

Restrictive Acceptance Suffices for Equivalence Problems¹

Bernd Borchert²
Mathematisches Institut
Universität Heidelberg
69120 Heidelberg, Germany

Lane A. Hemaspaandra³
Department of Computer Science
University of Rochester
Rochester, NY 14627, USA

Jörg Rothe⁴
Institut für Informatik
Friedrich-Schiller-Universität Jena
07740 Jena, Germany

¹Revises Friedrich-Schiller-Universität Jena Technical Report Math/Inf/96/13.

²Email: bb@math.uni-heidelberg.de.

³Email: lane@cs.rochester.edu. Supported in part by grants NSF-CCR-9322513, NSF-INT-9513368/DAAD-315-PRO-fo-ab, and NSF-INT-9815095/DAAD-315-PPP-gü-ab. Work done in part while visiting Friedrich-Schiller-Universität Jena.

⁴Email: rothe@informatik.uni-jena.de. Supported in part by grants NSF-INT-9513368/DAAD-315-PRO-fo-ab and NSF-INT-9815095/DAAD-315-PPP-gü-ab, and a NATO Post-doctoral Science Fellowship from the Deutscher Akademischer Austauschdienst (“Gemeinsames Hochschulsonderprogramm III von Bund und Ländern”). Work done in part while visiting the University of Rochester and Le Moyne College.

Abstract

One way of suggesting that an NP problem may not be NP-complete is to show that it is in the class UP. We suggest an analogous new approach—weaker in strength of evidence but more broadly applicable—to suggesting that concrete NP problems are not NP-complete. In particular we introduce the class EP, the subclass of NP consisting of those languages accepted by NP machines that when they accept always have a number of accepting paths that is a power of two. Since if any NP-complete set is in EP then all NP sets are in EP, it follows—with whatever degree of strength one believes that EP differs from NP—that membership in EP can be viewed as evidence that a problem is not NP-complete.

We show that the negation equivalence problem for OBDDs (ordered binary decision diagrams [22, 13]) and the interchange equivalence problem for 2-dags are in EP. We also show that for boolean negation [25] the equivalence problem is in EP^{NP} , thus tightening the existing NP^{NP} upper bound. We show that FewP [2], bounded ambiguity polynomial time, is contained in EP, a result that is not known to follow from the previous SPP upper bound. For the three problems and classes just mentioned with regard to EP, no proof of membership/containment in UP is known, and for the problem just mentioned with regard to EP^{NP} , no proof of membership in UP^{NP} is known. Thus, EP is indeed a tool that gives evidence against NP-completeness in natural cases where UP cannot currently be applied.

1 Introduction

NP languages can be defined via machines that reject by having zero accepting paths, and that accept by having their number of accepting paths belong to the set $\{1, 2, 3, \dots\}$. A number of researchers have sought to refine the class NP by shrinking the path-cardinality set signifying acceptance, while retaining the requirement that rejection be associated with having zero accepting paths. We will call any such class a *restricted counting class*. The most common restricted counting classes in the literature are random polynomial time (usually denoted R or RP) and ambiguity-bounded classes such as UP and FewP. Ambiguity-bounded classes will be of central interest to us in the present paper.

Valiant's class UP (unambiguous polynomial time) [37], which is known to differ from P exactly if one-way functions exist [24], has the acceptance set $\{1\}$, and so is a restricted counting class. Acceptance sets of the forms $\{1, 2, 3, \dots, n^{\mathcal{O}(1)}\}$ and $\{1, 2\}, \{1, 2, 3\}, \dots$ define, respectively, the class FewP [2] and the classes $UP_{\leq 2}, UP_{\leq 3}, \dots$ [4], and thus these too are restricted counting classes. (Note: $UP \subseteq UP_{\leq 2} \subseteq UP_{\leq 3} \subseteq \dots \subseteq UP_{\mathcal{O}(1)} \subseteq FewP \subseteq NP$, where $UP_{\mathcal{O}(1)} = \bigcup_{k \geq 1} UP_{\leq k}$.) These classes are also connected to the existence of one-way functions and have been extensively studied in a wide variety of contexts, such as class containments [20, 30], complete sets [28], reducibilities [27], boolean hierarchy equivalences [29], complexity-theoretic analogs of Rice's Theorem [12], and upward separations [33].

Of course, the litmus test of NP refinements such as UP, $UP_{\leq k}$, and FewP is *the extent to which they allow us to refine the upper bounds on the complexity of natural NP problems*. Of these classes, UP has been most successful in this regard. UP is known to provide an upper bound on the complexity of (a language version of) the discrete logarithm problem [24], and UP (indeed $UP \cap coUP$) is known to provide an upper bound on the complexity of primality testing [19].

However, there are certain NP problems whose richness of structure has to date defied attempts to put them in UP or even FewP, yet that nonetheless intuitively seem to use less than the full generality of NP's acceptance mechanism. To try to categorize these problems, we introduce the class EP, which is intermediate between FewP and NP: $FewP \subseteq EP \subseteq NP$. In particular, EP is the NP subclass whose acceptance set is $\{2^i \mid i \in \mathbb{N}\}$, $\mathbb{N} = \{0, 1, 2, 3, \dots\}$.

