mathrm{BPP} \neq \mathrm{E}_2$.

*Using results of Juedes and Lutz [42], Ambos-Spies, Terwijn, and Zheng [5], and Allender and Strauss [1], it is easy to see that*

$$1 \Rightarrow 2 \Rightarrow 3 \Leftrightarrow 4 \Rightarrow 5$$

*What else can be proven about the relative strengths of these five conditions?*

Recent, more sophisticated pseudorandom generator constructions appear to be verging on a complete derandomization of BPP. Impagliazzo and Wigderson [38] (improving on results of Andreev, Clementi, and Rolim, surveyed in this column [29]) have proven that $\mathrm{P} = \mathrm{BPP}$ unless every problem in E has subexponential-size Boolean circuits. More recently, Impagliazzo and Wigderson [39] have proven that, if $\mathrm{BPP} \neq \mathrm{E}_2$, than every problem in BPP can be decided deterministically in subexponential time for almost all inputs of infinitely many input lengths. As pointed out by van Melkebeek [83], this result implies that BPP has the "zero-one property" that, if $\mathrm{BPP} \neq \mathrm{E}_2$, then BPP has p-measure 0, hence measure 0 in E and $\mathrm{E}_2$. (This improved the result by Buhrman, Fenner, and Fortnow [19] that, if $\mathrm{AM} \neq \mathrm{E}_2$, then BPP has p-measure 0.)

The Graph Isomorphism problem is perhaps the canonical example of a problem known to be in NP but widely conjectured to be neither in P nor NP-complete [49]. This problem is known to be in $\mathrm{NP} \cap \mathrm{coAM}$ [48], and this fact has been used by many investigators to give increasingly strong evidence that it is not NP-complete. (See [48] for a survey of such results, and [59, 8] for more recent work using resource-bounded measure.) Very recently, Klivans and van Melkebeek [46] have used nontrivial derandomization techniques to give evidence that $\mathrm{AM} = \mathrm{NP}$, whence Graph Isomorphism would be in $\mathrm{NP} \cap \mathrm{coNP}$. It should be noted, however, that all these results involve unproven (though plausible) hypotheses, and none of them uses any property of Graph Isomorphism more specific than its membership in $\mathrm{NP} \cap \mathrm{coAM}$. The following problem suggests that an absolute result might be obtained by using resource-bounded measure and specific properties of Graph Isomorphism.

**Problem 4** *Prove that Graph Isomorphism is not weakly complete (and hence not complete) for exponential time.*

## 4 Nonuniform Complexity

The difficulty of solving an intractable problem may arise from one or both of two aspects of complexity. The problem may have high *nonuniform complexity*, meaning that it is combinatorially, or information-theoretically, infeasible. Even failing this, it may have high *uniform complexity*, meaning that no single algorithm can solve the problem on all inputs of all lengths. Understanding the relationship between these two kinds of complexity is one of the major challenges of computational complexity theory.

It is widely believed that $\mathrm{NP} \not\subseteq \mathrm{P/Poly}$, i.e., that problems complete for NP are *combinatorially* infeasible in the sense that they cannot be solved, even nonuniformly, by polynomial-size circuits. However, even the conjecture that $\mathrm{E}_2 \not\subseteq \mathrm{P/Poly}$ (equivalently, that $\mathrm{E} \not\subseteq \mathrm{P/Poly}$) has not been proven and appears to be very difficult.

