Immunity and Simplicity for Exact Counting and Other Counting Classes

Jörg Rothe [1]
Institut für Informatik
Friedrich-Schiller-Universität Jena
07740 Jena, Germany
rothe@informatik.uni-jena.de

Revision after Conference Final Version, May 12, 1998

[1]Supported in part by grants NSF-INT-9513368/DAAD-315-PRO-fo-ab and NSF-CCR-9322513 and by a NATO Postdoctoral Science Fellowship from the Deutscher Akademischer Austauschdienst ("Gemeinsames Hochschulsonderprogramm III von Bund und Ländern"). Work done in part while visiting the University of Rochester.

Abstract

Ko [Ko90] and Bruschi [Bru92] independently showed that, in some relativized world, PSPACE (in fact, $\oplus$P) contains a set that is immune to the polynomial hierarchy (PH). In this paper, we study and settle the question of (relativized) separations with immunity for PH and the counting classes PP, $\mathrm{C}_{=}\mathrm{P}$, and $\oplus$P in all possible pairwise combinations. Our main result is that there is an oracle A relative to which $\mathrm{C}_{=}\mathrm{P}$ contains a set that is immune to $\mathrm{BPP}^{\oplus\mathrm{P}}$. In particular, this $\mathrm{C}_{=}\mathrm{P}^{A}$ set is immune to PH^{A} and to $\oplus\mathrm{P}^{A}$. Strengthening results of Torán [Tor91] and Green [Gre91], we also show that, in suitable relativizations, NP contains a $\mathrm{C}_{=}\mathrm{P}$-immune set, and $\oplus$P contains a $\mathrm{PP}^{\mathrm{PH}}$-immune set. This implies the existence of a $\mathrm{C}_{=}\mathrm{P}^{B}$-simple set for some oracle B, which extends results of Balcázar et al. [Bal85,BR88], and provides the first example of a simple set in a class not known to be contained in PH. Our proof technique requires a circuit lower bound for "exact counting" that is derived from Razborov's [Raz87] circuit lower bound for majority.

Keywords: Computational complexity; immunity; counting classes; relativized computation; circuit lower bounds.

1 Introduction

A fundamental task in complexity theory is to prove separations or collapses of complexity classes. Unfortunately, results of this kind fall short for the most important classes between polynomial time and polynomial space. In an attempt to find the reasons for this frustrating failure over many years, and to gain more insight into why these questions are beyond current techniques, researchers have studied the problem of separating complexity classes in relativized settings. Baker, Gill, and Solovay, in their seminal paper [BGS75], gave for example relativizations A and B such that $\mathrm{P}^A \neq \mathrm{NP}^A$ and $\mathrm{P}^B = \mathrm{NP}^B$, setting the stage for a host of subsequent relativization results.

Separations are also evaluated with regard to their quality. A *simple separation* such as $\mathrm{P}^A \neq \mathrm{NP}^A$ merely claims the existence of a set S in NP^A that is not recognized by any P^A machine. This can be accomplished by a simple diagonalization ensuring that every P^A machine fails to recognize S by just one string, which is put into the symmetric difference of S and the machine's language. It may well be the case, however, that some P^A machine nonetheless accepts an infinite subset of S, thus "approximating from the inside" the set witnessing the separation. Thus, one might argue that the difference between P^A and NP^A, as witnessed by S, is negligible. In contrast, a *strong separation* of P^A and NP^A is witnessed by a P^A-immune set in NP^A. For any class $\mathcal{C}$ of sets, a set is *$\mathcal{C}$-immune* if it is an infinite set having no infinite subset in $\mathcal{C}$.

A relativization in which NP and P are strongly separated was first given by Bennett and Gill [BG81]. In fact, they prove a stronger result. Technically speaking, they show that relative to a random oracle R, NP^R contains a P^R bi-immune set with probability 1. This was recently strengthened by Hemaspaandra and Zimand [HZ96] to the strongest result possible: Relative to a random oracle R, NP^R contains a P^R *balanced* immune set with probability 1. See these references for the notions not defined here.

Many more immunity results are known—see, e.g., [HM83,SB84,Bal85,BR88,TvEB89, BJY90,Ko90,Lis,Bru92,EHTY92,BCS92,HRW97]. Most important for the present paper are the results and (circuit-based) techniques of Ko [Ko90] and Bruschi [Bru92]. In particular, both papers provide relativizations in which the levels of the polynomial hierarchy (PH) separate with immunity, Bruschi's results being somewhat stronger and more refined, as they refer not only to the Σ, but also to the Δ levels of PH. Also, both authors independently obtain the result that there exists a PH-immune set in PSPACE, relative to an oracle. Since Ko's proof is only briefly sketched, Bruschi includes a detailed proof of this result. This proof, however, is flawed.[1]

[1]In particular, looking into the proof of [Bru92, Thm. 8.3], the existence of the desired oracle extension, W, in Case (e) of the construction is not guaranteed by the circuit lower bound used. In Case (e) of Stage l, W is required to have an odd number of length $h(l)$ strings such that all circuits associated with a list of still unsatisfied requirements reject their inputs *simultaneously*—an input corresponds to the W chosen; so once W is fixed, every circuit has the same input, $\chi_W(0^{h(l)}) \cdots \chi_W(1^{h(l)})$. The used circuit lower bound for the parity function merely ensures that for each circuit C on that list, C computes parity correctly for at most

Using Ko's approach, it is not difficult to give a valid and complete proof of this result (and indeed the present paper provides such a full proof—note Corollary 3.6). However, the purpose of this paper goes beyond that: We study separations with immunity for counting classes inside PSPACE with respect to the polynomial hierarchy and among each other. Counting classes that have proven particularly interesting and powerful with regard to the polynomial hierarchy are PP (probabilistic polynomial time), the exact counting class $\mathrm{C}_=\mathrm{P}$, and $\oplus$P (parity polynomial time). Note that the PSPACE^A set that is shown by Ko [Ko90] (cf. [Bru92]) to be PH^A-immune in fact is contained in $\oplus\mathrm{P}^A$. Ko's technique [Ko90] is central to all results of the present paper.

The relationship between these counting classes and PH still is a major open problem in complexity theory, although surprising advances have been made showing the hardness of counting. In particular, Toda [Tod91] and Toda and Ogihara [TO92] have shown that each class $\mathcal{C}$ chosen among PP, $\mathrm{C}_=\mathrm{P}$, and $\oplus$P is hard for the polynomial hierarchy (and, in fact, is hard for $\mathcal{C}^{\mathrm{PH}}$) with respect to polynomial-time bounded-error random reductions. Toda [Tod91] showed that PP is hard for PH even with respect to deterministic polynomial-time Turing reductions. However, it is widely suspected that PH is not contained in, and does not contain, any of these counting classes. There are oracles known relative to which each such containment fails, and similarly there are oracles relative to which each possible containment for any pair of these counting classes fails (except the known containment $\mathrm{C}_=\mathrm{P} \subseteq \mathrm{PP}$ [Sim75,Wag86], which holds relative to every oracle), see [BGS75,Tor88,Tor91, Bei91,Gre91,Bei94].

Regarding relativized *strong* separations, however, the only results known are the above-mentioned result that for some A, $\oplus\mathrm{P}^A$ contains a PH^A-immune set [Ko90] (cf. [Bru92]), and that for some B, NP^B (and thus PH^B and PP^B) has a $\oplus\mathrm{P}^B$-immune set [BCS92]. In this paper, we strengthen to (relativized) strong separations all the other simple separations that are possible among pairs of classes chosen from $\{\mathrm{PH}, \mathrm{PP}, \oplus\mathrm{P}, \mathrm{C}_=\mathrm{P}\}$. Just as Balcázar and Russo [Bal85,BR88] exhaustively settled (in suitable relativizations) all possible immunity and simplicity questions among the probabilistic classes BPP, R, ZPP, and PP and among these classes and P and NP, we do so for the counting classes $\mathrm{C}_=\mathrm{P}$, PP, and $\oplus$P among each other and with respect to the polynomial hierarchy.

Ko's proof of the result that $\oplus\mathrm{P}^A$ contains a PH^A-immune set exploits the circuit lower bounds for the parity function provided by Yao [Yao85] and Håstad [Hås89]. Noticing that Håstad [Hås89] proved an equally strong lower bound for the majority function, one could as well show that PP^A contains a PH^A-immune set for some oracle A. We prove a stronger result: By deriving from Razborov's [Raz87] circuit lower bound for the majority function a sufficiently strong lower bound for the boolean function that corresponds to

20% of the "odd" inputs of length $h(l)$. Thus, the extension W must be chosen according to the remaining 80% of such inputs to make that circuit reject. However, if there are sufficiently many circuits on the list whose correct input regions happen to cover *all* "odd" inputs of length $h(l)$ (for instance, when there are 5 circuits each being correct on a different 20% of such inputs), then there is no room left to choose a set $W \subseteq \{0,1\}^{h(l)}$ of odd cardinality that makes all circuits reject simultaneously.

