On the Structure of Low Sets

Johannes Köbler
Abteilung Theoretische Informatik
Universität Ulm
89069 Ulm, Germany

Abstract

Over a decade ago, Schöning introduced the concept of lowness into structural complexity theory. Since then a large body of results has been obtained classifying various complexity classes according to their lowness properties. In this paper we highlight some of the more recent advances on selected topics in the area. Among the lowness properties we consider are polynomial-size circuit complexity, membership comparability, approximability, selectivity, and cheatability. Furthermore, we review some of the recent results concerning lowness for counting classes.

1 Introduction

The comparison of various complexity classes obtained by restricting different kinds of computational resources is a main theme in complexity theory. Indeed, much of the work in structural complexity originated from the fundamental unresolved question whether nondeterministic time computations are really more powerful than their deterministic counterparts. One approach to attack this and related problems has been to investigate the structure of "typical inhabitants" of the involved complexity classes (as, for example, complete sets which in some sense represent the whole class). The ultimate aim of this approach is to identify for two complexity classes such as $\mathcal{P}$ and $\mathcal{NP}$ a structural property that is shared by all typical sets from one class but not by all such sets from the other class, thus establishing that the two classes are indeed different.

This line of research at least dates back to the famous conjecture of Berman and Hartmanis in the mid 1970's stating that all $\mathcal{NP}$-complete sets are polynomially isomorphic [BH77]. Since the $\mathcal{NP}$-complete set SAT of satisfiable propositional formulas is dense (i.e., for some constant ε, it contains at least 2^{n^ε} many elements of length up to n), and since the density of a set is preserved by polynomial isomorphisms, the conjecture implies that *all* $\mathcal{NP}$-complete sets are dense. On the other hand, since every set in $\mathcal{P}$ (besides $\emptyset$ and Σ^*) is many-one complete for $\mathcal{P}$, not all such sets in $\mathcal{P}$ are dense. Therefore, under the assumption that the Berman-Hartmanis Conjecture is true, there is a structural property, namely the density of many-one complete sets, that differentiates between the classes $\mathcal{NP}$ and $\mathcal{P}$.

Over the last two decades, the Berman-Hartmanis Conjecture led to a series of controversial discussions and a sequence of structural results both in support of and against its validity (see, e.g., [JY85, GJ86, KMR89, KMR90, You90, FFK92]). Moreover, the fascinating idea behind the conjecture inspired many researchers to extensively investigate the structural properties of complete sets for $\mathcal{NP}$ and other complexity classes under various types of reducibilities (see, e.g., the surveys of Homer [Hom90] and of Buhrman and Torenvliet [BT94] on this subject).

The object of some research stream that originated from the conjecture is to reveal structural properties which are incompatible with various completeness or hardness notions (under plausible assumptions). For example, a weaker version of the Berman-Hartmanis Conjecture states that all $\mathcal{NP}$-complete sets are non-sparse (a set is sparse if there is a constant c such that it contains at most n^c elements of length up to n). After preliminary results by Berman [Ber78] and Fortune [For79], Mahaney [Mah82] finally settled this version of the conjecture by proving that no $\mathcal{NP}$-complete set many-one reduces to a sparse set unless $\mathcal{P} = \mathcal{NP}$. Thus, under the well-believed assumption that $\mathcal{P} \neq \mathcal{NP}$, sparseness is a structural property that is incompatible with being hard for $\mathcal{NP}$ under many-one reductions.

On the same line of research, Karp, Lipton, and Sipser [KL80] proved that having polynomial sized circuits is incompatible with being hard for $\mathcal{NP}$ under Turing reductions unless the polynomial hierarchy collapses to its second level. Besides, there have been many similar results for various other reducibilities to sparse sets; see, e.g., [Lon82b, Ukk83, Yap83, Yes83, Kad89, OW91, RR92, AKM92, AH$^+$93, AA95]. Almost ten years after Mahaney's theorem, Watanabe and Ogiwara [OW91] were able to show that unless $\mathcal{P} = \mathcal{NP}$, sparseness even is incompatible with being hard for $\mathcal{NP}$ under bounded truth-table reductions. For more information on this topic, the reader is referred to the survey by Hemachandra, Ogiwara, and Watanabe [HOW92].

As a further example, let us consider the graph isomorphism problem (GI). GI is one of the few known natural problems from the class $\mathcal{NP}$ that have not been classified to be either in $\mathcal{P}$ or complete for $\mathcal{NP}$. However, in [GMR89, GS86] (see also [BM88, Sch88]) it is shown that the complement of GI is contained in Babai's Arthur-Merlin class $\mathcal{AM}$, i.e. GI $\in$ *co*-$\mathcal{AM}$. Since $\mathcal{NP}$ is not contained in *co*-$\mathcal{AM}$ unless the polynomial hierarchy collapses to its second level [BHZ87], it follows that being $\mathcal{NP}$-complete is incompatible with being a member of *co*-$\mathcal{AM}$ (unless $\mathcal{PH} = \Sigma_2^{\mathrm{P}}$), and thus GI is unlikely to be $\mathcal{NP}$-complete.

In recursion theory, many properties that are incompatible with completeness have been classified as "lowness" properties, i.e., sets that possess the property are not very useful when used as oracles in certain computations (see, e.g., [Ler83]). This motivated Schöning [Sch83] to introduce the concept of lowness into structural complexity theory by defining the low and high hierarchies within $\mathcal{NP}$ (a formal definition is given in Section 3). The levels of the high hierarchy can be seen as generalizing the notion of $\mathcal{NP}$-completeness under polynomial-time Turing reductions to weaker and weaker reducibilities corresponding to higher and higher levels of the polynomial hierarchy. In contrast, the levels of the low hierarchy generalize in the same way the opposite notion of "incompleteness". More precisely, a set is in some level of the low hierarchy if – with respect to the corresponding reducibility – only those sets are reducible to it which can just as well be reduced to the empty set. By the way the low and high hierarchies are defined, a set that is located at some level of the low hierarchy cannot be at the same time $\mathcal{NP}$-complete (not even under very weak reducibilities) unless the polynomial hierarchy collapses. Moreover, the location of the set in the low hierarchy corresponds with the depth of the collapse of $\mathcal{PH}$ that is implied by the assumption that it is $\mathcal{NP}$-complete.

Going back to the example of graph isomorphism, Schöning [Sch86] was able to locate GI (and in fact all sets in $\mathcal{NP} \cap co\text{-}\mathcal{AM}$) at the second level of the low hierarchy by showing that $\Sigma_2^{\mathrm{P}}(\mathrm{GI}) = \Sigma_2^{\mathrm{P}}$. As a consequence, he obtained the stronger result that GI is not even $\mathcal{NP}$-complete under weaker reducibilities (such as the strong nondeterministic Turing reducibility [Lon82a] or the γ-reducibility [AM77], see also [GJ79]) unless $\mathcal{PH}$ collapses to Σ_2^{P}.

Actually, also the theorem of Ogiwara and Watanabe [OW91] is based on a lowness result showing that all *left sets* (a special kind of self-reducible sets) that are bounded truth-table reducible to a sparse set are located at the base level $\mathcal{L}ow_0^{\Sigma} = \mathcal{P}$ of the low hierarchy.

Looking at these (and many other) examples we see already one bonus that we get from the lowness approach, namely that it provides a unified method of proving collapse results of various types. Furthermore, it provides a classification of a variety of complexity classes. The lower a class is located in the low hierarchy the stronger is the evidence that being a member of the class is incompatible with being complete for $\mathcal{NP}$ (under various reducibilities).

In order to measure the information content of languages outside of $\mathcal{NP}$, the lowness concept has been extended to arbitrary complexity classes [BBS86]. Subsequently, lowness properties for a variety of classes have been extensively investigated. Among them are probabilistic complexity classes (see, e.g., [Sch89]) and sets reducible to sparse or tally sets (see, e.g., [HOW92]). Furthermore, apart from the levels of the polynomial hierarchy, lowness properties have been investigated also with respect to other relativizable complexity classes. Particularly fruitful has been the investigation of low sets for counting classes such as $\mathcal{PP}$ and $\mathcal{G}ap\mathcal{P}$; see, e.g., [Tor88, Tor91, To91a, KSTT92, KST92, BG92, KST93, FFK94, GKRST, KT]. We will review some of these results below.

Finally, let us mention another important application, namely in circuit complexity. Several lowness results concerning relativizable Turing machine classes have been successfully translated into corresponding circuit simulations. For example, the techniques used by Toda [To91a] – building on techniques of Valiant and Vazirani [VV86] – to obtain his celebrated result that the polynomial hierarchy and the

$\mathcal{M}od_k\mathcal{P}$ classes are low for $\mathcal{P}^{\#\mathcal{P}[1]}$ have been a main ingredient in the simulation of $\mathcal{ACC}$ circuits by small depth-2 circuits consisting of one symmetric gate over small fan-in AND gates [Smo87, Raz87, All89, AH90, Yao90, BT91]. By improving Toda's lowness result from $\mathcal{P}^{\#\mathcal{P}[1]}$ to the middle bit class $\mathcal{MP}$, the symmetric gate in the simulating circuit could subsequently be fixed to a middle bit gate [GKRST].

We shall present some preliminary notations and definitions in the next section. In Section 3, we define the low and extended low hierarchies and briefly discuss related basic facts. In Section 4, we consider the class $\mathcal{P}/poly$ of sets decidable by polynomial sized circuits and related classes. In Section 5, we discuss in some depth the recent advances in locating membership comparable, approximable, cheatable, selective, and multi-selective sets inside the low hierarchies. In Section 6, we review the recent progress that has been made in investigating the effect of combining lowness properties with properties of natural sets such as self-reducibility. Finally, in Section 7 we briefly discuss some lowness results for counting classes, among them the recent extensions of Toda's theorem to middle bit classes and their application in circuit complexity.

Please note that this survey is in no sense complete and only meant as a report on some selected recent advances in the area.

2 Preliminaries and notation

All languages are over the binary alphabet $\Sigma = \{0, 1\}$. The *length* of a string $x \in \Sigma^*$ is denoted by $|x|$. The cardinality of a finite set A is denoted by $\|A\|$. The characteristic function of a set A is denoted by $A(x)$. For a class $\mathcal{C}$ of sets, co-$\mathcal{C}$ denotes the class $\{\Sigma^* - A \mid A \in \mathcal{C}\}$. To encode pairs (or tuples) of strings we use a standard polynomial-time computable pairing function denoted by $\langle\cdot,\cdot\rangle$ whose inverses are also computable in polynomial time. Where intent is clear we write $f(x_1, \ldots, x_k)$ in place of $f(\langle x_1, \ldots, x_k\rangle)$.

The set $\{0, 1, 2, \ldots\}$ of non-negative integers is denoted by $\mathcal{N}$. Throughout the paper, the base of log is 2. The *join* of two sets A and B is $A \oplus B = \{0x \mid x \in A\} \cup \{1x \mid x \in B\}$. The join operator can be extended to language classes; $A \oplus \mathcal{C}$, e.g., denotes the class $\{A \oplus B \mid B \in \mathcal{C}\}$.

The reducibilities we are concerned with are the standard polynomial-time reducibilities defined by Ladner, Lynch, and Selman [LLS75]. Thus we mostly omit the addition "polynomial-time". Further, we will consider the strong nondeterministic Turing reducibility introduced by Long [Lon82a]: $A \leq_T^{SN} B$ if $A \in \mathcal{NP}(B) \cap co\text{-}\mathcal{NP}(B)$.

A deterministic polynomial-time oracle machine that asks on inputs of length n at most $O(\log n)$ (adaptive) queries to its oracle is called a Θ-machine. For a set A, the class $\Theta(A)$ [LS91] contains all languages $L(M, A)$ accepted by some Θ-machine M using oracle A. The Σ, Δ and Θ-levels of the (relativized) polynomial-time hierarchy [MS73, St77, LS91, Wag90] are defined as follows: $\Sigma_0(A) = \Delta_0(A) =$

$\Theta_0(A) = \mathcal{P}(A)$, and for $k \geq 1$, $\Sigma_k(A) = \mathcal{NP}(\Sigma_{k-1}(A))$, $\Delta_k(A) = \mathcal{P}((\Sigma_{k-1}(A))$, $\Theta_k^{\rm P}(A) = \Theta(\Sigma_{k-1}^{\rm P}(A))$.

We write $\mathcal{FP}$ for the class of all (total) functions that are computable in deterministic polynomial-time. For $k \geq 1$, $\mathrm{F}\Delta_k^{\rm P}(A) = \mathcal{FP}(\Sigma_{k-1}^{\rm P}(A))$.

Further information on common notions in complexity theory may be found in [BDG, BC93, KST93, Pap94, Sch86].

