Relativizing Function Classes

Christian Glaßer[*]
Institut für Informatik
Julius-Maximilians-Universität Würzburg
97072 Würzburg, Germany

Gerd Wechsung[†]
Institut für Informatik
Friedrich-Schiller-Universität Jena
07743 Jena, Germany

13th January 1999

Abstract

The relationships of min·, max·, and #· classes on the polynomial time hierarchy have been studied by various authors during the recent years. In general, inclusions between such classes are equivalent with inclusions between suitable complexity classes. In some cases, no or no satisfactory comparison result is known. For instance, it is not known how min·P relates to #·NP (see [HW97]).

In this paper we provide relativized worlds for most of those inclusion relationships that are not known to be true. As a typical instance for the type of results of this paper, we construct a relativized world for $\min\cdot\mathrm{P} \subseteq \#\cdot\mathrm{NP}$ and another one for $\min\cdot\mathrm{P} \not\subseteq \#\cdot\mathrm{NP}$, thus giving evidence for the problem of comparing these two classes in the unrelativized case to be hard. The strongest results, proved in the paper, are the constructions of oracles D and E, such that $\min\cdot\mathrm{coNP}^D \subseteq \#\cdot\mathrm{P}^D \wedge \mathrm{NP}^D \neq \mathrm{coNP}^D$ and $\mathrm{UP}^E = \mathrm{NP}^E \wedge \min\cdot\mathrm{P}^E \not\subseteq \#\cdot\mathrm{P}^E$.

1 Introduction

This paper deals with classes of the form $\max\cdot\mathcal{C}$, $\min\cdot\mathcal{C}$, and $\#\cdot\mathcal{C}$ where $\mathcal{C}$ belongs to the polynomial time hierarchy. They are defined as follows.

Definition 1 *Let $\mathcal{C}$ be an arbitrary complexity class. (Notice that binary words are also understood as binary representations of natural numbers where leading zeros are ignored.)*

$$f \in \max\cdot\mathcal{C} \iff_{df} \bigvee_{A\in\mathcal{C}} \bigvee_{p\in\mathrm{Pol}} \bigwedge_{x\in\Sigma^*} f(x) = \sup\{y : 0 \leq |y| \leq p(|x|) \wedge \langle x,y\rangle \in A\}$$

Remember that $\sup\emptyset = 0$.

$$f \in \min\cdot\mathcal{C} \iff_{df} \bigvee_{A\in\mathcal{C}} \bigvee_{p\in\mathrm{Pol}} \bigwedge_{x\in\Sigma^*} f(x) = \inf\{y : 0 \leq |y| \leq p(|x|) \wedge \langle x,y\rangle \in A\}$$

We define $\inf\emptyset = 2^{p(|x|)}$.

$$f \in \#\cdot\mathcal{C} \iff_{df} \bigvee_{A\in\mathcal{C}} \bigvee_{p\in\mathrm{Pol}} \bigwedge_{x\in\Sigma^*} f(x) = \#\{y : 0 \leq |y| \leq p(|x|) \wedge \langle x,y\rangle \in A\}$$

Traditionally, complexity classes are understood to be classes of sets (decision problems). Complexity classes of functions — henceforth called *function classes* — have gained much less attention in the literature. Nevertheless, there are quite a lot of mostly recent papers dealing with function classes. As early as 1979, L. Valiant introduced the famous class #P which turned out to be #·P [Val79a]. Along this line, J. Köbler, U. Schöning, and J. Torán considered a class spanP which has been identified to be #·NP, and furthermore the classes #·coNP and $\#\cdot\Delta_2^{\mathrm{P}}$

[*]Supported by Nortel (Northern Telecom).
[†]Supported in part by grant NSF-INT-9513368/DAAD-315-PRO-fo-ab.

([KST89], see also [Köb89]). The study of optimization problems by M. W. Krentel [Kre88], [Kre92] gave rise to consider the classes max·NP and min·NP which have also been investigated by H. Vollmer and K. W. Wagner ([Köb89], [KST89], [Vol94], [VW95]). Closure properties of these and further function classes have been studied by L. Hemachandra and M. Ogiwara [OH93].

The operators min·, max·, and #· are mapping the polynomial time hierarchy to certain hierarchies of function classes. In [HW97] it has been asked how these hierarchies are interrelated. Mainly three kinds of results are reported there (some of these results were known before, for precise references see [HW97]):

1. Inclusions between function classes like $\min\cdot\mathrm{NP} \subseteq \# \cdot \mathrm{coNP}$.

2. Incusions between two function classes being equivalent to inclusions between complexity classes. For example,
$$\#\cdot\mathrm{coNP} \subseteq \min\cdot\mathrm{coNP} \iff \mathrm{PP} \subseteq \mathrm{NP}.$$

3. Inclusions between function classes implying inclusions between complexity classes. For example,
$$\min\cdot\mathrm{coNP} \subseteq \#\cdot\mathrm{P} \Longrightarrow \mathrm{NP} \subseteq \mathrm{UP}.$$

As an exceptional case we mention that neither was it possible to prove the inclusion $\min\cdot\mathrm{P} \subseteq \#\cdot\mathrm{NP}$ nor was it possible to find an equivalent condition for this inclusion or a consequence of it. (By the way, the reverse inclusion $\#\cdot\mathrm{NP} \subseteq \min\cdot\mathrm{P}$ seems highly unlikely since it is equivalent to $\mathrm{P} = \mathrm{PP}$.) All results known by now are represented in Figure 1 which is copied from [HW97].

In this paper, we focus on the inclusion $\min\cdot\mathrm{P} \subseteq \#\cdot\mathrm{NP}$ and on the results of the third kind. We show that both $\min\cdot\mathrm{P} \subseteq \#\cdot\mathrm{NP}$ and $\min\cdot\mathrm{P} \not\subseteq \#\cdot\mathrm{NP}$ can be refuted in suitable relativized worlds (see [KSV98] for another approach). Furthermore, we show that the results of the third kind fail to be equivalences in suitable relativized worlds.

