International Journal of Foundations of Computer Science

THE COMPLEXITY OF FINDING MIDDLE ELEMENTS

HERIBERT VOLLMER
Theoretische Informatik, Universität Würzburg,
Am Exerzierplatz 3, D-97072 Würzburg, Germany

and

KLAUS W. WAGNER
Theoretische Informatik, Universität Würzburg
Am Exerzierplatz 3, D-97072 Würzburg, Germany

Received 22 April 1993
Revised 5 January 1994
Communicated by J. Y. Cai

ABSTRACT

Seinosuke Toda introduced the class Mid P of functions that yield the middle element in the *set* of output values over all paths of nondeterministic polynomial time Turing machines. We define two related classes: Med P consists of those functions that yield the middle element in the ordered *sequence* of output values of nondeterministic polynomial time Turing machines (i.e. we take into account that elements may occur with multiplicities greater than one). $\overline{\mathrm{Med}}\,\mathrm{P}$ consists of those functions that yield the middle element of all accepting paths (in some resonable encoding) of nondeterministic polynomial time Turing machines.
We exhibit similarities and differences between these classes and completely determine the inclusion structure between these classes and some well-known other classes of functions like Valiant's # P and Köbler, Schöning, and Torán's span-P, that holds under general accepted complexity theoretic assumptions such as the counting hierarchy doesn't collapse.
Our results help in clarifying the status of Toda's very important class Mid P in showing that it is closely related to the class $\mathrm{PP}^{\mathrm{NP}}$.

Keywords: complexity theory, nondeterministic polynomial time Turing machine, counting classes, complexity classes of functions, median classes, complexity theoretic operators

1. Introduction

The class PP is defined via nondeterministic polynomial time Turing machines. A language A belongs to PP, if there exists such a machine M such that for every input x, $x \in A$ if and only if more than half of the paths of the computation of M on x are accepting if and only if the middle element of the 0-1-output sequence in nondecreasing order is 1. If we generalize this definition to Turing machines which output arbitrary integer values on their paths, we are led to the natural class of functions $\mathrm{Med\,P}$.

Toda[14] defined a similar class $\mathrm{Mid\,P}$ by considering the median of the *set* of all output values of machines as above. In constrast, $\mathrm{Med\,P}$ is defined by the middle element of *sequences*, i.e. we take into account that elements may appear with multiplicity greater than 1 in the set of output values.

A third possibility to define median functions by taking the median of all accepting paths leads to the class $\mathrm{M\overline{ed}\,P}$ which is included in $\mathrm{Med\,P}$ and $\mathrm{Mid\,P}$.

In this paper, we systematically study these complexity classes of functions, exhibit their similarities and differences, and completely determine (at least under reasonable and widely believed complexity theoretic assumptions) the inclusion structure between these classes and some other well known classes of functions.

Our motivation to do so is the following: First, our results will show that the definition of Toda's class is less robust than one might have expected. Second, we think that our class $\mathrm{Med\,P}$ captures a natural notion of computing middle elements; think for example of the middle number of points achieved in an examination, where of course multiplicites should be considered. Moreover, it can be shown that a number of natural complete problems for $\mathrm{Med\,P}$ exist,[21] even under a stricter reducibility notion than Krentel's metric reductions.[11]

We first show that a result analogous to Toda's main theorem[14] holds also for $\mathrm{Med\,P}$ and $\mathrm{M\overline{ed}\,P}$: $\mathrm{FP}^{\#\mathrm{P}} = \mathrm{FP}^{\mathrm{Mid\,P}} = \mathrm{FP}^{\mathrm{Mid\,P}}[1] = \mathrm{FP}^{\mathrm{Med\,P}} = \mathrm{FP}^{\mathrm{Med\,P}}[1] = \mathrm{FP}^{\mathrm{M\overline{ed}\,P}} = \mathrm{FP}^{\mathrm{M\overline{ed}\,P}}[1]$, that is, given as an oracle to an FP-computation, all three classes have the same power. We show that an analogous result holds also for other classes of the form $\mathrm{FP}^{\mathcal{F}}$ where $\mathcal{F}$ is any class of the polynomial hierarchy of counting functions.[23]

At first sight, this is maybe not too surprising, since the differences between $\mathrm{Mid\,P}$ on the one side and $\mathrm{M\overline{ed}\,P}$ and $\mathrm{Med\,P}$ on the other side seem to be only minor. But we then show, that the classes indeed have very different properties: We show that $\mathrm{M\overline{ed}\,P}$ is included in both other classes and even that $\mathrm{Mid\,P}$ is a kind of relativization of $\mathrm{M\overline{ed}\,P}$ with NP-oracles. We show that $\mathrm{M\overline{ed}\,P}$ contains Valiant's class $\#\mathrm{P}$ and even the class Gap-P (see Ref. 3), while span-P (see Ref. 8), a superclass of $\#\mathrm{P}$, is only contained in $\mathrm{Mid\,P}$. These and some other results lead us to the inclusion structure between the classes under consideration given in Fig. 1.

We then show, that all these inclusions are strict and no more inclusions hold, unless some complexity classes collapse which are widely believed not to, e.g. the second level of the polynomial time hierarchy is contained in PP or the counting hierarchy[22,17] collapses. Moreover, for any two classes of the figure, we present an oracle separating them. The approach we choose is the following: When we want to separate two classes of functions $\mathcal{F}_1$ and $\mathcal{F}_2$, we look for an operator $\mathcal{O}$, taking the two classes and transforming them (relativizable) into other classes $\mathcal{O}\cdot\mathcal{F}_1$ and $\mathcal{O}\cdot\mathcal{F}_2$ which we know are different (or at least are commonly believed to be different). Thus, also $\mathcal{F}_1$ and $\mathcal{F}_2$ are different, since if $\mathcal{F}_1 = \mathcal{F}_2$ then also $\mathcal{O}\cdot\mathcal{F}_1 = \mathcal{O}\cdot\mathcal{F}_2$ contradicting our knowledge or beliefs. If there exists an oracle separating $\mathcal{O}\cdot\mathcal{F}_1$ and $\mathcal{O}\cdot\mathcal{F}_2$, then any technique that proves $\mathcal{F}_1 = \mathcal{F}_2$ will not relativize. We think that this in a sense "algebraic" approach to the examination of relationships between complexity classes is preferable to the usual "if something is equal, then something happens" theorems because it not only presents implicational propositions but also the reasons why these implications hold.

