Electronic Colloquium on Computational Complexity, Report No. 47 (2003)

Symmetric Polynomials over $\mathbb{Z}_m$ and Simultaneous Communication Protocols

Nayantara Bhatnagar	Parikshit Gopalan	Richard J. Lipton
College of Computing	College of Computing	College of Computing
Georgia Tech	Georgia Tech	Georgia Tech
nand@cc.gatech.edu	parik@cc.gatech.edu	rjl@cc.gatech.edu

June 22, 2003

Abstract

We study the problem of representing symmetric Boolean functions as symmetric polynomials over $\mathbb{Z}_m$. We show an equivalence between such representations and simultaneous communication protocols. Computing a function with a polynomial of degree d modulo pq is equivalent to a two player protocol where one player is given the first $\lceil \log_p d \rceil$ digits of the weight in base p and the other is given the first $\lceil \log_q d \rceil$ digits of the weight in base q. The players can decide on a protocol beforehand but they cannot communicate directly with each other. If m has t distinct prime factors, the protocols involve t players. This reduces the problem of proving bounds on the degree of symmetric polynomials to proving bounds on simultaneous communication protocols. We use this equivalence to prove the following results

- We show lower bounds of $\Omega(n)$ on symmetric polynomials weakly representing classes of Mod_r functions. Previously the best known lower bound for symmetric polynomials weakly representing any function over $\mathbb{Z}_m$ was $n^{\frac{1}{t}}$ where t is the number of distinct prime factors of m. We show a linear lower bound for some threshold functions when $t = 2$.
- We show that the strong degree[1] of threshold c, for c constant, is $o(n)$ using the fact that the number of solutions of certain Catalan like Diophantine equations are finite. The connection goes both ways: the fact that the degree is $o(n)$ implies that some classes of Diophantine equations can have only finitely many solutions.
- We study classes of randomized protocols which are equivalent to choosing randomly from a sample space of symmetric polynomials and show upper bounds for threshold functions. In the context of probabilistic polynomials, we show that general polynomials are provably stronger than symmetric polynomials.

Our results give simplifications of many previously known results and provide a simple explanation for why some functions have lower degree over composites than over primes.

[1] By strong representation, we mean $f(X) = 0 \Rightarrow P(x) = 0$ and $f(X) \neq 0 \Rightarrow P(X) \neq 0$

ISSN 1433-8092

Contents

1 Introduction

We study the problem of representing a symmetric Boolean function[2] as a symmetric polynomial over $\mathbb{Z}_m$. The inputs to the polynomial are 0-1 inputs denoted by $X = X_1, X_2 \cdots X_n$. When m is prime, $\mathbb{Z}_m$ is a field and we say that P represents f if $P(X) = f(X)$. Proving lower bounds is not hard in this setting. When m is composite, there are many possible definitions for what it means for P to represent a Boolean function f.

Definition 1.1 *P strongly represents f if $f(X) = 0 \Rightarrow P(X) = 0$ and $f(X) = 1 \Rightarrow P(X) \neq 0$.*

Definition 1.2 *P weakly represents f if $f(X) \neq f(Y) \Rightarrow P(X) \neq P(Y)$. Equivalently there exist sets $A, A^c \subset \mathbb{Z}_m$ so that $f(X) = 0 \Rightarrow P(X) \in A$, $f(X) \neq 0 \Rightarrow P(X) \in A^c$.*

Tardos and Barrington [TB95] use the terminology *one-sided representation* for what we call *strong representation*, but we use the latter for simplicity. Also, when we refer to polynomials and degree, we mean only symmetric polynomials unless otherwise specified. Barrington, Beigel and Rudich [BBR94] proved the surprising result that the OR function can be strongly represented by a symmetric polynomial of degree $O(\sqrt{n})$ over $\mathbb{Z}_6$. In contrast OR has degree $\Omega(n)$ over $\mathbb{Z}_p$. They prove that this is the best possible for symmetric polynomials. Proving lower bounds is considerably easier in the strong representation. Linear lower bounds exist for functions for representations using general (not only symmetric) polynomials [BBR94, Ts96, Gre95]. But as pointed out by [TB95] the task is simplified by the fact that P must output 0 whenever f is 0. The weak representation seems a more natural definition and here far less is known with regard to lower bounds. The best lower bound known in this case for general polynomials is $\Omega(\log n)$ [Gro95, TB95] and the best previously known lower bound for symmetric polynomials is $\sqrt{n}$ [BBR94]. Their argument can be used to a show a $\sqrt{n}$ lower bound for many other functions. The lower bound comes from the observation that a symmetric polynomial of degree d over $\mathbb{Z}_6$ has period $O(d^2)$. Clearly the strongest bound this argument can prove for any function is $\sqrt{n}$ for $\mathbb{Z}_6$ and $n^{\frac{1}{t}}$ when m has t distinct prime factors.

1.1 Symmetric Polynomials and Simultaneous Protocols

We show an equivalence between symmetric polynomials representing f over $\mathbb{Z}_m$ and certain simultaneous communication protocols for computing the function f. As a first step towards showing this equivalence, we consider symmetric polynomials over Z_p. Every symmetric polynomial $P(X)$ over $\mathbb{Z}_p$ computes a function $f : \{0, 1, \cdots n\} \rightarrow \mathbb{Z}_p$ where $f(w)$ is the value of P on a $0-1$ input of weight w. We show that the functions that can be computed by a low degree symmetric polynomial in $\mathbb{Z}_p[X]$ are exactly those than can be computed from the first few digits of the base p representation of the weight. This is a consequence of a classical result in number theory called Lucas' Theorem which tells us how to evaluate binomial coefficients modulo p. This is made precise by the following theorems.

[2] Since we are dealing with only symmetric functions, we consider them as functions from $\{0, \cdots n\} \rightarrow \{0, 1\}$.

Theorem 2.4: Let $f : \{0,1\}^n \rightarrow \mathbb{Z}_p$ be a function computed by a symmetric polynomial $P[X] \in \mathbb{Z}_p[X]$ of degree $d < p^l$. Then f is a function of just the first l digits of w written in base p. Equivalently f can be computed from w mod p^l.

Theorem 2.5: Let $f : \{0,1\}^n \rightarrow \mathbb{Z}_p$ be a function which depends only on the first l digits of w in base p. Then f is computed by a symmetric polynomial $P \in \mathbb{Z}_p[X]$ whose degree is less than p^l.

Over $\mathbb{Z}_{p^a}$ essentially the same relation holds. However both directions are considerably harder to prove. The proof uses Kummer's Theorem which is a classical result that computes the exact power of p that divides a given binomial coefficient and some facts about interpolation over $\mathbb{Z}_{p^a}$.

We now introduce the notion of a protocol for computing a Boolean function $f : w \in \{0, \cdots n\} \rightarrow \{0,1\}$. For convenience, we take $m = 6$.

Definition 2.14: A strong protocol for computing f is a protocol involving two players P_2 and P_3. P_3 is given $i = w$ mod 3^{k_3} as input and outputs a number in $\mathbb{Z}_3$. P_2 is given $j = w$ mod 2^{k_2} as input and outputs a number in $\mathbb{Z}_2$. If $f(w) = 0$, then both players must output 0. If $f(w) = 1$, at least one player must output a non-zero value. The cost of the protocol is $\max(2^{k_2}, 3^{k_3})$. The two players cannot communicate but they can agree on a procedure beforehand.

Definition 2.15: A weak protocol is defined similarly except that if $f(w) \neq f(w')$ then at least one player should give different outputs on w and w'.

Both strong and weak protocols are simultaneous protocols where the two players compute their outputs independently of one another and write them on a blackboard. A referee then reads their outputs and decides if the output of the protocol is 0 or 1. In a strong protocol, the referee's strategy is fixed, he outputs 0 iff both players say 0. In a weak protocol, the referee can choose any strategy. For m with t distinct prime factors $p_1, \cdots, p_t$, we define protocols with t players where player P_i reads the input in base p_i.

We can now make the connection between symmetric polynomials and simultaneous protocols. By the Chinese Remainder Theorem, a degree d symmetric polynomial $P(X)$ over $\mathbb{Z}_6$ corresponds to symmetric polynomials $P_2(X)$ and $P_3(X)$ over $\mathbb{Z}_2$ and $\mathbb{Z}_3$ respectively whose degrees are at most d. By theorem 2.4 this means that the function computed by P can be computed from the residues of w mod 2^{k_2} and 3^{k_3} where these are the smallest powers of 2 and 3 which exceed d. This gives us the following theorem.

Theorem 2.16: If there exists a symmetric function of degree d that strongly (weakly) represents f then there exists a strong (weak) protocol of cost at most $3d$ for computing f.

