Electronic Colloquium on Computational Complexity, Report No. 63 (2003)

The Size of SPP

John M. Hitchcock[*]
Department of Computer Science
University of Wyoming
Laramie, WY 82071   U.S.A.
jhitchco@cs.uwyo.edu

Abstract

Derandomization techniques are used to show that at least one of the following holds regarding the size of the counting complexity class SPP.

1. $\mu_{\mathrm{p}}(\mathrm{SPP}) = 0$.
2. $\mathrm{PH} \subseteq \mathrm{SPP}$.

In other words, SPP is small by being a negligible subset of exponential time or large by containing the entire polynomial-time hierarchy. This addresses an open problem about the complexity of the graph isomorphism problem: it is not weakly complete for exponential time unless PH is contained in SPP. It is also shown that the polynomial-time hierarchy is contained in $\mathrm{SPP}^{\mathrm{NP}}$ if NP does not have p-measure 0.

1 Introduction

Resource-bounded measure [21] provides a notion of relative size for complexity classes. The p-measure of a complexity class $\mathcal{C}$ is denoted by $\mu_{\mathrm{p}}(\mathcal{C})$. Since $\mu_{\mathrm{p}}(\mathrm{P}) = 0$ and $\mu_{\mathrm{p}}(\mathrm{EXP}) \neq 0$, it is interesting to investigate the p-measure of classes between P and EXP. Determining the p-measure of a class implies a separation from P or from EXP, so this is difficult to achieve for most classes. Instead, the largeness assertion $\mu_{\mathrm{p}}(\mathcal{C}) \neq 0$ is often investigated for its consequences. If $\mu_{\mathrm{p}}(\mathcal{C}) \neq 0$, then $\mathcal{C}$ is intuitively a large subclass of exponential time, but it is not immediately clear what this means in terms of $\mathcal{C}$'s relationship to other complexity classes.

Because of advances in derandomization, the p-measure of the probabilistic complexity classes ZPP, RP, and BPP is very well understood. Impagliazzo and Wigderson's derandomization of BPP under the assumption $\mathrm{BPP} \neq \mathrm{EXP}$ [15] was used by van Melkebeek [35] to show that BPP has p-measure 0 unless it is equal to EXP. A corollary in [35] implies that this statement also holds with BPP replaced by ZPP. Impagliazzo and Moser [13] have recently shown that the same holds for RP.

Theorem 1.1. ([35, 13]) *For each* $\mathcal{C} \in \{\mathrm{ZPP}, \mathrm{RP}, \mathrm{BPP}\}$, $\mu_{\mathrm{p}}(\mathcal{C}) \neq 0$ *implies* $\mathcal{C} = \mathrm{EXP}$.

In other words, if one of these probabilistic classes does not have p-measure 0, then it contains all of exponential time and truly is large.

A similar phenomenon also occurs for the counting complexity classes PP and $\oplus\mathrm{P}$. Toda [32] proved that $\mathrm{PH} \subseteq \mathrm{BP} \cdot \oplus\mathrm{P}$, that is, $\oplus\mathrm{P}$ is hard for the polynomial-time hierarchy under randomized reductions.

[*] This research was performed while the author was a postdoc at the University of Nebraska-Lincoln in summer 2003.

ISSN 1433-8092

Subsequently, Toda and Ogiwara [33] showed that $\mathrm{PH} \subseteq \mathrm{BP} \cdot \mathrm{PP}$. Arvind and Köbler [4] extended the results of Nisan and Wigderson [30], Allender and Strauss [1], and Lutz [22] to show that $\mu_{\mathrm{p}}(\mathcal{C}) \neq 0$ implies $\mathcal{C} = \mathrm{BP} \cdot \mathcal{C}$ for any class $\mathcal{C} \subseteq \mathrm{EXP}$ that is closed under join and polynomial-time truth table reductions. Combining these results yields an analogue of Theorem 1.1 for $\oplus\mathrm{P}$ and PP.

