Symmetric Polynomials over $\mathbb{Z}_m$ and Simultaneous Communication Protocols with tight bounds for Threshold Functions

Nayantara Bhatnagar*
nand@cc.gatech.edu

Parikshit Gopalan†
parik@cc.gatech.edu

Richard J. Lipton‡
rjl@cc.gatech.edu

College of Computing
Georgia Institute of Technology
Atlanta GA 30332

Abstract

We study the problem of representing symmetric Boolean functions as symmetric polynomials over $\mathbb{Z}_m$. We prove an equivalence between representations of Boolean functions by symmetric polynomials and and simultaneous communication protocols. We show that computing a function f on 0-1 inputs with a polynomial of degree d modulo pq is equivalent to a two player simultaneous protocol for computing f 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.

This equivalence allows us to show degree lower bounds by using techniques from communication complexity. For example, we show lower bounds of $\Omega(n)$ on symmetric polynomials weakly representing classes of Mod_r and Threshold functions. Previously the best known lower bound for such representations of any function modulo pq was $\Omega(n^{\frac{1}{2}})$ [BBR94]. The equivalence also allows us to use results from number theory to prove upper bounds for Threshold-k functions. We show that proving bounds on the degree of symmetric polynomials strongly representing the Threshold-k function is equivalent to counting the number of solutions to certain Diophantine equations. We use this to show an upper bound of $O(nk)^{\frac{1}{2}+\varepsilon}$ for Threshold-k assuming the *abc* conjecture. We show the same bound unconditionally for k constant. Prior to this, non-trivial upper bounds were known only for the OR function [BBR94]. We show an almost tight lower bound of $\Omega(nk)^{\frac{1}{2}}$, improving the previously known bound of $\Omega(\max(k, \sqrt{n}))$ [Tsa96].

*Research supported in part by NSF CCR-0105639
†Research supported in part by NSF CCR-0002299
‡Also with Telcordia. Supported in part by NSF CCR-0002299

1 Introduction

Representations of Boolean functions as polynomials over various rings such as $\mathbb{R}$ and $\mathbb{Z}_m$ have been well studied in computer science starting with the work of Minsky and Papert [MP68]. In addition to having applications to complexity theory and learning theory, this study has produced some surprising results and challenging open questions (see the survey by Beigel [Bei93]). One of the complexity theoretic motivations for studying polynomials over $\mathbb{Z}_m$ is to understand the power of modular counting. Razborov [Raz87] and Smolensky [Smo87] prove lower bounds for AC^0 with Mod-p gates when p is a prime. In contrast, proving lower bounds for circuits with Mod-6 gates is an important open problem. A first step towards this problem might be to better understand the computational power of polynomials over $\mathbb{Z}_6$.

In this paper, we study the problem of representing a Boolean function as a *symmetric* polynomial over $\mathbb{Z}_m$. We use the vector notation $\mathbf{X} = X_1, \cdots, X_n$. We use $\mathbf{a}, \mathbf{b}, \cdots$ to denote vectors in $\{0,1\}^n$. Let $f : \{0,1\}^n \to \{0,1\}$ denote a Boolean function. For $\mathbf{a} \in \{0,1\}^n$ let the weight be $w(\mathbf{a}) = \sum a_i$. A symmetric Boolean function is one whose value depends only on the weight of the input.

Definition 1.1 *Polynomial $P(\mathbf{X}) \in \mathbb{Z}_m[\mathbf{X}]$ strongly represents [1] function f if for $\mathbf{a} \in \{0,1\}^n$,*

$$f(\mathbf{a}) = 0 \Rightarrow P(\mathbf{a}) \equiv 0 \bmod m \qquad f(\mathbf{a}) = 1 \Rightarrow P(\mathbf{a}) \not\equiv 0 \bmod m$$

Polynomial $P(\mathbf{X}) \in \mathbb{Z}_m[\mathbf{X}]$ weakly represents function f if for $\mathbf{a}, \mathbf{b} \in \{0,1\}^n$,

$$f(\mathbf{a}) \neq f(\mathbf{b}) \Rightarrow P(\mathbf{a}) \neq P(\mathbf{b})$$

Let $\delta(f)$ denote the the smallest degree of a symmetric polynomial that strongly represents f over $\mathbb{Z}_m$. Define $\Delta(f)$ similarly for weak representations of f . We are interested in bounds on $\delta(f)$ and $\Delta(f)$ for a fixed modulus m as an asymptotic function of the number of variables n.

This study was initiated by the work of Barrington, Beigel and Rudich [BBR94] who proved the surprising result that the OR function can be strongly represented over $\mathbb{Z}_6$ by a polynomial of degree $\Theta(\sqrt{n})$. In this work, we prove an equivalence between representations of functions by symmetric polynomials over $\mathbb{Z}_m$ and certain simultaneous communication protocols. We show that computing a function f on 0-1 inputs with a symmetric polynomial of degree d modulo pq is equivalent to a two player simultaneous protocol for computing f 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. This equivalence allows us to use powerful tools from communication complexity and number theory to study such polynomial representations. We list some of our main results below.

We show $\Omega(n)$ lower bounds for weak representations of Mod and Threshold functions over $\mathbb{Z}_m$. The best lower bound previously known for $\Delta(f)$ for any function f was $\Omega(n^{\frac{1}{t}})$ where t is the number of distinct prime factors of m [BBR94]. We show that proving bounds on the degree of symmetric polynomials strongly representing the Threshold-k function T_k is equivalent to counting the number of solutions to certain Diophantine equations. We show $\delta(T_k) = \Omega(n^{\frac{1}{t}} k^{\frac{t-1}{t}})$, improving the previous lower bound of $\max(k, n^{\frac{1}{t}})$

[1] Tardos and Barrington [TB98] use the terminology *one-sided representation* for what we call *strong representation*

[Tsa96]. For constant k, we show a matching upper bound. When $t = 2$, we show that a matching upper bound holds for all values of k assuming the *abc* conjecture [GT02]. We also study randomized protocols and show that they are equivalent to representing a Boolean function by a probabilistic symmetric polynomial.

1.1 Previous Work

In this section we give the basic definitions and survey some known results about polynomial representations of functions over Z_m. In addition to strong and weak representations, we say that polynomial $P(\mathbf{X})$ 0-1 represents function f if for $\mathbf{a} \in \{0,1\}^n$, $P(\mathbf{a}) = f(\mathbf{a})$.

Such representations are easy to understand when p is a prime and $\mathbb{Z}_p$ is a field. Using the fact that every function from $\mathbb{Z}_p \to \mathbb{Z}_p$ is a polynomial, we can obtain a 0-1 representation from either a strong or a weak representation while increasing the degree only by a factor of $p - 1$. There is a unique multilinear polynomial that 0-1 represents any function f. Thus the minimum degree of any representation has to be within a factor $p - 1$ of the degree of this polynomial.

Over $\mathbb{Z}_m$ when m is not a prime power however, things are very different. If $P(X)$ 0-1 represents the OR function over $\mathbb{Z}_6$, it can be shown using the Chinese Remainder Theorem (CRT) that $P(X)$ has degree $\Omega(n)$. However it is not clear that one can obtain a 0-1 representation from a strong or a weak representation since $\mathbb{Z}_6$ is not a field. In fact, the degree of a strong or a weak representation can be very different from that of a 0-1 representation. Barrington, *et al.* [BBR94] show that $\delta(OR) = O(\sqrt{n})$ over $\mathbb{Z}_6$. They also show a lower bound of $\Omega(\sqrt{n})$ for $\delta(OR)$. It is not known if this lower bound holds for general polynomials. The best lower bound is $\Omega(\log n)$ due to Tardos and Barrington, who also conjecture that the right bound is $\Omega(\sqrt{n})$ [TB98].

Proving lower bounds is considerably easier in the strong representation. Lower bounds of $\Omega(n)$ are known in the strong representation for some functions using general (not just symmetric) polynomials [BBR94, Tsa96, Gre00]. Tsai shows a lower bound of $\Omega(k)$ on the degree of T_k for general polynomials using Moebius inversion [Tsa96]. As pointed out by [TB98] the task of proving lower bounds for strong representations 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, TB98]. Grolmusz proves a $\Omega(\log n)$ lower bound for general polynomials weakly representing the GIP function using a connection to the number on the forehead model from communication complexity [Gro95].

These polynomials also have some surprising combinatorial applications. Grolmusz uses this upper bound to construct a super-polynomial size set system where the size of each set is 0 mod 6 but all pairwise intersections are nonzero mod 6. He uses this to construct explicit Ramsey graphs whose parameters almost match the best known construction [Gro00].

1.2 Our Results

We present a sketch of the new techniques and results in this paper.

1.2.1 Symmetric Polynomials and Simultaneous Communication Protocols

The new insight in this paper is an equivalence between computing Boolean functions by symmetric polynomials modulo m and computing the functions by certain one-round simultaneous communication protocols.

A one-round simultaneous communication protocol [Yao79, KN97] involves two players Alice and Bob and a referee. Alice receives an input $\mathbf{a}$, Bob receives an input $\mathbf{b}$ and they wish to compute $f(\mathbf{a}, \mathbf{b}) \in \{0, 1\}$. They cannot directly communicate with each other. They simultaneously write messages on a blackboard. A referee reads the messages and decides the value of f. The players and the referee can agree an a strategy beforehand.

As a first step towards showing the equivalence, we consider symmetric polynomials over $\mathbb{Z}_p$. The value of a symmetric polynomial on 0-1 inputs depends only on the weight w. Thus every symmetric polynomial $P(\mathbf{X})$ over $\mathbb{Z}_p$ computes a symmetric function $f : \{0,1\}^n \to \mathbb{Z}_p$. We show that the symmetric functions $f : \{0,1\}^n \to \mathbb{Z}_p$ that can be computed by a symmetric polynomial $P[\mathbf{X}] \in \mathbb{Z}_p[X]$ of degree $d < p^l$ are exactly those functions that can be computed from the l least significant digits of w in base p. Equivalently, such functions can be computed from $w \bmod p^l$. This is a consequence of a classical result in number theory called Lucas' Theorem about binomial coefficients modulo p [Gra97]. A similar equivalence holds for prime powers.

Henceforth we will identify symmetric functions $f : \{0,1\}^n \to \mathbb{Z}_p$ with functions defined on integers $[0, 1, \cdots, n]$. We now define protocols for computing a symmetric Boolean function $f : w \in \{0, \cdots, n\} \to \{0, 1\}$.

Definition 1.2 *A strong protocol for computing f mod 6 with parameters (k_2, k_3) is a simultaneous protocol involving two players P_2 and P_3. P_2 is given $j \equiv w \bmod 2^{k_2}$ as input and outputs $P_2(j)$ in $\mathbb{Z}_2$. P_3 is given $i \equiv w \bmod 3^{k_3}$ as input and outputs $P_3(i)$ in $\mathbb{Z}_3$. If $f(w) = 0$, then both players must output 0. If $f(w) = 1$, at least one player must output a non-zero value. A weak protocol is defined similarly except that if $f(w) \neq f(w')$ then at least one of the players outputs different values on w and w'. The cost of the protocol is $\max(2^{k_2}, 3^{k_3})$.*

For m with t distinct prime factors $p_1, \cdots, p_t$, we define protocols with t players where player[2] P_i reads the input in base p_i. We can think of a strong protocol as one where the referee's strategy is fixed: he outputs 0 iff both players say 0. In a weak protocol, the referee can choose any strategy. The reason for defining the cost as above is that it equals the degree of the polynomial mod 6 that the players are computing, this is explained below.

We now make the connection between symmetric polynomials and simultaneous protocols. By the Chinese Remainder Theorem (CRT), 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. 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. Thus there is a protocol of cost $\Theta(d)$. Conversely assume there exists a protocol for f. The function computed by each player can be represented by a low degree symmetric polynomial. We now use the CRT to combine these polynomials and get a polynomial of

[2]For notational convenience, we use P_i as opposed to P_{p_i}

degree bounded by $\max(2^{k_2}, 3^{k_3})$ over $\mathbb{Z}_6$. Thus for fixed m, the minimum cost of a protocol for f equals the minimum degree of a symmetric polynomial representing f up to a constant factor depending only on m.