In Section 2, we provide improved upper bounds on the complexity of the problems OBDD (Ordered Binary Decision Diagram) Negation Equivalence, 2-Dag Interchange Equivalence, and Boolean Negation Equivalence. These three problems are trivially in, respectively, NP, NP, and NP^{NP} . We provide, respectively, EP, EP, and EP^{NP} upper bounds. The problems are not known to belong to (and do not seem to obviously belong to), respectively, FewP, FewP, and $FewP^{NP}$.

In Section 3, we prove a general result regarding containment of FewP in certain restricted counting classes. In particular, we establish a sufficient condition for when restricted counting classes contain FewP. From our result it follows that EP contains FewP and, moreover, our result subsumes as special cases some previously known results from the literature.

In Section 4, we list some open questions related to our work.

2 Concrete Problems and EP

In this section, we provide concrete problems known to be in NP (or NP^{NP}), and we prove they are in fact in EP (or EP^{NP}). We now define the class EP (mnemonic: the number of accepting computation paths is restricted to being either 0 or some power (some exponentiation) of 2). For any nondeterministic polynomial-time Turing machine N and any string x , let $\#acc_N(x)$ denote the number of accepting computation paths of N on input x . Our alphabet Σ will be $\{0, 1\}$. For any string $x \in \Sigma^*$, let $|x|$ denote the length of x .

Definition 2.1 EP denotes the class of all languages L for which there is a nondeterministic polynomial-time Turing machine N such that, for each input $x \in \Sigma^*$,

$$\begin{aligned} x \notin L &\implies \#acc_N(x) = 0, \text{ and} \\ x \in L &\implies \#acc_N(x) \in \{2^i \mid i \in \mathbb{N}\}. \end{aligned}$$

Consider the following well-known problem.

Problem: Boolean Negation Equivalence (BNE) (see the survey by Harrison [25] and the bibliography provided after the references in the paper by Borchert, Ranjan, and Stephan [11])

Input: Two boolean functions (input as boolean formulas using variable names and the symbols $\{\wedge, \vee, \neg, (,)\}$), $f(x_1, \dots, x_n)$ and $g(x_1, \dots, x_n)$, over the same n boolean variables.

Question: Are f and g negation equivalent? That is, can one negate some of the inputs of g such that f and the modified function g' are equivalent?¹

For concreteness as a language problem, $\text{BNE} = \{(f, g) \mid f \text{ and } g \text{ are negation equivalent}\}$.

For example, the two boolean functions described by the formulas $x_1 \vee x_2 \vee x_3$ and $x_1 \vee \neg x_2 \vee \neg x_3$ are negation equivalent by negating x_2 and x_3 . Regarding lower bounds, Borchert, Ranjan, and Stephan [11] have shown that BNE is US-hard [9], and thus in particular is coNP -hard. Regarding upper bounds, $\text{BNE} \in \text{NP}^{\text{NP}}$ [11] and $\text{BNE} \in \text{coAM}^{\text{NP}}$ (combining [11] and [1]). It follows from the latter that BNE is not NP^{NP} -complete unless the polynomial hierarchy collapses ([1], in light of [11, 34]). Interestingly, neither of these two upper bounds— NP^{NP} and coAM^{NP} —is known to imply the other.

We now prove $\text{BNE} \in \text{EP}^{\text{NP}}$, which is neither known to imply nor known to be implied by the coAM^{NP} upper bound, but which clearly improves the NP^{NP} upper bound as $\text{EP}^{\text{NP}} \subseteq \text{NP}^{\text{NP}}$.

Theorem 2.2 $\text{BNE} \in \text{EP}^{\text{NP}}$.

¹The notion of boolean function equivalence underlying the definition of negation equivalence is the standard one. Two boolean functions (over the same variables) are equivalent if they have the same truth value for every assignment to their variables. Testing equivalence of pairs of boolean formulas is in coNP .

Proof. Suppose a given instance of BNE consists of f and g , each over the variables x_1, \dots, x_n . A negation of some of the input variables of g as in the definition of BNE can be represented by a vector $\vec{v} = (c_1, \dots, c_n)$ in the vector space $\text{GF}(2)^n$, where each c_i is either 0 or 1 and $c_i = 1$ means that the variable x_i will be negated. Let $g_{\vec{v}}$ be the boolean function resulting from g after the application of the negations described by \vec{v} , i.e., $g_{\vec{v}}(\vec{u}) = g(\vec{v} + \vec{u})$. Now it is easy to see (double negation equals identity, and addition in $\text{GF}(2)^n$ is associative) that, for each fixed boolean function g , the set of negation vectors \vec{v} such that g equals $g_{\vec{v}}$ is a linear subspace V_g of $\text{GF}(2)^n$. It is not hard to see that if \vec{w} is *any* negation vector such that $f = g_{\vec{w}}$, then the affine subspace $\vec{w} + V_g$ is the set of *all* negation vectors witnessing the negation equivalence of f and g . Of course, $\vec{w} + V_g$ will be of the same cardinality as the subspace V_g (as addition by \vec{w} induces a bijection between $\text{GF}(2)^n$ and itself), and as an ℓ -dimensional vector space over the field $\text{GF}(2)$ has exactly 2^ℓ vectors, $\vec{w} + V_g$ will contain exactly 2^m vectors, where m is the dimension of V_g . So the following nondeterministic program shows that BNE is in EP with an NP oracle: Read the two input functions f and g (checking that they are both over the same number of variables and that the variables have the same naming scheme), guess a negation vector \vec{v} and accept if and only if the oracle confirms that f is equal to g altered by the negation vector \vec{v} . This shows that BNE is in EP^{NP} , since if f and g are not negation equivalent, then there is no accepting path, and otherwise there are exactly 2^m accepting paths, where m is the dimension of the affine subspace discussed above. ■

There are ways of describing boolean functions such that the equivalence problem is in P. The most prominent such way is by ordered binary decision diagrams (OBDDs).² So, essentially by the same type of discussion found in the proof of Theorem 2.2, the following computational problem, OBDD Negation Equivalence, is in (nonrelativized) EP: Given a pair (e, f) of OBDDs, are the boolean functions described by e and f negation equivalent?