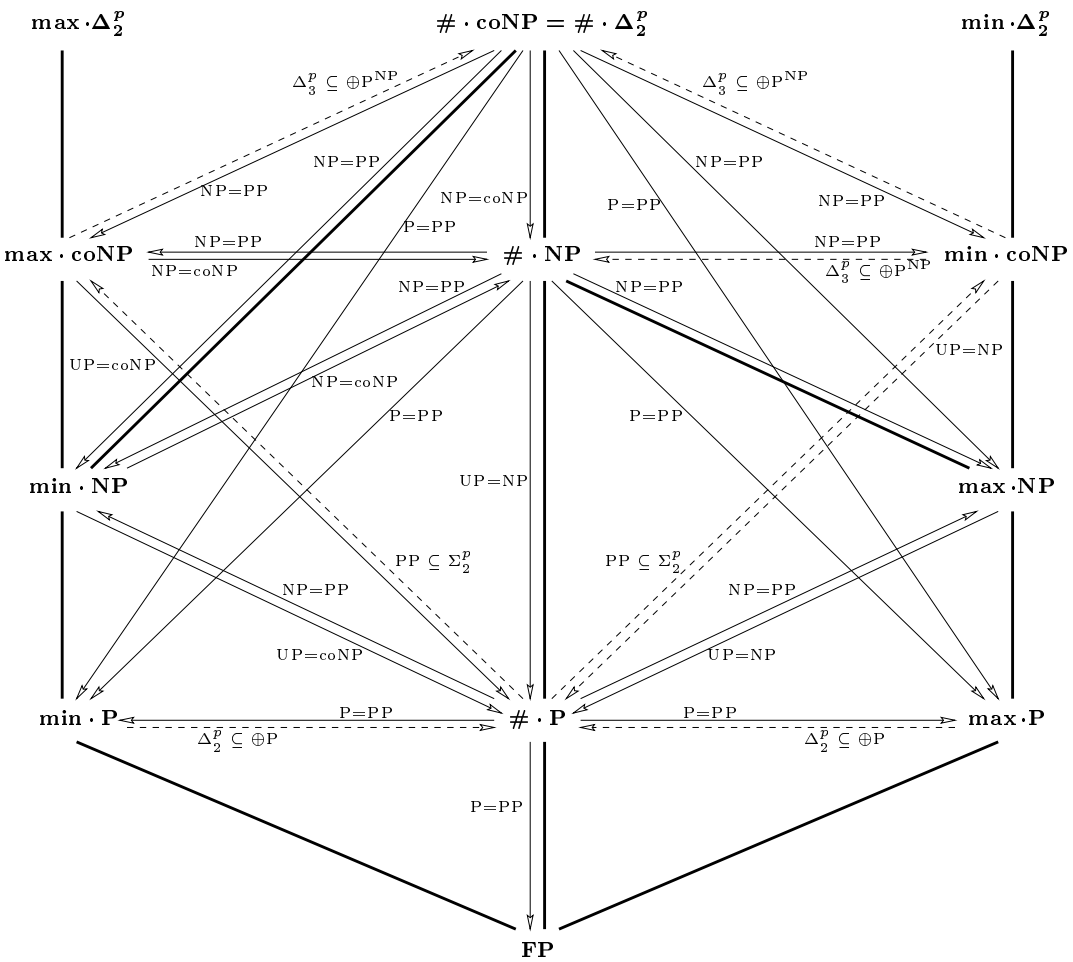
We make use of an appropriate generalization of Rackoff's relativization technique. It enables us to construct an oracle D with $\mathrm{UP}^D = \mathrm{NP}^D \neq \mathrm{coNP}^D$ and additional properties. This strengthens Rackoff's result $\mathrm{UP}^E = \mathrm{NP}^E \neq \mathrm{P}^E$ (for some E), see [Rac82]. The class UP has been introduced by L. Valiant [Val79b]. Remember that a language L belongs to UP if and only if there exists a nondeterministic polynomial time bounded Turing machine M accepting L and having the property $\#_M(x) \neq 0 \Longrightarrow \#_M(x) = 1$.

We summarize some notations. Pol means the set of all polynomials. For a *nondeterministic polynomial time bounded oracle Turing machine* M, NPOM M for short, we use the following abbreviations: $M^C(x)$ is the computation (computation tree) of M^C on input x. The number of accepting paths occuring in this computation is denoted by $\#_{M^C}(x)$. Throughout the paper, $\Sigma = \{0,1\}$, and the words of Σ^* are often understood to be binary representations of natural numbers, where leading zeros are simply ignored. The cardinality of a set X is denoted by $\#X$ or $|X|$. For an NPOM M^C the language accepted by M^C in the sense of coNP is defined to be $\mathrm{L}_{\mathrm{coNP}}(M^C) \stackrel{df}{=} \{x : \#_{M^C}(x) = 0\}$. We define $\Sigma^{\leq i}$, Σ^i, $\Sigma^{\geq i}$ to be the set of all words with lengths $\leq i$, $= i$, $\geq i$, respectively. $\langle x, y\rangle$ denotes a standard polynomial time computable pairing function whose inverses are also computable in polynomial time. For $v, w \in \Sigma^*$, $v \sqsubseteq w$ means that v is a prefix of w. $\overline{A}$ denotes the complement of $A \subseteq \Sigma^*$.

2 Basic Results

C. Rackoff [Rac82] has proved that there exists an oracle E such that $\mathrm{UP}^E = \mathrm{NP}^E \neq \mathrm{P}^E$. Generalizing his proof we get the following strengthened result. Since $\mathrm{UP}^D = \mathrm{NP}^D$ for every oracle D with $\min\cdot\mathrm{coNP}^D \subseteq \#\cdot\mathrm{P}^D$ (cf. Figure 1, the proofs are relativizable) we formulate our result as follows.

Theorem 1 *There exists an oracle D such that*
$$\min\cdot\mathrm{coNP}^D \subseteq \#\cdot\mathrm{P}^D \wedge \mathrm{NP}^D \neq \mathrm{coNP}^D.$$



Key: a bold line indicates an inclusion of the lower in the upper class

$\mathcal{F}_1 \overset{\alpha}{\dashrightarrow} \mathcal{F}_2$ means : $\mathcal{F}_1 \subseteq \mathcal{F}_2 \Longrightarrow \alpha$

$\mathcal{F}_1 \xrightarrow{\alpha} \mathcal{F}_2$ means : $\mathcal{F}_1 \subseteq \mathcal{F}_2 \iff \alpha$

Figure 1: Inclusions between function classes

Proof Let $M_1, M_2, \ldots$ be an effective enumeration of all NPOM and let p_i be the running time for M_i (independent of the oracle). Without loss of generality we may assume $p_i(j) < j^i$ for all i and j. For an arbitrary set D define

$$L^D \stackrel{df}{=} \left\{ x : \bigvee_y (|x| = |y| \wedge y \in D) \right\},$$

$$m^D(w) \stackrel{df}{=} \inf \left\{ y : |y| \leq m \wedge M_j^D(\langle x, y \rangle) \text{ has no path accepting within } k \text{ steps} \right\} \qquad \text{if } w = 0^j 10^k 10^m 1x,$$

$$m^D(w) \stackrel{df}{=} 0 \qquad \text{otherwise.}$$

Depending on the context we will consider m^D either as the word function $m^D : \Sigma^* \longrightarrow \Sigma^*$ or as the function of natural numbers $m^D : \mathbb{N} \longrightarrow \mathbb{N}$. Notice that $\inf \emptyset \stackrel{df}{=} 2^m$ in the above definition.

