Relativized Counting Classes: Relations among Thresholds, Parity, and Mods

Richard Beigel*
Dept. of Computer Science
51 Prospect Street
P.O. Box 2158, Yale Station
Yale University
New Haven, CT 06520-2158

January 31, 1990

Abstract

Well known complexity classes such as NP, co-NP, $\oplus$P (PARITY-P), and PP are produced by considering a nondeterministic polynomial time Turing machine N and defining acceptance in terms of the number of accepting paths in N. That is, they are subclasses of $\mathrm{P}^{\#\mathrm{P}[1]}$. Other interesting classes such as $\mathrm{MOD}_k\mathrm{P}$ and $\mathrm{C}_=\mathrm{P}$ are also subclasses of $\mathrm{P}^{\#\mathrm{P}[1]}$. Many relations among these classes are unresolved. Of course, these classes coincide if P = PSPACE. However, we develop a simple combinatorial technique for constructing oracles that separate counting classes. Our results suggest that it will be difficult to resolve the unknown relationships among different counting classes. In addition to presenting new oracle separations, we simplify several previous constructions.

1. Introduction

In [26], Valiant defined the class #P of counting functions.

Definition 1 [Valiant] #P is the class of functions for which there exists a nondeterministic polynomial-time Turing machine N such that $f(x)$ is the number of accepting computations of machine N on input x.

Many classes of languages, such as NP, PP [11], US [6], and $\oplus$P [12, 18] are contained in $\mathrm{P}^{\#\mathrm{P}[1]}$, the class of languages computable in polynomial time by making

*Research performed at the Johns Hopkins University. Supported in part by grants CCR-8808949 and CCR-8958528 from the National Science Foundation.

one query to a function in #P. The class $\mathrm{MOD}_k\mathrm{P}$, also contained in $\mathrm{P}^{\#\mathrm{P}[1]}$, is a generalization of $\oplus\mathrm{P}$ that has only recently begun to receive significant attention ([3, 8] and implicitly [21]). While some relations among counting classes were established in [3], many relations are still unknown. Therefore, we turn to relativizations in order to suggest which relations will be hard to establish. In this paper, we separate $\mathrm{MOD}_k\mathrm{P}$ from several other counting classes via an oracle, and we simplify several constructions that were previously known. In Section 8., we also obtain some interesting oracle separations involving R and UP.

2. Preliminaries

We assume a basic familiarity with oracle Turing machines (see [1]). We present some notation:

Notation 2

- Fix a two-character alphabet Σ (except where otherwise specified).
- $|x|$ denotes the length of the string x.
- $A^{[n]} = \{x \in A : |x| = n\}$.
- $A(x)$ denotes the characteristic function of the set A: 1 if $x \in A$, 0 if $x \notin A$.
- $|A|$ denotes the cardinality of the set A.
- $\mathrm{supp}(\alpha) = \{x : \alpha(x) \neq 0\}$.
- $p_i(n) = n^i + 1$.
- N_i denotes the ith nondeterministic oracle Turing machine. Without loss of generality we assume that N_i runs in time $p_i(n)$ for all oracles.
- $\textsc{paths}(N^A, x)$ denotes the set of all paths of machine N on input x using oracle A (by convention, a path includes the oracle answers given by A).
- $\textsc{accept}(N^A, x)$ denotes the set of accepting paths of machine N on input x using oracle A.

The classes NP, co-NP, PP, $\mathrm{C}_=\mathrm{P}$, $\oplus\mathrm{P}$, and $\mathrm{MOD}_k\mathrm{P}$ are defined by considering a nondeterministic polynomial-time Turing machine N, and defining acceptance in terms of the number of accepting paths in N.

Definition 3 Let N denote a nondeterministic polynomial-time Turing machine, f a polynomial-time computable function, and k an integer greater than one in what follows:

$$
\begin{array}{lcll}
\mathrm{NP} & = & \{L : (\exists N)(\forall x) & [x \in L \iff |\mathrm{ACCEPT}(N,x)| > 0]\}. \\
\text{co-NP} & = & \{L : (\exists N)(\forall x) & [x \in L \iff |\mathrm{ACCEPT}(N,x)| = 0]\}. \\
\mathrm{PP} & = & \{L : (\exists N, f)(\forall x) & [x \in L \iff |\mathrm{ACCEPT}(N,x)| > f(x)]\}. \\
\mathrm{C_{=}P} & = & \{L : (\exists N, f)(\forall x) & [x \in L \iff |\mathrm{ACCEPT}(N,x)| = f(x)]\}. \\
\oplus\mathrm{P} & = & \{L : (\exists N)(\forall x) & [x \in L \iff |\mathrm{ACCEPT}(N,x)| \equiv 0 \pmod 2]\}. \\
\mathrm{MOD}_k\mathrm{P} & = & \{L : (\exists N)(\forall x) & [x \in L \iff |\mathrm{ACCEPT}(N,x)| \equiv 0 \pmod k]\}.
\end{array}
$$

These classes have been considered in [3, 8, 10, 11, 12, 18, 19, 24, 25, 27]. Although the classes $\oplus$P and MOD$_k$P are sometimes defined so that the number of accepting paths is congruent to one, instead of congruent to zero, we showed in [3] that the definitions above give rise to the same classes. It is known that NP $\subseteq$ PP, co-NP $\subseteq$ C$_=$P $\subseteq$ PP, $\oplus$P $\subseteq$ MOD$_k$P when k is even, and $\oplus$P $=$ MOD$_k$P when k is a power of 2.

We assume that the reader is familiar with relativized complexity classes and machines (see [1] for background). Relativizations of the classes above are defined by relativizing the Turing machine N. Torán has shown that it does not matter whether one also relativizes the polynomial-time computation of the threshold f in the definition of PP and C$_=$P [25], because a threshold function equal to half the number of all paths is universal.

3. The Initial Segment Method and a Counting Trick

For the purpose of producing an oracle separation, the easiest oracle construction technique is diagonalization. The next easiest technique is the initial segment method. We describe an initial segment construction that will form the skeleton of each construction in this paper.

Let C and D be complexity classes defined in terms of C-machines and D-machines. Suppose we want to construct an oracle A such that $C^A \not\subseteq D^A$. We say that $L^A \subseteq 0^*$ is an oracle property (c.f. [5]) if there is a predicate Q such that

$$0^n \in L^A \iff Q(A^{[n]}).$$

Our first step is to define an oracle property such that for all A, $L^A \in C^A$. We construct $A = \lim_i A_i$ in stages so that $L^A \notin D^A$. Since $L^A \in C^A - D^A$, we obtain $C^A \not\subseteq D^A$.

Stage 0: Let $A_0 = \emptyset$ and $n = 0$.

Stage $i > 0$: Choose n' sufficiently large for the task at hand (the choice of n' will depend on the classes C and D in an *ad hoc* way so as to guarantee the existence of the set B required below). At a minimum, we require $n' > p_{i-1}(n)$. Choose $B \subseteq \Sigma^{n'}$ such that

$$0^{n'} \in L^{A_i \cup B} \iff D\text{-machine } N_i \text{ using oracle } A_i \cup B \text{ rejects } 0^{n'}. \qquad (1)$$

Let $A_{i+1} = A_i \cup B$, and let $n = n'$.

At stage i we guarantee that D-machine N_i^A does not accept L^A. (At the next stage, by choosing $n' > p_i(n)$, we ensure that our work at stage i is never spoiled.) The hard part of the construction consists of showing that if n' is sufficiently large then there exists a set B satisfying (1). If such a set B always exists then the construction produces an oracle A such that $C^A \not\subseteq D^A$. If C and D are recursive then we can search for B exhaustively, so that the oracle A constructed is recursive.