1.2.2 Lower Bounds

Techniques from communication complexity have been successfully applied to show lower bounds in many areas like circuit complexity, VLSI and data structures [KN97]. We show how to adapt tools from communication complexity to prove lower bounds on the degree. These tools are especially useful for weak representations. In general, proving deterministic lower bounds for simultaneous communication protocols is easy. There is a simple characterization of the deterministic communication complexity in terms of the number of distinct rows and columns of the input matrix. However, in our setting, proving lower bounds is a non-trivial task for the following reasons.

For parameters (k_2, k_3) of the protocol, we define an input matrix A^f of size $2^{k_2} \times 3^{k_3}$, where the (i,j)th entry is $f(w)$ where $w \equiv i \bmod 2^{k_2}$ and $w \equiv j \bmod 3^{k_3}$. Thus, the entries of A^f are not defined explicitly, instead they are defined through the CRT. Thus the value of the (i,j)th entry depends on the parameters (k_2, k_3). Further, we are primarily interested in proving linear lower bounds, which correspond to setting $2^{k_2}, 3^{k_3} = \Omega(n)$. The matrix A^f now has roughly n^2 entries, but only n of these correspond to valid inputs $w \leq n$.

To prove lower bounds, we carefully choose a submatrix of A^f whose entries are known explicitly and show that it has sufficiently many distinct rows or columns. We show that any symmetric polynomial that weakly represents Mod-k over $\mathbb{Z}_{pq}$ has degree $\Omega(n)$ where $k > p$ and k is relatively prime to pq. We obtain a linear lower bound for the Mod-k function when m has $t > 2$ distinct prime factors for sufficiently large k. This is proved by a reduction to computing the function Exactly-k in the *number on the forehead* model and using a lower bound by Chandra *et al.* [CFL83]. We give a necessary and sufficient condition for the existence of a strong protocol for a function f. We use this to give simple proofs of known bounds on strong representations for symmetric polynomials. We show a separation between strong and weak representations by constructing a function f which can be weakly represented by polynomials of degree $O(\sqrt{n})$ but both f and $\overline{f}$ need degree $\Omega(n)$ for strong representation.

1.2.3 Threshold Functions and Diophantine Equations

The Threshold-k function T_k is defined to be 1 if the weight of the input is at least k. We study the degree of the Threshold-k function (T_k) for various values of k. T_1 is the OR function and $\delta(T_1) = \Delta(T_1) = \Theta(\sqrt{n})$. T_n is the AND function. It is easy to show that $\delta(T_n) = \Omega(n)$, but $\Delta(T_n) = \Theta(\sqrt{n})$. This raises the question: What is the (strong/weak) degree of T_k is for $1 < k < n$?

We show that proving bounds on the degree is equivalent to showing that certain Diophantine equations have only finitely many solutions. More precisely, we show that there exists a strong protocol for T_k on n variables with parameters k_2, k_3 iff there are no non-trivial solutions to the equation

$$|a2^{k_2} - b3^{k_3}| = \ell \qquad\qquad a2^{k_2} \leq n,\ b3^{k_3} \leq n,\quad \ell < k$$

When k is a fixed constant, we show that $\delta(T_k) = O(n^{\frac{1}{2}+\varepsilon})$ for any $\varepsilon > 0$. The proof uses a result of Filaseta [Fil91] on factors of numbers of the form $n(n+d)$. We show $\delta(T_k) = O(n^{\frac{1}{t}+\varepsilon})$ when m has t distinct prime factors using a theorem due to Granville [Gra98] which is proved assuming the *abc* conjecture from number theory [GT02]. We also show that when m has only two prime divisors, the *abc* conjecture implies that $\delta(T_k) = O(nk)^{\frac{1}{2}+\varepsilon}$ for all values of k.

The $O(\sqrt{n})$ upper bound for the OR function can be interpreted as follows: For suitably chosen parameters (k_2, k_3) if $w \bmod 2^{k_2}$ and $w \bmod 3^{k_3}$ are both zero, then in fact the number w must equal 0. Our bounds for T_k give a similar result about the size of w: For suitably chosen parameters (k_2, k_3) if the residues $w \bmod 2^{k_2}$ and $w \bmod 3^{k_3}$ are both less than k, then in fact they are both equal to w itself and $w < k$. Conversely, if $w \geq k$, then one of the residues must be large.

We show a lower bound of $\Omega(n^{\frac{1}{t}} k^{\frac{t-1}{t}})$ for $\delta(T_k)$ over $\mathbb{Z}_m$. This improves the previous bound of $\Omega(\max(k, \sqrt{n}))$ [Tsa96]. When $t = 2$, the lower bound nearly matches the upper bound of $(nk)^{\frac{1}{2}+\varepsilon}$ for all values of k. These lower bounds are proved by constructing solutions to the equation above via a pigeonhole argument. Further, when $t = 2$, we also show an $\Omega(\sqrt{nk})$ lower bound for $\Delta(T_k)$.

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 construct strong and weak protocols for threshold k over $\mathbb{Z}_6$ of cost $O(\max(k, \sqrt{n}))$ which beats the deterministic lower bound of $\Omega(\sqrt{nk})$.

The rest of the paper is organized as follows. In Section 2, we establish the equivalence between polynomials and protocols. We study strong representations in Section 3 and weak representations in Section 4. In Section 5, we study representations of Threshold-k functions in depth. Section 6 discusses randomized protocols.

Preliminary versions of parts of this paper appeared in FOCS'03 [BGL03] and as ECCC TR04-22 [BGL04].

2 Symmetric Polynomials and Simultaneous Protocols

2.1 Symmetric Polynomials over $\mathbb{Z}_p$

In this section, we study functions $f : \{0,1\}^n \to \mathbb{Z}_p$. We are interested in polynomials over $\mathbb{Z}_p[X_1, \cdots, X_n]$ computing a given function f. Every function $f : \{0,1\}^n \to \mathbb{Z}_p$ is computed by a unique multilinear polynomial. This polynomial can be computed from the values of f using Moebius inversion. We use the following notation: for $B \subseteq [n]$, let $b = (b_1, \cdots, b_n)$ denote its characteristic vector where $b_i = 1$ if $i \in B$ and $b_i = 0$ otherwise.

Lemma 2.1 *[Tsa96] Every function $f : \{0,1\}^n \to \mathbb{Z}_p$ is computed by a polynomial $P(X)$ where*

$$\begin{aligned} P(X_1, \cdots, X_n) &= \sum_{A \subseteq [n]} c_A \prod_{i \in A} X_i \\ c_A &= \sum_{B \subseteq A} (-1)^{|A|-|B|} f(b) \end{aligned}$$

For the rest of the paper, we restrict ourselves to studying symmetric functions.

Definition 2.2 *A function $f : \{0,1\}^n \to \mathbb{Z}_p$ is* **symmetric** *if for every permutation σ on $[n]$,*

$$f(a_1, \cdots, a_n) = f(a_{\sigma(1)}, \cdots, a_{\sigma(n)}) \qquad \forall a \in \{0,1\}^n$$

Since a symmetric function only depends on the weight of the input, we can think of a symmetric function f as a function $f : \{0, \cdots, n\} \to \mathbb{Z}_p$. We will use these two views of symmetric functions interchangeably. Define the elementary symmetric polynomials $S_0(X), \cdots, S_n(X)$ as

$$S_0(X) = 1, \quad S_k(X) = \sum_{i_1 < i_2 \cdots < i_k} X_{i_1} X_{i_2} \cdots X_{i_k}$$

When f is symmetric, it follows from the Moebius inversion formula that the resulting polynomial $P(X)$ is symmetric. A symmetric multilinear polynomial can be written as a linear combination of the $S_i(X)$ over $\mathbb{Z}_p$. Hence

$$P(X) = \sum_{i=0}^{n} c_i S_i(X) \qquad c_i \in \mathbb{Z}_p$$

What does the degree of $P(X)$ tell us about the function f that it computes? This question can be answered using a result about binomial coefficients modulo p called Lucas' Theorem [Gra97].

Theorem 2.3 (Lucas' Theorem) *Let $w = \sum_{i \geq 0} w_i p^i$, $0 \leq w_i < p$ and $k = \sum_{i \geq 0} k_i p^i$, $0 \leq k_i < p$. Then*

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

Lemma 2.4 *Let $k < p^\ell$. On input $a \in \{0,1\}^n$ of weight w, $S_k(a)$ is a function of only the ℓ least significant digits $w_0, \cdots, w_{\ell-1}$.*

Proof: On an input $a \in \{0,1\}^n$ of weight w, by Lucas' Theorem

$$S_k(a) \;=\; \binom{w}{k} \;\equiv\; \prod_i \binom{w_i}{k_i} \bmod p$$

However $k < p^l$, so $k_i = 0$ for $i \geq l$. Hence

$$\binom{w}{k} \;\equiv\; \prod_{i=0}^{l-1} \binom{w_i}{k_i} \prod_{i \geq l} \binom{w_i}{0} \;\equiv\; \prod_{i=0}^{l-1} \binom{w_i}{k_i} \bmod p$$

□

Corollary 2.5 *Let $k < p^\ell$. Let $f : \{0,1\}^n \to \mathbb{Z}_p$ be computed by a symmetric polynomial $P(X)$ of degree k. Then f is a function of only the ℓ least significant digits $w_0, \cdots, w_{\ell-1}$.*

Proof: We can write $P(X)$ as a linear combination of $S_1(X), \cdots, S_k(X)$. By Lemma 2.4, for $1 \leq j \leq k$, the value of $S_j(a)$ depends only on $w_0, \cdots, w_{\ell-1}$. Hence the value of $P(a)$ depends only on $w_0, \cdots, w_{\ell-1}$. □

Lemma 2.6 *Let $1 \leq p^\ell \leq n$. On input $a \in \{0,1\}^n$ of weight w,*

$$S_{p^\ell}(a) \equiv w_\ell \bmod p$$

Proof: Applying Lucas' theorem,

$$S_{p^\ell}(a) \equiv \binom{w}{p^\ell} \equiv \binom{w_\ell}{1} \prod_{i \neq \ell} \binom{w_i}{0} \equiv w_\ell \bmod p$$

□

Corollary 2.7 *If f depends only on $w_0, \cdots, w_{\ell-1}$, then it can computed by a symmetric polynomial $P(X) \in \mathbb{Z}_p[X]$ of degree less than p^l.*

Proof: Consider any function f which depends on just the ℓ least significant digits $w_0, \cdots, w_{\ell-1}$. Using the fact that every function from $\mathbb{Z}_p^\ell \to \mathbb{Z}_p$ is computed by some polynomial, f can be written as a polynomial $Q(w_0, \cdots, w_{\ell-1})$ over $\mathbb{Z}_p$ with the degree of each $w_i \leq p-1$. But by Lemma 2.6, $S_{p^i}(a) \equiv w_i \bmod p$. Hence the polynomial $P(X) = Q(S_1(X), \cdots, S_{p^{\ell-1}}(X))$ computes the function f on 0-1 inputs. It is a symmetric polynomial whose degree is bounded by by $\sum_{i=0}^{\ell-1} p^i(p-1) = p^\ell - 1$. □

Saying that f depends only on $w_0, \cdots, w_{\ell-1}$ is equivalent to saying that f is a function of $w \bmod p^l$. Hence, we have proved the following theorem.

Theorem 2.8 *The symmetric functions $f : \{0,1\}^n \to \mathbb{Z}_p$ that can be computed by polynomials of degree $k < p^\ell$ are exactly the functions which depend only on $w \bmod p^\ell$.*

It is known that the polynomials $S_1(X), \cdots, S_n(X)$ generate the symmetric polynomials in $\mathbb{Z}_p[X]$ and further they are algebraically independent. We can think of symmetric multilinear polynomials as symmetric polynomials in the quotient ring $\mathbb{Z}_p[X_1, \cdots, X_n]/(X_1^2 - X_1, \cdots, X_n^2 - X_n)$. We have just proved that the symmetric polynomials in this quotient ring are generated by $S_1(X), S_p(X), \cdots, S_{p^\ell}(X)$ where $\ell = \lfloor \log_p n \rfloor$. 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 and are presented in the Appendix.