For functions f and g we define $f \leq_m^p g$ to mean that there exists a polynomial time computable function h s.t. $f(w) = g(h(w))$ for all w. If $\mathcal{F}$ is a function class then $g \in \mathcal{F}$ is called $\leq_m^p$-complete in $\mathcal{F}$ if $f \leq_m^p g$ for all $f \in \mathcal{F}$. The following fact is obvious.

Fact 1 *$L^D \in \mathrm{NP}^D$ and m^D is $\leq_m^p$-complete in $\min{\cdot}\mathrm{coNP}^D$.*

We construct D in such a way that it satisfies two conditions:

1. $L^D \notin \mathrm{coNP}^D$.
2. For a given $w \in \Sigma^*$ the number of words z with $|z| = 3 \cdot |w| \wedge wz \in D$ is exactly $m^D(w)$.

The former implies $\mathrm{NP}^D \neq \mathrm{coNP}^D$, the latter implies $m^D \in \#{\cdot}\mathrm{P}^D$ and thus $\min{\cdot}\mathrm{coNP}^D \subseteq \#{\cdot}\mathrm{P}^D$. We consider Σ^* to be ordered in the usual way $\varepsilon < 0 < 1 < 00 < 01 < \ldots$ (levelwise, and lexicographic within each level, ε being the empty word). Oracles are identified with the sequence of the values of their characteristic function c_D with respect to the given ordering of Σ^*. We say that an initial segment D' of D extends up to level n, if $D' = (c_D(\varepsilon), c_D(0), \ldots, c_D(1^n))$.

We define D by constructing a sequence $(D_i)_{i \in \mathbb{N}}$ of its initial segments with the following properties: $D_0 = \emptyset$, D_i extends up to level i, and $D_i \sqsubseteq D_{i+1}$.

During Step i it may happen that words of length greater than i must be put into $\overline{D}$. Since in this step, D is constructed only up to level i, we shall consider those words to be frozen which means that they must never become elements of D. Let F_i be the set of words from $\Sigma^{\geq i}$ frozen at the beginning of Step i, $F_0 = \emptyset$. We maintain the following condition

$$|F_i| \leq 2^{\frac{i}{4}} \qquad (*)$$

We keep a list L of natural numbers (indices of machines) which is initially empty. $j \in L$ means that $L^D \neq L_{\mathrm{coNP}}(M_j^D)$ has already been guaranteed. Now we describe Step i of the construction of D (construction of D_i).

$\underline{\mathbf{i \equiv 0 (4)}}$ — In this case, we contribute to satisfy Condition 2. For each $w \in \Sigma^{\frac{i}{4}}$ we determine $m^D(w)$. This can be done as follows. If $w = 0^l 10^k 10^m 1x$, then we determine the least y with $|y| \leq m$, such that $M_l^{D_{i-1}}(\langle x, y \rangle)$ has no path accepting within k steps. Since only words of length $\leq k < i$ can be queried about, the oracle D_{i-1} can be used instead of D.

Notice that $m^D(w) \leq 2^{\frac{i}{4}}$. Because of $(*)$, there are at least $2^{\frac{3i}{4}} - 2^{\frac{i}{4}}$ words of lenghts i with prefix w that are not frozen. Hence, for every w we find $m^D(w)$ words z such that wz is not frozen and $|wz| = i$. We obtain D_i by adding for every w exactly $m^D(w)$ such words to D_{i-1}. In this step, no new words are frozen. Hence, Condition $(*)$ is maintained. [1]

[1] This ensures $\min{\cdot}\mathrm{coNP}^D \subseteq \#{\cdot}\mathrm{P}^D$. To see this, consider an arbitrary $f \in \min{\cdot}\mathrm{coNP}^D$. Then there exist an NPOM M_j and a $q \in \mathrm{Pol}$ such that $f(x) = \inf \{ y : |y| \leq q(|x|) \wedge \langle x, y \rangle \in L_{\mathrm{coNP}}(M_j^D) \}$. Let p_j be the runtime of M_j. The function f belongs to $\#{\cdot}\mathrm{P}^D$ since $f = \#_M$ for the following machine M. On input x, M first computes the word $w = 0^j 10^{p_j(|x|)} 10^{q(|x|)} 1x$. Then in a nondeterministic way it generates all words z such that $|z| = 3 \cdot |w|$ and queries about wz. It accepts on exactly those paths, where the answer is positive. By the construction of D, the number of accepting paths is just $m^D(w) = f(x)$.

i $\not\equiv$ 0(4) — In these steps we make a distinction between several cases. Let j be the smallest number not on L.

Case 1. — $F_i \neq \emptyset \vee 2 \cdot p_j(i)^2 \geq 2^{\frac{i}{4}}$

In this case, we set $D_i = D_{i-1}$. No new words are frozen. Hence, Condition $(*)$ is maintained. If Case 1 happens, after a finite number of steps we reach an i such that the condition of Case 2 is satisfied.

Case 2. — $F_i = \emptyset \wedge 2 \cdot p_j(i)^2 < 2^{\frac{i}{4}}$

Here we contribute to satisfy Condition 1. We want to achieve that $L^D \neq L_{\mathrm{coNP}}(M_j^D)$.

Case 2.1. — $M_j^{D_{i-1}}$ does not accept 0^i in the sense of coNP, i.e. the computation $M_j^{D_{i-1}}(0^i)$ has an accepting path. We fix some accepting path α and try to extend D_{i-1} in such a way, that α is preserved. $M_j^{D_{i-1}}$ on input 0^i works at most $p_j(i) < 2^{\frac{i}{4}}$ steps. Thus, no more than $2^{\frac{i}{4}}$ queries can occur on α. As $F_i = \emptyset$ we can choose a word w of length i not queried about on α, and we set $D_i = D_{i-1} \cup \{w\}$ and freeze all queries on α of lengths $\geq i$. This guarantees $L^D \neq L_{\mathrm{coNP}}(M_j^D)$ since $0^i \in L^D$, but $0^i \notin L_{\mathrm{coNP}}(M_j^D)$. Put j on L. Notice that Condition $(*)$ is satisfied.

Case 2.2. — $M_j^{D_{i-1}}$ accepts 0^i in the sense of coNP. In this case we continue constructing the oracle segments $D'_i, D'_{i+1}, \ldots, D'_{p_j(i)}$ with the modification that in all steps i' with $i' \not\equiv 0(4)$ nothing will be done. The effect of this *tentative* construction phase is that $D'_{p_j(i)}$ is large enough to answer all possible queries of $M_j^{D_{i-1}}(0^i)$.