3 The low and high hierarchies

The low and high hierarchies measure the information content of a set according to the power it provides when used as an oracle in computations of certain types. More specifically, consider an arbitrary set $A \in \mathcal{NP}$. How useful is A when used as an oracle for $\Sigma_k^{\rm P}$ computations? Of course, the class of problems that is captured by $\Sigma_k^{\rm P}$ computations with the additional help of oracle A can only range between $\Sigma_k^{\rm P}(\emptyset) = \Sigma_k^{\rm P}$ and $\Sigma_k^{\rm P}(\mathrm{SAT}) = \Sigma_{k+1}^{\rm P}$, i.e.

$$\Sigma_k^{\rm P} \subseteq \Sigma_k^{\rm P}(A) \subseteq \Sigma_{k+1}^{\rm P}.$$

In the case that A does not increase the power of $\Sigma_k^{\rm P}$ computations, i.e. $\Sigma_k^{\rm P}(A) = \Sigma_k^{\rm P}(\emptyset) = \Sigma_k^{\rm P}$, A is said to be in the k-th Σ-level of the **low hierarchy** (denoted by $\mathcal{L}ow_k^{\Sigma}$, $k \geq 0$). In the opposite case that A provides $\Sigma_k^{\rm P}$ computations with as much power as an optimal oracle from $\mathcal{NP}$, i.e. $\Sigma_k^{\rm P}(A) = \Sigma_k^{\rm P}(\mathrm{SAT}) = \Sigma_{k+1}^{\rm P}$, A is said to be in the k-th Σ-level of the **high hierarchy** (denoted by $\mathcal{H}igh_k^{\Sigma}$, $k \geq 0$) [Sch83].

The Δ- and Θ-levels of the low and high hierarchies inside $\mathcal{NP}$ are defined analogously [Sch86, LS91], and are denoted by $\mathcal{L}ow_k^{\Delta}$, $\mathcal{L}ow_k^{\Theta}$, $\mathcal{H}igh_k^{\Delta}$, and $\mathcal{H}igh_k^{\Theta}$, $k \geq 1$, respectively.

The levels of the high hierarchy define more and more general versions of "$\mathcal{NP}$-completeness" (with respect to reducibilities of the form $\{(A,B) \mid \Sigma_k^{\rm P}(A) \subseteq \Sigma_k^{\rm P}(B)\}$), whereas the levels of the low hierarchy extend the step from $\mathcal{P}$ to $\mathcal{NP} \cap co\text{-}\mathcal{NP}$ in the sense that they only contain sets that w.r.t. the corresponding reducibilities reduce to the empty set. The most important fact concerning sets located at some level of the low hierarchy is that they are not contained in any level of the high hierarchy (and therefore they cannot be $\mathcal{NP}$ complete under any reasonable reducibility) unless SAT reduces to the empty set, i.e., the polynomial-time hierarchy collapses (see part *(vii)* of the next proposition which lists some additional basic facts).

Proposition 3.1 [Sch83, Sch86, LS91]

(i) $\mathcal{L}ow_0^{\Sigma} = \mathcal{L}ow_1^{\Theta} = \mathcal{L}ow_1^{\Delta} = \mathcal{P}$.

(ii) $\mathcal{L}ow_1^{\Sigma} = \mathcal{NP} \cap co\text{-}\mathcal{NP}$.

(iii) $\mathcal{L}ow_{k-1}^{\Sigma} \subseteq \mathcal{L}ow_k^{\Theta} \subseteq \mathcal{L}ow_k^{\Delta} \subseteq \mathcal{L}ow_k^{\Sigma}$, $k \geq 1$.

(iv) $\mathcal{H}igh_0^{\Sigma} = \mathcal{H}igh_1^{\Theta} = \mathcal{H}igh_1^{\Delta} = \{A \mid A$ *is* $\leq_T^P$*-complete for* $\mathcal{NP}\}$.

(v) $\mathcal{H}igh_1^{\Sigma} = \{A \mid A$ *is* $\leq_T^{SN}$*-complete for* $\mathcal{NP}\}$.

(vi) $\mathcal{H}igh_{k-1}^{\Sigma} \subseteq \mathcal{H}igh_k^{\Theta} \subseteq \mathcal{H}igh_k^{\Delta} \subseteq \mathcal{H}igh_k^{\Sigma}$, $k \geq 1$.

(vii) *If there is a set* A *in* $\mathcal{H}igh_k^{\Sigma} \cap \mathcal{L}ow_k^{\Sigma}$ *then* $\mathcal{PH}$ *collapses to* Σ_k^{P}*. Analogous consequences follow for the* Δ*- and* Θ*-levels.*

In order to classify language classes not contained in $\mathcal{NP}$ (e.g. nonuniform complexity classes), the low and high hierarchies have been extended to arbitrary sets outside $\mathcal{NP}$.

A set A is in the k-th Σ-level of the **extended low hierarchy** (denoted $E\mathcal{L}_k^{\Sigma}$, $k \geq 1$) [BBS86] if

$$\Sigma_k^{\mathrm{P}}(A) \subseteq \Sigma_{k-1}^{\mathrm{P}}(\mathrm{SAT} \oplus A).$$

The Δ- and Θ-levels of the extended low hierarchy are defined analogously [AH92, LS91], and are denoted by $E\mathcal{L}_k^{\Delta}$ and $E\mathcal{L}_k^{\Theta}$, $k \geq 2$, respectively.

Compared to the low hierarchy within $\mathcal{NP}$, the extended low hierarchy is to a lesser extend a tool to classify sets according to their information content. Rather, it classifies oracles according to how easy it is to extract some useful information out of the oracle. More precisely, a set A is included in some specific level of the extended low hierarchy (say, in level $E\mathcal{L}_5^{\Sigma}$) if all the information in A that can be accessed via an operator that corresponds to that level (i.e., the $\Sigma_5^{\mathrm{P}}(\cdot)$-operator) is already accessible by an operator that corresponds to the next smaller level (i.e., the $\Sigma_4^{\mathrm{P}}(\cdot)$-operator). An important point is that besides A the weaker operator can also query the $\mathcal{NP}$-complete set SAT. Thus, the only difference between the two operators is that the second operator's access to oracle A is restricted.

Intuitively, if the oracle contains only a limited amount of information, then giving more power to formulate clever queries does not result in a gain of more information from the oracle. However, the very same effect can be observed if the information contained in the oracle is well-organized and therefore easily amenable (as, for example, in the case of QBF, the set of quantified boolean formulas, which for this reason is even located at the base level of the extended low hierarchy).

The next proposition gives a complete picture of the inclusion structure of the levels of the extended low hierarchy, and relates them with the corresponding levels of the low hierarchy inside $\mathcal{NP}$. As proved in [SL94], the various levels form a proper hierarchy with starting point $E\mathcal{L}_2^{\Delta}$ (see part *(ii)* of the next proposition).

Proposition 3.2 [BBS86, AH92, LS91, SL94]

(i) $E\mathcal{L}_1^{\Sigma} = E\mathcal{L}_2^{\Theta} = E\mathcal{L}_2^{\Delta}$.

(ii) $E\mathcal{L}_k^{\Delta} \subset E\mathcal{L}_k^{\Sigma} \subset E\mathcal{L}_{k+1}^{\Theta} \subset E\mathcal{L}_{k+1}^{\Delta}$, $k \geq 2$.

(iii) *All levels of the extended low hierarchy are closed under Turing equivalence.*

(iv) $E\mathcal{L}_k^\Delta \cap \mathcal{NP} = \mathcal{L}ow_k^\Delta$, $E\mathcal{L}_k^\Sigma \cap \mathcal{NP} = \mathcal{L}ow_k^\Sigma$, $k \geq 2$, *and* $E\mathcal{L}_k^\Theta \cap \mathcal{NP} = \mathcal{L}ow_k^\Theta$, $k \geq 3$.

Note that because of part *(i)*, the correspondence between the $E\mathcal{L}_k$ and $\mathcal{L}ow_k$ levels only starts at level $E\mathcal{L}_2^\Delta$.

Lowness properties have also been investigated in a more general setting. For any relativizable class $\mathcal{C}$, we can define the class $\mathcal{C}$*-low* of sets that are *low for* $\mathcal{C}$ as $\{A \mid \mathcal{C}(A) = \mathcal{C}\}$. Thus, e.g., $\mathcal{L}ow_k^\Sigma$ contains all $\mathcal{NP}$ sets that are low for Σ_k^{P}, i.e., $\mathcal{L}ow_k^\Sigma = \Sigma_k^{\mathrm{P}}$*-low* $\cap\, \mathcal{NP}$.

4 Polynomial-size circuits

Perhaps the largest language class that in some sense can still be considered as being computationally tractable is the class of sets that can be recognized by polynomial sized circuits. Pippenger [Pip79] showed that this class contains exactly the languages that can be decided by polynomial-time Turing machines that in addition to the input get some polynomial length bounded advice string that depends only on the input's length. Furthermore, the class $\mathcal{P}/poly$ can be equivalently characterized as the class of sets that are polynomial-time Turing reducible to some sparse set (attributed to A. Meyer in [BH77]).

In their seminal paper, Karp and Lipton [KL80] introduced the general framework of advice classes in order to characterize nonuniform complexity classes.

Definition 4.1 [KL80] *For a class* $\mathcal{C}$ *of sets and a class* $\mathcal{F}$ *of functions from* $\mathcal{N}$ *to* Σ^**, let* $\mathcal{C}/\mathcal{F}$ *be the class of sets* A *such that there is a set* $B \in \mathcal{C}$ *and a function* $h \in \mathcal{F}$ *such that for all* $x \in \Sigma^*$,

$$x \in A \Leftrightarrow \langle x, h(|x|)\rangle \in B.$$

The function h *is called an* advice function *for* A*, and* B *is the corresponding* interpreter set.

Intuitively, $\mathcal{C}/\mathcal{F}$ is the class of sets that can be recognized given the power captured by the complexity class $\mathcal{C}$ plus an amount of advice provided by some function in $\mathcal{F}$. The well-known class $\mathcal{P}/poly$ is obtained by combining the interpreter class $\mathcal{P}$ with the class *poly* of all advice functions h such that $|h(n)| \in n^{O(1)}$.

The lowness properties of $\mathcal{P}/poly$ and related classes are strongly connected with upper bounds either on the complexity of computing advice functions or on the complexity of deciding the graph of advice functions. Actually, the proof of Ko and Schöning [KS85] showing that all $\mathcal{NP}$ sets $A \in \mathcal{P}/poly$ are contained in $\mathcal{L}ow_3^\Sigma$ is based on the fact that for any n and any potential advice string w, it can be decided in $\mathcal{NP}(A)$ whether w gives an incorrect answer (w.r.t. the underlying interpreter set) to some length n instance of A. In other words, the graph

$$\{\langle n, w\rangle \mid w \text{ is correct for all instances of length } n\}$$

of a suitable (multi-valued) advice function h can be computed in $co\text{-}\mathcal{NP}(A) \subseteq \Pi_2^{\mathrm{P}}$. Hence for any set $L \in \Sigma_3^{\mathrm{P}}(A)$, an $\mathcal{NP}(\Pi_2^{\mathrm{P}})$ machine M can first guess an advice string of appropriate length, then ask a suitable Π_2^{P} oracle whether it is correct, and finally – provided the answer is positive – simulate the $\Sigma_3^{\mathrm{P}}(A)$ computation of L by answering all queries to A with the help of the guessed advice string. (Here, we assume that in the simulated $\Sigma_3^{\mathrm{P}}(A)$ computation all queries to A are of the same length; if this is not the case, M has to guess a polynomial number of advice strings, one for each query length.) By the same argument, it follows that if A is an arbitrary set in $\mathcal{P}/poly$, i.e., not necessarily an $\mathcal{NP}$ set, then any set $L \in \Sigma_3^{\mathrm{P}}(A)$ can be computed in $\mathcal{NP}(\mathcal{NP}(A) \oplus \Sigma_2^{\mathrm{P}}) \subseteq \Sigma_2^{\mathrm{P}}(\mathrm{SAT} \oplus A)$, showing that $\mathcal{P}/poly$ is contained in $E\mathcal{L}_3^{\Sigma}$ [BBS86].

The location of $\mathcal{P}/poly$ (and also of the class $(\mathcal{NP} \cap co\text{-}\mathcal{NP})/poly$) in the extended low hierarchy has recently been improved to $E\mathcal{L}_3^{\Theta}$ [Köb94].[1] The improvement has been obtained in two steps. First to $E\mathcal{L}_3^{\Delta}$ by showing that every set in $\mathcal{P}/poly$ has an advice function in $\mathcal{FP}(\Sigma_2^{\mathrm{P}} \oplus \mathcal{NP}(A))$, and subsequently to $E\mathcal{L}_3^{\Theta}$ by showing that the correctness of a given advice string is decidable in $\Theta_2^{\mathrm{P}}(\mathrm{SAT} \oplus A)$. The proof of the first result builds on an elegant technique of Gavaldà [Gav92] who obtained a preceding $\mathcal{FP}(\Sigma_3^{\mathrm{P}} \oplus \mathcal{NP}(A))$ upper bound by combining the "majority vote strategy" known from machine learning (more specifically, exact learning via queries [An88]) with Sipser's application of the universal hashing technique [CW79, Si83].