2.2 Equivalence of Polynomials and Protocols

We now define simultaneous protocols for computing a function $f : \{0, 1, \cdots, n\} \to \{0,1\}$. The results of the previous section will allow us to interpret symmetric polynomials over $\mathbb{Z}_m$ as simultaneous protocols for any m. In a simultaneous protocol for computing a function, the players cannot communicate during

the protocol but they can agree on a procedure beforehand. They compute their outputs independent of one another and write them on a blackboard. A referee then reads these values and decides if the value of the function is 0 or 1. For ease of notation we state the definitions for the case where $m = 6$.

Definition 2.9 *A* strong protocol over $\mathbb{Z}_6$ *with parameters* (k_2, k_3) *for computing a function* $f : \{0, 1 \cdots, n\} \rightarrow \{0, 1\}$ *is a simultaneous protocol with players* P_2 *and* P_3.

- *Player* P_2 *is given* $i \equiv w \bmod 2^{k_2}$ *as input and outputs* $P_2(i) \mathbb{Z}_2$. *Player* P_3 *is given* $j \equiv w \bmod 3^{k_3}$ *as input and outputs* $P_3(j) \in \mathbb{Z}_3$.
- *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 $\max(2^{k_2}, 3^{k_3})$.

Definition 2.10 *A* weak protocol over $\mathbb{Z}_6$ *with parameters* (k_2, k_3) *for computing a function* $f : \{0, 1 \cdots, n\} \rightarrow \{0, 1\}$ *is a simultaneous protocol with players* P_2 *and* P_3.

- P_2 *is given* $i \equiv w \bmod 2^{k_2}$ *as input and outputs* $P_2(i) \in \mathbb{Z}_2$. *Player* P_3 *is given* $j \equiv w \bmod 3^{k_3}$ *as input and outputs* $P_3(j) \in \mathbb{Z}_3$.
- *If* $f(w) \neq f(w')$ *then at least one of the players outputs different values on* w *and* w'.

The cost of the protocol is $\max(2^{k_2}, 3^{k_3})$.

The reason for the above definition of cost is that we wish to model the degree of a polynomial, this will be clear from Theorem 2.11 proved below. 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 $p_1 < p_2 \cdots < p_t$, we define protocols with t players where player[3] P_i is given $w \bmod p_i^{k_i}$ as input. The cost of the protocol is $\max_i p_i^{k_i}$.

Theorem 2.11 *There exists a symmetric polynomial over* $\mathbb{Z}_m$ *of degree* d *that strongly (weakly) represents* f *iff there exists a strong (weak) protocol of cost* $\Theta(d)$ *over* $\mathbb{Z}_m$ *for computing* f.

Proof: The constant implicit in that $\Theta(d)$ depends only on m, and can be taken to be $max_i p_i$. We prove the theorem assuming $m = 6$. We prove the equivalence for the strong case, the weak case is similar. Let

$$P(X) = \sum_{i=0}^{d} a_i S_i(X)$$

be a symmetric polynomial of degree d over $\mathbb{Z}_6$ that strongly represents f. We will construct a strong protocol for computing f with cost at most $3d$. Let $b_i \equiv a_i \bmod 2, c_i \equiv a_i \bmod 3$. Let

$$P_2(X) \;=\; \sum_{i=0}^{d} b_i S_i(X), \quad P_3(X) \;=\; \sum_{i=0}^{d} c_i S_i(X)$$

[3]For notational convenience, we use P_i and k_i as opposed to P_{p_i} and k_{p_i} respectively

Both $P_2(X)$ and $P_3(X)$ are symmetric polynomials of degree at most d. Set parameters (k_2, k_3) so that $d < 2^{k_2} \leq 2d, d < 3^{k_3} \leq 3d$. By Corollary 2.5 the function computed by $P_2(X)$ on a 0-1 input depends on just the first k_2 bits of the weight w in base 2. This function is computed by player P_2. The function computed by $P_3(X)$ on a 0-1 input depends on just the first k_3 digits of w in base 3. This is computed by player P_3. We show that this indeed gives a strong protocol.

Let $a \in \{0,1\}^n$. Since $P(X)$ strongly represents f,

$$\begin{aligned}
f(a) = 0 &\Rightarrow P(a) \equiv 0 \bmod 6 \\
&\Rightarrow P_2(a) \equiv 0 \bmod 2 \quad \text{and} \quad P_3(a) \equiv 0 \bmod 3 \qquad \text{(by CRT)} \\
f(a) = 1 &\Rightarrow P(a) \not\equiv 0 \bmod 6 \\
&\Rightarrow P_2(a) \not\equiv 0 \bmod 2 \quad \text{or} \quad P_3(a) \not\equiv 0 \bmod 3 \qquad \text{(by CRT)}
\end{aligned}$$

Hence we have a strong protocol of cost $\max(2^{k_2}, 3^{k_3}) \leq 3d$.

Conversely assume there exists a protocol for f with parameters (k_2, k_3). The function computed by P_2 depends on only the first k_2 bits of the weight w. So it can be computed by a symmetric polynomial $P_2(X)$ in $\mathbb{Z}_2[X]$ of degree less than 2^{k_2} by Corollary 2.7. Similarly the function computed by P_3 can be computed by a symmetric polynomial $P_3(X)$ in $\mathbb{Z}_3[X]$ of degree less than 3^{k_3}. Let

$$P_2(X) = \sum_{i=0}^{d} b_i S_i(X), \quad P_3(X) = \sum_{i=0}^{d} c_i S_i(X)$$

By the CRT, we can pick $a_i \in \mathbb{Z}_6$ such that $a_i \equiv b_i \bmod 2, \quad a_i \equiv c_i \bmod 3$. Now set

$$P(X) = \sum_{i=0}^{d} a_i S_i(X)$$

We will show that $P(X)$ strongly represents $f \bmod 6$. If $f(w) = 0$, then both players P_2 and P_3 output 0 on w. Hence if $a \in \{0,1\}^n$ has weight w, then

$$P_2(a) \equiv 0 \bmod 2 \ \text{ and } \ P_3(a) \equiv 0 \bmod 3 \quad \Rightarrow \quad P(a) \equiv 0 \bmod 6 \qquad \text{(by CRT)}$$

If $f(w) = 1$, then at least one of P_2 and P_3 outputs a non-zero value on w. Hence if $a \in \{0,1\}^n$ has weight w, then

$$P_2(a) \not\equiv 0 \bmod 2 \ \text{ or } \ P_3(a) \not\equiv 0 \bmod 3 \quad \Rightarrow \quad P(a) \not\equiv 0 \bmod 6 \qquad \text{(by CRT)}$$

$P(X)$ is a symmetric polynomial of degree $d < \max(2^{k_2}, 3^{k_3})$. $\square$

Using this theorem, we will prove both upper and lower bounds on the degrees of polynomials for both representations by viewing them as simultaneous communication protocols. We first need some notation. Recall that player P_2 receives $i \equiv w \bmod 2^{k_2}$ and player P_3 receives $j \equiv w \bmod 3^{k_3}$ and they wish to compute $f(w)$. If $2^{k_2} 3^{k_3} \leq n$ there might be multiple values of w between 0 and n satisfying $w \equiv i \bmod 2^{k_2}$

and $w \equiv j \bmod 3^{k_3}$. If $f(w)$ is not the same for all these values, then clearly no protocol with parameters k_2, k_3 exists. Hence assume that the value of f is well defined for every pair (i,j) of possible residues of w. We can define a $2^{k_2} \times 3^{k_3}$ input matrix $A = (a_{ij})$ as follows.

$$\begin{aligned} 0 \leq \quad a_{ij} \quad &\leq 2^{k_2}3^{k_3} - 1 \\ a_{ij} \quad &\equiv \quad i \bmod 2^{k_2}, \qquad 0 \leq i < 2^{k_2} \\ a_{ij} \quad &\equiv \quad j \bmod 3^{k_3}, \qquad 0 \leq j < 3^{k_3} \end{aligned}$$

We use a_{ij} in place of w since some values a_{ij} could be greater than n. P_2 receives the same input i for all inputs in the same row of A and hence outputs the same value. Similarly inputs in a column are indistinguishable to P_3. Where convenient, we will refer to P_2 and P_3 as the row and column player respectively. For a function f, we then define the $2^{k_2} \times 3^{k_3}$ matrix A^f as below.

$$A^f_{ij} = \begin{cases} f(a_{ij}) & 0 \leq a_{ij} \leq n \\ \text{x} & a_{ij} > n \end{cases}$$

The symbol 'x' indicates that the function is not defined for this value of weight.

In the usual communication complexity setting, there is a fixed function f and a corresponding matrix A^f and we wish to know its communication complexity. In our setting however, the matrix A^f and hence the communication complexity of f depends on k_2 and k_3. There are restrictions on the values that the players can output since $P_2(i) \in \mathbb{Z}_2$ and $P_3(j) \in \mathbb{Z}_3$. As k_2 and k_3 increase, the amount of communication needed can only decrease. For instance, if one player reads all the bits of the input, she could compute $f(w)$ herself and write it on the board. Our goal is now to determine the smallest values of k_2 and k_3 so that the players can compute f with the restrictions on output size.

3 Strong Representations

3.1 Lower Bounds

A weak representation for f is also a representation for $\overline{f}$ and so $\Delta(f) = \Delta(\overline{f})$, but this need not be true for $\delta(f)$. A strong representation is a special case of a weak representation hence $\Delta(f) \leq \min(\delta(f), \delta(\overline{f}))$. We now present some simple upper and lower bounds for strong representations. We begin with a proof of the theorem by Barrington *et al.*. We use the following convention throughout this section, the results are stated for general $m = \prod_{i \leq t} p_i$ with t prime divisors. We present the proof only for $m = 6$ when there is an obvious extension to the case of general m.

Theorem 3.1 *[BBR94] Over $\mathbb{Z}_m$ $\delta(OR) = O(n^{\frac{1}{t}})$.*

Proof: We give a strong protocol for OR over $\mathbb{Z}_6$ of cost $\leq 3\sqrt{n}$.

Protocol 3.2 Protocol for OR mod 6

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

To prove correctness, we need to show that if both players output 0, $w = 0$.

$$w \equiv 0 \bmod 2^{k_2}, \quad w \equiv 0 \bmod 3^{k_3} \Rightarrow w \equiv 0 \bmod 2^{k_2}3^{k_3} \quad \text{(by CRT)}$$

By our choice of (k_2, k_3), $2^{k_2}3^{k_3} > n$ but $w \leq n$. Hence $w = 0$. □

Proposition 3.3 *[BBR94] Over $\mathbb{Z}_m$ $\Delta(OR) = \Omega(n^{\frac{1}{t}})$.*

Proof: We show that any weak protocol for OR has cost $\Omega(\sqrt{n})$. 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. However, $f(0) \neq f(2^{k_2}3^{k_3})$. So $2^{k_2}3^{k_3} > n$ which implies that $\max(2^{k_2}, 3^{k_3}) > \sqrt{n}$. □

To prove lower bounds better than $\sqrt{n}$ for other functions, we need stronger techniques. The output of a strong protocol on input a_{ij} is zero iff $P_2(i) = P_3(j) = 0$. Hence there exists a protocol for f with parameters (k_2, k_3) 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 with no 1s in it. This gives the following necessary and sufficient condition for the existence of a strong protocol.

Lemma 3.4 *[KN97] There is a strong protocol for f with parameters (k_2, k_3) iff $\forall\ i,\ j$ such that $f(a_{ij}) = 1$, either there are no 0s in row i or there are no 0's in column j of A^f.*

Proof: Assume there exist i, j such that $f(a_{ij}) = 1$ but there are 0s in both row i and column j of A^f. The row player must answer 0 on row i since it contains a 0. Similarly the column player must answer 0 on column j. Hence they both answer 0 on a_{ij} so the protocol is incorrect. Conversely, if row i does not have any 0s, the row player can answer 1 on input i and similarly for the column player. This gives a strong protocol for f. □

Lemma 3.4 gives a condition to test whether a protocol with parameters k_2, k_3 exists. Moreover, it follows from the proof that if the condition is satisfied, Protocol 3.5 given below works correctly. Conversely, if $\delta(f) > \max(2^{k_2}, 3^{k_3})$, then there must be an input w on which Protocol 3.5 with parameters k_2, k_3 is incorrect.