Case 2.2.1. — $M_j^{D'_{p_j(i)}}$ accepts 0^i in the sense of coNP. If we set $D_{p_j(i)} = D'_{p_j(i)}$ we conclude that M_j^D accepts 0^i also in the sense of coNP. This is true because M_j on input 0^i can ask only queries of length up to $p_j(i)$. This means, extending $D_{p_j(i)}$ will have no influence on the computation of M_j on input 0^i. During the tentative construction phase leading to $D'_{p_j(i)}$ no word of length i has been added to the oracle. Thus, $0^i \notin L^D$, and hence we have in this case $L^D \neq L_{\mathrm{coNP}}(M_j^D)$. Put j on L. No words are frozen, $(*)$ is satisfied. The next step $p_j(i)+1$ can be carried out.

Case 2.2.2. — $M_j^{D'_{p_j(i)}}$ rejects 0^i in the sense of coNP. In this case we fix an accepting path α of this computation. Our goal is to construct a new oracle $D_{p_j(i)}$ such that $\{w\} \subseteq D_{p_j(i)}$ for some word w of length i in such a way that α remains an accepting path of $M_j^D(0^i)$ and Condition 2 remains satisfied. The remainder of the proof makes sure that this is possible. This would lead to $L^D \neq L_{\mathrm{coNP}}(M_j^D)$.

We first analyze what has to be done to reach this goal. To preserve α with the oracle $D_{p_j(i)}$ we have to make sure that all queries on α of lengths greater than $i-1$ are, in all future, answered in the same way as they were answered with oracle $D'_{p_j(i)}$. Queries of lengths $\geq i$ which are answered negatively must be frozen, say in the set of frozen negative words F_1^-. Denote the set of positively answered queries of lengths $> i$ by P_1. It is easy to see that they must be of the form $q = 0^l 10^k 10^m 1xy$, where $3 \cdot |0^l 10^k 10^m 1x| = |y|$.[2] We will make sure that $P_1 \subseteq D_{p_j(i)}$, $F_1^- \subseteq \overline{D_{p_j(i)}}$, and $D_{p_j(i)}$ satisfies Condition 2.

Let $q = 0^l 10^k 10^m 1xy \in P_1$. We call $0^l 10^k 10^m 1x$ (i.e. the first $\frac{|q|}{4}$ bits of q) the prefix of q. We partition P_1 into classes $[v]$ of words with the same prefix. Let $P_1 = [v_1] \cup \ldots \cup [v_s]$ and $n_i = |[v_i]|$. If λ_1 is the sum of the lengths of all queries on α, l_1 is the sum of the lengths of all queries of P_1, and f_1 is the sum of the lengths of all words from F_1^-, we get $\lambda_1 = l_1 + f_1 = f_1 + n_1|v_1| + \ldots + n_s|v_s| \leq p_j(i)$. Now let u_1 be the largest word in P_1, let $n_1 = |[u_1]|$, and let its prefix be $w = 0^l 10^k 10^m 1x$. Since $D'_{p_j(i)}$ satisfies Condition 2 there exist exactly $m^{D'_{p_j(i)}}(w)$ words z with $|z| = 3 \cdot |w| \wedge wz \in D'_{p_j(i)}$. On the other hand $[u_1] \subseteq P_1 \subseteq D'_{p_j(i)}$, hence $n_1 = |[u_1]| \leq m^{D'_{p_j(i)}}(w)$. Thus the computations $M_l^{D'_{p_j(i)}}(\langle x, 0\rangle), \ldots, M_l^{D'_{p_j(i)}}(\langle x, n_1 - 1\rangle)$ have accepting paths $\alpha_0, \ldots, \alpha_{n_1-1}$ of lengths $\leq k$, respectively.

[2] Since we left out the steps $i' \equiv 0(4)$ during the construction of $D'_i, \ldots, D'_{p_j(i)}$.

To achieve $[u_1] \subseteq D_{p_j(i)}$ it suffices to preserve the accepting paths $\alpha_0, \ldots, \alpha_{n_1-1}$. This prevents the computations $M_l^D(\langle x, n' \rangle)$ with $n' < n_1$ from accepting in the sense of coNP which would imply $m^D(w) = n' < n_1$ which, in turn, would injure Condition 2 (remember that we want to achieve $[u_1] \subseteq D_{p_j(i)}$).
To preserve the accepting paths $\alpha_0, \ldots, \alpha_{n_1-1}$, we have to freeze all queries of lengths $\geq i$ which are answered negatively in a set F_2^-. The positively queried words of lengths $> i$ are put into a set P_2'. Now define $F_1^+ = [u_1]$ and $P_2 = (P_1 \setminus [u_1]) \cup P_2'$. Let l_2 be the sum of the lengths of all words of P_2. Since the paths $\alpha_0, \ldots, \alpha_{n_1-1}$ are no longer than $k < \frac{1}{4}|u_1|$, the sum of the lengths of all words of P_2' is smaller than $\frac{1}{4}n_1|u_1|$. Thus, $l_2 < l_1$.
Now P_2 is treated like P_1, i.e. we determine the largest $u_2 \in P_2$ and do for u_2 what we have done for u_1 finally getting some F_2^+ and some P_3. For the appropriately defined l_3 we get $l_3 < l_2$. If we repeat this procedure, three things should be observed:

1. To achieve $F_{\mu-1}^+ \subseteq D_{p_j(i)}$ it suffices to ensure that $P_\mu \subseteq D_{p_j(i)}$ (for $\mu > 1$).

2. Since u_1 (with prefix w) is the largest word in P_1, no words with prefix w will be added to the subsequent sets P_μ (for $\mu > 1$), because for each $\mu \geq 1$ we have $|u_\mu| > \max\{|v| : v \in P_\mu'\}$. Thus, in order to guarantee Condition 2 with respect to words with prefix w it is sufficient to preserve the paths $\alpha_0, \ldots, \alpha_{n_1-1}$ (i.e. to preserve $m^D(w) \geq n_1$). Similarly we argue for all subsequent steps.

3. Since $p_j(i) \geq l_1 > l_2 > \ldots$ is a strictly decreasing sequence, the procedure stops after at most $p_j(i)$ steps with an empty P_μ.

Altogether we reach sets $F^- = F_1^- \cup F_2^- \cup \ldots$ and $F^+ = F_1^+ \cup F_2^+ \cup \ldots$. Since in each of the at most $p_j(i)$ steps we add at most $p_j(i)$ words to F^- as well as to F^+, we conclude

$$|F^-| + |F^+| \leq 2 \cdot p_j(i)^2 < 2^{\frac{i}{4}}. \qquad (**)$$

Now we actually redo the steps of the tentative phase (again, in steps i' with $i' \not\equiv 0(4)$ nothing will be done) and we shall achieve the following two goals.