Conversely assume there exists a low cost protocol for f. The function computed by each player can be represented by a low degree symmetric polynomial. We can now use the Chinese remainder theorem to combine these polynomials and get a low degree polynomial over $\mathbb{Z}_6$.

Theorem 2.17: If there exists a strong (weak) protocol of cost d that computes f then there exists a polynomial of degree at most d that strongly (weakly) represents f.

This equivalence allows us to use techniques from communication complexity for proving both upper and lower bounds on the degree of a polynomial representing f. The nature of the protocols allow us to use results from number theory to prove degree bounds. For instance the problem of determining the degree of threshold functions is related to classical problems regarding Diophantine equations.

1.2 Lower Bounds

Linear lower bounds for general polynomials in the strong representation are known for many functions. Far less is known for weak representations. We show a lower bound of $\Omega(n)$ on the degree of symmetric polynomials weakly representing the Mod_r function over $\mathbb{Z}_m$ for large enough r. We show a lower bound of $\Omega(k)$ on the weak degree of the threshold k function when m has two prime factors.

To prove lower bounds for weak two player protocols, we define a $3^{k_3} \times 2^{k_2}$ matrix A where $a_{ij} \equiv i \bmod 3^{k_3}$ and $a_{ij} \equiv j \bmod 2^{k_2}$. We then define the matrix A^f whose i, jth entry is $f(a_{ij})$ if $a_{ij} \leq n$ and 'x' otherwise. The communication complexity of the protocol depends on the number of distinct rows and columns of A^f. The main difficulty in proving bounds is the fact that we do not know the structure of A^f explicitly, its entries are defined through the Chinese Remainder Theorem. Further, the size of the matrix A^f is $3^{k_3} \times 2^{k_2}$. When 2^{k_2} and 3^{k_3} are $\Omega(n)$, the matrix has $\Omega(n^2)$ entries of which only $n+1$ are 0-1 entries and all the rest are 'x's. Hence even the task of proving deterministic lower bounds is not trivial. In all our lower bound arguments, we first choose a submatrix of A^f whose entries can be computed explicitly and show that it has sufficiently many distinct rows or columns. Using this technique, we show that any symmetric polynomial that weakly represents Mod_r over $\mathbb{Z}_{pq}$ has degree $\Omega(n)$ provided $(r,p) = (r,q) = 1$ and $r > \min(p, q)$. We also show that every symmetric polynomial weakly representing the threshold function T_k over $\mathbb{Z}_{pq}$ has degree $\Omega(\max(k, \sqrt{n}))$ for $k \leq \frac{n}{pq}$.

These techniques will not work for t-player protocols since now the fraction of 0-1 entries is even smaller. However we do obtain a linear lower bound for the Mod_r function even in the t-player case for sufficiently large r. This result is proved by a reduction to computing the function Exactly-r in the number on the forehead model. In [CFL83] Chandra, Furst and Lipton show a lower bound of $\omega(1)$ on this function which proves to be sufficient for our purpose. This reduction is surprising since in our definition of t player protocols, each player only sees her own input.

Finally we also give simple proofs of known lower bounds on strong representations for symmetric polynomials. We also show a separation between strong and weak representations by constructing a function f which can be weakly represented by polynomials of degree $\sqrt{n}$ but both f and $\overline{f}$ need degree $\Omega(n)$ for strong representation.

1.3 Upper Bounds

We show a connection between strong representation of constant threshold functions and a well studied family of Diophantine equations related to Catalan's Conjecture. Catalan (1844) conjectured that 8 and 9 are the only two consecutive positive integers which are both perfect powers. This conjecture was recently proved by Mihailescu in 2002. The case of powers of primes (which is the case we use) was known earlier [Le77]. Pillai (1945) conjectured that for fixed non-zero integers a, b and c, the more general equation

$$ax^l - by^m = c \qquad l, m, x, y \in \mathbb{Z}$$

with $l, m, x, y > 1$ and $lm > 4$ has only finitely many solutions. This conjecture is still open to the best of our knowledge. However, with $x = p$ and $y = q$ also fixed, the equation

$$ap^l - bq^m = c \tag{1}$$

and $l, m > 1$ and $lm > 4$, has only finitely many solutions in l, m [ST86]. We use this to show that for any constant $\epsilon > 0$ and for sufficiently large n, there exist polynomials of degree ϵn strongly representing T_c. Conversely, we show that the fact that the degree is $o(n)$ implies that the number of solutions to equation (1) is finite. The best lower bound we can show for T_c is $\sqrt{n}$. Closing this gap is related to some asymptotic questions regarding equation (1).

1.4 Randomized Protocols

We investigate protocols where the players are allowed access to a shared random string. This corresponds to picking a random polynomial from a space of symmetric polynomials of bounded degree over $\mathbb{Z}_m$. We consider one and two sided error in both strong and weak representations. We construct a number of protocols for threshold k over $\mathbb{Z}_6$ of cost $\max(k, \sqrt{n})$ which equals the deterministic lower bound for both strong and weak protocols. These protocols are constructed by reducing the problem to designing public coin protocols for EQ and NEQ. Also, we show that any randomized protocol for the OR function has degree $\sqrt{n}$. Since the OR function can be probabilistically represented by general polynomials of degree 1, this shows that in the context of probabilistic polynomials, asymmetric polynomials are provably stronger than symmetric polynomials.

2 Symmetric Polynomials and Simultaneous Protocols

In this section we establish a relation between low degree symmetric polynomials over $\mathbb{Z}_m$ and certain communication protocols. We denote the ring of symmetric polynomials in n variables over $\mathbb{Z}_m$ by $\mathbb{Z}_m[X_1, \cdots X_n]^S$ or $\mathbb{Z}_m[X]^S$. The elementary symmetric polynomials $S_1, \cdots S_n$ are defined as follows.

$$\begin{aligned} S_1 &= \sum_i X_i \\ S_k &= \sum_{i_1 \neq i_2 \cdots \neq i_k} X_{i_1} X_{i_2} \cdots X_{i_k} \\ S_n &= \prod_i X_i \end{aligned}$$

Theorem 2.1 *[La92] The ring $\mathbb{Z}_m[X]^S$ is generated by the elementary symmetric polynomials $S_1, \cdots S_n$. If $P[X] \in \mathbb{Z}_m[X]^S$ has degree at most d, it can be expressed as a polynomial over $\mathbb{Z}_m$ in $S_1, \cdots S_d$.*

Given a symmetric polynomial $P[X] \in \mathbb{Z}_m[X]^S$, it computes a function $f : \{0,1\}^n \to \mathbb{Z}_p$ which is defined by $f(X) = P(X)$. Alternately, since f is symmetric, it is a function only of the weight $w(X)$ of the input. So we can think of f as a function from $w \in \{0, 1 \cdots n\}$ to $\mathbb{Z}_m$.

2.1 Polynomials over $\mathbb{Z}_p$

Lucas' theorem is a classical result in number theory which allows us to evaluate binomial coefficients efficiently modulo a prime p.

Theorem 2.2 *[Gra97]* **Lucas' Theorem:** *Let* $w = \sum_{i\geq 0} w_i p^i$, $k = \sum_{i\geq 0} k_i p^i$. *Then*

$$\binom{w}{k} = \prod_i \binom{w_i}{k_i} \bmod p$$

Corollary 2.3 *For fixed* $k < p^l$, $\binom{w}{k} \bmod p$ *is a function of only the first* l *digits of* w *in base* p.

Proof: By Lucas' theorem $\binom{w}{k} = \prod_i \binom{w_i}{k_i} \bmod p$. But $k < p^l$. So $k_i = 0\ \forall i \geq l$. Hence $\binom{w}{k} = \prod_{i=0}^{l-1} \binom{w_i}{k_i} \bmod p$. ▮

Theorem 2.4 *Let* $f : \{0,1\}^n \rightarrow \mathbb{Z}_p$ *be function computed by a polynomial* $P[X] \in \mathbb{Z}_p[X]^S$ *of degree* $d < p^l$. *Then* f *is a function of the first* l *digits of* w *written in base* p.

Proof: We can write $P[X]$ as a polynomial in $S_1, \cdots S_d$. For $1 \leq k \leq d$, the value of S_k on an input of weight w is $\binom{w}{k}$ which depends only on the first l digits of w by 2.3. Hence the value of $P[X]$ on a $0, 1$ input depends only on the first l digits of w in base p. ▮

This correspondence goes both ways, any function that depends on only a few bits of the weight can computed by a low degree symmetric polynomial.

Theorem 2.5 *Let* $f : \{0,1\}^n \rightarrow \mathbb{Z}_p$ *be a function which depends only on the first* l *digits of* w *in base* p. *Then* f *is computed by a polynomial* $P \in \mathbb{Z}_p X^S$ *whose degree is less than* p^l.