If we consider the special case that for the two OBDDs (e, f) above the order of the variables is required to be the same, we see that the following graph-theoretic problem is in (nonrelativized) EP. A *2-dag* is a directed acyclic graph (without labels) with a unique root and either 0 or 2 ordered successors for each node. For a 2-dag each node is assigned a depth, namely the distance to the root. Now consider the following computational problem (2-Dag Interchange Equivalence): Given two 2-dags F and G , is there a sequence of natural numbers (i_1, \dots, i_m) such that, if in G for each node of depth i_1, \dots, i_m its two successors (if they exist) are interchanged, then the modified 2-dag G' equals F ? This problem can be shown to be in EP (similarly to the argument above). Moreover, the problem can easily be reduced to Graph Isomorphism. The authors know of no P algorithm for the general case of 2-Dag Interchange Equivalence, though the special case of this problem with binary

²Fortune, Hopcroft, and Schmidt [22] were the ones who proved that equivalence for OBDDs is in P. OBDDs have recently become a structure of interest to theoretical computer scientists in a variety of settings, see, e.g., [35]. Recently, Feigenbaum et al. [18] showed that when one modifies certain graph problems, such as Independent Set or Graph Accessibility, so that the input graph is succinctly represented as an OBDD, there is an exponential blow-up in complexity. For general background on OBDDs see, for example, the survey by Bryant [13].

trees instead of general 2-dags has an easy deterministic polynomial-time algorithm.

3 Location of EP

3.1 Result

We state a general result that our technique gives, regarding the containment of FewP in restricted counting classes. We need some additional definitions.

Definition 3.1 *Let S be any set of positive integers. Define the restricted counting class RC_S as follows. $L \in \text{RC}_S$ if and only if there exists a nondeterministic polynomial-time Turing machine N such that, for every $x \in \Sigma^*$,*

1. *if $x \in L$ then $\#acc_N(x) \in S$, and*
2. *if $x \notin L$ then $\#acc_N(x) = 0$.*

For example, Valiant’s extensively studied class UP equals $\text{RC}_{\{1\}}$, and, for each $k \geq 2$, the class ModZ_kP of Beigel, Gill, and Hertrampf [7] equals $\text{RC}_{\mathbb{N}-\{a \mid (\exists b \in \mathbb{N}) [a=b \cdot k]\}}$.

A set is non-gappy if it has only small holes.

Definition 3.2 *Let S be any set of positive integers. We say S is non-gappy if $S \neq \emptyset$ and $(\exists k > 0)(\forall n \in S)(\exists m \in S)[m > n \wedge m/n \leq k]$.*

Definition 3.3 [26] *Let L be any subset of Σ^* . We say L is P-printable if there is a deterministic Turing machine M that runs in polynomial-time such that, for every nonnegative integer n , $M(0^n)$ prints out the set $\{x \mid x \in L \wedge |x| \leq n\}$.*

Theorem 3.4 *Let T be any set of positive integers such that T has a non-gappy, P-printable subset. Then $\text{FewP} \subseteq \text{RC}_T$.³*

Our proof technique builds (e.g., by adding a rate-of-growth argument) on that used by Cai and Hemachandra [15] to prove $\text{FewP} \subseteq \oplus\text{P}$, where $\oplus\text{P}$ [23, 32] is the class of languages L such that for some nondeterministic polynomial-time Turing machine N , on each x it holds that $x \in L \iff \#acc_N(x) \equiv 1 \pmod{2}$. We note that Köbler, Schöning, Toda, and Torán [30] interestingly built on that technique in their proof that $\text{FewP} \subseteq \text{C}_{\leq}\text{P}$, where C_{\leq}P [39] is the class of languages L such that there is a polynomial-time function f and

³Though this result is stated in a relatively general format, we mention in passing that even the restriction employed can be relaxed to the case of nonempty sets of positive integers for which, for some uniform constant, given any integer in the set finding another larger but at most multiplicatively-constantly-larger integer in the set is a polynomial-time task. One can even slightly relax the growth rate, but one has to be very careful to avoid a “bootstrapping” growth-explosion effect via clocking growth rates always with respect to the input. In any case, we feel the current statement of the theorem is general enough to capture the generality of the result without being so technical as to obscure its essence.

a nondeterministic polynomial-time Turing machine N such that for each x , $x \in L$ if and only if $\#acc_N(x) = f(x)$.

Proof of Theorem 3.4. Let S be a non-gappy, P-printable subset of T . Let $k > 0$ be, for S , some constant satisfying Definition 3.2.

Let L be any language in FewP. Let \hat{N} be a machine witnessing that $L \in \text{FewP}$, and let p be a polynomial bounding the nondeterministic ambiguity of \hat{N} , i.e., for each input x , $\#acc_{\hat{N}}(x) \leq p(|x|)$. To show that $L \in \text{RC}_T$, we describe a nondeterministic polynomial-time Turing machine N that accepts L via the RC_T acceptance mechanism.

