On Modular Counting with Polynomials

Kristoffer Arnsfelt Hansen

Department of Computer Science
University of Aarhus, Denmark
arnsfelt@daimi.au.dk

Abstract

For any integers m and l, where m has r sufficiently large (depending on l) factors, that are powers of r distinct primes, we give a construction of a (symmetric) polynomial over $\mathbf{Z}_m$ of degree $O(\sqrt[r]{n})$ that is a generalized representation (commonly also called weak representation) of the MOD_l function. We give a detailed study of the case when m has exactly two distinct prime factors, and classify the minimum possible degree for a symmetric representing polynomial.

1 Introduction

Motivated by the lack of understanding of $\mathbf{AC^0}$ circuits augmented with MOD_m gates for a composite integer m, Barrington et al. [1] studied a special case corresponding to polynomials. They defined what we will call a *one-sided representation* of a Boolean function by a polynomial over $\mathbf{Z}_m$, and with this representation they obtained lower bounds of $n^{\Omega(1)}$ on the degree for polynomials representing the MOD_l and $\neg\mathrm{MOD}_l$ functions if l has a prime factor not dividing m. Later these bounds was later improved to $\Omega(n)$ by Tsai [11]. For the AND and MAJORITY functions similar lower bounds of n and $\frac{n}{2}$ respectively, are easily obtained ([8] Lemma 9.8, [10] Proposition 1). In contrast to this Barrington et al. proved the surprising result that the OR function can be represented by a polynomial of degree $O(\sqrt[r]{n})$ where r is the number of distinct prime factors in m, giving a natural setting where counting modulo a composite integer is more powerful than counting modulo a prime power. The polynomial they construct is even symmetric, and they observed that for symmetric polynomials, degree $\Omega(\sqrt[r]{n})$ is necessary. For general polynomials however, the best lower bound for the OR function is just the $\Omega(\log^{\frac{1}{r-1}} n)$ bound proved by Tardos and Barrington [9].

Despite the fact that even symmetric polynomials can give surprising representations modulo a composite integer, only recently were symmetric polynomials studied systematically. Bhatnagar et al. [3] proved an equivalence between representations by symmetric polynomials and protocols for certain *simultaneous* promise communication games. Using this framework they showed that surprising upper bounds are a general phenomena for the Threshold k function T_k, generalizing the OR function. For *constant* k they prove a degree $O(n^{\frac{1}{2}+\epsilon})$ upper bound when m has two distinct prime factors and for a general m with r distinct prime factors, assuming the *abc*-conjecture, an $O(n^{\frac{1}{r}+\epsilon})$ upper bound. For nonconstant k and with m having two distinct prime factors they obtain an $O((nk)^{\frac{1}{2}+\epsilon})$ upper bound, again assuming the *abc*-conjecture. They also show that for symmetric polynomials these upper bounds are almost tight, by giving a lower bound of $\Omega(n^{\frac{1}{r}}k^{1-\frac{1}{r}})$.

In this paper we will focus on a different notion of representation of Boolean functions by polynomials we will call *generalized representation*, that Barrington et al. [1] proposed as a more robust notion of representation. This notion generalizes the one-sided version, and in fact coincides with it for the OR function. The best lower bound on the degree for generalized representation is the $\Omega(\log n)$ lower bound for the generalized inner product function proved by Grolmusz [7]. Recent results of Bourgain [4] and Green et al. [6] also imply a $\Omega(\log n)$ lower bound for the MOD_l function, when m and l are relatively prime.

The communication game framework of Bhatnagar et al. is completely general, and also provides an equivalence between generalized representations by symmetric polynomials and protocols for simultaneous promise communication games. Using this they proved that a symmetric polynomial over $\mathbf{Z}_m$ where $m = p_1^{e_1} p_2^{e_2}$ for distinct primes p_1 and p_2, require degree $\Omega(n)$ for representing MOD_l when $l > \min(p_1^{e_1}, p_2^{e_2})$ and p_1 and p_2 does not divide l. For general m they also gave a lower bound of $\Omega(n)$ on the degree for representing MOD_l for any sufficiently large l, relatively prime to m. They prove this by an interesting reduction from the Exactly-r function in the Number On the Forehead model of communication complexity and use a lower bound of $\omega(1)$ due to Chandra et al. [5]. This bound is obtained using a Ramsey-type argument and as a consequence the size of l required for obtaining a degree $\Omega(n)$ lower bound for polynomials is very large.

1.1 Our results

We continue the study of generalized representations of the MOD_l function by symmetric polynomials and show that in fact also for these functions nontrivial upper bounds can be found. To be more specific, we show that whenever m has r sufficiently large powers of distinct primes as factors, an $O(\sqrt[r]{n})$ upper bound holds.

Theorem 1 *Let $b_1, \ldots, b_r$ be positive integers such that $\sum_{i=1}^{r} \frac{1}{b_i} < 1$. For distinct primes $p_1, \ldots, p_r$, let $q_i = p_i^{e_i}$. Suppose that q_i divides m and that $q_i \geq b_i l$ for all i. Then there exists a symmetric polynomial over $\mathbf{Z}_m$ of degree $O(\sqrt[r]{n})$ that is a generalized representation of the MOD_l function.*

The above theorem is optimal in the sense that for any m relatively prime to l and having exactly r distinct prime factors, degree $\Omega(\sqrt[r]{n})$ is necessary. For the special case of $r = 2$ we will give a more detailed analysis.