- $0^i \in L^D$.
- $0^i \notin L_{\mathrm{coNP}}(M_j^D)$ by maintaining the path α.

Condition $(**)$ has the consequence that we can choose a word $w \in \Sigma^i$ not belonging to F^-. As $|w| \not\equiv 0(4)$, Condition 2 cannot be injured. We define $D_i = D_{i-1} \cup \{w\}$. This yields the first goal. To reach the second one we recall from $(**)$ that:

$$|F^-| < 2^{\frac{i}{4}}. \qquad (***)$$

In any step i' with $i' \equiv 0(4)$, words of the form $w' = 0^l 10^k 10^m 1x$ with $|w'| = \frac{i'}{4}$ will be treated w.r.t. F^- and F^+. This means, if we have to put n words with prefix w' into the oracle, then we choose at first the words of F^+ with prefix w', and then words not in F^-. By $(***)$, such words can always be found. Notice that w does not influence any of those words and paths which have been fixed (via F^- and F^+) during the tentative phase. From this it follows that $P_1 \subseteq F^+ \subseteq D_{p_j(i)}$. Hence $M_j^{D_{p_j(i)}}(0^i)$ has still the path α, i.e. $0^i \notin L_{\mathrm{coNP}}(M_j^D)$. Since F^- contains only words of lengths $\leq p_j(i)$ we have no frozen words on stages $\geq p_j(i) + 1$, thus $F_{p_j(i)+1} = \emptyset$ and Condition $(*)$ is maintained. Finally, j is put on L. The next step $p_j(i) + 1$ can be carried out.
$0^i \in L^D$, but $0^i \notin L_{\mathrm{coNP}}(M_j^D)$. Therefore, the constructed oracle satisfies Condition 1 and Condition 2. This proves our theorem. ∎

Theorem 2 *There exists an oracle D such that*

$$\mathrm{UP}^D = \mathrm{NP}^D \wedge \min\cdot\mathrm{P}^D \not\subseteq \#\cdot\mathrm{P}^D$$

Proof The proof is similar to that of Theorem 1. Let $M_1, M_2, \ldots$ be an effective enumeration of all NPOM and let p_i be the running time for M_i (independent of the oracle). We may assume $p_i(j) < j^i$ for all i and j. For an arbitrary set D define

$$\begin{aligned} A^D &\stackrel{df}{=} \{(x,y) : |x| = |y| \wedge y \in D\} \\ f^D(x) &\stackrel{df}{=} \inf\left\{y : |y| \leq |x| \wedge (x,y) \in A^D\right\} \qquad \textit{where} \quad \inf\emptyset \stackrel{df}{=} 2^{|x|} \\ K^D &\stackrel{df}{=} \left\{0^l 10^k 1x : M_l^D(x) \text{ accepts within } k \text{ steps}\right\} \end{aligned}$$

The following fact is obvious.

Fact 2 *$A^D \in \mathrm{P}^D$, $f^D \in \min\cdot\mathrm{P}^D$ and K^D is $\leq_m^p$-complete in NP^D.*

We construct D in such a way that it satisfies the following conditions:

1. $f^D \notin \#\cdot\mathrm{P}^D$.
2. For every $x \in K^D$ there exists exactly one word z with $|x| = |z| \wedge xz \in D$, and for every $x \notin K^D$ there is no word z with $|x| = |z| \wedge xz \in D$.

The former implies $\min\cdot\mathrm{P}^D \not\subseteq \#\cdot\mathrm{P}^D$, the latter implies $K^D \in \mathrm{UP}^D$ and thus $\mathrm{UP}^D = \mathrm{NP}^D$. As in the proof of Theorem 1 we consider Σ^* to be ordered in the usual way, oracles are identified with the sequence of the values of their characteristic function, and D is defined by constructing a sequence $(D_i)_{i\in\mathbb{N}}$ of its initial segments with the properties: $D_0 = \emptyset$, D_i extends up to level i, and $D_i \sqsubseteq D_{i+1}$. Let F_i be the set of words from $\Sigma^{\geq i}$ frozen at the beginning of Step i, $F_0 = \emptyset$. We maintain the following condition

$$|F_i| < 2^{\frac{i}{2}} \qquad (*)$$

We keep a list L of natural numbers (indices of machines) which is initially empty. $j \in L$ means that $f^D \neq \#_{M_j^D}$ has already been guaranteed. Now we describe Step i of the construction of D.

$\underline{\mathbf{i \equiv 0(2)}}$ — In this case, we contribute to satisfy Condition 2. For each $x \in \Sigma^{\frac{i}{2}}$ we find out whether $x \in K^D$. This can be done as follows. If $x = 0^l 10^k 1y$, then we let $M_l^{D_{i-1}}$ run on input y for k steps. Since only words of length $\leq k < i$ can be queried about, the oracle D_{i-1} can be used instead of D. Because of $(*)$ for each $x \in K^D \cap \Sigma^{\frac{i}{2}}$ we can find at least one $z \in \Sigma^{\frac{i}{2}}$ such that xz is not frozen. For each $x \in K^D \cap \Sigma^{\frac{i}{2}}$ we arbitrarily fix such a z_x and define $D_i = D_{i-1} \cup \left\{xz_x : x \in K^D \cap \Sigma^{\frac{i}{2}}\right\}$. In this step, no new words are frozen. Hence, Condition $(*)$ is maintained.

$\underline{\mathbf{i \equiv 1(2)}}$ — Let j be the smallest number not on L.

Case 1. — $F_i \neq \emptyset \vee 8 \cdot p_j(i)^2 \geq 2^{\frac{i}{2}}$
In this case, we set $D_i = D_{i-1}$. No new words are frozen. Hence, Condition $(*)$ is maintained. If Case 1 happens, after a finite number of steps we reach an i such that the condition of Case 2 is satisfied.