Proof: We can regard f as a function from $w_0, \cdots w_{l-1}$ to $\mathbb{Z}_p$ where $w_i \in \mathbb{Z}_p$. Hence f can be written as a polynomial P' in $w_0 \cdots w_k$ over $\mathbb{Z}_p$. But by Lucas' theorem, we can write each w_i as a polynomials in the inputs $X_1, \cdots X_n$, since $S_{p^i}[X_1 \cdots X_n] = w_i$. Hence we get a polynomial $P[X_1, \cdots X_n] = P'[S_1, \cdots S_{p^{l-1}}]$ which is a symmetric polynomial generated by $S_1 \cdots S_{p^{l-1}}$. Hence $deg(P) < p^l$. ▮

2.2 Polynomials over $\mathbb{Z}_{p^a}$

Over $\mathbb{Z}_{p^a}$ a similar relation holds between low degree symmetric polynomials and functions that depend on only a few bits of the weight. The proofs however are more involved.[3] We first show that low degree polynomials depend on only a few bits of the base p representation of the weight.

[3] We recommend reading just the statements of theorems 2.9 and 2.11 and skipping the rest of this subsection on first reading

Theorem 2.6 *[Gra97]* **Kummer's Theorem:** *The largest power of p that divides $\begin{pmatrix} n \\ k \end{pmatrix}$ equals the number of carries when k and $n-k$ are added in base p.*

Corollary 2.7 *If $0 < k < p^l$, $\begin{pmatrix} p^{l+a-1} \\ k \end{pmatrix} \equiv 0 \bmod p^a$.*

Proof: Let $k = \sum_i k_i p^i$. $k_i = 0$ for $i \geq l$. Hence when we add k and $(p^{l+a-1} - k)$ we get at least a carries. By Kummer's theorem, p^a divides $\begin{pmatrix} p^{l+a-1} \\ k \end{pmatrix}$. ▮

Corollary 2.8 *If $k < p^l$, $\begin{pmatrix} w \\ k \end{pmatrix} \bmod p^a$ depends only on the first $l+a-1$ digits of w in base p.*

Proof:

$$\begin{aligned} \begin{pmatrix} w + p^{l+a-1} \\ k \end{pmatrix} &= \sum_{j=0}^{k} \begin{pmatrix} w \\ k \end{pmatrix} \begin{pmatrix} p^{l+a-1} \\ j \end{pmatrix} \\ &\equiv \begin{pmatrix} w \\ k \end{pmatrix} \bmod p^a \end{aligned}$$

since corollary 2.7 states that $\begin{pmatrix} p^{l+a-1} \\ j \end{pmatrix}$ vanishes for all other values of j. Hence $\begin{pmatrix} w \\ k \end{pmatrix}$ has period $p^{l+a-1} \bmod p^a$ which implies that its value depends on only the first $l+a-1$ bits of w in base p. ▮

Theorem 2.9 *Let $f : \{0,1\}^n \rightarrow \mathbb{Z}_{p^a}$ be a function computed by $P[X] \in \mathbb{Z}_{p^a}[X]^S$ where $deg(P) = d < p^l$. Then f is a function of just the first $l+a-1$ digits of w in base p.*

Proof: We can write f as a polynomial in $S_1 \cdots S_d$ whose value on a $0,1$ input depends on just the first $l+a-1$ digits of w in base p. ▮

We now show that a function that looks at just a few bits of the weight can be computed by a low degree polynomial. Note that it is not obvious that every such function can be computed by some polynomial. Over $\mathbb{Z}_p$ Lucas' theorem gave a simple way to extract the k^{th} bit of the weight base p using a polynomial. We now have the k^{th} bit mod p^a and need to reduce it mod p.

Lemma 2.10 *There exist polynomials $\Delta_0(X), \cdots \Delta_{p-1}(X) \in \mathbb{Z}_{p^a}[X]$ of degree at most pa so that $\Delta_i(x) \equiv 1 \bmod p^a$ if $x \equiv i \bmod p$ and 0 otherwise.*

Proof: Consider the polynomial $X^{\phi(p^a)}$. If $x \not\equiv 0 \bmod p$, then $x \in \mathbb{Z}_{p^a}^*$ hence $x^{\phi(p^a)} \equiv 1 \bmod p^a$. If $x \equiv 0 \bmod p$, then $x^{\phi(p^a)} \equiv 0 \bmod p^a$. Hence we can take $\Delta_0(X) = 1 - X^{\phi(p^a)}$ and $\Delta_i(X) = \Delta_0(X - i)$. To prove the bound on the degree, observe that the polynomial

$$Q(X) = X^a \cdot (X-1)^a \cdots (X-p+1)^a$$

is a monic polynomial of degree pa which is identically 0 on $\mathbb{Z}_{p^a}$. Hence we can divide $\Delta_i(X)$ by $Q(X)$ and the reminder is a polynomial of degree less than pa which represents the same function on $\mathbb{Z}_{p^a}$. ▮

Theorem 2.11 *Let $f : \{0,1\}^n \to \mathbb{Z}_{p^a}$ be a symmetric function which depends only on the first k digits of $w(X)$ in base p. Then f is computed by $P(X) \in \mathbb{Z}_{p^a}[X]^S$ where $deg(P) < p^{k+1}a$.*

Proof: By Lucas' theorem

$$\binom{w}{p^j} \equiv w_j \bmod p$$

Hence by lemma 2.10

$$\Delta_c(S_{p^j}(X)) \equiv 1 \bmod p^a \iff S_{p^j}(X) \equiv c \bmod p \iff \binom{w(X)}{p^j} \equiv c \bmod p$$

Hence by Lucas' theorem $w_j = c$. Thus we get a polynomial over Z_{p^a} which is one only when the j^{th} digit is c. Similarly we construct a polynomial that is 1 only for a particular setting of the first k digits of w.

$$\prod_{j=0}^{k-1} \Delta_{c_j}(S_{p^j}(X)) \equiv 1 \bmod p^a \iff \Delta_{c_j}(S_{p^j}(X)) \equiv 1 \bmod p^a \ \forall j \iff w_j = c_j \ \forall j$$

The desired polynomial is now given by

$$P(X) = \sum_{c_0,\cdots c_{k-1}} \left(f(c_o, \cdots c_{k-1}) \cdot \prod_{j=0}^{k-1} \Delta_{c_j}(S_{p^j}(X)) \right)$$

The degree of this polynomial is bounded by

$$\sum_{j=0}^{k-1} pa \cdot p^{k-1} \leq p^{k+1}a$$

▮

2.3 Polynomials and Protocols over $\mathbb{Z}_m$

The results of the previous section allow a simple interpretation of symmetric polynomials over $\mathbb{Z}_m$ for any m. For convenience we state our results for $m = 6$. We first introduce some definitions.

Definition 2.12 *A polynomial $P[X] \in \mathbb{Z}_m[X]^S$ strongly represents $f : \{0,1\}^n \to \{0,1\}$ if*

- $f(x_1, \cdots x_n) = 0 \Rightarrow P(x_1, \cdots x_n) = 0$
- $f(x_1, \cdots x_n) = 1 \Rightarrow P(x_1, \cdots x_n) \neq 0$

$\delta(f)$ denotes the lowest degree of a symmetric polynomial that strongly represents f.

Definition 2.13 *A polynomial $P[X] \in \mathbb{Z}_m[X]^S$ weakly represents $f : \{0,1\}^n \to \{0,1\}$ if*

$$f(x_1, \cdots x_n) \neq f(y_1, \cdots y_n) \Rightarrow P(x_1, \cdots x_n) \neq P(y_1, \cdots y_n)$$

$\Delta(f)$ denotes the lowest degree of a symmetric polynomial that weakly represents f.

A weak representation for f is also a representation for f^c and so $\Delta(f) = \Delta(f^c)$, but this may not hold for $\delta(f)$. A strong representation is a special case of a weak representation hence $\Delta(f) \leq \min(\delta(f), \delta(f^c))$.

