Extension of Toda's Theorem to Middle Bit Classes

Johannes KÖBLER

Abteilung Theoretische Informatik
Universität Ulm
Oberer Eselsberg
89069 Ulm, Germany
koebler@informatik.uni-ulm.de

Abstract

In this paper we overview recent results concerning complexity classes that are defined in terms of the number of accepting paths of nondeterministic polynomial-time Turing machines. Of central interest are Toda's celebrated results showing the hardness of several counting classes for the polynomial-time hierarchy. Furthermore, we review the more recent progress that has been made in extending Toda's Theorem to middle bit classes, and we briefly describe how this work has been applied in circuit complexity to establish improved simulations of the class $\mathcal{ACC}$.

1 Introduction

The seminal results of Toda [Tod91] have sparked renewed interest in the complexity classes $\#\mathcal{P}$ (number-P [V79]), $\mathcal{PP}$ (probabilistic polynomial-time [G77]), and $\oplus\mathcal{P}$ (parity polynomial-time [PZ83, GP86]), as well as in Wagner's class $\mathcal{C}_=\mathcal{P}$ (exact counting; [W86]) and in the classes $\mathcal{M}od_k\mathcal{P}$ [CH90, H90, BG92]. Toda's Theorem is proved in two parts which are of independent interest. In the first part, using techniques introduced by Valiant and Vazirani [VV86] Toda shows that the polynomial-time hierarchy ($\mathcal{PH}$) is contained in $\mathcal{BPP}^{\oplus\mathcal{P}}$; and in the second part he proves that the evidently larger class $\mathcal{PP}^{\oplus\mathcal{P}}$ is contained in $\mathcal{P}^{\#\mathcal{P}}$. In other words, Toda's first result shows that any set in $\mathcal{PH}$ can be randomly reduced to $\oplus\mathcal{P}$, whereas the second result shows that $\oplus\mathcal{P}$ is low for $\mathcal{P}^{\#\mathcal{P}}$ (in symbols $\mathcal{P}^{\#\mathcal{P}^{\oplus\mathcal{P}}} = \mathcal{P}^{\#\mathcal{P}}$).

Obviously, the class $\oplus\mathcal{P}$ plays an important role in Toda's proof (though the proof can be easily extended to any of the other classes $\mathcal{M}od_k\mathcal{P}$, $k > 2$).

Intuitively speaking, a language A belongs to $\oplus\mathcal{P}$ if there is a $\#\mathcal{P}$ function f such that the membership question of a given x to A can be decided by knowing just the least significant bit of the binary representation of $f(x)$; for formal definitions see the next section. In other words, there is some polynomial-time nondeterministic Turing machine (NTM) N such that for every input x, the number $f(x)$ of accepting computations of N is congruent to $A(x)$ modulo 2, where $A(x)$ is the value of the characteristic function of A on x. Consequently, we speak of function f as a *$\oplus\mathcal{P}$-representation* for A.

Looking at Toda's proof of the second result (i.e., $\mathcal{PP}^{\oplus\mathcal{P}} \subseteq \mathcal{P}^{\#\mathcal{P}}$), one can easily observe that the full power of $\mathcal{P}^{\#\mathcal{P}}$ is not needed. Namely, the $\mathcal{P}^{\#\mathcal{P}}$ machine M in the proof asks only one query y to its oracle $f \in \#\mathcal{P}$, and furthermore the machine's decision depends on only one bit of the answer $f(y)$ in binary notation.

Motivated by this observation, the class $\mathcal{MP}$ (middle bit P; [GKRST]) was introduced as containing all languages that can be decided by knowing just one bit of the binary representation of a $\#\mathcal{P}$ function f. Indeed, for every language in $\mathcal{MP}$ it can be achieved that the number $f(x)$ of accepting computations of a suitable NTM N on any instance x has the following properties: its length when written in binary is odd, and further, the middle bit of $f(x)$ decides $x \in A$ (i.e., it coincides with the characteristic function of A on x). Henceforth, we call such an f an *$\mathcal{MP}$-representation* for A, and for every input x we call the computation (tree) of N on x an *$\mathcal{MP}$ computation* on x (with the convention that x is accepted by N iff the middle bit of $f(x)$ equals 1).

In other words, 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 $\mathcal{MP}$ (in symbols $\mathcal{MP}^{\oplus\mathcal{P}} = \mathcal{MP}$), i.e., a set A from $\oplus\mathcal{P}$ can not increase the power of $\mathcal{MP}$ computations when used as an oracle. The main ingredient for Toda's second result is a means of amplifying the modulus in the $\oplus\mathcal{P}$-representation of the oracle. Intuitively speaking, Toda showed that one can insert a polynomial number of 0's to the left of the important least significant bit. To be able to perform this process, Toda had to invent the so-called *modulus amplifying polynomials*.

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 $\mathcal{MP}^{\mathcal{A}mp\mathcal{MP}[O(1)]} = \mathcal{MP}$). As indicated below, the restriction of allowing only a constant number of oracle queries is essential. However, for many important subclasses of $\mathcal{A}mp\mathcal{MP}$ as, for example, $\mathcal{BPP}$, $\mathcal{PH}$, $\oplus\mathcal{P}$, and $\mathcal{BPP}^{\oplus\mathcal{P}}$, this restriction takes no effect since these subclasses are closed under Turing reductions.[1] 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 $\mathcal{P}^{\#\mathcal{P}}$ to the corresponding lowness result for $\mathcal{MP}$, it is not at all clear *à priori* whether such a transformation can also be transformed for the other $\mathcal{MOD}$ classes. As a matter of fact, 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 $\mathcal{MP}$. The key to this result is a means of converting representations involving counting modulo some prime p into middle bit representations in binary notation. More precisely speaking, by performing some carefully chosen arithmetic operations which do not lead outside of $\#\mathcal{P}$, the least significant digit of a number written in base p can be represented as a single bit in the middle of the resulting number in binary. By a preceding modulus amplification of the given base-p representation, this bit can be "isolated" by many 0's, which finally leads to the desired amplified $\mathcal{MP}$-representation.

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 ($\mathcal{CH}$) [W86] 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 surprising 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.

[1]All reducibilities considered in this paper are polynomial-time.