We believe that our paper helps to clarify the status of Toda's class Mid P which is a very important class but surely not the only interesting class of median functions. As we mentioned at the beginning of the introduction and as will be shown formally in the following, Med P is comparable in complexity to the class PP while Toda's class Mid P is very similar to $\mathrm{PP}^{\mathrm{NP}}$. Nevertheless, both classes given as oracles to a P or FP computation have the same power, namely the power of a PP-oracle. Thus, in this context the difference between Med P and Mid P disappears. The reason for this is that it is known[16] that $\mathrm{FP}^{\#\mathrm{P}} = \mathrm{FP}^{\#\mathrm{PH}}$ which implies $\mathrm{FP}^{\mathrm{PP}} = \mathrm{FP}^{\mathrm{PP}^{\mathrm{NP}}}$.

2. Preliminaries

Our notion of middle elements with or without multiplicities is made precise in the following definitions.

Let FP denote the class of functions computable deterministically in polynomial time. We remark that we admit (reasonably encoded) negative numbers. Thus, functions from FP map integers to integers.

2.1 Definition. Let $\mathcal{F}$ be a class of functions. Then the class $\mathrm{Med}\,\mathcal{F}$ consists of those functions h, for which there exist $f \in \mathcal{F}$, $g \in \mathrm{FP}$, $g \geq 0$, such that if the ordered sequence of all values $f(x, y)$ for $0 \leq y \leq g(x)$ (with multiplicities) is

$$z_0 \leq z_1 \leq \cdots \leq z_{g(x)},$$

then $h(x) =_{\mathrm{def}} z_{\lfloor g(x)/2 \rfloor}$.

2.2 Definition. Let $\mathcal{F}$ be a class of functions. Then the class $\mathrm{Mid}\,\mathcal{F}$ consists of those functions h, for which there exist $f \in \mathcal{F}$, $g \in \mathrm{FP}$, $g \geq 0$, such that if the set of all values $f(x, y)$ for $0 \leq y \leq g(x)$ is

$$\{z_0, z_1, \ldots, z_k\}, \quad z_0 < z_1 < \cdots < z_k,$$

then $h(x) =_{\mathrm{def}} z_{\lfloor k/2 \rfloor}$.

Following Toda,[14] we will write Mid P and Med P in the case $\mathcal{F} = \mathrm{FP}$. It is obvious, that Med P (Mid P, resp.) is the class of functions that yield the middle element in the sequence (set, resp.) of the outputs over all paths of a polynomial time metric Turing machine,[11,14] i.e. a nondeterministic machine that produces an output on every computation path. If there is a relation in that way between such a machine M and a function f from Med P or Mid P, we say that f is computed by M.

Classes of the form $\mathrm{Med}\,\mathcal{F}$ are examined structurally in a paper by the same authors[20]; and there the following is proved:

2.3 Proposition. $\left.\mathrm{Med\,P}^{\mathrm{Med\,P}^{\cdot^{\cdot^{\cdot^{\mathrm{Med\,P}}}}}}\right\}k \text{ times} = \underbrace{\mathrm{Med}\,\mathrm{Med}\cdots\mathrm{Med}}_{k\ \text{times}}\,\mathrm{P}$.

We will abbreviate the class of the last proposition by $\mathrm{Med}^k\,\mathrm{P}$. Moreover, we will use the abbreviation $\mathrm{Mid}^k\,\mathrm{P}$ for $\mathrm{Mid}\,\mathrm{Mid}\cdots\mathrm{Mid}\,\mathrm{P}$ (k times), for which it can be shown, using methods from Ref. 20 that

2.4 Proposition. $\mathrm{Mid}\,\mathrm{P}^{\mathrm{Mid}\,\mathrm{P}^{\cdot^{\cdot^{\mathrm{Mid}\,\mathrm{P}}}}}\Big\}k \text{ times} = \underbrace{\mathrm{Mid}\,\mathrm{Mid}\cdots\mathrm{Mid}}_{k \text{ times}}\,\mathrm{P}$.

The third kind of function classes we consider is defined as follows:

2.5 Definition. Let $\mathcal{K}$ be a class of sets. Then the class $\mathrm{M\overline{ed}}\,\mathcal{K}$ consists of those functions h, for which there exist $A \in \mathcal{K}$, $g_1, g_2 \in \mathrm{FP}$, $g_1 \leq g_2$, such that $h(x)$ is equal to the middle element of the set

$$\{\, y \mid g_1(x) \leq y \leq g_2(x) \wedge (x,y) \in A \,\}.$$

By nature of definiton, in this case only elements with multiplicity one can occur; and this allows us to show easily:

2.6 Proposition. $\mathrm{M\overline{ed}}\,\mathrm{P} \subseteq \mathrm{Med}\,\mathrm{P} \cap \mathrm{Mid}\,\mathrm{P}$.

Proof. Let $f \in \mathrm{M\overline{ed}}\,\mathrm{P}$ and let $f(x)$ be defined to be the middle element of the set $\{\, y \mid g_1(x) \leq y \leq g_2(x) \wedge (x,y) \in A \,\}$ for $A \in \mathrm{P}$ and $g_1, g_2 \in \mathrm{FP}$. Define a machine M, which on input x guesses a y, $g_1(x) \leq y \leq g_2(x)$. If $(x,y) \in A$, then M prints y, otherwise M branches again and prints $g_1(x) - 1$ and $g_2(x) + 1$ on two different paths. $\square$

In the definitions of the operators Med and Mid, we might have changed the condition for y from $0 \leq y \leq g(x)$ to the more general form used in Definition 2.5 without changing the results of this paper. Both formulations yield the same class for all function classes $\mathcal{F}$, for which $\mathcal{F} \circ \mathrm{FP} \subseteq \mathcal{F}$ holds, i.e. composition of an FP-function with a function from $\mathcal{F}$ can be simulated by another function from $\mathcal{F}$. In Definition 2.5 it is important to use the general form, since substituting 0 for $g_1(x)$ would yield only everywhere non-negative functions.

3. Another Characterization of Toda's Class Mid P

The main result of this section is the following equation relating two of our notions of finding middle elements:

3.1 Theorem. $\mathrm{Mid}\,\mathrm{P} = \mathrm{M\overline{ed}}\,\mathrm{NP}$.

Proof. $\supseteq$: Let $f \in \mathrm{M\overline{ed}}\,\mathrm{NP}$, $f(x) = \mathrm{med}\{\, y \mid g_1(x) \leq y \leq g_2(x) \wedge (x,y) \in A \,\}$, for $A \in \mathrm{NP}$ and $g_1, g_2 \in \mathrm{FP}$. Let M be a nondeterministic polynomial time Turing machine accepting A. Define a nondeterministic machine M' which works as follows:

> On input x, guess (y, y'), and output y' if M accepts on input (x, y') and path y. Otherwise, output $g_1(x) - 1$ and $g_2(x) + 1$.