Kannan [44] proved that $\mathrm{ESPACE} \not\subseteq \mathrm{P/Poly}$ and, in fact, that $\Sigma_2^{\mathrm{E}} \cap \Pi_2^{\mathrm{E}} \not\subseteq \mathrm{P/Poly}$, where $\Sigma_2^{\mathrm{E}} = \mathrm{NE(NP)}$ is the second level of the exponential hierarchy. In one of the first applications of resource-bounded measure, Lutz [56] strengthened the ESPACE result by proving that, for every real $\alpha < 1$, *almost every* problem in ESPACE requires a Boolean circuit of more than $\frac{2^n}{n}(1+\frac{\alpha \log n}{n})$ gates for all but finitely many input lengths $n$. This lower bound actually exceeds the lower bound $\frac{2^n}{n}(1-\varepsilon)$ proven by Shannon [79] for the worst case complexity of arbitrary problems, and it is not difficult to see that the proof in [56] also yields the *existence* of a problem in $\Sigma_2^{\mathrm{E}} \cap \Pi_2^{\mathrm{E}}$ that requires exponentially many gates for all but finitely many input lengths. Very recently, Buhrman, Fortnow, and Thierauf [20] have proven that $\mathrm{PE}_2 \not\subseteq \mathrm{P/Poly}$, where $\mathrm{PE}_2$ is the exponential-time version of PP. (Curiously, it is still not known whether $\mathrm{PE}_2$ requires exponentially many gates.) Lutz [56] has shown that P/Poly has measure 0 in $\mathrm{E}_3 = \mathrm{DTIME}(2^{n^{\mathrm{polylog}\ n}})$, which is the next class above E and $\mathrm{E}_2$ in a natural hierarchy of exponential-time complexity classes. Lutz [56] conjectured that P/Poly has measure 0 in E and in $\mathrm{E}_2$, and that proving this might be the easiest way to obtain separations $\mathrm{E} \not\subseteq \mathrm{P/Poly}$ and $\mathrm{E}_2 \not\subseteq \mathrm{P/Poly}$. This conjecture should now be viewed with extreme caution, because Regan, Sivakumar, and Cai [72] have used the "natural proofs" idea of Razborov and Rudich [71] to prove that, if exponentially secure pseudorandom generators exist, then P/Poly is not measurable in $\mathrm{E}_2$.

The measure of P/Poly in the classes of the exponential hierarchies over E and $\mathrm{E}_2$ is still not understood. As noted above, Kannan [44] showed that $\Sigma_2^{\mathrm{E}} \cap \Pi_2^{\mathrm{E}} \not\subseteq \mathrm{P/Poly}$. Wilson [88] exhibited an oracle relative to which $\Delta_2^{\mathrm{E}_2} \subseteq \mathrm{P/Poly}$ (and Heller [36] improved this to $\Delta_2^{\mathrm{E}_2} \subseteq \mathrm{BPP}$), where $\Delta_2^{\mathrm{E}_2} = \mathrm{E}_2(\mathrm{NP})$. Regarding measure, Mayordomo [66] used Stockmeyer's approximate counting method [80] to prove that P/Poly has measure 0 in $\Delta_3^{\mathrm{E}} = \mathrm{E}(\Sigma_2^{\mathrm{P}})$. Recently, Köbler and Lindner [47] have shown that, if $\mu_{\mathrm{p}}(\mathrm{NP}) \neq 0$ (a hypothesis discussed in section 5 below), then P/Poly has measure 0 in $\Delta_2^{\mathrm{E}_2} = \mathrm{E}_2(\mathrm{NP})$.

**Problem 5** *Close the gap between the above-mentioned results of [72] and [66]. Does* P/Poly *have measure 0 in a class lower than* $\Delta_3^{\mathrm{E}}$*? Does the existence of very secure pseudorandom generators imply that* P/Poly *is not measurable in a class higher than* $\mathrm{E}_2$*?*