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; the only restriction being 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 $\mathcal{P}^{\#\mathcal{P}}$ 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 [A89], using algebraic methods introduced by Razborov [R87] and Smolensky [Sm87]. It states that any $\mathcal{AC}^0$ predicate (computable by a family of unbounded fan-in Boolean circuits of constant depth and polynomial size; [C85]) 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* ($2^{(\log n)^{O(1)}}$) 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 [Y90] then used these techniques to obtain the first non-trivial upper bound for $\mathcal{ACC}$ (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; [B89, 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 $\mathcal{P}^{\#\mathcal{P}[1]}$.

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 [Y90] 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 [Y90] 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.*

2 Preliminaries and Notation

The characteristic function of a set A is denoted by $A(x)$. The set $\{0, 1, 2, \ldots\}$ of non-negative integers is denoted by $\mathcal{N}$. We fix some standard means of injectively encoding sequences $(x_1, \ldots x_k)$ of strings, where $k > 0$ is arbitrary, by single strings $\langle x_1, \ldots, x_k \rangle$, such that both the encoding and decoding are computable in polynomial time. Where intent is clear we write $f(x_1, \ldots, x_k)$ or $A(x, y)$ in place of $f(\langle x_1, \ldots, x_k \rangle)$ or $A(\langle x, y \rangle)$.

We write $\mathcal{FP}$ for the class of deterministic polynomial-time computable functions. An oracle machine M may have a function f instead of a language as its oracle. M is *nonadaptive* if for every computation path leading up to some query z, the set of possible next queries does not depend on the answer $f(z)$. Otherwise M is *adaptive*. The class of languages (respectively, functions) computed by polynomial-time nonadaptive machines M with an oracle from some class $\mathcal{C}$ is denoted by $\mathcal{P}_{tt}^{\mathcal{C}}$ (respectively, $\mathcal{FP}_{tt}^{\mathcal{C}}$). For a relativizable language class $\mathcal{C}$, and a class $\mathcal{D}$ of either languages or functions, $\mathcal{C}_{tt}^{\mathcal{D}}$ is the class of all languages in $\mathcal{C}^{\mathcal{D}}$ witnessed by a nonadaptive machine of type $\mathcal{C}$. Further, $\mathcal{C}^{\mathcal{D}[k]}$ is the class of all languages in $\mathcal{C}^{\mathcal{D}}$ witnessed by a machine of type $\mathcal{C}$ which asks at most k queries on every computation path; these queries may be adaptive. The class $\mathcal{D}$ is *low* for $\mathcal{C}$ if the class $\mathcal{D}$, when used as an oracle for $\mathcal{C}$, does not increase the power of $\mathcal{C}$, that is, $\mathcal{C}^{\mathcal{D}} = \mathcal{C}$. Further information on these concepts may be found in [BDG, BC93, KST93, Pa94, Sc86].

Next, we recall the definitions for the counting classes $\#\mathcal{P}$, $\mathcal{PP}$, $\mathcal{C}_=\mathcal{P}$, $\mathcal{M}od_k\mathcal{P}$, $k \geq 2$, $\mathcal{M}od\mathcal{P}$, $\mathcal{MP}$, and $\mathcal{A}mp\mathcal{MP}$. To every NTM we associate the *counting function* $\#acc_N(x)$, defined to be the number of accepting computations which N has on input x. The class of such functions is denoted by $\#\mathcal{P}$. Let #SAT be the function that for any Boolean formula (encoded by some string) x gives the number of satisfying assignments for x. It is well-known that #SAT is complete for $\#\mathcal{P}$ in the sense that for every $f \in \#\mathcal{P}$ there exists a function $g \in \mathcal{FP}$ such that for all strings x, $f(x) = \#\mathrm{SAT}(g(x))$. Of course, $\#\mathcal{P}$ is not closed under subtraction; the closure of $\#\mathcal{P}$ under subtraction is the class $\mathcal{G}ap\mathcal{P}$ [FFK94].

Definition 2.1 *A language L belongs to the class $\mathcal{PP}$ if there is a function $f \in \#\mathcal{P}$ and a polynomial p such that for all x, $0 \leq f(x) < 2^{p(|x|)}$ and $x \in L$ iff $f(x) \geq 2^{p(|x|)-1}$.*

In other words, an instance x is in L iff there is a 1 at position $p(|x|)-1$ in the binary representation of $f(x)$ (provided that leading 0's are used to extend the binary representation of $f(x)$ to length $p(|x|)$, and that we follow the convention that the position of the least significant bit is zero). We call such a $\#\mathcal{P}$ function f a *$\mathcal{PP}$-representation* for L. From the fact that $\mathcal{PP}$ is closed under $O(\log n)$-Turing reductions [BRS91] it follows that a language belongs already to $\mathcal{PP}$ if it can be decided knowing all the $O(\log n)$ many most significant bits of some $\#\mathcal{P}$ function. A standard many-one complete set for $\mathcal{PP}$ is the language $\mathrm{MajSAT} = \{\langle x, i\rangle \mid \#\mathrm{SAT}(x) \geq i\}$.

Definition 2.2 *A language L belongs to the class $\mathcal{C}_=\mathcal{P}$ if there is a function $f \in \#\mathcal{P}$ and a polynomial p such that for all x, $0 \leq f(x) < 2^{p(|x|)}$ and $x \in L$ iff $f(x) = 2^{p(|x|)-1}$.*

It has been observed that w.l.o.g. one can assume that for all x, $f(x)$ is not larger than $2^{p(|x|)-1}$. Hence, $\mathcal{C}_=\mathcal{P}$ is a subclass of $\mathcal{PP}$, and as a further consequence, $\mathcal{C}_=\mathcal{P}$ is closed under (polynomially length bounded) universal quantification [GNW90, Tor91, BCO93, OH93, G93]. Ogiwara [O94] has shown that $\mathcal{C}_=\mathcal{P}$ is closed under positive Turing reductions. A standard many-one complete set for $\mathcal{C}_=\mathcal{P}$ is the language $\mathrm{ExactSAT} = \{\langle x, i\rangle \mid \#\mathrm{SAT}(x) = i\}$.