On input x , N chooses $p(|x|)$ natural numbers $c_1, c_2, \dots, c_{p(|x|)}$ as follows. Initially, we assume that c_1 , which is defined to be the least element of S , is hard-coded into the program of N . Successively, for $i = 2, \dots, p(|x|)$, machine N on input x does the following:

- Let c_1, \dots, c_{i-1} be the constants that have already been chosen. Define

$$b_i = \binom{i}{1}c_1 + \binom{i}{2}c_2 + \dots + \binom{i}{i-1}c_{i-1}.$$

- Let a_i be the least element of S such that $b_i \leq a_i$.
- Set $c_i = a_i - b_i$.

After having chosen these constants, N (still on input x) will do the following: Nondeterministically guess an integer $i \in \{1, 2, \dots, p(|x|)\}$ and, for each i guessed, nondeterministically guess each (unordered) i -tuple of distinct paths of $\hat{N}(x)$. On each path α resulting from such a guess series, $N(x)$ sees whether the i paths of $\hat{N}(x)$ that were guessed on α are all accepting paths. If all are accepting paths, then path α , via trivial nondeterministic guesses, splits itself into c_i accepting paths. On the other hand, if at least one of the i guessed paths is a rejecting path, then path α simply rejects. This completes the description of N .

The intuition behind the construction of N is that for each input x the following holds. $N(x)$ has c_1 accepting paths for each accepting path of $\hat{N}(x)$; $N(x)$ has c_2 additional accepting paths for each pair of distinct accepting paths of $\hat{N}(x)$; and so on. So, if $x \in L$, $N(x)$ has $c_{\#acc_{\hat{N}}(x)}$ additional accepting paths for the (one) $\#acc_{\hat{N}}(x)$ -tuple of distinct accepting paths of $\hat{N}(x)$. However, if for some z with $\#acc_{\hat{N}}(x) < z \leq p(|x|)$ a z -tuple of distinct paths of $\hat{N}(x)$ was guessed on a path α of $N(x)$, then α must contain a rejecting path of $\hat{N}(x)$, and thus $N(x)$ will have no accepting paths related to c_z . This intuition is expressed formally by:

$$\#acc_N(x) = \binom{\#acc_{\hat{N}}(x)}{1}c_1 + \binom{\#acc_{\hat{N}}(x)}{2}c_2 + \dots + \binom{\#acc_{\hat{N}}(x)}{\#acc_{\hat{N}}(x)}c_{\#acc_{\hat{N}}(x)}.$$

Assume $x \in L$. Thus, $0 < \#acc_{\hat{N}}(x) \leq p(|x|)$. Since $c_{\#acc_{\hat{N}}(x)}$ was chosen such that

$$\begin{aligned} \#acc_{\hat{N}}(x) = 1 &\implies \#acc_N(x) = c_1, \text{ and} \\ \#acc_{\hat{N}}(x) \geq 2 &\implies \#acc_N(x) = b_{\#acc_{\hat{N}}(x)} + c_{\#acc_{\hat{N}}(x)} = a_{\#acc_{\hat{N}}(x)}, \end{aligned}$$

and since both c_1 and $a_{\#\text{acc}_{\hat{N}}(x)}$ are elements of S , it follows that $\#\text{acc}_N(x) \in T$. On the other hand, if $x \notin L$ then $\#\text{acc}_{\hat{N}}(x) = 0$, and so $\#\text{acc}_N(x) = 0$.

So now, to prove that $L \in \text{RC}_T$, it suffices to establish an exponential (in $|x|$) upper bound on the value of $\max_{i \leq p(|x|)} c_i$.

We will consider, for $j \geq 2$, what bounds hold on the value of c_j . By construction of N and since S is non-gappy, we have $c_j \leq a_j \leq kb_j$. Regarding the latter inequality, note that b_j is not necessarily an element of S . However, for each j , $c_1 \leq b_j$; so for each j , there exists a $\hat{b}_j \in S$ such that $\hat{b}_j \leq b_j$ and \hat{b}_j is the greatest such integer in S . Since a_j is defined to be the least element of S such that $b_j \leq a_j$, we have $a_j \leq k\hat{b}_j \leq kb_j$.

From the above and the definition of b_j , we have:

$$\begin{aligned} c_j &\leq k \left(\binom{j}{1} c_1 + \binom{j}{2} c_2 + \cdots + \binom{j}{j-1} c_{j-1} \right) \\ (1) \quad &\leq k(j-1) \binom{j}{\lceil \frac{j}{2} \rceil} \max_{1 \leq i \leq j-1} c_i. \end{aligned}$$

The factor $j-1$ in inequality (1) is the number of terms in b_j , and the coefficient $\binom{j}{\lceil \frac{j}{2} \rceil}$ is the biggest binomial coefficient of any term in b_j .

