On the Power of Generalized MOD-Classes

Johannes Köbler* Seinosuke Toda†
Universität Ulm U. Electro-Comm.

Abstract

We investigate the computational power of the new counting class ModP which generalizes the classes $\mathrm{Mod}_p\mathrm{P}$, p prime. We show that ModP is polynomial-time truth-table equivalent in power to #P and that ModP is contained in the class AmpMP. As a consequence, the classes PP, ModP and AmpMP are all Turing equivalent, and thus AmpMP and ModP are not low for MP unless the counting hierarchy collapses to MP. Furthermore, we show that every set in $\mathsf{C}_=\mathrm{P}$ is reducible to some set in ModP via a random many-one reduction that uses only logarithmically many random bits. Hence, ModP and AmpMP are not closed under polynomial-time conjunctive reductions unless the counting hierarchy collapses.

1 Introduction

The study of counting classes has been a major research stream in structural complexity theory since Gill [Gi77] introduced the probabilistic class PP (for formal definitions see the next section). Simon [Sim75] characterized PP as a counting (more precisely, threshold) class, and Wagner [Wag86] generalized PP to the classes of the counting hierarchy CH by introducing the counting operator C. As a variant of the operator C, Wagner defined the exact counting operator $\mathsf{C}_=$, leading to the interesting class $\mathsf{C}_=\mathrm{P}$. Later on, Torán [Tor91] gave a characterization of the counting hierarchy in terms of an oracle hierarchy, and he observed that $\mathsf{C}_=\mathrm{P}$ is a subclass of $\mathsf{C}\mathrm{P} = \mathrm{PP}$.

Another important counting class is $\oplus\mathrm{P}$ introduced by Papadimitriou and Zachos[1] [PZ83] as a "moderate version of the counting idea". Membership in a $\oplus\mathrm{P}$ set is decided by the parity of the number of accepting paths of a polynomial-time

*Abteilung für Theoretische Informatik, Universität Ulm, Oberer Eselsberg, D-89069 Ulm, Germany; email address: koebler@informatik.uni-ulm.de

†Department of Computer Science and Information Mathematics, University of Electro-Communications, Chofu-shi, Tokyo 182, Japan. Work done in part while visiting Fakultät für Informatik, Universität Ulm; email address: toda@cs.uec.ac.jp

[1]The class $\oplus\mathrm{P}$ was independently defined in [GoPa86] where it is called EP.

nondeterministic machine. By considering arbitrary (but constant) moduli, $\oplus$P was subsequently generalized to the classes $\mathrm{Mod}_k\mathrm{P}$, $k \geq 2$, [CH89, Her90, BG92]. The class $\oplus$P plays a key role in Toda's recent result [Tod91] that the polynomial-time hierarchy PH is contained in P^{PP}, whose proof proceeds in two steps, namely $\mathrm{PH} \subseteq \mathrm{BPP}^{\oplus\mathrm{P}}$ and $\mathrm{PP}^{\oplus\mathrm{P}} \subseteq \mathrm{P}^{\mathrm{PP}}$.

By the definitions of $\mathrm{C_{=}P}$, PP, and $\mathrm{Mod}_k\mathrm{P}$, $k \geq 2$, it is clear that every set in these counting classes can be decided in polynomial time by asking one query to an oracle from Valiant's function class #P [Val79]. Moreover, in order to decide for a set A from PP or $\oplus$P whether a given input x belongs to A it suffices to know one single bit in the binary representation of $f_A(x)$ for a suitable #P function f_A. It follows from Toda's proof of the inclusion $\mathrm{PP}^{\oplus\mathrm{P}} \subseteq \mathrm{P}^{\mathrm{PP}}$ that this is even true for every set A in $\mathrm{PP}^{\oplus\mathrm{P}}$. The computational power provided by looking at a single bit of a #P function is exactly captured by the class MP introduced[2] by Green et al. [GKRST].

As mentioned above, $\oplus$P, PP, $\mathrm{PP}^{\oplus\mathrm{P}}$, and thus the polynomial-time hierarchy are subclasses of MP. Furthermore, it is proved in [GKRST] that also the classes $\mathrm{Mod}_k\mathrm{P}$, $k > 2$, are contained in MP, and that many subclasses of MP, as for example PH, $\mathrm{BPP}^{\oplus\mathrm{P}}$, and the classes $\mathrm{Mod}_k\mathrm{P}$, $k \geq 2$, are even low for MP. The key to the lowness of any oracle set A in these classes is provided by an "amplified" middle bit representation of A. That is, it can be accomplished that there are as many 0's as desired around the deciding bit. More specifically, there is a two-place #P function f_A such that $f_A(x, 0^m)$ has m 0's to the left and to the right of the bit that decides membership of x in A. The connection of this notion of amplification to lowness properties for MP was formalized in [GKRST] by showing that a constant number of queries to an AmpMP oracle does not increase the power of MP, where AmpMP is the class that contains exactly the languages in MP which allow such an amplified representation. Consequently, any subclass $\mathcal{C}$ of AmpMP which is closed under polynomial-time conjunctive and disjunctive reducibilities is low for MP and for AmpMP [GKRST].