Theorem 2 *Let $q_1 < q_2$ be powers of distinct primes p_1 and p_2, let $m = q_1 q_2$ and let l be an integer relatively prime to m. If $q_1 = l + 1$ and $q_2 < 2(l + 1)$ any symmetric polynomial over $\mathbf{Z}_m$ that is a generalized representation of the MOD_l function must have degree $\Omega(n)$. If either $q_1 \geq l + 1$ and $q_2 \geq 2(l + 1)$ or $q_1 \geq l + 2$ and $q_2 \geq 2l + 1$ then there exists a symmetric polynomial over $\mathbf{Z}_m$ of degree $O(\sqrt{n})$ that is a generalized representation of the MOD_l function.*

For example, every symmetric polynomial over $\mathbf{Z}_{15}$ that is a generalized representation of MOD_2 must have degree $\Omega(n)$, while for every odd $m > 15$ having two distinct prime factors, there is symmetric polynomial over $\mathbf{Z}_m$ of degree $O(\sqrt{n})$ that is a generalized representation of MOD_2.

While the above theorem does not give a complete characterization of the degree in terms of the prime powers q_1 and q_2, we can give a classification of the minimum possible degree for a representing polynomial.

Theorem 3 *Let q_1 and q_2 be powers of distinct primes p_1 and p_2, let $m = q_1 q_2$ and let l be an integer relatively prime to m. Either there exist a polynomial over $\mathbf{Z}_m$ of degree $O(\sqrt{n})$ that is a generalized representation of the MOD_l function, or every polynomial over $\mathbf{Z}_m$ that is a generalized representation of the MOD_l function must have degree $\Omega(n)$.*

Furthermore we have the following monotonicity property.

Theorem 4 *Let q_1 and q_2 be powers of distinct primes p_1 and p_2 and let q_1' and q_2' be powers of distinct primes p_1' and p_2'. Let $m = q_1 q_2$, $m' = q_1' q_2'$ and let l be an integer relatively prime to m and m'. Suppose that $q_1 \leq q_1'$ and $q_2 \leq q_2'$. Then, if there exist a polynomial over $\mathbf{Z}_m$ of degree $O(\sqrt{n})$ that is a generalized representation of the MOD_l function, there also exist a polynomial over $\mathbf{Z}_{m'}$ of degree $O(\sqrt{n})$ that is a generalized representation of the MOD_l function.*

For the general case of $r > 2$ distinct prime factors we have no similar results. However by combining Theorem 1 and the $\Omega(n)$ lower bound of Bhatnagar et al. [3] we have the following statement about the minimum possible degree for a representing polynomial.

Theorem 5 *For every r and s there exists relatively prime integers l and m with the following properties.*

- *m has $r + s$ distinct prime factors.*
- *There exists a symmetric polynomial over $\mathbf{Z}_m$ of degree $O(\sqrt[r]{n})$ that is a generalized representation of the MOD_l function.*
- *Every symmetric polynomial over $\mathbf{Z}_m$ that is a generalized representation of the MOD_l function must have degree $\Omega(n^{\frac{1}{r+1}})$.*

1.2 Representation by polynomials

Let f be a Boolean function in n variables, and let P be a polynomial in n variables over $\mathbf{Z}_m$. We will consider the following two notions of representation of f by P.[1]

- P is a *one-sided* representation of f if $f(x) = 1$ if and only if $P(x) \not\equiv 0 \pmod m$ for all $x \in \{0,1\}^n$.

[1] We have chosen our terminology to avoid ambiguities found in the literature. Bhatnagar et al. [3] uses the terms *strong* and *weak* instead.

- P is a *generalized* representation of f if for every $x, x' \in \{0,1\}^n$ where $f(x) \neq f(x')$ it holds that $P(x) \neq P(x')$.

Equivalently, P is a *generalized* representation of f if there is a set $S \subset \mathbf{Z}_m$ such that $f(x) = 1$ if and only if $P(x) \in S$ for all $x \in \{0,1\}^n$.

1.3 Simultaneous protocols

Since we will only deal with Boolean functions $f : \{0,1\}^n \to \{0,1\}$ that are symmetric, i.e. only depending on the *weight* of its input, we will identify these with functions $f : \{0,\ldots,n\} \to \{0,1\}$.

Let $q_1,\ldots,q_r$ be powers of distinct primes $p_1,\ldots,p_r$. We consider r-player protocols with respect to $q_1,\ldots,q_r$, with players $P_1,\ldots,P_r$ for computing a symmetric Boolean function f on n variables. The parameters of the protocol are integers $k_1,\ldots,k_r$. Player P_i must provide an output in $\mathbf{Z}_{q_i}$ given an input w_i from $\mathbf{Z}_{n_i}$, where $n_i = p_i^{k_i}$. On inputs $w_1,\ldots,w_r$, the players are promised that there exists $0 \leq w \leq n$ such that $w_i \equiv w \pmod{n_i}$ for all i. The cost of a protocol is $\max_{i=1}^r n_i$.

We say that a protocol is a *one-sided* protocol for f if for every $0 \leq w \leq n$, $f(w) = 1$ if and only if there exists an i such that player P_i on input $(w \mod n_i)$ outputs a nonzero element of $\mathbf{Z}_{q_i}$.

Similarly we say that a protocol is a *generalized* protocol for f if for every $0 \leq w, w' \leq n$ where $f(w) \neq f(w')$ there exists an i such that player P_i give different outputs on inputs $(w \mod n_i)$ and $(w' \mod n_i)$.