Recall that once we were given $S \subseteq T$ we fixed k . For all sufficiently large j the following holds:

$$(2) \quad k(j-1) \binom{j}{\lceil \frac{j}{2} \rceil} \leq \left(\binom{j}{\lceil \frac{j}{2} \rceil} \right)^2 \leq (2^j)^2.$$

In particular, let $j_{\text{bad}} = j_{\text{bad}}(k)$ be the largest j for which the above inequality fails to hold (if it always holds, set $j_{\text{bad}} = 1$). Let $I_{\text{bad}} = \max_{1 \leq i \leq j_{\text{bad}}} c_i$. From inequalities (1) and (2), we clearly have that, for $j > j_{\text{bad}}$:

$$c_j \leq I_{\text{bad}} \cdot \prod_{j_{\text{bad}} < i \leq j} 2^{2^i},$$

and, for $j \leq j_{\text{bad}}$, $c_j \leq I_{\text{bad}}$. This implies that $c_j = 2^{\mathcal{O}(j^2)}$.

Thus, for the fixed k associated with $S \subseteq T$, the value of $\max_{i \leq p(|x|)} c_i$ indeed is bounded by an exponential function in $|x|$. Hence, $L \in \text{RC}_T$, and thus $\text{FewP} \subseteq \text{RC}_T$. \blacksquare

It is immediate from its definition that $\text{EP} \subseteq \text{NP}$. It is also clear that the quantum-computation-related class $\text{C}_{=} \text{P}[\text{half}]$ of Berthiaume and Brassard [8] is contained in EP .⁴ From Theorem 3.4 it immediately follows that $\text{FewP} \subseteq \text{EP}$, since $\text{EP} = \text{RC}_{\{2^i \mid i \in \mathbb{N}\}}$ and $\{2^i \mid i \in \mathbb{N}\}$ is clearly a P-printable, non-gappy set.

Corollary 3.5 $\text{FewP} \subseteq \text{EP}$.

⁴ $\text{C}_{=} \text{P}[\text{half}]$, introduced by Berthiaume and Brassard [8] in their study of quantum complexity, is a variant of the class WPP of Fenner, Fortnow, and Kurtz [20]. Namely, $\text{C}_{=} \text{P}[\text{half}]$ is the class of languages L such that there is some nondeterministic Turing machine such that if the input is in L exactly half of the paths are accepting paths and if the input is not in L none of the paths are accepting paths.

The comments attached to our on-line technical report version [10] give some of the history of the proof of our results and of some valuable comments made by Richard Beigel, in particular that FewP is also contained in the EP analog based on any integer n (note that the acceptance sets for such classes are P-printable and non-gappy).

Cai and Hemachandra's result $\text{FewP} \subseteq \oplus\text{P}$ [15] has been generalized to $\text{FewP} \subseteq \text{ModZ}_k\text{P}$, for each $k \geq 2$ [7]. This generalization also follows as a special case of Theorem 3.4, since $\text{ModZ}_k\text{P} = \text{RC}_{\mathbb{N}-\{a \mid (\exists b \in \mathbb{N}) [a=b \cdot k]\}}$ as mentioned above.

Corollary 3.6 [7] *For each $k \geq 2$, $\text{FewP} \subseteq \text{ModZ}_k\text{P}$.*

3.2 Discussion

An immediate question is how Corollary 3.5 relates to known results about FewP. Clearly, Corollary 3.5 represents an improvement on the trivial inclusion $\text{FewP} \subseteq \text{NP}$. However, how does it compare with the nontrivial result of Köbler et al. [30] and Fenner, Fortnow, and Kurtz [20] that $\text{FewP} \subseteq \text{Few} \subseteq \text{SPP} \subseteq \oplus\text{P} \cap \text{C}_{\leq}\text{P}$? Informally stated, Few [15] is what a P machine can do given one call to a #P function that obeys the promise that its value is always at most polynomial. SPP [20, 31] is the class of sets L such that for some nondeterministic polynomial-time Turing machine N it holds that if $x \notin L$ then $N(x)$ has one fewer accepting path than it has rejecting paths, and if $x \in L$ then the numbers of accepting and rejecting paths of $N(x)$ are equal. Curiously, note that the nontrivial result that $\text{FewP} \subseteq \text{SPP}$ itself neither is known to imply nor is known to be implied by the trivial result $\text{FewP} \subseteq \text{NP}$.

There are a number of related aspects to the question raised above. First, is $\text{SPP} \subseteq \text{EP}$? This inclusion—which would make Corollary 3.5 a trivial consequence of the known result $\text{FewP} \subseteq \text{SPP}$ —seems unlikely, as if $\text{SPP} \subseteq \text{EP}$, then $\text{SPP} \subseteq \text{NP}$, and $\text{SPP} \subseteq \text{NP}$ is considered unlikely (see [20, 36]). Second, is $\text{EP} \subseteq \text{SPP}$? (This inclusion would make Corollary 3.5 a strengthening of the known result that $\text{FewP} \subseteq \text{SPP}$.) We do not know. Third, notice that we proved $\text{FewP} \subseteq \text{EP}$ but that the Köbler et al. [30] and Fenner, Fortnow, and Kurtz [20] work shows that $\text{Few} \subseteq \text{SPP}$. Can our result be extended to show $\text{Few} \subseteq \text{EP}$? The reason we mention this is that often it is the case that when one can prove something about FewP, then one can also prove it about the slightly bigger class Few. For example, Cai and Hemachandra, after showing that FewP is in $\oplus\text{P}$, then easily applied their technique to show that even Few is in $\oplus\text{P}$ [15]. Similarly, it is immediately clear that FewP has Turing-complete sets if and only if Few has Turing-complete sets, and so the proof that there is a relativized world in which FewP lacks Turing-complete sets [28] implicitly proves that there is a world in which Few lacks Turing-complete sets (see also [38]). However, in the case of Corollary 3.5, it is unlikely that by modifying the technique in a way similar to that done by Cai and Hemachandra one could hope to establish the slightly stronger result that EP even contains Few. Why? Clearly $\text{coUP} \subseteq \text{Few}$ and $\text{EP} \subseteq \text{NP}$, so the assumption $\text{Few} \subseteq \text{EP}$ would imply (along with other even more unlikely things) $\text{coUP} \subseteq \text{NP}$.