Meyer [67] showed that $\mathrm{P/Poly} = \mathrm{P_T(SPARSE)}$, i.e., a decision problem has (nonuniform) polynomial-size circuits if and only if it is $\leq_{\mathrm{T}}^{\mathrm{P}}$-reducible to some problem $S \in \{0,1\}^*$ that is *sparse* (i.e., there is a polynomial $q$ such that $\mid S \cap \{0,1\}^{\leq n} \mid < q(n)$ for all $n$). Meyer [67] also showed that $\mathrm{E} \not\subseteq \mathrm{P_m(SPARSE)}$, and in fact that $\mathrm{E} \not\subseteq \mathrm{P_m(DENSE^c)}$, where DENSE is the set of all problems $D \subseteq \{0,1\}^*$ that are *dense* (i.e., there is a real $\varepsilon > 0$ such that $\mid D \cap \{0,1\}^{\leq n} \mid > 2^{n^\varepsilon}$ for all sufficiently large $n$) and $\mathrm{DENSE}^{\mathrm{c}}$ is the complement of DENSE. This suggested the program of trying to prove theorems of the form $\mathrm{E} \not\subseteq \mathrm{P_r(SPARSE)}$ for successively large classes $\mathrm{P_r(SPARSE)}$ in the range between $\mathrm{P_m(SPARSE)}$ and $\mathrm{P_T(SPARSE)}$. Ideally, of course, such results will be of the stronger form $\mathrm{E} \not\subseteq \mathrm{P_r(DENSE^c)}$. Watanabe [87] took the second big step in this program by proving that $\mathrm{E} \not\subseteq \mathrm{P}_{O(\log n)-\mathrm{tt}}(\mathrm{DENSE^c})$. The next big step used resource-bounded measure: Lutz and Mayordomo [62] proved that, for every real $\alpha < 1$, $\mathrm{P}_{n^\alpha-\mathrm{tt}}(\mathrm{DENSE^c})$ has measure 0 in E (and in $\mathrm{E_2}$), whence it certainly follows that $\mathrm{E} \not\subseteq \mathrm{P}_{n^\alpha-\mathrm{tt}}(\mathrm{DENSE^c})$. Subsequently, and independently, Fu [32] proved that, for every $\alpha < \frac{1}{2}$, $\mathrm{E} \not\subseteq \mathrm{P}_{n^\alpha-\mathrm{T}}(\mathrm{DENSE^c})$ and, for every $\alpha < 1$, $\mathrm{E_2} \not\subseteq \mathrm{P}_{n^\alpha-\mathrm{T}}(\mathrm{DENSE^c})$. Recently, Lutz and Zhao [53] unified this work with much of that in [62] by proving that, for every $\alpha < \frac{1}{2}$, $\mathrm{P}_{n^\alpha-\mathrm{T}}(\mathrm{DENSE^c})$ has measure 0 in E and, for every $\alpha < 1$, $\mathrm{P}_{n^\alpha-\mathrm{T}}(\mathrm{DENSE^c})$ has measure 0 in $\mathrm{E_2}$. These results leave a curious gap that may be technically significant.

**Problem 6** *For $\frac{1}{2} \leq \alpha < 1$, is it the case that $\mathrm{P}_{n^\alpha-\mathrm{T}}(\mathrm{DENSE^c})$ has p-measure 0 (or, at least, that $\mathrm{E} \not\subseteq \mathrm{P}_{n^\alpha-\mathrm{T}}(\mathrm{SPARSE})$)?*

Problems that are sparse have very low information content, and reducibility to such problems has been extensively investigated. (Much of this work is surveyed in the ten-author paper [7].) Reducibility to problems of very high information content is also of interest, but the study has barely begun. It is already clear that there are some (perhaps surprising) connections between the two subjects. For example Book and Lutz [16] have shown that, if a problem in ESPACE is $\leq^{\mathrm{P}}_{\mathrm{btt}}$-reducible to a problem of very high space-bounded Kolmogorov complexity, then it is $\leq^{\mathrm{P}}_{\mathrm{btt}}$-reducible to a sparse problem. Arvind, Köbler, and Mundhenk [9, 10] have improved on this result in several respects.

A problem that is *random* in the sense of Martin-Löf [64] has extremely high information content. It is sometimes (e.g., in the context of computational depth [13]) of interest to know whether an algorithm can, from a random object, compute an object that could not have been computed from *any* random object with significantly less resources. In this connection, Book, Lutz, and Martin [17] proved that, if RAND is the set of all random decision problems, then for every $R \in \mathrm{RAND}$ and $k \in \mathbb{N}$, $\mathrm{P}_{(k+1)-\mathrm{tt}}(R) \not\subseteq \mathrm{P}_{k-\mathrm{tt}}(\mathrm{RAND})$, whence $\mathrm{P}_{k-\mathrm{tt}}(\mathrm{RAND}) \subsetneqq \mathrm{P}_{(k+1)-\mathrm{tt}}(\mathrm{RAND})$.

Resource-bounded measure provides notions of resource-bounded randomness that are exactly analogous to Martin Löf's notion [56]. For example, a problem $R$ is defined to be p-random, and we write $R \in \mathrm{RAND(p)}$, if the singleton set $\{R\}$ does not have p-measure 0. It is easy to see that $\mathrm{E} \cap \mathrm{RAND(p)} = \emptyset$, but it is known that almost every element of $\mathrm{E_2}$ is p-random [56].