Definition 2.3 *A language L belongs to $\oplus\mathcal{P}$ if there is a function $f \in \#\mathcal{P}$ such that for all x, $x \in L$ iff $f(x)$ is odd.*

In other words, an instance x is in L iff there is a 1 at position 0 in the binary representation of $f(x)$. As shown in [BG92], a language belongs already to $\oplus\mathcal{P}$ if it can be decided knowing the $O(\log n)$ many least significant bits of some $\#\mathcal{P}$ function. The classes $\mathcal{M}od_k\mathcal{P}$, $k > 2$, are generalizations of the class $\oplus\mathcal{P} = \mathcal{M}od_2\mathcal{P}$.

Definition 2.4 *Let $k \geq 2$ be an integer. A language L belongs to $\mathcal{M}od_k\mathcal{P}$ if there is a function $f \in \#\mathcal{P}$ such that for all x, $x \in L$ iff $f(x) \not\equiv 0 \pmod{k}$.*

It is easy to see that if m divides k, then $\mathcal{M}od_m\mathcal{P}$ is a subclass of $\mathcal{M}od_k\mathcal{P}$. The class $\mathcal{M}od\mathcal{P}$ is a further generalization of the classes $\mathcal{M}od_p\mathcal{P}$, p prime.

Definition 2.5 *A set L belongs to $\mathcal{M}od\mathcal{P}$ if there exist a function $f \in \#\mathcal{P}$ and a function $g \in \mathcal{FP}$ such that for all strings x,*

- *$g(x) = 0^p$ for some prime p, and*
- *$x \in L \Leftrightarrow f(x) \not\equiv 0 \pmod{p}$.*

Let $p_1 = 2$, $p_2 = 3$, ... be the prime numbers in increasing order, that is, the i-th smallest prime number is denoted by p_i. Then the following language

$$\text{ModSAT} = \{\langle x, 0^i\rangle \mid \#\text{SAT}(x) \not\equiv 0 \pmod{p_i}\}$$

is many-one complete for $\mathcal{M}od\mathcal{P}$. Indeed, by the prime number theorem, we know that $p_i = O(i \log i)$. Hence, the value of the i-th prime p_i is polynomially bounded in i, and thus the unary encoding 0^{p_i} of p_i can be computed in polynomial time from 0^i and vice versa. It is an open problem whether besides the classes $\mathcal{M}od_p\mathcal{P}$, p prime, also the classes $\mathcal{M}od_k\mathcal{P}$, k composite, are contained in $\mathcal{M}od\mathcal{P}$.

Using the following fact which is a consequence of Kummer's theorem and which was applied in [BG92] to show that $\mathcal{M}od_{p^k}\mathcal{P} = \mathcal{M}od_p\mathcal{P}$ for every prime p and all $k \geq 2$, one can show [KT] that a language belongs already to $\mathcal{M}od\mathcal{P}$ if there is a $\mathcal{G}ap\mathcal{P}$ function g and an $\mathcal{FP}$ function f that produces for every string x a prime power $f(x) = 0^{p^e}$ in unary such that $x \in L$ iff $g(x) \equiv 0 \pmod{p^e}$.

Fact 2.6 [BG92] Let $n, e \in \mathcal{N}$, and let p be a prime. Then, $\binom{n}{p^e} \equiv 0 \pmod{p}$ if and only if the coefficient of p^e in the base-p expansion of n is 0.

Finally, we give the definitions of the two middle bit classes $\mathcal{MP}$ and $\mathcal{A}mp\mathcal{MP}$.

Definition 2.7 *A language L belongs to $\mathcal{MP}$ if there is a function $f \in \#\mathcal{P}$ and an $\mathcal{FP}$ function $g : \Sigma^* \to \mathcal{N}$ (called bit-selection function) such that for all x, $x \in L$ iff $\lfloor f(x)/2^{g(x)} \rfloor \equiv 1 \pmod{2}$.*

Put another way, $x \in L$ iff there is a 1 at position $g(x)$ in the binary representation of $f(x)$.

Definition 2.8 *A language L belongs to $\mathcal{A}mp\mathcal{MP}$ if there are a $\#\mathcal{P}$ function f and a function $g \in \mathcal{FP}$ such that for every $x \in \Sigma^*$ and every $d \geq 0$ there exist non-negative integers a and c such that $c < 2^{g(x,0^d)-d}$ and*

$$f(x, 0^d) = a2^{g(x,0^d)+d+1} + L(x)2^{g(x,0^d)} + c.$$

In other words, the binary representation of $f(x, 0^d)$ is of the form (for a suitable integer k, and writing g for $g(x, 0^d)$)

$$\underbrace{b_k \cdots b_{g+d+1}}_{a}\ \underbrace{b_{g+d} \cdots b_{g+1}}_{\text{all } 0'\text{s}}\ L(x)\ \underbrace{b_{g-1} \cdots b_{g-d}}_{\text{all } 0'\text{s}}\ \underbrace{b_{g-d-1} \cdots b_0}_{c}.$$

We call such a function f an $\mathcal{A}mp\mathcal{MP}$*-representation* for A.

$\mathcal{A}mp\mathcal{MP}$-representations of the following interesting special types exist for languages in $\oplus\mathcal{P}$ as well as for languages in $\mathcal{BPP}$ (cf. Section 4): Any $\oplus\mathcal{P}$ language can be represented in such a way that function g is constantly zero (i.e., integer c is always zero); whereas for languages in $\mathcal{BPP}$ there exist $\mathcal{A}mp\mathcal{MP}$-representations where the value of a is always zero.

3 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 was the first who constructed modulus-amplifying polynomials: Let $P_2(k) = 3k^4 + 4k^3$ and for $i > 1$, let $P_{2^i}(k) = P_2(P_{2^{i-1}}(k))$. For $2^{i-1} < d < 2^i$, take $P_d = P_{2^i}$. Then the modulus-amplification property can be easily proved by induction [Tod91]. In the next theorem we define very simple polynomials which exhibit nearly the same behavior as Toda's original polynomials.