"exact counting," we construct an oracle relative to which even in $\mathrm{C_{=}P}$ (which is contained in PP) there exists a set that is immune even to the class $\mathrm{BPP}^{\oplus\mathrm{P}}$ (which contains PH by Toda's result [Tod91]). This implies a number of new immunity results, including (relativized) $\oplus$P-immunity and PH-immunity of $\mathrm{C_{=}P}$.

Conversely, we show that, in some relativized world, NP (and thus PH and PP) contains a $\mathrm{C_{=}P}$-immune set, which strengthens Torán's simple separation of NP and $\mathrm{C_{=}P}$ [Tor88, Tor91]. As a corollary of this result, we obtain that, in the same relativization, $\mathrm{C_{=}P}$ has a *simple* set, i.e., a coinfinite $\mathrm{C_{=}P}$ set whose complement is $\mathrm{C_{=}P}$-immune. Just like immunity, the notion of simplicity originates from recursive function theory and has later proved useful also in complexity theory. The existence of a simple set in a class $\mathcal{C}$ provides strong evidence that $\mathcal{C}$ separates from the corresponding class co$\mathcal{C}$. Our result that, for some oracle B, $\mathrm{C_{=}P}^B$ has a simple set extends Balcázar's result that, for some A, NP^A has a simple set [Bal85]. We also strengthen to a strong separation Green's simple separation that, relative to some oracle, $\oplus\mathrm{P} \not\subseteq \mathrm{PP}^{\mathrm{PH}}$ [Gre91]. Similarly, the (relativized) simple separation of the levels of the $\mathrm{PP}^{\mathrm{PH}}$ hierarchy [BU] also can be turned into a strong separation. As a special case, this includes the existence of a PP-immune set in P^{NP} (and thus in PH) relative to some oracle, which improves upon a simple separation of Beigel [Bei94].

2 Preliminaries

Fix the two-letter alphabet $\Sigma \stackrel{\mathrm{df}}{=} \{0,1\}$. The set of all strings over Σ is denoted Σ^*, and the set of strings of length n is denoted Σ^n. For any string $x \in \Sigma^*$, let $|x|$ denote its length. For any set $L \subseteq \Sigma^*$, the complement of L is $\overline{L} \stackrel{\mathrm{df}}{=} \Sigma^* \setminus L$, and the characteristic function of L is denoted by χ_L, i.e., $\chi_L(x) = 1$ if $x \in L$, and $\chi_L(x) = 0$ if $x \notin L$. For the definition of relativized complexity classes and of oracle Turing machines, we refer to any standard text book on computational complexity (see, e.g., [Pap94,BDG88,HU79]). For any oracle Turing machine M and any oracle A, we denote the language of M^A by $L(M^A)$, and we simply write $L(M)$ if $A = \emptyset$. For classes $\mathcal{C}$ and $\mathcal{D}$ of sets, define $\mathcal{C}^{\mathcal{D}}$ to be $\bigcup_{D \in \mathcal{D}} \mathcal{C}^D$, where $\mathcal{C}^D$ denotes the class of languages accepted by $\mathcal{C}$ oracle machines with oracle D. For any class $\mathcal{C}$, let co$\mathcal{C}$ denote $\{L \mid \overline{L} \in \mathcal{C}\}$. We use NPOTM as a shorthand for "nondeterministic polynomial-time oracle Turing machine." Let $\mathrm{acc}_{M^A}(x)$ (respectively, $\mathrm{rej}_{M^A}(x)$) denote the number of accepting (respectively, rejecting) computation paths of NPOTM M with oracle A on input x, and let $\mathrm{tot}_{M^A}(x)$ be the total number of computation paths of M^A on input x.

Definition 2.1 *Let A be any oracle set.*

1. [MS72,Sto77] *The (relativized) polynomial hierarchy can be defined as follows, see also* [Wra77]*:*

   - *For each $k \geq 0$, a set L is in $\Sigma_k^{p,A}$ if and only if there exists a polynomial p and* *a predicate σ computable in* P^A *such that for all strings* x,

$$x \in L \iff (\mathrm{Q}_1 w_1)\,(\mathrm{Q}_2 w_2) \cdots (\mathrm{Q}_k w_k)\,[\sigma(x, w_1, w_2, \ldots, w_k) = 1],$$

where the w_j *range over the length* $p(|x|)$ *strings, and for each* i, $1 \le i \le k$, $\mathrm{Q}_i = \exists$ *if* i *is odd, and* $\mathrm{Q}_i = \forall$ *if* i *is even. Let* $\Pi_k^{p,A}$ *denote* $\mathrm{co}\Sigma_k^{p,A}$.

- *Define* $\mathrm{PH}^A \stackrel{\mathrm{df}}{=} \bigcup_{i \ge 0} \Sigma_i^{p,A}$.

2. [PZ83,GP86] $\oplus\mathrm{P}^A \stackrel{\mathrm{df}}{=} \{L \mid (\exists\,\mathrm{NPOTM}\ M)\,(\forall x \in \Sigma^*)\,[x \in L \iff \mathrm{acc}_{M^A}(x)$ is odd$]\}$.
3. [Gil77] $\mathrm{PP}^A \stackrel{\mathrm{df}}{=} \{L \mid (\exists\,\mathrm{NPOTM}\ M)\,(\forall x \in \Sigma^*)\,[x \in L \iff \mathrm{acc}_{M^A}(x) \ge \mathrm{rej}_{M^A}(x)]\}$.
4. [Sim75,Wag86] $\mathrm{C}_{=}\mathrm{P}^A \stackrel{\mathrm{df}}{=} \{L \mid (\exists\,\mathrm{NPOTM}\ M)\,(\forall x \in \Sigma^*)\,[x \in L \iff \mathrm{acc}_{M^A}(x) = \mathrm{rej}_{M^A}(x)]\}$.
5. [Gil77] BPP^A *is the class of languages* L *for which there exists an NPOTM* M *such that for each input* x, $x \in L$ *implies that* $\mathrm{rej}_{M^A}(x) \le \frac{1}{4}\mathrm{tot}_{M^A}(x)$, *and* $x \notin L$ *implies that* $\mathrm{acc}_{M^A}(x) \le \frac{1}{4}\mathrm{tot}_{M^A}(x)$.
6. *We write* Σ_k^p *for* $\Sigma_k^{p,\emptyset}$ *and* PH *for* $\mathrm{PH}^{\emptyset}$, *and similarly for the other classes.*

Clearly, $\mathrm{PH} \cup \oplus\mathrm{P} \cup \mathrm{PP} \cup \mathrm{C}_{=}\mathrm{P} \subseteq \mathrm{PSPACE}$ and $\mathrm{BPP} \subseteq \mathrm{PP}$, and it is also known that $\mathrm{BPP} \subseteq \Sigma_2^p \cap \Pi_2^p$ [Lau83,Sip83b] and $\mathrm{coNP} \subseteq \mathrm{C}_{=}\mathrm{P} \subseteq \mathrm{PP}$ [Sim75,Wag86].

An n-ary boolean function is a mapping f_n from $\{0,1\}^n$ to $\{0,1\}$. Some of the most important boolean functions are the parity function and the majority function. Let us define those functions that will be considered in this paper:

- $\textsc{Par}_n(x) = 1$ if and only if the number of bits of x that are 1 is odd.
- $\textsc{Maj}_n(x) = 1$ if and only if at least $\lceil \frac{n}{2} \rceil$ bits of x are 1.
- $\textsc{Equ}_n^k(x) = 1$ if and only if exactly k bits of x are 1, where $0 \le k \le n$.
- $\textsc{Equ}_n^{\mathrm{half}}(x) = 1$ if and only if exactly $\lceil \frac{n}{2} \rceil$ bits of x are 1.