Bhatnagar et al. [3] proved the following equivalence between these protocols and representations by symmetric polynomials.

Theorem 6 *Let f be a symmetric Boolean function, and let $m = q_1 \cdots q_r$, where $q_i = p_i^{e_i}$ for all i and $p_1,\ldots,p_r$ are distinct primes. There exists a symmetric polynomial of degree d over $\mathbf{Z}_m$ that is a one-sided representation of f if and only if there exists a r-player one-sided protocol, with respect to $q_1,\ldots q_r$, computing f of cost $\Theta(d)$. Similarly there exists a symmetric polynomial of degree d over $\mathbf{Z}_m$ that is a generalized representation of f if and only if there exists a r-player generalized protocol, with respect to $q_1,\ldots q_r$, computing f of cost $\Theta(d)$.*

This view on symmetric polynomials turns out to be very useful. Consider first two-player generalized simultaneous protocols with respect to the prime powers q_1 and q_2, with parameters k_1 and k_2 and let f be a Boolean function in n variables. If there exists w and w' such that $w \equiv w' \pmod{n_1}$ and $w \equiv w' \pmod{n_2}$ and such that $f(w) \neq f(w')$ then clearly no protocol with parameters k_1 and k_2 can exist.

Assuming this is not the case, we construct the $n_1 \times n_2$ matrix A^f as follows. For $0 \leq w \leq n$ fill the entry $(w \mod n_1, w \mod n_2)$ of A^f with $f(w)$. Entries not filled in this way are marked by '$\times$', meaning "don't care" entries. Any protocol for f can now be viewed as a coloring of the rows of A^f with elements of $\mathbf{Z}_{q_1}$ and the columns of A^f with elements of $\mathbf{Z}_{q_2}$, where the colorings corresponds to the outputs of the two players. This coloring has the property, that if w and w' are such that $f(w) \neq f(w')$ either the rows $(w \mod n_1)$ and $(w' \mod n_1)$ or the columns $(w \mod n_2)$ and $(w' \mod n_2)$ have different colors. Conversely given a coloring with this property, it defines a protocol for f.

More generally, consider r-player protocols with respect to the prime powers $q_1,\ldots,q_r$ with parameters $k_1,\ldots,k_r$. Again, if there exists w and w' such that $w \equiv w' \pmod{n_i}$ for all i and $f(w) \neq f(w')$, no protocol with parameters $k_1,\ldots,k_r$ can exist. Assuming this is not the case define the r-dimensional $n_1 \times \cdots \times n_r$ matrix A^f by filling entry $(w \mod n_1,\ldots,w \mod n_r)$ with $f(w)$ for $0 \leq w \leq n$. Unfilled entries are again marked with '$\times$'. As before we can identify protocols with colorings of each dimension of A^f, where dimension i is colored with elements of $\mathbf{Z}_{q_i}$, such that, if entry $(a_1,\ldots,a_r)$ is 0 and entry $({a'}_1,\ldots,{a'}_r)$ is 1, then for some i, the indices a_i and ${a'}_i$ of dimension i have different colors.

In the remaining part of this section, we will describe a generic approach to constructing and analyzing two-player protocols. Consider again the $n_1 \times n_2$ matrix A^f. We will say that two rows a_1 and ${a_1}'$ are in *conflict* if there is a column a_2 such the entry (a_1, a_2) of A^f is 0 and entry $({a_1}', a_2)$ of A^f is 1, or the other way around. Clearly, given a coloring of the rows of A^f a necessary condition for being able to color the columns and obtain a valid protocol is that conflicting rows are colored with different colors. We call such a coloring of the rows a *proper* coloring. Sometimes this condition is also sufficient.

Lemma 7 *Assume that $2^{q_1} \leq q_2$. Let k_1 and k_2 be given parameters and consider the matrix A^f. Then there exists a protocol for f with parameters k_1 and k_2 if and only if the rows of A^f can be properly colored.*

Proof Consider any proper coloring of the rows with elements of $\mathbf{Z}_{q_1}$. We will then color the columns of A^f with elements of $\{0,1\}^{q_1}$. For a column a_2 and for every possible row-color c, we look for the rows colored with

c. If for such a row a_1 entry (a_1, a_2) of A^f contains a 0 or 1 we record that in entry c of the column-color. Since the coloring is proper, this is well defined. Entries in the column-color not filled in this way can be filled arbitrarily. We claim this gives a valid protocol. Suppose that w and w' are such that $f(w) \neq f(w')$. If the rows $(w \mod n_1)$ and $(w' \mod n_1)$ are colored with the same color c, then by definition the coloring assigned to the columns $(w \mod n_2)$ and $(w \mod n_2)$ differ in entry c. $\square$

The fact that possibly not every entry in the column-colors are filled, sometimes means that it can be enough with much fewer colors for the columns. We will now define the *cost* of a proper coloring. We will first, for every column a_2 associate a string in $\{0, 1, \times\}^{q_1}$. For a column a_2 and for every possible row-color c, we look for the rows colored with c. If for such a row a_1 entry (a_1, a_2) of A^f contains a 0 or 1 we record that in entry c of the string. If no such row can be found we let entry c in the string be $\times$. After generating these strings, we can fill 0's or 1's in place of the '$\times$'s in any way. The cost of the coloring is then defined to be the minimum number of different strings in $\{0, 1, \times\}^{q_1}$ that can result from doing this. We now have the following necessary and sufficient condition for the existence of a protocol.