Proposition 3.1 *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 $k \geq 0$,*

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

Proof. We 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

$$k^d \equiv 0 \pmod{m^d} \quad\Rightarrow\quad k^d + 1 \equiv 1 \pmod{m^d} \quad\Rightarrow\quad (k^d + 1)^d \equiv 1 \pmod{m^d},$$

and for $k \equiv -1 \pmod{m}$ it follows that

$$k^d \equiv -1 \pmod{m} \;\Rightarrow\; k^d + 1 \equiv 0 \pmod{m} \;\Rightarrow\; (k^d+1)^d \equiv 0 \pmod{m^d}.$$

This completes the proof. □

By using negative coefficients, modulus amplifying polynomials of smaller degree have been constructed. Toda's as well as the polynomials Q_d above have degree $\Theta(d^2)$. By starting the recursive definition with the polynomial $P_2'(k) = 3k^2 - 2k^3$ (instead of the Toda polynomial $P_2(k) = 3k^4 + 4k^3$), Yao [Y90] obtained modulus amplifying polynomials $P_d'(k)$ of degree $\Theta(d^{\log_2 3})$. The polynomials of Yao have been further improved by Beigel and Tarui [BT91] to polynomials of degree exactly $2d-1$ which is optimal:

$$P_d''(k) = 1 \;+\; (-1)^{d+1}\,(k-1)^d \sum_{j=0}^{d-1} \binom{d+j-1}{j} k^j.$$

As a main application, we consider the modulus amplification of $\mathcal{M}od_p\mathcal{P}$-representations for p prime [Tod91].

Theorem 3.2 *Let A be in $\mathcal{M}od_p\mathcal{P}$, p prime. Then there exists a function $f \in \#\mathcal{P}$ such that for all x, $A(x) \equiv f(x, 0^d) \pmod{p^d}$.*

Proof. By definition of $\mathcal{M}od_p\mathcal{P}$, there is a function $h \in \#\mathcal{P}$ such that for all x, $x \in L$ iff $h(x) \not\equiv 0 \pmod{p}$. Define the $\#\mathcal{P}$ function g as $g(x) = h(x)^{p-1} + p - 1$, and let $f(x, 0^d) = Q_d(g(x))$. Since p is prime, it follows by Fermat's Theorem and by Proposition 3.1 that for all $x \in L$,

$$h(x) \not\equiv 0 \pmod{p} \;\Rightarrow\; g(x) \equiv 0 \pmod{p} \;\Rightarrow\; f(x, 0^d) \equiv 1 \pmod{p^d},$$

and for all $x \notin L$,

$$h(x) \equiv 0 \pmod{p} \;\Rightarrow\; g(x) \equiv -1 \pmod{p} \;\Rightarrow\; f(x, 0^d) \equiv 0 \pmod{p^d}.$$

Thus, the proof is complete. □

The above statement can be easily extended to $\mathcal{M}od\mathcal{P}$ languages.

Theorem 3.3 [KT] *Let A be in $\mathcal{M}od\mathcal{P}$. Then there exist a function $f \in \#\mathcal{P}$ and a function $g \in \mathcal{FP}$ such that for all strings x, $g(x) = 0^i$ for some index i, and $A(x) \equiv f(x, 0^d) \pmod{p_i^d}$.*

4 Lowness of $\mathcal{MOD}$ and other classes for $\mathcal{MP}$

In this section we exploit certain properties of the subclass $\mathcal{A}mp\mathcal{MP}$ of $\mathcal{MP}$ that are very useful in obtaining lowness results for a variety of complexity classes including $\oplus\mathcal{P}$, $\mathcal{BPP}$, $\mathcal{PH}$, $\mathcal{M}od_k\mathcal{P}$, $k \geq 2$, and $\mathcal{M}od\mathcal{P}$. First we show that all these classes are contained in $\mathcal{A}mp\mathcal{MP}$.

Toda's proof of the containment $\mathcal{PP}^{\oplus\mathcal{P}} \subseteq \mathcal{P}^{\#\mathcal{P}}$ actually shows that languages L in $\oplus\mathcal{P}$ have $\oplus\mathcal{P}$-representations of a special kind. Namely, for every polynomial r, there is a $\#\mathcal{P}$ function f such that for all x, not only does the least significant bit of $f(x)$ equal 1 iff $x \in L$, but also the $r(|x|)$ bits to the *left* of this bit are always 0. This property is an immediate consequence of the ability to "amplify" the modulus in the $\oplus\mathcal{P}$-representation (cf. Theorem 3.2). Furthermore, looking at $\mathcal{PP}$-representations for languages in the subclass $\mathcal{BPP}$ of $\mathcal{PP}$, one can apply the well-known probability amplification technique to insert a polynomial number of 0's to the *right* of the deciding most significant bit. Moreover, by combining the amplification of $\oplus\mathcal{P}$-representations on the left of the decision bit with the amplification of $\mathcal{BPP}$-representations on the right of the decision bit, it is possible to get for every language L in $\mathcal{BPP}^{\oplus\mathcal{P}}$ an $\mathcal{MP}$-representation, in which any desired number m of 0's can be inserted on *both* the left and the right of the decision bit.

Hence, using Toda's result that $\mathcal{PH} \subseteq \mathcal{BPP}^{\oplus\mathcal{P}}$, the next corollary follows.

Proposition 4.1 [GKRST] *$\oplus\mathcal{P}$, $\mathcal{BPP}$, $\mathcal{PH}$, and $\mathcal{BPP}^{\oplus\mathcal{P}}$ are contained in $\mathcal{A}mp\mathcal{MP}$.*

The containment of the classes $\mathcal{M}od_p\mathcal{P}$, p prime, in $\mathcal{A}mp\mathcal{MP}$ was first shown in [GKRST], and was subsequently extended to the class $\mathcal{M}od\mathcal{P}$ in [KT]. The proof performs some arithmetic in order to transform an amplified $\mathcal{M}od_p\mathcal{P}$-representation into a binary $\mathcal{A}mp\mathcal{MP}$-representation.