Definition 2.14 *A strong protocol for computing $f : w \in \{0, \cdots n\} \to \{0,1\}$ is a protocol involving two players P_2 and P_3. The two players cannot directly communicate but they can agree on a procedure beforehand.*

- *P_3 is given $i = w \bmod 3^{k_3}$ as input and outputs $P_3(i) \in \mathbb{Z}_3$.*
- *P_2 is given $j = w \bmod 2^{k_2}$ as input and outputs $P_2(j) \in \mathbb{Z}_2$.*
- *If $f(w) = 0$, $P_3(w) = 0$ and $P_2(w) = 0$.*
- *If $f(w) = 1$, $P_3(w) \neq 0$ or $P_2(w) \neq 0$.*
- *The cost of the protocol is $\max(2^{k_2}, 3^{k_3})$.*

Definition 2.15 *A weak protocol is defined similarly except that if $f(w) \neq f(w')$, at least one of the players outputs distinct values on inputs w and w'.*

Lemma 2.16 *If there exists a symmetric function of degree d that strongly (weakly) represents f then there exists a strong (weak) protocol of cost at most $3d$ for computing f.*

Proof: Let

$$P[X] = \sum_i a_i X^{\alpha_i}$$

be a symmetric polynomial over $\mathbb{Z}_6$ that strongly(weakly) represents f. Let

$$\begin{aligned} b_i &\equiv a_i \bmod 2 \\ P_2(X) &= \sum_i b_i X^{\alpha_i} \\ c_i &\equiv a_i \bmod 3 \\ P_3(X) &= \sum_i c_i X^{\alpha_i} \end{aligned}$$

Both $P_2(X)$ and $P_3(X)$ are symmetric polynomials of degree at most d. Let $d < 2^{k_2} \leq 2d, d < 3^{k_3} \leq 3d$. By corollary 2.4 the function computed $P_2(X)$ depends on just the first k_2 bits of $w(X)$ in base 2. This function is computed by player P_2. The function corresponding to $P_3(X)$ can be computed from the first k_3 digits of $w(X)$ in base 3. This is computed by player P_3. The cost of this protocol is $\max(2^{k_2}, 3^{k_3}) \leq 3d$ ▮

Lemma 2.17 *If there exists a strong (weak) protocol of cost d that computes f then there exists a polynomial of degree at most d that strongly (weakly) represents f.*

Proof: Suppose the players read k_2 and k_3 digits respectively. The function computed by P_2 depends on only the first k_2 bits of $w(X)$. So it can be computed by a polynomial $P_2(X)$ in$\mathbb{Z}_2[X]^S$ of degree at most 2^{k_2} by corollary 2.5. Similarly the function computed by P_3 depends only of the first k_3 digits and is computed by $P_3(X)$ in $\mathbb{Z}_3[X]^S$ whose degree is less than 3^{k_3}. By The Chinese remainder theorem, there is a unique polynomial $P(X) \in \mathbb{Z}_6[X]$ which is congruent to $P_2(X)$ mod 2 and $P_3(X)$ mod 3. $P(X)$ is also symmetric and its degree is at most $\max(2^{k_2}, 3^{k_3}) = d$. ▮

We can now view both strong and weak protocols for f as simultaneous protocols in the communication complexity setting.

- P_2 and P_3 have inputs i and j and they wish to compute $f(w)$ where $w \equiv i \bmod 3^{k_3}$ and $w \equiv j \bmod 2^{k_2}$.
- The two players cannot communicate with each other. We can imagine both players see their inputs and then simultaneously write their outputs on a blackboard. A referee then reads what they have written and decides the output of the protocol.
- There are restrictions on the values that the players can output since $P_3(i) \in \mathbb{Z}_3$ and $P_2(j) \in \mathbb{Z}_2$. Hence the function should have $O(1)$ deterministic simultaneous communication complexity.

If $2^{k_2}3^{k_3} \leq n$ there might be multiple values of w between 0 and n satisfying this congruence. If f does not agree on all these values, then clearly no protocol with parameters k_2, k_3 exists. Assuming this is not the case we can define an input matrix analogous to communication complexity.

We define a $3^{k_3} \times 2^{k_2}$ matrix $A = a_{ij}$, $0 \leq i < 3^{k_3}$, $0 \leq j < 2^{k_2}$ as follows

$$\begin{aligned} a_{ij} &\equiv i \bmod 3^{k_3} \\ a_{ij} &\equiv j \bmod 2^{k_2} \\ 0 \leq\ a_{ij} &< 2^{k_2}3^{k_3} \end{aligned}$$

P_2 receives the same input j for all inputs in the same column of A and hence outputs the same value. Similarly inputs in a row are indistinguishable to P_3. For a function f, we then define the $3^{k_3} \times 2^{k_2}$ matrix A^f as follows

- If $0 \leq a_{ij} \leq n, A^f_{ij} = f(a_{ij})$.
- If $a_{ij} > n$, $A^f_{ij} = \mathrm{x}$. The symbol x indicates that the function is not defined for this value of weight.

If 2^{k_2} and 3^{k_3} are much larger than $\sqrt{n}$, many of the entries of A^f are marked x.

3 Strong Representations

3.1 Lower Bounds

Theorem 3.1 *[BBR94] The Or function can be strongly represented by a polynomial of degree $O(\sqrt{n})$ over $\mathbb{Z}_6$. Any symmetric polynomial that weakly represents the Or function has degree $\Omega(\sqrt{n})$.*

Proof: We design a strong protocol for OR of cost $\leq 3\sqrt{n}$.

Or Protocol

- Choose k_2 and k_3 so that $\sqrt{n} < 2_2^k \leq 2\sqrt{n}$ and $\sqrt{n} < 3_3^k \leq 3\sqrt{n}$.
- If $i = 0$ then $P_3(i) = 0$ else $P_3(i) = 1$.
- If $j = 0$ then $P_2(j) = 0$ else $P_2(j) = 1$.

To prove that this protocol computes the OR function, we need to show that $i = j = 0 \Rightarrow w = 0$. But

$$w \equiv 0 \bmod 2^{k_2}, \quad w \equiv 0 \bmod 3^{k_3} \quad \Rightarrow w \equiv 0 \bmod 2^{k_2}3^{k_3}$$

Also $2^{k_2}3^{k_3} > n$ but $w \leq n$. Hence $w = 0$.

To prove that this is tight for any weak protocol, if $2^{k_2}3^{k_3} \leq n$ then $i = j = 0$ for inputs of weight 0 and $2^{k_2}3^{k_3}$. Hence any protocol will output the same value on these inputs. So $2^{k_2}3^{k_3} > n \;\Rightarrow\; \min(2^{k_2}, 3^{k_3}) > \sqrt{n}$. ▮

To prove bounds better than $\sqrt{n}$ however we need stronger techniques. The value of the protocol on input a_{ij} is zero iff $P_3(i) = P_2(j) = 0$. Hence there exists a protocol for f where P_3 reads k_3 bits and P_2 reads k_2 bits iff there exist $I \subset \{0, \cdots 3^{k_3} - 1\}$ and $J \subset \{0, \cdots 2^{k_2} - 1\}$ such that

- If $f(a_{ij}) = 0$ then $i \in I, j \in J$.
- If $f(a_{ij}) = 1$ then $i \notin I$ or $j \notin J$.

In other words, all the 0s in A^f must be contained in a single rectangle. Hence we can show that such a protocol is impossible by finding a showing that any rectangle containing all the 0s must contain a 1.

Lemma 3.2 *There is a strong protocol for f where P_2 and P_3 read k_2 and k_3 digits of the weight respectively iff $\forall i,\ j$ such that $f(a_{ij}) = 1$, either there are no 0s in row i or there are no 0s in column j of A^f.*

Proof: If there exist $i,\ j$ such that $f(a_{ij}) = 1$ but there are 0s in both row i and column j of A^f, then the row player must answer 0 on row i and the column player must answer 0 on column j. Hence they both answer 0 on a_{ij} so the protocol is incorrect. We can think of the two zero entries as a fooling set. Conversely, if row i does not have any 0s, the row player can answer 0 on input i and similarly for the column player. This gives a strong protocol for f. ▮

Lemma 3.2 gives a condition to test whether a protocol with parameters k_2, k_3 exists. If a protocol does exist, the lemma guarantees that the following protocol works correctly.

Protocol

- If $\exists w \leq n$ such that $w \equiv i \bmod 3^{k_3}$ and $f(w) = 0$ then $P_3(i) = 0$. Else $P_3(i) = 1$.
- If $\exists w \leq n$ such that $w \equiv j \bmod 2^{k_2}$ and $f(w) = 0$ then $P_2(j) = 0$. Else $P_2(j) = 1$.

Define the weight function W_a as $W_a(X) = 1$ if $w(X) = a$ and 0 otherwise.

Corollary 3.3 *Every symmetric polynomial that strongly represents W_a has degree $\Omega(n)$. The function $\overline{W}_a$ is strongly represented by polynomials of degree $\Theta(\sqrt{n})$.*

Proof: Let $2^{k_2} \leq \frac{n}{2}, 3^{k_3} \leq \frac{n}{2}$. Assume $a \geq (\leq)\frac{n}{2}$. Set

$$\begin{aligned} b &= a - (+)2^{k_2} \\ c &= a - (+)3^{k_3} \end{aligned}$$

Observe that b lies in the same column as a while c lies in the same row. But now

$$\begin{aligned} f(a) &= 1 \\ f(b) &= 0 \\ f(c) &= 0 \end{aligned}$$

Hence by lemma 3.2 such a protocol does not exist. Hence $\max(2^{k_2}, 3^{k_3}) > \frac{n}{2}$. The proof that $\Delta(\overline{W}_a) = \Theta(\sqrt{n})$ is similar to the proof for OR in theorem 3.1 ▮

Corollary 3.4 *Every symmetric polynomial that strongly represents the NOR function has degree $\Omega(n)$.*

Define the threshold function T_k as $T_k(X) = 1$ if $w(X) \geq k$ and 0 otherwise.