Case 2. — $F_i = \emptyset \wedge 8 \cdot p_j(i)^2 < 2^{\frac{i}{2}}$
Here we contribute to satisfy Condition 1. We want to achieve that $f^D(0^i) \neq \#_{M_j^D}(0^i)$. As in the proof of Theorem 1 we perform a *tentative* construction phase. This means that we continue constructing the oracle segments $D'_i, D'_{i+1}, \ldots, D'_{p_j(i)}$ with the modification that in all odd steps $> i$ nothing will be done, and in Step i at most two words will be added to the oracle.
Let $m \stackrel{df}{=} 8 \cdot p_j(i)^2$. We introduce the following notation for words of length i (remember that $bin(a)$ is the binary representation of the natural number a):

$$w_a \stackrel{df}{=} 0^{i-|bin(a)|} bin(a).$$

(Actually, w_a depends also on i, but for the sake of simplicity we suppress this index.) This means that we enlarge the word $bin(a)$ to size i. For every oracle D', the length of queries asked about in compuation $M_j^{D'}(0^i)$ is no larger than $p_j(i)$. In even steps (of our *tentative* construction

phase) there are several possibilities to choose the words z_x. Thus there are different ways to construct the oracle up to Stage $p_j(i)$ (i.e. $D'_{p_j(i)}$), simultaneously maintaining Condition 2. We want to show that among these oracles there exists an $E \stackrel{df}{=} D'_{p_j(i)}$ which extends to stage $p_j(i)$, such that $f^E(0^i) \neq \#_{M^E}(0^i)$. We will show this by contradiction.

Assumption: Suppose, $f^E(0^i) = \#_{M_j^E}(0^i)$ for every continuation $D'_i, D'_{i+1}, \ldots, D'_{p_j(i)} = E$ in the *tentative* construction phase. If we consider those continuations, where $D'_i = D_{i-1} \cup \{w_m\}$, then our assumption says $f^E(0^i) = \#_{M_j^E}(0^i) = m$. We denote the accepting paths of computation $M_j^E(0^i)$ by $q_1, \ldots, q_m$.

In the following we want to preserve these paths, i.e. we have to freeze the positive and negative answers given along these paths. Before we do this, let us compare the freezing-methods of Theorem 1 and of this theorem.

In the proof of Theorem 1 we could not freeze single words, but we were able to freeze groups of words having the same prefix. To freeze such a group (say of size n' and with prefix p') we had to guarantee that the min·coNP-function induced by p' has a value $\geq n'$. We did this by preserving n' paths of n' different rejecting coNP-computations. For a *single* word w' with prefix p' we could not determine the set of words on which w' depends (for this we would need the remaining words with prefix p'). Let us check this in the following example:

- If u' is the only word with prefix p' we want to freeze, then it is sufficient to guarantee that the min·coNP-function induced by p' has a value ≥ 1. Thus u' depends on path α'_0.
- If v', v'' are the only words with prefix p' we want to freeze, then it is sufficient to guarantee that the min·coNP-function induced by p' has a value ≥ 2. Thus either v' or v'' depends on path α'_1.

Hence, for one word w' (either v' or v'') we cannot determine the set of words on which w' depends, because this set is not well defined (it depends on the other words with prefix p').

In contrast to Theorem 1 now we are able to determine this set for a single word w'. We will see that other words we want to freeze do not change this set. Therefore, the set of words on which w' depends is well defined and we can work with this notion.

The difference between these freezing-methods is important. Otherwise we could apply the method of Theorem 2 to Theorem 1. We would obtain an oracle D' with $\min\cdot\mathrm{coNP}^{D'} \subseteq \#\cdot\mathrm{P}^{D'} \wedge \min\cdot\mathrm{P}^{D'} \not\subseteq \#\cdot\mathrm{P}^{D'}$, this would be a contradiction.

Now we can describe the freezing-method for this theorem. Let us consider a $w \in E$ of length $\geq i$. Thus w is of the form $w = 0^l 10^k 1xy$ with $|y| = \frac{|w|}{2}$. This means $M_l^E(x)$ accepts within k steps, say on path α. Therefore, if we want to keep w in the oracle, we have to preserve the path α. Notice that the length of α is $\leq k < \frac{|w|}{2}$. We freeze the set of negatively answered queries in the set N_w. If P_w is the set of positively answered queries on α, then the sum of lengths of words in $P_w \cup N_w$ is smaller than $\frac{|w|}{2}$. We can use this argument inductively to freeze the words of P_w. Therefore, we can guarantee $w \in E$ by freezing at most $|w|$ words of lengths $\leq |w|$.

Now let us consider a path q of $M_j^E(0^i)$. Notice that the length of q is $\leq p_j(i)$, thus on q at most $p_j(i)$ words of lengths $\leq p_j(i)$ can be queried about. If F^+ (F^-, resp.) denotes the set of positive (negative, resp.) words, frozen in order to preserve q, we obtain:

$$|F^-| + |F^+| \leq p_j(i)^2 < 2 \cdot p_j(i)^2 < 2^{\frac{i}{2}}. \qquad (**)$$

For every $k = 1, \ldots, m$ we denote the set of positive (negative) frozen words to preserve path q_k by $F^+_{q_k}$ ($F^-_{q_k}$, resp.). Now we can make a list of statements:

1. For all paths $q \in \{q_1, \ldots, q_m\}$ we have $w_0 \in F_q^- \cup F_q^+$. Otherwise let $r_1 \in \{q_1, \ldots, q_m\}$ be a path with $w_0 \notin F^-_{r_1} \cup F^+_{r_1}$. Then we can take w_0 to our oracle, and we can preserve path r_1 via $F^+_{r_1}$ and $F^-_{r_1}$. Thus $f^E(0^i) = 0$, but $\#_{M_j^{(E)}}(0^i) > 0$. This would be a contradiction to our assumption.

2. For at least $m-1$ paths $q \in \{q_1, \ldots, q_m\}$ we have $w_1 \in F_q^- \cup F_q^+$. Otherwise let $r_1, r_2 \in \{q_1, \ldots, q_m\}$ be different paths with $w_1 \notin F^-_{r_1} \cup F^+_{r_1} \cup F^-_{r_2} \cup F^+_{r_2}$. Then we can take w_1 to

our oracle, and we can preserve paths r_1, r_2 via $F^+_{r_1}$, $F^-_{r_1}$, $F^+_{r_2}$ and $F^-_{r_2}$. Thus $f^E(0^i) = 1$, but $\#_{M_j^{(E)}}(0^i) > 1$. This would be a contradiction to our assumption.