The present work is motivated by the questions whether AmpMP itself is low for MP and whether the closure condition above is essential for $\mathcal{C}$ being low for MP. To answer these questions (under commonly believed complexity theoretic assumptions), we introduce the counting class ModP as a generalization of the classes $\mathrm{Mod}_p\mathrm{P}$, p prime. Instead of being a constant, the prime modulus p that is used to decide a ModP language can vary with the input. It is only assumed that the unary representation 0^p of p is computable in polynomial time. We show that ModP is as computationally powerful as #P by proving that any #P function can be computed in polynomial time by making one round of parallel queries to an oracle set from ModP. This result implies that ModP oracles are able to provide MP with the full power of polynomial-time counting, i.e. $\mathrm{MP}^{\mathrm{ModP}} = \mathrm{MP}^{\#\mathrm{P}}$. Hence, unlike the classes $\mathrm{Mod}_p\mathrm{P}$, their generalization ModP is not low for MP unless the

[2]The "M" in "MP" stands for "middle bit" since the bit that decides the membership in an MP set can always be shifted to the middle; see [GKRST].

counting hierarchy collapses to MP.

In the light of this result it is very surprising that the containment of $\mathrm{Mod}_k\mathrm{P}$ in AmpMP carries over to ModP. In fact, combining the two results, it follows that the polynomial-time truth-table closures of ModP, AmpMP and MP coincide. This coincidence reveals that access to an AmpMP oracle (even when restricted to nonadaptive queries) provides MP with the full oracle power of polynomial-time counting, i.e. $\mathrm{MP}_{\mathrm{tt}}^{\mathrm{AmpMP}} = \mathrm{MP}^{\#\mathrm{P}}$, and thus the lowness of AmpMP for MP would imply the collapse of the counting hierarchy. This contrasts to the partial lowness result [GKRST] mentioned above that a constant number of oracle queries to AmpMP does not suffice to increase the power of MP, i.e. $\mathrm{MP}^{\mathrm{AmpMP}[O(1)]} = \mathrm{MP}$.

The paper is organized as follows. In Section 2 we fix notation and give basic definitions. The results mentioned above are proved in Section 3. Finally, in Section 4 we investigate the question whether the classes ModP and AmpMP are closed under various reducibilities. We show that every set in $\mathrm{C_{=}P}$ is randomly many-one reducible to some set in ModP via a reduction that uses only logarithmically many random bits. Since the containment of $\mathrm{C_{=}P}$ in AmpMP implies the collapse of the counting hierarchy [GKRST], it follows that ModP and AmpMP are not closed under the random many-one reducibility (which lies in strength between the polynomial-time many-one and conjunctive reducibilities) unless CH collapses. Furthermore, we give natural characterizations of the polynomial-time conjunctive closure of ModP.

2 Preliminaries and notation

The languages considered here are over the alphabet $\Sigma = \{0,1\}$. The length of a string $x \in \Sigma^*$ is denoted by $|x|$. We will make use of a polynomial-time computable pairing function $\langle \cdot, \cdot \rangle : \Sigma^* \times \Sigma^* \to \Sigma^*$ that has inverses also computable in polynomial time. Such a pairing function can be extended in a standard way to encode arbitrary sequences $(x_1, \ldots, x_k)$ of strings into a string $\langle x_1, \ldots, x_k \rangle$. Where intent is clear we write $f(x_1, \ldots, x_k)$ in place of $f(\langle x_1, \ldots, x_k \rangle)$. For a set A, $\|A\|$ denotes its cardinality. The characteristic function of a set A is denoted by χ_A. The set of integers is denoted by $\mathcal{Z}$, and the set $\{0, 1, 2, \ldots\}$ of non-negative integers is denoted by $\mathcal{N}$. For integers k, m, where $m \geq 2$, we denote by $k \bmod m$ the uniquely determined integer $l \in \{0, 1, \ldots, m-1\}$ such that $l \equiv k \pmod{m}$. Further, unless otherwise specified, we denote the i-th smallest prime number by p_i that is, $p_1 = 2$, $p_2 = 3$, ... are the prime numbers in increasing order.

We assume that the reader is familiar with (nondeterministic, polynomial-time bounded, oracle) Turing machines and complexity classes (see [BDG 87, Schö86]). The class of functions computable by a deterministic polynomial-time Turing transducer is denoted by FP. The reducibilities discussed in this paper are the standard polynomial-time reducibilities defined by Ladner, Lynch, and Selman [LLS75], and the following randomized many-one reducibility.

Definition 2.1 (see [AM79, VV83, CKR91, Schö93]) A set A is co-rp many-one reducible to a set B ($A \leq_m^{co\text{-}rp} B$) if there exist a function $f \in \mathrm{FP}$ and a polynomial q such that for all strings x,

$$\begin{aligned} x \in A &\Rightarrow \mathrm{Prob}[f(x,w) \in B] = 1, \\ x \notin A &\Rightarrow \mathrm{Prob}[f(x,w) \in B] \leq 1/2. \end{aligned}$$

Here, the string w is chosen uniformly at random from the set $\Sigma^{q(|x|)}$.