The combinatorial technique of "reversing the order of summation" provides oracles that separate a large number of counting classes. Let ρ denote a computation path. Throughout this paper we adopt the convention that a computation of an oracle Turing machine *includes the oracle answers*. The key observation that we use is that

$$\sum_B |\text{ACCEPT}(N_i^{A_i \cup B}, 0^{n'})| = \sum_\rho |\{B : \rho \in \text{ACCEPT}(N_i^{A_i \cup B}, 0^{n'})\}| \tag{2}$$

For each path ρ, we consider the number of extensions B that make ρ accept. While it may not be convenient to compute that number exactly, it is often possible to obtain an upper bound or a lower bound or to compute the value modulo a power of a prime. Summing over all B, we draw a strong conclusion about the left-hand-side of (2). If we assume that the desired extension B does not exist, then we can similarly draw conclusions about the right-hand-side of (2); in many cases we obtain a contradiction. In addition to providing new oracle separations, this technique simplifies several previous constructions.

4. NP^A versus PARITY-P^A and $\mathrm{MOD}_k\mathrm{P}^A$

Cai, Hastad, Smolensky, and Yao [7, 15, 21, 28] have constructed oracles A such that $\oplus\mathrm{P}^A \not\subseteq \mathrm{PH}^A$, where PH denotes the polynomial-time hierarchy [16, 22]. We will not attempt to simplify their difficult constructions. On the other hand, Torán [25] has constructed an oracle A such that $\mathrm{NP}^A \not\subseteq \oplus\mathrm{P}^A$. Because both constructions use the initial segment technique, they can be combined to produce a single oracle that yields both separations simultaneously. This is interesting because it suggests that $\oplus$P is too difficult for the PH, but not as powerful as NP.

Although Torán's proof involves some nice identities, it is complex, and he admits that "probably any intuitive idea of what [the notation] represents is already gone." Like Torán, we use the initial segment method to construct an oracle A such that $\mathrm{NP}^A \not\subseteq \oplus\mathrm{P}^A$; however our proof that there exists a set B satisfying equation (1) is simple and intuitive.

Theorem 4 *There exists an oracle A such that*

$$\mathrm{NP}^A \not\subseteq \oplus\mathrm{P}^A.$$

Proof: Define
$$L^A = \{0^n : A^{[n]} \neq \emptyset\}.$$
Obviously $L^A \in \mathrm{NP}^A$. We construct $A = \lim_i A_i$ via the initial segment method so as to guarantee that
$$L^A \notin \oplus\mathrm{P}^A.$$

Stage 0: Let $A_0 = \emptyset$. Let $n = 0$.

Stage $i > 0$: Choose $n' > p_{i-1}(n)$ such that $2^{n'} > p_i(n')$. As justified below, choose $B \subseteq \Sigma^{n'}$ such that
$$B = \emptyset \iff |\text{ACCEPT}(N_i^{A_i \cup B}, 0^{n'})| \equiv 0 \pmod 2.$$

Let $A_{i+1} = A_i \cup B$. Let $n = n'$.

Obviously the construction guarantees that $L^A \notin \oplus\mathrm{P}^A$. It remains to show that the construction is possible. Suppose that stage i cannot be accomplished. Then
$$|\text{ACCEPT}(N_i^{A_i}, 0^{n'})| \not\equiv 0 \pmod 2,$$
and for all nonempty $B \subseteq \Sigma^{n'}$
$$|\text{ACCEPT}(N_i^{A_i \cup B}, 0^{n'})| \equiv 0 \pmod 2.$$
Summing over all B we obtain
$$\sum_B |\text{ACCEPT}(N_i^{A_i \cup B}, 0^{n'})| \not\equiv 0 \pmod 2. \tag{3}$$
Let ρ be any path, and let x be any string of length n' not queried along ρ. Then $B(x)$ can be assigned either of 2 values without affecting the acceptance behavior of ρ, so
$$|\{B : \rho \in \text{ACCEPT}(N_i^{A_i \cup B}, 0^{n'})\}| \equiv 0 \pmod 2.$$
Summing over all ρ we obtain
$$\sum_\rho |\{B : \rho \in \text{ACCEPT}(N_i^{A_i \cup B}, 0^{n'})\}| \equiv 0 \pmod 2.$$
By equation (2),
$$\sum_B |\text{ACCEPT}(N_i^{A_i \cup B}, 0^{n'})| \equiv 0 \pmod 2,$$
contradicting (3). ∎

$\oplus\mathrm{P}$ is a special case of $\mathrm{MOD}_k\mathrm{P}$, namely $k = 2$. By slightly modifying the preceding proof, we obtain the result in general for $\mathrm{MOD}_k\mathrm{P}$. This theorem is new.

Theorem 5 *For all $k \geq 2$, there exists an oracle A such that*
$$\mathrm{NP}^A \not\subseteq \mathrm{MOD}_k\mathrm{P}^A.$$

Proof: For simplicity of exposition, we construct a mapping α from Σ^* to $\{0,\ldots,k-1\}$ such that $\mathrm{NP}^\alpha \not\subseteq \mathrm{MOD}_k\mathrm{P}^\alpha$, and then we convert α to an equivalent set A. Let

$$L^\alpha = \{0^n : \mathrm{supp}(\alpha)^{[n]} \neq \emptyset\}.$$

Obviously $L^\alpha \in \mathrm{NP}^\alpha$. We construct $\alpha = \lim_i \alpha_i$ via the initial segment method so as to guarantee that

$$L^\alpha \notin \mathrm{MOD}_k\mathrm{P}^\alpha.$$

Stage 0: Let α_0 be the constant function $\lambda x[0]$. Let $n = 0$.

Stage $\boldsymbol{i > 0}$: Choose $n' > p_{i-1}(n)$ such that $2^{n'} > p_i(n')$. As justified below, choose a mapping β from Σ^* to $\{0,\ldots,k-1\}$ such that $\mathrm{supp}(\beta) \subseteq \Sigma^{n'}$ and

$$\mathrm{supp}(\beta) = \emptyset \iff |\textsc{accept}(N_i^{\max(\alpha_i,\beta)}, 0^{n'})| \equiv 0 \pmod{k}.$$

(Here $\max(u,v)$ is the function w such that for each x, $w(x) = \max(u(x), v(x))$. Its salient characteristic is that $\max(\alpha_i,\beta)(x)$ is equal to $\alpha_i(x)$ when $|x| < n'$, and equal to $\beta(x)$ when $|x| = n'$.) Let $\alpha_{i+1} = \max(\alpha_i, \beta)$. Let $n = n'$.