Theorem 4.2 *$\mathcal{M}od\mathcal{P} \subseteq \mathcal{A}mp\mathcal{MP}$.*

Proof. Let A be a set in $\mathcal{M}od\mathcal{P}$. Using Theorem 3.3 we obtain a function $f \in \#\mathcal{P}$ and a function $g \in \mathcal{FP}$ such that for all strings x, $g(x) = 0^p$ for some prime p, and $A(x) \equiv f(x, 0^d) \pmod{p^{2d+2}}$. Let h be an $\mathcal{FP}$ function such that $h(x, 0^d) \equiv -p^{2d+2} \pmod{2^{d+1}}$ and $0 \leq h(x, 0^d) < 2^{d+1}$ (the prime p tacitly depends on x and d). Further, let q be a polynomial such that $f(x, 0^d) < 2^{q(|x|+d)-d-1}$. Now define the $\#\mathcal{P}$ function

$$f'(x, 0^d) = f(x, 0^d) \left\lceil 2^{q(|x|+d)}(1 + h(x, 0^d)/p^{2d+2}) \right\rceil .$$

Then it follows (for some integers a, a', some rational ε, $0 \leq \varepsilon < 1$, which, of course, depend on x and d; and writing f', f, q, and h for $f'(x, 0^d)$, $f(x, 0^d)$,

$q(|x|+d)$, and $h(x,0^d)$ respectively) that

$$\begin{aligned} f' &= f\left(2^q(1+h/p^{2d+2})+\varepsilon\right) \\ &= \left(a\cdot p^{2d+2}+A(x)\right)\left(2^q+2^q h/p^{2d+2}\right)+\varepsilon f \\ &= \left(p^{2d+2}+h\right)a\cdot 2^q+2^q A(x)+2^q A(x)h/p^{2d+2}+\varepsilon f \\ &= a'a\cdot 2^{q+d+1}+2^q A(x)+c, \end{aligned}$$

where $c = 2^q A(x)h/p^{2d+2}+\varepsilon f < 2^{q-d}$. Thus it follows that A is contained in $\mathcal{A}mp\mathcal{MP}$. □

Now we proceed to the lowness properties of the class $\mathcal{A}mp\mathcal{MP}$. As a first step we prove that $\mathcal{A}mp\mathcal{MP}$ is closed under bounded truth-table reductions.

Proposition 4.3 [GKRST] $\mathcal{P}^{\mathcal{A}mp\mathcal{MP}[O(1)]} \subseteq \mathcal{A}mp\mathcal{MP}$.

Proof. We first show that $\mathcal{A}mp\mathcal{MP}$ is closed under complement. Let L be in $\mathcal{A}mp\mathcal{MP}$, and let $f \in \#\mathcal{P}$ provide an $\mathcal{A}mp\mathcal{MP}$-representation for L, i.e., for every x, the binary representation of $f(x)$ is for suitable integers $k, l \geq 0$ of the form

$$a_k \cdots a_0 \underbrace{0\cdots 0}_{m \text{ times}} L(x) \underbrace{0\cdots 0}_{m \text{ times}} b_l \cdots b_0.$$

Consider the function $f'(x,0^m)$ whose value in binary is

$$a_k \cdots a_0 \underbrace{1\cdots 1}_{m \text{ times}} L(x) \underbrace{1\cdots 1}_{m \text{ times}} b_l \cdots b_0.$$

Since this equals $f(x,0^m)$ plus some powers of 2, f' is also in $\#\mathcal{P}$. Let N be an NTM and p' be a polynomial such that N on input x has exactly $2^{p'(|x|+m)}-1$ computation paths of which exactly $f'(x,0^m)$ many are accepting. Then, by interchanging accept and reject states in N, the function $f''(x,0^m) = 2^{p'(|x|+m)} - 1 - f'(x,0^m)$ is also in $\#\mathcal{P}$. In $f''(x,0^m)$, the complement of the bit $L(x)$ is flanked by m 0's.

Next we show that $\mathcal{A}mp\mathcal{MP}$ is closed under intersection. Let L_1, L_2 be two sets in $\mathcal{A}mp\mathcal{MP}$, with respective $\mathcal{A}mp\mathcal{MP}$-representations f_1 and f_2. Let $h(x,0^m)$ be an $\mathcal{FP}$ function that bounds the length of $f_1(x,0^m)$. Then $f_2(x,0^{h(x,0^m)})$ has the form

$$a_k \cdots a_0 \quad \underbrace{0\cdots 0}_{h(x,0^m) \text{ times}} \quad L_2(x) \quad \underbrace{0\cdots 0}_{h(x,0^m) \text{ times}} \quad b_l \cdots b_0.$$

The function $f_3(x,0^m) = f_1(x,0^m)\cdot f_2(x,0^{h(x,0^m)})$ also belongs to $\#\mathcal{P}$. Because of all the 0's around the bit $L_2(x)$, the value $L_2(x)\cdot f_1(x,0^m)$ appears as a substring of $f_3(x, 0^m)$, and in particular, the decision bit $L_1(x) \cdot L_2(x)$ for $L_1 \cap L_2$ is flanked by m 0's.

It follows that $\mathcal{A}mp\mathcal{MP}$ is closed under Boolean operations. Hence, closure under many-one reductions implies already closure under bounded truth-table reductions [KSW87]. Suppose A many-one reduces to $B \in \mathcal{A}mp\mathcal{MP}$. Let f provide an $\mathcal{A}mp\mathcal{MP}$-representation for B, and let t be the polynomial-time computable function used in the reduction from A to B, i.e., $B(t(x)) = A(x)$. Define the function $f'(x, 0^m) = f(t(x), 0^m)$. The value $f'(x, 0^m)$ has the form

$$a_k \cdots a_0 \underbrace{0 \cdots 0}_{m \text{ times}} B(t(x)) \underbrace{0 \cdots 0}_{m \text{ times}} b_l \cdots b_0,$$

and hence f' provides an $\mathcal{A}mp\mathcal{MP}$-representation for A. $\square$

By standard techniques, we get as a consequence of Proposition 4.3 the following partial lowness property of $\mathcal{A}mp\mathcal{MP}$ oracles for $\mathcal{MP}$.

Corollary 4.4 [GKRST] $\mathcal{MP}^{\mathcal{A}mp\mathcal{MP}[O(1)]} = \mathcal{MP}$.

The limitation of this corollary is that only a constant number of queries to the $\mathcal{A}mp\mathcal{MP}$ oracle are allowed. To apply it for unbounded Turing reductions, technical conditions on subclasses $\mathcal{C}$ of $\mathcal{A}mp\mathcal{MP}$ are needed under which a polynomial number of queries to $\mathcal{C}$ made by a nondeterministic machine can be replaced by a constant number.