Let $\leq_\alpha$ be any reducibility. Then the reduction class $\{A \mid \exists B \in \mathcal{C} : A \leq_\alpha B\}$ of all sets that are $\leq_\alpha$-reducible to some set in $\mathcal{C}$ is denoted by $\mathrm{P}_\alpha^{\mathcal{C}}$ [BK88, AHOW92]. Furthermore, let $\mathcal{D}$ be an oracle class and let $\mathcal{C}$ be a relativizable complexity class. Then the class of all sets (or functions) computable by a machine M of type $\mathcal{C}$ by asking on every computation path one round of parallel queries (at most k adaptive queries) to an oracle from $\mathcal{D}$ is denoted by $\mathcal{C}_{tt}^{\mathcal{D}}$ (respectively, $\mathcal{C}^{\mathcal{D}[k]}$).

For completeness, we briefly recall the definitions for the language classes $\mathrm{Mod}_k\mathrm{P}$, $k \geq 2$, MP, AmpMP, and for the function classes #P and GapP. #P was introduced by Valiant [Val79] and contains for every polynomial-time nondeterministic Turing machine M a function f that determines the number $f(x)$ of accepting paths of M on input x. The classes $\mathrm{Mod}_k\mathrm{P}$, $k \geq 2$, [CH89, Her90, BG92] are generalizations of the counting class $\oplus\mathrm{P}$ [PZ83] which equals $\mathrm{Mod}_2\mathrm{P}$. $\mathrm{Mod}_k\mathrm{P}$ contains for every function $f \in \#\mathrm{P}$ the language

$$\{x \in \Sigma^* \mid f(x) \not\equiv 0 \pmod{k}\}.$$

Recently, Green et al. [GKRST] introduced the class MP that contains for every function $f \in \#\mathrm{P}$ and every FP function $g : \Sigma^* \to \mathcal{N}$ (called bit-selection function) the language

$$\{x \in \Sigma^* \mid \lfloor f(x)/2^{g(x)} \rfloor \equiv 1 \pmod{2}\}.$$

That is, a string x is in the language if and only if there is a 1 at position $g(x)$ in the binary representation of $f(x)$. An important subclass of MP that plays a crucial role in the proofs that PH and the classes $\mathrm{Mod}_k\mathrm{P}$, $k \geq 2$, are low for MP is the class AmpMP. Intuitively, an MP language is in AmpMP if it can be achieved that there are many 0's around the deciding bit in the binary representation of the corresponding #P function value. Formally, a language L is in AmpMP [GKRST] if there are a function $g \in \mathrm{FP}$ and a #P function f such that for every $x \in \Sigma^*$ and every $m > 0$ there exist non-negative integers a and b such that $b < 2^{g(x,0^m)}$ and

$$f(x, 0^m) = a2^{g(x,0^m)+2m+1} + \chi_L(x)2^{g(x,0^m)+m} + b.$$

In other words, L is in AmpMP if there are functions $g, h \in \mathrm{FP}$ and a #P function f such that for every $x \in \Sigma^*$ and $m > 0$, there exist $b_1, \ldots, b_{g(x,0^m)}, a_1, \ldots, a_{h(x,0^m)} \in \{0,1\}$ such that the binary representation of $f(x, 0^m)$ is given by

$$a_{h(x,0^m)} \ldots a_1 \underbrace{0 \ldots 0}_{m \text{ times}} \chi_L(x) \underbrace{0 \ldots 0}_{m \text{ times}} b_{g(x,0^m)} \ldots b_1.$$

Fenner et al. [FFK91] generalized Valiant's class #P to the class GapP as follows. For a nondeterministic Turing machine M the function $gap_M : \Sigma^* \to \mathcal{Z}$ is defined as

$$gap_M(x) = acc_M(x) - acc_{\overline{M}}(x),$$

where $acc_M(x)$ is the number of accepting computations of $M(x)$, and $\overline{M}$ is the same Turing machine as M but with accepting and rejecting computations interchanged. Then GapP is the class of all functions gap_M where M is a polynomial-time nondeterministic Turing machine. GapP is the smallest function class that contains #P and is closed under subtraction [FFK91]. In addition, GapP inherits all important arithmetic closure properties of #P.

Lemma 2.2 [FFK91]

i) GapP is closed under addition and multiplication. Moreover, if g is a GapP function and q is a polynomial, then also the functions $f(x) = \sum_{y \in \Sigma^{q(|x|)}} g(x, y)$ and $h(x) = \prod_{i=1}^{q(|x|)} g(x, 1^i)$ are in GapP.

ii) If $f \in$ GapP and $k : \Sigma^* \to \mathcal{N}$ is an FP function whose value $k(x)$ is bounded by a polynomial in $|x|$, then the function $g(x) = \binom{f(x)}{k(x)}$ is in GapP.