<u>Discussion</u>. Allender and Hemachandra [AH92] have shown that there exist sparse sets that are not contained in the next lower level $E\mathcal{L}_2^{\Sigma}$ of the extended low hierarchy. Thus, the location of $\mathcal{P}/poly$ in $E\mathcal{L}_3^{\Theta}$ is optimal. However, an interesting problem that remains open is whether the $\mathcal{L}ow_3^{\Theta}$ location of all $\mathcal{NP}$ sets in $\mathcal{P}/poly$ in the low hierarchy can be further improved. The $E\mathcal{L}_2^{\Sigma}$ lower bound for sparse sets in the extended low hierarchy is in no way an indication that also the $\mathcal{L}ow_3^{\Theta}$ location of all $\mathcal{NP}$ sets in $\mathcal{P}/poly$ is optimal. In fact, all sparse sets in $\mathcal{NP}$ are located even at the $\mathcal{L}ow_2^{\Theta}$ level of the low hierarchy [Kad89, LS91].

Of course, it is not possible to obtain absolute lower bounds on the location of classes in the low hierarchy unless we are able to prove that $\mathcal{P} \neq \mathcal{NP}$. Oracle separations at least can tell us the limits of what we might be able to prove by relativizable techniques. Thus it is useful to have *relativized* lower bounds. As shown in [LS91], not all co-sparse sets in $\mathcal{NP}$ are contained in $\mathcal{L}ow_2^{\Delta}$ relative to some oracle. However, for the $\mathcal{L}ow_2^{\Sigma}$ level no relativized lower bound is known, not even for the larger class of all $\mathcal{P}/poly$ sets in $\mathcal{NP}$.

An even more interesting result would be to derive unlikely structural consequences from the assumption that, e.g., all $\mathcal{NP}$ sets in $\mathcal{P}/poly$ are contained in $\mathcal{L}ow_2^{\Sigma}$. For example, it is known that the question whether all sparse sets in $\mathcal{NP}$ are already contained in the $\mathcal{L}ow_1^{\Sigma}$ level (which coincides with $\mathcal{NP} \cap co\text{-}\mathcal{NP}$) is equivalent to the open problem whether the class NE ($= \mathrm{NTIME}(2^{O(n)})$) is closed

[1] The class $(\mathcal{NP} \cap co\text{-}\mathcal{NP})/poly$ is not known to coincide with the possibly larger class $\mathcal{NP}/poly \cap co\text{-}\mathcal{NP}/poly$; see [GB91]. For the latter class, the best known location is $E\mathcal{L}_3^{\Sigma}$ [HHOSTW93].

under complementation [Bo74, HY84, LS91].

5 Membership comparable sets

Ogihara [Ogi94] has recently introduced the notion of membership comparable sets and he showed that complete sets are unlikely to possess this property (see the next section). Intuitively, for a membership comparable set A it might not be possible to determine for each individual instance whether it belongs to A. However, regarding their belonging to set A, it is possible to detect some connection between the elements of any large enough group of instances.

Let $F^A(x_1, \ldots, x_m) = A(x_1) \cdots A(x_m)$ be the function that determines for each of its arguments x_i the membership status with respect to A (see [AG88, ABG, Bei91, BGGO88] for further investigations of notions defined in terms of this function). Furthermore, g denotes in this section always a non-decreasing function $g : \mathcal{N} \to \mathcal{N}^+$ for which there exists a polynomial-time transducer that on input 0^n outputs $0^{g(n)}$. This in particular implies that $g(n) \in n^{O(1)}$.

Definition 5.1 [Ogi94]
A set A is called **polynomial-time g-membership comparable** *– in symbols, $A \in \mathcal{P}\text{-}mc(g)$ – if there is a function $f \in \mathcal{FP}$ such that for all n and all strings $x_1, \ldots, x_{g(n)}$ of length at most n,*

- $f(x_1, \ldots, x_{g(n)}) \in \{0,1\}^{g(n)}$, *and*
- $f(x_1, \ldots, x_{g(n)}) \neq F^A(x_1, \ldots, x_{g(n)})$.

In other words, when given as input a collection of sufficiently many strings $x_1, \ldots, x_m$, then f excludes at least one out of the 2^m many possible values of $F^A(x_1, \ldots, x_m)$.

The union of the classes $\mathcal{P}\text{-}mc(g)$ over all g is denoted by $\mathcal{P}\text{-}mc$.[2] Further, $\mathcal{P}\text{-}mc(log)$ denotes the class of all g-membership comparable sets where $g(n) \in O(\log n)$, and $\mathcal{P}\text{-}mc(const) = \bigcup_{k \geq 1} \mathcal{P}\text{-}mc(k)$ is the corresponding subclass where $g(n) \in O(1)$.

The class $\mathcal{P}\text{-}mc(const)$ coincides with the class of *approximable* sets that were independently introduced in [BKS94]. It is known (see [Bei87b]) that $\mathcal{P}\text{-}mc(const)$ further coincides with the class of all *non-p-superterse* sets introduced by Beigel in [Bei87a].

As shown in [ABG], any non-p-superterse set is contained in $\mathcal{P}/poly$. Ogihara [Ogi94] observed that it follows by essentially the same proof that $\mathcal{P}\text{-}mc \subseteq \mathcal{P}/poly$. He also proved that the classes $\mathcal{P}\text{-}mc(k)$, $k \geq 1$, and $\mathcal{P}\text{-}mc$ are all closed under polynomial-time one-truth-table reducibility, and further, that the latter class contains all sparse sets. In [Bei87a] it is further shown that $\mathcal{P}\text{-}mc(const)$ is closed

[2]Though Ogihara uses $\mathcal{P}\text{-}mc(poly)$ to denote this class.

under bounded truth-table reductions. It has been conjectured by Ogihara that $\mathcal{P}$-*mc* is a proper subclass of $\mathcal{P}/poly$. However, as pointed out in [Ogi94], proving the conjecture is at least as hard as showing that $\mathcal{P} \neq \mathcal{NP}$.

Prominent and well-studied examples of membership comparable sets are the $\mathcal{P}$-*selective* sets introduced by Selman [Sel79] and the $\mathcal{P}$-*cheatable* sets introduced by Beigel [Bei87a, Bei91].

$\mathcal{P}$-*selective* sets are a polynomial-time version of the semi-recursive sets introduced by Jockusch [Joc68]. Informally, a $\mathcal{P}$-*selective* set A can be decided in polynomial time by some *semi-membership* algorithm M (see [DHHT94] for a survey on the recent progress that has been made in the investigation of various notions of selectivity). That is, M takes as input a pair x, y of strings and selects one of them as belonging "more likely" to A in the sense that if exactly one of the two strings belongs to A, then it is guaranteed that this one is selected by M. Hence, if $M(x, y)$ selects x, then it is not possible that $F^A(x, y) = (0, 1)$. Similarly, if $M(x, y)$ selects y, then it follows that $F^A(x, y) \neq (1, 0)$. This shows that every $\mathcal{P}$-*selective* set A is contained in $\mathcal{P}$-*mc*(2) (the inclusion is proper [Ogi94]). Ogihara [Ogi94] further shows that all sets that are (bounded) truth-table reducible to some $\mathcal{P}$-*selective* set are contained in $\mathcal{P}$-*mc*(*log*) (resp., $\mathcal{P}$-*mc*(*const*)).

Like the $\mathcal{P}$-*selective* sets, the $\mathcal{P}$-*cheatable* sets also form a proper subclass[3] of $\mathcal{P}$-*mc*(*const*). For any constant k, let F^A_k be the restriction of F^A to the domain of all k-tuples $\langle x_1, \ldots, x_k\rangle$. A set A is $\mathcal{P}$-*cheatable* [Bei87a] if for some constant k, the function F^A_k is k-*enumerable* [CH89], i.e., there is a polynomial-time function f that when given k strings $x_1, \ldots, x_k$ as input computes a list of k candidate values $\vec{b}_1, \ldots, \vec{b}_k \in \{0, 1\}^k$ such that $F^A_k(x_1, \ldots, x_k) = \vec{b}_i$ for some $i \in \{1, \ldots, k\}$. As shown in [ABG], the class of $\mathcal{P}$-*cheatable* sets is closed under Turing reductions.

We also consider *multi-selective* sets [HJRW95] that have been very recently introduced as a further possibility to generalize the class of $\mathcal{P}$-*selective* sets. From the lowness point of view, the most interesting class investigated in [HJRW95] is the class denoted by *fair*-$S(n-1, 1)$.

Formally, a set A is in *fair*-$S(n-1, 1)$ if there is a polynomial-time computable function f such that for all n and all pairwise different strings $x_1, \ldots, x_n$ of length at most n, $f(x_1, \ldots, x_n)$ selects one string x_i, $1 \leq i \leq n$, with the property that whenever at least $n - 1$ elements among the given strings do belong to A, then also x_i belongs to A. In other words, it is guaranteed that the selected string is not the only one among the given strings that does not belong to A. Obviously, this implies that *fair*-$S(n-1, 1) \subseteq \mathcal{P}$-*mc*$(n)$; as further shown in [HJRW95], the inclusion is proper.

Let us proceed by discussing the lowness properties of these classes. It is known that all $\mathcal{P}$-*selective* and all $\mathcal{P}$-*cheatable* sets are contained in $E\mathcal{L}^{\Sigma}_2$ [ABG]. In fact, in [ABG] the $E\mathcal{L}^{\Sigma}_2$ lowness is proved for a larger class of sets that we call *strongly membership comparable* in this paper.[4]

[3]As shown in [NOS93], there exist even recursive $\mathcal{P}$-*selective* tally sets that are not cheatable.

[4]For the case $g(n) \in O(1)$, this class is implicitly defined in [ABG, Theorem 3.4] in terms of a

Definition 5.2 *Let A be a polynomial-time g-membership comparable set via function f. A is called* **polynomial-time strongly g-membership comparable** – *in symbols, $A \in \mathcal{P}$-smc(g) – if in addition to the requirements of Definition 5.1, f has the property that for all n and all strings $x_1, \ldots, x_{g(n)}$ of length at most n, $f(x_1, \ldots, x_{g(n)})$ contains at most one "0".*

We call A **polynomial-time strongly membership comparable** – in symbols, $A \in \mathcal{P}$-*smc* – if it is strongly g-membership comparable for a suitable g.

In the case that $f(x_1, \ldots, x_{g(n)}) = 1^{g(n)}$, f excludes the possibility that all of its arguments are in A. In the other cases, i.e. $f(x_1, \ldots, x_{g(n)}) = 1^{i-1}01^{g(n)-i}$ for some $i \in \{1, \ldots, g(n)\}$, the information given by f is that if the $g(n) - 1$ many arguments that correspond to a "1" in $f(x_1, \ldots, x_{g(n)})$ indeed are in A, then the remaining argument (the one that corresponds to the unique "0" in $f(x_1, \ldots, x_{g(n)})$) also belongs to A.

It is interesting to note that the information provided by f can be expressed by a Horn clause (over boolean variables z_i, $1 \leq i \leq g(n)$, asserting that $x_i \in A$). Actually, in [ABG] this restriction on f is heavily exploited in order to obtain stronger lowness results as it is possible for general membership comparable sets.

Of course, all $\mathcal{P}$-*cheatable* sets, all $\mathcal{P}$-*selective* sets, and all sets in *fair-S*$(n-1, 1)$ are strongly membership comparable; the $\mathcal{P}$-*cheatable* sets because if F_k^A is k-enumerable, then it is possible to exclude as the value of F_k^A at least one of the $k+1$ vectors in $\{0,1\}^k$ that contain at most one "0"; the $\mathcal{P}$-*selective* sets and, more generally, all sets in *fair-S*$(n-1, 1)$ because they even fulfill the stronger condition that they have a membership comparing function f which only takes values that contain *exactly* one "0". Now we can state the extended lowness result proved in [ABG].[5]

Theorem 5.3 (cf. [ABG]) *If a set A and its complement are both strongly membership comparable, then A is contained in $E\mathcal{L}_2^{\Sigma}$, i.e. $\mathcal{P}$-smc $\cap$ co-($\mathcal{P}$-smc) $\subseteq E\mathcal{L}_2^{\Sigma}$.*

The proof of the above theorem is a clever refinement of the earlier proof of Ko and Schöning [Ko83, KS85] that all $\mathcal{P}$-*selective* sets in $\mathcal{NP}$ are in $\mathcal{L}ow_2^{\Sigma}$. In fact, by combining the arguments used in both proofs the next theorem follows easily (we will give a proof sketch of a more general result below; see Theorem 5.11).

Theorem 5.4 *Any strongly membership comparable set in $\mathcal{NP}$ is in $\mathcal{L}ow_2^{\Sigma}$, i.e. $\mathcal{P}$-smc $\cap\, \mathcal{NP} \subseteq \mathcal{L}ow_2^{\Sigma}$.*

Since the class of $\mathcal{P}$-*selective* sets as well as the class of $\mathcal{P}$-*cheatable* sets are closed under complement, we have a unified method to prove the following lowness results.

---

separability notion.

[5] As indicated above, [ABG] only consider the case $g(n) \in O(1)$ but the generalization to $g(n) \in n^{O(1)}$ is straightforward.