**Problem 7** *Prove (or disprove) that, for all $k \in \mathbb{N}$, $\mathrm{P}_{k-\mathrm{tt}}(\mathrm{RAND(p)}) \subsetneqq \mathrm{P}_{(k+1)-\mathrm{tt}}(\mathrm{RAND(p)})$. Ideally, prove that, for all $k \in \mathbb{N}$ and $R \in \mathrm{RAND(p)}$, $\mathrm{E_2} \cap \mathrm{P}_{(k+1)-\mathrm{tt}}(R) \not\subseteq \mathrm{P}_{k-\mathrm{tt}}(\mathrm{RAND(p)})$.*

# 5 Strong Hypotheses

Even if we *assume* that $\mathrm{P} \neq \mathrm{NP}$, most open questions about computational complexity remain open. There are, of course, exceptions, the most notable of which is the proof by Arora, Lund, Motwani, Sudan, and Szegedy [6] that, if $\mathrm{P} \neq \mathrm{NP}$, then no MAXSNP-complete problem has a polynomial-time approximation scheme. Nevertheless, for the most part, relative to our current knowledge, the $\mathrm{P} \neq \mathrm{NP}$ hypothesis *lacks explanatory power* in the sense that we do not know how to use it to resolve many questions. Other "traditional" complexity-theoretic hypotheses such as the separation of the polynomial-time hierarchy into infinitely many levels, also lack explanatory power in this sense.

In order to progress toward a remedy of this situation, Lutz proposed investigation of various strong, measure-theoretic hypotheses, the most notable of which is the hypothesis that NP does not have p-measure 0 (written $\mu_{\mathrm{p}}(\mathrm{NP}) \neq 0$). This hypothesis holds if and only if NP is a nonnegligible subset of $\mathrm{E}_2$ [5]. By the resource-bounded Kolmogorov zero-one law of Lutz [61] and the "most is all" theorem of Regan, Sivakumar, and Cai [72], this hypothesis implies that NP is a nonmeasurable subset of $\mathrm{E}_2$ (a condition defined in [61]) unless $\mathrm{NP} = \mathrm{E}_2$. Lutz and Juedes [42] have shown that the $\mu_{\mathrm{p}}(\mathrm{NP}) \neq 0$ hypothesis holds if NP contains a nonnegligible subset of E, but the converse has not been proven. The $\mu_{\mathrm{p}}(\mathrm{NP}) \neq 0$ hypothesis is now known to have many provable, plausible consequences that are not known to follow from more traditional hypotheses. Among these are the following.

- NP contains a P-bi-immune problem (Mayordomo [65]).
- $\mathrm{E} \neq \mathrm{NE}$ and $\mathrm{EE} \neq \mathrm{NEE}$ (Lutz and Mayordomo [63]).
- There is an NP search problem that does not reduce to the corresponding decision problem (Bellare and Goldwasser [12], Lutz and Mayordomo [63]).
- Every problem that is $\leq_{\mathrm{m}}^{\mathrm{P}}$-hard for NP has a dense exponential complexity core (Juedes and Lutz [41]).
- There is a problem that is $\leq_{\mathrm{T}}^{\mathrm{P}}$-complete (in fact, $\leq_{2-\mathrm{T}}^{\mathrm{P}}$-complete), but not $\leq_{\mathrm{m}}^{\mathrm{P}}$-complete, for NP (Lutz and Mayordomo [63]).
- For every $k \geq 2$, there is a problem that is $\leq_{(k+1)-\mathrm{tt}}^{\mathrm{P}}$-complete, but not $\leq_{k-\mathrm{tt}}^{\mathrm{P}}$-complete, for NP (Ambos-Spies and Bentzien [2]).
- For every $k \geq 1$, there is a problem that is $\leq_{(k+1)-\mathrm{T}}^{\mathrm{P}}$-complete, but not $\leq_{k-\mathrm{T}}^{\mathrm{P}}$-complete, for NP (Ambos-Spies and Bentzien [2]).
- There is a problem that is $\leq_{\mathrm{tt}}^{\mathrm{P}}$-complete, but not $\leq_{\mathrm{btt}}^{\mathrm{P}}$-complete, for NP (Ambos-Spies and Bentzien [2]).
- For every real number $\alpha < 1$, every $\leq_{n^{\alpha}-\mathrm{tt}}^{\mathrm{P}}$-hard problem for NP is dense (Lutz and Mayordomo [62]).
- For every real number $\alpha < 1/2$, every $\leq_{n^{\alpha}-\mathrm{T}}^{\mathrm{P}}$-hard problem for NP is dense (Lutz and Zhao [53]).
- For every $k \geq 2$, there is a sequence $\vec{D} = (D_1, \ldots, D_k)$ of NP decision problems such that $\vec{D}$ is sequentially complete for NP, but no nontrivial permutation of $\vec{D}$ is sequentially complete for NP (Dai and Lutz [30]).