3 Relations among ModP, #P, and AmpMP

In this section we show that every #P function can be computed in polynomial time by asking one round of parallel queries to an oracle from ModP. Further it turns out that ModP is a subclass of AmpMP. Hence, the polynomial-time truth-table closures of ModP, AmpMP and MP coincide, and thus the counting hierarchy would collapse to MP if AmpMP or ModP were low for MP. We start by formally introducing the class ModP which will play a crucial role in proving our results.

Definition 3.1 A set L is in ModP if there exist a function $f \in$ #P and a function $g \in$ FP such that for all strings x,

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

In the next proposition we list some basic properties of the class ModP.

Proposition 3.2

i) $\mathrm{Mod}_p\mathrm{P} \subseteq$ ModP for all primes p.

ii) ModP is closed under complementation.

iii) ModP has complete sets under $\leq_m^p$, and is closed under join and under one truth-table reducibility.

Proof.

i) Obvious.

ii) The proof is analogous to the one given in [BG92] that the classes $\mathrm{Mod}_p\mathrm{P}$, p prime, are closed under complementation. Let A be in ModP, that is, $A = \{x \mid f(x) \not\equiv 0 \pmod{|g(x)|}\}$ for functions $f \in \#\mathrm{P}$ and $g \in \mathrm{FP}$, where for every string x, $g(x)$ evaluates to the unary representation of some prime. Define the #P function h as $h(x) = f(x)^{|g(x)|-1}$. By Fermat's Theorem, since $|g(x)|$ is prime, it holds for all $x \in \Sigma^*$,

$$\begin{aligned} f(x) \equiv 0 \pmod{|g(x)|} &\;\Rightarrow\; h(x) \equiv 0 \pmod{|g(x)|}, \\ f(x) \not\equiv 0 \pmod{|g(x)|} &\;\Rightarrow\; h(x) \equiv 1 \pmod{|g(x)|}. \end{aligned}$$

Thus, letting $\hat{h}(x) = h(x) + (|g(x)| - 1)$, it follows that $\overline{A} \in \mathrm{ModP}$.

iii) Let #SAT [Val79] be the well-known #P complete function that for any Boolean formula (encoded by the string) x determines the number $\#\mathrm{SAT}(x)$ of satisfying assignments for x. As an example of a many-one complete set in ModP we define the language

$$\mathrm{ModSAT} = \{\langle x, 0^k, 0^i \rangle \mid \#\mathrm{SAT}(x) \equiv k \pmod{p_i}\}.$$

Observe that by the prime number theorem, $p_i = O(i \log i)$. 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.

Using part (*ii*), it is straightforward to show that ModP is closed under join and $\leq_{1\text{-}tt}^p$. □

It is an open problem whether also the classes $\mathrm{Mod}_k\mathrm{P}$, k composite, are contained in ModP. This would follow if ModP were closed under the polynomial-time bounded truth-table reducibility. By the proof of parts *ii*) and *iii*) of the previous proposition, ModP can be characterized as the class of all languages A such that $\chi_A(x)$ can be represented as the remainder $f(x) \bmod p_{i(x)}$ for some #P function f and a polynomially bounded function $i \in \mathrm{FP}$. We will make use of this characterization for ModP later on.

In the following theorem we prove that every #P function can be computed in polynomial time by asking one round of parallel queries to a ModP oracle set. This result indicates that ModP seems to be substantially stronger than its subclasses $\mathrm{Mod}_p\mathrm{P}$, p prime.

Theorem 3.3 $\#\mathrm{P} \subseteq \mathrm{FP}_{tt}^{\mathrm{ModP}}$.

Proof. Let f be a function in #P and let q be a polynomial such that for all strings x, $f(x) \leq 2^{q(|x|)}$. Then, all the remainders

$$r_i = f(x) \bmod p_i, \quad \text{for} \quad i = 1, \ldots, q(|x|)$$

can be determined in polynomial time relative to the ModP oracle

$$L = \{\langle x, 0^k, 0^i \rangle \mid f(x) \equiv k \pmod{p_i}\}$$

by asking 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 sequence r_i, $i = 1, \ldots, q(|x|)$, it follows that $f \in \mathrm{FP}_{tt}^{\mathrm{ModP}}$. $\square$

Next we show that ModP is a subclass of AmpMP. The proof is similar to the one given in [GKRST] showing the inclusion of the classes $\mathrm{Mod}_p\mathrm{P}$, p prime, in AmpMP. We need the following lemma which is implicit in [GKRST] and shows how an amplified $\mathrm{Mod}_p\mathrm{P}$ representation can be transformed into a binary AmpMP representation.