Theorem 1.2. ([4]) *For each* $\mathcal{C} \in \{\oplus\mathrm{P}, \mathrm{PP}\}$, $\mu_{\mathrm{p}}(\mathcal{C}) \neq 0$ *implies* $\mathrm{PH} \subseteq \mathcal{C}$.

If one of these counting classes does not have p-measure 0, then it contains the polynomial-time hierarchy and is large in a traditional complexity theoretic sense.

The class SPP, introduced by Fenner, Fortnow, and Kurtz [8], is the smallest reasonable counting complexity class. In particular, it is low for all "gap-definable" classes, including PP and $\oplus\mathrm{P}$. It is not known if $\mathrm{PH} \subseteq \mathrm{BP} \cdot \mathrm{SPP}$. In fact, Toda and Ogiwara [33] conjectured that this is not the case. Nevertheless, we show that Theorem 1.2 also holds for SPP. To prove this we extend via relativization the results of Klivans and van Melkebeek [20] that involve a conditional derandomization of the Valiant-Vazirani theorem [34].

Theorem 1.3. $\mu_{\mathrm{p}}(\mathrm{SPP}) \neq 0$ *implies* $\mathrm{PH} \subseteq \mathrm{SPP}$.

Arvind and Kurur [5] recently showed that SPP contains the graph isomorphism problem. Using this, Theorem 1.3 yields a sufficient condition for a conjecture of Lutz and Mayordomo [26] to hold. If the polynomial-time hierarchy is not contained in SPP, then the graph isomorphism problem is not weakly complete for exponential time.

The hypothesis on the p-measure of SPP in Theorem 1.3 has not been previously investigated. The "NP is not small" hypothesis, $\mu_{\mathrm{p}}(\mathrm{NP}) \neq 0$, has been extensively investigated and shown to have many plausible consequences [1, 2, 4, 6, 7, 12, 13, 16, 22, 24, 25, 27, 28, 29, 31, 38]. The techniques for proving Theorem 1.3 also yield that $\mathrm{PH} \subseteq \mathrm{SPP}^{\mathrm{NP}}$ if $\mu_{\mathrm{p}}(\mathrm{NP}) \neq 0$. It is therefore likely that SPP algorithms, despite their restrictive nature, are powerful enough to solve the entire polynomial-time hierarchy when given access to an NP oracle.

2 Preliminaries

We now define the counting complexity classes used in this paper. Let A be an oracle.

1. The class $\#\mathrm{P}^A$ consists of all functions $f : \{0,1\}^* \to \mathbb{N}$ for which there is a nondeterministic polynomial-time oracle machine M such that for all $x \in \{0,1\}^*$, $f(x)$ is the number of accepting paths of M^A on input x.

2. The class GapP^A consists of all functions $f : \{0,1\}^* \to \mathbb{Z}$ that are of the form $f = g - h$ for some $g, h \in \#\mathrm{P}^A$.

3. The class SPP^A consists all languages whose characteristic function is a GapP^A function.

As is usual, when $A = \emptyset$, we omit it from the notation.

We will use the following basic properties of SPP.

Theorem 2.1. (Fenner, Fortnow, and Kurtz [8]) SPP *is low for all gap-definable counting classes. In particular,* $\mathrm{SPP}^{\mathrm{SPP}} = \mathrm{SPP}$ *and* SPP *is closed under* $\leq_{\mathrm{T}}^{\mathrm{P}}$*-reductions.*

We will use relativized versions of the satisfiability problem as complete languages for the polynomial-time hierarchy [11, 9]. Let A be an oracle. An *A-relativized 3CNF formula* is a CNF formula where each clause is of the form

$$x_{i1} \vee x_{i2} \vee x_{i3} \vee A(x_{j1} \cdots x_{jn}),$$

where $A(x_{j1} \cdots x_{jn})$ evaluates to true if the string $x_{j1} \cdots x_{jn}$ is in A. Any of the variables or the $A(\cdot)$ term may be negated. A formula is *satisfiable* if there exists an assignment under which it evaluates to true. We write SAT^A for the class of all satisfiable A-relativized propositional formulas. We define $\mathrm{SAT}_0 = \emptyset$ and $\mathrm{SAT}_{k+1} = \mathrm{SAT}^{\mathrm{SAT}_k}$ for all $k \geq 0$.