Then $f(x)$ is the middle element in the set of outputs over all paths of M'. Thus $f \in \mathrm{Mid}\,\mathrm{P}$.

$\subseteq$: Let $f \in \mathrm{Mid}\,\mathrm{P}$ be computed by M. Let $g_1, g_2 \in \mathrm{FP}$ such that $g_1(x) \leq f(x) \leq g_2(x)$ for all x. Then, $f(x)$ is the middle element in the set

$$\{\, y \mid g_1(x) \leq y \leq g_2(x) \wedge \text{ there exists a path with output } y \text{ of } M \text{ on input } x \,\}.$$

Thus, $f \in \overline{\mathrm{Med}}\,\mathrm{NP}$. $\square$

3.2 Corollary. $\mathrm{Mid}\,\mathrm{P} \subseteq \mathrm{Med}\,\mathrm{P}^{\mathrm{NP}}$.

Proof. Follows from Theorem 3.1 and the observation, that 2.6 can be relativized. $\square$

4. Counting Paths Can Be Simulated by Finding Middle Elements

In this section we show that our classes of median functions allow simulations of different powerful counting processes. We show that $\mathrm{Med}\,\mathrm{P}$ contains Valiant's class $\#\,\mathrm{P}$ of functions counting accepting paths of nondeterministic polynomial time Turing machines,[19] whereas $\mathrm{Mid}\,\mathrm{P}$ also contains the class span-P of functions counting the number of different output values over all paths of nondeterministic polynomial time Turing machines.[8] Since in later sections we will see that this cannot be improved (in the sense that it is unlikely that $\mathrm{Med}\,\mathrm{P}$ contains span-P), we thus point out that $\mathrm{Mid}\,\mathrm{P}$ in a sense is a more powerful class than $\mathrm{Med}\,\mathrm{P}$.

4.1 Definition.

1. Let $\mathcal{K}$ be a class of sets. Then the class $\#\,\mathcal{K}$ consists of those functions f for which there exists a set $A \in \mathcal{K}$ and a function $g \in \mathrm{FP}$ such that $f(x) = \big|\{\, y \mid 0 \leq y \leq g(x) \wedge (x,y) \in A \,\}\big|$.
2. The class Gap-P (see Ref. 3) consists of those functions f for which there exists a nondeterministic polynomial time Turing machine M such that $f(x)$ is equal to the number of accepting paths of M on input x minus the number of rejecting paths of M on input x.
3. The class span-P (see Ref. 8) consists of those functions f for which there exists a nondeterministic polynomial time Turing machine M such that $f(x)$ is equal to the number of different output values over all paths of M on input x.

The following is known from the literature[3,7,2] (for function classes $\mathcal{F}$ and $\mathcal{G}$, let $\mathcal{F} - \mathcal{G} =_{\mathrm{def}} \{\, f - g \mid f \in \mathcal{F} \wedge g \in \mathcal{G} \,\}$):

4.2 Theorem.

1. $\text{Gap-P} = \#\,\mathrm{P} - \#\,\mathrm{P} = \#\,\mathrm{P} - \mathrm{FP}$.
2. $\text{span-P} = \#\,\mathrm{NP} \subseteq \#\,\text{co-NP} = \#\,\mathrm{P}^{\mathrm{NP}} \subseteq \#\,\mathrm{NP} - \mathrm{FP} = \#\,\mathrm{NP} - \#\,\mathrm{NP} = \#\,\text{co-NP} - \mathrm{FP} = \#\,\text{co-NP} - \#\,\text{co-NP} = \#\,\mathrm{P}^{\mathrm{NP}} - \mathrm{FP} = \mathrm{FP} - \#\,\mathrm{P}^{\mathrm{NP}}$.

Then we have the following result, whose proof follows an idea of J. Köbler:

4.3 Theorem.

1. $\#\,\mathrm{P} \subseteq \overline{\mathrm{Med}}\,\mathrm{P} \subseteq \mathrm{Med}\,\mathrm{P}$.
2. $\text{span-P} = \#\,\mathrm{NP} \subseteq \mathrm{Mid}\,\mathrm{P}$.

Proof. To prove $\#\mathrm{P} \subseteq \mathrm{M\overline{ed}\,P}$ let $B \in \mathrm{P}$, let $g \in \mathrm{FP}$ and let $f(x) = \left|\{\, y \mid 0 \le y \le g(x) \wedge (x,y) \in B \,\}\right|$. Define

$$\begin{aligned} D =_{\mathrm{def}} & \{\, (x,y) \mid -g(x) \le y \le g(x) \,\} \\ & \cup \{\, (x, g(x)+2y+1) \mid 0 \le y \le g(x) \wedge (x,y) \in B \,\} \\ & \cup \{\, (x, g(x)+2y+2) \mid 0 \le y \le g(x) \wedge (x,y) \in B \,\} \end{aligned}$$

Obviously, $D \in \mathrm{P}$ and the "middle y" such that $(x,y) \in D$ is equal to $\left|\{\, y \mid 0 \le y \le g(x) \wedge (x,y) \in B \,\}\right|$. In the same way one proves $\#\mathrm{NP} \subseteq \mathrm{M\overline{ed}\,NP}$. Theorem 3.1 now completes the proof. □

Since all the median classes are closed under subtraction of FP functions, we obtain (using Theorem 4.2)

4.4 Corollary.

1. $\text{Gap-P} \subseteq \mathrm{M\overline{ed}\,P} \subseteq \mathrm{Med\,P}$.
2. $\#\mathrm{P}^{\mathrm{NP}} = \#\,\text{co-NP} \subseteq \text{span-P} - \mathrm{FP} \subseteq \mathrm{Mid\,P}$.