Theorem 4.5 [GKRST] *Let $\mathcal{C}$ be a subclass of $\mathcal{A}mp\mathcal{MP}$ which is closed downward under both conjunctive and disjunctive reductions. Then $\mathcal{C}$ is low for $\mathcal{MP}$.*

Theorem 4.5 has the interesting consequence that the class $\mathcal{C}_=\mathcal{P}$ is probably too powerful to be contained in $\mathcal{A}mp\mathcal{MP}$.

Proposition 4.6 [GKRST] *If $\mathcal{C}_=\mathcal{P} \subseteq \mathcal{A}mp\mathcal{MP}$, then $\mathcal{CH} = \mathcal{MP}$.*

On the other hand, since $\mathcal{BPP}$ and $\oplus\mathcal{P}$ are closed under Turing reductions [K82, PZ83], it follows from Theorem 4.5 together with Proposition 4.1 that they are low for $\mathcal{MP}$.

Corollary 4.7 [GKRST]

i) *$\mathcal{BPP}^{\oplus\mathcal{P}}$ and $\mathcal{PH}$ are low for $\mathcal{MP}$.*

ii) *For any $k \geq 2$, $\mathcal{M}od_k\mathcal{P}$ is low for $\mathcal{MP}$.*

Proof. i) follows from Theorem 4.5. For ii), suppose first that k is prime. Then $\mathcal{M}od_k\mathcal{P}$ is closed under Turing reductions [BG92]. Hence by Theorems 4.2 and 4.5, $\mathcal{M}od_k\mathcal{P}$ is low for MP. Now suppose k is composite; then we can write $k = p^e k'$ where p is prime, $e \geq 1$, and $\gcd(p, k') = 1$. Further, by the representation theorem of Hertrampf [H90], $\mathcal{M}od_k\mathcal{P} \subseteq \mathcal{M}od_p\mathcal{P}^{\mathcal{M}od_{k'}\mathcal{P}}$. Since the lowness result for the prime case relativizes, the lowness of $\mathcal{M}od_k\mathcal{P}$ follows by iterating this argument for all the prime factors of k. $\square$

Let $\mathcal{M}od\mathcal{PH}$ be the closure of $\mathcal{P}$ under the operations $\mathcal{C} \mapsto \mathcal{NP}^{\mathcal{C}}$ and $\mathcal{C} \mapsto \mathcal{M}od_k\mathcal{P}^{\mathcal{C}}$ for $k \geq 2$. This is intuitively an extension of the polynomial hierarchy by the $\mathcal{M}od_k\mathcal{P}$ classes, and can be regarded as the polynomial-time analogue of the circuit class $\mathcal{ACC}$. Since all lowness results in this section relativize, the following corollary is immediate.

Corollary 4.8 [GKRST] *$\mathcal{M}od\mathcal{PH}$ is low for MP.*

We finally remark that all lowness results in this section also hold for the base class $\mathcal{A}mp\mathcal{MP}$ instead of $\mathcal{MP}$.

5 The power of $\mathcal{M}od\mathcal{P}$ and of $\mathcal{A}mp\mathcal{MP}$

In the preceding section we saw that except for $\mathcal{M}od\mathcal{P}$ and the class $\mathcal{A}mp\mathcal{MP}$ itself all considered subclasses of $\mathcal{A}mp\mathcal{MP}$ are low for $\mathcal{MP}$. In this section we will see that this is no accident. In fact, the following theorem states that every $\#\mathcal{P}$ function can be computed in polynomial time by asking one round of parallel queries to a $\mathcal{M}od\mathcal{P}$ oracle. This result indicates that $\mathcal{M}od\mathcal{P}$ seems to be a substantially more powerful counting class than its subclasses $\mathcal{M}od_p\mathcal{P}$, p prime.

Theorem 5.1 [KT] $\#\mathcal{P} \subseteq \mathcal{FP}_{tt}^{\mathcal{M}od\mathcal{P}}$.

Proof. Let $f(x)$ be a function in $\#\mathcal{P}$ bounded by $2^{q(|x|)}$ for some polynomial q. Consider the $\mathcal{M}od\mathcal{P}$ oracle $L = \{\langle x, 0^k, 0^i\rangle \mid f(x) \equiv k \pmod{p_i}\}$. Then, for $i = 1, \ldots, q(|x|)$, the remainders $r_i = f(x) \bmod p_i$ can be determined in polynomial time by asking oracle L in parallel the queries $\langle x, 0^k, 0^i\rangle$, for $i = 1, \ldots, q(|x|)$, and $k = 0, \ldots, p_i - 1$. Since by the Chinese remainder theorem, $f(x)$ can be easily computed from the r_i's, $f \in \mathcal{FP}_{tt}^{\mathcal{M}od\mathcal{P}}$ follows. $\square$

The following corollary is an immediate consequence of Theorem 4.2 and of Theorem 5.1.

Corollary 5.2 [GKRST, KT] $\mathcal{P}_{tt}^{\#\mathcal{P}} = \mathcal{P}_{tt}^{\mathcal{M}od\mathcal{P}} = \mathcal{P}_{tt}^{\mathcal{A}mp\mathcal{MP}} = \mathcal{P}_{tt}^{\mathcal{MP}} \subseteq \mathcal{P}^{\mathcal{PP}}$.

Fortnow and Reingold [FR91] proved that $\mathcal{PP}$ is closed downward under truth-table reductions, i.e., $\mathcal{P}_{tt}^{\mathcal{PP}} = \mathcal{PP}$. Since their result relativizes, the subclass $\mathcal{PP}^{\oplus\mathcal{P}}$ of $\mathcal{MP}$ is also closed downward under truth-table reductions. Hence if $\mathcal{MP} \subseteq \mathcal{PP}^{\oplus\mathcal{P}}$, then it follows that $\mathcal{P}_{tt}^{\#\mathcal{P}} = \mathcal{PP}^{\oplus\mathcal{P}}$.