Lemma 2.2. (Goldsmith and Joseph [11]) *For all A, SAT^A is $\leq_{\mathrm{m}}^{\mathrm{p}}$-complete for NP^A. In particular, SAT_k is $\leq_{\mathrm{m}}^{\mathrm{p}}$-complete for Σ_k^{P} for all $k \geq 0$.*

3 Circuit Complexity and Resource-Bounded Measure

We now recall the basics of resource-bounded measure. For more details, we refer to the survey papers [21, 23, 3].

1. A *martingale* is a function $d : \{0,1\}^* \rightarrow [0,\infty)$ satisfying the averaging condition $2d(w) = d(w0) + d(w1)$ for all $w \in \{0,1\}^*$.

2. The *success set* of a martingale d is the class $S^\infty[d]$ of all infinite binary sequences S for which the sequence of values $d(S \upharpoonright n)$ is unbounded, where $S \upharpoonright n$ is the length n prefix of S.

3. A class X of infinite binary sequences has *p-measure 0,* denoted by $\mu_{\mathrm{p}}(X) = 0$, if there is a polynomial-time computable martingale d with $X \subseteq S^\infty[d]$.

In resource-bounded measure it is standard to identify a decision problem with its infinite binary characteristic sequence, where the strings are listed in standard lexicographic order. In this way, complexity classes are viewed as sets of infinite binary sequences.

For a Boolean function $f : \{0,1\}^* \rightarrow \{0,1\}$ and an oracle B, the *circuit complexity $C_f^B(n)$ of f at length n relative to B* is the size of the smallest B-oracle circuit that correctly computes f on all strings of length n. The *hardness $H_f^B(n)$ of f at length n relative B* is the largest integer t such that for any oracle circuit D of size at most t with n inputs,

$$\left| \Pr_x[D^B(x) = f(x)] - \frac{1}{2} \right| < \frac{1}{t},$$

where x is uniformly distributed over $\{0,1\}^n$.

The following theorem was used in conjunction with the pseudorandom generators of Nisan and Wigderson [30] to prove relationships between resource-bounded measure and derandomization.

Theorem 3.1. (Allender and Strauss [1], Lutz [22]) *For every $B \in \mathrm{E}$ and $\alpha < \frac{1}{3}$,*

$$\mu_{\mathrm{p}}\left(\left\{ A \,\middle|\, (\forall f \in \mathrm{E}^A)\; H_f^{A \oplus B}(n) \leq 2^{\alpha n} \text{ i.o.} \right\}\right) = 0.$$

Because of advances in hardness amplification for derandomization [14, 20], the full strength of Theorem 3.1 is not needed in this paper. We will only use the following consequence of it.

Corollary 3.2. *Let $\mathcal{C}$ be a class of languages and assume that $\mu_{\mathrm{p}}(\mathcal{C}) \neq 0$. Then for every $B \in \mathrm{E}$, there is a function $f \in \mathrm{E}^{\mathcal{C}}$ such that $C_f^B(n) = 2^{\Omega(n)}$.*

Proof. Assume that $\mathcal{C}$ does not have p-measure 0 and let $B \in \mathrm{E}$. Then for $\alpha = \frac{1}{4}$, $\mathcal{C}$ is not contained in the set that has p-measure 0 in Theorem 3.1. This means that there is some $A \in \mathcal{C}$ such that some boolean function $f \in \mathrm{E}^A$ satisfies $H_f^{A \oplus B}(n) > 2^{\frac{1}{4}n}$ almost everywhere. This f certainly has the weaker property $C_f^B(n) = 2^{\Omega(n)}$. □

4 Derandomization and SPP

In this section we verify that the following relativization of a theorem of Klivans and van Melkebeek [20] holds.