Lemma 8 *Let q_1 and q_2 be powers of distinct primes p_1 and p_2. Let k_1 and k_2 be given parameters and consider the matrix A^f. Then there exists a protocol for f with parameters k_1 and k_2 if and only if there exists a proper coloring of the rows of A^f with q_1 colors of cost at most q_2.*

Proof Consider any protocol for f, and the induced proper coloring of the rows of A^f. Consider the strings in $\{0, 1, \times\}^{q_1}$ associated with columns of a given color. For all row colors c, the strings must have either all 0's or '$\times$'s in entry c or all 1's or '$\times$'s in entry c, as otherwise the protocol would not compute f correctly. We can thus make all these string equal by filling 0's or 1's in place of some of the '$\times$'s. It follows that the cost of the coloring is at most q_2. The converse statement, constructing a protocol from a proper coloring of cost at most q_2 is done in the same way as Lemma 7. $\square$

2 Protocols for MOD_l

Two different definitions of the MOD_l function are commonly used, one being the complement of the other. For our purposes the chosen definition does not matter, but to be precise we define the MOD_l function on n variables as $\mathrm{MOD}_l(x) = 1$ if and only if $\sum_{i=1}^{n} x_i \equiv 0 \pmod{l}$.

We will first establish the general upper bound of Theorem 1 by constructing a protocol for the multi-player communication game. For this we will use the following version of the *explicit* Chinese remainder theorem (see for instance [2]).

Theorem 9 (Explicit Chinese remainder theorem) *Let $n_1, \ldots, n_r$ be relatively prime positive integers. Let $N = n_1 \cdots n_r$. Suppose that w is an integer such that $0 \leq w < N$ and $((\frac{N}{n_i})^{-1} \mod n_i)w \equiv a_i \pmod{n_i}$ for all i. Then $w = N(z - \lfloor z \rfloor)$, where $z = \sum_{i=1}^{r} \frac{a_i}{n_i}$.*

Proof We have $zN = \sum_{j=1}^{r} a_j \frac{N}{n_j} \equiv w((\frac{N}{n_i})^{-1} \mod n_i)\frac{N}{n_i} \equiv w \pmod{n_i}$ for all i. Hence $zN \equiv w \pmod{N}$. Write $zN = w + rN$ for an integer r. Since then $(z - r)N = w$, we have $0 \leq z - r < N$ and it follows that $r = \lfloor z \rfloor$. $\square$

Note that, in the usual formulation of the Chinese remainder theorem, we would instead assume that $0 \leq w < N$ and $w \equiv a_i \pmod{n_i}$ for all i, and conclude that $w = (z - \lfloor z \rfloor)N$, where $z = \sum_{i=1}^{r} \frac{a_i}{n_i}((\frac{N}{n_i})^{-1} \mod n_i)$.

Proof (Theorem 1) As in the statement of the theorem, let $b_1, \ldots, b_r$ be positive integers such that $\sum_{i=1}^{r} \frac{1}{b_i} < 1$, let $p_1, \ldots, p_r$ be distinct primes and let $q_i = p_i^{e_i}$. Assume that q_i divides m and that $q_i \geq b_i l$ for all i. Consider parameters $k_1, \ldots, k_r$. Let $n_i = p_i^{k_i}$ and $N = n_1 \cdots n_r$. For $f = \mathrm{MOD}_l$ on n variables we consider the matrix A^f. Let A^f_π be the matrix obtained from A^f by permuting the indices along dimension i by multiplying the indices by $((\frac{N}{n_i})^{-1} \mod n_i)$. We color the indices of A^f_π along dimension i as follows: Partition the indices of dimension i into b_i blocks each containing at most $\lceil \frac{n_i}{b_i} \rceil$ (consecutive) indices, and color each such block with l colors used only in that block. Specifically, we color index a_i occurring in block j by $jl + (a_i \mod l)$. In this way we have the property, that if indices a_i and a'_i, where $0 \leq a_i < a'_i < n_i$, are colored with the same color we have $a_i \equiv a'_i \pmod{l}$ and $|a'_i - a_i| \leq \lceil \frac{n_i}{b_i} \rceil - 1$.

We claim that for $n \leq (1 - \sum_{i=1}^{r} \frac{1}{b_i})\frac{N}{2}$ this defines a valid protocol for f. Let $(a_1, \ldots, a_r)$ and $(a'_1, \ldots, a'_r)$ be $0/1$ entries of A^f_π such that for all i, the indices a_i and a'_i have the same color along dimension i. By construction we have $a_i \equiv a'_i \pmod{l}$ and $|a'_i - a_i| \leq \lceil \frac{n_i}{b_i} \rceil - 1$ for all i. Let $z = \sum_{i=1}^{r} \frac{a_i}{n_i}$ and $z' = \sum_{i=1}^{r} \frac{a'_i}{n_i}$. By Theorem 9 we have $z - \lfloor z \rfloor \leq \frac{n}{N} \leq \frac{1}{2}(1 - \sum_{i=1}^{r} \frac{1}{b_i})$ and likewise $z' - \lfloor z' \rfloor \le \frac{n}{N} \le \frac{1}{2}(1 - \sum_{i=1}^{r} \frac{1}{b_i})$. Since $|z' - z| \le \sum_{i=1}^{r} \frac{|a'_i - a_i|}{n_i} \le \sum_{i=1}^{r} \frac{\lceil \frac{n_i}{b_i} \rceil - 1}{n_i} \le \sum_{i=1}^{r} \frac{1}{b_i}$, we must have $\lfloor z \rfloor = \lfloor z' \rfloor$. (Assume without loss of generality that $z \ge z'$. Then $\lfloor z \rfloor - \lfloor z' \rfloor = (z' - \lfloor z' \rfloor) + (z - z') - (z - \lfloor z \rfloor) \le \frac{1}{2}(1 - \sum_{i=1}^{r} \frac{1}{b_i}) + \sum_{i=1}^{r} \frac{1}{b_i} = \frac{1}{2}(1 + \sum_{i=1}^{r} \frac{1}{b_i}) < 1$). By Theorem 9 again, the entry $(a_1, \ldots, a_r)$ of A_π^f is $f(w)$, where $w = (z - \lfloor z \rfloor)N$ and entry $(a'_1, \ldots, a'_r)$ of A_π^f is $f(w')$, where $w' = (z' - \lfloor z' \rfloor)N$.