Lemma 3.4 Let $h, m, p, r, s \in \mathcal{N}$ be given such that for some $a \in \mathcal{N}$ and $b \in \{0, 1\}$,

$$h = ap^r + b \leq 2^s \quad \text{and} \quad p^r \geq 2^{2m+2}.$$

Then, for $t = s + 2m + 2$, $k = -p^r \bmod 2^{m+1}$, and $g = 2^m h \left(2^t + k \left\lceil \frac{2^t}{p^r} \right\rceil\right)$, there are $a', c \in \mathcal{N}$ such that

$$g = a' 2^{t+2m+1} + b 2^{t+m} + c \quad \text{and} \quad c < 2^t.$$

Proof. Let $\left\lceil \frac{2^t}{p^r} \right\rceil = 2^t/p^r + \varepsilon$ for some $0 \leq \varepsilon < 1$. Then

$$\begin{aligned} g &= (2^m a p^r + 2^m b)(2^t + k 2^t/p^r + k\varepsilon) \\ &= (p^r + k) a 2^{t+m} + b 2^{t+m} + 2^m b k 2^t/p^r + 2^m h k \varepsilon \end{aligned}$$

where $p^r + k \equiv 0 \pmod{2^{m+1}}$, $2^m bk 2^t/p^r < 2^{t-1}$, and $2^m hk\varepsilon < 2^{s+2m+1} = 2^{t-1}$. $\square$

Theorem 3.5 ModP $\subseteq$ AmpMP.

Proof. Let A be a set in ModP. Then the characteristic function of A can be represented as $\chi_A(x) = f(x) \bmod p_{i(x)}$ for a function $f \in$ #P and a polynomially bounded function $i \in$ FP. The following claim shows that the representation of χ_A can be "amplified by powering the modulus". The "modulus amplifying polynomials" were developed by Toda [Tod91] to prove the inclusion of $\mathrm{PP}^{\oplus\mathrm{P}}$ in P^{PP} and their degree was subsequently minimized by [Yao90, BT91]. The proof of the next claim is inspired by [BT91].

Claim 1 There is a function h in #P such that for all $m \geq 1$ and all strings x,

$$h(x, 0^m) \equiv \chi_A(x) \pmod{(p_{i(x)})^m}.$$

Proof of Claim 1. For any integer $m \geq 1$, let q_m be the polynomial

$$q_m(z) \;=\; (z-1) \cdot \sum_{i=0}^{m-1} z^i,$$

and define the functions $\hat{f}(x, 0^m) = f(x)^m (p_{i(x)} - 1)$ and $\hat{h}(x, 0^m) = q_m(\hat{f}(x, 0^m) + 1)$. It is easy to see that $\hat{h}$ is in #P. Furthermore, since $q_m(z) = z^m - 1$, we have

$$\begin{array}{lllll} x \in A & \Rightarrow & \hat{f}(x,0^m) \equiv -1 \pmod{p_{i(x)}} & \Rightarrow & \hat{h}(x,0^m) \equiv -1 \pmod{(p_{i(x)})^m}, \\ x \notin A & \Rightarrow & \hat{f}(x,0^m) \equiv 0 \pmod{(p_{i(x)})^m} & \Rightarrow & \hat{h}(x,0^m) \equiv 0 \pmod{(p_{i(x)})^m}. \end{array}$$

Thus the claim follows by letting $h(x, 0^m) = ((p_{i(x)})^m - 1)\hat{h}(x, 0^m)$.

$\square$ *Proof of Claim 1.*

To complete the proof of the theorem, let $r(x,m) = \lceil \frac{2m+2}{\log_2 p_{i(x)}} \rceil$ and let $s(x, 0^m) \in$ FP be a polynomially bounded function such that $h(x, 0^{r(x,m)}) \leq 2^{s(x,0^m)}$. Then we can apply Lemma 3.4 (with $h = h(x, 0^{r(x,m)})$, $p = p_{i(x)}$, $r = r(x,m)$, and $s = s(x, 0^m)$) to get a #P function

$$g(x,0^m) = 2^m h(x, 0^{r(x,m)}) \left(2^{t(x,0^m)} + k(x,0^m) \left\lceil \frac{2^{t(x,0^m)}}{(p_{i(x)})^{r(x,m)}} \right\rceil \right),$$

where $t(x,0^m) = s(x,0^m) + 2m + 2$ and $k(x, 0^m) = -(p_{i(x)})^{r(x,m)} \bmod 2^{m+1}$. Since the bit at position $t(x, 0^m) + m$ in the binary representation of $g(x, 0^m)$ decides the membership of x in A, and since this bit is flanked by at least m 0's to the left and to the right, it follows that A is contained in AmpMP. $\square$

As an immediate consequence of Theorems 3.3 and 3.5 we obtain the following corollary.

Corollary 3.6

i) $\mathrm{P}^{\#\mathrm{P}}_{\mathrm{tt}} = \mathrm{P}^{\mathrm{ModP}}_{\mathrm{tt}} = \mathrm{P}^{\mathrm{AmpMP}}_{\mathrm{tt}} = \mathrm{P}^{\mathrm{MP}}_{\mathrm{tt}}$.

ii) $\mathrm{P}^{\#\mathrm{P}} = \mathrm{P}^{\mathrm{ModP}} = \mathrm{P}^{\mathrm{AmpMP}} = \mathrm{P}^{\mathrm{MP}} = \mathrm{P}^{\mathrm{PP}}$.

It was shown in [GKRST] that $\mathrm{MP}^{\mathrm{AmpMP}[k]} = \mathrm{MP}$ for every constant k, that is, an oracle set A from AmpMP does not provide MP with any additional power if the number of oracle queries on every computation path is bounded by a constant. This lowness result cannot be extended to the case of a polynomial number of (nonadaptive) queries unless the counting hierarchy collapses.