Families of boolean functions are realized by circuit families. By convention, when we speak of "a" circuit C computing "a" function f, we implicitly mean a family $C = (C_n)_{n \ge 0}$ of circuits computing a family $f = (f_n)_{n \ge 0}$ of functions (i.e., for each n, C_n is a circuit with n input gates and one output gate that outputs the value $f_n(x)$ for each $x \in \{0,1\}^n$). The *size* of a circuit is the number of its gates. The *circuit complexity* (or *size*) of a boolean function f is the size of a smallest circuit computing f. Unless stated otherwise, we will consider only constant depth, unbounded fanin circuits with AND, OR, and $\oplus$ (parity) gates. An AND (respectively, OR) gate outputs 1 (respectively, 0) if and only if all its inputs are 1 (respectively, 0), and a $\oplus$ gate outputs 1 if and only if an odd number of its inputs are 1. Since $\{\mathrm{AND}, \mathrm{OR}, \oplus\}$ (and indeed, $\{\mathrm{AND}, \oplus\}$) forms a complete basis, we do not need negation gates. Note that switching from one complete basis to another increases the size of a circuit at most by a constant. The *depth* of a circuit is the length of a longest path from its input gates to its output gate. Since adjacent levels of gates of the same type can be collapsed to one level of gates of this type, we view a circuit to consist of alternating levels of respectively AND, OR, and $\oplus$ gates, where the sequence of these operations is arbitrary—the depth of the circuit thus also measures the number of alternations.

3 Immunity and Simplicity Results for Exact Counting

In this section, we prove the main result of this paper:

Theorem 3.1 *There exists some oracle A such that* $\mathrm{C_{=}P}^A$ *contains a* $\mathrm{BPP}^{\oplus\mathrm{P}^A}$*-immune set.*

Before turning to the actual proof, some technical details need be discussed. First, we need a sufficiently strong lower bound on the size of the "exact counting" function, $\mathrm{E{\scriptstyle QU}}_n^{\mathrm{half}}$, when computed by circuits as described in the previous section. Razborov proved the following exponential lower bound on the size of the majority function when computed by such circuits (see [Smo87] for a generalization of this result and a simplification of its proof).

Theorem 3.2 [Raz87] *For every k, any depth k circuit with* AND, OR, *and* $\oplus$ *gates that computes* $\mathrm{M{\scriptstyle AJ}}_n$ *has size at least* $2^{\Omega(n^{1/(2k+2)})}$.

Using this lower bound for majority, we could (by essentially the same proof as that of Theorem 3.1) directly establish $\mathrm{BPP}^{\oplus\mathrm{P}^A}$-immunity of PP^A. However, to obtain the stronger result of Theorem 3.1, we now derive from the above lower bound for majority a slightly weaker lower bound for the $\mathrm{E{\scriptstyle QU}}_n^{\mathrm{half}}$ function, still being sufficiently strong to establish Theorem 3.1.

Lemma 3.3 *For every k, there exists a constant $\alpha_k > 0$ and an $n_k \in \mathbb{N}$ such that for all $n \geq n_k$, every depth k circuit with* AND, OR, *and* $\oplus$ *gates that computes* $\mathrm{E{\scriptstyle QU}}_n^{\mathrm{half}}$ *has size at least* $n^{-1} \cdot 2^{\alpha_k n^{1/(2k+4)}}$.

Proof. Fix a sufficiently large n. Clearly, the majority function can be expressed as $\mathrm{M{\scriptstyle AJ}}_n(x) = \bigvee_{i=\lceil \frac{n}{2} \rceil}^{n} \mathrm{E{\scriptstyle QU}}_n^i(x)$. Each function $\mathrm{E{\scriptstyle QU}}_n^i$, $0 \leq i \leq n$, is a subfunction of $\mathrm{E{\scriptstyle QU}}_{2n}^{\mathrm{half}}$, since for each $x \in \{0,1\}^n$, $\mathrm{E{\scriptstyle QU}}_n^i(x) = \mathrm{E{\scriptstyle QU}}_{2n}^{\mathrm{half}}(x0^i1^{n-i})$. Thus, the circuit complexity of $\mathrm{E{\scriptstyle QU}}_n^i$ is at most that of $\mathrm{E{\scriptstyle QU}}_{2n}^{\mathrm{half}}$ for each i. Now let $\mathrm{size}_k(\mathrm{E{\scriptstyle QU}}_n^{\mathrm{half}})$ denote the size of a smallest depth k circuit with AND, OR, and $\oplus$ gates that computes $\mathrm{E{\scriptstyle QU}}_n^{\mathrm{half}}$. By the above observation, we can realize $\mathrm{M{\scriptstyle AJ}}_{\lceil \frac{n}{2} \rceil}$ with less than $n \cdot \mathrm{size}_k(\mathrm{E{\scriptstyle QU}}_n^{\mathrm{half}})$ gates in depth $k+1$. Hence, by Theorem 3.2,

$$\mathrm{size}_k(\mathrm{E{\scriptstyle QU}}_n^{\mathrm{half}}) \geq n^{-1} \cdot \mathrm{size}_{k+1}(\mathrm{M{\scriptstyle AJ}}_{\lceil \frac{n}{2} \rceil}) = n^{-1} \cdot 2^{\alpha_k n^{1/(2k+4)}}$$

for some suitable constant $\alpha_k > 0$ that depends on k. ∎

For technical reasons, since we want to apply the above circuit lower bound to obtain (relativized) $\mathrm{BPP}^{\oplus\mathrm{P}}$-immunity, we will now give an equivalent definition of the class $\mathrm{BPP}^{\oplus\mathrm{P}}$ in terms of a hierarchy denoted $\mathrm{PH}^{\oplus}$. As explained later, $\mathrm{PH}^{\oplus}$ will only serve as a tool in the upcoming proof of Theorem 3.1. $\mathrm{PH}^{\oplus}$ generalizes the polynomial hierarchy by allowing—in addition to existential and universal quantifiers—the *parity* quantifier $\oplus$, where $(\oplus w)$ means "for an odd number of strings w."

Definition 3.4 *Let A be any oracle set.*

1. *For each $k \geq 0$, a set L is in $\mathrm{PH}_k^{\oplus,A}$ if and only if there exists a polynomial p and a predicate σ computable in P^A such that for all strings x,*

$$x \in L \iff (\mathrm{Q}_1 w_1)(\mathrm{Q}_2 w_2)\cdots(\mathrm{Q}_k w_k)\,[\sigma(x, w_1, w_2, \ldots, w_k) = 1],$$

   where the w_j range over the length $p(|x|)$ strings and the quantifiers Q_j are chosen from $\{\exists, \forall, \oplus\}$.

2. *Define $\mathrm{PH}^{\oplus,A} \stackrel{\mathrm{df}}{=} \bigcup_{i\geq 0} \mathrm{PH}_i^{\oplus,A}$.*

3. *We write $\mathrm{PH}_k^{\oplus}$ for $\mathrm{PH}_k^{\oplus,\emptyset}$ and $\mathrm{PH}^{\oplus}$ for $\mathrm{PH}^{\oplus,\emptyset}$.*

We stress that $\mathrm{PH}^{\oplus}$ is *not* a new complexity class or hierarchy, since it is just another name for the class $\mathrm{BPP}^{\oplus\mathrm{P}}$, as can be proven by an easy induction from the results of Toda [Tod91] and Regan and Royer [RR95] that $\oplus\mathrm{P}^{\mathrm{BPP}^{\oplus\mathrm{P}}}$, $\mathrm{NP}^{\mathrm{BPP}^{\oplus\mathrm{P}}}$, and $\mathrm{coNP}^{\mathrm{BPP}^{\oplus\mathrm{P}}}$ each are contained in $\mathrm{BPP}^{\oplus\mathrm{P}}$.[2] Rather, the purpose of $\mathrm{PH}^{\oplus}$ is merely to simplify the proof of Theorem 3.1. In particular, when using $\mathrm{PH}^{\oplus}$ in place of $\mathrm{BPP}^{\oplus\mathrm{P}}$, we do not have to deal with the promise nature of BPP and, more importantly, we can straightforwardly transform circuit lower bounds for constant depth circuits over the basis $\{\mathrm{AND}, \mathrm{OR}, \oplus\}$ into computations of $\mathrm{PH}_d^{\oplus}$ oracle Turing machines.

Furst, Saxe, and Sipser [FSS84] discovered the connection between computations of oracle Turing machines and circuits that allows one to transform lower bounds on the circuit complexity of boolean functions such as parity into separations of relativized PSPACE from the relativized polynomial hierarchy. (We adopt the convention that for relativizing PSPACE, the space bound of the oracle machine be also a bound on the length of queries it may ask, for without that convention the problem of separating PSPACE^A from PH^A becomes trivial, see [FSS84].) Sufficiently strong (i.e., exponential) lower bounds for parity were then provided by Yao [Yao85] and Håstad [Hås89], and were used to separate PSPACE^A

[2]In particular, due to these results, $\mathrm{PH}^{\oplus}$ in fact consists of only four levels not known to be the same: $\mathrm{PH}_0^{\oplus} = \mathrm{P}$, $\mathrm{PH}_1^{\oplus} = \mathrm{NP} \cup \mathrm{coNP} \cup \oplus\mathrm{P}, \ldots$, and $\mathrm{PH}_3^{\oplus} = \mathrm{PH}^{\oplus} = \mathrm{BPP}^{\oplus\mathrm{P}}$. Note also that in [Tod91], Toda preferred the operator-based notation, which due to the closure of $\oplus\mathrm{P}$ under Turing reductions is equivalent, i.e., $\mathrm{BP} \cdot \oplus\mathrm{P} = \mathrm{BPP}^{\oplus\mathrm{P}}$.

from PH^A. They also proved lower bounds for variations of the Sipser functions [Sip83a] to separate all levels of PH^A from each other (see also [Ko89]).