Protocol 3.5 Strong Protocol for general function f

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

Let m have t prime factors $p_1, \cdots, p_t$. To extend Lemma 3.4 to t player protocols, we use the notion of a *star*. Our notion of a star is different from the notion used in multi-party protocols [KN97].

Definition 3.6 *Fix parameters $k_1, \cdots, k_t$. A star in the input matrix A is a set of $t+1$ distinct inputs $w_0, \cdots, w_t \leq n$ such that $w_0 \equiv w_u \bmod p_u^{k_u}$ for $1 \leq u \leq t$. The input w_0 is called the center of the star and $w_1, \cdots w_t$ are called the endpoints.*

Unlike in the multi-party protocol setting, we require the endpoints of the star to agree with the center only on a single co-ordinate. Since we are interested in proving lower bounds of the form $\Omega(n)$, distinct inputs can agree modulo at most one prime power (by the CRT). We prove a condition for the existence of a strong protocol over $\mathbb{Z}_m$ which generalizes Lemma 3.4.

Lemma 3.7 *There exists a strong protocol for computing f over $\mathbb{Z}_m$ with parameters $k_1, \cdots, k_t$ iff there does not exist a star $w_0, \cdots, w_t$ such that $f(w_0) = 1$ and $f(w_u) = 0$ for $1 \leq u \leq t$.*

Proof: Assume that such a star exists. Then player P_u must answer 0 on input $w_u \bmod p_u^{k_u}$ since $f(w_u) = 0$. This implies that every player outputs 0 on input w_0 since $w_0 \equiv w_u \bmod p_u^{k_u}$. But $f(w_0) = 1$ and so the protocol is incorrect.

Conversely, assume that a star satisfying these conditions does not exist. Then for every w_0 such that $f(w_0) = 1$, there exists an index u such that

$$\forall w_u \text{ s.t. } w_u \equiv w_0 \bmod p_u^{k_u}, \quad f(w_u) = 1 \tag{1}$$

Now consider the following extension of Protocol 3.5 to t players.

On input $j \in [0, \cdots, p_u^{k_u} - 1]$, if $\exists w \leq n$ such that $w \equiv j \bmod p_u^{k_u}$ and $f(w) = 0$ then player P_u outputs 0. Else P_u outputs 1.

If $f(w) = 0$, then every player outputs 0 on input $w \bmod p_u^{k_u}$. If $f(w) = 1$, by Equation 1 there exists u such that $\forall w_u \equiv w \bmod p_u^{k_u}, f(w_u) = 1$. Hence P_u outputs 1 on input $w \bmod p_u^{k_u}$ and the protocol is correct.

□

We can use the above Lemmas to prove degree bounds for various functions. Define the Weight-k function W_k on $\{0,1\}^n$ as $W_k(a) = 1$ if $w(a) = k$ and 0 otherwise. Using an argument similar to the one used for the OR function, one can show that over $\mathbb{Z}_m$, $\delta(\overline{W}_k) = \Theta(n^{\frac{1}{t}}$. We now show bounds on $\delta(W_k)$.

Corollary 3.8 *Over $\mathbb{Z}_m$, $\delta(W_k) = \Omega(n)$.*

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

$$b = k - 2^{k_2}, \quad c = k - 3^{k_3}$$

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

$$f(k) = 1, \quad f(b) = 0, \quad f(c) = 0$$

Hence by Theorem 3.4 such a protocol does not exist. Hence $\max(2^{k_2}, 3^{k_3}) > \frac{n}{2}$. When $k < \frac{n}{2}$, repeat the same argument with $b = k + 2^{k_2}$ and $c = k + 3^{k_3}$. □

Define the Threshold-k function T_k on $\{0,1\}^n$ as $T_k(a) = 1$ if $w(a) \geq k$ and 0 otherwise.

Corollary 3.9 *Over* $\mathbb{Z}_m$, $\delta(T_k) = \Omega(\max(k, n^{\frac{1}{t}})$.

Proof: We first show a lower bound of $\Omega(\sqrt{n})$ over $\mathbb{Z}_6$. Suppose $2^{k_2}3^{k_3} \leq n$. We can choose a w so that $w < k \leq w + 2^{k_2}3^{k_3}$. Both players receive the same inputs for weights w and $w + 2^{k_2}3^{k_3}$ but $T_k(w) = 0$ while $T_k(w + 2^{k_2}3^{k_3}) = 1$. Hence the protocol is incorrect. This proves a lower bound of $\sqrt{n}$.

Now suppose $\max(2^{k_2}, 3^{k_3}) < k$. Consider any $w \geq k$. Since $i \equiv w \bmod 2^{k_2}$ and $2^{k_2} < k, i < k$. Similarly $j < k$. The entry i lies in the same row as w while j lies in the same column.

$$T_k(w) = 1, \quad T_k(i) = 0, \quad T_k(j) = 0$$

Now apply Theorem 3.4. Hence $\max(2^{k_2}, 3^{k_3}) > k$. □

In the next section, we will show a better lower bound of $\Omega(n^{\frac{1}{t}}k^{\frac{t-1}{t}})$ for T_k.

Corollary 3.10 *Over* $\mathbb{Z}_m$, $\delta(\overline{T}_k) = \Omega(n)$ *for* $k \leq \frac{n}{2}$.

Proof: Assume that $2^{k_2}, 3^{k_3} \leq \frac{n}{2}$. There exist multiples $a2^{k_2}, b3^{k_3}$ so that

$$k \leq \frac{n}{2} \leq a2^{k_2}, \quad b3^{k_3} \leq n$$

Now observe that $a2^{k_2}$ and $b3^{k_3}$ are in the same row and column respectively as 0, and

$$\overline{T}_k(0) = 1, \quad \overline{T}_k(a2^{k_2}) = 0, \quad \overline{T}_k(b3^{k_3}) = 0$$

Hence by Theorem 3.4, $\max(2^{k_2}, 3^{k_3}) > \frac{n}{2}$. □

Define the Mod-k function M_k on $\{0,1\}^n$ as $M_k(a) = 1$ if $a \equiv 0 \bmod k$ and 0 otherwise. We can show that if $k \neq 2^a3^b$ both M_k and its complement have $\delta = \Theta(n)$. If $k = 2^a3^b$ then $\overline{M}_k$ has degree $O(1)$ while M_k has degree $\Theta(n)$. We skip the proof.

4 Weak Representations

In this section we will show lower bounds of $\Omega(n)$ for weak representations of various functions using tools from communication complexity. The lower bounds of $\Omega(n^{\frac{1}{t}})$ do not make use of the *simultaneous* nature of the protocol, the same bounds would hold even if the players were allowed to send their inputs to each other. To prove bounds of $\Omega(n)$, we exploit the fact that the players cannot communicate and there are restrictions on their output size.

4.1 Lower Bounds for Two Player Protocols

Using a classical result about deterministic simultaneous communication protocols, we give a necessary and sufficient condition for the existence of a weak protocol in terms of the number of distinct rows and columns in A^f.

Definition 4.1 *Two rows i, i' in the matrix A^f are distinct, if there exists a column index j such that $a_{ij}, a_{i'j} \leq n$ and $f(a_{ij}) \neq f(a_{i'j})$. Rows $i_1, \cdots, i_k$ are said to be distinct if they are pairwise distinct.*

Lemma 4.2 *For a weak protocol for f over $\mathbb{Z}_{pq}$ with parameters (k_p, k_q) to exist, the matrix A^f must have at most p distinct rows and q distinct columns.*

Proof: We will show that over $\mathbb{Z}_6$, A^f can have at most 2 distinct rows and 3 distinct columns.

Assume that there are at least 3 distinct rows. Since P_2 must output a value in $\mathbb{Z}_2$, she outputs the same value for some two distinct rows i, i'. Since the rows are distinct, there is a column index j such that $a_{i,j}, a_{i',j} \leq n$ and $f(a_{ij}) \neq f(a_{i'j})$. Player P_3 will also output the same value for inputs a_{ij} and $a_{i'j}$ since they lie in the same column. This violates the definition of a weak protocol. □

Recall that we define the function M_k on $\{0,1\}^n$ as $M_k(a) = 1$ if $a \equiv 0 \bmod k$ and 0 otherwise.

Theorem 4.3 *Let $(k,p) = (k,q) = 1$ and $k > min(p,q)$. Over $\mathbb{Z}_{pq}$, $\Delta(M_k) = \Omega(n)$.*

Proof: We consider the case $k = 5, p = 2, q = 3$. 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.

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

Elements in the same row of V have the same residue modulo 2^{k_2} and elements in a column have the same residue modulo 3^{k_3}. So V is a submatrix of A. Since $2^{k_2}, 3^{k_3} \neq 0 \bmod 5$, we can find $a_1, a_2, b_1, b_2 < 5$ s.t.

$$\begin{aligned} a_1 2^{k_2} &\equiv 1 \bmod 5 & a_2 2^{k_2} &\equiv 2 \bmod 5 \\ b_1 3^{k_3} &\equiv -1 \bmod 5 & b_2 3^{k_3} &\equiv -2 \bmod 5 \end{aligned}$$

Hence

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

This implies that A^f has at least 3 different rows and a weak protocol cannot exist by Lemma 4.2. 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 $\min(2^{k_2}, 3^{k_3}) \geq \frac{n}{24}$. For T_k over $\mathbb{Z}_{pq}$ the lower bound obtained is $\Omega(\frac{n}{kq})$. $\square$

The same proof works for the Mod-ℓ function where $\ell = p^a q^b k$ provided $(k,p) = (k,q) = 1$ and $k > \min(p,q)$. The condition $k > \min(p,q)$ implies that we cannot for instance show that Mod-2 is hard over $\mathbb{Z}_{15}$. While an $\Omega(n)$ lower bound probably holds, to prove this we will need to choose a different submatrix as it is easy to verify that a simple protocol exists for the inputs in V. We now show a lower bound for Threshold functions in the two player case.

Theorem 4.4 *Over $\mathbb{Z}_{pq}$, $\Delta(T_k) = \Omega(\max(k, \sqrt{n}))$ for $k \leq \frac{n}{pq}$.*

Proof: A lower bound of $\sqrt{n}$ is easy to show for all k as in the proof of Corollary 3.9. So 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

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

Clearly V^f has at least three distinct rows for all settings of the x's. To ensure that the entries of V are at most n we need $2 \cdot 3^{k_3+1} < n$. 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 $k \leq \frac{n}{pq}$. $\square$

In Section 5, we will improve this bound to $\Omega(\sqrt{kn})$ for $k \leq \frac{n}{p}$.

4.2 Multi-player Protocols for Mod-k

We now consider the case when m has $t > 2$ distinct prime factors and the protocols involve t players. We show a lower bound for the t player case by a reduction to the function Exactly-k in the number on the forehead model. There is a lower bound of $\omega(1)$ on the deterministic complexity of Exactly-k due to Chandra *et al.* [CFL83]. We first need some results from the number on the forehead model. There are t

players $P_1, \cdots, P_t$ and t inputs $x_1, \cdots, x_t$. Player P_j receives inputs x_i for all $i \neq j$. They wish to compute some function $f(x_1, \cdots, x_t)$. $D(f)$ denotes the deterministic complexity of the function f. For further definitions about the model as well as an exposition of the result of Chandra *et al.*, see [KN97].

Definition 4.5 *For $x_1, \cdots, x_t \in \{0, \cdots, k-1\}$, the Exactly-k function $E_k^t(x_1, \cdots, x_t) = 1$ iff $\sum_{i=1}^t x_i = k$.*

Theorem 4.6 *[CFL83] $D(E_k^t(x_1, \cdots, x_t)) = \omega(1)$.*

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

Definition 4.7 *For $x_1, \cdots, x_t \in \{0, \cdots, k-1\}$, $M_k^t(x_1, \cdots, x_t) = 1$ iff $\sum_{i=1}^t x_i \equiv 0 \bmod k$.*

Lemma 4.8 *$D(M_k^t(x_1, \cdots, x_t)) = \omega(1)$.*

Proof: We prove the lower bound by reducing computing E_k^t to computing M_k^t. Let $S = \sum_{i=1}^t x_i$. Assume the players have a protocol for M_k^t. If they run this protocol and find that $M_k^t(x_1, \cdots, x_t) = 0$, then $S \neq 0 \bmod k$. Hence $S \neq k$, which implies $E_k^t(x_1, \cdots, x_t) = 0$.