As a last remark in this section, we want to point out that by a simple inductive argument Theorem 4.3, Statement 1, can be generalized to other classes of the polynomial time hierarchy of counting functions. This hierarchy was defined by Wagner[23] to consist of the classes

$$0\,\#\mathrm{P} =_{\mathrm{def}} \mathrm{FP}, \quad \text{and} \quad (i+1)\,\#\mathrm{P} =_{\mathrm{def}} \#\mathrm{P}^{i\,\#\mathrm{P}} \text{ for } i \ge 0.$$

4.5 Corollary. $k\,\#\mathrm{P} \subseteq \mathrm{Med}^k\,\mathrm{P}$.

5. Characterizations of $\mathrm{FP}^{\#\mathrm{P}}$

Toda[14] gave the following interesting characterization of $\mathrm{P}^{\#\mathrm{P}}$ and $\mathrm{FP}^{\#\mathrm{P}}$: He proved that a language in $\mathrm{P}^{\#\mathrm{P}}$ or a function in $\mathrm{FP}^{\#\mathrm{P}}$ can be decided or computed by asking one query to a function from Mid P; and that on the other hand, Mid P functions are in $\mathrm{FP}^{\#\mathrm{P}}$; thus

$$\mathrm{FP}^{\#\mathrm{P}} = \mathrm{FP}^{\mathrm{Mid\,P}} = \mathrm{FP}^{\mathrm{Mid\,P}}[1].$$

We now give a corresponding result for the class $\mathrm{M\overline{ed}\,P}$. We use the well-known fact that the language class PP (see Refs. 13 and 4) is of the same power as the function class $\#\mathrm{P}$ when given as an oracle to an FP-computation. PP turns out to be a very robust class. Besides the definition given in the introduction it has the following characterization: A language A belongs to PP if and only if there exist $f \in \#\mathrm{P}$ and $g \in \mathrm{FP}$ such that $x \in A \iff f(x) \ge g(x)$. This immediately implies the just mentioned results $\mathrm{FP}^{\#\mathrm{P}} = \mathrm{FP}^{\mathrm{PP}}$.

5.1 Theorem. $\mathrm{FP}^{\mathrm{PP}} = \mathrm{FP}^{\mathrm{M\overline{ed}\,P}}[1] = \mathrm{M\overline{ed}\,P} - \mathrm{M\overline{ed}\,P}$.

Proof. We first prove $\mathrm{FP}^{\mathrm{PP}} = \mathrm{FP}^{\mathrm{M\overline{ed}\,P}}[1]$. Though our proof is very similar to the corresponding one from Ref. 14, we briefly give it here because only a simple modification allows us then to prove $\mathrm{FP}^{\mathrm{PP}} = \mathrm{M\overline{ed}\,P} - \mathrm{M\overline{ed}\,P}$.

$\supseteq$: The middle element can be determined asking questions to PP by binary search.

$\subseteq$: Let $h \in \mathrm{FP}^{\mathrm{PP}}$ be computed by a polynomial time machine M asking queries to $A \in \mathrm{PP}$, and let M' be a polynomial time machine as described in the introduction witnessing $A \in \mathrm{PP}$. Suppose without loss of generality, that on every input, M' branches on an odd number of paths. Let r be a polynomial such that for each input of length n, M asks exactly $r(n)$ queries. Suppose further without loss of generality, that for each of these queries, M' branches on the same number of paths, i.e. this number depends only on the input x to machine M. Let $g \in \mathrm{FP}$, $g > 0$, be such that for each input x, all queries of M and all paths of computations of M' on such queries, encoded as integers, are greater than $-g(x)$ and less than or equal to $g(x)$. We use the following encoding of sequences of integers in natural numbers[20]: For $m, y \in \mathbb{N}$ and $u_1, u_2, \ldots, u_m \in \mathbb{Z}$, let

$$\langle u_1, u_2, \ldots, u_m \rangle_y =_{\mathrm{def}} \sum_{i=1}^{m} (u_i + y) \cdot (2y)^{i-1} - 1.$$

Note that for given $U, y \in \mathbb{N}$, there is exactly one decomposition $m \in \mathbb{N}$, $u_1, \ldots, u_m \in \{-y+1, \ldots, y\}$, such that $\langle u_1, \ldots, u_m \rangle_y = U$.

Define B as the set of all

$$(x, \langle z, p_{r(|x|)}, y_{r(|x|)}, a_{r(|x|)}, \ldots, p_1, y_1, a_1 \rangle_{g(x)}),$$

such that

- $a_i \in \{0, 1\}$ for $i = 1, 2, \ldots, r(|x|)$.
- on input x machine M asks the queries $y_1, y_2, \ldots, y_{r(|x|)}$ and prints the value z when using the answers $a_1, a_2, \ldots, a_{r(|x|)}$, resp., to the queries
- on input y_i machine M' answers a_i on computation path p_i ($i = 1, 2, \ldots, r(|x|)$)

Then it can be shown using an induction similar to that given in Ref. 14 that for every x, in the middle of all

$$y = \langle z, p_{r(|x|)}, y_{r(|x|)}, a_{r(|x|)}, \ldots, p_1, y_1, a_1 \rangle_{g(x)}$$

such that $(x, y) \in B$, the bits $a_1, a_2, \ldots, a_{r(|x|)}$ encode the answers of the oracle A during the computation of M on input x, and z encodes the result of that computation. Since $B \in \mathrm{P}$, we therefore have $\mathrm{FP}^{\mathrm{PP}} \subseteq \mathrm{FP}^{\mathrm{M\overline{ed}\,P}}[1]$.

To show $\mathrm{FP}^{\mathrm{PP}} \subseteq \mathrm{M\overline{ed}\,P} - \mathrm{M\overline{ed}\,P}$ define a set B' analogous to B but now requiring in the second condition that $z = 0$. Then, subtracting the middle y such that $(x, y) \in B'$ from the middle y such that $(x, y) \in B$ yields the value $h(x)$. □

5.2 Corollary.

$$\mathrm{FP}^{\#\mathrm{P}} = \mathrm{FP}^{\mathrm{Med\,P}} = \mathrm{FP}^{\mathrm{Med\,P}}[1] = \mathrm{Med\,P} - \mathrm{Med\,P}.$$

Proof. Since $\mathrm{Med\,P} \subseteq \mathrm{FP}^{\mathrm{PP}}$ (again, the middle element can be determined by binary search) the corollary is a consequence of 5.1 and 2.6. □

For Toda's class $\mathrm{Mid\,P}$ we obtain additionally to Toda's result $\mathrm{FP}^{\#\mathrm{P}} = \mathrm{FP}^{\mathrm{Mid\,P}} = \mathrm{FP}^{\mathrm{Mid\,P}}[1]$ that

5.3 Corollary. $\mathrm{FP}^{\#\mathrm{P}} = \mathrm{Mid\,P} - \mathrm{Mid\,P}$.

By an induction using Propositions 2.3 and 2.4 and relativized versions of Corollaries 5.2 and 5.3, we obtain an analogous result for higher levels of the polynomial hierarchy of counting functions.