To conclude, we have $w = \sum_{i=1}^{r} a_i \frac{N}{n_i} - \lfloor z \rfloor N \equiv \sum_{i=1}^{r} a'_i \frac{N}{n_i} - \lfloor z' \rfloor N = w' \pmod{l}$, and we have $f(w) = f(w')$. Since we can choose $n = \Omega(N)$, the result follows. $\square$

To justify the remark about the optimality of the construction, note that any protocol give the same result on the two inputs 0 and $n_1 \cdots n_r$. When m and l are relatively prime, we have $n_1 \cdots n_r \not\equiv 0 \pmod{l}$ and thus must have $n < n_1 \cdots n_r$.

We now formally state the result of Bhatnagar et al. [3] that we will use in the proof of Theorem 5.

Theorem 10 (Bhatnagar et al.) *Let m be an integer with r distinct prime factors. Then for every sufficiently large integer l, that is relatively prime to m, it holds that every symmetric polynomial over $\mathbf{Z}_m$ that is a generalized representation of the MOD_l function must have degree $\Omega(n)$.*

Proof (Theorem 5) Pick s distinct primes $p_1, \ldots, p_s$ and let $m' = p_1 \cdots p_s$. Using Theorem 10 we may choose l relatively prime to m' such that every symmetric polynomial over $\mathbf{Z}_{m'}$ that is a generalized representation of the MOD_l function must have degree $\Omega(n)$.

Now further pick distinct primes $p_{s+1}, \ldots, p_{s+r}$ such that $p_{s+i} \ge (r+1)l$ for all i, and let $m = p_1 \cdots p_{s+r}$. Clearly m and l are relatively prime. From Theorem 1 we furthermore have a symmetric polynomial over $\mathbf{Z}_m$ of degree $O(\sqrt[r]{n})$ that is a generalized representation of the MOD_l function.

Consider now any $(s+r)$-player protocol for MOD_l on n inputs with parameters $k_1, \ldots, k_{r+s}$, and let $n_i = p_i^{k_i}$ for all i. Let $n' = n(\prod_{j=s+1}^{s+r} n_j)^{-1}$. We now restrict the protocol to inputs of the form $w \prod_{j=s+1}^{s+r} n_j$, for $0 \le w \le n'$. Since $w \prod_{j=s+1}^{s+r} n_j \equiv 0 \pmod{l}$ if and only if $w \equiv 0 \pmod{l}$ the restriction gives a s-player protocol for MOD_l on n' inputs. From Theorem 10 we have $\max_{i=1}^{s} n_i = \Omega(n')$, which implies $(\max_{i=1}^{s+r} n_i)^{r+1} = \Omega(n)$, and thus the original protocol has cost $\Omega(n^{\frac{1}{r+1}})$. $\square$

For the proofs of Theorem 2, 3 and 4 we introduce a *shifting game* and we will show that these precisely capture two-player communication protocols computing the MOD_l function. In fact, we will show that solutions to these games essentially capture every proper coloring, in the sense of Lemma 8, of the rows of A^f, where $f = \mathrm{MOD}_l$. The cost of a solution to the shifting game is therefore defined such that it corresponds to the cost of the coloring.

Define the (a, b)-*shifting game* as follows: The goal is to transform the list $(0, 1, \ldots, a-1)$ into $(a-1, 0, 1, \ldots, a-2)$ through any number of steps. Each step is a new list consisting of a distinct integers from $\mathbf{Z}_b$. The requirement is that if the same number occurs in two consecutive lists, it must be in the same position in each of the lists. We now define the *cost* of a solution to the game. Every two consecutive lists will give rise to a different strings in $\{0, 1, \times\}^b$. Let $(x_0, \ldots, x_{a-1})$ and $(y_0, \ldots, y_{a-1})$ be consecutive lists and let $i \in \mathbf{Z}_a$. The ith string is obtained by setting every position not occurring as x_j or y_j to '$\times$' in the string. We put 1 in position x_i and y_i, and for every $j \ne i$ we put 0 in position x_j and y_j. After generating these strings, we can fill 0's or 1's in place of the '$\times$'s in any way. The cost of the solution to the game is then defined to be the minimum number of different strings in $\{0, 1, \times\}^b$ that can result from doing this. Below we give solutions to 3 different shifting games.

$(a, a+1)$-shifting game.

$(0, 1, 2, \ldots, a-2, a-1)$
$(a, 1, 2, \ldots, a-2, a-1)$
$(a, 0, 2, \ldots, a-2, a-1)$
$(a, 0, 1, \ldots, a-2, a-2)$
$\cdots$
$(a, 0, 1, \ldots, a-3, a-2)$
$(a-1, 0, 1, \ldots, a-2)$

$(a, a+2)$-shifting game.