- There is a decision problem that, relative to every polynomial time computable distribution, is in DistNP but not AVP (Cai and Selman [25]).
- Every DistNP-complete problem has a reasonable distribution (Pavan and Selman [70]).
- BPP $\subseteq \Delta_2^{\mathrm{P}}$ (Allender and Strauss [1]).
- For all $k \geq 2$, $\mathrm{BP} \cdot \Delta_k^{\mathrm{P}} = \Delta_k^{\mathrm{P}}$. Thus $\Delta_2^{\mathrm{P}} \neq \mathrm{PH}$ implies that Graph Isomorphism is not NP-complete, and that $\mathrm{NP} \not\subseteq \mathrm{P/Poly}$ (Lutz [59]).
- For all $k \geq 2$, $\mathrm{BP} \cdot \Sigma_k^{\mathrm{P}} = \Sigma_k^{\mathrm{P}}$ and $\mathrm{BP} \cdot \Theta_k^{\mathrm{P}} = \Theta_k^{\mathrm{P}}$ (Arvind and Köbler [8]).
- AM $\subseteq$ NP/log (Arvind and Köbler [8]).
- P/Poly has measure 0 in $\Delta_2^{\mathrm{E}_2} = \mathrm{E}_2(\mathrm{NP})$ (Köbler and Lindner [47]).

It is evident that the hypothesis $\mu_{\mathrm{p}}(\mathrm{NP}) \neq 0$ has considerable explanatory power, but the full extent of this power has yet to be understood.

**Problem 8** *Does $\mu_{\mathrm{p}}(\mathrm{NP}) \neq 0$ imply an exponential lower bound on approximation schemes for* MAXSAT*?*

**Problem 9** ([63], [22]) *Does $\mu_{\mathrm{p}}(\mathrm{NP}) \neq 0$ imply the existence of a problem that is $\leq_{\mathrm{T}}^{\mathrm{P}}$-complete, but not $\leq_{\mathrm{tt}}^{\mathrm{P}}$-complete, for* NP*?*

**Problem 10** ([66]) *Can the Berman-Hartmanis Isomorphism Conjecture be resolved under the hypothesis $\mu_{\mathrm{p}}(\mathrm{NP}) \neq 0$, or perhaps the hypothesis $\mu_{\mathrm{p}}(\mathrm{UP}) \neq 0$? Is the latter hypothesis reasonable?*

**Problem 11** ([78]) *Does the hypothesis $\mu_{\mathrm{p}}(\Sigma_2^{\mathrm{P}} - \Pi_2^{\mathrm{P}}) \neq 0$ imply that* $\mathrm{NP} \not\subseteq \mathrm{P/Poly}$*?*

The reasonableness of the $\mu_{\mathrm{p}}(\mathrm{NP}) \neq 0$ hypothesis is not easy to asses. Since it implies that $\mathrm{P} \neq \mathrm{NP}$ and its negation implies $\mathrm{NP} \neq \mathrm{E}_2$, it is not likely to be proven or refuted mathematically in the near future. Kautz and Miltersen [45] have shown that it holds relative to a random oracle, but this appears to tell us nothing about the unrelativized case [27]. Cai, Sivakumar, and Strauss [26] have shown that a "bounded-depth analog" of the hypothesis is false, but this involves a severely constrained computational model and also appears unlikely to tell us anything about the $\mu_{\mathrm{p}}(\mathrm{NP}) \neq 0$ hypothesis. For the time being, Lutz [60] has advocated evaluating $\mu_{\mathrm{p}}(\mathrm{NP}) \neq 0$ as a *scientific hypothesis*, in terms of the extent and plausibility of its provable consequences.