Theorem 4.1. *Let A be an oracle and let $k \geq 1$. If there is a Boolean function $f \in \mathrm{E}^A$ such that $C_f^{\mathrm{SAT}_k}(n) = 2^{\Omega(n)}$, then $\Sigma_k^{\mathrm{P}} \subseteq \mathrm{SPP}^A$.*

Using $A = \emptyset$ in Theorem 4.1 gives a hypothesis that implies the polynomial-time hierarchy is contained in SPP. By weakening this hypothesis to allow $A \in \mathrm{SPP}$, we obtain a necessary and sufficient condition.

Theorem 4.2. *The following are equivalent.*

(1) *For every $k \geq 1$, there is a Boolean function $f \in \mathrm{E}^{\mathrm{SPP}}$ such that $C_f^{\mathrm{SAT}_k}(n) = 2^{\Omega(n)}$.*

(2) $\mathrm{PH} \subseteq \mathrm{SPP}$.

Proof. That (1) implies (2) follows immediately from Theorems 4.1 and 2.1.

If (2) holds, then the exponential hierarchy $\mathrm{EH} = \mathrm{E}^{\mathrm{PH}}$ is contained in $\mathrm{E}^{\mathrm{SPP}}$. Relativizing a result of Kannan [18] shows that for every k, there are functions in EH with maximal SAT_k-oracle circuit complexity. Therefore (1) follows. □

To prove the unrelativized version of Theorem 4.1, Klivans and van Melkebeek gave a derandomization of the Valiant-Vazirani theorem [34] under the assumption that there is a function $f \in \mathrm{E}$ with $C_f^{\mathrm{SAT}}(n) = 2^{\Omega(n)}$. The following relativized version of their derandomization holds.

Theorem 4.3. *Let A and B be any two oracles. Assume that there is a Boolean function $f \in \mathrm{E}^A$ such that $C_f^{\mathrm{SAT}^B}(n) = 2^{\Omega(n)}$. Then there is a function computable in polynomial time relative to A that maps any relativized propositional formula ϕ_B into a list of relativized propositional formulas $\phi_B^{(1)}, \ldots, \phi_B^{(k)}$ (where k is polynomial in $|\phi_B|$) such that the following hold.*

- *For all i, every satisfying assignment of $\phi_B^{(i)}$ also satisfies ϕ_B.*
- *If ϕ_B is satisfiable, then for some i, $\phi_B^{(i)}$ is uniquely satisfiable.*

Klivans and van Melkebeek used their conditional derandomization of the Valiant-Vazirani theorem to make a connection with SPP under the same hypothesis. We obtain the following relativization in the same way.

Corollary 4.4. *Let A and B be any two oracles. If there is a Boolean function $f \in \mathrm{E}^A$ such that $C_f^{\mathrm{SAT}^B}(n) = 2^{\Omega(n)}$, then $\mathrm{SAT}^B \in \mathrm{SPP}^{A \oplus B}$.*

Proof. For each relativized formula ϕ_B and i, let $h(\phi_B, i)$ be the number of satisfying assignments to the relativized formula $\phi_B^{(i)}$ from Theorem 4.3. Then the function

$$g(\phi_B) = 1 - \prod_{i=1}^{k}(1 - h(\phi_B, i))$$

is the characteristic function of SAT^B. Since $h \in \#\mathrm{P}^{A \oplus B}$, we have $g \in \mathrm{GapP}^{A \oplus B}$ by relativizing the closure properties of GapP [8], so $\mathrm{SAT}^B \in \mathrm{SPP}^{A \oplus B}$. □

A key lemma of Toda and Ogiwara [33] was also conditionally derandomized by Klivans and van Melkebeek. We will use the following relativized extension.