Corollary 3.7 AmpMP is low for MP if and only if the counting hierarchy collapses to MP.

Proof. Since $\mathrm{MP}^{\mathrm{MP}} = \mathrm{MP}^{\#\mathrm{P}[1]}$, and since we have $\mathrm{MP}^{\#\mathrm{P}[1]} = \mathrm{MP}_{tt}^{\mathrm{AmpMP}}$ from Corollary 3.6, it follows that if AmpMP is low for MP, then $\mathrm{MP}^{\mathrm{MP}} = \mathrm{MP}$ implying that the counting hierarchy collapses to MP. On the other hand, since $\mathrm{MP}^{\mathrm{AmpMP}} \subseteq$ CH, if CH = MP then AmpMP is low for MP. $\square$

Since AmpMP and ModP are Turing equivalent, Corollary 3.7 also holds for the class ModP instead of AmpMP. Thus, the MP-lowness of the classes $\mathrm{Mod}_k\mathrm{P}$, $k \geq 2$, cannot be extended to the generalized MOD-class ModP unless the counting hierarchy collapses. A further consequence of (the proof of) Corollary 3.7 is that AmpMP is not closed under bounded truth-table reductions unless CH collapses. We further investigate the closure properties of ModP and AmpMP in the next section.

4 Extensions of ModP

In this section, we investigate the closure of ModP under various reducibilities. We first show that $\mathrm{C}_=\mathrm{P}$ is contained in the closure of ModP under the polynomial-time conjunctive reducibility. In fact, every set in $\mathrm{C}_=\mathrm{P}$ is even co-rp many-one reducible to some ModP set via a reduction function that uses only logarithmically many random bits. Moreover, the error probability of the reduction can be made polynomially small, i.e. less than $1/p(|x|)$ for an arbitrary polynomial p. Once more, we make use of the Chinese remainder theorem (see also [Sal93, Schö93]).

Theorem 4.1 There is a function $h \in \mathrm{FP}$ such that for every set A in $\mathrm{C}_=\mathrm{P}$ there is a ModP set B such that for every polynomial p and all strings x,

$$\begin{aligned} x \in A &\Rightarrow \mathrm{Prob}[h(x,w) \in B] = 1, \\ x \notin A &\Rightarrow \mathrm{Prob}[h(x,w) \in B] \leq 1/p(|x|), \end{aligned}$$

where the string w is chosen uniformly at random from $\Sigma^{O(\log |x|)}$.

Proof. Let $A = \{x \mid f(x) = g(x)\}$ for a #P function f and an FP function $g : \Sigma^* \to \mathcal{N}$. Define h to be the function $h(x,w) = \langle x, 0^{i+1}\rangle$, where i is the integer in $\{0, 1, \ldots, 2^{|w|} - 1\}$ which has the binary representation given by w, and define the set

$$B = \{\langle x, 0^i\rangle \mid f(x) \equiv g(x) \pmod{p_i}\}$$

which is easily seen to be in ModP. Let r be a polynomial such that $f(x), g(x) < 2^{r(|x|)}$ for all strings x, and let $l(n) \in O(\log n)$ be a function such that $r(n) \cdot p(n) \leq 2^{l(n)}$. By the Chinese remainder theorem, it holds that

$$f(x) \neq g(x) \Rightarrow \|\{i \geq 1 \mid f(x) \equiv g(x) \pmod{p_i}\}\| < r(|x|).$$

Now it follows that

$$\begin{aligned} x \in A &\Rightarrow \mathrm{Prob}[h(x,w) \in B] = 1, \\ x \notin A &\Rightarrow \mathrm{Prob}[h(x,w) \in B] < 1/p(|x|), \end{aligned}$$

provided that the string w is chosen uniformly at random from the set $\Sigma^{l(|x|)}$. □

A co-rp many-one reduction that uses only logarithmically many random bits is obviously a special kind of conjunctive reduction, and therefore we have the following corollary.

Corollary 4.2 $\mathrm{C_{=}P} \subseteq \mathrm{P}^{\mathrm{ModP}}_{\mathrm{ctt}}$.

Since the inclusion $\mathrm{C_{=}P} \subseteq$ AmpMP implies the collapse of the counting hierarchy to MP [GKRST], we can state the following corollaries.

Corollary 4.3 If the closure of ModP under co-rp many-one reductions that use logarithmically many random bits is contained in AmpMP, then the counting hierarchy collapses to MP.

Corollary 4.4 If either ModP or AmpMP is closed under conjunctive (or disjunctive) reductions, then the counting hierarchy collapses to MP.