If $M_k^t(x_1, \cdots, x_t) = 1$, then $S \in \{0, k, 2k, \cdots, (t-1)k\}$. However player P_1 (or any other player) can distinguish between these outcomes. In particular if $S = k$, then $1 \leq S - x_1 \leq k$. If $S = Ck$ where $C \neq 1$ then $S - x_1$ cannot take values between 1 and k . But $S - x_1 = \sum_{i=2}^t x_i$ and this can be computed by P_1. P_1 writes one additional bit on the blackboard which tells the referee whether $1 \leq S - x_1 \leq k$. Hence $D(E_k^t) \leq D(M_k^t) + 1$. But now by Theorem 4.6, $D(M_k^t) = \omega(1)$. $\square$

We now prove a lower bound for Mod-k in the t player case.

Theorem 4.9 *Over $\mathbb{Z}_m$, for k sufficiently large as a function of m and $(k, m) = 1$, $\Delta(M_k) = \Omega(n)$.*

Proof: 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.

We identify a fooling set comprising of a subset of the inputs. We will show that on this subset, the problem can be reduced to computing M_k^t in the number on the forehead model. The fooling set consists of inputs $a2^{k_2} + b3^{k_3} + c5^{k_5}$ where $a, b, c \in \{0, \cdots, k-1\}$. The values of k_2, k_3 and k_5 will be set later. 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 can give $b3^{k_3}$ and $c5^{k_5}$ as inputs to P_2 since the value of u can be computed from this. Since $(3^{k_3}, k) = 1$ and $b \in \{0, \cdots, k-1\}$, there is a one-to-one correspondence between the numbers $b3^{k_3}$ and $\{0, \cdots, k-1\}$.

Hence it is sufficient to give P_2 the inputs

$$\begin{aligned} x_3 &\equiv b3^{k_3} \bmod k \\ x_5 &\equiv c5^{k_5} \bmod k \end{aligned}$$

The values of $b3^{k_3}$ and $c5^{k_5}$ can be recovered from x_3 and x_5 respectively. Similarly set $x_2 \equiv a2^{k_2} \bmod k$. Observe that now $0 \leq x_i \leq k-1$, player P_i has inputs x_j for all $i \neq j$ and they wish to know if the sum of the x_i's is 0 mod k. Thus we have a reduction to the problem of computing $M_k^3(x_2, x_3, x_5)$ in the number in the forehead model.

In any weak protocol over $\mathbb{Z}_{30}$, the number of bits of communication available to the players is bounded by a fixed constant ($\log_2 30$). Lemma 4.8 implies that for k sufficiently large, this is insufficient, hence a weak protocol cannot exist. We now set k_2, k_3 and k_5 so that the entries in our fooling set are no larger than n. The largest entry is bounded by $k(2^{k_2} + 3^{k_3} + 5^{k_5})$. So we set each of $2^{k_2}, 3^{k_3}, 5^{k_5} < \frac{n}{3k}$. This gives a lower bound on the degree of $\Omega(\frac{n}{k})$.

In general over $\mathbb{Z}_m$ where m has t distinct prime factors, we choose k large enough so that $D(M_k^t) \geq \log_2 m$. We then choose a fooling set of inputs of the form $\sum_{i \leq t} a_i p_i^{k_i}$. To ensure that these numbers are less than n, take $p_i^{k_i} \leq \frac{n}{t}$. This gives a degree bound of $\Omega(\frac{n}{tkp_t})$.

□

4.3 Separating Strong and Weak Representations

In a strong protocol, w.l.o.g. the players output either 0 or 1. The referee's strategy is fixed. On the other hand, in a weak protocol, a player can output a value from $\mathbb{Z}_p$. The referee is allowed to choose any strategy. A natural question therefore is whether weak protocols are actually more powerful than strong protocols. Recall that $\Delta(f) \leq \min(\delta(f), \delta(\overline{f}))$. We will show a gap between these quantities by constructing a function f such that $\Delta(f) = O(\sqrt{n})$ but $\min(\delta(f), \delta(\overline{f})) = \Omega(n)$.

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

$$f(w) = \begin{cases} 1 & \text{exactly one of } 2^{l_2}, 3^{l_3} \text{ divides } w \\ 0 & \text{otherwise} \end{cases}$$

Since $2^{l_2} 3^{l_3} > n$, if both 2^{l_2} and 3^{l_3} divide w, then $w = 0$.

Lemma 4.10 *Over* $\mathbb{Z}_6$, $\min(\delta(f), \delta(\overline{f})) = \Omega(n)$.

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

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

We now consider the matrix

$$V = \begin{pmatrix} 0 & 3^{m_3} \\ 2^{m_2} & 2^{m_2} + 3^{m_3} \end{pmatrix} \Rightarrow$$
$$V^f = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \quad V^{\overline{f}} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

Hence by Lemma 3.4, both f and $\overline{f}$ have strong degree $\Omega(n)$. $\square$

Lemma 4.11 *Over $\mathbb{Z}_6$, $\Delta(f) = O(\sqrt{n})$.*

Protocol 4.12 Weak Protocol for function f

- Set $k_2 = l_2$ and $k_3 = l_3$.
- If $i = 0$ then $P_2(i) = 0$ else $P_2(i) = 1$.
- If $j = 0$ then $P_3(j) = 0$ else $P_3(j) = 1$.
- The output of the protocol is 1 if $P_2(i) = P_3(j)$ and 0 if $P_2(i) \neq P_3(j)$.

It is easy to see that the above protocol computes f with cost $O(\sqrt{n})$. The referee's strategy is to take the XOR of the players outputs which cannot be done in a strong protocol.

Theorem 4.13 *There exists a function f for which $\Delta(f) = O(\sqrt{n})$ whereas $\delta(f)$ and $\delta(\overline{f})$ are $\Theta(n)$.*

5 Threshold Functions and Diophantine Equations

We now begin a detailed study of the degree of the Threshold-k function for values of k between 1 and n. We prove a theorem that equates showing degree bounds on threshold to the number of solutions to certain families of equations. Note that we already have a lower bound of $\max(k, n^{\frac{1}{t}})$ by Corollary 3.9. Since we wish to minimize the cost of the protocol which is defined as $\max(p_i^{k_i})$, we will assume that $p_i^{k_i}$s are nearly equal and that they are greater than $\max(k, n^{\frac{1}{t}})$.

Theorem 5.1 *There exists a strong protocol for T_k over $\mathbb{Z}_m$ with parameters k_i for $1 \leq i \leq t$ iff the following equation has no non-trivial solutions*

$$\begin{aligned} \forall\, i, \quad a_i p_i^{k_i} &\leq n \\ \forall\, i \neq j, \quad |a_i p_i^{k_i} - a_j p_j^{k_j}| &< k \end{aligned} \tag{2}$$

Proof: Clearly $a_i = 0$ for all i is a solution and we call this a trivial solution. We show that a protocol over $\mathbb{Z}_6$ exists iff the following equation does not have solutions. The extension to general m is easy.

$$|a2^{k_2} - b3^{k_3}| = \ell \qquad\qquad a2^{k_2} \leq n,\ b3^{k_3} \leq n,\quad \ell < k \tag{3}$$

As a first step, we show that it suffices to analyze the following strong protocol. This is essentially the argument for the correctness of Protocol 3.5 specialized to the Threshold-k function.

Protocol 5.2 Strong Protocol for Threshold-k

- If $i \geq k$, P_2 outputs 1, else P_2 outputs 0.
- If $j \geq k$, P_3 outputs 1, else P_3 outputs 0.

In a strong protocol, if $f(w) = 0$ both players must output 0. Hence when $i < k$, P_2 must output 0 since the input could be i. If $i \geq k$, then clearly $w \geq k$, hence P_2 can wlog output 1. Similarly, this is also the best strategy for P_3.

We analyze inputs on which the protocol fails. Let $w \geq k, i < k, j < k$. On such inputs, both players output 0 whereas the value of the function is 1, and so the protocol is incorrect. Note that $i \neq j$ since if $i = j$, by the CRT $w = i$. This contradicts the fact that $w \geq k$. But now

$$w = a2^{k_2} + i = b3^{k_3} + j$$

Assume that $i > j$ and let $i - j = \ell$ where $0 < \ell < k$. Then, we have

$$\begin{aligned} b3^{k_3} - a2^{k_2} &= \ell \\ a2^{k_2}, b3^{k_3} \leq w &\leq n \end{aligned}$$

Hence any such input gives a solution to Equation (3).

Conversely, we will show that any solution to Equation (3) for fixed n gives an input w so that the protocol is incorrect. Assume that we have

$$|a2^{k_2} - b3^{k_3}| = \ell \quad s.t.\ \ a2^{k_2} \leq n,\ b3^{k_3} \leq n,\quad \ell < k$$

Assume $b3^{k_3} > a2^{k_2}$. Set $w = b3^{k_3} = a2^{k_2} + \ell$. From this setting, we obtain

$$\begin{aligned} i \equiv w \bmod 2^{k_2} &= \ell \\ j \equiv w \bmod 3^{k_3} &= 0 \end{aligned}$$

Hence we have $w > 2^{k_2} \geq k$ whereas $i, j < k$ and hence the protocol is incorrect. $\square$

As an example, suppose we were trying to show a bound of $n^{\frac{3}{4}}$ on T_2. We set $2^{k_2}, 3^{k_3} > n^{\frac{3}{4}}$. This implies that $a, b < n^{\frac{1}{4}} = (2^{k_2})^{\frac{1}{3}}$. We are looking for solutions to

$$|a2^{k_2} - b3^{k_3}| = 1 \qquad\qquad a < (3^{k_3})^{\frac{1}{3}} \;\; b < (2^{k_2})^{\frac{1}{3}}$$

If we relax the constraints on a, b to $a < 3^{k_3}$ and $b < 2^{k_2}$, by the GCD equation, we will have a solution for every value of k_2, k_3 Since $(2^{k_2}, 3^{k_3}) = 1$. We are asking how many solutions exist with the constraint that $a, b < (2^{k_2})^{\frac{1}{3}}$. We will show that the answer is only finitely many.

5.1 Upper Bounds

5.1.1 Constant Threshold with Two Players

We now prove an upper bound for constant threshold when m has two prime factors. We set $m = 6$ for convenience. We will use the following result of Filaseta [Fil91].

Proposition 5.3 *Let ℓ be a fixed non-zero integer. Let M be a fixed positive integer. Let $\varepsilon > 0$. Let D be the largest divisor of $N(N - \ell)$ which is relatively prime to M. If N is sufficiently large (depending on ℓ, M and ε), then $D > N^{1-\varepsilon}$.*

Theorem 5.4 *Let $c \geq 1$ be any fixed constant. Over $\mathbb{Z}_{pq}$, $\delta(T_c) = O(n^{\frac{1}{2}+\varepsilon})$ for all $\varepsilon > 0$.*

Proof: We prove the theorem over $\mathbb{Z}_6$.