The next corollary provides fairly strong evidence that the lowness result $\mathcal{MP}^{\mathcal{A}mp\mathcal{MP}[O(1)]} = \mathcal{MP}$ cannot be extended to the case of a polynomial number of nonadaptive queries.

Corollary 5.3 [KT] *If $\mathcal{MP}_{tt}^{\mathcal{A}mp\mathcal{MP}} = \mathcal{MP}$, then the counting hierarchy collapses to $\mathcal{MP}$.*

Proof. Suppose that $\mathcal{MP}_{tt}^{\mathcal{A}mp\mathcal{MP}} = \mathcal{MP}$. Then, since $\mathcal{MP}^{\mathcal{MP}} = \mathcal{MP}^{\#\mathcal{P}[1]} = \mathcal{MP}_{tt}^{\mathcal{A}mp\mathcal{MP}}$ by Corollary 5.2, it follows that $\mathcal{MP}^{\mathcal{MP}} = \mathcal{MP}$ implying that the counting hierarchy collapses to $\mathcal{MP}$. □

Since $\mathcal{A}mp\mathcal{MP}$ and $\mathcal{M}od\mathcal{P}$ are truth-table equivalent, Corollary 5.3 also holds for the class $\mathcal{M}od\mathcal{P}$ instead of $\mathcal{A}mp\mathcal{MP}$. Thus, the $\mathcal{MP}$-lowness of the classes $\mathcal{M}od_k\mathcal{P}$, $k \geq 2$, cannot be extended to the generalized $\mathcal{MOD}$-class $\mathcal{M}od\mathcal{P}$ unless the counting hierarchy collapses. A further consequence of Corollary 5.3 is that $\mathcal{A}mp\mathcal{MP}$ and $\mathcal{M}od\mathcal{P}$ are not closed under (unbounded) truth-table reductions unless $\mathcal{CH}$ collapses. As follows from the next theorem, $\mathcal{A}mp\mathcal{MP}$ and $\mathcal{M}od\mathcal{P}$ are probably not even closed under conjunctive reductions of a very strong form.

Theorem 5.4 [KT] *Every set A in $\mathcal{C}_=\mathcal{P}$ reduces via some conjunctive reduction $h \in \mathcal{FP}$ to some $\mathcal{M}od\mathcal{P}$ set B. Moreover, the reduction has the following property: for all strings x and every $m \geq 1$, $h(x, 0^m)$ computes a list $(y_1, \ldots, y_k)$ of queries such that*

$$\begin{array}{lclcl} x \in A & \Rightarrow & \#\{i \mid 1 \leq i \leq k,\, y_i \in B\} & = & k, \\ x \notin A & \Rightarrow & \#\{i \mid 1 \leq i \leq k,\, y_i \in B\} & \leq & k/m. \end{array}$$

Proof. Let $A = \{x \mid f(x) = 2^{q(|x|)-1}\}$ for a $\#\mathcal{P}$ function f and some polynomial q such that for all x, $f(x) < 2^{q(|x|)}$. Define the $\mathcal{M}od\mathcal{P}$ set $B = \{\langle x, 0^i\rangle \mid f(x) \equiv 2^{q(|x|)-1} \pmod{p_i}\}$ and let h be the function $h(x, 0^m) = (\langle x, 0\rangle, \ldots, \langle x, 0^{m\cdot q(|x|)}\rangle)$. By the Chinese remainder theorem,

$$f(x) \neq 2^{q(|x|)-1} \quad \Rightarrow \quad \|\{i \geq 1 \mid f(x) \equiv 2^{q(|x|)-1} \pmod{p_i}\}\| < q(|x|),$$

and hence the theorem follows. □

We close this section by remarking that the conjunctive closure of $\mathcal{A}mp\mathcal{MP}$ (as well as the classes $\forall\cdot\mathcal{A}mp\mathcal{MP}$, $\exists\cdot\mathcal{A}mp\mathcal{MP}$, and $\mathsf{C}\cdot\mathcal{A}mp\mathcal{MP}$) are contained in $\mathcal{MP}$.

References

[A89] E. Allender, A note on the power of threshold circuits. In *Proceedings of the 30th Symposium on Foundations of Computer Science*, (1989), 580-584.

[AHOW92] E. Allender, L. Hemachandra, M. Ogiwara, and O. Watanabe, Relating equivalence and reducibility to sparse sets. *SIAM Journal on Computing* **21(3)** (1992), 521-539.

[AH90] E. Allender, U. Hertrampf, On the power of uniform families of constant depth threshold circuits. In *Proceedings 15th Symposium on Mathematical Foundations Computer Science*, Springer-Verlag *Lecture Notes in Computer Science #452*, (1990), 158-164.

[AM79] L. Adleman and K. Manders, Reductions that lie. *Proceedings of the 20th Annual Conference on Foundations of Computer Science*, (IEEE Computer Society Press, 1979), 397-410.

[BDG] J.L. Balcázar, J. Díaz and J. Gabarró, *Structural Complexity I+II*, (Springer, 1988 and 1990).

[B89] D. Barrington, Bounded-width polynomial-size branching programs recognize exactly those languages in NC^1. *Journal of Computer and System Sciences* **38**, (1989), 150-164.

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

[B91] R. Beigel, Relativized counting classes: relations among thresholds, parity, and mods. *Journal of Computer and System Sciences* **42**, (1991), 76-96.

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

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

[BRS91] R. Beigel, N. Reingold and D. Spielman, PP is closed under intersection. In *Proceedings of the 23rd ACM Symposium on the Theory of Computation*, (1991), 1-11. A journal version is to appear in *Journal of Computer and System Sciences.*

[BT91] R. Beigel and J. Tarui, On ACC. In *Proceedings of the 32nd Symposium on Foundations of Computer Science*, (1991), 783-792.

[BTT92] R. Beigel, J. Tarui and S. Toda, On probabilistic ACC circuits with an exact-threshold output gate. In *Proceedings 3rd Symposium on Algorithms and Computation,* (1992), 420-429.

[BK88] R. Book and K. Ko, On sets truth-table reducible to sparse sets. *SIAM Journal on Computing*, **17(5)** (1988), 903-919.

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

[CH89] J. Cai and L. Hemachandra, Enumerative Counting is Hard. *Information and Computation* **92(1)**, (1989), 34-44.