Proof. Since closure under conjunctive reductions implies closure under co-rp many-one reductions that use logarithmically many random bits, the part regarding conjunctive reductions follows immediately from Corollary 4.3. Furthermore, since ModP (as shown in part *ii*) of Proposition 3.2) and AmpMP (as shown in [GKRST]) are closed under complementation, each of these two classes is closed under conjunctive reductions if and only if it is closed under disjunctive reductions. □

By Corollary 4.3, the question of whether the polynomial-time conjunctive closure of ModP is contained in AmpMP is closely related to the structure of the counting hierarchy. This motivates us to further investigate that closure and to give natural characterizations for it. As a first step, we show that the class ModP remains unchanged if we use polynomially bounded prime powers as moduli. For the proof we need the following fact which is a consequence of Kummer's theorem and which was used in [BG92] to show that $\mathrm{Mod}_{p^k}\mathrm{P} = \mathrm{Mod}_p\mathrm{P}$ for every prime p and all $k \geq 2$.

Fact 4.5 [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.

Theorem 4.6 If g is a GapP function and f is an FP function that produces for every string x a prime power $f(x) = 0^{p^e}$ in unary representation, then the set $B = \{x \mid g(x) \equiv 0 \pmod{|f(x)|}\}$ is in ModP.

Proof. Let $g \in$ GapP and $f \in$ FP as stated in the theorem, and let $i(x), e(x)$ be FP functions such that $|f(x)| = (p_{i(x)})^{e(x)}$. Without limitation of generality we can assume that $g(x)$ is non-negative for all $x \in \Sigma^*$. (This can be achieved for example by adding to $g(x)$ the FP function $|f(x)|^{q(|x|)}$ for a large enough polynomial q.) Define the function

$$\hat{g}(x) \quad = \quad \prod_{j=0}^{e(x)-1} \left(1 - \binom{g(x)}{(p_{i(x)})^j}^{p_{i(x)}-1}\right).$$

By Proposition 2.2, $\hat{g}$ is in GapP, and by Fact 4.5, it follows that for all x,

$$\begin{aligned}
x \in B \quad &\Leftrightarrow \quad g(x) \equiv 0 \pmod{(p_{i(x)})^{e(x)}} \\
&\Leftrightarrow \quad \text{for } j = 0, \ldots, e(x) - 1 : \text{the coefficient of } (p_{i(x)})^j \text{ in the base-}p_{i(x)} \\
&\qquad\quad \text{expansion of } g(x) \text{ is } 0 \\
&\Leftrightarrow \quad \text{for } j = 0, \ldots, e(x) - 1 : \binom{g(x)}{(p_{i(x)})^j} \equiv 0 \pmod{p_{i(x)}} \\
&\Leftrightarrow \quad \hat{g}(x) \not\equiv 0 \pmod{p_{i(x)}}
\end{aligned}$$

This shows that $B \in$ ModP, since $\hat{g}(x) = h(x) - 2^{q(|x|)}$ for a #P function h and a polynomial $q > 0$, implying that $\hat{g}(x) \equiv \hat{h}(x) \pmod{p_{i(x)}}$, where $\hat{h}(x) = \hat{g}(x) + (p_{i(x)})^{q(|x|)} = h(x) + ((p_{i(x)})^{q(|x|)} - 2^{q(|x|)})$ is a function in #P. □

If we remove in the above theorem the condition that f produces a prime power, then B is conjunctive reducible to a ModP set (via a reduction that asks only $O(\log n)$ queries).

Corollary 4.7 For every GapP function g and FP function f, the set $B = \{x \mid g(x) \equiv 0 \pmod{|f(x)|}\}$ is in $\mathrm{P}_{\mathrm{ctt}}^{\mathrm{ModP}}$.

Proof. Let $g \in$ GapP and $f \in$ FP. For a string x, let $I(x) = \{i \mid p_i \text{ divides } |f(x)|\}$ be the index set of all prime factors of $|f(x)|$. Note that $|I(x)| = O(\log |x|)$. Further, let $e_i(x)$ be the exponent of p_i in the prime factorization of $|f(x)|$, i.e. $|f(x)| = \prod_{i \in I(x)} p_i^{e_i(x)}$. Then,

$$\begin{aligned}
x \in B \quad &\Leftrightarrow \quad \text{for all } i \in I(x) : g(x) \equiv 0 \pmod{p_i^{e_i(x)}} \\
&\Leftrightarrow \quad \text{for all } i \in I(x) : \langle x, 0^{p_i^{e_i(x)}} \rangle \in B',
\end{aligned}$$

where

$$B' = \{\langle x, 0^m \rangle \mid \exists i, e : m = p_i^e \text{ and } g(x) \equiv 0 \pmod{m}\}.$$

By Theorem 4.6, B' is in ModP, and thus it follows that $A \in \mathrm{P}_{\mathrm{ctt}}^{\mathrm{ModP}}$. □

Theorem 4.8 The following are equivalent.

i) A is in $\mathrm{P}_{\mathrm{ctt}}^{\mathrm{ModP}}$.

ii) There exist a #P function f and a polynomial q such that for all strings x,

$$x \in A \quad \Leftrightarrow \quad \text{for all } k = 1, \ldots, q(|x|) : f(x) \equiv 0 \pmod{p_k}.$$

iii) There exist functions $g \in \mathrm{GapP}$ and $h \in \mathrm{FP}$ such that for all strings x, $h(x)$ produces a list $\langle 0^{m_1}, \ldots, 0^{m_k} \rangle$ of positive integers (not necessarily primes) in unary representation, and

$$x \in A \quad \Leftrightarrow \quad \text{for all } j = 1, \ldots, k : g(x, j) \equiv 0 \pmod{m_j}.$$