Corollary 5.5

(i) [ABG] *Any $\mathcal{P}$-selective set is in $E\mathcal{L}_2^\Sigma$.*

(ii) [ABG] *Any $\mathcal{P}$-cheatable set is in $E\mathcal{L}_2^\Sigma$.*

(iii) [HJRW95] *fair-S$(n-1,1) \cap \mathcal{NP} \subseteq \mathcal{L}ow_2^\Sigma$.*

(iv) *If a set A as well as its complement are both in fair-S$(n-1,1)$, then A is contained in $E\mathcal{L}_2^\Sigma$.*

Another interesting class of sets that have been recently located at the $\mathcal{L}ow_2^\Sigma$ level (by a somewhat different proof technique using the notion of promise problems [Sel88, LS93]) are the *$\mathcal{NPSV}$-selective* sets introduced in [HNOS94]. In fact, it is not hard to extend the class of strongly membership comparable sets in such a way that, on the one side, it additionally contains the *$\mathcal{NPSV}$-selective* sets, whereas on the other side, Theorems 5.3 and 5.4 remain valid.

Let us continue by restating the formal definition of general *$\mathcal{FC}$-selectivity*, where $\mathcal{FC}$ is any class of functions (possibly multi-valued and/or partial). For a function $f \in \mathcal{FC}$, *set-$f(x)$* denotes the set of all values of f on input x. If $f(x)$ is undefined, then *set-$f(x)$* $= \emptyset$.

Definition 5.6 [Sel79, HHOSTW93, HNOS94]
*A set A is $\mathcal{FC}$-**selective** if there is a function $s \in \mathcal{FC}$ (called an $\mathcal{FC}$-**selector** for A) such that for every x and y,*

- *set-$s(x,y) \subseteq \{x, y\}$, and*
- *$\emptyset \neq A \cap \{x,y\} \Rightarrow \emptyset \neq$ set-$s(x,y) \subseteq A$.*

In other words, s is a selector for A if for every x and y, *set-$s(x,y)$* obeys the restrictions indicated by the following table.

	$x \in A$	$x \notin A$
$y \in A$	$\{x\},\{y\},\{x,y\}$	$\{y\}$
$y \notin A$	$\{x\}$	$\emptyset,\{x\},\{y\},\{x,y\}$

In particular, the following (selector) function classes [BLS85] have been considered. The class $\mathcal{NPMV}$ contains all (partial, multi-valued) functions f for which there is an $\mathcal{NP}$ transducer T such that for any input x, *set-$f(x)$* contains all output values produced by T on input x. The subclass $\mathcal{NPSV}$ contains all single-valued (partial) functions in $\mathcal{NPMV}$. For any class $\mathcal{FC}$ of functions, $\mathcal{FC}_t$ denotes the subclass of all total functions in $\mathcal{FC}$. The following proposition follows easily from the definition of *$\mathcal{FC}$-selectivity*.

We say that a function f reduces to a function g via a reduction function h if for all x, *set-$f(x)$* $= \{h(x,y) \mid y \in$ *set-$g(x)$*$\}$.

Proposition 5.7 *Let $\mathcal{FC}$ be a function class that is closed under reductions by $\mathcal{FP}$ functions. Then the class of $\mathcal{FC}_t$-selective sets is closed under complement.*

Proof. Let A be $\mathcal{FC}_t$*-selective* via selector $f \in \mathcal{FC}_t$. Consider the $\mathcal{FP}$ function h defined as

$$h(\langle x, y\rangle, z) = \begin{cases} y, & x = z, \\ x, & \text{otherwise.} \end{cases}$$

Then the function $\bar{f}$ defined as

$$set\text{-}\bar{f}(x,y) = \begin{cases} \{x\}, & set\text{-}f(x,y) = \{y\}, \\ \{y\}, & set\text{-}f(x,y) = \{x\}, \\ \{x,y\}, & set\text{-}f(x,y) = \{x,y\}, \end{cases}$$

is a selector for the complement of A that reduces to f via reduction function h.

□

The above proposition implies that if a set A is $\mathcal{FC}_t$*-selective*, then A and its complement $\bar{A}$ are both $\mathcal{FC}$*-selective*. Interestingly, for $\mathcal{FC} = \mathcal{NPMV}$ also the converse is true, i.e., A is $\mathcal{NPMV}_t$*-selective* if and only if A and $\bar{A}$ are $\mathcal{NPMV}$*-selective*. However, for $\mathcal{FC} = \mathcal{NPSV}$ this seems not to be the case.

A main motivation for investigating the notion of $\mathcal{NPSV}$*-selectivity* stems from the following interesting link to the question (raised in [FHOS93, Sel]) whether some $\mathcal{NPSV}$ function is able to produce for any satisfiable formula some satisfying assignment.

Theorem 5.8 [HNOS94] SAT *is $\mathcal{NPSV}$-selective if and only if there exists an $\mathcal{NPSV}$ function that produces for any satisfiable formula a satisfying assignment. Hence, there exist no such functions in $\mathcal{NPSV}$ unless $\mathcal{PH} = \Sigma_2^{\mathrm{P}}$.*

The latter conclusion stated in the theorem is a consequence of the fact that all $\mathcal{NPSV}$*-selective* sets in $\mathcal{NP}$ reside within the $\mathcal{L}ow_2^{\Sigma}$ level of the low hierarchy [HNOS94]. Trivially, satisfying assignments can be produced by $\mathcal{FP}(\mathcal{NP})$ (and also $\mathcal{NPMV}$) functions, whereas this is not possible for $\mathcal{FP}$ functions (unless $\mathcal{P} = \mathcal{NP}$). An interesting remaining question in this context is whether satisfying assignments can be computed in deterministic polynomial time by asking *non-adaptive* queries to an $\mathcal{NP}$ oracle (see [NOS93, HNOS93, HNOS94, Sel] for discussions concerning this problem).

In order to get a unified proof for all lowness results of this section, we have to extend the class of strongly membership comparable sets to general function classes $\mathcal{FC}$.

Definition 5.9 *A set A is* **strongly g-membership comparable by $\mathcal{FC}$ functions** *– in symbols, $A \in \mathcal{FC}\text{-smc}(g)$ – if there is a function $f \in \mathcal{FC}$ that for all n and all strings $x_1, \ldots, x_{g(n)}$ of length at most n has the property that*

- $F^A(x_1, \ldots, x_{g(n)}) \notin$ *set-*$f(x_1, \ldots, x_{g(n)})$,
- *set-*$f(x_1, \ldots, x_{g(n)}) \subseteq \{b \in \{0,1\}^{g(n)} \mid$ *the number of zeroes in* b *is at most one*$\}$, *and*
- *if all or all but one of the given strings belong to* A, *then set-*$f(x_1, \ldots, x_{g(n)}) \neq \emptyset$.

Clearly, $\mathcal{FP}$-*smc*(g) is just another name for $\mathcal{P}$-*smc*(g) (this even remains true if we replace $\mathcal{FP}$ by the larger class of all partial functions computable in polynomial time).

The containment of all $\mathcal{P}$-*selective* sets in the class $\mathcal{P}$-*smc*(2) can be easily extended to any function class $\mathcal{FC}$ that is closed under reductions by $\mathcal{FP}$ functions. Hence, for function classes $\mathcal{FC}$ like $\mathcal{NPMV}$, $\mathcal{NPSV}$, $\mathcal{NPMV}_t$, or $\mathcal{NPSV}_t$, all $\mathcal{FC}$-*selective* sets are contained in $\mathcal{FC}$-*smc*(2).

The following lemma extracts a combinatorial argument that has been used in several proofs showing that, e.g., cheatable, selective, and multi-selective sets are included in certain advice classes as well as in certain levels of the low hierarchies; see, e.g., [Ko83, ABG, HNOS94, HJRW95].

For a set A, $[A]^m$ denotes the set of m-element subsets of A.

Lemma 5.10 *Let* $m \geq 1$ *and let* $G \subseteq [A]^m \times A$ *be a (bipartite) graph with the property that*

- *for all* $(Y, x) \in G$, $x \notin Y$, *and*
- *for all* $B \subseteq A$, $\|G_B\| \geq \binom{b}{m+1}$, *where* $b = \|B\|$ *and* G_B *is defined as* $G \cap ([B]^m \times B)$.

Then there exist sets $Y_i \in [A]^m$, $1 \leq i \leq \lceil m \log \|A\| \rceil$, *with the property that for all* x *in* A *there is some* Y_i *such that* $x \in Y_i$ *or* $(Y_i, x) \in G$.

Proof. Consider an arbitrary subset $B \subseteq A$ of cardinality $\|B\| = b \geq m$. We say that a set $Y \in [B]^m$ *covers* x if either x is in Y or (Y, x) is in G. Since by assumption there are at least $\binom{b}{m+1}$ many edges in G_B, each starting from one of $\binom{b}{m}$ many vertices $Y \in [B]^m$, it follows that some Y must have at least $\binom{b}{m+1}/\binom{b}{m}$ outgoing edges and thus covers at least $m + (b-m)/(m+1) > b/(m+1)$ elements in B.

Hence, by iteratively selecting a suitable Y, the number of uncovered strings in A can be decreased in every step by a factor smaller than $\frac{m}{m+1}$. Since $\|A\| \cdot \left(\frac{m}{m+1}\right)^t \leq 1$ for $t \geq \log(\|A\|)/\log\left(\frac{m+1}{m}\right)$, and since $\log\left(\frac{m+1}{m}\right) \geq 1/m$ for $m \geq 1$, the lemma follows. $\square$

Now we are ready to state an extended version of [ABG, Theorem 3.4] which covers all lowness results of this section.

Theorem 5.11

(i) If A and $\bar{A}$ are both in $\mathcal{NPSV}$-smc, then A is in $E\mathcal{L}_2^{\Sigma}$, i.e. $\mathcal{NPSV}$-smc $\cap$ co-($\mathcal{NPSV}$-smc) $\subseteq E\mathcal{L}_2^{\Sigma}$.

(ii) $\mathcal{NPSV}$-smc $\cap\, \mathcal{NP} \subseteq \mathcal{L}ow_2^{\Sigma}$.

Proof sketch. Let A be a set in $\mathcal{NPSV}$-smc(g) via some function $f \in \mathcal{NPSV}$. We first show that A as well as its complement are in $\mathcal{NP}/poly$. We denote the set $A \cap \{0,1\}^n$ by $A^{=n}$ and the index set $\{1, \ldots, n \cdot g(n)\}$ by I_n. Consider the multi-valued advice function h defined as follows.

$$\begin{aligned}
&(Y_i)_{i \in I_n} \in set\text{-}h(n) \Leftrightarrow \\
&\quad \forall i \in I_n : Y_i \in [A^{=n}]^{g(n)-1}, \text{ and} \\
&\quad \forall x \in A^{=n} \exists i \in I_n : x \in Y_i \text{ or } f(Y_i, x) = 1^{g(n)-1}0.
\end{aligned}$$

(Here, for a set $Y = \{y_1, \ldots, y_{g(n)-1}\}$, we simply write $f(Y, x)$ instead of $f(y_1, \ldots, y_{g(n)-1}, x)$ since without loss of generality we can assume that the information given by f does not depend on the order of its arguments.)

By applying Lemma 5.10 above to the graph $G = \{(Y, x) \in [A^{=n}]^{g(n)-1} \times A^{=n} \mid x \notin Y \text{ and } f(Y, x) = 1^{g(n)-1}0\}$, it follows that h is total. Furthermore, for any sequence $(Y_i)_{i \in I_n} \in set\text{-}h(n)$ and all strings x of length n,

$$x \in A \Leftrightarrow \exists i \in I_n : x \in Y_i \text{ or } f(Y_i, x) = 1^{g(n)-1}0$$

and

$$x \notin A \Leftrightarrow \forall i \in I_n : x \notin Y_i \text{ and } f(Y_i, x) = \vec{b} \neq 1^{g(n)-1}0.$$

Since on input $\langle x, (Y_i)_{i \in I_n} \rangle$, each of the two conditions appearing on the right hand sides can be evaluated by an $\mathcal{NP}$ interpreter, this shows that $\mathcal{NPSV}$-*smc* $\subseteq \mathcal{NP}/poly \cap$ co-$\mathcal{NP}/poly$.

If A is an $\mathcal{NP}$ set, then it is easy to see that the graph of h can be decided in Σ_2^{P}, implying part *(ii)* of the theorem.

If instead also $\bar{A}$ is in $\mathcal{NPSV}$-*smc*(g) via some function $\bar{f} \in \mathcal{NPSV}$, then the graph of h can be decided by the following algorithm.

> **input** $\langle n, (Y_i)_{i \in I_n} \rangle$
> **guess** $(Z_i)_{i \in I_n}$
> **accept** if
>
> - for all $i \in I_n$, $Y_i \in [A^{=n}]^{g(n)-1}$ and $Z_i \in [\bar{A}^{=n}]^{g(n)-1}$, and
> - for all x of length n there is an $i \in I_n$ s.t. either $x \in Y_i \cup Z_i$, $f(Y_i, x) = 1^{g(n)-1}0$, or $\bar{f}(Z_i, x) = 1^{g(n)-1}0$.