$(0, 1, 2, 3, \ldots, a-2, a-1)$
$(a, a+1, 2, 3, \ldots, a-2, a-1)$
$(a, a+1, 1, 3, \ldots, a-2, a-1)$
$(a, a+1, 1, 2, \ldots, a-2, a-1)$
$\cdots$
$(a, a+1, 1, 2, \ldots, a-3, a-2)$
$(a-1, 0, 1, 2, \ldots, a-3, a-2)$

$(a, 2a)$-shifting game.

$(0, 1, \ldots, a-1)$
$(a, a+1, \ldots, 2a-1)$
$(a-1, 0, 1, 2, \ldots, a-2)$.

We now analyze the costs of these solutions.

Lemma 11 *The $(a, a+1)$-shifting game shifting game can be solved with cost $2(a+1)$, the $(a, a+2)$-shifting game shifting game can be solved with cost $2a+1$, and finally the $(a, 2a)$-shifting game can be solved with cost $2a$.*

Proof Using regular expression notation, the strings generated by the solution to the $(a, a+1)$-shifting game are precisely the strings of the form 10^*1, 0^*10^* and 0^*110^* of which there are $2(a+1)$. The strings generated by the solution to the $(a, 2a)$-shifting are precisely the strings of the form $0^*10^{a-1}10^*$, $0^*10^a10^*$ and $0^{a-1}110^{a-1}$ of which there are $2a$.

Finally consider the strings generated by the solution to the $(a, a+2)$-shifting game. The first two lists generate the strings of the form 10^*10, 010^*1 and 000^*10^*00. The last two lists generate the strings 0^*110, 10^*1 and 00^*10^*000. All remaining consecutive lists generate all strings of the form $\times 0^*10$, $\times 0^*01$, $\times 0^*10^*00$ and $\times 0^*110^*00$. Of these we fill in 1 for the '$\times$ in the first two obtaining 10^*10 and 10^*1 and we fill in 0 for the '$\times$' in the last two obtaining 0^*10^*00 and 0^*110^*00.

In this way we end up with all strings of the form 10^*10, 010^*1, 0^*110, 10^*1, 0^*10^*00 and 0^*110^*00, totaling $1+1+1+1+(a-1)+(a-2) = 2a+1$ different strings. $\square$

We can also show that the solution given to the $(a, a+1)$-shifting game is optimal.

Lemma 12 *Every solution to the $(a, a+1)$-shifting game must have cost at least $2(a+1)$.*

Proof Consider any solution to the $(a, a+1)$-shifting game. Without loss of generality, assume that all consecutive lists are distinct. Now, since every number occurring in two consecutive lists must be in the same position, consecutive lists must contain all the $a+1$ numbers, and exactly one position have changed. Let $x_1 = a$ and for $i \geq 1$ let x_{i+1} be the number in list i that is changed to x_i in list $i+1$. Note that the lists i and $i+1$ will generate the following strings in $\{0,1\}^{a+1}$: First all strings of the form 0^*10^* where the 1 can occur in any position different from x_i and x_{i+1} and finally the string of the form $0^*10^*10^*$ containing a 1 in position x_i and x_{i+1}. Since every number must occur in the sequence, all $a+1$ strings of the form 0^*10^* and at least $a+1$ distinct strings of the form form $0^*10^*10^*$ will be generated. We can conclude that any solution must have cost at least $2(a+1)$. $\square$

Finally we will now show a correspondence between solutions to shifting games and two-player protocols for the MOD_l functions. From this Theorem 3 and 4 will directly follow, and combining the theorem with Lemma 11 and Lemma 12 we also obtain Theorem 2. (Note that the solution given to the $(a, 2a)$-shifting game does not give any degree upper bound not covered by the first two solutions).

Theorem 13 *Let l be an integer, let q_1 and q_2 be powers of distinct primes p_1 and p_2, such that $l < q_1$ and $l < q_2$ and p_1 and p_2 does not divide l. Suppose that the (l, q_1)-shifting game can be solved with cost at most q_2. Then there exists a two-player protocol for MOD_l with respect to q_1 and q_2 of cost $O(\sqrt{n})$. On the other hand, there exists $\epsilon > 0$, such that if there exists a two-player protocol for MOD_l of cost ϵn, with respect to q_1 and q_2, then there is a solution to the (l, q_1)-shifting game of cost at most q_2.*

Proof For $f = \mathrm{MOD}_l$ on n variables and parameters k_1 and k_2 given we consider the matrix A^f. For convenience assume that $n_1 = p_1^{k_1} \equiv 1 \pmod{l}$ and $n_2 = p_2^{k_2} \equiv 1 \pmod{l}$. (This can be obtained by increasing k_1 and k_2 by at most $l-1$). Let A^f_π be the matrix obtained from permuting the rows and columns of A^f by multiplying a row index by $(n_2^{-1} \mod n_1)$ and a column index by $(n_1^{-1} \mod n_2)$.