5.4 Corollary. $\mathrm{FP}^{k\,\#\mathrm{P}} = \mathrm{FP}^{\mathrm{Med}^k\mathrm{P}}[1] = \mathrm{FP}^{\mathrm{Mid}^k\mathrm{P}}[1]$.

6. Relationships to Classes of Languages

Up to now, we have shown the inclusions given in Fig. 1. $\mathrm{Med\,P}^{\mathrm{NP}} \subseteq \mathrm{FP}^{\mathrm{PP}}$ follows by a relativization of $\mathrm{Med\,P} \subseteq \mathrm{FP}^{\mathrm{PP}}$ and the result $\mathrm{PP}^{\mathrm{NP}} \subseteq \mathrm{P}^{\mathrm{PP}}$ (see Ref. 15).

Now it will be our goal to show that (under reasonable complexity theoretic assumptions) all the above inclusions are strict and there are no additional inclusions between the considered classes. Our general outline will be as follows:

Suppose $\mathcal{F}_1$ and $\mathcal{F}_2$ are two function classes which we want to separate. Then we will present an operator $\mathcal{O}$, transforming function classes into language classes which clearly exhibits the differences between $\mathcal{F}_1$ and $\mathcal{F}_2$ by transforming them into classes $\mathcal{O}\cdot\mathcal{F}_1 = \mathcal{K}_1$ and $\mathcal{O}\cdot\mathcal{F}_2 = \mathcal{K}_2$ which are far away from each other. To be more specific, we will introduce the operator S and show that $\mathrm{S}\cdot\mathrm{Med\,P} = \mathrm{PP}$ and $\mathrm{S}\cdot\mathrm{Mid\,P} = \mathrm{PP}^{\mathrm{NP}}$. Since we know that there exists an oracle separating PP and $\mathrm{PP}^{\mathrm{NP}}$, we also have an oracle that separates $\mathrm{Med\,P}$ from $\mathrm{Mid\,P}$. This could be taken as evidence that $\mathrm{Med\,P} \not\supseteq \mathrm{Mid\,P}$. To be more accurate, it states that no relativizable proof technique can be used to show $\mathrm{Med\,P} \supseteq \mathrm{Mid\,P}$. (Note, that the transformations under all operators we use are themselves relativizable.)

We start by introducing our operator S:

6.1 Definition. Let $\mathcal{F}$ be a class of functions. Then we say that $A \in \mathrm{S}\cdot\mathcal{F}$ if and only if there exist $f \in \mathcal{F}$, $g \in \mathrm{FP}$ such that $x \in A \iff f(x) \geq g(x)$.

S has been studied extensively in the context of classes of the form $\#\mathcal{K}$ (see Ref. 22 and 17); e.g. $\mathrm{S}\cdot\#\mathrm{P} = \mathrm{PP}$ directly by the characterization of PP mentioned in Section 5.

Applied to the classes of Fig. 1, S yields the following classes:

6.2 Theorem.

1. $\mathrm{S}\cdot\mathrm{FP}^X = \mathrm{P}^X$ for every (function or set) class X.
2. $\mathrm{S}\cdot\#\mathrm{P} = \mathrm{S}\cdot\text{Gap-P} = \mathrm{S}\cdot\mathrm{\overline{Med}\,P} = \mathrm{S}\cdot\mathrm{Med\,P} = \mathrm{PP}$.
3. $\mathrm{S}\cdot\text{span-P} = \mathrm{S}\cdot\mathrm{Mid\,P} = \mathrm{S}\cdot\mathrm{Med\,P}^{\mathrm{NP}} = \mathrm{PP}^{\mathrm{NP}}$.

Proof.

1. is obvious.

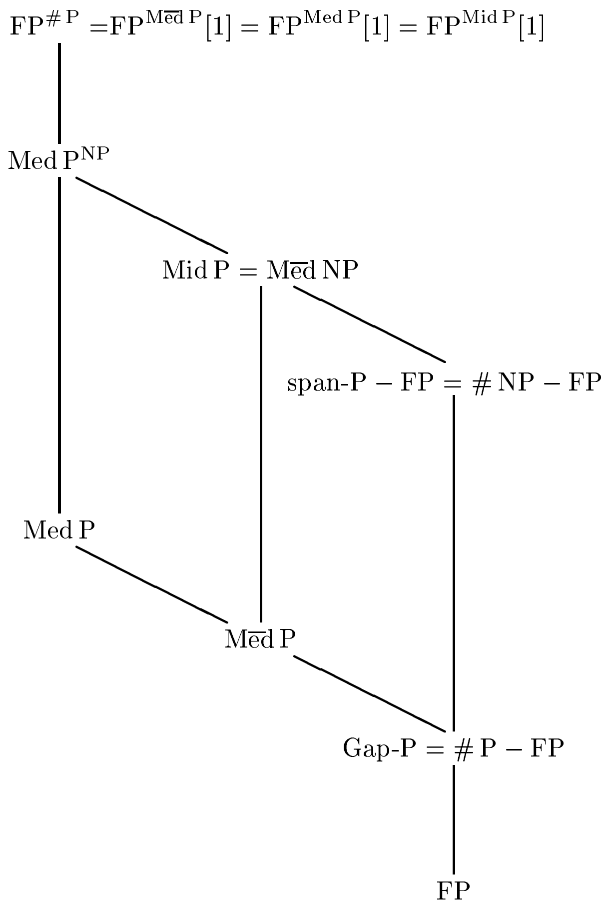

Fig. 1. Inclusionships between the considered function classes

2. $\mathrm{PP} \subseteq \mathrm{S} \cdot \#\mathrm{P}$ by the above remarks. Thus it remains to show $\mathrm{S} \cdot \mathrm{Med\,P} \subseteq \mathrm{PP}$:

   Let $A \in \mathrm{S} \cdot \mathrm{Med\,P}$ via $x \in A \iff f(x) \geq g(x)$ for $f \in \mathrm{Med\,P}$ and $g \in \mathrm{FP}$. Let f be computed by the nondeterministic polynomial time machine M. Define functions

$$\begin{aligned}\mathrm{gr}(x) &= \left|\left\{\, z \;\middle|\; \text{path } z \text{ of } M \text{ on } x \text{ yields an output } \geq g(x) \,\right\}\right| \\ \mathrm{le}(x) &= \left|\left\{\, z \;\middle|\; \text{path } z \text{ of } M \text{ on } x \text{ yields an output } < g(x) \,\right\}\right|\end{aligned}$$

   Surely, $\mathrm{le}, \mathrm{gr} \in \#\mathrm{P}$, and $x \in A \iff \mathrm{gr}(x) > \mathrm{le}(x)$. Thus,[3] $A \in \mathrm{PP}$.