Note that by the way the class $\mathcal{NPSV}$-*smc* is defined, f and $\bar{f}$ are both defined on all arguments given to them by the above algorithm. Since furthermore f and $\bar{f}$ are single-valued, the algorithm can be implemented in $\mathcal{NP}(\mathrm{SAT} \oplus A)$, implying the $E\mathcal{L}_2^{\Sigma}$ lowness of A. □

Corollary 5.12

(i) [HNOS94] *Any $\mathcal{NPSV}$-selective set in $\mathcal{NP}$ is contained in $\mathcal{L}ow_2^{\Sigma}$.*

(ii) If a set A as well as its complement are both $\mathcal{NPSV}$-selective, then A is contained in $E\mathcal{L}_2^{\Sigma}$.

(iii) All $\mathcal{NPSV}_t$-selective sets are contained in $E\mathcal{L}_2^{\Sigma}$.

As stated in [HNOS94], the containment of any $\mathcal{NPSV}_t$-*selective* set in the class $(\mathcal{NP} \cap co\text{-}\mathcal{NP})/poly$ [HHOSTW93] which is contained in $E\mathcal{L}_3^{\Theta}$ [Köb94] implies already that $\mathcal{NPSV}_t$-*selective* $\subseteq E\mathcal{L}_3^{\Theta}$.

Discussion. Allender and Hemachandra [AH92] have shown that in some relativized world, there is a set that is $\mathcal{P}$-*selective* and $\mathcal{P}$-*cheatable* but which is not contained in the $E\mathcal{L}_2^{\Delta}$ level of the extended low hierarchy. By the result in [NOS93] that if $\mathcal{P} = \mathcal{PP}$, then all $\mathcal{P}$-*selective* sets are Turing equivalent to some tally set, and thus contained in $E\mathcal{L}_2^{\Delta}$ [BB86], it follows that proving an unrelativized $E\mathcal{L}_2^{\Delta}$ lower bound for the class of $\mathcal{P}$-*selective* sets is at least as hard as proving $\mathcal{P} \neq \mathcal{PP}$. For the case of $\mathcal{P}$-*cheatable* sets, the situation even seems to be worse, since if $\mathcal{P} = \mathcal{NP}$, then every $\mathcal{P}$-*cheatable* set is many-one equivalent to some tally set [NOS93].

Thus, an open question for further research is whether the just mentioned results in [NOS93] can be extended to larger subclasses of $\mathcal{P}$-*smc*$\cap$ *co*-($\mathcal{P}$-*smc*), or whether on the other side, it is possible to show an unrelativized $E\mathcal{L}_2^{\Delta}$ lower bound for them. Similarly, it would be interesting to prove unlikely structural consequences from the assumption that, say, all sets in $\mathcal{NPSV}$-*smc* $\cap$ *co*-($\mathcal{NPSV}$-*smc*) are contained in $E\mathcal{L}_2^{\Delta}$.

We close this section by observing that Ogihara's proof of the containment of all sparse sets in $\mathcal{P}$-*mc* actually shows containment in $\mathcal{P}$-*smc*. This implies that $\mathcal{P}$-*smc* is not contained in $E\mathcal{L}_2^{\Sigma}$, and hence not closed under complementation (cf. Theorem 5.3).

6 Combining lowness and naturalness

In this section, we are concerned with the question of what consequences can be derived from the assumption that complete sets (or other natural sets) have a certain lowness property. As it turns out, it can make a subtle difference to assume that just *some* complete set or that *all* complete sets have the lowness property in question. The reason is that although we know that there exist complete sets having special structural properties, we do not know whether all complete sets possess these additional properties.

Among the structural properties that have been investigated and that many natural sets possess are various kinds of self-reducibility (see, e.g., the survey [JY90]) or having self-computable witnesses ([Bal89]; also called "search reduces to decision", see, e.g., [NOS93]). Informally, a set A is self-reducible if it is possible to reduce the membership question for a given instance x to the membership question for a number of "smaller" instances $x_1, \ldots, x_m$. If it additionally holds that x is in the set if and only if at least one of the x_i's is in the set, then A is called disjunctive self-reducible.

Let us consider some examples. From the fact that all sets in $\mathcal{NP}$ that are many-one reducible to a sparse set are located in $\mathcal{L}ow_2^{\Theta}$ [Kad89, LS91] we can conclude that if *some* set in $\mathcal{H}igh_2^{\Theta}$ (e.g., some $\leq_T^{SN}$ complete set for $\mathcal{NP}$) many-one reduces to a sparse set, then $\mathcal{PH}$ collapses to Θ_2^{P}. On the other hand, from the stronger assumption that *every* $\leq_T^{SN}$ complete set (equivalently, some many-one complete set) many-one reduces to a sparse set, it follows that SAT many-one reduces to a sparse set, and thus we get a deeper collapse of $\mathcal{PH}$ down to $\mathcal{P}$ [Mah82].

Similarly, from the fact that all $\mathcal{NP}$ sets in $\mathcal{P}/poly$ are contained in the $\mathcal{L}ow_3^{\Theta}$ level of the low hierarchy we can conclude that no set in $\mathcal{H}igh_3^{\Theta}$ (and therefore no $\leq_T^{SN}$ complete set for $\mathcal{NP}$) can have polynomial sized circuits unless $\mathcal{PH}$ collapses to Θ_3^{P}. However, since SAT is self-reducible, it follows that SAT does not have polynomial sized circuits unless $\mathcal{PH}$ collapses down to Σ_2^{P} [KL80] (and in fact down to $\mathcal{ZPP}(\mathcal{NP})$, see below).

The above examples suggest that natural properties (like being self-reducible) can be exploited to obtain improved lowness results. In fact, as shown in [OW91], every left set A that is bounded truth-table reducible to a sparse set is located in $\mathcal{L}ow_0^{\Sigma} = \mathcal{P}$.[6] Furthermore, it has been shown in [KS85] that all self-reducible sets A in $\mathcal{P}/poly$ are Σ_2^{P}-*low*, i.e., $\Sigma_2^{\mathrm{P}}(A) = \Sigma_2^{\mathrm{P}}$.

Inspired by the work of Bshouty, Cleve, Kannan, and Tamon [BCKT94], the lowness of all self-reducible sets in $\mathcal{P}/poly$ has recently been improved from Σ_2^{P}-*low* to $\mathcal{ZPP}(\mathcal{NP})$-*low* [KW95]. As shown in [BCKT94] by using a result of Jerrum, Valiant, and Vazirani [JVV86], the class of all circuits is exactly learnable in (randomized) expected polynomial time with equivalence queries and the aid of an $\mathcal{NP}$ oracle. From this result it immediately follows that every set A in $\mathcal{P}/poly$ has an advice function that relative to an oracle from $\mathcal{NP}(A)$ is computable by a probabilistic transducer T in the following way: With probability at least $1/2$, T stops on input 0^n within a polynomial number of steps, and on every path, T outputs some advice string that correctly decides all instances of length n (w.r.t. the underlying interpreter set).

[6]Note that besides A being disjunctive self-reducible and many-one reducible to a sparse set, the proof of Mahaney's theorem showing that $A \in \mathcal{P}$ additionally requires that A is $\mathcal{NP}$ complete.

By refining the technique in [BCKT94], it could be shown that every set A in $\mathcal{P}/poly$ that is self-reducible (with respect to a very weak notion of self-reducibility, see [KW95]) has an advice function computable by a probabilistic transducer in the way described above that only uses an oracle from $\mathcal{NP}$ (instead of an $\mathcal{NP}(A)$ oracle). As a consequence, all self-reducible sets A in $\mathcal{P}/poly$ are $\mathcal{ZPP}(\mathcal{NP})$-*low*, i.e., $\mathcal{ZPP}(\mathcal{NP}(A)) = \mathcal{ZPP}(\mathcal{NP})$ (see [KW95] where a direct and self-contained proof for this result is given).

Let us proceed by discussing the recent progress [AA94, BKS94, Ogi94] in extending Selman's [Sel82] result that $\mathcal{NP}$ does not positive truth-table reduce to a $\mathcal{P}$-*selective* set unless $\mathcal{NP} = \mathcal{P}$.[7] This question has attracted many researchers, in particular after Ogiwara and Watanabe were able to generalize Mahaney's theorem to the bounded truth-table case [OW91].

In [Bei88, To91b], it has been proved that if every $\mathcal{NP}$ set truth-table reduces to some $\mathcal{P}$-*selective* set, then $\mathcal{NP} = \mathcal{RP}$. In [BHT93], the result of Selman has been extended by showing that any (Turing) self-reducible set that positive Turing reduces to a $\mathcal{P}$-*selective* set is in $\mathcal{P}$. Furthermore, in [HHOSTW93] it has been shown that if all sets in $\mathcal{NP}$ are 1-truth-table reducible to a $\mathcal{P}$-*selective* set, then $\mathcal{NP} = \mathcal{P}$.

But the bounded truth-table case remained open until recently (a weaker conclusion than $\mathcal{NP} = \mathcal{P}$ has been obtained in [TTW93]). Independently of each other, it has been shown in [AA94, BKS94, Ogi94] that for any constant $c < 1$, $\mathcal{NP}$ does not $O(n^c)$-truth-table reduce to a $\mathcal{P}$-*selective* set unless $\mathcal{NP} = \mathcal{P}$. Whereas Agrawal and Arvind [AA94] attacked the problem directly, Beigel, Kummer, and Stephan [BKS94], as well as Ogihara [Ogi94] used membership comparable sets to prove even more general results. In the proofs of all three papers, the notion of *OR-functions* for a set played an important (implicit or explicit) role.

Definition 6.1 (cf. [Kad88, CKR91, LT92])
An *OR*-**function** for a set A is a function $or_A \in \mathcal{FP}$ such that for every sequence $x_1, \ldots, x_m$ of instances,

$$\mathrm{or}_A(x_1, \ldots, x_m) \in A \Leftrightarrow \exists i, 1 \leq i \leq m, x_i \in A.$$

We call or_A of order l if $|or_A(x_1, \ldots, x_m)| \in m^l n^{O(1)}$, where $n = \max_{1 \leq i \leq m} |x_i|$.

It is well known that *OR-functions* exist for many natural sets like SAT (of order 1), GA (the graph automorphism problem, also of order 1), or GI (of order 2, see [KST92]). Theorem 6.2 below has been proved by Ogihara [Ogi94] for the special case of A = SAT, but it is straightforward to extend his proof to sets having *OR*-functions of arbitrary order.

Theorem 6.2 (cf. [Ogi94]) *Any set A in the class $\mathcal{P}$-mc$(c \log n)$, $c < 1/l$, that has an OR-function of order l and is disjunctive self-reducible is in $\mathcal{P}$.*

[7] Actually, Selman proves that any disjunctive self-reducible set that positive truth-table reduces to a $\mathcal{P}$-*selective* set is in $\mathcal{P}$.

Proof sketch. Let or_A be an *OR*-function of order l for A and let M_{self} be a disjunctive self-reducing machine for A. Further, let $\hat{k}$ be a constant such that

- $|\mathrm{or}_A(x_1,\ldots,x_m)| \le \hat{k}\cdot n^{\hat{k}}\cdot m^l$ for all instances $x_1,\ldots,x_m$ of length at most n, and
- the length of the queries in the self-reduction tree of M_{self} on inputs of length n is bounded by $n^{\hat{k}}$.

The polynomial-time algorithm M for A performs a simple breadth-first search through the self-reduction tree of M_{self} on a given input x combined with pruning at each level. We only describe how the pruning step can be performed. Assume that we are given a set of r instances $x_1,\ldots,x_r$ of length at most $n^{\hat{k}}$ with the property

$$x \in A \Leftrightarrow \exists i, 1 \le i \le r, x_i \in A. \quad (*)$$

For a large enough value of r, we want to exclude one element x_{i_0} from the set in such a way that property $(*)$ is maintained, i.e., x_{i_0} should not be the only one among the given instances that belongs to A.

Let us assume that $r = 2^d$ is a power of two. Then each of the indices $i = 1,\ldots,r$ can be represented by a d-bit vector $b_1\ldots b_d$. For each $j \in \{1,\ldots,d\}$, let $I_j \subseteq \{1,\ldots,r\}$ be the set of all indices with binary representation $b_1\ldots b_d$ for which $b_j = 1$. Of course, each I_j contains exactly $r/2 = 2^{d-1}$ many indices. Further, let y_j be the value of the *OR*-function or_A when given the strings x_i, $i \in I_j$, as arguments.

Now let $f(y_1,\ldots,y_d) = b_1\ldots b_d$, and let i_0 be the index with binary representation $b_1\ldots b_d$. We claim that if x_{i_0} is in A, then it is not the only one in A. Assume to the contrary, it is. Then exactly those y_j are in A for which $b_j = 1$, implying that $F^A(y_1,\ldots,y_d) = b_1\ldots b_d$, a contradiction.

It remains to show that r can be polynomially bounded in $n = |x|$. By assumption, the length of the strings y_j is at most $(\hat{k}n^{\hat{k}})^{\hat{k}}\cdot(2^{d-1})^l \le k'\cdot n^{k'}\cdot 2^{ld}$ for a suitable constant k'. Thus $f(y_1,\ldots,y_d) \ne F^A(y_1,\ldots,y_d)$ provided that $d \ge c\log(k'\cdot n^{k'}\cdot 2^{ld})$, i.e., $(1-cl)d \ge c\log k' + ck'\log n$. But this can be achieved by choosing, e.g., $d = 2ck'\lceil\log n\rceil/(1-cl)$. □

Using a technique of Toda [To91b], Ogihara showed that for any constant $c > 1$, the class $\mathcal{P}$-mc$(c\log f(n))$ contains all sets that are $f(n)$-truth-table reducible to a $\mathcal{P}$-*selective* set. Thus, Theorem 6.2 gives the following corollary that, independently of the work of Ogihara, has been directly proved in [AA94].