One more intrinsic aspect of the $\mu_{\mathrm{p}}(\mathrm{NP}) \neq 0$ hypothesis *has* been investigated, namely, its robustness with respect to the underlying probability measure. Breutzmann and Lutz [18] have shown that if $\vec{\beta} = (\beta_0, \beta_1, \ldots)$ is any P-computable sequence of biases $\beta_i \in [0,1]$ that are bounded away from 0 and 1, and if $\mu^{\vec{\beta}}$ is the probability measure in which a decision problem $A \subseteq \{0,1\}^*$ is chosen by placing the $i$-th string in $A$ with probability $\beta_i$ *independently of all other strings*, then $\mu_{\mathrm{p}}^{\vec{\beta}}(\mathrm{NP}) = 0$ if and only if $\mu_{\mathrm{p}}(\mathrm{NP}) = 0$ (and similarly for other "reasonable" complexity classes). Thus the hypothesis $\mu_{\mathrm{p}}(\mathrm{NP}) \neq 0$ is robust with respect to a wide variety of probability measures. Nevertheless, the hypothesis placed on $\mu^{\vec{\beta}}$ is substantial, especially in its requirement of independence.

**Problem 12** ([18]) *How extensive is the class of* p*-computable probability measures* $\nu$ *for which* $\nu_{\mathrm{p}}(\mathrm{NP}) = 0$ *is equivalent to* $\mu_{\mathrm{p}}(\mathrm{NP}) = 0$*?*

## Acknowledgment

We thank Eric Allender for several editorial improvements.

## References

[1] E. Allender and M. Strauss. Measure on small complexity classes with applications for BPP. In *Proceedings of the 35th Symposium on Foundations of Computer Science*, pages 807–818, Piscataway, NJ, 1994. IEEE Computer Society Press.

[2] K. Ambos-Spies and L. Bentzien. Separating NP-completeness notions under strong hypotheses. In *Proceedings of the 12th IEEE Conference on Computational Complexity*, pages 121–127, 1997.

[3] K. Ambos-Spies and E. Mayordomo. Resource-bounded measure and randomness. In A. Sorbi, editor, *Complexity, Logic and Recursion Theory*, Lecture Notes in Pure and Applied Mathematics, pages 1–47. Marcel Dekker, New York, N.Y., 1997.

[4] K. Ambos-Spies, H.-C. Neis, and S. A. Terwijn. Genericity and measure for exponential time. *Theoretical Computer Science*, 168:3–19, 1996.

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

[6] S. Arora, C. Lund, R. Motwani, M. Sudan, and M. Szegedy. Proof verification and the hardness of approximation problems. *Journal of the ACM*, 45:501–555, 1998.

[7] V. Arvind, Y. Han, L. Hemachandra, J. Köbler, A. Lozano, M. Mundhenk, A. Ogiwara, U. Schöning, R. Silvestri, and T. Thierauf. Reductions to sets of low information content. In K. Ambos-Spies, S. Homer, and U. Schöning, editors, *Recent Developments in Complexity Theory*. Cambridge University Press, 1993.

[8] V. Arvind and J. Köbler. On pseudorandomness and resource-bounded measure. In *Proceedings 17th Conference on the Foundations of Software Technology and Theoretical Computer Science*, pages 235–249. Springer-Verlag, 1997.

[9] V. Arvind, J. Köbler, and M. Mundhenk. Hausdorff reductions to sparse sets and to sets of high information content. In *Symposium on Mathematical Foundations of Computer Science*, 1993.

[10] V. Arvind, J. Köbler, and M. Mundhenk. On reductions to sets that avoid EXPSPACE. *Information Processing Letters*, 56, 1995.

[11] J. L. Balcázar and U. Schöning. Bi-immune sets for complexity classes. *Mathematical Systems Theory*, 18:1–10, 1985.

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

[13] C. H. Bennett. Logical depth and physical complexity. In R. Herken, editor, *The Universal Turing Machine: A Half-Century Survey*, pages 227–257. Oxford University Press, London, 1988.

[14] C. H. Bennett and J. Gill. Relative to a random oracle $A$, $\mathrm{P}^A \neq \mathrm{NP}^A \neq \text{co-NP}^A$ with probability 1. *SIAM Journal on Computing*, 10:96–113, 1981.

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

[16] R. V. Book and J. H. Lutz. On languages with very high space-bounded Kolmogorov complexity. *SIAM Journal on Computing*, 22:395–402, 1993.

[17] R. V. Book, J. H. Lutz, and David M. Martin Jr. The global power of additional queries to random oracles. *Information and Computation*, 120:49–54, 1995.

[18] J. M. Breutzmann and J. H. Lutz. Equivalence of measures of complexity classes. *SIAM Journal on Computing.* To appear. See also *Proceedings of the 14th Symposium on Theoretical Aspects of Computer Science*, Springer-Verlag, 1997, pp. 535–545.