3. A direct relativization of $\mathrm{S} \cdot \mathrm{Med\,P} = \mathrm{PP}$ yields $\mathrm{S} \cdot \mathrm{Med\,P}^{\mathrm{NP}} = \mathrm{PP}^{\mathrm{NP}}$, and $\mathrm{PP}^{\mathrm{NP}} \subseteq \mathrm{S} \cdot \#\mathrm{NP}$ can be found in the literature.[22]

□

6.3 Corollary.

1. If $\mathrm{Med\,P}^{\mathrm{NP}} = \mathrm{FP}^{\#\mathrm{P}}$, then $\mathrm{PP}^{\mathrm{NP}} = \mathrm{P}^{\mathrm{PP}}$.

2. If $\text{span-P} - \mathrm{FP} \subseteq \mathrm{Med\,P}$, then $\mathrm{PP} = \mathrm{PP}^{\mathrm{NP}}$.

It is not hard to see that these inclusions imply in the first case that the inclusion chain $\mathrm{PP}^{\mathrm{NP}} \subseteq \mathrm{PP}^{\mathrm{PH}} \subseteq \mathrm{MidbitP} \subseteq \mathrm{P}^{\mathrm{PP}}$ collapses to $\mathrm{PP}^{\mathrm{NP}}$ contradicting our beliefs. (For the class MidbitP see Ref. 6 and 10. Note that the above collapse would also imply that MidbitP is closed unter intersection, which is still open.[6]) Moreover,[5] there is an oracle separating $\mathrm{PP}^{\mathrm{PH}}$ and P^{PP}. In the second case we have the implication that the second level of the polynomial time hierarchy is contained in PP, contradicting some relativized worlds, see e.g. Ref. 1. Thus, under generally accepted assumptions, all inclusions indicated in Fig. 1 by vertical lines are strict.

Next, we turn to the inclusions depicted by diagonal lines. Using operators from the literature,[18,12] we give evidence that they are strict.

For a set A, let c_A denote its characteristic function. Then we define:

6.4 Definition. Let $\mathcal{F}$ be a class of functions.

1. $\mathrm{U} \cdot \mathcal{F} =_{\mathrm{def}} \left\{\, A \;\middle|\; c_A \in \mathcal{F} \,\right\}$.

2. $\mathrm{X} \cdot \mathcal{F} =_{\mathrm{def}} \left\{\, A \;\middle|\; c_A \in \mathcal{F} - \mathcal{F} \,\right\}$.

By definition,[18,12] $\mathrm{U} \cdot \#\mathrm{P} = \mathrm{UP}$ and $\mathrm{X} \cdot \#\mathrm{P} = \mathrm{XP}$. (The latter class is also known[3] under the name SPP.) Moreover,[8,2] it is known:

6.5 Proposition.

1. $\mathrm{U} \cdot \text{Gap-P} = \mathrm{X} \cdot \text{Gap-P} = \mathrm{XP}$.

2. $\mathrm{U} \cdot (\text{span-P} - \mathrm{FP}) = \mathrm{X} \cdot (\text{span-P} - \mathrm{FP}) = \mathrm{XP}^{\mathrm{NP}}$.

Additionally, we now show:

6.6 Theorem. $\mathrm{U} \cdot \mathrm{M\overline{ed}\,P} = \mathrm{XP}$ and $\mathrm{U} \cdot \mathrm{Med\,P} = \mathrm{PP}$.

Proof. $\mathrm{PP} \subseteq \mathrm{U} \cdot \mathrm{Med}\,\mathrm{P}$ is a simple consequence of the definition of PP. $\mathrm{U} \cdot \mathrm{Med}\,\mathrm{P} \subseteq \mathrm{PP}$ follows from 6.2, since obviously $\mathrm{U} \cdot \mathcal{F} \subseteq \mathrm{S} \cdot \mathcal{F}$. $\mathrm{XP} \subseteq \mathrm{U} \cdot \mathrm{M\overline{ed}}\,\mathrm{P}$ is a simple consequences of the definition of XP and Corollary 4.4. We now prove $\mathrm{U} \cdot \mathrm{M\overline{ed}}\,\mathrm{P} \subseteq \mathrm{XP}$:

Let $A \in \mathrm{U} \cdot \mathrm{M\overline{ed}}\,\mathrm{P}$. Then, there exist $B \in \mathrm{P}$, $g_1, g_2 \in \mathrm{FP}$ such that $c_A(x) = \mathrm{med}\{\, y \mid g_1(x) \le y \le g_2(x) \wedge (x,y) \in B \,\}$. Define

$$\begin{aligned} h_1(x) &= \left|\{\, y \mid g_1(x) \le y \le 0 \wedge (x,y) \in B \,\}\right| \\ h_2(x) &= \left|\{\, y \mid 1 \le y \le g_2(x) \wedge (x,y) \in B \,\}\right| \end{aligned}$$

Thus, if $x \in A$, then $h_2(x) \in \{h_1(x)+1, h_1(x)+2\}$ and therefore $h_2(x) - h_1(x) + 1 \in \{2,3\}$; and if $x \notin A$, then $h_2(x) \in \{h_1(x)-1, h_1(x)\}$ and therefore $h_2(x)-h_1(x)+1 \in \{0,1\}$. Obviously, $h_2 - h_1 + 1 \in$ Gap-P. Now it follows[9,3] that $A \in$ Gap-Few = XP. □

6.7 Corollary. $\mathrm{U} \cdot \mathrm{Mid}\,\mathrm{P} = \mathrm{XP}^{\mathrm{NP}}$ and $\mathrm{U} \cdot \mathrm{Med}\,\mathrm{P}^{\mathrm{NP}} = \mathrm{PP}^{\mathrm{NP}}$.