Obviously the construction guarantees that $L^\alpha \notin \mathrm{MOD}_k\mathrm{P}^\alpha$. It remains to show that the construction is possible. Suppose that stage i cannot be accomplished. Then

$$|\textsc{accept}(N_i^{\alpha_i}, 0^{n'})| \not\equiv 0 \pmod{k},$$

and for all β other than $\lambda x[0]$

$$|\textsc{accept}(N_i^{\max(\alpha_i,\beta)}, 0^{n'})| \equiv 0 \pmod{k}.$$

Summing over all β we obtain

$$\sum_\beta |\textsc{accept}(N_i^{\max(\alpha_i,\beta)}, 0^{n'})| \not\equiv 0 \pmod{k}. \tag{4}$$

However, for each path ρ, there is some string x in $\Sigma^{n'}$ that is not queried along ρ, because $2^{n'} > p_i(n')$. Since $\beta(x)$ can be assigned any of k values without affecting the acceptance behavior of ρ,

$$|\{\beta : \rho \in \textsc{accept}(N_i^{\max(\alpha_i,\beta)}, 0^{n'})\}| \equiv 0 \pmod{k}.$$

Summing over all ρ we obtain

$$\sum_\rho |\{\beta : \rho \in \textsc{accept}(N_i^{\max(\alpha_i,\beta)}, 0^{n'})\}| \equiv 0 \pmod{k}.$$

By equation (2),

$$\sum_\beta |\textsc{accept}(N_i^{\max(\alpha_i,\beta)}, 0^{n'})| \equiv 0 \pmod{k},$$

contradicting (4). Hence we have constructed α such that

$$\mathrm{NP}^{\alpha} \not\subseteq \mathrm{MOD}_k\mathrm{P}^{\alpha}.$$

Given α, we construct A by using $\lceil \log k \rceil$ bits of A to encode the value of $\alpha(x)$ for each x. Since A is polynomial-time Turing equivalent to α, we have $\mathrm{NP}^A = \mathrm{NP}^{\alpha}$ and $\mathrm{MOD}_k\mathrm{P}^A = \mathrm{MOD}_k\mathrm{P}^{\alpha}$, so

$$\mathrm{NP}^A \not\subseteq \mathrm{MOD}_k\mathrm{P}^A.$$

∎

Because initial segment constructions can be combined, we obtain the following:

Corollary 6 *There exists an oracle A such that for all $k \geq 2$,*

$$\mathrm{NP}^A \not\subseteq \mathrm{MOD}_k\mathrm{P}^A.$$

5. PP^A versus $\oplus\mathrm{P}^A$ and $\mathrm{MOD}_k\mathrm{P}^A$

Since NP $\subseteq$ PP [11] via a proof that relativizes, the oracle A constructed in the preceding section has the property that for all $k \geq 2$,

$$\mathrm{PP}^A \not\subseteq \mathrm{MOD}_k\mathrm{P}^A.$$

On the other hand, the question of whether there exists an oracle A such that $\oplus\mathrm{P}^A \not\subseteq \mathrm{PP}^A$ has a long history. Although they never discussed relativizations, an oracle construction can be obtained as a corollary to Minsky and Papert's Theorem 3.1.1 in [17]. The separation was claimed to hold relative to almost all oracles by Bennett and Gill [5]; however their proof is incorrect. A correct oracle construction is given by Torán in [25]. We present a construction that exploits a simple combinatorial symmetry: Every nonempty set S has as many subsets with odd cardinality as with even cardinality. (Why? Fix any string $x \in S$. A subset of T of S with odd cardinality is uniquely determined by $T - \{x\}$. The same is true of subsets with even cardinality.) Subsequently, we will refer to this property and similar properties as symmetry.

Theorem 7 *There exists an oracle A such that*

$$\oplus\mathrm{P}^A \not\subseteq \mathrm{PP}^A.$$

Proof: Define

$$L^A = \{0^n : |A^{[n]}| \equiv 0 \pmod 2\}.$$

Obviously $L^A \in \oplus\mathrm{P}^A$. We construct $A = \lim_i A_i$ via the initial segment method so as to guarantee that

$$L^A \notin \mathrm{PP}^A.$$

Stage 0: Let $A_0 = \emptyset$. Let $n = 0$.

Stage $i > 0$: Choose $n' > p_{i-1}(n)$ such that $2^{n'} > p_i(n')$. Compute the acceptance threshold t of N_i on input $0^{n'}$. As justified below, choose $B \subseteq \Sigma^{n'}$ such that

$$|B| \equiv 0 \pmod 2 \Longleftrightarrow |\text{ACCEPT}(N_i^{A_i \cup B}, 0^{n'})| \leq t.$$

Let $A_{i+1} = A_i \cup B$. Let $n = n'$.

Obviously the construction guarantees that $L^A \notin \text{PP}^A$. It remains to show that the construction is possible. Suppose that stage i cannot be accomplished. Then

$$|B| \equiv 0 \pmod 2 \Longrightarrow |\text{ACCEPT}(N_i^{A_i \cup B}, 0^{n'})| > t, \tag{5}$$

and

$$|B| \equiv 1 \pmod 2 \Longrightarrow |\text{ACCEPT}(N_i^{A_i \cup B}, 0^{n'})| \leq t. \tag{6}$$

Summing over B with $|B| \equiv 0 \pmod 2$ we obtain

$$\begin{aligned} \sum_{|B| \equiv 0 \pmod 2} |\text{ACCEPT}(N_i^{A_i \cup B}, 0^{n'})| &> \sum_{|B| \equiv 0 \pmod 2} t \qquad \text{by (5)} \\ &= \sum_{|B| \equiv 1 \pmod 2} t \qquad \text{by symmetry} \\ &\geq \sum_{|B| \equiv 1 \pmod 2} |\text{ACCEPT}(N_i^{A_i \cup B}, 0^{n'})| \qquad \text{by (6),} \end{aligned}$$

so

$$\sum_{|B| \equiv 0 \pmod 2} |\text{ACCEPT}(N_i^{A_i \cup B}, 0^{n'})| > \sum_{|B| \equiv 1 \pmod 2} |\text{ACCEPT}(N_i^{A_i \cup B}, 0^{n'})|. \tag{7}$$

However, for each path ρ, there is some string x in $\Sigma^{n'}$ that is not queried along ρ, because $2^{n'} > p_i(n')$. Since $B(x)$ can be either 0 or 1 without affecting the acceptance behavior of ρ,

$$\begin{aligned} &|\{B. |B| \equiv 0 \pmod 2 : \rho \in \text{ACCEPT}(N_i^{A_i \cup B}, 0^{n'})\}| \\ &= \ |\{B. |B| \equiv 1 \pmod 2 : \rho \in \text{ACCEPT}(N_i^{A_i \cup B}, 0^{n'})\}|. \end{aligned}$$

Summing over all ρ we obtain

$$\begin{aligned} &\sum_\rho |\{B. |B| \equiv 0 \pmod 2 : \rho \in \text{ACCEPT}(N_i^{A_i \cup B}, 0^{n'})\}| \\ &= \ \sum_\rho |\{B. |B| \equiv 1 \pmod 2 : \rho \in \text{ACCEPT}(N_i^{A_i \cup B}, 0^{n'})\}|. \end{aligned}$$

By equation (2),

$$\sum_{|B| \equiv 0 \pmod 2} |\text{ACCEPT}(N_i^{A_i \cup B}, 0^{n'})| = \sum_{|B| \equiv 1 \pmod 2} |\text{ACCEPT}(N_i^{A_i \cup B}, 0^{n'})|,$$

contradicting (7). ∎

In [5] it was claimed that this result holds for almost all oracles A. Bennett and Gill used the same test language L^A that we use in our construction. Their proof depended on showing that every PP-machine N fails to compute L^A for at least one-half of all oracles A. They showed correctly that on sufficiently long inputs, every path gives the correct answer for exactly one-half of all oracles (because there is at least one string not queried on the path). However, this leaves open the possibility in principal that for 80% of all oracles we have 60% of N's paths give the correct answer, while for the remaining 20% of all oracles we have only 1% of N's paths give the correct answer. Then N is correct for 80% of all oracles. In fact, although we might expect that deciding membership in L^A would require 2^n steps on a probabilistic Turing machine, work in progress by Steven Rudich and this author shows that for almost all oracles A, the language L^A is accepted by a probabilistic Turing machine with oracle A that runs in time $O(n2^{n/2})$.