Corollary 3.5 *Every symmetric polynomial that strongly represents T_k has degree $\Omega(\max(k, \sqrt{n}))$.*

Proof: Suppose $2^{k_2}3^{k_3} \leq n$. Choose $a < k \leq a + 2^{k_2}3^{k_3}$. Both players receive the same inputs for these weights but $T_k(a) = 0$ while $T_k(a + 2^{k_2}3^{k_3}) = 1$. This proves a lower bound of $\sqrt{n}$. Now suppose $\max(2^{k_2}, 3^{k_3}) < k$. Consider any $w > k$. Since $j \equiv w \bmod 2^{k_2}$ and $2^{k_2} < k, j < k$. Similarly $i < k$. The entry i lies in the same row as a while j lies in the same column.

$$\begin{aligned} T_k(w) &= 1 \\ T_k(i) &= 0 \\ T_k(j) &= 0 \end{aligned}$$

Now apply lemma 3.2. Hence $\max(2^{k_2}, 3^{k_3}) > k$ ▮

Corollary 3.6 *Every symmetric polynomial that strongly represents $\overline{T}_k$ has degree $\Omega(n)$ for $k \leq \frac{n}{3}$.*

Proof: Choose $l_2 \geq k_2$ such that $k \leq 2^{l_2} \leq n$. Choose $l_3 \geq k_3$ such that $k < 3^{l_3} \leq n$.

$$\begin{aligned} \overline{T}_k(0) &= 1 \\ \overline{T}_k(2^{l_2}) &= 0 \\ \overline{T}_k(3^{l_3}) &= 0 \end{aligned}$$

Hence by lemma 3.2, $\max(2^{k_2}, 3^{k_3}) > k$. ▌

Define $Mod_r(X)$ to be 1 if $w(X) \equiv 0 \bmod r$ and 0 otherwise. We can show that if $r \neq 2^a 3^b$ both Mod_r and its complement have $\delta = \Theta(n)$. If $r = 2^a 3^b$ then $\overline{Mod_r}$ has degree $O(1)$ while Mod_r has degree $\Theta(n)$. We skip the proof.

3.2 Constant Threshold Functions and Catalan's Equation

Catalan (1844) conjectured that 8 and 9 are the only two consecutive positive integers which are both perfect powers. Catalan's conjecture says that the equation

$$x^l - y^m = 1 \quad l, m, x, y \in \mathbb{Z} \tag{2}$$

with $l, m, x, y > 1$ has only one solution, $l = y = 2, m = x = 3$. Pillai (1945) conjectured that for given non-zero integers a, b and c, the more general equation

$$ax^l - by^m = c \quad l, m, x, y \in \mathbb{Z} \tag{3}$$

with $l, m, x, y > 1$ and $lm > 4$ has only finitely many solutions. However, [ST86] with a, b, p, q and c fixed positive integers,

$$ap^l - bq^m = c \tag{4}$$

and $l, m > 1$ and $lm > 4$, has only finitely many solutions in l, m. Interestingly this has the following consequence for the strong degree of threshold functions:

Theorem 3.7 *Let c be a constant. For any constant $\epsilon > 0, \exists n_0$ such that for $n > n_0$, $\delta(T_c) < \epsilon n$.*

Proof: T_1 is the Or function. We prove the theorem for $c = 2$. We use the following simple protocol.

Protocol

- If either player receives an input less than c, she outputs 0.
- If either player receives an input greater than c, she outputs 1.

We first show that this protocol works correctly if both players do not read the last digit of the weight. Hence

$$i \equiv w \bmod 3^{k_3}$$

$$\begin{array}{rcl} j & \equiv & w \bmod 2^{k_2} \\ 3^{k_3} < & n & \leq 3^{k_3+1} \\ 2^{k_2} < & n & \leq 2^{k_2+1} \end{array}$$

We must prove that there does not exist w such that $w \geq 2$, $i \leq 1$ and $j \leq 1$. There are four cases to consider.

1. $i = 0$ and $j = 0$. But then $w \equiv 0 \bmod 2^{k_2}3^{k_3}$. Hence $w = 0$.
2. $i = 1$ and $j = 1$. But then $w - 1 \equiv 0 \bmod 2^{k_2}3^{k_3}$. Hence $w = 1$.
3. $i = 1$ and $j = 0$. If the most significant digit of w in base 3 is 2, then $w = 2 \cdot 3^{k_3} + 1$, which is odd but on the other hand $w = 2^{k_2}$, which is even. If the last bit of w in base 3 is 1, then

$$w = 2^{k_2} = 3^{k_3} + 1 \Rightarrow 2^{k_2} - 3^{k_3} = 1$$

   But the only successive powers of $2, 3$ are $8, 9$ [ST86]. So for n sufficiently large this cannot happen.
4. $i = 0$ and $j = 1$. Similar to case 3.

Similarly in the case when the players do not read the last d digits, we get equations of the form $a2^{k_2} - b3^{k_3} = \pm 1$, where $a < 2^d, b < 3^d$. But since equation (4) has only finitely many solutions, we can take n sufficiently large enough so that this equation cannot be true. This proves the theorem for T_2. For $c > 2$, by repeating the same argument, we get an equation of the form $a2^{k_2} - b3^{k_3} = k$ with $k < c$ which has finitely many solutions by equation (4). ▮

We show that the connection is tight in the following sense: If $\delta(T_c)$ is sufficiently small asymptotically, then for all fixed a, b, c equation (4) has only finitely many solutions in l and m.

Theorem 3.8 *For constant c, if there exists* $0 < \epsilon \leq \min(2^{-d}, 3^{-(e+1)})$ *such that* $\forall n \geq n_0$ $\delta(T_c) < \epsilon n$ *over* $\mathbb{Z}_6$*, then*

$$a2^l - b3^m = c' \tag{5}$$

has only finitely many solutions for $|a| \leq 2^d, |b| \leq 3^e$ *and* $1 \leq c' < c$.

Proof: If $\delta(T_c) \leq \epsilon n$ $\forall n > n_0$ then there exists a strong protocol P for T_c such that $\max(2^{k_2}, 3^{k_3}) \leq \epsilon n$. Now assume that there exist infinitely many solutions to equation 5 for some a, b, c'. Assume that $a, b, c' > 0$. Since there are infinitely many solutions, there exist solutions with $a2^l > n_0$. Set $n = a2^l = c' + b3^m$. Let $w = n$.

$$2^l = \frac{n}{a} \geq \frac{n}{2^d} \geq \epsilon n \geq 2^{k_2}$$

Hence $j \equiv a2^l \bmod 2^{k_2} = 0$. Similarly

$$3^m = \frac{n - c'}{b} \geq \frac{n - c'}{3^e} \geq \frac{n}{3^{e+1}} \geq \epsilon n \geq 3^{k_3}$$

Hence $i \equiv c' + b3^m \bmod 3^{k_3} = c'$. But now

$$\begin{aligned} f(w) &= 1 \\ f(0) &= 0 \\ f(c') &= 0 \end{aligned}$$

Hence by lemma 3.2 a protocol does not exist. If the solution was such that $a, b < 0$ while $c' > 0$, we could take $n = -b3^m = c' - a2^l$ and reach a similar contradiction. So there can exist only finitely many solutions to equation (5). An analogous result holds for general p and q. ▮

Currently the best lower bound we can show for T_c is $\sqrt{n}$, so there is a substantial gap between the upper and lower bounds. Closing this gap relates to some asymptotic questions about equation (4). We discuss this in detail in section 6.

4 Weak Representations

4.1 Lower Bounds for Mod_r

We use the following classical result about simultaneous communication to prove lower bounds on weak protocols.

Lemma 4.1 *There exists a weak protocol for f with parameters (k_p, k_q) iff the matrix A^f has at most p distinct columns and q distinct rows.*

Proof: The column player receives $i \equiv w \bmod p^{k_p}$ as input and outputs a value over $\mathbb{Z}_p$. If the number of distinct columns exceeds p, then there are two distinct rows j and j' on which the row player gives the same output. But there is a row index i on which these two rows differ. Now consider the inputs a_{ij} and $a_{ij'}$. The values of the function at these inputs are different, but both players output the same value contradicting the definition of a weak protocol. A similar argument holds for the number of rows. Conversely, if there are at most p distinct columns, the column player can assign a different output for each type of column. Similarly for the row player. It is easy to see that this gives a valid protocol. ▮

Since the matrix A^f has some entries marked 'x', we need to specify what it means to have at most p distinct columns and q distinct rows. We mean that there is a way to set the x's to 0 or 1 so that the resulting matrix satisfies this condition.