A technical prerequisite for this transformation to work is that the computation of any $\Sigma_i^{p,A}$ machine can be simulated by a $\Sigma_{i+1}^{p,A}$ machine that has the property that on all computation paths at most one query is asked and this query is asked at the end of the path (see [FSS84, Cor. 2.2]). An oracle machine having this property is said to be *weak*. Similarly, the computation of any $\mathrm{PH}_i^{\oplus,A}$ machine can be simulated by a weak $\mathrm{PH}_{i+1}^{\oplus,A}$ machine. The computation of a weak oracle machine M^A on some input x can then be associated with a circuit whose gates correspond to the nodes of the computation tree of $M^A(x)$, and whose inputs are the values $\chi_A(z)$ for all strings $z \in \Sigma^*$ that can be queried by $M^A(x)$. This correspondence can straightforwardly be extended to the case of weak $\mathrm{PH}^{\oplus,A}$ oracle machines and is formally stated in Proposition 3.5 below. The proof of Proposition 3.5 is standard (see, e.g., [FSS84, Lemma 2.3] and [Ko89, Lemma 2.1] for analogous results) and thus omitted. Let $\mathcal{CIR}(i,t)$ denote the collection of all depth $i+1$ circuits with AND, OR, and $\oplus$ gates, bottom fanin at most t, and fanin at most 2^t at all remaining levels.

Proposition 3.5 *Let A be any oracle and let M be any weak $\mathrm{PH}_i^{\oplus,A}$ oracle machine running in time p for some polynomial p. Then, for each $x \in \Sigma^*$ of length n, there exists a circuit $C_{M,x}$ in $\mathcal{CIR}(i,p(n))$ whose inputs are the values of $\chi_A(z)$ for all strings $z \in \Sigma^*$ with $|z| \leq p(n)$ such that $C_{M,x}$ outputs 1 if and only if M^A accepts x. In particular, it follows from the bounded depth and fanin of the circuits in $\mathcal{CIR}(i,p(n))$ that the size of circuit $C_{M,x}$ is bounded by $2^{s_M(n)}$ for some polynomial s_M depending on M.*

Now we are ready to prove our main result.

Proof of Theorem 3.1. For any set S, let

$$L_S \stackrel{\mathrm{df}}{=} \{0^N \mid N \geq 1 \text{ and the number of length } N \text{ strings in } S \text{ equals } 2^{N-1}\}.$$

Clearly, for each S, L_S is in $\mathrm{C}_{=}\mathrm{P}^S$.

We will construct the set A such that $L_A \in \mathrm{C}_{=}\mathrm{P}^A$ is $\mathrm{PH}^{\oplus,A}$-immune, i.e., L_A is infinite and no infinite subset of L_A is contained in $\mathrm{PH}^{\oplus,A}$. Since $\mathrm{BPP}^{\oplus\mathrm{P}} = \mathrm{PH}^{\oplus}$ holds true in the presence of any fixed oracle, this will prove the theorem. Also, since every $\mathrm{PH}_d^{\oplus,A}$ machine can be transformed into a weak $\mathrm{PH}_{d+1}^{\oplus,A}$ machine, it suffices to ensure in the construction of A that

(a) L_A is infinite, and

(b) for each weak $\mathrm{PH}^{\oplus,A}$ oracle machine M for which $L(M^A)$ is an infinite subset of L_A, it holds that M^A does not recognize L_A.

Fix an enumeration $M_1^{(\cdot)}, M_2^{(\cdot)}, \ldots$ of all weak $\mathrm{PH}^{\oplus,(\cdot)}$ oracle machines; we assume the machines to be clocked so that for each i, the runtime of machine $M_i^{(\cdot)}$ is bounded by $p_i(n) = n^i + i$ for inputs of length n. In particular, if $i = \langle d, j \rangle$, the ith machine $M_i^{(\cdot)}$ in this enumeration is the jth weak $\mathrm{PH}_d^{\oplus,(\cdot)}$ oracle machine, $M_{\langle d,j\rangle}^{(\cdot)}$, in the underlying enumeration of weak $\mathrm{PH}_d^{\oplus,(\cdot)}$ oracle machines. Satisfying Property (b) above then means to satisfy in the construction the following requirement R_i for each $i \geq 1$ for which M_i^A accepts an infinite subset of L_A:

$$R_i : \quad L(M_i^A) \cap \overline{L_A} \neq \emptyset.$$

We say that Requirement R_i is *satisfied* if, at some point in the construction of A, $L(M_i^A) \cap \overline{L_A} \neq \emptyset$ can be enforced.

As a technical detail that is often used in immunity constructions, we require our enumeration of machines to satisfy that for infinitely many indices i it holds that M_i^X accepts the empty set for every oracle X, which can be assumed without loss of generality. We will need this property in order to establish (a).

Now we give the construction of A, which proceeds in stages. In Stage i, the membership in A of all strings up to length t_i will be decided, and the previous initial segment of the oracle is extended to A_i. Strings of length $\leq t_i$ that are not explicitly added to A_i are never added to the oracle. We define A to be $\bigcup_{i\geq 0} A_i$. Initially, A_0 is set to the empty set and $t_0 = 0$. Also, throughout the construction, we keep a list $\mathcal{L}$ of unsatisfied requirements. Stage $i > 0$ is as follows.

Stage *i*. Add i to $\mathcal{L}$. Consider all machines $M_{\ell_1}^{(\cdot)}, \ldots, M_{\ell_m}^{(\cdot)}$ corresponding to indices ℓ_r that at this point are in $\mathcal{L}$. Let $k = \max\{d_r \mid \ell_r = \langle d_r, j_r\rangle \text{ and } 1 \leq r \leq m\}$ be the maximum level of the $\mathrm{PH}^{\oplus,(\cdot)}$ hierarchy to which these machines belong (not taking into account the collapse of $\mathrm{PH}^{\oplus} = \mathrm{BPP}^{\oplus\mathrm{P}}$ mentioned in Footnote 2). Let $\alpha_{k+2} > 0$ be the constant and $n_{k+2} \in \mathbb{N}$ be the number that exist for depth $k+2$ circuits according to Lemma 3.3. Choose $N = N_i > \max\{t_{i-1}, \log n_{k+2}\}$ to be the smallest integer such that

$$\alpha_{k+2} \cdot 2^{N/(2k+8)} > N + i + \sum_{r=1}^{m} s_{\ell_r}(N),$$

where the polynomials $s_{\ell_r} = s_{M_{\ell_r}}$ correspond to the machines with indices in $\mathcal{L}$ according to Proposition 3.5.

Distinguish two cases.

Case 1: There exists an r, $1 \leq r \leq m$, and an extension $E \subseteq \Sigma^N$ of A_{i-1} such that $0^N \notin L_E$ and yet $M_{\ell_r}^{A_{i-1}\cup E}$ accepts 0^N. Let $\tilde{r}$ be the smallest such r. Cancel $\ell_{\tilde{r}}$ from $\mathcal{L}$, set A_i to $A_{i-1} \cup E$, and set t_i to $p_i(N)$. Note that Requirement $R_{\ell_{\tilde{r}}}$ has been satisfied at this stage.

Case 2: For all r, $1 \leq r \leq m$, and for all extensions $E \subseteq \Sigma^N$ of A_{i-1}, $0^N \notin L_E$ implies that $M_{\ell_r}^{A_{i-1}\cup E}$ rejects 0^N. In this case, no requirement can be satisfied at this stage. However, to achieve Property (a), we will force 0^N into L_A. Choose some extension $\tilde{E} \subseteq \Sigma^N$ of A_{i-1} such that (i) the number of length N strings in $\tilde{E}$ equals 2^{N-1}, and (ii) for each r, $1 \le r \le m$, $M_{\ell_r}^{A_{i-1} \cup \tilde{E}}$ rejects 0^N. We will argue later (in Claim 1 below) that such an extension $\tilde{E}$ exists. Set A_i to $A_{i-1} \cup \tilde{E}$ and set t_i to $p_i(N)$.