Set $2^{k_2} \cdot 3^{k_3} > n^{1+\varepsilon}$. We will show with this setting of parameters, Protocol 5.2 works for sufficiently large n. By Theorem 5.1, the protocol for n fails iff there is a solution to

$$|a2^{k_2} - b3^{k_3}| \;\; = \;\; \ell \qquad\qquad a2^{k_2} \leq n, \; b3^{k_3} \leq n, \; \ell < c \tag{4}$$

We first show that for each $\ell < c$, this equation has only finitely many solutions. Set $M = 6$. Take

$$\begin{aligned} N \;\; &= \;\; a2^{k_2} \;\; = \;\; b3^{k_3} + \ell \\ \Rightarrow \;\; N(N - \ell) \;\; &= \;\; ab2^{k_2}3^{k_3} \end{aligned}$$

Let D be largest divisor of $N(N - \ell)$ relatively prime to 6. It follows that $D \leq ab$. By our setting of parameters,

$$\begin{aligned} 2^{k_2}3^{k_3} > n^{1+\varepsilon} \;\; &\geq \;\; N^{1+\varepsilon} \\ ab2^{k_2}3^{k_3} = N(N - \ell) \;\; &< \;\; N^2 \\ \Rightarrow \qquad D \leq ab &< N^{1-\varepsilon} \end{aligned}$$

By Proposition 5.3, this is possible for only finitely many N. Hence, with fixed ℓ, there are only finitely many solutions. There are only finitely many possibilities for ℓ since $1 \leq \ell < c$. Hence Equation 4 has only

finitely many solutions in $a2^{k_2}, b3^{k_3}$. This implies an upper bound on n since

$$2^{k_2} \cdot 3^{k_3} \geq n^{1+\varepsilon} \quad \Rightarrow \quad n \leq ab2^{k_2}3^{k_3}$$

Hence there are only finitely many solutions in n. Hence Protocol 5.2 works for all sufficiently large n. We can take 2^{k_2} and 3^{k_3} approximately equal to give the desired degree bound. $\square$

By the CRT, we know that if $2^{k_2}3^{k_3} > n$, and if $w \equiv 0$ modulo 2^{k_2} and 3^{k_3} then in fact $w = 0$. The above theorem states that if $2^{k_2}3^{k_3} > n^{1+\varepsilon}$ for any positive ε, and if the residues of w modulo 2^{k_2} and 3^{k_3} are both less than c then in fact $w < c$ for sufficiently large n. Also we have established an equivalence between proving bounds on the strong degree and showing that certain equations have only finitely many solutions. This equivalence allows us to use number theoretic results to show bounds on degree. On the other hand, it implies than an alternative proof of the degree bound for symmetric polynomials will have interesting number theoretic implications.

5.1.2 Constant Threshold with Multiple Players

In this section we consider the case when m has t distinct prime divisors $p_1, p_2, \cdots p_t$. For T_c with c constant, it is easy to show a lower bound of $\Omega(n^{\frac{1}{t}})$. We will show an upper bound of $O(n^{\frac{1}{t}+\varepsilon})$ for all $\varepsilon > 0$. We will use a result due to Granville which generalizes Filaseta's result. But this result holds only under the assumption of the *abc*−conjecture. This is a very powerful conjecture which has many important implications, including an asymptotic version of Fermat's Last Theorem [GT02].

Definition 5.5 *The Radical of M denoted by $R(M)$ is the product of distinct primes dividing M.*

Conjecture 5.6 (The *abc*-conjecture) *Fix $\epsilon > 0$. If a, b, c are coprime positive integers satisfying $a + b = c$, then*

$$c < D \cdot R(abc)^{1+\epsilon}$$

where D is a constant that depends only on ϵ.

Theorem 5.7 *[Gra98] Assume the abc-conjecture is true. Suppose that $g(X) \in \mathbb{Z}[X]$ has no repeated roots. Fix $\varepsilon > 0$. Then for w sufficiently large,*

$$R(g(w)) > |w|^{deg(g)-1-\varepsilon}$$

Using this result, we analyze the following protocol which is the natural generalization of Protocol 5.2.

Protocol 5.8 Threshold-c with multiple players

- Take $p_1^{k_1}p_2^{k_2}\cdots p_t^{k_t} > n^{1+\varepsilon}$.
- Set $w_i \equiv w \bmod p_i^{k_i}$. If $w_i < c$, Player i outputs 0 else player i outputs 1.

Theorem 5.9 *Let $c \geq 1$ be any fixed constant. Assuming the* abc *conjecture, over $\mathbb{Z}_m$, $\delta(T_c) = O(n^{\frac{1}{t}+\varepsilon})$.*

Proof: Fix a value of n. If Protocol 5.8 is incorrect, by Theorem 5.1 there must be a non-trivial solution to the following system of equations.

$$\begin{array}{rll} a_i p_i^{k_i} & \leq n & \forall\, i \in \{1, \cdots t\} \\ |a_i p_i^{k_i} - a_j p_j^{k_j}| & < c & \forall\, i < j \end{array} \tag{5}$$

We now set

$$g(X) \;=\; X(X-1)\cdots(X-c+1)$$

Clearly $g(X)$ has no repeated roots and we can apply Theorem 5.7. Hence, $\forall \varepsilon > 0$, for all but finitely many n,

$$R(g(w)) > w^{c-1-\varepsilon} \tag{6}$$

We will show that if Protocol 5.8 is incorrect on w, then $g(w)$ is divisible by high prime powers, and so $R(g(w))$ is small, which contradicts Equation (6).

$$g(w) = w(w-1)\cdots(w-c+1)$$

We know that $w - a_i p_i^{k_i} = w_i$ where $0 \leq w_i < c$. Hence for all i,

$$\begin{array}{rl} & w - w_i \mid g(w) \\ & w - w_i \;=\; a_i p_i^{k_i} \\ \Rightarrow & \quad p_i^{k_i} | g(w) \end{array}$$

By the CRT, for a suitable constant C,

$$g(w) = C \prod_i p_i^{k_i}$$

We now bound the size of C.

$$\begin{array}{rcl} \prod_i p_i^{k_i} & > & n^{1+\varepsilon} \;\geq\; w^{1+\varepsilon} \\ g(w) & = & w(w-1)\cdots(w-c+1) \;<\; w^c \\ \Rightarrow\; C & = & \dfrac{g(w)}{\prod_i p_i^{k_i}} \;<\; w^{c-1-\varepsilon} \end{array}$$

This gives an upper bound on $R(g(w))$.

$$\begin{aligned} R(g(w)) &< Cp_1p_2\cdots p_t \\ &< w^{c-1-\varepsilon}p_1p_2\cdots p_t \\ &= w^{c-1-\varepsilon'} \end{aligned}$$

The last equality holds since $\prod p_i \leq m$ is a constant. This gives a contradiction to Equation 6. Hence w must be one of only finitely many exceptions. This bounds the value of n since

$$\begin{aligned} w \geq a_i p_i^{k_i} \geq p_i^{k_i} \\ \prod_i p_i^{k_i} > n^{1+\varepsilon} \\ \Rightarrow w^t > n^{1+\varepsilon} \\ \Rightarrow n < w^{\frac{t}{1+\varepsilon}} \end{aligned}$$

Hence there are only finitely many solutions in n and the protocol works correctly for n sufficiently large. The degree bound follows by taking nearly equal powers of p_i. □

5.1.3 Upper Bounds for General Threshold Functions

We now return to the case when m has two prime divisors and show that the *abc*−conjecture implies an upper bound of $O(nk)^{\frac{1+\varepsilon}{2}}$ on T_k for all values of k in the strong representation. We begin with the following technical lemma.

Lemma 5.10 *Assume the* abc *conjecture holds for some $\varepsilon > 0$. For $n > n_0(\varepsilon)$, the equation*

$$|a2^{k_2} - b3^{k_3}| = \ell \qquad\qquad a2^{k_2} \leq n, \quad b3^{k_3} \leq n, \quad 2^{k_2}3^{k_3} \geq (n\ell)^{1+\varepsilon}$$

has no solutions with $a2^{k_2}, b3^{k_3}, \ell$ relatively prime.

Proof: Assume that we have a solution where $a2^{k_2} > b3^{k_3}$. Applying the *abc* conjecture to the equation $a2^{k_2} = b3^{k_3} + \ell$, we must have

$$D \cdot R(a2^{k_2}b3^{k_3}\ell)^{1+\varepsilon} > a2^{k_2} \geq (a2^{k_2}b3^{k_3})^{\frac{1}{2}} \tag{7}$$

where the last inequality holds since $a2^{k_2} > b3^{k_3}$. We can bound $R(a2^{k_2}, b3^{k_3}, \ell)$ by $6ab\ell$. Plugging this bound into (7), for a suitable constant D' depending only on ε, we get

$$D' \cdot (ab\ell)^{1+\varepsilon} > (ab2^{k_2}3^{k_3})^{\frac{1}{2}} \geq (ab)^{\frac{1}{2}}(n\ell)^{\frac{1+\varepsilon}{2}}$$

The last inequality uses the fact that $2^{k_2}3^{k_3} \geq (n\ell)^{1+\varepsilon}$. Rearranging terms,

$$D' \cdot (ab)^{\frac{1}{2}+\varepsilon}\ell^{1+\varepsilon} > (n\ell)^{\frac{1+\varepsilon}{2}} \tag{8}$$

We now upper bound the size of ab.

$$a2^{k_2}b3^{k_3} \leq n^2, \quad 2^{k_2}3^{k_3} \geq (n\ell)^{1+\varepsilon} \quad \Rightarrow ab \leq \frac{n^{1-\varepsilon}}{\ell^{1+\varepsilon}}$$

A calculation now gives the following bound on the LHS of (8).

$$D' \cdot (ab)^{\frac{1}{2}+\varepsilon}\ell^{1+\varepsilon} \leq D' n^{\frac{1+\varepsilon}{2}-\varepsilon^2}\ell^{\frac{1-\varepsilon}{2}-\varepsilon^2} \tag{9}$$

Plugging this bound into (8), we have

$$D' n^{\frac{1+\varepsilon}{2}-\varepsilon^2}\ell^{\frac{1-\varepsilon}{2}-\varepsilon^2} > (n\ell)^{\frac{1+\varepsilon}{2}}$$

For all $n > n_0(\varepsilon)$, this gives a contradiction. Hence for sufficiently large n, the equation has no solutions. □

There is an easy extension to the case of general p and q. Using this, we can show the following degree bound for T_k over $\mathbb{Z}_{pq}$ assuming the *abc*-conjecture.

Theorem 5.11 *If the abc−conjecture is true for some $\varepsilon > 0$, over $\mathbb{Z}_{pq}$, $\delta(T_k) = O((nk)^{\frac{1+\varepsilon}{2}})$ for any $k \leq n$.*

Proof: Note that for a non-trivial bound, we need $\varepsilon < 1$, else $(nk)^{\frac{1+\varepsilon}{2}} = \Omega(n)$ for all k. Take $n > n_0(\varepsilon)$ as in Lemma 5.10. Set $2^{k_2}3^{k_3} \geq (nk)^{1+\varepsilon}$. We claim that there are no solutions to

$$|a2^{k_2} - b3^{k_3}| = \ell \qquad\qquad a2^{k_2} \leq n,\ b3^{k_3} \leq n, \quad \ell < k \tag{10}$$

Assume that a solution exists. Note that $a2^{k_2}, b3^{k_3}, \ell$ need not be coprime. Their GCD can be written as $2^{t_2}3^{t_3}g$ where g is relatively prime to 2 and 3. Dividing throughout we get

$$|a'2^{k_2-t_2} - b'3^{k_3-t_3}| = \ell' \qquad\qquad a'2^{k_2-t_2} \leq n,\ b'3^{k_3} \leq n, \quad \ell' < \frac{k}{2^{t_2}3^{t_3}}$$

Further, we now have that $a'2^{k_2-t_2}, b'3^{k_3-t_3}, \ell'$ are relatively prime. To apply Lemma 5.10, we need to check that $2^{k_2-t_2}3^{k_3-t_3} \geq (n\ell')^{1+\varepsilon}$. It is easy to see that this condition does hold.

$$2^{k_2-t_2}3^{k_3-t_3} \geq \frac{(nk)^{1+\varepsilon}}{2^{t_2}3^{t_3}} \geq \left(\frac{nk}{2^{t_2}3^{t_3}}\right)^{1+\varepsilon} \geq (n\ell')^{1+\varepsilon}$$

However, by Lemma 5.10, our choice of n guarantees that such a solution cannot exist. Hence in fact Equation (10) has no solutions. The degree bound then follows by taking 2^{k_2} and 3^{k_3} nearly equal and applying Theorem 5.1. □

We are unable to extend the above bound to the t-player case for $t \geq 3$.

5.2 Lower Bounds for Threshold-k Functions

5.2.1 Strong Representations

In this section, we will show a $\Omega(\sqrt{kn})$ lower bound on the strong degree of the T_k function over $\mathbb{Z}_{pq}$. For small ε, this matches the upper bound of the previous section. Over $\mathbb{Z}_m$, when m has t distinct prime factors, we show a lower bound of $\Omega(n^{\frac{1}{t}}k^{1-\frac{1}{t}})$ on the strong degree of T_k.