[19] H. Buhrman, S. Fenner, and L. Fortnow. Results on resource-bounded measure. In *In Proceedings of the 24th International Colloquium on Automata, Languages and Programming*, pages 188–194. Springer-Verlag, 1997.

[20] H. Buhrman, L. Fortnow, and T. Thierauf. Nonrelativizing separations. In *In Proceedings of the 13th IEEE Conference on Computational Complexity*, pages 8–12. IEEE, 1998.

[21] H. Buhrman, L. Fortnow, D. van Melkebeek, and L. Torenvliet. Using autoreducibility to separate complexity classes. *SIAM Journal on Computing*, 1999. To appear.

[22] H. Buhrman and L. Torenvliet. Complete sets and structure in subrecursive classes. In *Proceedings of Logic Colloquium '96*, pages 45–78. Springer-Verlag, 1998.

[23] H. Buhrman and D. van Melkebeek. Hard sets are hard to find. In *Proceedings of the 13th IEEE Conference on Computational Complexity*, pages 170–181, New York, 1998. IEEE.

[24] H. Buhrman, D. van Melkebeek, K. Regan, D. Sivakumar, and M. Strauss. A generalization of resource-bounded measure, with an application. In *Proceedings of the 15th Annual Symposium on Theoretical Aspects of Computer Science*, pages 161–171, Berlin, 1998. Springer-Verlag.

[25] J. Cai and A. Selman. Fine separation of average time complexity classes. *SIAM Journal on Computing*, 28:1310–1325, 1999.

[26] J. Cai, D. Sivakumar, and M. J. Strauss. Constant-depth circuits and the Lutz hypothesis In *Proceedings of the 38th IEEE Symposium on Foundations of Computer Science*, pages 595–604, 1997.

[27] R. Chang, B. Chor, O. Goldreich, J. Hartmanis, J. Hastad, D. Ranjan, and R. Rohatgi. The random oracle hypothesis is false. *Journal of Computer and System Sciences*, 49, 1994.

[28] A. Church. On the concept of a random sequence. *Bulletin of the American Mathematical Society*, 46:130–135, 1940.

[29] A. Clementi, J. Rolim, and L. Trevisan. Recent advances towards proving P = BPP. *Bulletin of the EATCS*, 64:96–103, 1998.

[30] J. Dai and J. Lutz. Query order and NP-completeness. In *Proceedings of the 14th IEEE Conference on Computational Complexity*, pages 142–148, 1999.

[31] R. I. Freidzon. Families of recursive predicates of measure zero. translated in *Journal of Soviet Mathematics*, 6(1976):449–455, 1972.

[32] B. Fu. With quasi-linear queries, EXP is not polynomial time Turing reducible to sparse sets. *SIAM Journal on Computing*, 24:1082–1090, 1995.

[33] R. W. Hamming. Mathematics on a distant planet. *American Mathematical Monthly*, 105:640–650, 1998.

[34] J. Hartmanis and R. E. Stearns. On the computational complexity of algorithms. *Transactions of the American Mathematical Society*, 117:285–306, 1965.

[35] J. Hartmanis and Y. Yesha. Computation times of NP sets of different densities. *Theoretical Computer Science*, 34:17–32, 1984.

[36] H. Heller. On relativized exponential and probabilistic complexity classes. *Information and Control*, 71:231–243, 1986.

[37] D. T. Huynh. Some observations about the randomness of hard problems. *SIAM Journal on Computing*, 15:1101–1105, 1986.

[38] R. Impagliazzo and A. Wigderson. P = BPP if E requires exponential circuits: Derandomizing the XOR lemma. In *Proceedings of the 29th Symposium on Theory of Computing*, pages 220–229, 1997.

[39] R. Impagliazzo and A. Wigderson. Randomness vs. time: derandomization under a uniform assumption. In *Proceedings of the 39th IEEE Symposium on Foundations of Computer Science*, 1998.

[40] D. W. Juedes. Weakly complete problems are not rare. *Computational Complexity*, 5:267–283, 1995.

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

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

[43] D. W. Juedes and J. H. Lutz. Completeness and weak completeness under polynomial-size circuits. *Information and Computation*, 125:13–31, 1996.

[44] R. Kannan. Circuit-size lower bounds and non-reducibility to sparse sets. *Information and Control*, 55:40–56, 1982.