Lemma 4.5. *Let A and B be any two oracles and assume there is a Boolean function $f \in \mathrm{E}^A$ such that $C_f^{\mathrm{SAT}^B}(n) = 2^{\Omega(n)}$, Then $\mathrm{GapP}^{A \oplus \mathrm{NP}^B}$ is contained in $\mathrm{GapP}^{A \oplus B}$. In particular, $\mathrm{SPP}^{A \oplus \mathrm{NP}^B}$ is contained in $\mathrm{SPP}^{A \oplus B}$.*

Corollary 4.6. *Let A be any oracle and let $k \geq 1$. If there is a function $f \in \mathrm{E}^A$ such that $C_f^{\mathrm{SAT}_k}(n) = 2^{\Omega(n)}$, then $\mathrm{SPP}^{A \oplus \Sigma_k^{\mathrm{P}}}$ is contained in SPP^A.*

Proof. This follows from k applications of Lemma 4.5 since $C_f^{\mathrm{SAT}_k}(n) = 2^{\Omega(n)}$ implies $C_f^{\mathrm{SAT}^{\mathrm{SAT}_i}}(n) = 2^{\Omega(n)}$ for all $i < k$. □

Theorem 4.1 now follows.

Proof of Theorem 4.1. Let f satisfy the hypothesis. Then $C_f^{\mathrm{SAT}_k}(n) = C_f^{\mathrm{SAT}^{\mathrm{SAT}_{k-1}}}(n) = 2^{\Omega(n)}$, so Corollaries 4.4 and 4.6 tell us that $\mathrm{SAT}_k \in \mathrm{SPP}^{A \oplus \mathrm{SAT}_{k-1}} \subseteq \mathrm{SPP}^A$. □

5 Resource-Bounded Measure and SPP

We can now establish that SPP is small in polynomial-time measure or is large enough to contain the entire polynomial-time hierarchy.

Theorem 5.1. *If $\mu_{\mathrm{p}}(\mathrm{SPP}) \neq 0$, then $\mathrm{PH} \subseteq \mathrm{SPP}$.*

Proof. The hypothesis together with Corollary 3.2 implies that condition (1) of Theorem 4.2 holds. □

Given the restrictive nature of the definition of SPP and the difficulty with which problems have been placed in SPP [36, 37, 5], the consequence $\mathrm{PH} \subseteq \mathrm{SPP}$ of Theorem 5.1 is quite striking. However, it is not clear if the hypothesis that $\mu_{\mathrm{p}}(\mathrm{SPP}) \neq 0$ is reasonable. If we assume the "NP is not small" hypothesis, then SPP algorithms with access to an NP oracle are powerful enough to solve the entire polynomial-time hierarchy, even if SPP has p-measure 0.

Theorem 5.2. *If $\mu_{\mathrm{p}}(\mathrm{NP}) \neq 0$, then $\mathrm{PH} \subseteq \mathrm{SPP}^{\mathrm{NP}}$.*

Proof. This follows from Corollary 3.2 and Theorem 4.1. □

Since SPP is closed under $\leq_{\mathrm{T}}^{\mathrm{p}}$-reductions (Theorem 2.1), we know that $\mathrm{NP} \subseteq \mathrm{SPP}$ if and only if $\Delta_2^{\mathrm{P}} \subseteq \mathrm{SPP}$. This upward collapse is strengthened to the entire polynomial-time hierarchy if we assume that NP does not have p-measure 0.

Corollary 5.3. *Assume* $\mu_{\mathrm{p}}(\mathrm{NP}) \neq 0$. *Then* $\mathrm{NP} \subseteq \mathrm{SPP}$ *if and only if* $\mathrm{PH} \subseteq \mathrm{SPP}$.

Proof. This is immediate from Theorems 5.2 and 2.1. □

Let $\leq_r^{\mathrm{p}}$ be a polynomial-time reducibility and let $\mathcal{C} \in \{\mathrm{E}, \mathrm{EXP}\}$. A language $A \in \mathcal{C}$ is *weakly* $\leq_r^{\mathrm{p}}$-*complete for* $\mathcal{C}$ if the class of all problems in $\mathcal{C}$ that are $\leq_r^{\mathrm{p}}$-reducible to A does not have measure 0 in $\mathcal{C}$. (For more details, see [17].) Lutz and Mayordomo [26] conjectured that GI, the graph isomorphism problem, is not weakly $\leq_{\mathrm{m}}^{\mathrm{p}}$-complete for EXP. Recently it has been shown that SPP contains GI.