We hope that some subtler counting argument might apply to PP machines and lead to a proof of Bennett and Gill's claim. We note that circuit-complexity techniques have established certain separations relative to a random oracle (see [7, 21], which are discussed at the beginning of Section 7.). In order for current circuit-complexity techniques to be applicable it would be necessary to have $\mathrm{PH}^{\mathrm{MOD}_k\mathrm{P}^A} \not\subseteq \mathrm{PH}^{\mathrm{PP}^A}$. However, Hastad has pointed out that this is false, because

$$\mathrm{MOD}_k\mathrm{P} \subseteq \mathrm{P}^{\#\mathrm{P}[1]} \subseteq \mathrm{NP}^{\mathrm{PP}[1]},$$

where the number in brackets indicates that only one query to the oracle is allowed per computation path (a similar observation appears in [21]). Hence substantially new circuit-complexity techniques may be required.

By slightly modifying the proof of Theorem 7, we obtain the separation in general for $\mathrm{MOD}_k\mathrm{P}$. This theorem is new.

Theorem 8 *For all $k \geq 2$, there exists an oracle A such that*

$$\mathrm{MOD}_k\mathrm{P}^A \not\subseteq \mathrm{PP}^A.$$

Proof: We will construct a function oracle α from Σ^* to $\{0, \ldots, k-1\}$. Let

$$L^\alpha = \{0^n : \sum_{x \in \Sigma^n} \alpha(x) \equiv 0 \pmod{k}\}.$$

$L^\alpha \in \mathrm{MOD}_k\mathrm{P}^\alpha$ via a nondeterministic Turing machine that guesses (i, x) with $|x| = n$ and accepts if $0 \leq i < \alpha(x)$. (This machine has exactly $\alpha(x)$ accepting paths for each x of length n.)

We construct $\alpha = \lim_i \alpha_i$ via the initial segment method so as to guarantee that

$$L^\alpha \notin \mathrm{PP}^\alpha.$$

Stage 0: Let α_0 be the constant function $\lambda x[0]$. Let $n = 0$.

Stage $i > 0$: Choose $n' > p_{i-1}(n)$ such that $2^{n'} > p_i(n')$. Compute the acceptance threshold t of N_i on input $0^{n'}$. Define an equivalence class $[s]$ by

$$\beta \in [s] \iff \sum_{x \in \Sigma^{n'}} \beta(x) \equiv s \pmod{k}.$$

(Note that an easy symmetry argument shows that $|[s]| = |[t]|$ for all s and t.) As justified below, choose a mapping β from Σ^* to $\{0, \ldots, k-1\}$ such that $\mathrm{supp}(\beta) \subseteq \Sigma^{n'}$ and

$$\beta \in [0] \iff |\text{ACCEPT}(N_i^{\max(\alpha_i, \beta)}, 0^{n'})| \leq t.$$

Let $\alpha_{i+1} = \max(\alpha_i, \beta)$. Let $n = n'$.

Obviously the construction guarantees that $L^\alpha \notin \mathrm{PP}^\alpha$. It remains to show that the construction is possible. Suppose that stage i cannot be accomplished. Then

$$|\beta| \in [0] \Longrightarrow |\text{ACCEPT}(N_i^{\max(\alpha_i, \beta)}, 0^{n'})| > t, \tag{8}$$

and

$$|\beta| \in [1] \Longrightarrow |\text{ACCEPT}(N_i^{\max(\alpha_i, \beta)}, 0^{n'})| \leq t. \tag{9}$$

Summing over $\beta \in [0]$ we obtain

$$\begin{aligned}
\sum_{\beta \in [0]} |\text{ACCEPT}(N_i^{\max(\alpha_i, \beta)}, 0^{n'})| &> \sum_{\beta \in [0]} t \qquad \text{by (8)} \\
&= \sum_{\beta \in [1]} t \qquad \text{by symmetry} \\
&\geq \sum_{\beta \in [1]} |\text{ACCEPT}(N_i^{\max(\alpha_i, \beta)}, 0^{n'})| \qquad \text{by (9)},
\end{aligned}$$

so

$$\sum_{\beta \in [0]} |\text{ACCEPT}(N_i^{\max(\alpha_i, \beta)}, 0^{n'})| > \sum_{\beta \in [1]} |\text{ACCEPT}(N_i^{\max(\alpha_i, \beta)}, 0^{n'})|. \tag{10}$$

(Note that we could have used any equivalence class $[s]$ except $[0]$ in place of $[1]$.) However, for each path ρ, there is some string x in $\Sigma^{n'}$ that is not queried along ρ, because $2^{n'} > p_i(n')$. Since $\beta(x)$ can take any value in $\{0, \ldots, k-1\}$ without affecting the acceptance behavior of ρ,

$$|\{\beta \in [0] : \rho \in \text{ACCEPT}(N_i^{\max(\alpha_i, \beta)}, 0^{n'})\}| = |\{\beta \in [1] : \rho \in \text{ACCEPT}(N_i^{\max(\alpha_i, \beta)}, 0^{n'})\}|.$$

Summing over all ρ we obtain

$$\sum_\rho |\{\beta \in [0] : \rho \in \text{ACCEPT}(N_i^{\max(\alpha_i, \beta)}, 0^{n'})\}| = \sum_\rho |\{\beta \in [1] : \rho \in \text{ACCEPT}(N_i^{\max(\alpha_i, \beta)}, 0^{n'})\}|.$$

By equation (2),

$$\sum_{\beta \in [0]} |\text{ACCEPT}(N_i^{\max(\alpha_i, \beta)}, 0^{n'})| = \sum_{\beta \in [1]} |\text{ACCEPT}(N_i^{\max(\alpha_i, \beta)}, 0^{n'})|,$$

contradicting (10). We obtain A from α as in the proof of Theorem 7. ∎

Because $\mathrm{C_{=}P} \subseteq \mathrm{PP}$ [19] via a proof that relativizes, it follows that there exists an oracle A such that for all k, $\mathrm{MOD}_k\mathrm{P}^A \not\subseteq \mathrm{C_{=}P}^A$.

6. NP^A **versus** $\mathrm{C_{=}P}^A$

The class $\mathrm{C_{=}P}$ was defined by Wagner in [27] and also studied by Torán. An important subclass of $\mathrm{C_{=}P}$ is co-NP, which is obtained by using the constant function $\lambda x[0]$ as the threshold. Another important subclass of $\mathrm{C_{=}P}$ is the class US obtained by using the constant function $\lambda x[1]$ for the threshold.

$$\mathrm{US} = \{L : (\exists N)(\forall x)[x \in L \iff |\textsc{accept}(N, x)| = 1]\}.$$

US was studied by Blass and Gurevich [6], who showed that co-NP $\subseteq$ US. Other subclasses of $\mathrm{C_{=}P}$ are studied in [3].

Blass and Gurevich constructed an oracle A such that $\mathrm{NP}^A \not\subseteq \mathrm{US}^A$, and Torán constructed an oracle A such that more generally $\mathrm{NP}^A \not\subseteq \mathrm{C_{=}P}^A$. We present a simple proof of Torán's result; in some ways our proof is simpler than Blass and Gurevich's.

Theorem 9 *There exists an oracle A such that*

$$\mathrm{NP}^A \not\subseteq \mathrm{C_{=}P}^A.$$

Proof: Define

$$L^A = \{0^n : A^{[n]} \neq \emptyset\}.$$

Obviously $L^A \in \mathrm{NP}^A$. We construct $A = \lim_i A_i$ via the initial segment method so as to guarantee that

$$L^A \notin \mathrm{C_{=}P}^A.$$

Stage 0: Let $A_0 = \emptyset$. Let $n = 0$.