End of Stage i.

Note that by the definition of t_i and by our choice of N_i, the oracle extension in Stage i does not injure the computations considered in earlier stages. Thus,

(1) $\qquad (\forall i \ge 1) \qquad [0^{N_i} \in L_{A_i} \iff 0^{N_i} \in L_A]$, and

(2) $\qquad (\forall i, j \ge 1) \qquad [M_j^{A_i} \text{ accepts } 0^{N_i} \iff M_j^A \text{ accepts } 0^{N_i}]$.

The correctness of the construction will now follow from the following claims.

Claim 1. For each $i \ge 1$, there exists an oracle extension $\tilde{E}$ satisfying (i) and (ii) in Case 2 of Stage i.

Proof of Claim 1. Consider Stage i. For each $r \in \{1, \dots, m\}$, let $C_{M_{\ell_r}, 0^N}$ be the circuit that, according to Proposition 3.5, corresponds to the computation of M_{ℓ_r} running on input 0^N. Fix all inputs to these circuits except those of length N consistently with A_{i-1}. That is, for each $r \in \{1, \dots, m\}$, substitute in $C_{M_{\ell_r}, 0^N}$ the value $\chi_{A_{i-1}}(z)$ for all inputs corresponding to strings z with $|z| \le t_{i-1}$, and substitute the value 0 for all inputs corresponding to strings z with $t_{i-1} < |z| \le t_i$ and $|z| \ne N$. Call the resulting circuits $\widehat{C}_{\ell_1, 0^N}, \dots, \widehat{C}_{\ell_m, 0^N}$. By Proposition 3.5, for each r, $\widehat{C}_{\ell_r, 0^N}$ is in $\mathcal{CIR}(k, p_{\ell_r}(N))$, its 2^N inputs correspond to the length N strings, and for each $E \subseteq \Sigma^N$, it holds that

(3) $\qquad \widehat{C}_{\ell_r, 0^N}$ on input $\chi_E(0^N) \cdots \chi_E(1^N)$ outputs 1 $\iff$ $M_{\ell_r}^{A_{i-1} \cup E}$ accepts 0^N.

Create a new circuit $C_{2^N} = \mathrm{OR}_{r=1}^m \widehat{C}_{M_{\ell_r}, 0^N}$ whose 2^N inputs correspond to the length N strings and whose output gate is an OR gate over the subcircuits $\widehat{C}_{\ell_1, 0^N}, \dots, \widehat{C}_{\ell_m, 0^N}$. Thus, C_{2^N} is a depth $k+2$ circuit with AND, OR, and $\oplus$ gates whose size is bounded by

$$1 + \sum_{r=1}^{m} 2^{s_{\ell_r}(N)} \le 2^{i + \sum_{r=1}^m s_{\ell_r}(N)}$$

(note that $m \le i$). By our choice of N, we have $2^N > n_{k+2}$ and

$$2^{i + \sum_{r=1}^m s_{\ell_r}(N)} < 2^{-N} \cdot 2^{\alpha_{k+2}(2^N)^{1/(2k+8)}}.$$

Thus, by Lemma 3.3, circuit C_{2^N} cannot compute the function $\mathrm{EQU}_{2^N}^{\mathrm{half}}$ correctly for all inputs. Since by the condition stated in Case 2 and by Equivalence (3) above, C_{2^N} behaves correctly for all inputs corresponding to any set E of length N strings with $0^N \notin L_E$, it follows that C_{2^N} must be incorrect on an input corresponding to some set $\tilde{E}$ of length N strings with $0^N \in L_{\tilde{E}}$, i.e., C_{2^N} on input $\chi_{\tilde{E}}(0^N)\cdots\chi_{\tilde{E}}(1^N)$ outputs 0. Since C_{2^N} is the OR of its subcircuits, each subcircuit outputs 0 on this input. Thus, Equivalence (3) implies that for each r, $1 \leq r \leq m$, $M_{\ell_r}^{A_{i-1}\cup\tilde{E}}$ rejects 0^N. $\blacksquare_{\text{Claim 1}}$

Claim 2. L_A is an infinite set.

Proof of Claim 2. Recall our assumption that the index set of the empty set is infinite. Since no requirement R_i for which i is an index of the empty set can ever be satisfied and since, by construction, some requirement is satisfied whenever Case 1 occurs, this assumption implies that Case 2 must happen infinitely often. By construction, some string is forced into L_A whenever Case 2 occurs. Hence, L_A is an infinite set. This proves the claim and establishes Property (a). $\blacksquare_{\text{Claim 2}}$

Claim 3. For every $i \geq 1$, M_i^A does not accept an infinite subset of L_A.

Proof of Claim 3. For each i, Requirement R_i either is satisfied at some stage of the construction, or is never satisfied. If R_i is satisfied at Stage j, then Case 1 happens in Stage j, and so $0^{N_j} \in L(M_i^{A_j}) \cap \overline{L_{A_j}}$. By Equivalences (1) and (2), $0^{N_j} \in L(M_i^A) \cap \overline{L_A}$, so $L(M_i^A) \not\subseteq L_A$. Now suppose that Requirement R_i is never satisfied. We will argue that $L(M_i^A) \cap L_A$ then is a finite set. By construction, since we added to A only strings of lengths N_j, where $j \geq 1$ and N_j is the integer chosen in Stage j, L_A contains only strings of the form 0^{N_j} for some $j \geq 1$. Note that i is added to $\mathcal{L}$ in Stage i and will stay there forever. For each $j \geq i$, if $0^{N_j} \in L_A$ (and thus $0^{N_j} \in L_{A_j}$ by (1)), then Case 2 must have occurred in Stage j. Consequently, $M_i^{A_j}$ (and thus M_i^A by (2)) rejects 0^{N_j} for every $j \geq i$. It follows that for each i, $L(M_i^A) \cap L_A$ has at most $i-1$ elements, proving the claim. $\blacksquare_{\text{Claim 3}}$

Hence, L_A is a $\mathrm{BPP}^{\oplus\mathrm{P}^A}$-immune set in $\mathrm{C}_=\mathrm{P}^A$. $\blacksquare$

In particular, Theorem 3.1 immediately gives the following corollary. All strong separations in Corollary 3.6 are new, except the PH^A-immunity of PSPACE^A (and of $\mathrm{P}^{\mathrm{PP}^A}$, since $(\forall B)\,[\oplus\mathrm{P}^B \subseteq \mathrm{P}^{\mathrm{PP}^B}]$), which is also stated (or is implicit) in [Ko90,Bru92], and except the BPP^C-immunity of PP^C (and its superclasses) proven in [BR88]. We also mention that Bovet et al. [BCS92] noted that PP^D strongly separates from $\Sigma_2^{p,D}$ for some oracle D.

Corollary 3.6 *Let $\mathcal{C}_1$ be any class chosen among* $\mathrm{C}_=\mathrm{P}$, PP, $\mathrm{P}^{\mathrm{C}_=\mathrm{P}}$, P^{PP}, *and* PSPACE, *and let $\mathcal{C}_2$ be any class chosen among* $\mathrm{BPP}^{\oplus\mathrm{P}}$, BPP, PH, *and* $\oplus\mathrm{P}$. *There exists some oracle A such that $\mathcal{C}_1^A$ contains a $\mathcal{C}_2^A$-immune set.*

What about the converse direction? Does $\mathrm{BPP}^{\oplus\mathrm{P}}$, or even some smaller class, contain a $\mathrm{C}_=\mathrm{P}$-immune, or even a PP-immune, set relative to some oracle? Note that Torán [Tor88, Tor91] provided a simple separation of this kind: There exists an oracle A such that $\mathrm{NP}^A \not\subseteq \mathrm{C}_=\mathrm{P}^A$ (see [Bei91] for a simplification of the proof of Torán's result). We strengthen this result by showing that the separation is witnessed by a $\mathrm{C}_=\mathrm{P}^B$-immune set in NP^B for another oracle set B. Indeed, the only property of $\mathrm{C}_{=}\mathrm{P}$ needed to obtain a relativized separation from NP with immunity is that $\mathrm{C}_{=}\mathrm{P}$ is closed under finite unions,[3] and this closure property relativizes.