Proof. The second equality is a direct relativization of the previous result. The first equality follows from $\mathrm{U} \cdot \mathrm{Mid}\,\mathrm{P} \subseteq \mathrm{U}\,\mathrm{M\overline{ed}}\,\mathrm{P}^{\mathrm{NP}}$, relativizing the previous result, and $\mathrm{XP}^{\mathrm{NP}} = \mathrm{X} \cdot \#\,\mathrm{P}^{\mathrm{NP}} = \mathrm{X} \cdot \#\,\mathrm{NP}$ and Theorem 4.2 and Corollary 4.4. □

Next, we examine the operator X:

6.8 Theorem. $\mathrm{X} \cdot \mathrm{M\overline{ed}}\,\mathrm{P} = \mathrm{X} \cdot \mathrm{Med}\,\mathrm{P} = \mathrm{X} \cdot \mathrm{Mid}\,\mathrm{P} = \mathrm{X} \cdot \mathrm{Med}\,\mathrm{P}^{\mathrm{NP}} = \mathrm{P}^{\mathrm{PP}}$.

Proof.

$$\begin{aligned} \mathrm{X} \cdot \mathrm{M\overline{ed}}\,\mathrm{P} &= \mathrm{U} \cdot (\mathrm{M\overline{ed}}\,\mathrm{P} - \mathrm{M\overline{ed}}\,\mathrm{P}) && \text{by Definition of U and X} \\ &= \mathrm{U} \cdot \mathrm{FP}^{\mathrm{PP}} && \text{by Theorem 5.1} \\ &= \mathrm{P}^{\mathrm{PP}} \end{aligned}$$

The proofs for the other cases follow, since all considered classes lie between $\mathrm{X} \cdot \mathrm{M\overline{ed}}\,\mathrm{P}$ and P^{PP}. □

Taken together, these results imply the following corollaries:

6.9 Corollary. The following statements are equivalent:

1. Gap-P $= \mathrm{M\overline{ed}}\,\mathrm{P}$.
2. $\mathrm{M\overline{ed}}\,\mathrm{P} = \mathrm{Med}\,\mathrm{P}$.
3. The counting hierarchy collapses to XP.
4. The hierarchy of counting functions collapses to Gap-P.

Proof. From the previous results, we get

1. If Gap-P $= \mathrm{M\overline{ed}}\,\mathrm{P}$, then $\mathrm{XP} = \mathrm{P}^{\mathrm{PP}}$.
2. If $\mathrm{M\overline{ed}}\,\mathrm{P} = \mathrm{Med}\,\mathrm{P}$, then XP = PP.

From 1 or 2, we therefore conclude that XP = PP. Since XP is low for PP (see Ref. 3), this implies that the hierarchy of counting functions collapses to Gap-P and the counting hierarchy to XP. This in turn implies Gap-P $= \mathrm{FP}^{\mathrm{PP}}$ and therefore also statements 1 and 2. □

6.10 Corollary. The following statements are equivalent:

1. $\mathrm{M\overline{ed}\,P} \subseteq \text{span-P} - \mathrm{FP}$.
2. $\mathrm{Med\,P} \subseteq \mathrm{Mid\,P}$.
3. $\text{span-P} - \mathrm{FP} = \mathrm{Mid\,P}$.
4. $\mathrm{Mid\,P} = \mathrm{Med\,P}^{\mathrm{NP}}$.
5. The counting hierarchy collapses to $\mathrm{XP}^{\mathrm{NP}}$.
6. The hierarchy of counting functions collapses to $\text{Gap-P}^{\mathrm{NP}}$.

Proof. From the previous results, we get

1. If $\mathrm{M\overline{ed}\,P} \subseteq \text{span-P} - \mathrm{FP}$, then $\mathrm{P}^{\mathrm{PP}} = \mathrm{XP}^{\mathrm{NP}}$.
2. If $\mathrm{Med\,P} \subseteq \mathrm{Mid\,P}$, then $\mathrm{PP} \subseteq \mathrm{XP}^{\mathrm{NP}}$.
3. If $\text{span-P} - \mathrm{FP} = \mathrm{Mid\,P}$, then $\mathrm{XP}^{\mathrm{NP}} = \mathrm{P}^{\mathrm{PP}}$.
4. If $\mathrm{Mid\,P} = \mathrm{Med\,P}^{\mathrm{NP}}$, then $\mathrm{XP}^{\mathrm{NP}} = \mathrm{PP}^{\mathrm{NP}}$.

Equivalence of all the statements can now be shown in a way similar to that of the proof of the previous corollary. □

Thus, we now have that if any inclusion depicted in Fig. 1 by a diagonal line is not strict, then the counting hierarchy collapses at least to $\mathrm{XP}^{\mathrm{NP}}$. Moreover, if any additional inclusions not given in that Figure hold, e.g. $\mathrm{Med\,P} \subseteq \mathrm{Mid\,P}$, then again the counting hierarchy collapses to $\mathrm{XP}^{\mathrm{NP}}$. Observe that the above mentioned oracle results[1,5] separate the counting hierarchy from $\mathrm{XP}^{\mathrm{NP}}$. Thus, for any two classes from Fig. 1, we have an oracle separating them.

Our transformations of function classes to language classes are summarized in Fig. 2. Since every line for an inclusionsship between function classes is crossed at least once by a dotted line we have evidence that every inclusion given is strict.

Acknowledgement

Thanks Krzysztof Loryś (Wrocław) for many helpful discussions about several topics of this paper. Thanks to Richard Beigel (Yale) for pointing out the oracle result from Ref. 5. Thanks to Johannes Köbler (Ulm) for pointing out and correcting an error in a previous proof of one of our theorems. Thanks to Johannes Köbler, Martin Mundhenk, and Thomas Thierauf (Ulm) and to the anonymous referees for helpful discussions and hints on Corollaries 6.9 and 6.10.

References

1. R. Beigel, "Perceptrons, PP, and the polynomial time hierarchy", *Proc. 7^{th} Structure in Complexity Theory Conference*, IEEE Computer Society Press, 1992, pp. 14–19.
2. H. J. Burtschick, "Notes of a seminar on complexity theory", Georgenthal, 1991.