Stage $i > 0$: Choose $n' > p_{i-1}(n)$ so that $2^{n'} > 2p_i(n')$. Compute the acceptance threshold t of N_i on input $0^{n'}$. Without loss of generality, assume that $0 \leq t \leq 2^{p_i(n')} + 1$, because all thresholds less than 0 or greater than $2^{p_i(n')}$ lead to rejection. As justified below, choose $B \subseteq \Sigma^{n'}$ such that

$$B = \emptyset \iff |\textsc{accept}(N_i^{A_i \cup B}, 0^{n'})| = t.$$

Let $A_{i+1} = A_i \cup B$. Let $n = n'$.

Obviously the construction guarantees that $L^A \notin \mathrm{C_{=}P}^A$. It remains to show that the construction is possible. Suppose that stage i cannot be accomplished. Then

$$|\textsc{accept}(N_i^{A_i}, 0^{n'})| \neq t, \tag{11}$$

and for all nonempty $B \subseteq \Sigma^{n'}$

$$|\textsc{accept}(N_i^{A_i \cup B}, 0^{n'})| = t.$$

Summing over all B we obtain

$$\begin{aligned}\sum_B |\text{ACCEPT}(N_i^{A_i \cup B}, 0^{n'})| &= |\text{ACCEPT}(N_i^{A_i}, 0^{n'})| + \sum_{B \neq \emptyset} t \\ &= |\text{ACCEPT}(N_i^{A_i}, 0^{n'})| + (2^{2^{n'}} - 1)t \\ &= 2^{2^{n'}} t + |\text{ACCEPT}(N_i^{A_i}, 0^{n'})| - t. \end{aligned} \tag{12}$$

Therefore by (11),

$$\sum_B |\text{ACCEPT}(N_i^{A_i \cup B}, 0^{n'})| \neq 2^{2^{n'}} t. \tag{13}$$

Since $0 \leq t \leq 2^{p_i(n')} + 1$ and $0 \leq |\text{ACCEPT}(N_i^{A_i}, 0^{n'})| \leq 2^{p_i(n')}$, subtracting inequalities yields

$$-2^{p_i(n')} - 1 \leq |\text{ACCEPT}(N_i^{A_i}, 0^{n'})| - t \leq 2^{p_i(n')}.$$

Adding $2^{2^{n'}} t$ and using (12) we obtain

$$2^{2^{n'}} t - 2^{p_i(n')} - 1 \leq \sum_B |\text{ACCEPT}(N_i^{A_i \cup B}, 0^{n'})| \leq 2^{2^{n'}} t + 2^{p_i(n')},$$

so

$$2^{2^{n'}} t - 2^{p_i(n')+1} < \sum_B |\text{ACCEPT}(N_i^{A_i \cup B}, 0^{n'})| < 2^{2^{n'}} t + 2^{p_i(n')+1}.$$

Together with (13) this implies that

$$\sum_B |\text{ACCEPT}(N_i^{A_i \cup B}, 0^{n'})| \not\equiv 0 \pmod{2^{p_i(n')+1}}. \tag{14}$$

However, for each path ρ, there are at least $p_i(n') + 1$ strings x in $\Sigma^{n'}$ that are not queried along ρ, because $2^{n'} > 2p_i(n')$. Since membership for each of those strings can be defined arbitrarily without changing the acceptance behavior of ρ,

$$|\{B : \rho \in \text{ACCEPT}(N_i^{A_i \cup B}, 0^{n'})\}| \equiv 0 \pmod{2^{p_i(n')+1}}.$$

Summing over all ρ we obtain

$$\sum_\rho |\{B : \rho \in \text{ACCEPT}(N_i^{A_i \cup B}, 0^{n'})\}| \equiv 0 \pmod{2^{p_i(n')+1}}.$$

By equation (2),

$$\sum_B |\text{ACCEPT}(N_i^{A_i \cup B}, 0^{n'})| \equiv 0 \pmod{2^{p_i(n')+1}},$$

contradicting (14). ∎

Since NP $\subseteq$ PP [11] via a proof that relativizes, the oracle A in the preceding theorem has the property that

$$\text{PP}^A \not\subseteq \text{C}_=\text{P}^A,$$

as communicated to us by Torán.

7. $\mathrm{MOD}_j\mathrm{P}^A$ versus $\mathrm{MOD}_k\mathrm{P}^A$

In [3], we proved some relations between $\mathrm{MOD}_j\mathrm{P}^A$ and $\mathrm{MOD}_k\mathrm{P}^A$. For example, if j is a power of a prime p and k is divisible by p, then $\mathrm{MOD}_j\mathrm{P}^A \subseteq \mathrm{MOD}_k\mathrm{P}^A$. When j and k are distinct primes, we think it is unlikely that $\mathrm{MOD}_j\mathrm{P}^A \subseteq \mathrm{MOD}_k\mathrm{P}^A$. In fact, Smolensky has separated $\mathrm{PH}^{\mathrm{MOD}_j\mathrm{P}^A}$ from $\mathrm{PH}^{\mathrm{MOD}_k\mathrm{P}^A}$ for almost all oracles. In this section, we prove a special case of his result via easier techniques: we construct an oracle A such that $\mathrm{MOD}_j\mathrm{P}^A \not\subseteq \mathrm{MOD}_k\mathrm{P}^A$.

Theorem 10 *Let $j > 1$, and let k be a prime number that is not a divisor of j. There exists an oracle A such that*

$$\mathrm{MOD}_j\mathrm{P}^A \not\subseteq \mathrm{MOD}_k\mathrm{P}^A.$$

Proof: We will construct a function oracle α from Σ^* to $\{0,\ldots,j-1\}$. Let

$$L^\alpha = \{0^n : \sum_{x\in\Sigma^n} \alpha(x) \equiv 0 \pmod{j}\}.$$

As in the proof of Theorem 8, $L^\alpha \in \mathrm{MOD}_j\mathrm{P}^\alpha$. We construct $\alpha = \lim_i \alpha_i$ via the initial segment method so as to guarantee that

$$L^\alpha \notin \mathrm{MOD}_k\mathrm{P}^\alpha.$$

Stage 0: Let α_0 be the constant function $\lambda x[0]$. Let $n = 0$.

Stage $i > 0$: Choose $n' > p_{i-1}(n)$ such that $2^{n'} > p_i(n')$. Define an equivalence class $[s]$ by

$$\beta \in [s] \iff \sum_{x\in\Sigma^{n'}} \beta(x) \equiv s \pmod{j}.$$

As justified below, choose a mapping β from Σ^* to $\{0,\ldots,j-1\}$ such that $\mathrm{supp}(\beta) \subseteq \Sigma^{n'}$ and one of the following two conditions holds:

i. $\beta \in [0]$ and $|\textsc{accept}(N_i^{\max(\alpha_i,\beta)}, 0^{n'})| \not\equiv 0 \pmod{k}$,

ii. $\beta \in [1]$ and $|\textsc{accept}(N_i^{\max(\alpha_i,\beta)}, 0^{n'})| \not\equiv 1 \pmod{k}$.

Let $\alpha_{i+1} = \max(\alpha_i, \beta)$. Let $n = n'$.