Lemma 3.7 *For every oracle A, $\mathrm{C}_{=}\mathrm{P}^A$ is closed under finite unions. That is, given a finite collection $N_1, N_2, \ldots, N_k$ of NPOTMs, there exists an NPOTM N such that for each input x, N^A accepts x (in the sense of $\mathrm{C}_{=}\mathrm{P}$) if and only if for some j, N_j^A accepts x (in the sense of $\mathrm{C}_{=}\mathrm{P}$), i.e., for each $x \in \Sigma^*$,*

$$\mathrm{acc}_{N^A}(x) = \mathrm{rej}_{N^A}(x) \iff (\exists j : 1 \leq j \leq k)\, [\mathrm{acc}_{N_j^A}(x) = \mathrm{rej}_{N_j^A}(x)].$$

Theorem 3.8 *There exists some oracle B such that NP^B contains a $\mathrm{C}_{=}\mathrm{P}^B$-immune set.*

Proof. The witness set here will be L_B, where for any set S,

$$L_S \stackrel{\mathrm{df}}{=} \{0^n \mid n \geq 1 \text{ and there exists a string of length } n \text{ in } S\}$$

is a set in NP^S. Fix an enumeration $N_1^{(\cdot)}, N_2^{(\cdot)}, \ldots$ of all NPOTMs, again having the property that for infinitely many indices the machine with that index accepts the empty set regardless of the oracle. (Throughout this proof, "acceptance" means "$\mathrm{C}_{=}\mathrm{P}$ acceptance" as in Lemma 3.7.) As in the proof of Theorem 3.1, we try to satisfy for each $i \geq 1$ for which N_i^B accepts an infinite subset of L_B, the requirement

$$R_i : \quad L(N_i^B) \cap \overline{L_B} \neq \emptyset.$$

Again, the stage-wise construction of $B = \bigcup_{i \geq 0} B_i$ is initialized by setting B_0 to the empty set and the restraint function t_0 to 0, and we keep a list $\mathcal{L}$ of currently unsatisfied requirements. Stage $i > 0$ is as follows.

Stage *i*. Add i to $\mathcal{L}$. Consider all machines $N_{\ell_1}^{(\cdot)}, \ldots, N_{\ell_m}^{(\cdot)}$ corresponding to indices ℓ_r that at this point are in $\mathcal{L}$. Let $N_{\mathcal{L}}^{(\cdot)}$ be the machine that exists for $N_{\ell_1}^{(\cdot)}, \ldots, N_{\ell_m}^{(\cdot)}$ by Lemma 3.7, i.e., for every oracle Z and for each input x,

$$N_{\mathcal{L}}^Z \text{ accepts } x \iff (\exists r : 1 \leq r \leq m)\, [N_{\ell_r}^Z \text{ accepts } x]. \tag{4}$$

Let $p_{\mathcal{L}}$ be the polynomial bounding the runtime of $N_{\mathcal{L}}^{(\cdot)}$. Choose $n = n_i > t_{i-1}$ to be the smallest integer such that $2^n > 2p_{\mathcal{L}}(n)$. Choose an oracle extension $E \subseteq \Sigma^n$ of B_{i-1} such that

$$E = \emptyset \iff N_{\mathcal{L}}^{B_{i-1} \cup E} \text{ accepts } 0^n. \tag{5}$$

[3]It is known that $\mathrm{C}_{=}\mathrm{P}$ is closed even under polynomial-time "positive" Turing reductions, which is implicit in the methods of [GNW90], as has been noted in [Rot93] for the positive truth-table case; the same result was noted independently in [BCO93]. We refer to those sources for a proof of Lemma 3.7.

It has been shown in [Bei91] that an oracle extension E satisfying (5) exists if n is chosen as above. Set B_i to $B_{i-1} \cup E$ and set t_i to $p_{\mathcal{L}}(n)$. If the extension E chosen is the empty set, then by (5) and (4), there exists an r, $1 \leq r \leq m$, such that $N_{\ell_r}^{B_{i-1}}$ accepts 0^n. Let $\tilde{r}$ be the smallest such r, and cancel $\ell_{\tilde{r}}$ from $\mathcal{L}$.

End of Stage i.

Note that if we have chosen $E = \emptyset$ in Stage i, then $0^n \notin L_E$ and Requirement $R_{\ell_{\tilde{r}}}$ has been satisfied. On the other hand, if $E \neq \emptyset$, then by (5) and (4), we have ensured that (i) $0^n \in L_E$, and (ii) for each r, $1 \leq r \leq m$, $N_{\ell_r}^{B_{i-1}\cup E}$ rejects 0^n. Now, an argument analogous to Claims 2 and 3 in the proof of Theorem 3.1 shows that L_B is a $\mathrm{C}_=\mathrm{P}^B$-immune set in NP^B, completing the proof. ∎

Similarly, there exists some oracle C such that NP^C (and thus PH^C and PP^C) has a $\oplus\mathrm{P}^C$-immune set—this result was obtained by Bovet et al. [BCS92], based on their sufficient condition for proving relativized strong separations and on Torán's simple separation of NP and $\oplus$P [Tor91].

Since the inclusions NP $\subseteq$ PP and coNP $\subseteq$ $\mathrm{C}_=\mathrm{P}$ hold relative to every fixed oracle, Theorem 3.8 immediately gives the following corollaries.

Corollary 3.9 *There exists some oracle B such that PP^B contains a $\mathrm{C}_=\mathrm{P}^B$-immune set.*

Recall from the introduction that for any complexity class $\mathcal{C}$, a set is said to be *simple* for $\mathcal{C}$ (or $\mathcal{C}$-*simple*) if it belongs to $\mathcal{C}$ and its complement is $\mathcal{C}$-immune. Homer and Maass [HM83] proved the existence of a recursively enumerable set A such that NP^A contains a simple set, and Balcázar [Bal85] improved this result by making A recursive via a novel and very elegant trick: his construction starts with a *full* oracle instead of an empty oracle and then proceeds by *deleting* strings from it. Balcázar's result in turn was generalized by Torenvliet and van Emde Boas [Tor86,TvEB89] to the second level and by Bruschi [Bru92] to all levels of the polynomial hierarchy. Balcázar and Russo [BR88] also proved (relative to some oracle) the existence of a simple set in the one-sided error probabilistic class R, which is contained in NP $\cap$ BPP. Our result below that $\mathrm{C}_=\mathrm{P}$ has a simple set in some relativization (all our oracles are recursive) extends those previous simplicity results that each are restricted to classes contained in the polynomial hierarchy. Since of the classes we consider (PH, PP, $\oplus$P, and $\mathrm{C}_=\mathrm{P}$), all classes except $\mathrm{C}_=\mathrm{P}$ are known to be closed under complement, $\mathrm{C}_=\mathrm{P}$ is the only class for which it makes sense to ask about the existence of simple sets.

Corollary 3.10 *There exists some oracle B such that $\mathrm{C}_=\mathrm{P}^B$ contains a simple set.*

Proof. Let B be the oracle constructed in the proof of Theorem 3.8 and let L_B be the witness set of this proof. Consider the complement $\overline{L_B}$ of L_B in Σ^*. Since $L_B \in \mathrm{NP}^B$, $\overline{L_B}$ is in coNP^B and thus in $\mathrm{C}_=\mathrm{P}^B$. It has been shown in the proof of Theorem 3.8 that L_B, the complement of $\overline{L_B}$, is an infinite set having no infinite subset in $\mathrm{C}_=\mathrm{P}^B$. That is, $\overline{L_B}$ is $\mathrm{C}_=\mathrm{P}^B$-simple. ∎

4 Immunity Results for $\oplus$P and the PP$^{\text{PH}}$ Hierarchy

The last section in particular showed that, in suitable relativizations, $\mathrm{C}_{=}\mathrm{P}$ (and thus PP) is immune to both PH and $\oplus$P (Corollary 3.6), and NP (and thus PH and PP) is immune to $\mathrm{C}_{=}\mathrm{P}$ (Theorem 3.8 and Corollary 3.9) and to $\oplus$P [BCS92]. In this section, we will prove the existence of oracles relative to which P^{NP} (and thus PH) is immune to PP, and relative to which $\oplus$P is immune to $\mathrm{PP}^{\mathrm{PH}}$. The latter result strengthens the previously known (relativized) strong separation of $\oplus$P from PH [Ko90] (cf. [Bru92]), and it also implies the new (relativized) strong separation of $\oplus$P from PP. Noticing that $\mathrm{C}_{=}\mathrm{P} \subseteq \mathrm{PP}$ holds in all relativizations, we thus have settled all possible (relativized) strong separation questions involving any pair of classes chosen among PH, PP, $\oplus$P, and $\mathrm{C}_{=}\mathrm{P}$, as claimed earlier.

We show these remaining results by improving known (relativized) simple separations to strong ones. The simple separation $(\exists A)\,[\oplus\mathrm{P}^A \not\subseteq \mathrm{PP}^A]$ [Tor88,Tor91] (see also [Bei91]) was strengthened by Green to $(\exists B)\,[\oplus\mathrm{P}^B \not\subseteq \mathrm{PP}^{\mathrm{PH}^B}]$ [Gre91].