Assume that $n < n_1 n_2$ and consider a fixed column $(a_2 \mod n_2)$ of A^f_π, where $-n_2 < a_2 \leq 0$. We will look at the $0/1$ entries as occurring in rows $(a_1 \mod n_1)$, where a_1 is chosen such that $0 \leq \frac{a_1}{n_1} + \frac{a_2}{n_2} < 1$. By Theorem 9, the $0/1$ entry $(a_1 \mod n_1, a_2 \mod n_2)$ is then $f(w)$, where $w = (\frac{a_1}{n_1} + \frac{a_2}{n_2}) n_1 n_2 = a_1 n_2 + a_2 n_1 \equiv a_1 + a_2 \pmod{l}$. Since $0 \leq w \leq n$, we thus have that the $0/1$ entries in column $(a_2 \mod n_2)$ are precisely those in rows $(a_1 \mod n_1)$, where $\frac{-a_2}{n_2} n_1 \leq a_1 \leq \frac{-a_2}{n_2} n_1 + \frac{n}{n_2}$.

Furthermore, since $0 \leq -a_2 < n_2$ we have that $0 \leq \frac{-a_2}{n_2} n_1 < n_1$. If $a_1 < n_1$ then $(a_1 \mod n_1) = a_1$ and thus $(a_1 \mod n_1) \equiv a_1 \pmod{l}$. If $a_1 \geq n_1$ we have $(a_1 \mod n_1) = a_1 - n_1$ and thus $(a_1 \mod n_1) \equiv a_1 - 1 \pmod{l}$.

We now describe how to transform a solution to the shifting game into a coloring giving a protocol. We will follow Lemma 8 and construct a proper coloring of the rows of cost at most the cost of the solution to the shifting game. Suppose that the shifting game is solved in $s+1$ steps. We partition the rows of A^f_π into $\lfloor \frac{n_1}{l} \rfloor$ groups of l (consecutive) rows, with a left-over row, $n_1 - 1$. Each of these groups will be colored according to a list in the solution to the shifting game. Each of the first $s-1$ lists are used to color $\lfloor \frac{n_1}{sl} \rfloor$ (consecutive) groups. List s is used to color the last $\lfloor \frac{n_1}{l} \rfloor - (s-1) \lfloor \frac{n_1}{sl} \rfloor \geq \lfloor \frac{n_1}{sl} \rfloor$

groups. Finally we color the remaining row $n_1 - 1$ with color $l - 1$.

Assume now that $\lfloor \frac{n}{n_2} \rfloor + 1 \leq l \lfloor \frac{n_1}{sl} \rfloor$. This implies, that in a given column $(a_2 \mod n_2)$, the $0/1$ entries are either all colored according to (at most) two consecutive of the first s lists, or they are colored according to list 1 and s (we include row $n_1 - 1$ in this case). In the first case, we have $\frac{-a_2}{n_2} n_1 + \frac{n}{n_2} < n_1$, which means that a row $(a_1 \mod n_1) = a_1$ will be colored by entry $(a_1 \mod l)$ of the used list. Thus there will be a 1 in rows colored using element $(-a_2 \mod l)$ of a list, and otherwise a 0. In the second case, for a row $(a_1 \mod n_1)$ colored according to list s, we have $(a_1 \mod n_1) = a_1$ and it is thus colored by entry $(a_1 \mod l)$ of list s. For a row colored according to list 1, we have $(a_1 \mod n_1) = a_1 - n_1$ and it is thus colored by entry $((a_1 - n_1) \mod l) = ((a_1 - 1) \mod l)$ of list 1, which is precisely the same as entry $(a_1 \mod l)$ of list $s + 1$. Finally, row $n_1 - 1$ is colored by $l - 1$ which is entry $((n_1 - 1) \mod l) = 0$ of list $s + 1$. Thus there will be a 1 in rows colored using element $(-a_2 \mod l)$ of list s or $s + 1$, and otherwise a 0. The requirement of the shifting game thus implies that, if two rows $(a_1 \mod n_1)$ and $(a_1' \mod n_1)$ are colored with the same color, we have $a_1 \equiv a_1' \pmod{l}$, which implies that the coloring is proper. Finally observe that the strings associated with the columns for finding the cost of the coloring corresponds (after possibly filling some '$\times$'s entries by 0's or 1's) to the strings generated by the solution to the shifting game. Thus the cost of the coloring is at most q_2. Since we can choose $n = \Omega(n_1 n_2)$, the result follows.

We now conversely show how to transform a protocol into a solution to the shifting game. Again, partition the rows of A_π^f into $\lfloor \frac{n_1}{l} \rfloor$ groups of l (consecutive) rows, with a left-over row, $n_1 - 1$. For two consecutive groups and every $0 \leq i < l$ we will find a column with a 1 in row i of each group and 0 elsewhere. For the last group we will for every $0 \leq i < l$ find a column with 1 in row i of the last group and row $((i - 1) \mod l)$ of the first group and 0 elsewhere. To be able to do this, we assume that $n_1 \geq 2(l + 1)$, $n_2 \geq 2l$ and $n \geq 2l(n_1 + n_2)$.