In [3], we showed for prime k that $L \in \mathrm{MOD}_k\mathrm{P}$ if and only if there exists a nondeterministic polynomial-time Turing machine N such that

$$|\textsc{accept}(N,x)| \equiv \begin{cases} 0 \pmod{k} & \text{if } x \in L \\ 1 \pmod{k} & \text{if } x \notin L. \end{cases}$$

Since that proof relativizes, the construction guarantees that $L^\alpha \notin \mathrm{MOD}_k\mathrm{P}^\alpha$. It remains to show that the construction is possible. Suppose that stage i cannot be accomplished. Then for all β,

$$\beta \in [0] \Longrightarrow |\textsc{accept}(N_i^{\max(\alpha_i,\beta)}, 0^{n'})| \equiv 0 \pmod{k},$$

and

$$\beta \in [1] \Longrightarrow |\mathrm{ACCEPT}(N_i^{\max(\alpha_i,\beta)}, 0^{n'})| \equiv 1 \pmod{k}.$$

Summing over β in each case we obtain

$$\sum_{\beta \in [0]} |\mathrm{ACCEPT}(N_i^{\max(\alpha_i,\beta)}, 0^{n'})| \equiv 0 \pmod{k}, \tag{15}$$

and (by symmetry)

$$\sum_{\beta \in [1]} |\mathrm{ACCEPT}(N_i^{\max(\alpha_i,\beta)}, 0^{n'})| \equiv j^{2^{n'}-1} \pmod{k}. \tag{16}$$

However, as shown in the proof of Theorem 8,

$$\sum_{\beta \in [0]} |\mathrm{ACCEPT}(N_i^{\max(\alpha_i,\beta)}, 0^{n'})| = \sum_{\beta \in [1]} |\mathrm{ACCEPT}(N_i^{\max(\alpha_i,\beta)}, 0^{n'})|,$$

so $j^{2^{n'}-1} \equiv 0 \pmod{k}$ by (15) and (16), a contradiction because j and k are relatively prime. We obtain A from α as in the proof of Theorem 7. ▮

Note that in this proof we use the assumption that k is prime and the assumption that j and k are relatively prime. It would be interesting to perform the construction making only the latter assumption.

8. Classes Without Complete Languages: R and UP

In this section we will see how to extend the preceding techniques to complexity classes like R and UP that do not seem to contain many-one complete languages. (See [20] and [13] respectively for relativized worlds where R and UP do not contain many-one complete languages. See [14] for related results.) We begin by constructing an oracle A such that $\mathrm{R}^A \not\subseteq \mathrm{MOD}_k\mathrm{P}^A$ for prime k. The new twist is that we consider only a restricted class of oracles so that the test language L^A is guaranteed to belong to R^A, meanwhile making sure that the counting argument can proceed smoothly.

Definition 11 R consists of those languages L for which there exists a nondeterministic polynomial-time machine N such that for all x

$$\begin{array}{ll} |\mathrm{ACCEPT}(N,x)| \geq \frac{1}{2}|\mathrm{PATHS}(N,x)| & \text{if } x \in L \\ |\mathrm{ACCEPT}(N,x)| = 0 & \text{if } x \notin L. \end{array}$$

Proposition 12 *If k is prime then there exists an oracle A such that*

$$\mathrm{R}^A \not\subseteq \mathrm{MOD}_k\mathrm{P}^A.$$

Proof: Let Σ be the k-character alphabet $\{0, 1, \ldots, k-1\}$. We will construct a mapping α from Σ^* to Σ. Let

$$L^\alpha = \{0^n : \mathrm{supp}(\alpha)^{[n+1]} \neq \emptyset\}.$$

Obviously $L^\alpha \in \mathrm{NP}^\alpha$. We construct $\alpha = \lim_i \alpha_i$ via the initial segment method so as to guarantee that

$$L^\alpha \notin \mathrm{MOD}_k\mathrm{P}^\alpha.$$

In order to make the counting work out nicely, we will ensure that

$$\mathrm{supp}(\alpha)^{[n+1]} \subseteq 0\Sigma^n \cup 1\Sigma^n - 0^{n+1}$$

and that α restricted to $\mathrm{supp}(\alpha)^{[n+1]}$ is a constant function. We will also ensure for each n that $|\mathrm{supp}(\alpha)^{[n+1]}|$ is either 0 or k^n; thus $L^\alpha \in \mathrm{R}^\alpha$. Strings belonging to $0\Sigma^n \cup 1\Sigma^n - 0^{n+1}$ will be called *relevant.*

Every $\mathrm{MOD}_k\mathrm{P}$ oracle machine can be simulated by an exponential-time MOD_k machine E_i such that on input 0^n each path queries exactly $k^n - 1$ relevant strings of length $n+1$ (and possibly some strings of other lengths). We construct α so that L^α is not accepted by any machine of this kind.

Stage 0: Let α_0 be the constant function $\lambda x[0]$. Let $n = 0$.

Stage $i > 0$: Choose $n' > p_{i-1}(n)$ such that n' is larger than the length of any string queried at a previous stage. Call a mapping β allowable if $\mathrm{supp}(\beta)$ contains only relevant strings of length $n'+1$ and $|\mathrm{supp}(\beta)|$ is 0 or $k^{n'}$. As justified below, choose an allowable mapping β such that

$$\mathrm{supp}(\beta) = \emptyset \Longleftrightarrow |\textsc{accept}(E_i^{\max(\alpha_i,\beta)}, 0^{n'})| \equiv 0 \pmod{k}.$$

Let $\alpha_{i+1} = \max(\alpha_i, \beta)$. Let $n = n'$.

Obviously the construction guarantees that $L^\alpha \notin \mathrm{MOD}_k\mathrm{P}^\alpha$. It remains to show that the construction is possible. Suppose that stage i cannot be accomplished. Then

$$|\textsc{accept}(E_i^{\alpha_i}, 0^{n'})| \not\equiv 0 \pmod{k},$$

and for all allowable β except $\lambda x[0]$

$$|\textsc{accept}(E_i^{\max(\alpha_i,\beta)}, 0^{n'})| \equiv 0 \pmod{k}.$$

Summing over all allowable β we obtain

$$\sum_\beta |\textsc{accept}(E_i^{\max(\alpha_i,\beta)}, 0^{n'})| \not\equiv 0 \pmod{k}. \tag{17}$$

Let ρ be any accepting path. Then ρ queries exactly $k^{n'} - 1$ relevant strings of length $n'+1$. If all of the oracle answers are negative, then ρ accepts on exactly k allowable oracles (β restricted to the remaining $k^{n'}$ relevant strings must be a constant function). If exactly j of the oracle answers are positive, where $1 \leq j \leq k^{n'}-1$, then ρ accepts on exactly $\binom{k^{n'}}{k^{n'}-j}$ allowable oracles, which is 0 (mod k) because k is prime. Summing over all ρ (and restricting β to be allowable) we obtain

$$\sum_{\rho} |\{\beta : \rho \in \text{ACCEPT}(E_i^{\max(\alpha_i,\beta)}, 0^{n'})\}| \equiv 0 \pmod{k}.$$

By equation (2),

$$\sum_{\beta} |\text{ACCEPT}(E_i^{\max(\alpha_i,\beta)}, 0^{n'})| \equiv 0 \pmod{k},$$

contradicting (17). ∎

Note that in the preceding proof, it was very helpful to have the number of relevant, but unqueried strings be a power of k. The counting would have been much more complicated if we did not strictly control the number of queries made by each path.