Corollary 6.3 [AA94] *If a disjunctive self-reducible set A has an OR-function of order l and is $O(n^c)$-truth-table reducible to a $\mathcal{P}$-selective set for some $c < 1/l$, then it is in $\mathcal{P}$.*

The above corollary should be compared with the following theorem that has been proved (again only for the special case of $A = \text{SAT}$) in [BKS94]. Theorem 6.5 generalizes Corollary 6.3 (taking $k = 1$) but is incomparable to Theorem 6.2. The proof makes use of the next proposition which states a very useful property of sets in $\mathcal{P}$-$mc(k)$.

Proposition 6.4 [Bei87a, Bei87b] *For any set A in $\mathcal{P}$-$mc(k+1)$, the function $F^A(x_1, \ldots, x_n)$ is $S(n, k+1)$-enumerable, where $S(n, k+1) = \sum_{i=0}^{k} \binom{n}{i}$ is a polynomial in n of degree k.*

Theorem 6.5 (cf. [BKS94]) *If A is disjunctive self-reducible and has an OR-function of order l, and if for some constant $c < 1/lk$, A is $O(n^c)$-truth-table reducible to a set $B \in \mathcal{P}$-$mc(k+1)$, then A is in $\mathcal{P}$.*

Proof sketch. As in the proof of Theorem 6.2, it suffices to exclude from a given set of r instances $x_1, \ldots, x_r$, $r = 2^d$, of length at most $n^{O(1)}$ some element x_{i_0} such that x_{i_0} is not the only one of the given instances that belongs to A. Exactly as in the proof of Theorem 6.2, we can compute strings y_j, $1 \leq j \leq d$, of length at most $n^{O(1)} \cdot 2^{ld}$ with the property that

$$\begin{aligned} &F^A(y_1, \ldots, y_d) \neq b_1 \ldots b_d \\ &\quad \Rightarrow F^A(x_1, \ldots, x_r) \neq 0^{i_0 - 1} 1 0^{r - i_0}, \end{aligned}$$

where i_0 is the index with binary representation $b_1 \ldots b_d$.

Since A is $O(n^c)$-truth-table reducible to a set $B \in \mathcal{P}$-$mc(k+1)$, we can compute $m = d \cdot n^{O(1)} \cdot 2^{cld}$ instances $z_1, \ldots, z_m$ such that knowing membership in B for each of these strings allows us to determine membership in A for each of the instances $y_1, \ldots, y_d$. Since B is in $\mathcal{P}$-$mc(k+1)$, it follows from Proposition 6.4 that $F^B(z_1, \ldots, z_m)$ is $h(m)$-enumerable for some function $h(m) \in O(m^k) = d^k \cdot n^{O(1)} \cdot 2^{cldk}$. Since by assumption $ckl < 1$, it is possible to choose $d \in O(\log n)$ such that $h(m) < 2^d$. □

<u>Discussion</u>. We have seen that self-reducibility can have a considerable impact on the lowness properties of the corresponding languages. Few and only relativized lower bounds for such languages are known. For example, in [Hel86, Wil85] an oracle B is constructed relative to which $\mathcal{NP}$ is contained in $\mathcal{P}/poly$ but $\mathcal{PH}$ does not collapse to $\mathcal{P}(\mathcal{NP})$. Thus, relative to B there exist self-reducible languages in $\mathcal{P}/poly$ that are not $\mathcal{P}(\mathcal{NP})$-*low*. Interestingly, relative to B all self-reducible languages in $\mathcal{P}/poly$ are in $\mathcal{BPP}$ and thus $\mathcal{BPP}$-*low*. This raises the question whether there are any unlikely consequences from the assumption that all self-reducible languages in $\mathcal{P}/poly$ are in $\mathcal{BPP}$. As a first step to improve the $\mathcal{ZPP}(\mathcal{NP})$ lowness of these languages one might also try to show that they can be decided in $\mathcal{ZPP}$ with non-adaptive queries to an $\mathcal{NP}$ oracle.

Regarding self-reducible membership comparable sets, the obvious question is whether the results reported in this section can be improved or generalized. For example, looking at Theorems 6.2 and 6.5, one might suspect that there is a trade-off between the number of queries in the truth-table reduction of A to set B in $\mathcal{P}$-$mc(g(n))$ and the number $g(n)$ of elements that are needed in order to derive some information about their membership in B.

7 Lowness for counting classes

In this section we briefly discuss some recent lowness results concerning counting classes, i.e., complexity classes that are defined in terms of the number of accepting paths of nondeterministic polynomial-time Turing machines.

Toda's Theorem [To91a] is proved in two parts which are of independent interest from the lowness point of view. In the first part, he strengthened the result of Valiant and Vazirani [VV86] showing that $\mathcal{NP}$ is contained in the class $\mathcal{BPP}(\oplus\mathcal{P})$ to a lowness result, thus obtaining the inclusion (and in fact the lowness) of the whole polynomial hierarchy in $\mathcal{BPP}(\oplus\mathcal{P})$. In the second part he proves that the evidently larger class $\mathcal{PP}(\oplus\mathcal{P})$ is contained in $\mathcal{P}^{\#\mathcal{P}[1]}$, i.e., one query to the $\#\mathcal{P}$ oracle suffices. Actually, Toda proved that all the classes $\mathcal{M}od_p\mathcal{P}$, p prime, are low for $\mathcal{P}^{\#\mathcal{P}[1]}$.

It has been observed by many researchers that the $\mathcal{P}^{\#\mathcal{P}[1]}$ machine M in Toda's proof of the second result needs only to ask its oracle $f \in \#\mathcal{P}$ about one particular bit in the binary representation of $f(y)$. Motivated by this observation, the complexity class $\mathcal{MP}$ (middle bit P) has been introduced as containing all languages that can be decided by knowing just one bit of the binary representation of a $\#\mathcal{P}$ function f.

Thus, Toda's second result shows that $\mathcal{PP}(\oplus\mathcal{P})$ is a subclass of $\mathcal{MP}$. From Toda's proof it can be moreover derived that $\oplus\mathcal{P}$ is low for the class $\mathcal{MP}$. Let us have a closer look at Toda's proof of his second result. The main ingredient is a means of amplifying the modulus in the $\oplus\mathcal{P}$-representation $f \in \#\mathcal{P}$ of an oracle $A \in \oplus\mathcal{P}$. Intuitively speaking, Toda showed that one can insert a polynomial number of 0's to the left of the important least significant bit in the binary representation of the values of f. To be able to perform this process, Toda had to invent the so-called *modulus amplifying polynomials*.

The **modulus-amplifying** polynomials P_d have for every $m \geq 1$ and $k \geq 0$ the following properties:

$$\begin{aligned} k &\equiv 0 \pmod{m} &\Rightarrow\quad P_d(k) &\equiv 0 \pmod{m^d}, \\ k &\equiv -1 \pmod{m} &\Rightarrow\quad P_d(k) &\equiv -1 \pmod{m^d}. \end{aligned}$$

Toda inductively defined his polynomials as follows: $P_2(k) = 3k^4 + 4k^3$ and for $i > 1$, $P_{2^i}(k) = P_2(P_{2^{i-1}}(k))$. For $2^{i-1} < d < 2^i$, one can take $P_d = P_{2^i}$. Then the modulus-amplification property is easily proved by induction [To91a].

The following polynomials exhibit nearly the same behavior as Toda's original polynomials (similar polynomials have been used in [KT, Sch95]).

Proposition 7.1 *For odd d, let $Q_d(k) = (k^d + 1)^d$, and in case d is even, let $Q_d(k) = (k^{d+1} + 1)^d$. Then, for every $m \geq 1$ and $k \geq 0$,*

$$\begin{aligned} k \equiv 0 \pmod{m} &\Rightarrow Q_d(k) \equiv 1 \pmod{m^d}, \\ k \equiv -1 \pmod{m} &\Rightarrow Q_d(k) \equiv 0 \pmod{m^d}. \end{aligned}$$

Proof. We only give the proof for the case that d is odd; the case d even is analogous. For $k \equiv 0 \pmod{m}$ it follows that

$$\begin{aligned} k^d \equiv 0 \pmod{m^d} &\Rightarrow k^d + 1 \equiv 1 \pmod{m^d} \\ &\Rightarrow (k^d + 1)^d \equiv 1 \pmod{m^d}, \end{aligned}$$

and for $k \equiv -1 \pmod{m}$, we have

$$\begin{aligned} k^d \equiv -1 \pmod{m} &\Rightarrow k^d + 1 \equiv 0 \pmod{m} \\ &\Rightarrow (k^d + 1)^d \equiv 0 \pmod{m^d}. \Box \end{aligned}$$

By using negative coefficients, modulus amplifying polynomials of smaller degree have been constructed [Yao90, BT91]. The polynomials of Beigel and Tarui have degree exactly $2d - 1$ which is optimal.

By abstracting this amplification property of $\oplus\mathcal{P}$ oracles to general $\mathcal{MP}$ sets, Green et al. [GKRST] were led to the interesting subclass $\mathcal{A}mp\mathcal{MP}$ of $\mathcal{MP}$. By definition, for languages in $\mathcal{A}mp\mathcal{MP}$ it is possible to insert any desired number of 0's on both the left and the right of the membership deciding bit. Based on Toda's first result, Green et al. observed that all languages in $\mathcal{PH}$ allow for such an amplified middle bit representation (i.e. $\mathcal{PH} \subseteq \mathcal{BPP}(\oplus\mathcal{P}) \subseteq \mathcal{A}mp\mathcal{MP}$). As further observed in [GKRST], Toda's second theorem (in the form stated above, namely that $\oplus\mathcal{P}$ is low for $\mathcal{MP}$) can be partially extended from $\oplus\mathcal{P}$ to arbitrary $\mathcal{A}mp\mathcal{MP}$ oracles: Asking a *constant* number of queries (on every computation path) to an $\mathcal{A}mp\mathcal{MP}$ oracle does not increase the power of $\mathcal{MP}$ computations (in symbols $\mathcal{MP}^{\mathcal{A}mp\mathcal{MP}[O(1)]} = \mathcal{MP}$).

For many important subclasses of $\mathcal{A}mp\mathcal{MP}$ as, for example, $\mathcal{BPP}$, $\mathcal{PH}$, $\oplus\mathcal{P}$, and $\mathcal{BPP}(\oplus\mathcal{P})$, the restriction of allowing only a constant number of oracle queries takes no effect since these subclasses are closed under Turing reductions. Actually, every subclass of $\mathcal{A}mp\mathcal{MP}$ which is closed under both conjunctive and disjunctive reducibilities is low for $\mathcal{MP}$ [GKRST]. As an interesting consequence, since the class $\mathcal{C}_=\mathcal{P}$ has these closure properties, $\mathcal{C}_=\mathcal{P}$ is not contained in $\mathcal{A}mp\mathcal{MP}$ unless $\mathcal{CH}$ collapses to $\mathcal{MP}$.

Whereas for the case of $\oplus\mathcal{P}$ oracles it is a straightforward task to transform Toda's lowness result for $\mathcal{P}^{\#\mathcal{P}[1]}$ to the corresponding lowness result for $\mathcal{MP}$, it is not at all clear *à priori* whether such a transformation can also be performed for the other $\mathcal{MOD}$ classes. It is not even obvious that, say, $\mathcal{M}od_3\mathcal{P}$ is *contained* in

$\mathcal{MP}$, since in order to decide whether a number written in base 2 is congruent to 0 modulo 3, one needs the information of all of its bits. Nevertheless, as shown in [GKRST], also for $k > 2$, the classes $\mathcal{M}od_k\mathcal{P}$ are contained in $\mathcal{A}mp\mathcal{MP}$ and furthermore low for $\mathcal{MP}$.

So far, all considered subclasses of $\mathcal{A}mp\mathcal{MP}$ are low for $\mathcal{MP}$, and one might suspect that even $\mathcal{A}mp\mathcal{MP}$ itself has this property. This suspicion seems to be supported by the fact that the "hard" counting classes $\mathcal{C}_=\mathcal{P}$, $\mathcal{PP}$, and $\mathcal{MP}$ are not contained in $\mathcal{A}mp\mathcal{MP}$ unless $\mathcal{CH}$ collapses. (By a "hard" counting class $\mathcal{C}$ we mean that the whole counting hierarchy ($\mathcal{CH}$) [Wag86] can be built as a union of towers of $\mathcal{C}$, i.e., $\mathcal{CH} = \mathcal{C} \cup \mathcal{C}^{\mathcal{C}} \cup \mathcal{C}^{\mathcal{C}^{\mathcal{C}}} \cup \ldots$).