Fourth, one might wonder directly, since $\text{FewP} \subseteq \oplus\text{P}$ is known, about the relationship between EP and $\oplus\text{P}$. That is, how is EP (powers-of-two acceptance) related to $\oplus\text{P}$

(multiples-of-two acceptance).⁵ We note the following. By a diagonalization so routine as to not be worth including here, one can show $(\exists A) [\text{coUP}^A \not\subseteq \text{EP}^A]$. It follows immediately, since (for each B) $\text{coUP}^B \subseteq \text{Few}^B$, that $(\exists A) [\text{Few}^A \not\subseteq \text{EP}^A]$ and $(\exists A) [\oplus\text{P}^A \not\subseteq \text{EP}^A]$. Similarly, if one looks at the test language inside the proof of Proposition 12 of Beigel’s 1991 “mod classes” paper [5], one can see that for his case “ $k = 2$ ” the test language is in (relativized) $\text{C}_{\leq}\text{P}[\text{half}]$, and thus as a corollary to his proof one can claim $(\exists A) [\text{C}_{\leq}\text{P}[\text{half}]^A \not\subseteq \oplus\text{P}^A]$. It follows immediately that $(\exists A) [\text{EP}^A \not\subseteq \oplus\text{P}^A]$. Since these are standard diagonalizations that can easily be interleaved, it is easy to see that there is a relativized world in which EP and $\oplus\text{P}$ are incomparable (i.e., neither is contained in the other).⁶

Fifth and finally, to complete this discussion, what is the relation between EP and C_{\leq}P ? Proposition 3.7 below shows that EP is contained in C_{\leq}P .⁷ Thus, Corollary 3.5 improves upon Köbler et al.’s result that $\text{FewP} \subseteq \text{C}_{\leq}\text{P}$ [30]—an improvement that seems to neither imply nor be implied by other improvements of their result such as $\text{Few} \subseteq \text{SPP}$ ([30], see also [20]).

Proposition 3.7 $\text{EP} \subseteq \text{C}_{\leq}\text{P}$.

Proof. Let ES (which is the nonpromise version of EP) denote the class of all languages L for which there is a nondeterministic polynomial-time Turing machine N such that, for each input $x \in \Sigma^*$, $x \in L \iff \#\text{acc}_N(x) \in \{2^i \mid i \in \mathbb{N}\}$. Note that, clearly, $\text{EP} \subseteq \text{ES}$. However, note that $\text{ES} = \text{C}_{\leq}\text{P}$ as we now argue. $\text{ES} \subseteq \{L \mid (\exists A \in \text{C}_{\leq}\text{P})[L \leq_d^p A]\}$ is immediately clear from the definitions, where \leq_d^p is polynomial-time disjunctive reducibility. So $\text{ES} \subseteq \text{C}_{\leq}\text{P}$, as it is known that $\text{C}_{\leq}\text{P} = \{L \mid (\exists A \in \text{C}_{\leq}\text{P})[L \leq_d^p A]\}$ [6]. To show $\text{C}_{\leq}\text{P} \subseteq \text{ES}$, consider a C_{\leq}P machine and the function f giving the number of paths on which it would accept. Let $w(x)$ be the smallest integer such that $2^{w(x)} > f(x)$. Consider the EP machine that on input x has $2^{1+w(x)} - f(x)$ paths that immediately accept, and that also has paths that simulate the C_{\leq}P machine. Note that this machine accepts the C_{\leq}P language. ■

4 Open Questions

Does EP equal NP? It would be nice to give evidence that such an equality would, for example, collapse the polynomial hierarchy. However, $\text{UP} \subseteq \text{EP} \subseteq \text{NP}$, and at the present

⁵However, one should keep in mind the contrasting rejection sets of these two classes.

⁶Concerning Mod_qP classes for values $q > 2$ [15, 7], it follows easily from the known relations among such classes [7] and the obvious fact that powers of 2 are never congruent to zero modulo j , where j is any number greater than 2 that is not a power of two, that EP is contained in Mod_qP for all $q > 2$ such that q is not a power of two. (q values that are powers of two give just $\oplus\text{P}$ and thus as noted above are incomparable to EP in some relativized world.) So it also follows from this, in light of Beigel’s [5] result that for any distinct primes q_1 and q_2 there are oracles relative to which Mod_{q_1}P and Mod_{q_2}P are incomparable (i.e., neither contains the other), that for every $q > 1$ there is an oracle such that Mod_qP is not contained in EP.

⁷After seeing an earlier draft of this paper, Richard Beigel has communicated (February, 1998) to the authors that he observed that EP is even contained in the class LWPP [20]. Since it is known from the work of Fenner, Fortnow, and Kurtz [20] that $\text{SPP} \subseteq \text{LWPP} \subseteq \text{C}_{\leq}\text{P}$, this improves upon our result and in particular shows that EP is PP-low (i.e., $\text{PP} = \text{PP}^{\text{EP}}$), where PP denotes probabilistic polynomial time.

time, it is open whether even the stronger assumption $UP = NP$ implies any startling collapses. Also, does EP, in contrast to most promise classes, have complete sets? We conjecture that EP lacks complete sets (of course, if EP equals NP then EP has complete sets).