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

[46] A. Klivans and D. van Melkebeek. Graph nonisomorphism has subexponential size proofs unless the polynomial-time hierarchy collapses. In *In Proceedings of 31st ACM Symposium on Theory of Computing*, pages 659–667, 1999.

[47] J. Köbler and W. Lindner. On the resource bounded measure of P/poly. In *Proceedings 13th IEEE Conference on Computational Complexity*, pages 132–140, 1998.

[48] J. Köbler, U. Schöning, and J. Torán. *The Graph Isomorphism Problem: Its Structural Complexity*. Birkhäuser, 1993.

[49] R. Ladner. On the structure of polynomial-time reducibility. *Journal of the ACM*, 22:155–171, 1975.

[50] W. Lindner. On the polynomial time bounded measure of one-truth-table degrees and p-selectivity, 1993. Diplomarbeit, Technische Universität Berlin.

[51] J. Lutz. A small span theorem for P/Poly-Turing reductions. In *Proceedings of the Tenth IEEE Structure in Complexity Theory Conference*, pages 324–330. IEEE Computer Society Press, 1995.

[52] J. Lutz. Resource-bounded measure. In *Proceedings of the Thirteen Annual IEEE Conference on Computational Complexity*, pages 236–248. IEEE Computer Society Press, 1998.

[53] J. Lutz and Y. Zhao. The density of weakly complete problems under adaptive reductions. *SIAM Journal on Computing*. To appear.

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

[55] J. H. Lutz. An upward measure separation theorem. *Theoretical Computer Science*, 81:127–135, 1991.

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

[57] J. H. Lutz. A pseudorandom oracle characterization of BPP. *SIAM Journal on Computing*, 22:1075–1086, 1993.

[58] J. H. Lutz. Weakly hard problems. *SIAM Journal on Computing*, 24:1170–1189, 1995.

[59] J. H. Lutz. Observations on measure and lowness for $\Delta_2^{\mathrm{P}}$. *Theory of Computing Systems*, 30:429–442, 1997.

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

[61] J. H. Lutz. Resource-bounded measure. In *Proceedings of the 13th IEEE Conference on Computational Complexity*, pages 236–248, New York, 1998. IEEE.

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

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

[64] P. Martin-Löf. The definition of random sequences. *Information and Control*, 9:602–619, 1966.

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

[66] E. Mayordomo. *Contributions to the study of resource-bounded measure*. PhD thesis, Universitat Politècnica de Catalunya, 1994.

[67] A. R. Meyer, 1977. reported in [15].

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

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

[70] A. Pavan and A. Selman. Complete distributional problems, hard languages, and resource-bounded measure. *Theoretical Computer Science*. To appear.

[71] A. Razborov and S. Rudich. Natural proofs. In *Proceedings of the* $26^{th}$ *ACM Symposium on Theory of Computing*, pages 204–214, 1994.

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

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

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

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

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

[77] U. Schöning. Complete sets and closeness to complexity classes. *Mathematical Systems Theory*, 19:29–41, 1986.

[78] A. Selman. Personal communication, reported in [62].

[79] C. E. Shannon. The synthesis of two-terminal switching circuits. *Bell System Technical Journal*, 28:59–98, 1949.

[80] L. Stockmeyer. On approximation algorithms for #P. *SIAM Journal on Computing*, 14:849–861, 1985.

[81] L. Stockmeyer and A. K. Chandra. Provably difficult combinatorial games. *SIAM Journal on Computing*, 8:151–174, 1979.

[82] S. Terwijn. *Computability and Measure*. PhD thesis, University of Amsterdam, 1998.

[83] D. van Melkebeek. On the measure of BPP. Technical Report TR-98-07, Department of Computer Science, University of Chicago, June 1998.

[84] J. Ville. Étude critique de la notion de collectif, 1939.

[85] R. von Mises. Grundlagen der Wahrscheinlichkeitsrechnung. *Mathematische Zeitschrift*, 5:52–99, 1919.

[86] A. Wald. Die Widerspruchsfreiheit des Kollectivbegriffs in der Wahrscheinlichkeitsrechnung. *Ergebnisse eines Mathematichen Kolloquiums*, 8:38–72, 1938.

[87] O. Watanabe. Polynomial time reducibility to a set of small density. In *Proceedings of the Second Structure in Complexity Theory Conference*, pages 138–146, 1987.

[88] C. B. Wilson. Relativized circuit complexity. *Journal of Computer and System Sciences*, 31:169–181, 1985.