The preceding construction can be made to work for composite k. For each n and each prime p in the factorization of k (including repetitions), we set aside $2p^n - 1$ *p-relevant* strings of length $n+1$, and we require that E_i query exactly $p^n - 1$ of those strings on input 0^n. We require that $\text{supp}(\alpha)^{[n+1]}$ either contain 0 or p^n p-relevant strings. Also α restricted to p-relevant strings in $\text{supp}(\alpha)^{[n+1]}$ must be a constant between 0 and $p-1$. The details of the construction and proof are left to the reader. Because the oracle constructions can be combined for all k, we obtain the following result:

Theorem 13 *There exists an oracle A such that for every k*

$$\mathrm{R}^A \not\subseteq \mathrm{MOD}_k\mathrm{P}^A.$$

In [3], we defined the class $\mathrm{MODZ}_k\mathrm{P}$, which is a subclass of $\mathrm{NP} \cap \mathrm{MOD}_k\mathrm{P}$, and we showed that FewP is contained in $\mathrm{MODZ}_k\mathrm{P}$.

Definition 14 $\mathrm{MODZ}_k\mathrm{P}$ consists of those languages L for which there exists a nondeterministic polynomial-time machine N such that for all x

$$\begin{array}{ll} |\text{ACCEPT}(N,x)| \not\equiv 0 \pmod{k} & \text{if } x \in L, \\ |\text{ACCEPT}(N,x)| = 0 & \text{if } x \notin L. \end{array}$$

Since $\mathrm{MOD}_k\mathrm{P}$ is closed under complement, it is clear that $\mathrm{MODZ}_k\mathrm{P}$ is a subset of $\mathrm{NP} \cap \mathrm{MOD}_k\mathrm{P}$. It is not known whether $\mathrm{MODZ}_k\mathrm{P}$ is a *proper* subset of $\mathrm{NP} \cap \mathrm{MOD}_k\mathrm{P}$, although we suspect that it is. For prime k, we construct an oracle relative to which that is the case; in fact it is easier to prove a stronger result.

Definition 15 UP consists of those languages L for which there exists a nondeterministic polynomial-time machine N such that for all x

$$|\text{ACCEPT}(N,x)| = \begin{cases} 1 & \text{if } x \in L \\ 0 & \text{otherwise.} \end{cases}$$

Theorem 16 *For all prime k there exists an oracle A such that*

$$\mathrm{NP}^A \cap \text{co-UP}^A \not\subseteq \mathrm{MODZ}_k\mathrm{P}^A.$$

Proof: Let $\Sigma = \{0,1\}$. We will construct a function oracle α from Σ^* to $\{0,\ldots,k-1\}$. Let

$$L^A = \{0^n : \mathrm{supp}(\alpha)^{[2n]} \neq \emptyset\}.$$

Obviously $L^\alpha \in \mathrm{NP}^\alpha$. We construct $\alpha = \lim_i \alpha_i$ via the initial segment method so as to guarantee that

$$L^\alpha \notin \mathrm{MODZ}_k\mathrm{P}^\alpha.$$

Our construction will also ensure for each n that

$$|\mathrm{supp}(\alpha)^{[2n+1]}| = \begin{cases} 0 & \text{if } |\mathrm{supp}(\alpha)^{[2n]}| \geq 0 \\ 1 & \text{otherwise;} \end{cases} \tag{18}$$

thus $L^\alpha \in \text{co-UP}^\alpha$.

Stage 0: Let $\alpha_0 = \emptyset$. Let $n = 0$.

Stage $i > 0$: Choose $n' > n$ such that $2n'$ is larger than the length of any string queried at a previous stage and $2^{2n'} > p_i(n)$. Call a mapping β *allowable* if $\mathrm{supp}(\beta)$ contains only strings of length $2n'$ or $2n'+1$ and equation (18) is satisfied when $\alpha = \beta$ and $n = n'$. As justified below, choose an allowable mapping β such that one of the following two conditions holds:

i. $\mathrm{supp}(\beta)^{[2n']} = \emptyset$ and $|\mathrm{ACCEPT}(N_i^{\max(\alpha_i,\beta)}, 0^{n'})| > 0$

ii. $\mathrm{supp}(\beta)^{[2n']} \neq \emptyset$ and $|\mathrm{ACCEPT}(N_i^{\max(\alpha_i,\beta)}, 0^{n'})| \not\equiv 1 \pmod{k}$

In [3], we showed for prime k that $L \in \mathrm{MODZ}_k\mathrm{P}$ if and only if there exists a nondeterministic polynomial-time Turing machine N such that

$$\begin{array}{ll} |\mathrm{ACCEPT}(N,x)| \equiv 1 \pmod{k} & \text{if } x \in L, \\ |\mathrm{ACCEPT}(N,x)| = 0 & \text{if } x \notin L. \end{array}$$

Since that proof relativizes, the construction guarantees that $L^\alpha \notin \mathrm{MODZ}_k\mathrm{P}^\alpha$. It remains to show that the construction is possible. Suppose that stage i cannot be accomplished. Then

$$|\mathrm{ACCEPT}(N_i^{\alpha_i}, 0^{n'})| = 0$$

and for all allowable β such that $\mathrm{supp}(\beta)^{[2n']} \neq \emptyset$

$$|\mathrm{ACCEPT}(N_i^{\max(\alpha_i,\beta)}, 0^{n'}) \equiv 1 \pmod{k}.$$

Summing over all allowable β we obtain

$$\sum_\beta |\mathrm{ACCEPT}(N_i^{\max(\alpha,\beta)}, 0^{n'})| \equiv k^{2^{2n'}} - 1 \equiv -1 \pmod{k}. \tag{19}$$

Let ρ be any accepting path (for an allowable β). Then ρ must query a string belonging to $\mathrm{supp}(\beta)^{[2n']}$ (otherwise we can easily choose a β with $\mathrm{supp}(\beta)^{[2n']} = \emptyset$ to satisfy condition (i)). Since $2^{2n'} > p_i(n')$ the path ρ must have failed to query at least one string x of length $2n'$. Since ρ queries at least one string that actually belongs $\mathrm{supp}(\beta)^{[2n']}$, there are k values that $\beta(x)$ could take (regardless of other oracle answers) without affecting whether β is allowable and without affecting whether ρ accepts. Therefore ρ accepts for 0 (mod k) choices of β. Summing over all ρ (and restricting β to be allowable) we obtain

$$\sum_{\rho} |\beta : \rho \in \textsc{accept}(N_i^{\max(\alpha_i,\beta)}, 0^{n'})| \equiv 0 \pmod{k}.$$

By equation (2),

$$\sum_{\beta} |\textsc{accept}(N_i^{\max(\alpha_i,\beta)}, 0^{n'})| \equiv 0 \pmod{k},$$

contradicting (19). ∎

Corollary 17 *There exists an oracle A such that for all prime k*

$$\mathrm{P}^A \subset \mathrm{MODZ}_k\mathrm{P}^A \subset \mathrm{NP}^A \cap \mathrm{MOD}_k\mathrm{P}^A.$$

Proof: Clearly, $\mathrm{MODZ}_k\mathrm{P}^A \subseteq \mathrm{NP}^A \cap \mathrm{MOD}_k\mathrm{P}^A$ for all A. Since co-UP^A is contained in $\mathrm{MOD}_k\mathrm{P}^A$ for all A (by definition), Theorem 16 provides an oracle for which the former containment is proper. That oracle also satisfies

$$\mathrm{P}^A \subset \text{co-}\mathrm{NP}^A \cap \mathrm{UP}^A \subseteq \mathrm{UP}^A \subseteq \mathrm{MODZ}_k\mathrm{P}^A$$

(the last containment being obtained by definition), so $\mathrm{P}^A \subset \mathrm{MODZ}_k\mathrm{P}^A$. Finally, note that the constructions for distinct values of k can all be combined. ∎

The preceding theorem also answers a question posed by Ken Regan:

Corollary 18 *There exists an oracle A such that*

$$\mathrm{P}^A \subset \mathrm{UP}^A \subset \mathrm{NP}^A \cap \mathrm{US}^A.$$

Proof: By definition, $\mathrm{UP}^A \subseteq \mathrm{NP}^A \cap \mathrm{US}^A$ for all A. Since co-$\mathrm{UP}^A \subseteq$ co-$\mathrm{NP}^A \subseteq \mathrm{US}^A$ [6] and $\mathrm{UP}^A \subseteq \mathrm{MODZ}_k\mathrm{P}^A$ (by definition) for all A, the Theorem 16 provides an oracle A for which the former containment is proper. As in the preceding proof, $\mathrm{P}^A \subset \mathrm{UP}^A$. ∎

9. Known Inclusions and Separations

In the table below we indicate whether the class in the left column is a subset of the class in the top row. In parentheses we indicate whether the relation holds for at least one, for almost all, or for all oracles. The numbers j and k denote two distinct primes. The results in this table are due to [3, 5, 21, 25] and this paper.