Since the analog of Lemma 3.7 as well holds for PP (in fact, PP is closed under polynomial-time truth-table reductions [FR91], and this proof relativizes), the following theorem can be shown by the technique used to prove Theorem 3.8. First, we state the analog of Lemma 3.7 in terms of weak $\mathrm{PP}^{\mathrm{PH}}$ oracle machines. The proof of this lemma simply follows from the relativized version of the proof that PP is closed under finite unions, which is a special case of its closure under truth-table reductions [FR91].

Lemma 4.1 *Let A be any oracle and $d \geq 0$ be any integer. Given any finite collection $N_1, N_2, \ldots, N_k$ of weak $\mathrm{PP}^{\mathrm{PH}}$ oracle machines, there exists a weak $\mathrm{PP}^{\mathrm{PH}}$ oracle machine N such that for each input x, N^A accepts x if and only if for some j, $1 \leq j \leq k$, N_j^A accepts x.*

Theorem 4.2 *There exists some oracle D such that $\oplus\mathrm{P}^D$ (and thus $\mathrm{P}^{\mathrm{PP}^D}$ and PSPACE^D) contains a $\mathrm{PP}^{\mathrm{PH}^D}$-immune set.*

Proof. Since the proof is very similar to that of Theorem 3.8, we only mention the differences. The witness set here will be L_D, where for any set S,

$$L_S \stackrel{\text{df}}{=} \{0^n \mid n \geq 1 \text{ and there exists an odd number of length } n \text{ strings in } S\}$$

is a set in $\oplus\mathrm{P}^S$. Now, $N_1^{(\cdot)}, N_2^{(\cdot)}, \ldots$ is an enumeration of all weak $\mathrm{PP}^{\mathrm{PH}^{(\cdot)}}$ oracle machines, and "acceptance" refers to such machines. In Stage i of the construction, we again consider all machines $N_{\ell_1}^{(\cdot)}, \ldots, N_{\ell_m}^{(\cdot)}$ corresponding to indices ℓ_r that at this point are in the list $\mathcal{L}$ of currently unsatisfied requirements, and the machine $N_{\mathcal{L}}^{(\cdot)}$ (with polynomial time bound $p_{\mathcal{L}}$) that exists for them by Lemma 4.1. Assume $N_{\mathcal{L}}^{(\cdot)}$ is a $\mathrm{PP}^{\Sigma_d^{p,(\cdot)}}$ machine, and let c_d be the constant that exists for such machines by [Gre91, Thm. 5]. Then, as shown in [Gre91, Thm. 7], choosing $n = n_i > t_{i-1}$ to be the smallest integer such that

$$2p_{\mathcal{L}}(n) \leq \min\{(2^n)^{1/d^2}, c_d 2^{n(d+1)/d^2} - 1\}$$

implies that there exists an extension $E \subseteq \Sigma^n$ of the oracle as constructed so far, D_{i-1}, such that $0^n \in L_E$ if and only if $N_{\mathcal{L}}^{D_{i-1}\cup E}$ rejects 0^n. ∎

Corollary 4.3 *There exists some oracle D such that $\oplus\mathrm{P}^D$ contains a set immune to PP^D and to PH^D.*

By essentially the same arguments, also the very recent result of Berg and Ulfberg [BU] that there is an oracle relative to which the levels of the $\mathrm{PP}^{\mathrm{PH}} = \bigcup_{d\geq 0} \mathrm{PP}^{\Sigma_d^p}$ hierarchy separate (which generalizes Beigel's result that $(\exists A)\,[\mathrm{P}^{\mathrm{NP}^A} \not\subseteq \mathrm{PP}^A]$ [Bei94]) can be strengthened to level-wise strong separations of this hierarchy. The proof of Theorem 4.4 is omitted, since it is very similar to the previous proofs, the only difference being that it is based on the construction given in [BU]. The interested reader is referred to [Rot98] for a complete proof of this result.

Theorem 4.4 *For any $d \geq 1$, there exists some oracle F such that $\mathrm{P}^{\Sigma_d^{p,F}}$ contains a $\mathrm{PP}^{\Sigma_{d-1}^{p,F}}$-immune set. In particular, $\mathrm{P}^{\mathrm{NP}^F}$ (and thus PH^F) has a PP^F-immune set.*

5 Conclusions and Open Problems

In this paper, we have shown that all possible relativized separations involving the polynomial hierarchy and the counting classes $\mathrm{C}_=\mathrm{P}$, PP, and $\oplus$P can be made strong. In particular, we have extended to these counting classes previously known strong separations of Ko [Ko90] and Bruschi [Bru92], and we have strengthened to strong separations previously known simple separations of Torán [Tor88,Tor91], Green [Gre91], and Berg and Ulfberg [BU]. We have also shown that $\mathrm{C}_=\mathrm{P}$ contains a simple set relative to some oracle, complementing the corresponding results of Balcázar and Russo [Bal85,BR88] for NP and R, and of Torenvliet and van Emde Boas [Tor86,TvEB89] and Bruschi [Bru92] for Σ_k^p, $k > 1$. However, many questions remain open. The most obvious question is whether these immunity results can be strengthened to bi-immunity or even to balanced immunity (see, e.g., [HZ96]).

Regarding the existence of simple sets in $\mathrm{C}_=\mathrm{P}^B$, note that our construction of B can easily be interleaved with other immunity oracle constructions to show results such as: There exists an oracle A such that $\mathrm{C}_=\mathrm{P}^A$ contains a simple set and another set that is P^A-immune (see [Bal85] for the analogous result for NP). Torenvliet and van Emde Boas [Tor86, TvEB89] have even constructed an oracle relative to which NP contains a language that *simultaneously* is simple and P-immune. Can this also be shown to hold for $\mathrm{C}_=\mathrm{P}$?

Our main result that there exists some A such that $\mathrm{C}_=\mathrm{P}^A$ contains a $\mathrm{BPP}^{\oplus\mathrm{P}^A}$-immune set is optimal in the sense that for all oracles B, $\mathrm{C}_=\mathrm{P}^B$ clearly is contained in PP^B and thus in $\mathrm{PP}^{\oplus\mathrm{P}^B}$. However, it is also known that $\mathrm{BPP}^{\oplus\mathrm{P}} \subseteq \mathrm{Almost}[\oplus\mathrm{P}]$ [TO92,RR95], where for any relativized class $\mathcal{C}$, $\mathrm{Almost}[\mathcal{C}]$ denotes the class of languages L such that for almost all oracle sets X, L is in $\mathcal{C}^X$ [NW94]. It is an open problem (see [RR95]) whether $\mathrm{BPP}^{\oplus\mathrm{P}} = \mathrm{Almost}[\oplus\mathrm{P}]$, so it is possible that Almost[$\oplus$P] is a strictly larger class than $\mathrm{BPP}^{\oplus\mathrm{P}}$. It is unlikely that $\mathrm{C}_=\mathrm{P}$ is contained in Almost[$\oplus$P]. Is there an oracle relative to which $\mathrm{C}_=\mathrm{P}$ is even immune to Almost[$\oplus$P]? We conjecture that this is the case. Relatedly, can any of the immunity results of this paper be shown to hold with probability 1 relative to a random oracle?

Acknowledgments. I am very grateful to Lane Hemaspaandra for his constant and warm encouragement, for many incisive comments and important suggestions that have much improved this paper, and for careful proofreading. Interesting and helpful discussions with Gerd Wechsung and Eric Allender are also acknowledged. I thank Christer Berg and Staffan Ulfberg for providing me with an advance copy of their paper [BU].

References

[Bal85] J. Balcázar. Simplicity, relativizations and nondeterminism. *SIAM Journal on Computing*, 14(1):148–157, 1985.

[BCO93] R. Beigel, R. Chang, and M. Ogiwara. A relationship between difference hierarchies and relativized polynomial hierarchies. *Mathematical Systems Theory*, 26(3):293–310, 1993.

[BCS92] D. Bovet, P. Crescenzi, and R. Silvestri. A uniform approach to define complexity classes. *Theoretical Computer Science*, 104(2):263–283, 1992.

[BDG88] J. Balcázar, J. Díaz, and J. Gabarró. *Structural Complexity I*. EATCS Monographs in Theoretical Computer Science. Springer-Verlag, 1988.

[Bei91] R. Beigel. Relativized counting classes: Relations among thresholds, parity, and mods. *Journal of Computer and System Sciences*, 42(1):76–96, 1991.

[Bei94] R. Beigel. Perceptrons, PP, and the polynomial hierarchy. *Computational Complexity*, 4(4):339–349, 1994.