In the first case, suppose that the two group are contained in rows b_1 to $b_1 + 2l - 1$, where $0 \leq b_1$ and $b_1 + 2l - 1 < n_1$. If $\frac{b_1}{n_1} n_2 \geq l$, we may pick $0 \leq \frac{b_1}{n_1} n_2 - l \leq -a_2 \leq \frac{b_1}{n_1} n_2$ such that $-a_2 \equiv i \pmod{l}$. This implies $b_1 - l\frac{n_1}{n_2} \leq \frac{-a_2}{n_2} n_1 \leq b_1$, and we thus have $0/1$ entries in rows b_1 to $b_1 - l\frac{n_1}{n_2} + \frac{n}{n_2} \geq b_1 + 2l - 1$, with a 1 in rows $b_1 + i$ and $b_1 + l + i$ and 0 elsewhere in the two groups. Otherwise, if $\frac{b_1}{n_1} n_2 < l$ we have $b_1 < l\frac{n_1}{n_2}$. Choose $n_2 - l \leq -a_2 < n_2$ such that $-a_2 \equiv i + 1 \pmod{l}$. We then have $0/1$ entries in rows $(a_1 \mod n_1)$ where $\frac{n_2 - 1}{n_2} n_1 \leq a_1 \leq \frac{n_2 - l}{n_2} n_1 + \frac{n}{n_2}$, and thus in rows $0 \leq b_1$ to $\frac{n_2 - l}{n_2} n_1 - n_1 + \frac{n}{n_2} = \frac{n}{n_2} - l\frac{n_1}{n_2} \geq b_1 + 2l - 1$, again with a 1 in rows $b_1 + i$ and $b_1 + l + i$ and 0 elsewhere in the two groups.

In the second case, note that $\frac{n_1 - l - 1}{n_1} n_2 \geq l$. Hence we may pick $0 \leq \frac{n_1 - l - 1}{n_1} n_2 - l \leq -a_2 \leq \frac{n_1 - l - 1}{n_1} n_2$ such that $-a_2 \equiv i \pmod{l}$. This implies $n_1 - l - 1 - l\frac{n_1}{n_2} \leq \frac{-a_2}{n_2} n_1 \leq n_1 - l - 1$, and we thus have $0/1$ entries in rows $(a_1 \mod n_1)$, where $n_1 - l - 1 \leq a_1 \leq n_1 - l - 1 - l\frac{n_1}{n_2} + \frac{n}{n_2}$, and thus in rows $n_1 - l - 1$ to $n_1 - 1$ and rows 0 to $\frac{n}{n_2} - l - 1 - l\frac{n_1}{n_2} \geq l - 1$, with a 1 in rows $n_1 - l - 1 + i$ and $((i - 1) \mod l)$, and 0 elsewhere in the two groups.

From this we first conclude, that in every group, all rows are colored by different colors. Thus without loss of generality assume that the first group is colored by the list $(0, 1, \ldots, l-1)$ of colors. The solution to the shifting game will then be of length $\lfloor \frac{n_1}{l} \rfloor + 1$ and will consist, first of the lists of colors given by the $\lfloor \frac{n_1}{l} \rfloor$ groups and then ending with the list $(l - 1, 0, 1, \ldots, l - 2)$.

Finally, observe that the columns found above, precisely gives the strings that are generated in the definition of the cost of the solution to the shifting game, where we let entries not occurring as a row color in a given group be '$\times$'. By correctness of the protocol we may fill in 0's and 1's in place of some of the '$\times$'s obtaining at most q_2 strings. $\square$

3 Conclusion

We have obtained nontrivial degree upper bounds for generalized representation of the MOD_l function, contrasting the $\Omega(n)$ lower bounds of Bhatnagar et al. [3]. Ultimately we would like to understand the precise strength of general polynomials, rather than symmetric polynomials and in this respect *upper* bounds on the degree of representations by symmetric polynomials become the most interesting. On the other hand, understanding precisely under which conditions nontrivial upper bounds may be found, might give a hint of the difficulties of understanding the general case. We have given a detailed study of the case of two distinct prime factors, providing a classification of the minimum possible degree for a symmetric representing polynomial. It would be interesting to obtain the same for the general case.

4 Acknowledgment

The author is supported by BRICS, Basic Research in Computer Science, a Centre of the Danish National Research Foundation.

References

[1] D. A. M. Barrington, R. Beigel, and S. Rudich. Representing Boolean functions as polynomials modulo composite numbers. *Computational Complexity*, 4(4):367–382, 1994.

[2] D. J. Bernstein and J. P. Sorenson. Modular exponentiation via the explicit chinese remainder theorem. *Mathematics of Computation*, (to appear). Available from `http://cr.yp.to/papers.html`.

[3] N. Bhatnagar, P. Gopalan, and R. J. Lipton. Symmetric polynomials over $\mathbb{Z}_m$ and simultaneous communication protocols. *Journal of Computer and System Sciences*, 72(2):252–285, 2006.

[4] J. Bourgain. Estimation of certain exponential sums arising in complexity theory. *C. R. Acad. Sci. Paris, Ser. I*, 341:627–631, 2005.

[5] A. K. Chandra, M. L. Furst, and R. J. Lipton. Multi-party protocols. In *Proceedings of the 15th Annual ACM Symposium on Theory of Computing*, pages 94–99, 1983.

[6] F. Green, A. Roy, and H. Straubing. Bounds on an exponential sum arising in boolean circuit complexity. *C. R. Acad. Sci. Paris, Ser. I*, 341:279–282, 2005.

[7] V. Grolmusz. On the weak mod m representation of Boolean functions. *Chicago Journal of Theoretical Computer Science*, 1995.

[8] J. Håstad. *Computational limitations of small-depth circuits*. MIT Press, 1987.

[9] G. Tardos and D. A. M. Barrington. A lower bound on the mod 6 degree of the OR function. *Computational Complexity*, 7(2):99–108, 1998.

[10] J. Tarui. Degree complexity of Boolean functions and its applications to relativized separations. In *Proceedings of the 6th Annual Structure in Complexity Theory Conference*, pages 382–390. IEEE Computer Society Press,, 1991.

[11] S. C. Tsai. Lower bounds on representing Boolean functions as polynomials in Z_m. *SIAM Journal on Discrete Mathematics*, 9(1):55–62, 1996.