[CH90] J. Cai and L. Hemachandra, On the power of parity. *Mathematical Systems Theory* **23**, (1990) 95-106.

[CKR91] R. Chang, J. Kadin, and P. Rohatgi, Connections between the complexity of unique satisfiability and the threshold behavior of randomized reductions. *Proceedings 6th Structure in Complexity Theory Conference*, 255-269, IEEE Computer Society Press, 1991.

[C85] S.A. Cook, A taxonomy of problems with fast parallel algorithms. *Information and Control* **64**, (1985), 2-22.

[FFK94] S.A. Fenner, L.J. Fortnow, S.A. Kurtz, Gap-definable counting classes. *Journal of Computer and System Sciences* **48**, (1994), 116-148.

[FR91] L. Fortnow and N. Reingold, PP is closed under truth-table reductions. In *Proceedings of the 6th Annual Conference on Structure in Complexity Theory*, (1991), 13-15.

[G77] J. Gill, Computational complexity of probabilistic Turing machines. *SIAM Journal on Computing* **6**, (1977), 675-695.

[GP86] L. Goldschlager, I. Parberry, On the construction of parallel computers from various bases of Boolean functions. *Theoretical Computer Science* **21**, (1986), 43-58.

[G93] F. Green, On the power of deterministic reductions to $\mathcal{C}_{=}\mathcal{P}$. *Mathematical Systems Theory* **26**, (1993), 215-233.

[GKRST] F. Green, J. Köbler, K. Regan, T. Schwentick and J. Torán, The power of the middle bit of a $\#\mathcal{P}$ function. To appear in *Journal of Computer and System Sciences.* Preliminary versions appeared in *Proceedings 7th Structure in Complexity Theory Conference,* p. 111-117, IEEE Computer Society, 1992, and in *Proceedings Fourth Italian Conference on Theoretical Computer Science,* p. 317-329, World Scientific, Singapur, 1992.

[GNW90] T. Gundermann, N. Nasser, and G. Wechsung, A survey on counting classes. In *Proceedings of the 5th Annual Conference on Structure in Complexity Theory,* (1990), 140-153.

[H90] U. Hertrampf, Relations among MOD-classes. *Theoretical Computer Science* **74**, (1990), 325-328.

[K82] K. Ko, Some observations on the probabilistic algorithms and NP-hard problems. *Information Processing Letters* **14**, (1982), 39-43.

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

[KSTT92] J. Köbler, U. Schöning, S. Toda, and J. Torán, Turing machines with few accepting computations and low sets for PP. *Journal of Computer and System Sciences* **44**, (1992), 272-286.

[KSW87] J. Köbler, U. Schöning, and K. W. Wagner, The difference and truth-table hierarchies of NP. *Theoretical Informatics and Applications* **21(4)**, (1987), 419-435.

[KT] J. Köbler and S. Toda, On the power of generalized MOD-classes. To appear in *Mathematical Systems Theory.* A preliminary version appears in *Proceedings of the 8th Structure in Complexity Theory Conference*, (1993), 147-155.

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

[MT89] P. McKenzie and D. Barrington, Automata theory meets circuit complexity. In *Proceedings of the 16th Annual International Colloquium on Automata, Languages and Programming.* Springer-Verlag *Lecture Notes in Computer Science #372*, (1989), 589-602.

[MP68] M. L. Minsky and S. A. Papert, *Perceptrons.* MIT Press, Cambridge, MA, 1988. Expanded Edition. The first edition appeared in 1968.

[O94] M. Ogiwara, Generalized theorems on relationships among reducibility notions to certain complexity classes. *Mathematical Systems Theory* **27**, (1994), 189-200.

[OH93] M. Ogiwara and L. Hemachandra, A complexity theory of feasible closure properties. *Journal of Computer and System Sciences* **46** (1993) 295-325.

[Pa94] C.H. Papadimitriou, *Computational Complexity.* Addison-Wesley, 1994.

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

[Pi79] N. Pippenger, On simultaneous resource bounds. In *Proceedings of the 20th Symposium on Foundations of Computer Science*, (1979), 307-311.

[R87] 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.

[Sa93] S. Saluja, Relativized limitations of the left set technique and closure classes of sparse sets. *Proceedings of the 8th Structure in Complexity Theory Conference*, 215-222, IEEE Computer Society Press, May 1993.

[Sc83] U. Schöning, A low and a high hierarchy within NP. *Journal of Computer and System Sciences* **27**, (1983), 14-28.

[Sc86] U. Schöning, *Complexity and Structure.* Springer-Verlag *Lecture Notes in Computer Science #211*, (1986).

[Sc93] U. Schöning, On random reductions from sparse sets to tally sets. *Information Processing Letters 46* (1993), 239-241.

[Si75] J. Simon, *On some central problems in computational complexity.* PhD thesis, Cornell University, Ithaca, New York, January 1975.

[Sm87] R. Smolensky, Algebraic methods in the theory of lower bounds for Boolean circuit complexity. In *Proceedings of the 19th ACM Symposium on the Theory of Computation*, (1987), 77-82.

[Ta93] J. Tarui, Probabilistic polynomials, AC^0 functions, and the polynomial time hierarchy. *Theoretical Computer Science* **113** (1993) 167-183.

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

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

[TW92] S. Toda and O. Watanabe, Polynomial time 1-Turing reducibility from #PH to #P. *Theoretical Computer Science* **100**, (1992), 205-221.

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

[V79] L.G. Valiant, The complexity of computing the permanent. *Theoretical Computer Science* **8**, (1979), 189-201.

[VV83] U. Vazirani and V. Vazirani, A natural encoding scheme proved probabilistic polynomial complete. *Theoretical Computer Science* **24**, (1983), 291-300.

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

[W86] K. Wagner, The complexity of combinatorial problems with succinct input representation. *Acta Informatica* **23**, (1986), 325-356.

[Y90] A. Yao, On ACC and threshold circuits. In *Proceedings of the 31st Symposium on Foundations of Computer Science*, (1990), 619-627.

[Z82] S. Zachos, Robustness of probabilistic computational complexity classes under definitional perturbations. *Information and Control* **54**, (1982), 143-154.