Theorem 5.12 *Over $\mathbb{Z}_{pq}$, $\delta(T_k) = \Omega(\sqrt{nk})$.*

Proof: We prove the theorem over $\mathbb{Z}_6$. Set $2^{k_2}, 3^{k_3} \leq \frac{\sqrt{kn}}{2}$. We will construct solutions to the following equation for all n.

$$|a2^{k_2} - b3^{k_3}| = \ell \qquad\qquad a2^{k_2}, b3^{k_3} \leq n, \ell < k \tag{11}$$

By Theorem 5.1 this implies $\delta(T_k) = \Omega(\sqrt{nk})$.

We construct the solutions by a pigeonhole argument. By Lemma 3.9 we may assume $2^{k_2}, 3^{k_3} \geq \max(k, \sqrt{n})$. Consider all pairs (u, v) such that $u2^{k_2} \leq n,\ v3^{k_3} \leq n$. We map the pair (u, v) to the point $P_{uv} = u2^{k_2} - v3^{k_3}$, so that $P_{uv} \in [-n, n]$. Each pair u, v is mapped to a distinct point, since if

$$\begin{aligned} & P_{uv} = P_{st},\ (u,v) \neq (s,t) \\ \Rightarrow\ & (u-s)2^{k_2} - (v-t)3^{k_3} = 0 \\ \Rightarrow\ & 2^{k_2}3^{k_3} | (u-s)2^{k_2} \\ \Rightarrow\ & |(u-s)2^{k_2}| > n \end{aligned}$$

However, $|(u-s)2^{k_2}| \leq n$ by our choice of u and s.

We can now count the total number of points $P_{u,v}$. We can take $0 \leq u, v < 2\sqrt{\frac{n}{k}}$. Hence there are $4\frac{n}{k}$ points lying in the interval $[-n, n]$, and hence by the pigeonhole principle, there are two points within a distance of $\frac{(2n+1)k}{4n} < k$. Call them P_{uv} and P_{st}. Hence

$$|(u-s)2^{k_2} - (v-t)3^{k_3}| = \ell \qquad\qquad \ell < k$$

Set $a = u - s$, and $b = v - t$. Assume that $a \geq 0$. This implies that $b \geq 0$, since $2^{k_2} > k, 3^{k_3} > k$ so we cannot add multiples of 2^{k_2} and 3^{k_3} to get $\ell < k$. Also, $a2^{k_2} \leq u2^{k_2} \leq n$ and similarly $b3^{k_3} \leq v3^{k_3} \leq n$. Hence a, b, ℓ give the desired solution to Equation 11. $\square$

Note that the lower bound of $\sqrt{nk}$ almost matches the upper bound of $(nk)^{\frac{1}{2}+\varepsilon}$ implied by the $abc-$conjecture. In [Bei03], Beigel shows unconditionally that the bound of $O(\sqrt{nk})$ holds for *infinitely many* n for $k \leq c\sqrt{n}$ for some constant c.

We now generalize this proof to get a lower bound for the t- player case. This result can also be derived from Dirichlet's theorem on simultaneous Diophantine approximation [HW85].

Theorem 5.13 *Over $\mathbb{Z}_m$, $\delta(T_k) = \Omega(n^{\frac{1}{t}}k^{\frac{t-1}{t}})$.*

Proof: Let $p_i^{k_i} < \frac{1}{3} n^{\frac{1}{t}} k^{1-\frac{1}{t}}$ $\forall i$. We will construct solutions to the equation

$$\begin{aligned} \forall\, i, \quad a_i p_i^{k_i} &\leq n \\ \forall\, i \neq j, \quad |a_i p_i^{k_i} - a_j p_j^{k_j}| &< k \end{aligned} \tag{12}$$

By Theorem 5.1, this will imply the desired lower bound.

By Lemma 3.9 we may assume that $p_i^{k_i} > k, n^{\frac{1}{t}}$ $\forall i$. We define t vectors $v_1, \cdots v_t$ in $t-1$ dimensions.

$$\begin{aligned} v_1 &= (p_1^{k_1}, p_1^{k_1}, \cdots, p_1^{k_1}) \\ v_2 &= (p_2^{k_2}, 0, \cdots, 0) \\ v_i &= (0,\ 0,\ p_i^{k_i}\ , 0) \\ v_t &= (0, 0, \cdots, p_t^{k_t}) \end{aligned}$$

For $i = 1, \cdots t$, consider b_i such that $b_i p_i^{k_i} \leq n$. We map every such t-tuple $b = (b_1, b_2, \cdots, b_t)$ to a point P_b in $t-1$ dimensional space.

$$\begin{aligned} P_b &= b_1 v_1 - b_2 v_2 \cdots - b_t v_t \\ &= (b_1 p_1^{k_1} - b_2 p_2^{k_2}, b_1 p_1^{k_1} - b_3 p_3^{k_3}, \cdots, b_1 p_1^{k_1} - b_t p_t^{k_t}) \end{aligned}$$

We can use the fact that $p_1^{k_1} p_2^{k_2} \cdots p_t^{k_t} > n$ to show that if $b \neq c$, then $P_b \neq P_c$. For each i we can take $0 \leq b_i < 3(\frac{n}{k})^{1-\frac{1}{t}}$. This gives a total of $3^t(\frac{n}{k})^{t-1}$ points. Since each co-ordinate of P_b lies between $[-n, n]$, every point lies in $[-n, n]^{t-1}$ which is a cube of volume $(2n+1)^{t-1}$. We can partition this cube into $\lceil \frac{2n+1}{k-1} \rceil^{t-1} < (\frac{3n}{k})^{t-1}$ smaller cubes with each side of length $k-1$. However there are $3^t(\frac{n}{k})^{t-1}$ distinct points. By the pigeonhole principle, two points lie in the same cube of side $k-1$. Call these points P_b and P_c. This implies for $2 \leq i \leq t$ we have

$$|(b_1 - c_1) p_1^{k_1} - (b_i - c_i) p_i^{k_i}| \leq k - 1$$

Assume that $b_1 - c_1 \geq 0$. Since $p_i^{k_i} > k$ for every i, this implies $b_i - c_i \geq 0$ for every i. We set $a_i = b_i - c_i$. This gives

$$\begin{aligned} \forall i, \quad a_i p_i^{k_i} \leq b_i p_i^{k_i} &\leq n \\ \forall\, i \neq j, \quad |a_i p_i^{k_i} - a_j p_j^{k_j}| &< k \end{aligned}$$

Hence we get a solution to Equation 12. □

5.3 Weak Representations

In Theorem 4.4, we show a lower bound of $\Omega(\max(k, \sqrt{n}))$ for $\Delta(T_k)$ over $\mathbb{Z}_{pq}$. We can improve this to $\Omega(\sqrt{nk})$ using the results obtained above on the strong degree of T_k.

Theorem 5.14 *Over $\mathbb{Z}_{pq}$, for $k \leq \frac{n}{p}$, $\delta(T_k) = \Omega(\sqrt{nk})$.*

Proof: We prove the bound over $\mathbb{Z}_6$. We apply the construction in the proof of Theorem 5.12 with $\frac{n}{2}$ and $\frac{k}{2}$. Set $2^{k_2}, 3^{k_3} \leq \frac{\sqrt{kn}}{4}$. There exist a, b and ℓ satisfying the following equation.

$$|a2^{k_2} - b3^{k_3}| = \ell \qquad\qquad a2^{k_2}, b3^{k_3} \leq \frac{n}{2}, \ell < \frac{k}{2} \tag{13}$$

We show that there does not exist a weak protocol for T_k of cost $\max(2^{k_2}, 3^{k_3})$. By Lemma 4.2 it suffices to show that A^{T_k} has a submatrix with 3 distinct rows. We use solutions to Equation (13) to construct this submatrix. Assume $a2^{k_2} \geq b3^{k_3}$. By Lemma 3.9 we may assume $2^{k_2}, 3^{k_3} \geq \max(k, \sqrt{n})$ and hence $a2^{k_2} \geq k$. We choose the submatrix V of A

$$\begin{aligned} V &= \begin{pmatrix} 0 & a2^{k_2} & 2 \cdot a2^{k_2} \\ \times & a2^{k_2} - b3^{k_3} & 2 \cdot a2^{k_2} - b3^{k_3} \\ \times & \times & 2(a2^{k_2} - b3^{k_3}) \end{pmatrix} \\ &= \begin{pmatrix} 0 & a2^{k_2} & 2 \cdot a2^{k_2} \\ \times & \ell & \ell + a2^{k_2} \\ \times & \times & 2\ell \end{pmatrix} \\ \Rightarrow \quad V^{T_k} &= \begin{pmatrix} 0 & 1 & 1 \\ \times & 0 & 1 \\ \times & \times & 0 \end{pmatrix} \end{aligned}$$

We need to ensure that all entries in the fooling set are valid. The largest entry in the fooling set is $2 \cdot a2^{k_2}$. From Equation (13), we have $2 \cdot a2^{k_2} \leq n$. By Lemma 4.2 a weak protocol cannot exist since V^{T_k} has at least 3 distinct columns. Hence $\max(2^{k_2}, 3^{k_3}) > \frac{\sqrt{nk}}{4}$. Note that $2a2^{k_2} \leq n$, on the other hand, $a2^{k_2} \geq k$. Combining the inequalities, we obtain $k \leq \frac{n}{2}$.□

We believe that this bound holds for $k \leq \frac{n}{2}$. It is natural to ask if one can show linear bounds for all $k > \frac{n}{2}$. The next theorem shows that the answer is no (see Figure 2). It explains the remark in the introduction that the weak degree of the AND function is $\Theta(\sqrt{n})$.

Theorem 5.15 $\Delta(T_k) = \Delta(n - k + 1)$.

Proof: Assume that there is a weak protocol for T_k where the players read k_2 and k_3 digits respectively. On an input w, let $i \equiv w \bmod 2^{k_2}, j \equiv w \bmod 3^{k_3}$. Since both players know the value of n, they can compute

$$\begin{aligned} i' &\equiv (n - i) \bmod 2^{k_2} \equiv (n - w) \bmod 2^{k_2} \\ j' &\equiv (n - j) \bmod 3^{k_3} \equiv (n - w) \bmod 3^{k_3} \end{aligned}$$

Now if the players use the protocol for T_k with the values i' and j' instead, they can differentiate the values w such that $n - w < k$ and $n - w \geq k$. This is then a weak protocol differentiating values of $w \geq n - k + 1$

and $w < n - k + 1$ of cost $\max(2^{k_2}, 3^{k_3})$. A symmetric argument shows that a weak protocol for T_{n-k+1} gives a weak protocol for T_k. $\square$

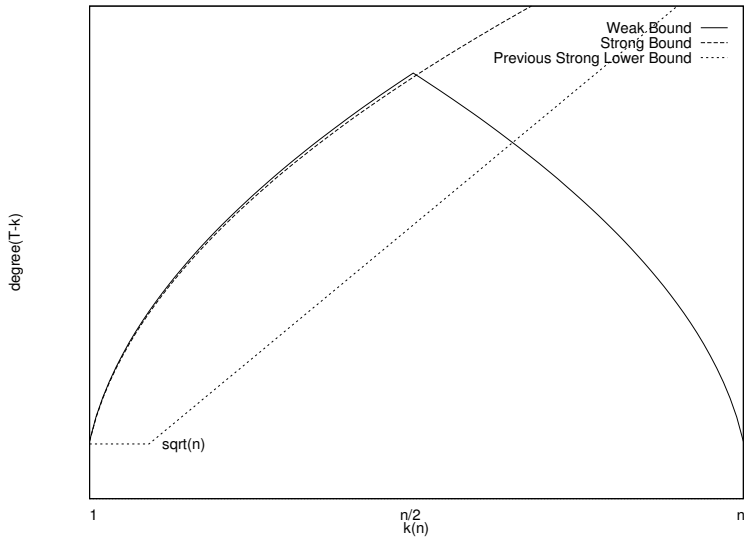

Figure 1: Degree of T_k over $\mathbb{Z}_6$

This shows that for $k > \frac{n}{2}$, there is a gap between the strong and weak degree.

6 Randomized Protocols

Simultaneous protocols where the players have access to a shared random string are well studied in communication complexity [KN97]. 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 beat the best deterministic lower bounds shown in Lemma 5.12. This shows that even when restricted to symmetric polynomials, randomness does in fact help to reduce the degree.

6.1 Types of Protocols

Definition 6.1 *[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 6.2 *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 6.3 *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 (see Lemma 6.9).