Theorem 4.2 *Let $(r, p) = (r, q) = 1$ and $r > min(p, q)$. Any symmetric polynomial that weakly represents Mod_r over $\mathbb{Z}_{pq}$ has degree $\Omega(n)$.*

Proof: For convenience we consider the case $r = 5, p = 2, q = 3$. The general case is similar. The values of k_2 and k_3 will be determined later. We exhibit a 3×3 submatrix V of A such that V^f is the identity matrix.

$$V = \begin{pmatrix} 0 & a_1 2^{k_2} & a_2 2_2^k \\ b_1 3^{k_3} & a_1 2^{k_2} + b_1 3^{k_3} & a_2 2^{k_2} + b_2 3^{k_3} \\ b_2 3^{k_3} & a_1 2^{k_2} + b_2 3^{k_3} & a_2 2^{k_2} + b_2 3^{k_3} \end{pmatrix}$$

Elements in the same row of V have the same residue modulo 3^{k_3} and elements in a column have the same residue modulo 2^{k_2}. So V is a sub matrix of A. Since $2^{k_2} \neq 0 \bmod 5$, we can find $a_1, a_2 < 5$ so that

$$\begin{aligned} a_1 2^{k_2} &\equiv 1 \bmod 5 \\ a_2 2^{k_2} &\equiv 2 \bmod 5 \end{aligned}$$

Similarly since $3^{k_3} \neq 0 \bmod 5$, we can find $b_1, b_2 < 5$ so that

$$\begin{aligned} b_1 3^{k_3} &\equiv -1 \bmod 5 \\ b_2 3^{k_3} &\equiv -2 \bmod 5 \end{aligned}$$

To ensure that all entries are at most n, we set $4(2^{k_2} + 3^{k_3}) \leq n$. To satisfy this, we can take $\frac{n}{16} \leq 2^{k_2} \leq \frac{n}{8}$ and $\frac{n}{24} \leq 3^{k_3} \leq \frac{n}{8}$. Hence $\min(2^{k_2}, 3^{k_3}) \geq \frac{n}{24}$. Hence

$$V^f = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

Hence if $\max(2^{k_2}, 3^{k_3}) \leq \frac{n}{24}$ then A^f has at least 3 different columns and a weak protocol cannot exist by lemma 4.1. ▮

Corollary 4.3 *Let $s = p^a q^b r$ where $(r, p) = (r, q) = 1$ and $r > min(p, q)$. Any symmetric polynomial that weakly represents* mod$s$ *over $\mathbb{Z}_{pq}$ has degree $\Omega(n)$.*

The proof is exactly the same as the previous one.

Our proof requires $r > \min(p, q)$. We cannot for instance show that Mod_2 is hard over $\mathbb{Z}_{15}$. While this is probably true, to prove a lower bound, we will need to choose a different submatrix as it is easy to verify that a simple protocol exists for the inputs in V.

4.2 Multi-player Protocols for Mod_r

We now consider the case when m has $t > 2$ distinct prime factors and protocols involve t players. As a first attempt we could try and apply the rank lower bound to a two dimensional sub matrix of the input. However these sub matrices are very sparse and contains mainly x's, so this approach is unlikely to work. We show a lower bound for the t player case by a reduction to the function Exactly-r in the number on the forehead model. There is a lower bound of $\omega(1)$ on the deterministic complexity of Exactly-r due to Chandra, Furst and Lipton [CFL83]. The reduction seems surprising since in our definition of t player protocols, each player only sees her own input. We first need some results from the number on the forehead model. Here there are t players $P_1, \cdots P_t$ and t inputs $x_1, \cdots x_t$ and player P_j receives inputs x_i $\forall i \neq j$. They wish to compute some function $f(x_1, \cdots x_t)$.

Definition 4.4 *For $x_1 \cdots x_n \in \{0, \cdots r-1\}$, the Exactly-r function $E_r^t(x_1, \cdots x_t) = 1$ iff $\sum_{i=1}^{t} x_i = r$.*

Theorem 4.5 *[CFL83] The deterministic complexity of the Exactly-r function $D(E_r^t(x_1, \cdots x_t))$ is $\omega(1)$.*

Here $\omega(1)$ means that for t fixed, the value of $D(E_r^t(x_1, \cdots x_t))$ goes to infinity as r tends to infinity. We now define the Mod-r function in the number on the forehead model which should not be confused with the Mod_r function.

Definition 4.6 *For $x_1 \cdots x_t \in \{0, \cdots r-1\}$, the Mod-r function $M_r^t(x_1, \cdots x_t) = 1$ iff $\sum x_i \equiv 0 \bmod r$.*

Lemma 4.7 *The deterministic complexity of the Mod-r function $D(M_r^t(x_1, \cdots x_t))$ is $\omega(1)$.*

Proof: We reduce the Exactly-r problem to the Mod-r problem. Assume that there is a protocol for Mod-r. We will show that we can use it to compute the Exactly-r function at the cost of just one more bit of communication. Let $S = \sum_{i=1}^{t} x_i$. P_1 computes $s_1 = \sum_{i=2}^{t} x_i$. If $s_1 = 0$ then since $0 \leq x_1 < r$, $S < r$. If $s_1 > r$, then $S > r$. In either case, $E_r^t(x_1, \cdots x_t) = 0$. Hence P_1 writes a special output on the board. On the other hand, if $0 < s_1 \leq r$, then $0 < S < 2r$. Hence if $M_r^t(x_1, \cdots x_t) = 1$, then $S = r$, hence $E_r^t(x_1, \cdots x_t) = 1$. Hence the players can run the protocol for E_r^t and the referee outputs the appropriate value. Hence $D(E_r^t) \leq D(M_r^t) + 1$. But now by theorem 4.5, $D(M_r^t) = \omega(1)$. ▮

We are now ready to prove a lower bound for Mod_r in the t player case. For convenience, we consider the case of $\mathbb{Z}_{30}$. The protocols now have three players P_2, P_3 and P_5 who receive $y_2 = w \bmod 2^{k_2}, y_3 = w \bmod 3^{k_3}$ and $y_5 = w \bmod 5^{k_5}$ respectively.

Theorem 4.8 *There exists r_0 such that $\forall r > r_0$ and $(r,2) = (r,3) = (r,5) = 1$, any symmetric polynomial that weakly represents $\bmod r$ over $\mathbb{Z}_{30}$ has degree $\Omega(n)$.*

Proof: We use a fooling set comprising of inputs $a2^{k_2} + b3^{k_3} + c5^{k_5}$ where $a, b, c \in \{0, \cdots r-1\}$. The inputs received by P_2, P_3 and P_5 respectively are

$$\begin{aligned} u &\equiv b3^{k_3} + c5^{k_5} \bmod 2^{k_2} \\ v &\equiv a2^{k_2} + c5^{k_5} \bmod 3^{k_3} \\ w &\equiv a2^{k_2} + b3^{k_3} \bmod 5^{k_5} \end{aligned}$$

We may as well give P_2 $b3^{k_3}$ and $c5^{k_5}$ since the value of u can be computed from this. Since $(3^{k_3}, r) = (5^{k_5}, r) = 1$, and $b, c \in \{0, \cdots r-1\}$, it is sufficient to give P_2 the inputs

$$\begin{aligned} x_2 &\equiv b3^{k_3} \bmod r \\ x_3 &\equiv c5^{k_5} \bmod r \end{aligned}$$

The values of $b3^{k_3}$ and $c5^{k_5}$ can be recovered from x_2 and x_3 respectively. Similarly set $x_1 \equiv a2^{k_2} \bmod r$. We now have a reduction to the problem of computing $M_r^3(x_1, x_2, x_3)$ in the number in the forehead model with some added restrictions. We want a simultaneous protocol, and P_2, P_3 and P_5 can write only $2, 3$ and 5 distinct outputs respectively. Overall the communication complexity of the protocol must be less than 5 bits since $2^5 = 32$. However by lemma 4.7, for $r > r_0$, $D(M_r^t) > 5$. Hence for $r > r_0$ a weak protocol cannot exist provided all the entries in our fooling set are no larger than n. The largest entry is bounded by $r(2^{k_2} + 3^{k_3} + 5^{k_5})$. So we set each of $2^{k_2}, 3^{k_3}, 5^{k_5} < \frac{n}{3r}$. This gives a bound on the degree of $\frac{n}{15r}$. In general over $\mathbb{Z}_m$ where m has t distinct prime factors, the largest of which is p_t, the value of r_0 depends on t and m and the bound we get is $\frac{n}{tp_t r}$. ▮

4.3 Lower Bounds for Threshold

We show a lower bound for Threshold functions in the two player case.