We can continue this list of statements, we consider the first $\frac{m}{2}$ of them. From Statement k with $k \in \{1, \ldots, \frac{m}{2}\}$ we obtain the following weakened statement: For at least $\frac{m}{2}$ paths $q \in \{q_1, \ldots, q_m\}$ we have $w_k \in F^-_q \cup F^+_q$. By a pigeon hole argument we conclude, that there exists a path $\tilde{q} \in \{q_1, \ldots, q_m\}$, such that $w \in F^-_{\tilde{q}} \cup F^+_{\tilde{q}}$ for at least $\frac{m}{4}$ different words $w \in \{w_0, \ldots, w_{m-1}\}$. Together with $(**)$ this implies

$$2 \cdot p_j(i)^2 = \frac{m}{4} \leq |F^-_{\tilde{q}} \cup F^+_{\tilde{q}}| \leq |F^-_{\tilde{q}}| + |F^+_{\tilde{q}}| < 2 \cdot p_j(i)^2.$$

This is a contradiction. Therefore, our assumption was false, and we are sure that there exists a continuation $D'_i, D'_{i+1}, \ldots, E$ with $f^E(0^i) \neq \#_{M_j^E}(0^i)$. Since we have no frozen words of lengths $\geq p_j(i) + 1$, $F_{p_j(i)+1} = \emptyset$ and Condition $(*)$ is maintained. Finally, put j on L. The next step can be carried out. This proves the theorem. ■

3 Relationships between #·-classes and min·-max· classes

If we want to establish all possible relationships between #·-classes (#·P, #·NP) and the min·-max· classes (cf. Figure 1) in relativized worlds it is sufficient that we restrict ourselfs to the strongest possible ones. If, for instance, $\max\cdot\mathrm{coNP}^A \subseteq \#\cdot\mathrm{P}^A$ for some oracle A has been proved, then for this oracle all statements $\mathcal{C}^A \subseteq \mathcal{D}^A$ with $\mathcal{C} \subseteq \max\cdot\mathrm{coNP}$ and $\#\cdot\mathrm{P} \subseteq \mathcal{D}$ are also true ($\mathcal{C}$, $\mathcal{D}$ are classes from Figure 1). In this sense we have to focus on the following relationships:

1. $\max\cdot\mathrm{coNP}, \min\cdot\mathrm{coNP} \subseteq \#\cdot\mathrm{P}$
2. $\#\cdot\mathrm{NP} \subseteq \min\cdot\mathrm{P}, \max\cdot\mathrm{P}$
3. $\#\cdot\mathrm{P} \not\subseteq \max\cdot\mathrm{coNP}, \min\cdot\mathrm{coNP}$
4. $\min\cdot\mathrm{P} \not\subseteq \#\cdot\mathrm{NP}$
5. $\max\cdot\mathrm{P} \not\subseteq \#\cdot\mathrm{P}$

Notice the slight asymmetry in the behavior of min·P and max·P as expressed in 4 and 5. We show that all these statements are possible in suitable relativized worlds. For the first and the second statement it suffices to choose an oracle E with $\mathrm{P}^E = \mathrm{PSPACE}^E$.

Theorem 3 *There exists an oracle E such that*

$$\max\cdot\mathrm{coNP} = \min\cdot\mathrm{coNP} = \#\cdot\mathrm{P} = \#\cdot\mathrm{NP} = \min\cdot\mathrm{P} = \max\cdot\mathrm{P}.$$

The following theorem provides an oracle for Statement 3.

Theorem 4 *There exists an oracle D such that*

$$\#\cdot\mathrm{P}^D \not\subseteq \min\cdot\mathrm{coNP}^D \wedge \#\cdot\mathrm{P}^D \not\subseteq \max\cdot\mathrm{coNP}^D.$$

Proof It is known from [Yao85] that there is an oracle D such that PH^D does not collapse to a finite level. Suppose $\#\cdot\mathrm{P}^D \subseteq \min\cdot\mathrm{coNP}^D$ or $\#\cdot\mathrm{P}^D \subseteq \max\cdot\mathrm{coNP}^D$. This implies $\mathrm{PP}^D \subseteq \Sigma_2^{\mathrm{P}D}$ (cf. Figure 1, the proofs are relativizable). Since Toda's theorem [Tod89] $\mathrm{PH} \subseteq \mathrm{P}^{\mathrm{PP}}$ is relativizable we obtain a collapse of PH^D. This is a contradiction. Thus, $\#\cdot\mathrm{P}^D \not\subseteq \min\cdot\mathrm{coNP}^D$ and $\#\cdot\mathrm{P}^D \not\subseteq \max\cdot\mathrm{coNP}^D$. ■

Now we consider Statement 5. J. Torán [Tor91] has constructed an oracle E such that $\mathrm{NP}^E \not\subseteq \oplus\cdot\mathrm{P}^E$. It is easy to see that $\mathrm{NP}^D \subseteq \oplus\cdot\mathrm{P}^D$ for every oracle D with either $\min\cdot\mathrm{P}^D \subseteq \#\cdot\mathrm{P}^D$

or $\max\cdot\mathrm{P}^D \subseteq \#\cdot\mathrm{P}^D$, (cf. Figure 1, the proofs are relativizable). Therefore, Torán's oracle proves the following theorem.

Theorem 5 *There exists an oracle E such that*

$$\min\cdot\mathrm{P}^E \not\subseteq \#\cdot\mathrm{P}^E \wedge \max\cdot\mathrm{P}^E \not\subseteq \#\cdot\mathrm{P}^E.$$

Since $\max\cdot\mathrm{P} \subseteq \#\cdot\mathrm{NP}$ is relativizable, $\max\cdot\mathrm{P}^D \not\subseteq \#\cdot\mathrm{P}^D$ implies $\#\cdot\mathrm{P}^D \neq \#\cdot\mathrm{NP}^D$. Hence, for the oracle of Theorem 5 we must have $\#\cdot\mathrm{P}^E \neq \#\cdot\mathrm{NP}^E$. On the other hand, $\min\cdot\mathrm{P}^D \not\subseteq \#\cdot\mathrm{P}^D$ is compatible with $\#\cdot\mathrm{P}^D = \#\cdot\mathrm{NP}^D$ as is stated in the next theorem. Simultaneously, this also shows that Statement 4 is reachable in some relativized world.

Theorem 6 *There exists an oracle D such that*

$$\min\cdot\mathrm{P}^D \not\subseteq \#\cdot\mathrm{P}^D = \#\cdot\mathrm{NP}^D \wedge \mathrm{UP}^D = \mathrm{NP}^D \neq \mathrm{coNP}^D.$$

Proof This theorem is an easy consequence of Theorem 2. Notice that the proofs for $\mathrm{UP} = \mathrm{NP} \Longrightarrow \#\cdot\mathrm{P} = \#\cdot\mathrm{NP}$ and $\mathrm{NP} = \mathrm{coNP} \Longrightarrow \min\cdot\mathrm{P} \subseteq \#\cdot\mathrm{NP}$ are relativizable (cf. Figure 1). ■

4 Further remarks and open problems

From [HW97] we know the implications

- $\min\cdot\mathrm{coNP} \subseteq \#\cdot\mathrm{P} \Longrightarrow \mathrm{UP} = \mathrm{NP}$
- $\min\cdot\mathrm{coNP} \subseteq \#\cdot\mathrm{P} \Longleftarrow \mathrm{UP} = \mathrm{coNP}$

We would like to find a statement that is equivalent to $\min\cdot\mathrm{coNP} \subseteq \#\cdot\mathrm{P}$. However, none of these right hand sides is likely to serve this purpose. This follows from the next two theorems showing that

$$\begin{aligned} \min\cdot\mathrm{coNP} \subseteq \#\cdot\mathrm{P} &\Longrightarrow \mathrm{UP} = \mathrm{coNP} \\ \mathrm{UP} = \mathrm{NP} &\Longrightarrow \min\cdot\mathrm{coNP} \subseteq \#\cdot\mathrm{P} \end{aligned}$$

are not relativizable.