Proof. $i) \rightarrow ii)$: Let h be a conjunctive reduction function of A to a set B in ModP, that is, for all strings x, $h(x)$ produces a list $\langle y_1, \cdots, y_m \rangle$ of strings such that

$$x \in A \quad \Leftrightarrow \quad \text{for all } k = 1, \ldots, m : y_k \in B.$$

Let $f \in \#\mathrm{P}$, $i \in \mathrm{FP}$ be functions witnessing that $B \in \mathrm{ModP}$, i.e., $\forall y : \chi_B(y) = f(y) \bmod p_{i(y)}$. For a string x, let $I(x) = \{i(y_1), \cdots, i(y_m)\}$ be the index set of primes corresponding to the queries in the list $h(x) = \langle y_1, \cdots, y_m \rangle$, and for every $k \geq 1$, let $Y_k(x) = \{y_j \mid i(y_j) = k\}$ be the set of queries in $h(x)$ that are decided using the modulus p_k. Then there is a polynomial q such that for all x, $I(x) \subseteq \{1, \ldots, q(|x|)\}$, and thus

$$\begin{aligned}
x \in A \quad &\Leftrightarrow \quad \text{for all } j = 1, \ldots, m : f(y_j) \equiv 1 \pmod{p_{i(y_j)}} \\
&\Leftrightarrow \quad \forall k \in I(x) : \prod_{y \in Y_k(x)} f(y) \equiv 1 \pmod{p_k} \\
&\Leftrightarrow \quad \forall k \in I(x) : (p_k - 1) + \prod_{y \in Y_k(x)} f(y) \equiv 0 \pmod{p_k} \\
&\Leftrightarrow \quad \forall k = 1, \ldots, q(|x|) : \hat{f}(x) \equiv 0 \pmod{p_k},
\end{aligned}$$

where

$$\hat{f}(x) \quad = \quad \sum_{i \in I(x)} \left(\prod_{j \in \{1, \ldots, q(|x|)\} - \{i\}} p_j \right) \left((p_i - 1) + \prod_{y \in Y_i(x)} f(y) \right)$$

is in #P.

The implication $ii) \rightarrow iii)$ is obvious, and the implication $iii) \rightarrow i)$ follows from Corollary 4.7. □

As a last remark we note that the conjunctive closure of AmpMP (as well as the classes $\forall \cdot \mathrm{AmpMP}$, $\exists \cdot \mathrm{AmpMP}$, and $\mathsf{C} \cdot \mathrm{AmpMP}$) are easily seen to be contained in $\mathrm{MP}^{\mathrm{AmpMP}[1]} = \mathrm{MP}$.

Acknowledgment

The second author is very grateful to Uwe Schöning for giving him an opportunity to visit Universität Ulm and for making this collaboration possible.

References

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

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

[BDG 87] J.L. Balcázar, J. Díaz and J. Gabarró. *Structural Complexity I*, Springer, 1987.

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

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

[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,* 420-429, 1992.

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

[CH89] J. Cai, L.A. Hemachandra. On the power of parity. In *Proceedings 6th Symposium on Theoretical Aspects of Computer Science, Lecture Notes in Computer Science 349*, 229-240, 1989.

[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.

[FFK91] S.A. Fenner, L.J. Fortnow, S.A. Kurtz. Gap-definable counting classes. *Proceedings of the 6th Structure in Complexity Theory Conference*, 30-42, IEEE Computer Society Press, 1991.

[Gi77] J. Gill. Computational complexity of probabilistic complexity classes. *SIAM Journal on Computing* 6, 675-695, 1977.

[GoPa86] L. Goldschlager, I. Parberry. On the construction of parallel computers from various bases of boolean functions. *Theoretical Computer Science* 43, 43-58, 1986.

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

[Her90] U. Hertrampf. Relations among MOD-classes. *Theoretical Computer Science 74*, 325-328, 1990.

[LLS75] R. Ladner, N. Lynch and A. Selman. A comparison of polynomial time reducibilities. *Theoretical Computer Science*, 1(2):103-124, 1975.

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

[Sal93] 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.

[Schö86] U. Schöning. *Complexity and Structure.* Springer-Verlag *Lecture Notes in Computer Science* 211, 1986.

[Schö93] U. Schöning. On random reductions from sparse sets to tally sets. In *Information Processing Letters 46* (1993), 239-241.

[Sim75] J. Simon. *On some central problems in computational complexity.* PhD thesis, Cornell University, Ithaca, New York, January 1975.

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

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

[Val79] L.G. Valiant. The complexity of computing the permanent. *Theoretical Computer Science* 8, 189-201, 1979.

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

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

[Yao90] A. Yao. On ACC and threshold circuits. In *Proceedings of the 31st Symposium on Foundations of Computer Science*, 619-627, 1990.