Theorem 5.4. (Arvind and Kurur [5]) $\mathrm{GI} \in \mathrm{SPP}$.

Theorems 5.4 and 5.1 together yield a condition that implies the conjecture of Lutz and Mayordomo, even for $\leq_{\mathrm{T}}^{\mathrm{p}}$-reductions.

Corollary 5.5. *If* $\mathrm{PH} \not\subseteq \mathrm{SPP}$, *then* GI *is not weakly* $\leq_{\mathrm{T}}^{\mathrm{p}}$-*complete for* E *or for* EXP.

Proof. By Theorem 5.1, the hypothesis implies that SPP has p-measure 0. From Theorems 2.1 and 5.4 we know that the class of problems that are $\leq_{\mathrm{T}}^{\mathrm{p}}$-reducible to GI is contained in SPP, so it has p-measure 0 and therefore measure 0 in E and in EXP. □

6 Conclusion

As discussed by Fortnow [10], it is difficult to assess the power of SPP. Theorem 5.1 says that the class must be negligible within exponential time or larger than the polynomial-time hierarchy. More specifically, at least one of the following holds.

(1) $\mu_{\mathrm{p}}(\mathrm{SPP}) = 0$.

(2) $\mathrm{PH} \subseteq \mathrm{SPP}$.

It is possible that both conditions hold; ruling this out would imply $\mathrm{P} \neq \mathrm{PP}$. If $\mathrm{P} = \mathrm{PP}$, then $\mathrm{P} = \mathrm{PH} = \mathrm{SPP}$ follows from Toda's Theorem [32] and the fact that SPP is contained in PP, so both (1) and (2) hold.

The proof of Theorem 5.1 relativizes, so there is no oracle relative to which (1) and (2) both fail. On the other hand, relative to a random oracle R, we have $\mu_{\mathrm{p}^R}(\mathrm{NP}^R) \neq 0$ [19] and $\mathrm{PH}^R \subseteq \mathrm{SPP}^R$ [8]. Therefore (2) holds and (1) fails relative to random R. There is also an oracle A where $\mathrm{P}^A = \mathrm{SPP}^A$ and PH^A has infinitely many levels [10]. Relative to A, (1) holds and (2) fails.

It would be interesting to see conditions (1) and (2) and their negations related to other questions in complexity theory. In particular, what else follows if SPP does not have p-measure 0?

Acknowledgments. I thank N. V. Vinodchandran and Jack Lutz for helpful discussions.

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, 1994.

[2] K. Ambos-Spies and L. Bentzien. Separating NP-completeness notions under strong hypotheses. *Journal of Computer and System Sciences*, 61(3):335–361, 2000.

[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] V. Arvind and J. Köbler. On pseudorandomness and resource-bounded measure. *Theoretical Computer Science*, 255(1–2):205–221, 2001.

[5] V. Arvind and P. P. Kurur. Graph isomorphism is in SPP. In *Proceedings of the 43rd Symposium on Foundations of Computer Science*, pages 743–750, 2002.

[6] J. Cai and A. Selman. Fine separation of average time complexity classes. *SIAM Journal on Computing*, 28(4):1310–1325, 1999.

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

[8] S. A. Fenner, L. Fortnow, and S. A. Kurtz. Gap-definable counting classes. *Journal of Computer and System Sciences*, 48(1):116–148, 1994.

[9] L. Fortnow. The role of relativization in complexity theory. *Bulletin of the European Association for Theoretical Computer Science*, 52:229–244, February 1994.

[10] L. Fortnow. Counting complexity. In L. A. Hemaspaandra and A. L. Selman, editors, *Complexity Theory Retrospective II*, pages 81–107. Springer-Verlag, 1997.