It is clear that EP is closed under conjunctive reductions and under disjoint union, and (thus) under intersection. Is EP closed under disjunctive reductions or union?

Finally, define:

Definition 4.1 $ListP_{\mathcal{F}}$ is the class of all sets L such that $(\exists f \in FP, f : \Sigma^* \rightarrow 2^{\mathbb{N}})$ $(\exists h \in \mathcal{F}) (\exists \text{ nondeterministic polynomial-time Turing machine } N) (\forall x)$

$$[|f(x)| \leq h(|x|) \wedge \#acc_N(x) \in f(x) \cup \{0\} \wedge (x \in L \iff \#acc_N(x) \geq 1)],$$

where FP denotes the class of (total) polynomial-time functions.

Let $ListP = ListP_{poly}$, where $poly$ is the set of all polynomials. That is, $ListP$ is very similar to EP, except the list of potential numbers of accepting paths on an input, rather than being $\{0, 1, 2, 4, 8, \dots\}$, is instead some polynomial-time computable polynomial-sized list (of numbers written in binary) that may depend on the input. Clearly, $EP \subseteq ListP$, and in fact the EP analogs based not on powers of 2 but on powers of k are also in $ListP$. Is $SAT \in ListP$? We do not know. However, note that $ListP$ is in some sense a language analog of the function-based notion of “enumerative counting” [14]. It follows immediately from an enumerative counting result of Cai and Hemachandra [16] and, independently, Amir, Beigel, Gasarch, and Toda (included in [3]) that SAT is in $ListP$ via a machine M that uses the canonical witness scheme for SAT (or any witness scheme whose numbers of witnesses are 1-Turing interreducible with those of the canonical witness scheme in the context of the input) if and only if $P = P^{\#P}$. So if we knew that all witness schemes for SAT were closely related to the canonical one, then we would know that SAT was in $ListP$ if and only if $P = P^{\#P}$. However, can SAT thwart this by having some bizarre witness scheme deeply unrelated to its canonical witness scheme? In fact, Fischer, Hemaspaandra, and Torenvliet have recently provided sufficient conditions for such schemes to exist [21].

Similar comments apply to Graph Automorphism (GA). Is $GA \in ListP$? We do not know. However, it follows immediately from a result of Chang, Gasarch, and Torán [17] that GA is in $ListP$ via a machine M that uses the canonical witness scheme for GA (or any witness scheme whose numbers of witnesses are 1-Turing interreducible with those of the canonical witness scheme in the context of the input) only if Graph Isomorphism [sic] is in R , random polynomial time.

Acknowledgments

We thank Richard Beigel, Frank Stephan, and Gerd Wechsung for interesting comments or discussions, and Dieter Kratsch, Haiko Müller, and Johannes Waldmann for very kindly letting us use their office’s computers to type in part of this paper.

References

- [1] M. Agrawal and T. Thierauf. The boolean isomorphism problem. In *Proceedings of the 37th IEEE Symposium on Foundations of Computer Science*, pages 422–430. IEEE Computer Society Press, October 1996.
- [2] E. Allender and R. Rubinfeld. P-printable sets. *SIAM Journal on Computing*, 17(6):1193–1202, 1988.
- [3] A. Amir, R. Beigel, and W. Gasarch. Some connections between bounded query classes and non-uniform complexity. In *Proceedings of the 5th Structure in Complexity Theory Conference*, pages 232–243. IEEE Computer Society Press, July 1990.
- [4] R. Beigel. On the relativized power of additional accepting paths. In *Proceedings of the 4th Structure in Complexity Theory Conference*, pages 216–224. IEEE Computer Society Press, June 1989.
- [5] R. Beigel. Relativized counting classes: Relations among thresholds, parity, and mods. *Journal of Computer and System Sciences*, 42(1):76–96, 1991.
- [6] R. Beigel, R. Chang, and M. Ogiwara. A relationship between difference hierarchies and relativized polynomial hierarchies. *Mathematical Systems Theory*, 26(3):293–310, 1993.
- [7] R. Beigel, J. Gill, and U. Hertrampf. Counting classes: Thresholds, parity, mods, and fewness. In *Proceedings of the 7th Annual Symposium on Theoretical Aspects of Computer Science*, pages 49–57. Springer-Verlag *Lecture Notes in Computer Science #415*, February 1990.
- [8] A. Berthiaume and G. Brassard. The quantum challenge to structural complexity theory. In *Proceedings of the 7th Structure in Complexity Theory Conference*, pages 132–137. IEEE Computer Society Press, June 1992.
- [9] A. Blass and Y. Gurevich. On the unique satisfiability problem. *Information and Control*, 55:80–88, 1982.
- [10] B. Borchert, L. Hemaspaandra, and J. Rothe. Powers-of-two acceptance suffices for equivalence and bounded ambiguity problems. Technical Report TR96-045, Electronic Colloquium on Computational Complexity, <http://www.eccc.uni-trier.de/eccc/>, August 1996.
- [11] B. Borchert, D. Ranjan, and F. Stephan. On the computational complexity of some classical equivalence relations on boolean functions. *Theory of Computing Systems*, 31:679–693, 1998.
- [12] B. Borchert and F. Stephan. Looking for an analogue of Rice’s Theorem in circuit complexity theory. In *Proceedings of the 1997 Kurt Gödel Colloquium*, pages 114–127. Springer-Verlag *Lecture Notes in Computer Science #1289*, 1997.
- [13] R. Bryant. Symbolic boolean manipulation with ordered binary decision diagrams. *ACM Computing Surveys*, 24(3):293–318, 1992.
- [14] J. Cai and L. Hemachandra. Enumerative counting is hard. *Information and Computation*, 82(1):34–44, 1989.
- [15] J. Cai and L. Hemachandra. On the power of parity polynomial time. *Mathematical Systems Theory*, 23(2):95–106, 1990.
- [16] J. Cai and L. Hemachandra. A note on enumerative counting. *Information Processing Letters*, 38(4):215–219, 1991.