However, the initial hope that the lowness of $\mathcal{A}mp\mathcal{MP}$ for $\mathcal{MP}$ (without any extra condition on the number of queries) might be provable has been deemed by the recent result [KT] that $\mathcal{A}mp\mathcal{MP}$ is truth-table equivalent in power to $\mathcal{MP}$ (and consequently Turing equivalent to $\mathcal{PP}$). As an immediate consequence, unless $\mathcal{CH}$ collapses, $\mathcal{A}mp\mathcal{MP}$ is not low for $\mathcal{MP}$ (and hence for the partial lowness property of $\mathcal{A}mp\mathcal{MP}$ for $\mathcal{MP}$ it is crucial that the number of oracle queries is bounded).

The unexpected power of the class $\mathcal{A}mp\mathcal{MP}$ has been revealed in two steps. First, it turned out that the newly defined class $\mathcal{M}od\mathcal{P}$ is a "hard" counting class (in the sense explained above). Second, the containment of the $\mathcal{M}od_k\mathcal{P}$ classes in $\mathcal{A}mp\mathcal{MP}$ could be extended to the class $\mathcal{M}od\mathcal{P}$; thus carrying over the power of $\mathcal{M}od\mathcal{P}$ to $\mathcal{A}mp\mathcal{MP}$. The counting class $\mathcal{M}od\mathcal{P}$ is a generalization of the classes $\mathcal{M}od_p\mathcal{P}$, p prime. Intuitively speaking, in the case of a $\mathcal{M}od\mathcal{P}$ language A, one can choose different prime moduli p for different inputs x, with the only restriction that p in unary can be computed from x in polynomial time. As shown in [KT], this amount of flexibility suffices to provide $\mathcal{M}od\mathcal{P}$ with the full power of polynomial-time counting: any $\#\mathcal{P}$ function can be computed in polynomial time by making one round of parallel queries to some oracle in $\mathcal{M}od\mathcal{P}$. Hence, the lowness properties of the classes $\mathcal{M}od_p\mathcal{P}$ for $\mathcal{MP}$ do not pass over to their generalization $\mathcal{M}od\mathcal{P}$ unless the counting hierarchy collapses to $\mathcal{MP}$.

We close this section by a brief description of how the lowness results for the classes $\mathcal{P}^{\#\mathcal{P}[1]}$ and $\mathcal{MP}$ have been translated into circuit complexity.

The circuit analogue of Toda's first result (namely that $\mathcal{PH}$ is contained in $\mathcal{BPP}(\oplus\mathcal{P})$) was proved by Allender [All89], using algebraic methods introduced by Razborov [Raz87] and Smolensky [Smo87]. It states that any $\mathcal{AC}^0$ predicate (i.e., computable by a family of unbounded fan-in Boolean circuits of constant depth and polynomial size; [Co85]) can be probabilistically computed by a family of PARITY$^+$ circuits, i.e., they have a parity gate at the root which is connected to a *quasi-polynomial* (i.e., $2^{(\log n)^{O(1)}}$) number of AND gates of *small* (i.e., polylog) fan-in. Allender and Hertrampf [AH90] subsequently applied the Valiant-Vazirani technique to obtain a uniform version of Allender's result.

Yao [Yao90] then used these techniques to obtain the first non-trivial upper bound for $\mathcal{ACC}$ (i.e., the class of predicates computable by a family of unbounded fan-in Boolean circuits of constant depth and polynomial size, augmented by MOD$_m$ gates for a fixed modulus m; [Bar89, BT88, MT89]). By combining the Valiant-Vazirani method with improved versions of Toda's amplifying polynomials, he showed that every language in $\mathcal{ACC}$ can be recognized by a family of depth-2 probabilistic circuits of quasi-polynomial size with a symmetric gate at the root and small AND gates at the leaves.

Then Beigel and Tarui [BT91] simplified Yao's proof and strengthened the result in two respects: (1) they use *deterministic* circuits of the same form, and (2) their simulation applies not only to $\mathcal{ACC}$ circuits, but also to circuits consisting of one symmetric gate (at the root) connected to $\mathcal{ACC}$ sub-circuits. This is the circuit analogue of the (relativizable) result that $\mathcal{PH}$ and all the $\mathcal{M}od_k\mathcal{P}$ classes are low for $\mathcal{P}^{\#\mathcal{P}[1]}$.

Discussion. One of the open problems in circuit complexity is whether $\mathcal{ACC}$ is a proper subclass of $\mathcal{TC}^0$ (it is not hard to see that $\mathcal{ACC}$ is contained in $\mathcal{TC}^0$, the class of predicates computable by a family of unbounded fan-in threshold circuits of constant depth and polynomial size; see, e.g., [MP68]). Actually, Yao [Yao90] conjectured that there are languages in $\mathcal{TC}^0$ which cannot be computed by probabilistic circuits consisting of a symmetric gate over a quasi-polynomial number of small AND's. Likewise, Beigel and Tarui [BT91] made a nominally weaker conjecture for deterministic circuits of this kind. Of course, each of these conjectures implies that $\mathcal{ACC}$ is properly contained in $\mathcal{TC}^0$. However, in the proofs of Yao as well as of Beigel and Tarui, the symmetric gate at the root depends on the number of inputs and the types of modular gates used in the $\mathcal{ACC}$ circuit. Thus, it might be hard to show for a specific $\mathcal{TC}^0$ predicate that it is not computable by depth-2 circuits of the type given in [Yao90] or [BT91].

In contrast, the $\mathcal{ACC}$ simulation given by Green et al. [GKRST] is based on the lowness of $\mathcal{PH}$ and all $\mathcal{M}od_k\mathcal{P}$ classes for $\mathcal{MP}$, and consequently has a gate of fixed type MidBit at the root. By definition, a MidBit gate with inputs $x_1, \ldots, x_n$ outputs the $\lfloor \log_2(n)/2 \rfloor^{\text{th}}$ bit in the binary representation of the number $\sum_{i=1}^{n} x_i$. Hence, the conjectures of Yao and of Beigel and Tarui have been further weakened to the following one which is still strong enough to imply that $\mathcal{ACC}$ is properly contained in $\mathcal{TC}^0$: *There are* $\mathcal{TC}^0$ *predicates that cannot be computed by circuits consisting of a* MidBit *gate over a quasi-polynomial number of small* AND*'s.*

References

[AM77] L. Adleman and K. Manders, Reducibility, randomness, and intractability, *Proc. 9th STOC* (1977) 151–163.

[AA94] M. Agrawal, V. Arvind, Polynomial time truth-table reductions to P-selective sets, *Proc. 9th STRUCTURES* (IEEE, 1994) 24–30.

[AA95] M. Agrawal, V. Arvind, Reductions of self-reducible sets to depth-1 weighted threshold circuit classes, and sparse sets. To appear in *Proc. 10th STRUCTURES* (IEEE, 1995).

[AH+93] V. Arvind, Y. Han, L. Hemachandra, J. Köbler, A. Lozano, M. Mundhenk, M. Ogiwara, U. Schöning, R. Silvestri, and T. Thierauf, Reductions to sets of low information content, In: K. Ambos-Spies, S. Homer und U. Schöning (Hrsg.), *Complexity Theory, Current Research* (Cambridge U. Press, 1993) 1–45.

[AKM92] Arvind, J. Köbler, and M. Mundhenk, Upper bounds for the complexity of sparse and tally descriptions. To appear in *MST*. A preliminary version appeared in *Proc. 3rd ISAAC* (Springer, LNCS #650, 1992) 249–258.

[All89] E. Allender, A note on the power of threshold circuits, *Proc. 30th FOCS* (1989) 580–584.

[AH92] E. Allender and L. Hemachandra, Lower bounds for the low hierarchy, *J. ACM* **39** (1992) 234–250.

[AH90] E. Allender and U. Hertrampf, On the power of uniform families of constant depth threshold circuits, *Proc. 15th MFCS* (Springer, LNCS #452, 1990) 158–164.

[ABG] A. Amir, R. Beigel, and W. Gasarch, Some connections between bounded query classes and non-uniform complexity. Submitted. A preliminary version appeared in *Proc. 5th STRUCTURES* (IEEE, 1990) 232–243.

[AG88] A. Amir and W. Gasarch, Polynomial terse sets, *Inf. and Comp.* **77** (1988) 37–56.

[An88] D. Angluin, Queries and concept learning, *Machine Learning* **2** (1988) 319–342.

[BM88] L. Babai and S. Moran, Arthur-Merlin games: a randomized proof system and a hierarchy of complexity classes, *JCSS* **36** (1988) 254–276.

[Bal89] J. Balcázar, Self-reducibility structures and solutions of NP problems, *Revista Matematica,* Universidad Complutense de Madrid, Vol. 2, No. 2/3 (1989) 175–184.

[Bal90] J. Balcázar, Self-reducibility, *JCSS* **41** (1990) 367–388.

[BB86] J.L. Balcázar and R. Book, Sets with small generalized Kolmogorov complexity. *Acta Informatica* **23** (1986) 679–688.

[BBS86] J. Balcázar, R. Book, and U. Schöning, Sparse sets, lowness and highness, *SIAM J. Comp.* **23** (1986) 679–688.

[BDG] J. Balcázar, J. Díaz, J. Gabarró, *Structural Complexity Theory.* (Springer, 1988 and 1990).

[Bar89] D. Barrington, Bounded-width polynomial-size branching programs recognize exactly those languages in NC^1, *JCSS* **38** (1989) 150–164.

[BT88] D. Barrington and D. Thérien, Finite monoids and the fine structure of NC^0, *J. ACM* **35** (1988) 941–952.

[Bei87a] R. Beigel, Query-limited reducibilities, Ph.D. thesis (Stanford University, 1987).

[Bei87b] R. Beigel, A structural theorem that depends quantitatively on the complexity of SAT, *Proc. 2nd STRUCTURES* (IEEE, 1987) 28–32.

[Bei88] R. Beigel, NP-hard sets are p-superterse unless R = NP, Tech. Rep. 88-04 (John Hopkins U., 1988).

[Bei91] R. Beigel, Bounded queries to SAT and the Boolean hierarchy, *TCS* **84** (1991) 199–223.

[BGGO88] R. Beigel, W. Gasarch, J. Gill, and J. Owings, Terse, superterse, and verbose sets, *Inf. and Comp.* **103** (1988) 68–85.

[BG92] R. Beigel and J. Gill, Counting classes: thresholds, parity, mods, and fewness, *TCS* **103** (1992) 3–23.

[BKS94] R. Beigel, M. Kummer, and F. Stephan, Approximable sets, *Proc. 9th STRUCTURES* (IEEE, 1994) 12–23.

[BT91] R. Beigel and J. Tarui, On ACC, *Proc. 32nd FOCS* (1991) 783–792.

[Ber78] P. Berman, Relationship between density and deterministic complexity of NP-complete languages, *Proc. 5th ICALP* (Springer, LNCS #62, 1978) 63–71.

[BH77] L. Berman, J. Hartmanis, On isomorphism and density of NP and other complexity classes, *SIAM J. Comp.* **6** (1977) 305–327.

[BHZ87] R. Boppana, J. Hastad, and S. Zachos, Does co-NP have short interactive proofs? *IPL* **25** (1987) 27–32.

[Bo74] R. Book, Tally languages and complexity classes, *Inf. and Control* **26** (1974) 186–193.

[BLS85] R. Book, T. Long and A. Selman, Qualitative relativizations of complexity classes, *JCSS* **30** (1991) 395–413.

[BC93] D. Bovet and P. Crescenzi, *Introduction to the Theory of Complexity* (Prentice-Hall, 1993).

[BCKT94] N. Bshouty, R. Cleve, S. Kannan, and C. Tamon, Oracles and queries that are sufficient for exact learning, *Proc. 7th COLT* (1994) 130–139.

[BHT93] H. Buhrman, P. v. Helden, and L. Torenvliet, Selective self-reducible sets: A new characterization of P, *Proc. 8th STRUCTURES* (IEEE, 1993) 44–51.

[BT94] H. Buhrman and L. Torenvliet, On the structure of complete sets, *Proc. 9th STRUCTURES* (IEEE, 1994) 118–133.

[CH89] J. Cai and L. Hemachandra, Enumerative counting is hard, *Inf. and Comp.* **92(1)** (1989) 34–44.

[CW79] J. Carter and M. Wegman, Universal classes of hash functions, *JCSS* **18** (1979) 143–154.

[CKR91] R. Chang, J. Kadin, and P. Rohatgi, Connections between the complexity of unique satisfiability and the threshold behavior of randomized reductions, *Proc. 6th STRUCTURES* (IEEE, 1991) 255–269.

[Co85] S. Cook, A taxonomy of problems with fast parallel algorithms, *Inf. and Control* **64** (1985) 2–22.

[DHHT94] D. Denny-Brown, Y. Han, L. Hemaspaandra, L. Torenvliet, Semi-membership algorithms: Some recent advances, *SIGACT News* **25(3)** (1994) 12–23.

[FFK92] S. Fenner, L. Fortnow, and S. Kurtz, The isomorphism conjecture holds relative to an oracle, *Proc. 33rd FOCS* (IEEE, 1992) 30–39.

[FFK94] S. Fenner, L. Fortnow, and S. Kurtz, Gap-definable counting classes, *JCSS* **48** (1994) 116–148.