Theorem 4.9 *Every symmetric polynomial weakly representing the threshold function T_k over $\mathbb{Z}_{pq}$ has degree $\Omega(\max(k, \sqrt{n}))$ for $k \leq \frac{n}{pq}$.*

Proof: Since a lower bound of $\sqrt{n}$ is easy to show for all k, we assume that $k > \sqrt{n}$. We consider the case of $\mathbb{Z}_6$. Let $2^{k_2}, 3^{k_3} < k$ and let $3^{k_3+1} \geq k$. We define

$$\begin{aligned} \overline{a} &\equiv 3^{k_3+1} \bmod 2^{k_2} \\ \overline{2a} &\equiv 2 \cdot 3^{k_3+1} \bmod 2^{k_2} \end{aligned}$$

Since $2^{k_2} < k$, $\overline{a} < k$ and $\overline{2a} < k$. Now set

$$V = \begin{pmatrix} 0 & 3^{k_3+1} & 2 \cdot 3^{k_3+1} \\ \times & \overline{a} & \overline{a} + 3^{k_3+1} \\ \times & \times & \overline{2a} \end{pmatrix} \Rightarrow V^f = \begin{pmatrix} 0 & 1 & 1 \\ \times & 0 & 1 \\ \times & \times & 0 \end{pmatrix}$$

Clearly V^f has at least three distinct rows for all settings of the $\times$s. To ensure that the entries of V are at most n we need $2.3^{k_3+1} < n$. This is possible provided $k \leq \frac{n}{6}$. In the case of $\mathbb{Z}_{pq}$, we can construct a similar matrix of size $(p+1) \times (p+1)$ provided $k \leq \frac{n}{pq}$. ▮

4.4 Separating Strong and Weak Representations

We construct a function f for which $\Delta(f) = O(\sqrt{n})$ whereas $\delta(f)$ and $\delta(\overline{f})$ are $\Theta(n)$. Choose l_2, l_3 such that $\sqrt{n} < 2^{l_2} \leq 2\sqrt{n}$ and $\sqrt{n} < 3^{l_3} \leq 3\sqrt{n}$. Define $f : \{0, \cdots, n\} \to 0, 1$ by $f(w) = 1$ if exactly one of 2^{l_2} and 3^{l_3} divides w. Note that since $0 \leq w \leq n < 2^{l_2}3^{l_3}$, if both 2^{l_2} and 3^{l_3} divide w, then $w = 0$. So equivalently, $f(w) = 1$ if $w \neq 0$ and exactly one of 2^{l_2} and 3^{l_3} divides w.

Lemma 4.10 *Every polynomial that strongly represents the function $f(\overline{f})$ has degree $\Omega(n)$.*

Proof: Let $2^{k_2} + 3^{k_3} \leq n$. Set $m_2 = \max(k_2, l_2)$ and $m_3 = \max(k_3, l_3)$. Observe that

$$\begin{aligned} 2^{m_2} &\equiv 0 \bmod 2^{l_2} \\ 2^{m_2} &\not\equiv 0 \bmod 3^{l_3} \end{aligned}$$

$$\begin{aligned}3^{m_3} &\equiv 0 \bmod 3^{l_3}\\ 3^{m_3} &\not\equiv 0 \bmod 2^{l_2}\\ 2^{m_2}+3^{m_3} &\not\equiv 0 \bmod 2^{l_2}\\ 2^{m_2}+3^{m_3} &\not\equiv 0 \bmod 3^{l_3}\end{aligned}$$

We now consider the matrix

$$V = \begin{pmatrix} 0 & 3^{m_3} \\ 2^{m_2} & 2^{m_2}+3^{m_3} \end{pmatrix}$$

Hence

$$V^f = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \quad V^{\bar{f}} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

Hence by 3.2, such a protocol cannot exist. $\blacksquare$

Weak Protocol for f

- Set $k_2 = l_2$ and $k_3 = l_3$. Hence $i \equiv w \bmod 2^{l_2}$ and $j \equiv w \bmod 3^{l_3}$.
- If $i = 0$ then $P_3(i) = 0$ else $P_3(i) = 1$.
- If $j = 0$ then $P_2(j) = 0$ else $P_2(j) = 1$.
- The output of the protocol is 1 if $P_3(i) = P_2(j)$ and 0 if $P_3(i) \neq P_2(j)$.

It is easy to see that the above protocol computes f. The cost of the protocol is $O(\sqrt{n})$.

5 Randomized Protocols

Simultaneous protocols where the players have access to a shared random string are well studied in communication complexity [BKL95]. Such protocols are of interest to us since they have can be interpreted as selecting a symmetric polynomial at random from a sample space of symmetric polynomials. We use the fact that the matrix A^f for T_k is similar to the matrix for EQ to give a number of randomized protocols for the threshold function. These protocols match the best deterministic lower bounds shown in lemma 3.5 and theorem 4.9. We are unable to show any non trivial lower bounds for such protocols though we believe they exist for functions like Mod_5 over Z_6.

5.1 Types of Protocols

Definition 5.1 *[Tar93] A sample space of polynomials probabilistically represents a Boolean function if on every input, a randomly chosen polynomial from the space computes the function correctly with good probability.*

Definition 5.2 *A randomized protocol is a protocol where P_2 and P_3 have access to a shared random string. P_2 reads the first k_2 bits of the input in base 2 and P_3 reads the first k_3 digits in base 3. Each of them computes some function of the input bits and the bits of the random string. The cost of the protocol is defined as* $\max(2^{k_2}, 3^{k_3})$.

Lemma 5.3 *Choosing a polynomial from a sample space of symmetric polynomials of degree $\leq d$ is equivalent to a randomized protocol of cost d.*

Proof: Each polynomial in the sample space corresponds to a deterministic protocol. Hence choosing a random polynomial is equivalent to choosing a random protocol from a space of protocols. We can imagine the players having access to a public string of random bits which allows them to choose a protocol from a space of protocols. The function that each player computes is some function of the input bits read and the shared random bits. Private coins are clearly not sufficient since the players do not pick their protocols independently. ▌

We can define both strong and weak randomized protocols with both one and two sided error. Let us first consider one sided error for strong representations. The next lemma states that to beat deterministic protocols, we must allow for some error on the 0 entries. If we insist on always getting the 0s correct, the same lower bound applies as in the deterministic case. However, for protocols that are allowed to err on 0s, this lower bound does not apply. Indeed we can design protocols (see for example lemma 5.8) that beat the best known deterministic protocols.

Lemma 5.4 *There exists a strong randomized protocol with parameters k_2 and k_3 for a function f which always answers 0 on 0 inputs and which answers 1 on 1 inputs with probability $\epsilon > 0$ iff there exists a strong deterministic protocol for f with identical parameters.*

Proof: One direction is trivial. For the other direction, by lemma 3.2 if there does not exist a deterministic protocol, then $\exists\, i, j$ so that $f(a_{ij}) = 1$ but there are 0s in row i and column j. But then in any randomized protocol that always answers 0s correctly, the row player says 0 on row i with probability 1 and the column player says 0 on column j with probability 1. Hence the protocol outputs an incorrect answer for input a_{ij} with probability 1. ▌

Hence when we consider strong protocols with one-sided error, the error is on 0 inputs. We also consider strong protocols with two-sided error and weak protocols with one and two-sided error. Unlike in the case of RP and BPP where the success probability can be amplified by repetition, running any of the above kinds of protocols twice is not always equivalent to sampling from another space of protocols. This is because the 0 and 1 sets obtained by repetition may not be rectangular partitions of the inputs. Hence, proving that a weak two sided error protocol with success probability $\frac{2}{3}$ does not exist does not rule out the possibility that there exists a protocol with success probability $\frac{3}{5}$.

5.2 Randomized Protocols for Threshold

We consider the threshold k function for various values of k. We first start with a general lower bound for any kind of randomized protocol for T_k.

Lemma 5.5 *Any randomized protocol for T_k has cost $\Omega(\sqrt{n})$.*

Proof: Suppose $2^{k_2}3^{k_3} \leq n$. Choose $i < k \leq i + 2^{k_2}3^{k_3}$. Since both players receive the same input for weights i and $i + 2^{k_2}3^{k_3}$, their output distributions will be identical but the value of T_k on these weights is different. ▮

Our upper bounds for T_k come from the observation that when $2^{k_2}, 3^{k_3} > k$, the matrix A^f looks like the matrix for equality of strings in two party communication complexity. We can imagine that each player has a *color* in $\{0, \cdots, k-1\}$ and they are trying to decide if they have the same color.