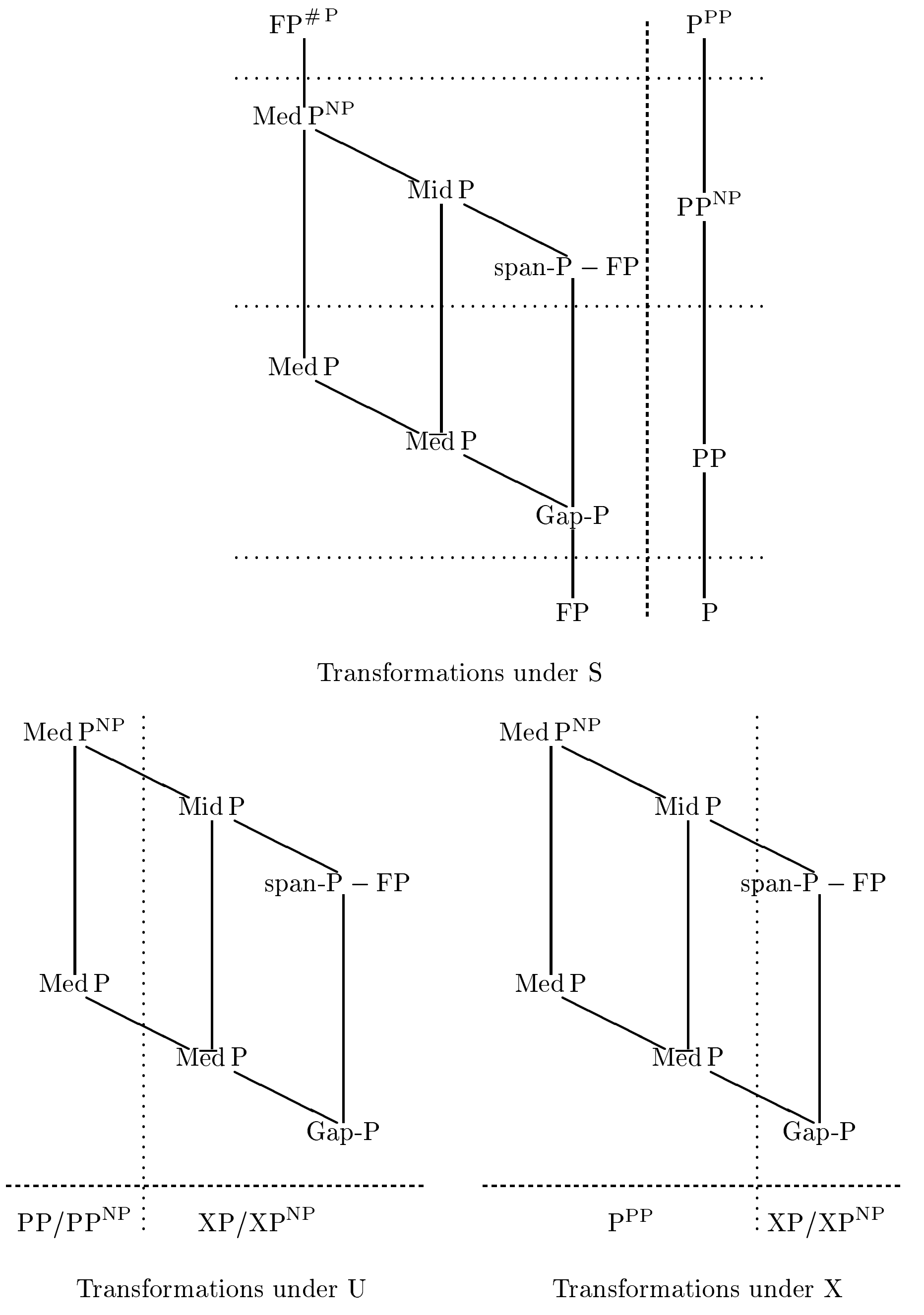

Fig. 2. Summary of transformations

3. S. Fenner, L. Fortnow, S. Kurtz, "Gap-definable counting classes", *Proc.* 6^{th} *Structure in Complexity Theory Conference*, IEEE Computer Society Press, 1991, pp. 30–42.

4. J. Gill, "Computational complexity of probabilistic complexity classes", *SIAM Journal on Computing* **6** (1977), pp. 675–695.

5. F. Green, "An oracle separating $\oplus$P from $\mathrm{PP}^{\mathrm{PH}}$", *Proc.* 5^{th} *Structure in Complexity Theory Conference*, IEEE Computer Society Press, 1990, pp. 295–298.

6. F. Green, J. Köbler, K. W. Regan, T. Schwentick, J. Torán, "The power of the middle bit of a #P function". to appear in the *Journal of Computer and System Sciences.*

7. J. Köbler, "Strukturelle Komplexität von Anzahlproblemen", Ph. D. Thesis, Fakultät für Informatik, Universität Stuttgart, 1989.

8. J. Köbler, U. Schöning, J. Torán, "On counting and approximation", *Acta Informatica* **26** (1989), pp. 363–379.

9. J. Köbler, U. Schöning, S. Toda, J. Torán, "Turing machines with few accepting configurations and low sets for PP", *Journal of Computer and Systems Sciences* **44** (1992), pp. 272–286.

10. J. Köbler, S. Toda, "On the power of generalized MOD-classes", *Proc.* 8^{th} *Structure in Complexity Theory Conference*, IEEE Computer Society Press, 1993, pp. 147–155.

11. M. W. Krentel, "The complexity of optimization problems", *Journal of Computer and Systems Sciences* **36** (1988), pp. 490–509.

12. M. Ogiwara, L. Hemachandra, "A complexity theory for feasible closure properties", *Journal of Computer and Systems Sciences* **46** (1993), pp. 295–325.

13. J. Simon, "On some central problems in computational complexity", Ph. D. Thesis, Cornell University, Ithaca, New York, 1975.

14. S. Toda, "The complexity of finding medians", *Proc.* 31^{st} *Symposium on Foundations of Computer Science*, IEEE Computer Society Press, 1990, pp. 778–787.

15. S. Toda, "PP is as hard as the polynomial time hierarchy", *SIAM J. Comput.* **20** (1991), 865–877.

16. S. Toda, O. Watanabe, "Polynomial time 1-Turing reductions from #PH to #P", *Theoretical Computer Science* **100** (1992), pp. 205–221.

17. J. Torán, "Complexity classes defined by counting quantifiers", *Journal of the ACM* **38** (1991), pp. 753–774.

18. L. G. Valiant, "Relative complexity of checking and evaluation", *Information Processing Letters* **5** (1976), pp. 20–23.

19. L. G. Valiant, "The complexity of computing the permanent", *Theoretical Computer Science* **8** (1979), pp. 189–201.

20. H. Vollmer, K. W. Wagner, "Complexity classes of optimization functions", *submitted for publication.*

21. H. Vollmer, "On different reducibility notions for function classes", to appear in *Proc.* 11^{th} *Symposium on Theoretical Aspects of Computer Science (STACS)*, Springer Lecture Notes in Computer Science, 1994.

22. K. W. Wagner, "The complexity of combinatorial problems with succinct input representation", *Acta Informatica* **23** (1986), pp. 325—356.

23. K. W. Wagner, "Some observations on the connection between counting and recursion", *Theoretical Computer Science* **47** (1986), pp. 131–147.