[FHOS93] S. Fenner, S. Homer, M. Ogiwara, and A. Selman, On using oracles that compute values, *Proc. 10th STACS* (Springer, LNCS #665, 1993) 398–407.

[For79] S. Fortune, A note on sparse complete sets, *SIAM J. Comp.* **8(3)** (1979) 431–433.

[GJ79] M. Garey, D. Johnson, *Computers and Intractability – A Guide to the Theory of NP-Completeness*, (Freeman and Company, 1979).

[Gav92] R. Gavaldà, Bounding the complexity of advice functions, *Proc. 7th STRUCTURES* (IEEE, 1992) 249–254.

[GB91] R. Gavaldà and J. Balcázar, Strong and robustly strong polynomial time reducibilities to sparse sets, *TCS* **88(1)** (1991) 1–14.

[Gil77] J. Gill, Computational complexity of probabilistic Turing machines. *SIAM J. Comp.* **6** (1977) 675–695.

[GJ86] J. Goldsmith and D. Joseph, Three results on the polynomial isomorphism of sets, *Proc. 27th FOCS* (IEEE, 1986) 390–397.

[GMR89] S. Goldwasser, S. Micali, C. Rackoff, The knowledge complexity of interactive proof systems, *SIAM J. Comp.* **18** (1989) 186–208.

[GS86] S. Goldwasser, M. Sipser, Private coins versus public coins in interactive proof systems. In: S. Micali (Ed), *Advances in Computing Research, Vol 5: Randomness and Computation* (JAI Press, 1989) 73–90.

[GKRST] F. Green, J. Köbler, K. Regan, T. Schwentick and J. Torán, The power of the middle bit of a #P function. To appear in *JCSS*.

[HY84] J. Hartmanis and Y. Yesha. Computation times of NP sets of different densities, *TCS* **34** (1984) 17–32.

[Hel86] H. Heller, On relativized exponential and probabilistic complexity classes, *Inf. and Control* **71** (1986) 231–243.

[HHOSTW93] L. Hemachandra, A. Hoene, M. Ogiwara, A. Selman, T. Thierauf, and J. Wang, Selectivity, *Proc. 5th ICCI* (IEEE, 1993) 55–59.

[HJRW95] L. Hemaspaandra, Z. Jiang, J. Rothe, and O. Watanabe, Multi-selectivity and complexity-lowering joins, Tech. Rep. TR-568 (U. of Rochester, 1995).

[HNOS94] L. Hemaspaandra, A. Naik, M. Ogihara, and A. Selman, Computing solutions uniquely collapses the polynomial hierarchy, *Proc. 5th ISAAC* (1994) 56–64.

[HOW92] L. Hemachandra, M. Ogiwara, and O. Watanabe, How hard are sparse sets? *Proc. 7th STRUCTURES* (IEEE, 1992) 222–238.

[HNOS93] E. Hemaspaandra, A. Naik, M. Ogiwara and A. Selman, P-selective sets, and reducing search to decision vs. self-reducibility, Tech. Rep. 93–21 (SUNY-Buffalo, 1993).

[Hom90] S. Homer, Structural properties of nondeterministic complete sets, *Proc. 5th STRUCTURES* (IEEE, 1990) 3–10.

[JVV86] M. Jerrum, L. Valiant, V. Vazirani, Random generation of combinatorial structures from a uniform distribution, *TCS* **43** (1986) 169–188.

[Joc68] C. Jockusch, Semirecursive sets and positive reducibility, *Trans. AMS* **131** (1968) 420–436.

[JY85] D. Joseph and P. Young, Some remarks on witness functions for non-polynomial and non-complete sets in NP, *TCS* **39** (1985) 225–237.

[JY90] D. Joseph and P. Young, Self-reducibility: effects of internal structure on computational complexity. In A. Selman (Ed). *Complexity Theory Retrospective* (Springer, 1990) 82–107.

[Kad88] J. Kadin, *Restricted Turing Reducibilities and the Structure of the Polynomial Time Hierarchy,* Ph.D. Thesis (Cornell University, 1988).

[Kad89] J. Kadin, $\mathrm{P}^{\mathrm{NP}[\log n]}$ and sparse Turing-complete sets for NP, *JCSS* **39** (1989) 282–298.

[KL80] R. Karp and R. Lipton, Some connections between nonuniform and uniform complexity classes, *Proc. 12th STOC* (1980) 302–309.

[Ko83] K. Ko, On self-reducibility and weak p-selectivity. *JCSS* **26** (1983) 209–221.

[KS85] K. Ko and U. Schöning, On circuit-size complexity and the low hierarchy in NP, *SIAM J. Comp.* **14** (1985) 41–51.

[Köb94] J. Köbler, Locating P/poly optimally in the extended low hierarchy, *TCS* **134** (1994) 263–285.

[KSTT92] J. Köbler, U. Schöning, J. Torán and S. Toda, Turing Machines with few accepting computations and low sets for PP, *JCSS* **44** (1992) 272–286.

[KST92] J. Köbler, U. Schöning, and J. Torán, Graph isomorphism is low for PP. *Comput. Complexity* **2** (1992) 301–330.

[KST93] J. Köbler, U. Schöning, J. Torán, *The Graph Isomorphism Problem: Its Structural Complexity* (Birkhäuser, 1993).

[KT] J. Köbler and S. Toda, On the power of generalized MOD-classes. To appear in *MST*. A preliminary version appears in *Proc. 8th STRUCTURES* (1993) 147–155.

[KW95] J. Köbler and O. Watanabe, New collapse consequences of NP having small circuits. To appear in *Proc. 22nd ICALP* (Springer, 1995).

[KMR89] S. Kurtz, S. Mahaney, and J. Royer, The isomorphism conjecture fails relative to a random oracle, *Proc. 19th STOC* (1989) 157–166.

[KMR90] S. Kurtz, S. Mahaney, and J. Royer, The structure of complete degrees. In A. Selman (Ed). *Complexity Theory Retrospective* (Springer, 1990) 108–146.

[LLS75] R. Ladner, N. Lynch, and A. Selman, A comparison of polynomial time reducibilities, *TCS* **1** (1975) 103–123.

[Ler83] M. Lerman, *Degrees of Unsolvability.* (Springer, 1983).

[Lon82a] T. Long, Strong nondeterministic polynomial-time reducibilities, *TCS* **21** (1982) 1–25.

[Lon82b] T. Long, A note on sparse oracles for NP, *JCSS* **24** (1982) 224–232.

[LS91] T. Long and M. Sheu, A refinement of the low and high hierarchies, Tech. Rep. OSU-CISRC-2/91-TR6 (The Ohio State U., 1991).

[LS93] L. Longpré and A. Selman, Hard promise problems and nonuniform complexity, *TCS* **115** (1993) 277–290.

[LT92] A. Lozano, J. Torán, On the non-uniform complexity of the graph isomorphism problem, *Proc. 7th STRUCTURES* (IEEE, 1992) 118–131.

[Mah82] S. MAHANEY, Sparse complete sets for NP: Solution of a conjecture of Berman and Hartmanis, *JCSS* **25(2)** (1982) 130–143.

[MT89] P. MCKENZIE AND D. BARRINGTON, Automata theory meets circuit complexity, *Proc. 16th ICALP* (Springer, LNCS #372, 1989) 589–602.

[MP79] A. MEYER, M. PATERSON, With what frequency are apparently intractable problems difficult? Tech. Report MIT/LCS/TM-126 (MIT, 1979).

[MS73] A. MEYER AND L. STOCKMEYER, The equivalence problem for regular expressions with squaring requires exponential time, *Proc. 13th IEEE Symp. on Switching and Automata Theory* (1973) 125–129.

[MP68] M. L. MINSKY AND S. A. PAPERT, *Perceptrons.* MIT Press (Cambridge, MA, 1988). The first edition appeared in 1968.

[NOS93] A. NAIK, M. OGIWARA AND A. SELMAN, P-selective sets, and reducing search to decision vs. self-reducibility, *Proc. 8th STRUCTURES* (IEEE, 1993) 52–64.

[Ogi94] M. OGIHARA, Polynomial-time membership comparable sets, *Proc. 9th STRUCTURES* (IEEE, 1994) 2–11.

[OL93] M. OGIWARA AND A. LOZANO, On sparse hard sets for counting classes, *TCS* **112** (1993) 255–275.

[OW91] M. OGIWARA, O. WATANABE, On polynomial-time bounded truth-table reducibility of NP sets to sparse sets, *SIAM J. Comp.* **20** (1991) 471–483.

[Pap94] C. PAPADIMITRIOU, *Computational Complexity.* (Addison-Wesley, 1994).

[Pip79] N. PIPPENGER, On simultaneous resource bounds, *Proc. 20th FOCS* (1979) 307–311.

[RR92] D. RANJAN AND P. ROHATGI, Randomized reductions to sparse sets, *Proc. 7th STRUCTURES* (IEEE,1992) 239-242.

[Raz87] A. RAZBOROV, Lower bounds for the size of circuits of bounded depth with basis $\{\wedge, \oplus\}$, *Math. Notes Acad. Sci. USSR* **41(4)** (1987) 333–338.

[Schn76] C. SCHNORR, Optimal algorithms for self-transformable problems, *Proc. 3rd ICALP* (Edinburgh U. Press, 1976) 322–337.

[Sch83] U. SCHÖNING, A low and a high hierarchy within NP, *JCSS* **27** (1983) 14–28.

[Sch86] U. SCHÖNING, *Complexity and Structure.* (Springer, LNCS #211, 1986).

[Sch88] U. SCHÖNING, Graph isomorphism is in the low hierarchy. *JCSS* **37** (1988) 312–323.

[Sch89] U. Schöning, Probabilistic complexity classes and lowness. *JCSS* **39** (1989) 84–100.

[Sch95] U. Schöning, Perlen der Theoretischen Informatik. (BI-Wiss.-Verl., 1995).

[SL94] M. Sheu and T. Long, The extended low hierarchy is an infinite hierarchy, *SIAM J. Comp.* **23(3)** (1994) 488–509.

[Sel79] A. Selman, P-selective sets, tally languages, and the behavior of polynomial time reducibilities on NP, *MST* **13** (1979) 55–65.

[Sel82] A. Selman, Reductions on NP and p-selective sets, *TCS* **19** (1982) 287–304.

[Sel88] A. Selman, Promise problems complete for complexity classes, *Inf. and Comp.* **78** (1988) 87–98.

[Sel] A. Selman, A Taxonomy of Complexity Class of Functions. To appear in *JCSS*.

[Smo87] R. Smolensky, Algebraic methods in the theory of lower bounds for Boolean circuit complexity, *Proc. 19th STOC* (1987) 77–82.

[Si83] M. Sipser, A complexity theoretic approach to randomness. *Proc. 15th STOC* (1983) 330–335.

[St77] L. Stockmeyer, The polynomial-time hierarchy. *TCS* **3** (1977) 1–22.

[To91a] S. Toda, PP is as hard as the polynomial-time hierarchy, *SIAM J. Comp.* **20** (1991) 865–877.

[To91b] S. Toda, On polynomial-time truth-table reducibility of intractable sets to p-selective sets, *MST* **24** (1991) 69–82.

[TO92] S. Toda and M. Ogiwara, Counting classes are at least as hard as the polynomial-time hierarchy, *SIAM J. Comp.* **21** (1992) 316–328.

[TTW93] T. Thierauf, S. Toda, and O. Watanabe, On sets bounded truth-table reducible to p-selective sets, *Proc. 11th STACS* (Springer, LNCS # 775, 1994) 427–438.

[Tor88] J. Torán, *Structural Properties of the Counting Hierarchies,* Doctoral dissertation (UPC Barcelona, 1988).

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

[Ukk83] E. Ukkonen, Two results on polynomial time truth-table reductions to sparse sets, *SIAM J. Comp.* **12(3)** (1983) 580–587.

[VV86] L. Valiant and V. Vazirani, NP is as easy as detecting unique solutions, *TCS* **47** (1986) 85–93.

[Wag86] K.W. Wagner, The complexity of combinatorial problems with succinct input representation, *Acta Informatica* **23** (1986) 325–356.

[Wag90] K.W. Wagner, Bounded query classes, *SIAM J. Comp.* **19** (1990) 833–846.

[Wil85] C. Wilson, Relativized circuit complexity, *JCSS* **31(2)** (1985) 169–181.

[Yao90] A. Yao, On ACC and threshold circuits, *Proc. 31st FOCS* (1990) 619–627.

[Yap83] C. Yap, Some consequences of non-uniform conditions on uniform classes, *TCS* **26** (1983) 287–300.

[Yes83] Y. Yesha, On certain polynomial-time truth-table reducibilities of complete sets to sparse sets, *SIAM J. Comp.* **12(3)** (1983) 411–425.

[You90] P. Young, Juris Hartmanis: Fundamental contributions to the isomorphism problems. In A. Selman (Ed), *Complexity Theory Retrospective* (Springer, 1990) 28–58.

[Zac82] S. Zachos, Robustness of probabilistic computational complexity classes under definitional perturbations, *Inf. and Control* **54** (1982) 143–154.