[11] J. Goldsmith and D. Joseph. Three results on the polynomial isomorphism of complete sets. In *Proceedings of the 27th Symposium on Foundations of Computer Science*, pages 390–397, 1986.

[12] J. M. Hitchcock. MAX3SAT is exponentially hard to approximate if NP has positive dimension. *Theoretical Computer Science*, 289(1):861–869, 2002.

[13] R. Impagliazzo and P. Moser. A zero-one law for RP. In *Proceedings of the 18th IEEE Conference on Computational Complexity*, 2003. To appear.

[14] 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.

[15] R. Impagliazzo and A. Wigderson. Randomness vs. time: Derandomization under a uniform assumption. *Journal of Computer and System Sciences*, 63:672–688, 2001.

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

[17] D. W. Juedes and J. H. Lutz. Weak completeness in E and E_2. *Theoretical Computer Science*, 143(1):149–158, 1995.

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

[19] S. M. Kautz and P. B. Miltersen. Relative to a random oracle, NP is not small. *Journal of Computer and System Sciences*, 53(2):235–250, 1996.

[20] A. Klivans and D. van Melkebeek. Graph nonisomorphism has subexponential size proofs unless the polynomial-time hierarchy collapses. *SIAM Journal on Computing*, 31:1501–1526, 2002.

[21] J. H. Lutz. Almost everywhere high nonuniform complexity. *Journal of Computer and System Sciences*, 44(2):220–258, 1992.

[22] J. H. Lutz. Observations on measure and lowness for Δ_2^{P}. *Theory of Computing Systems*, 30(4):429–442, 1997.

[23] 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.

[24] J. H. Lutz and E. Mayordomo. Measure, stochasticity, and the density of hard languages. *SIAM Journal on Computing*, 23(4):762–779, 1994.

[25] J. H. Lutz and E. Mayordomo. Cook versus Karp-Levin: Separating completeness notions if NP is not small. *Theoretical Computer Science*, 164(1–2):141–163, 1996.

[26] J. H. Lutz and E. Mayordomo. Twelve problems in resource-bounded measure. *Bulletin of the European Association for Theoretical Computer Science*, 68:64–80, 1999.

[27] J. H. Lutz, V. Mhetre, and S. Srinivasan. Hard instances of hard problems. In *Proceedings of the 17th Annual Symposium on Theoretical Aspects of Computer Science*, pages 324–333, 2000.

[28] J. H. Lutz and Y. Zhao. The density of weakly complete problems under adaptive reductions. *SIAM Journal on Computing*, 30(4):1197–1210, 2000.

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

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

[31] A. Pavan and A. Selman. Complete distributional problems, hard languages, and resource bounded measure. *Theoretical Computer Science*, 234:273–286, 2000.

[32] S. Toda. On the computational power of PP and $\oplus$P. *SIAM Journal on Computing*, 20(5):865–877, 1991.

[33] S. Toda and M. Ogiwara. Counting classes are at least as hard as the polynomial-time hierarchy. *SIAM Journal on Computing*, 21(2):316–328, 1992.

[34] L. Valiant and V. Vazirani. NP is as easy as detecting unique solutions. *Theoretical Computer Science*, 47(3):85–93, 1986.

[35] D. van Melkebeek. The zero-one law holds for BPP. *Theoretical Computer Science*, 244(1–2):283–288, 2000.

[36] N. V. Vinodchandran. Improved lowness results for solvable black-box group problems. In *Proceedings of the 17th Conference on Foundations of Software Technology and Theoretical Computer Science*, pages 220–234, 1997.

[37] N. V. Vinodchandran. *Counting Complexity and Computational Group theory*. PhD thesis, Institute of Mathematical Sciences, Chennai, India, 1998.

[38] Y. Wang. NP-hard sets are superterse unless NP is small. *Information Processing Letters*, 61(1):1–6, 1997.

ECCC ISSN 1433-8092
http://www.eccc.uni-trier.de/eccc
ftp://ftp.eccc.uni-trier.de/pub/eccc
ftpmail@ftp.eccc.uni-trier.de, subject 'help eccc'