	NP^A	PH^A	$\mathrm{C_{=}P}^A$	PP^A	$\mathrm{MOD}_k\mathrm{P}^A$	$\mathrm{MOD}_j\mathrm{P}^A$	$\mathrm{MOD}_{k^i}\mathrm{P}^A$
NP^A		$\subseteq (\forall)$	$\not\subseteq (\exists)$	$\subseteq (\forall)$	$\not\subseteq (\exists)$		
PH^A	$\not\subseteq$ (a.a.)		$\not\subseteq (\exists)$	?	$\not\subseteq (\exists)$		
$\mathrm{C_{=}P}^A$	$\not\subseteq$ (a.a.)	$\not\subseteq$ (a.a.)		$\subseteq (\forall)$	$\not\subseteq$ (a.a.)		
PP^A	$\not\subseteq$ (a.a.)	$\not\subseteq$ (a.a.)	$\not\subseteq (\exists)$		$\not\subseteq$ (a.a.)		
$\mathrm{MOD}_k\mathrm{P}^A$	$\not\subseteq$ (a.a.)	$\not\subseteq$ (a.a.)	$\not\subseteq (\exists)$	$\not\subseteq (\exists)$		$\not\subseteq$ (a.a.)	$= (\forall)$

Techniques similar to those in this paper have been used to separate other kinds of classes in [2, 9].

10. Open Problems

The last two sections suggest several open problems. We mention the most interesting ones below:

- Is $\mathrm{MOD}_j\mathrm{P} \subseteq \mathrm{MOD}_k\mathrm{P}$ for some j and k relatively prime?
- Is $\mathrm{PH} \subseteq \mathrm{PP}$? This is interesting in light of the recent discovery that $\mathrm{P}^{\mathrm{NP[log]}} \subseteq \mathrm{PP}$ [4] and the very exciting discovery that $\mathrm{PH} \subseteq \mathrm{P}^{\mathrm{PP}}$ [23].
- Is $\oplus\mathrm{P}^A$ or PSPACE^A contained in PP^A for a random oracle A?
- Does $\mathrm{MODZ}_k\mathrm{P}$ have complete sets?

11. Acknowledgments

I am grateful to Bob Floyd for his hospitality during my visit to Stanford University; to John Gill, Johan Hastad, Lane Hemachandra, and Ken Regan for helpful discussions; and to Bill Gasarch and Jacobo Torán for proofreading and valuable suggestions.

References

[1] T. Baker, J. Gill, and R. Solovay. Relativizations of the $P =? NP$ question. *SIAM J. Comput.*, 4:431–442, 1975.

[2] R. Beigel. On the relativized power of additional accepting paths. In *Proceedings of the 4th Annual Conference on Structure in Complexity Theory*, pages 216–224. IEEE Computer Society Press, June 1989.

[3] 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, Feb. 1990. Vol. 415 of *LNCS*.

[4] R. Beigel, L. A. Hemachandra, and G. Wechsung. On the power of probabilistic polynomial time: $\mathrm{P}^{\mathrm{NP}[\log]} \subseteq \mathrm{PP}$. In *Proceedings of the 4th Annual Conference on Structure in Complexity Theory*, pages 225–227, June 1989.

[5] C. H. Bennett and J. Gill. Relative to a random oracle A, $\mathrm{P}^A \neq \mathrm{NP}^A \neq \text{co-NP}^A$ with probability 1. *SIAM J. Comput.*, 10:96–112, Feb. 1981.

[6] A. Blass and Y. Gurevich. On the unique satisfiability problem. *Information and Control*, 55:80–88, 1982.

[7] J. Cai. With probability one, a random oracle separates PSPACE from the polynomial-time hierarchy. In *Proceedings of the 18th Annual ACM Symposium on Theory of Computing*, pages 21–29, 1986.

[8] J. Cai and L. Hemachandra. On the power of parity polynomial time. *Mathematical Systems Theory*. To appear.

[9] J. Díaz and J. Torán. Classes of bounded nondeterminism. Manuscript, 1988.

[10] M. R. Garey and D. S. Johnson. *Computers and Intractability*. W. H. Freeman and Company, New York, 1979.

[11] J. Gill. Computational complexity of probabilistic Turing machines. *SIAM J. Comput.*, 6:675–695, 1977.

[12] L. M. Goldschlager and I. Parberry. On the construction of parallel computers from various bases of Boolean functions. *Theoretical Comput. Sci.*, 43:43–58, 1986.

[13] J. Hartmanis and L. Hemachandra. Complexity classes without machines: On complete languages for UP. *Theoretical Comput. Sci.*, 58:129–142, 1988.

[14] J. Hartmanis and N. Immerman. On complete problems for $\mathrm{NP} \cap \text{co-NP}$. In *Proceedings of the 12th International Colloquium on Automata, Languages, and Programming*, pages 250–259. Springer-Verlag, 1985. Volume 194 of *Lecture Notes in Computer Science*.

[15] J. Hastad. Almost optimal lower bounds for small depth circuits. In *Proceedings of the 18th Annual ACM Symposium on Theory of Computing*, pages 6–20, 1986.

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

[17] M. L. Minksy and S. A. Papert. *Perceptrons*. MIT Press, Cambridge, MA, 1988. Expanded Edition.

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

[19] D. A. Russo. *Structural Properties of Complexity Classes*. PhD thesis, University of California at Santa Barbara, Mar. 1985.

[20] M. Sipser. On relativization and the existence of complete sets. In *Proceedings of the 9th International Colloquium on Automata, Languages, and Programming*, pages 523–531. Springer-Verlag, 1982. Volume 140 of *Lecture Notes in Computer Science*.

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

[22] L. J. Stockmeyer. The polynomial-time hierarchy. *Theoretical Comput. Sci.*, 3:1–22, 1977.

[23] S. Toda. On the computational power of PP and P. In *Proceedings of the 30th IEEE Symposium on Foundations of Computer Science*, pages 514–519, 1989.

[24] J. Torán. An oracle characterization of the counting hierarchy. In *Proceedings of the 3rd Annual Conference on Structure in Complexity Theory*, pages 213–223. IEEE Computer Society Press, June 1988.

[25] J. Torán. *Structural Properties of The Counting Hierarchies*. PhD thesis, Facultat d'Informàtica de Barcelona, 1988.

[26] L. G. Valiant. The complexity of computing the permanent. *Theoretical Comput. Sci.*, 8:189–201, 1979.

[27] K. W. Wagner. The complexity of combinatorial problems with succinct input representation. *Acta Inf.*, 23:325–356, 1986.

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