- [17] R. Chang, W. Gasarch, and J. Torán. On finding the number of graph automorphisms. In *Proceedings of the 10th Structure in Complexity Theory Conference*, pages 288–298. IEEE Computer Society Press, June 1995.
- [18] J. Feigenbaum, S. Kannan, M. Vardi, and M. Viswanathan. Complexity of problems on graphs represented as OBDDs. In *Proceedings of the 15th Annual Symposium on Theoretical Aspects of Computer Science*, pages 216–226. Springer-Verlag *Lecture Notes in Computer Science #1373*, February 1998.
- [19] M. Fellows and N. Koblitz. Self-witnessing polynomial-time complexity and prime factorization. In *Proceedings of the 7th Structure in Complexity Theory Conference*, pages 107–110. IEEE Computer Society Press, June 1992.
- [20] S. Fenner, L. Fortnow, and S. Kurtz. Gap-definable counting classes. *Journal of Computer and System Sciences*, 48(1):116–148, 1994.
- [21] S. Fischer, L. Hemaspaandra, and L. Torenvliet. Witness-isomorphic reductions and local search. In A. Sorbi, editor, *Complexity, Logic, and Recursion Theory*, pages 207–223. Marcel Dekker, Inc., 1997.
- [22] S. Fortune, J. Hopcroft, and E. Schmidt. The complexity of equivalence and containment for free single program schemes. In *Proceedings of the 5th International Colloquium on Automata, Languages, and Programming*, pages 227–240. Springer-Verlag *Lecture Notes in Computer Science #62*, 1978.
- [23] L. Goldschlager and I. Parberry. On the construction of parallel computers from various bases of boolean functions. *Theoretical Computer Science*, 43:43–58, 1986.
- [24] J. Grollmann and A. Selman. Complexity measures for public-key cryptosystems. *SIAM Journal on Computing*, 17(2):309–335, 1988.
- [25] M. Harrison. Counting theorems and their applications to classification of switching functions. In A. Mukhopadhyay, editor, *Recent Developments in Switching Theory*, pages 4–22. Academic Press, 1971.
- [26] J. Hartmanis and Y. Yesha. Computation times of NP sets of different densities. *Theoretical Computer Science*, 34:17–32, 1984.
- [27] E. Hemaspaandra and L. Hemaspaandra. Quasi-injective reductions. *Theoretical Computer Science*, 123(2):407–413, 1994.
- [28] L. Hemaspaandra, S. Jain, and N. Vereshchagin. Banishing robust Turing completeness. *International Journal of Foundations of Computer Science*, 4(3):245–265, 1993.
- [29] L. Hemaspaandra and J. Rothe. Unambiguous computation: Boolean hierarchies and sparse Turing-complete sets. *SIAM Journal on Computing*, 26(3):634–653, 1997.
- [30] J. Köbler, U. Schöning, S. Toda, and J. Torán. Turing machines with few accepting computations and low sets for PP. *Journal of Computer and System Sciences*, 44(2):272–286, 1992.
- [31] M. Ogiwara and L. Hemachandra. A complexity theory for closure properties. *Journal of Computer and System Sciences*, 46(3):295–325, 1993.
- [32] C. Papadimitriou and S. Zachos. Two remarks on the power of counting. In *Proceedings 6th GI Conference on Theoretical Computer Science*, pages 269–276. Springer-Verlag *Lecture Notes in Computer Science #145*, 1983.

- [33] R. Rao, J. Rothe, and O. Watanabe. Upward separation for FewP and related classes. *Information Processing Letters*, 52(4):175–180, 1994.
- [34] U. Schöning. Probabilistic complexity classes and lowness. *Journal of Computer and System Sciences*, 39(1):84–100, 1989.
- [35] Y. Takenaga, M. Nouzoe, and S. Yajima. Size and variable ordering of OBDDs representing threshold functions. In *Proceedings of the 3rd Annual International Computing and Combinatorics Conference*, pages 91–100. Springer-Verlag *Lecture Notes in Computer Science #1276*, August 1997.
- [36] 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.
- [37] L. Valiant. The relative complexity of checking and evaluating. *Information Processing Letters*, 5(1):20–23, 1976.
- [38] N. Vereshchagin. Relativizable and nonrelativizable theorems in the polynomial theory of algorithms. *Russian Academy of Sciences–Izvestiya–Mathematics*, 42(2):261–298, 1994.
- [39] K. Wagner. The complexity of combinatorial problems with succinct input representations. *Acta Informatica*, 23:325–356, 1986.