[BG81] C. Bennett and J. Gill. Relative to a random oracle A, $\mathrm{P}^A \neq \mathrm{NP}^A \neq \mathrm{coNP}^A$ with probability 1. *SIAM Journal on Computing*, 10(1):96–113, 1981.

[BGS75] T. Baker, J. Gill, and R. Solovay. Relativizations of the P=?NP question. *SIAM Journal on Computing*, 4(4):431–442, 1975.

[BJY90] D. Bruschi, D. Joseph, and P. Young. Strong separations for the boolean hierarchy over RP. *International Journal of Foundations of Computer Science*, 1(3):201–218, 1990.

[BR88] J. Balcázar and D. Russo. Immunity and simplicity in relativizations of probabilistic complexity classes. *R.A.I.R.O. Theoretical Informatics and Applications*, 22(2):227–244, 1988.

[Bru92] D. Bruschi. Strong separations of the polynomial hierarchy with oracles: Constructive separations by immune and simple sets. *Theoretical Computer Science*, 102(2):215–252, 1992.

[BU] C. Berg and S. Ulfberg. A lower bound for perceptrons and an oracle separation of the $\mathrm{PP}^{\mathrm{PH}}$ hierarchy. *Journal of Computer and System Sciences.* To appear. A preliminary version appeared in the *Proceedings of the 12th Annual IEEE Conference on Computational Complexity*, pages 165–172. IEEE Computer Society Press, 1997.

[EHTY92] D. Eppstein, L. Hemachandra, J. Tisdall, and B. Yener. Simultaneous strong separations of probabilistic and unambiguous complexity classes. *Mathematical Systems Theory*, 25(1):23–36, 1992.

[FR91] L. Fortnow and N. Reingold. PP is closed under truth-table reductions. In *Proceedings of the 6th Structure in Complexity Theory Conference*, pages 13–15. IEEE Computer Society Press, June/July 1991.

[FSS84] M. Furst, J. Saxe, and M. Sipser. Parity, circuits, and the polynomial-time hierarchy. *Mathematical Systems Theory*, 17(1):13–27, 1984.

[Gil77] J. Gill. Computational complexity of probabilistic Turing machines. *SIAM Journal on Computing*, 6(4):675–695, 1977.

[GNW90] T. Gundermann, N. Nasser, and G. Wechsung. A survey on counting classes. In *Proceedings of the 5th Structure in Complexity Theory Conference*, pages 140–153. IEEE Computer Society Press, July 1990.

[GP86] L. Goldschlager and I. Parberry. On the construction of parallel computers from various bases of boolean functions. *Theoretical Computer Science*, 43(1):43–58, 1986.

[Gre91] F. Green. An oracle separating $\oplus\mathrm{P}$ from $\mathrm{PP}^{\mathrm{PH}}$. *Information Processing Letters*, 37(3):149–153, 1991.

[Hås89] J. Håstad. Almost optimal lower bounds for small depth circuits. In S. Micali, editor, *Randomness and Computation,* volume 5 of *Advances in Computing Research*, pages 143–170. JAI Press, Greenwich, 1989.

[HM83] S. Homer and W. Maass. Oracle dependent properties of the lattice of NP sets. *Theoretical Computer Science*, 24(3):279–289, 1983.

[HRW97] L. Hemaspaandra, J. Rothe, and G. Wechsung. Easy sets and hard certificate schemes. *Acta Informatica*, 34(11):859–879, 1997.

[HU79] J. Hopcroft and J. Ullman. *Introduction to Automata Theory, Languages, and Computation.* Addison-Wesley, 1979.

[HZ96] L. Hemaspaandra and M. Zimand. Strong self-reducibility precludes strong immunity. *Mathematical Systems Theory*, 29(5):535–548, 1996.

[Ko89] K. Ko. Relativized polynomial time hierarchies having exactly k levels. *SIAM Journal on Computing*, 18(2):392–408, 1989.

[Ko90] K. Ko. A note on separating the relativized polynomial time hierarchy by immune sets. *R.A.I.R.O. Theoretical Informatics and Applications*, 24(3):229–240, 1990.

[Lau83] C. Lautemann. BPP and the polynomial hierarchy. *Information Processing Letters*, 17(4):215–217, 1983.

[Lis] G. Lischke. Towards the actual relationship between NP and exponential time. *Mathematical Logic Quarterly*. To appear. A preliminary version has appeared as: Impossibilities and possibilities of weak separation between NP and exponential time. In *Proceedings of the 5th Structure in Complexity Theory Conference*, pages 245–253. IEEE Computer Society Press, 1990.

[MS72] A. Meyer and L. Stockmeyer. The equivalence problem for regular expressions with squaring requires exponential space. In *Proceedings of the 13th IEEE Symposium on Switching and Automata Theory*, pages 125–129, 1972.

[NW94] N. Nisan and A. Wigderson. Hardness vs randomness. *Journal of Computer and System Sciences*, 49(2):149–167, 1994.

[Pap94] C. Papadimitriou. *Computational Complexity*. Addison-Wesley, 1994.

[PZ83] C. Papadimitriou and S. Zachos. Two remarks on the power of counting. In *Proceedings of the 6th GI Conference on Theoretical Computer Science*, pages 269–276. Springer-Verlag *Lecture Notes in Computer Science #145*, 1983.

[Raz87] A. A. Razborov. Lower bounds on the size of bounded depth circuits over a complete basis with logical addition. *Mat. Zametki*, 41(4):598–607, 1987. In Russian. English Translation in *Mathematical Notes of the Academy of Sciences of the USSR*, 41(4):333–338, 1987.

[Rot93] J. Rothe. Some closure properties of GAP-definable classes. Technical Report TR Math/93/6, Friedrich-Schiller-Universität Jena, Jena, Germany, 1993. Appeared as part of: A promise class at least as hard as the polynomial hierarchy. In *Proceedings of the 6th International Conference on Computing and Information*, pages 92–107, 1994.

[Rot98] J. Rothe. Immunity and simplicity for exact counting and other counting classes. Technical Report TR 679, University of Rochester, Rochester, NY, January 1998.

[RR95] K. Regan and J. Royer. On closure properties of bounded two-sided error complexity classes. *Mathematical Systems Theory*, 28(3):229–243, 1995.

[SB84] U. Schöning and R. Book. Immunity, relativization, and nondeterminism. *SIAM Journal on Computing*, 13(2):329–337, 1984.

[Sim75] J. Simon. *On Some Central Problems in Computational Complexity*. PhD thesis, Cornell University, Ithaca, NY, January 1975. Available as Cornell Department of Computer Science Technical Report TR75-224.

[Sip83a] M. Sipser. Borel sets and circuit complexity. In *Proceedings of the 15th ACM Symposium on Theory of Computing*, pages 61–69, 1983.

[Sip83b] M. Sipser. A complexity theoretic approach to randomness. In *Proceedings of the 15th ACM Symposium on Theory of Computing*, pages 330–335, 1983.

[Smo87] R. Smolensky. Algebraic methods in the theory of lower bounds for boolean circuit complexity. In *Proceedings of the 19th ACM Symposium on Theory of Computing*, pages 77–82. ACM Press, May 1987.

[Sto77] L. Stockmeyer. The polynomial-time hierarchy. *Theoretical Computer Science*, 3(1):1–22, 1977.

[TO92] 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.

[Tod91] S. Toda. PP is as hard as the polynomial-time hierarchy. *SIAM Journal on Computing*, 20(5):865–877, 1991.

[Tor86] L. Torenvliet. *Structural Concepts in Relativised Hierarchies*. PhD thesis, Universiteit van Amsterdam, Amsterdam, The Netherlands, 1986.

[Tor88] J. Torán. *Structural Properties of the Counting Hierarchies*. PhD thesis, Universitat Politècnica de Catalunya, Barcelona, Spain, 1988.

[Tor91] J. Torán. Complexity classes defined by counting quantifiers. *Journal of the ACM*, 38(3):753–774, 1991.

[TvEB89] L. Torenvliet and P. van Emde Boas. Simplicity, immunity, relativizations and nondeterminism. *Information and Computation*, 80(1):1–17, 1989.

[Wag86] K. Wagner. The complexity of combinatorial problems with succinct input representations. *Acta Informatica*, 23:325–356, 1986.

[Wra77] C. Wrathall. Complete sets and the polynomial-time hierarchy. *Theoretical Computer Science*, 3:23–33, 1977.

[Yao85] A. Yao. Separating the polynomial-time hierarchy by oracles. In *Proceedings of the 26th IEEE Symposium on Foundations of Computer Science*, pages 1–10. IEEE Computer Society Press, 1985.