Theorem 7 *There exists an oracle D such that*

$$\min\cdot\mathrm{coNP}^D \subseteq \#\cdot\mathrm{P}^D \wedge \mathrm{UP}^D = \mathrm{NP}^D \neq \mathrm{coNP}^D.$$

Proof This follows from Theorem 1, since $\min\cdot\mathrm{coNP} \subseteq \#\cdot\mathrm{P} \Longrightarrow \mathrm{UP} = \mathrm{NP}$ is relativizable. ■

Theorem 8 *There exists an oracle D such that*

$$\min\cdot\mathrm{coNP}^D \not\subseteq \#\cdot\mathrm{P}^D \wedge \mathrm{UP}^D = \mathrm{NP}^D \neq \mathrm{coNP}^D.$$

Proof This follows from Theorem 2 and the relativizable facts

- $\min\cdot\mathrm{P} \subseteq \min\cdot\mathrm{coNP}$
- $\mathrm{UP} = \mathrm{coNP} \Longrightarrow \min\cdot\mathrm{NP} \subseteq \#\cdot\mathrm{P}$.

■

Regarding the relationship between min·P and #·NP which has been left open in [HW97] we have proved that there exists relativized worlds for min·P $\subseteq$ #·NP (Theorem 3) and for min·P $\not\subseteq$ #·NP (Theorem 6). This explains why it is hard to find a proof for min·P $\subseteq$ #·NP.

It is also hard to find an implication of the form min·P $\subseteq$ #·NP $\Longrightarrow \alpha$. At least three possible statements α coming to mind when considering Figure 1 are not likely to be necessary for min·P $\subseteq$ #·NP, namely NP = coNP, UP = NP and UP = coNP, since the statements

- min·P $\subseteq$ #·NP $\Longrightarrow$ NP = coNP
- min·P $\subseteq$ #·NP $\Longrightarrow$ UP = NP
- min·P $\subseteq$ #·NP $\Longrightarrow$ UP = coNP

are not relativizable. The first statement follows from Theorem 7, the last two statements follow from the next theorem.

Theorem 9 *There exists an oracle D such that*

$$\text{min·P}^D \subseteq \#\text{·NP}^D \wedge \text{UP}^D \neq \text{NP}^D = \text{coNP}^D.$$

Proof Since NP = coNP $\Longrightarrow$ min·P $\subseteq$ #·NP is relativizable (cf. Figure 1), it suffices to construct an oracle for $\text{UP}^D \neq \text{NP}^D = \text{coNP}^D$. In [Hem93] Lemma 4.7., L. Hemaspaandra constructs even a stronger oracle E such that $\text{UP}^E \neq \text{NP}^E = \text{PSPACE}^E$. ■

The oracle D showing that the first statement is not relativizable (i.e. the oracle of Theorem 7) has the additional property $\text{UP}^D = \text{NP}^D$ or, equivalently, $\#\text{·P}^D = \#\text{·NP}^D$. We leave it open whether an oracle E with

$$\text{min·P}^E \subseteq \#\text{·NP}^E \wedge \text{UP}^E \neq \text{NP}^E \wedge \text{NP}^E \neq \text{coNP}^E$$

can be constructed.

Acknowledgements

We are grateful to Lane Hemaspaandra, Harald Hempel, and Kolya Vereshchagin for many helpful comments and suggestions. We are especially grateful to an unknown referee whose hints have considerably simplified our paper.

References

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

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

[FR94] L. Fortnow and J. Rogers. Separability and one-way functions. In *Proceedings of the 5th International Symposium on Algorithms and Computation*, pages 396–404. Springer-Verlag *Lecture Notes in Computer Science #834*, August 1994.

[Hem93] L. A. Hemachandra. *A Complexity Theory for Feasible Closure Properties. Journal of Computer and System Sciences*, 46:295–325, 1993.

[HW97] H. Hempel and G. Wechsung. The operators min and max on the polynomial hierarchy. In *Proceedings of the 14th Annual Symposium on Theoretical Aspects of Computer Science*, pages 93–104. Springer-Verlag *Lecture Notes in Computer Science #1200*, 1997.

[Köb89] J. Köbler. *Strukturelle Komplexität von Anzahlproblemen.* PhD thesis, University of Stuttgart, Stuttgart, Germany, 1989.

[Kre88] M. Krentel. The complexity of optimization problems. *Journal of Computer and System Sciences*, 36:490–509, 1988.

[Kre92] M. Krentel. Generalizations of OptP to the polynomial hierarchy. *Theoretical Computer Science*, 97:183–198, 1992.

[KST89] J. Köbler, U. Schöning, and J. Torán. On counting and approximation. *Acta Informatica*, 26:363–379, 1989.

[KSV98] S. Kosub, H. Schmitz and H. Vollmer. Uniformly Defining Complexity Classes of Functions. In *Proceedings of the 15th Symposium on Theoretical Aspects of Computer Science*, pages 607–617. Springer-Verlag *Lecture Notes in Computer Science #1373*, 1998.

[MV96] An.A. Muchnik and N.K. Vereshchagin. A general method to construct oracles realizing given relationships between complexity classes. *Theoretical Computer Science*, 157:227–258, 1996.

[OH93] M. Ogiwara and L. Hemachandra. A complexity theory for closure properties. *Journal of Computer and System Sciences*, 46:295–325, 1993.

[Rac82] C. Rackoff. Relativized questions involving probabilistic algorithms. *Journal of the ACM*, 29(1):261–268, 1982.

[Tod89] S. Toda. On the computational power of PP and $\oplus$P. *Proc. 30th IEEE Symp. on the Foundations of Computer Science*, pp. 514–519, 1989.

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

[Val79a] L. Valiant. The complexity of computing the permanent. *Theoretical Computer Science*, 8:189–201, 1979.

[Val79b] L. Valiant. The complexity of enumeration and reliability problems. *SIAM Journal on Computing*, 8(3):410–421, 1979.

[Vol94] H. Vollmer. *Komplexitätsklassen von Funktionen.* PhD thesis, Universität Würzburg, Institut für Informatik, Würzburg, Germany, 1994.

[VW95] H. Vollmer and K . Wagner. Complexity classes of optimization functions. *Information and Computation*, 120:198–219, 1995.

[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, 1985.