Lemma 5.6 *There is a strong randomized protocol P_1 of cost $O(\max(k, \sqrt{n}))$ with two sided error for T_k such that $\forall\ 0 < p < 1$ if $w < k$, both players say 0 with probability p and if $w \geq k$ at least one player says 1 with probability $1 - p^2$.*

Proof: Set $2^{k_2}, 3^{k_3} > \max(k, \sqrt{n})$. By setting x's to 1, the corresponding matrix A^f has its first k diagonal entries set to 0 and the rest to 1. The players wish to design a protocol so that if $i = j < k$, they both say 0, else someone says 1.

Protocol 1

- If either input is greater than k that player says 1.
- Using their shared random string, P_2 and P_3 select a random subset of colors S. Each color from $\{0 \cdots k-1\}$ is included in S independently with probability p.
- Each player says 0 if her color is in S, else she says 1.

If both players have the same color i, they both say 0 provided $i \in S$ which happens with probability p. If they have distinct colors i, j, they both answer 0 iff $i, j \in S$ which happens with probability p^2. Hence they answer 1 with probability at least $1 - p^2$. By setting $p = \frac{3}{5}$ the protocol answers correctly on all inputs with probability at least $\frac{3}{5}$. ▮

Theorem 5.7 *T_k is strongly represented by a probabilistic polynomial of degree $O(\max(k, \sqrt{n}))$ with two sided error.*

We now design a one sided error protocol for the complementary problem $\overline{T}_k$.

Lemma 5.8 *There is a strong randomized protocol for $\overline{T}_k$ whose cost is $O(\max(k, \sqrt{n}))$. The protocol always answers 1 if $w \geq k$ and answers 0 if $w < k$ with probability at least $\frac{1}{4}$.*

Proof: We want a protocol where if $i = j < k$, then one of the players says 1. If not, then with some probability they should both say 0.

Protocol 2

- If either player sees a number bigger than k, she says 0.
- P_2 and P_3 choose a random subset S of $\{0, 1 \cdots k-1\}$ by including each color in it with probability $\frac{1}{2}$.
- P_2 answers 1 on every $i \in S$ and 0 on $j \in \overline{S}$.
- P_3 answers 1 on every color in $\overline{S}$ and 0 on $j \in S$.

Suppose both players receive the same color $c < k$. Either $c \in S$ or $c \in \overline{S}$, hence one of them will always answer 1. If $i \neq j$ and $i > k$, P_2 always says 0 while P_3 says 0 if $j \notin \overline{S}$ which happens with probability at least $\frac{1}{2}$. Similarly for the case when $j \geq k$. If $i \neq j$ and $i, j < k$, then both players say 0 iff $i \notin S$ while $j \in S$ which happens with probability exactly $\frac{1}{4}$. ▮

Theorem 5.9 *$\overline{T}_k$ is strongly represented by a probabilistic polynomial of degree $O(\max(k, \sqrt{n})$ with one sided error.*

The public coin communication protocol for equality of strings gives a protocol which weakly represents T_k with one sided error.

Theorem 5.10 *T_k can be weakly represented by a probabilistic polynomial of degree $O(\max(k, \sqrt{n}))$ with one sided error.*

Proof: Again we choose $2^{k_2}, 3^{k_3} > \max(k, \sqrt{n})$.

Protocol 3

- If $i, j < k$ the players both encode their inputs using the Hadamard code. They use the public coins to select a random bit in the codeword and output that bit.
- If $i \geq k$ P_2 outputs a random bit independent of P_3. If $j \geq k$ P_3 outputs a random bit independent of P_2.
- If both players output the same bit, then the output of the protocol is 0 else it is 1.

If either player sees an input greater than k she outputs a random bit independent of the other player, hence the probability that they output the same bit is $\frac{1}{2}$. In the case when $i = j < k$, the Hadamard encodings of both inputs are the same, hence they always output the same bit. If $i \neq j$, since the relative distance of the Hadamard code is $\frac{1}{2}$, with probability $\frac{1}{2}$, the two players will output different bits. ▮

6 Conclusions

The Strong Degree of Threshold

The best lower bound for T_k in the strong representation is $\max(k, \sqrt{n})$. The only non trivial upper bound we know is $o(n)$ for constant threshold. Any improvement in either direction would be very interesting. These questions are related to (and in fact equivalent to) some interesting number theoretic questions. We shall consider the case of T_2. For every k, choose $3^{k'} < 2^k < 3^{k'+1}$. Since $(2^k, 3^{k'}) = 1$, there exist $0 < a_k < 3^{k'}$ and $0 < b_k < 2^k$ such that

$$a_k 2^k - b_k 3^{k'} = 1 \tag{6}$$

This defines sequences $a = \{a_1, a_2, \cdots\}$ and $b = \{b_1, b_2, \cdots\}$. We are interested in the asymptotic behavior of these sequences. Note that a_k and b_k are within a constant factor of each other by equation (6) and our choice of k'. Hence we can consider just the sequence a. Equation 4 implies that for any constant c, $a_k < c$ for only finitely many values of k. In other words the $\liminf(a)$ tends to ∞ as k tends to ∞. To prove a stronger upper bound, we would need to show that for some function $c(k)$ which is $\omega(1)$, there are only finitely many solutions to 6 with $a_k < c(k)$. On the other hand, finding a function $d(k)$ which is $o(2^k)$ such that for infinitely many values of k, $a_k < d(k)$ will show a lower bound of better than $\sqrt{n}$. In other words proving that $\liminf(a) < o(2^k)$ will give a better lower bound. Conversely, improving either bound will imply something about $\liminf(a)$.

Weak protocols for threshold seem harder to analyze since unlike in the strong case, the protocol is not fixed.

Threshold for $t > 2$

For $t > 2$, the best lower bound for any representation in this paper is $n^{\frac{1}{t}}$. It seems that better lower bounds should exist especially for large values of k. On the other hand, for small values of k, it seems possible that as t increases the degree may decrease. Since each player reads w in a different base, it seems harder to come up with large numbers that look small to every player.

Weak Representation of Mod_r for small r

Our bounds for weak protocols for Mod_r in both the two player and multi-player cases require r to be sufficiently large. The only cases for which upper bounds are known is when $r = p_1^{a_1} \cdots p_t^{a_t}$. It would be nice to show a lower bound of $\Omega(n)$ for all other r. For instance is there a lower bound of $\Omega(n)$ for Mod_2 over $\mathbb{Z}_{15}$?

Randomized Protocols

There exist randomized protocols for T_k that essentially equal the best deterministic lower bounds. Are there functions where randomized protocols beat the deterministic lower bounds? We also do not know any lower bounds for randomized protocols except the trivial $n^{\frac{1}{t}}$ lower bound.

References

[BKL95] L. Babai, P. Kimmel, S. V. Lokam. Simultaneous Messages vs Communication. In Proc. 12th STACS (1995) 361-372.

[BBR94] David A. Barrington, Richard Beigel, Steven Rudich. Representing Boolean Functions As Polynomials Modulo Composite Numbers Computational Complexity, 4:367–382, 1994.

[CFL83] A. Chandra, M. Furst, R. Lipton: Multi-party Protocols. In Proc. of the 15th Annual ACM Symposium on Theory of Computing, (1983) 94-99.

[Gra97] Andrew Granville. Arithmetic Properties of Binomial Coefficients, Canadian Mathematical Society Conference Proceedings, 20 (1997), 253-275.

[Gre95] Frederic Green. Complex Fourier technique for lower bounds on the Mod-m degree. Computational Complexity, 9:16–38, 2000.

[Gro95] Vince Grolmusz. On the weak mod m representation of boolean functions. Chicago Journal of Theoretical Computer Science, 1995(2).

[KN97] E. Kushilevitz, N. Nisan. Communication Complexity. Cambridge Univ. Press, 1997.

[La92] S. Lang. Algebra, Addison-Wesley, 3rd ed, November 1992.

[Le77] W. Leveque. Fundamentals of Number Theory, Addison-Wesley, 1977.

[ST86] T.N. Shorey, R. Tijdeman. Exponential Diophantine Equations, Ch. 12 The Catalan Equation and Related Equations, Cambridge University Press, 1986.

[TB95] Gabor Tardos, David A. Mix Barrington. A Lower Bound On The Mod 6 Degree Of The Or Function. Computational Complexity, 7:99–108, 1998.

[Ts96] S-C. Tsai. Lower bounds on representing boolean functions as polynomials in $\mathbb{Z}_m$, In SIAM J. Discrete Math., 9 (1996), pp. 55–62.

[Tar93] J. Tarui. Probabilistic polynomials. AC^0 functions and the polynomial time hierarchy. Theoretical Computer Science, 113:167-183. 1993.