Lemma 6.4 *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: If a deterministic protocol with parameters k_2, k_3 exists, trivially there is a randomized protocol. For the other direction, if there does not exist a deterministic protocol, then by Lemma 3.4 $\exists\ i, j$ so that $f(a_{ij}) = 1$ but there are 0s in row i and column j. 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 $\frac{3}{5}$.

6.2 Randomized Protocols for Threshold

We first show a lower bound for any randomized protocol for T_k.

Lemma 6.5 *Any randomized protocol for T_k over $\mathbb{Z}_{pq}$ has cost $\Omega(\sqrt{n})$.*

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

We are unable to show any other lower bounds for such protocols though we believe they exist for functions like Mod_5 over Z_6. However, note that the above bound shows that even probabilistic representations of OR using symmetric polynomials need high degree. In contrast, if we allow general polynomials, we can construct probabilistic representations of degree $O(1)$.

Our upper bounds for T_k come from the observation that when $2^{k_2}, 3^{k_3} > \max(k, \sqrt{n})$, the matrix A^f looks like the matrix for equality of strings in two party communication complexity [KN97]. If $w < k$, then $i = j = w$. Hence both players get the same input, which is less than k. On the other hand, if $w \geq k$, then either $i = j \geq k$ or $i \neq j$. The case when either i or j is $\geq k$ is generally easy to handle. We can reduce the other cases to designing a protocol for the following problem: each player has a *color* in $\{0, \cdots, k-1\}$ and they are trying to decide if they have the same color.

Lemma 6.6 *There is a strong randomized protocol P_1 of cost $O(\max(k, \sqrt{n}))$ with two sided error for T_k such that*

- *If $w < k$, with probability $\frac{3}{5}$, both players say 0.*
- *If $w \geq k$ at least one player says 1 with probability at least $\frac{3}{5}$.*

Proof: Set $2^{k_2}, 3^{k_3} > \max(k, \sqrt{n})$. By setting the x's in A 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. Set $0 < p < 1$.

Protocol 6.7 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 $\frac{3}{5}$.□

The above protocol can be generalized to the t-player case.

Theorem 6.8 *T_k is strongly represented by a symmetric probabilistic polynomial over $\mathbb{Z}_m$ of degree $O(\max(k, n^{\frac{1}{t}}))$ with two sided error.*

Next, we design a one sided error protocol for the complementary problem $\overline{T}_k$.

Lemma 6.9 *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. Set $2^{k_2}, 3^{k_3} > \max(k, \sqrt{n})$

Protocol 6.10 Protocol 2

- If either player sees a number $\geq k$, 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 $i \in \overline{S}$.
- P_3 answers 1 on every $j \in \overline{S}$ 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 $\frac{1}{4}$. $\square$

Theorem 6.11 *$\overline{T}_k$ is strongly represented by a probabilistic polynomial over $\mathbb{Z}_6$ 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 6.12 *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 6.13 Protocol 3

- If $i, j < k$ the players both treat their inputs as bit strings and 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. $\square$

7 Conclusions

Our bounds for weak protocols for Mod-k in both the two player and multi-player cases require r to be sufficiently large. For instance we cannot prove a lower bound for Mod-2 over $\mathbb{Z}_{15}$. Since the only cases for which upper bounds are known is when $k = p_1^{a_1} \cdots p_t^{a_t}$ one would expect a lower bound of $\Omega(n)$ for all other k. For T_k with $t \geq 3$ players, the best upper bound we can show is $(nk)^{\frac{1}{2}+\varepsilon}$ assuming the *abc* conjecture. It seems that the right bound should be close to the $\Omega(n^{\frac{1}{t}} k^{\frac{t-1}{t}})$ lower bound.

We have shown that resolving the degree of Threshold functions for symmetric polynomials is equivalent to questions regarding Diophantine equations. These are rather hard questions and it does not seem that tight upper bounds can be shown unconditionally. Is showing tight bounds on threshold for general polynomials as hard? Perhaps we run into hard number theoretic questions because we are restricted to symmetric polynomials and proving upper bounds with general polynomials is easy. We do not believe that this is the case, but we cannot rule out this possibility. Proving lower bounds on the other hand can only be harder for general polynomials. The fact that the best known lower bound for OR is $\Omega(\log n)$ suggests that indeed lower bounds are much harder for general polynomials.

In all our strong protocols, each player outputs either 0 or 1. What about protocols where both players cannot simultaneously say 1? It is not hard to show an $\Omega(n)$ lower bound for symmetric polynomials representing OR with this restriction. Can one show a better lower bound for general polynomials representing OR with this restriction? A similar question is raised in [Gro00]

8 Acknowledgments

We thank Ernie Croot for many useful discussions and pointers and for help with Theorem 5.9. Thanks to Michael Filaseta for help with Theorem 5.4 and the reference to [Fil91]. Thanks to Richard Beigel for his comments [Bei03].

References

[BBR94] David A. Barrington, Richard Beigel, and Steven Rudich. Representing Boolean functions as polynomials modulo composite numbers. *Computational Complexity*, 4:367–382, 1994.

[Bei93] Richard Beigel. The polynomial method in circuit complexity. *Structures in Complexity Theory: 8th Annual Conference*, pages 82–95, 1993.

[Bei03] Richard Beigel. Personal communication. 2003.

[BGL03] Nayantara Bhatnagar, Parikshit Gopalan, and Richard J. Lipton. Symmetric polynomials over $\mathbb{Z}_m$ and simultaneous communication protocols. *Proceedings of the* 44^{th} *Annual Symposium on the Foundations of Computer Science*, 2003.

[BGL04] Nayantara Bhatnagar, Parikshit Gopalan, and Richard J. Lipton. The degree of threshold mod 6 and Diophantine equations. Technical Report ECCC TR04-022, Electronic Colloqium on Computational Complexity, 2004.

[CFL83] Ashok Chandra, Merrick Furst, and Richard J. Lipton. Multi-party protocols. *Proceedings of the 15th Annual ACM Symposium on Theory of Computing*, pages 94–99, 1983.

[Fil91] Michael Filaseta. A generalization of an irreducibility theorem of I. Schur. *Acta Arithmetica*, 58(3):251–272, 1991.

[Gra97] Andrew Granville. Arithmetic properties of binomial coefficients. *Canadian Mathematical Society Conference Proceedings*, 20:253–275, 1997.

[Gra98] Andrew Granville. *abc* means we can count squarefrees. *International Mathematical Research Notices*, 19:1224–1231, November 1998.

[Gre00] 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*, 2, 1995.

[Gro00] Vince Grolmusz. Superpolynomial size set-systems with restricted intersections mod 6 and explicit Ramsey graphs. *Combinatorica*, 20(1):71–86, 2000.

[GT02] Andrew Granville and Thomas J. Tucker. It's as easy as *abc*. *Notices of the AMS*, 49(10):991–1009, 2002.

[HW85] G.H. Hardy and E.M. Wright. *An Introduction to the Theory of Numbers.* Clarendon Press, Oxford, 1985.

[KN97] Eyal Kushilevitz and Noam Nisan. *Communication Complexity.* Cambridge University Press, 1997.

[MP68] Marvin Minsky and Seymour Papert. *Perceptrons: an Introduction to Computational Geometry.* MIT Press, 1968.

[Raz87] Alexander Razborov. Lower bounds for the size of circuits of bounded depth with basis $\{\wedge, \oplus\}$. *Methematical Notes of the Academy of Science of the USSR*, (41):333–338, 1987.

[Smo87] Roman Smolensky. Algebraic methods in the theory of lower bounds for Boolean circuit complexity. *Proceedings of the Nineteenth Annual ACM Symposium on Theoretical Computer Science.*, pages 77–82, 1987.

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

[TB98] Gabor Tardos and David Barrington. A lower bound on the mod 6 degree of the OR function. *Computational Complexity*, 7:99–108, 1998.

[Tsa96] Shi-Chun Tsai. Lower bounds on representing Boolean functions as polynomials in $\mathbb{Z}_m$. *SIAM Journal of Discrete Mathematics*, 9:55–62, 1996.

[Yao79] Andrew C. Yao. Some complexity questions related to distributive computing. *Proceedings of the 11th Annual ACM Symposium on Theory of Computation*, pages 209–213, 1979.

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

We first show that low degree polynomials depend on only a few bits of the base p representation of the weight. The proof uses Kummer's Theorem, a proof of which can be found in [Gra97].

Theorem A.1 (Kummer's Theorem) *The largest power of p that divides $\binom{n}{k}$ equals the number of carries when k and $n-k$ are added in base p.*

Corollary A.2 *If $k < p^l$, $\binom{w}{k} \bmod p^a$ depends only on the first $l+a-1$ digits of w in base p.*

Proof: This is equivalent to proving

$$\binom{w}{k} \equiv \binom{w+p^{\ell+a-1}}{k} \bmod p^a$$

Let $1 \le j \le k$. Then $j < p^\ell$ which implies $j_i = 0$ for $i \ge \ell$. When we add j and $(p^{\ell+a-1} - j)$ we get at least a carries. By Kummer's theorem,

$$\begin{aligned} \binom{p^{\ell+a-1}}{j} &\equiv 0 \bmod p^a \quad 1 \le j < p^\ell \qquad (14) \\ \binom{w+p^{l+a-1}}{k} &= \sum_{j=0}^{k} \binom{w}{k-j}\binom{p^{l+a-1}}{j} \\ &\equiv \binom{w}{k} \bmod p^a \qquad \text{by (14)} \end{aligned}$$

□

Corollary A.3 *Let $k < p^\ell$. Let $f : \{0,1\}^n \to \mathbb{Z}_{p^a}$ be computed by a symmetric polynomial $P(X)$ of degree k. Then f is a function of only the $\ell + a - 1$ least significant digits of w in base p.*

We next show that a function depending on few lower order digits of the weight can be computed by a low degree polynomial.

Lemma A.4 *For $0 \leq c \leq p-1$, there exist univariate polynomials $\Delta_c(Y) \in \mathbb{Z}_{p^a}[Y]$ of degree at most pa so that*

$$\Delta_c(y) \equiv \begin{cases} 1 \bmod p^a & y \equiv c \bmod p \\ 0 \bmod p^a & y \not\equiv c \bmod p \end{cases}$$

Proof: Let ϕ denote Euler's totient function. Consider the polynomial $Y^{\phi(p^a)}$.

$$y \not\equiv 0 \bmod p \Rightarrow y^{\phi(p^a)} \equiv 1 \bmod p^a, \quad y \equiv 0 \bmod p \ \Rightarrow y^{\phi(p^a)} \equiv 0 \bmod p^a$$

The second congruence uses the fact that $\phi(p^a) \geq a$. Hence we can set

$$\Delta_0(Y) = 1 - Y^{\phi(p^a)}, \quad \Delta_c(Y) = \Delta_0(Y - c)$$

To prove the bound on the degree, observe that $Q(Y) = (Y^p - Y)^a$ is a monic polynomial of degree pa which is identically 0 on $\mathbb{Z}_{p^a}$ by Fermat's theorem . Hence we can divide $\Delta_c(Y)$ by $Q(Y)$ and the reminder is a polynomial of degree less than pa which represents the same function on $\mathbb{Z}_{p^a}$. $\square$

Theorem A.5 *Let $f : \{0,1\}^n \to \mathbb{Z}_{p^a}$ be a symmetric function which depends only on the first ℓ digits of w in base p. Then f is computed by $P(X) \in \mathbb{Z}_{p^a}[X]$ where $deg(P) < 2p^\ell a$.*

Proof: Let $b \in \{0,1\}^n$ have weight w. By Lemmas A.4 and 2.6,

$$\Delta_c(S_{p^j}(b)) \equiv 1 \bmod p^a \iff S_{p^j}(b) \equiv c \bmod p \iff w_j = c \bmod p$$

Similarly we construct a polynomial that is 1 only if $w_j = c_j$ for $j \leq \ell$.

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

Let $f(c_0, \cdots c_{\ell-1})$ denote the value of f when the first ℓ digits are set to $c_0, \cdots, c_{\ell-1}$ in base p. The desired polynomial is

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

The degree of this polynomial is bounded by

$$\sum_{j=0}^{\ell-1} pa \cdot p^j = pa \frac{p^\ell - 1}{p-1} \leq 2p^\ell a$$

$\square$