In Brute-Force Search of Correlation Bounds for Polynomials

Frederic Green* Daniel Kreymer† Emanuele Viola†

March 19, 2011

Abstract

We report on some initial results of a brute-force search for determining the maximum correlation between degree-d polynomials modulo p and the n-bit mod q function. For various settings of the parameters n, d, p, and q, our results indicate that symmetric polynomials yield the maximum correlation. This contrasts with the previously-analyzed settings of parameters, where non-symmetric polynomials yield the maximum correlation.

We also prove new properties of maximum-correlation polynomials, and use those to obtain a new setting of parameters where those polynomials are not symmetric.

1 Introduction

Brute-force search is frequently used in cryptography and combinatorics, for two up-to-date accounts see for example [BK10] and [Rad09]. It is also occasionally used in theoretical computer science, for example Williams [Wil07, Chapter 5] uses it to search over certain proofs of time-space lower bounds for SAT. But overall, brute-force search seems to be used little in theoretical computer science. We wish to reverse this trend. We believe that the combination of computational resources that are easily available and the apparent lack of progress on fundamental lower-bound questions make for a suitable territory.

For starters, we report on initial results on obtaining correlation bounds for polynomials. This challenge is surveyed in [Vio09, Chapter 1]. The more specific challenge we tackle is that of obtaining upper bounds on the "maximum correlation" between multivariate polynomials of degree d in n variables modulo p, and the mod q function [Smo87, AB01, Gre04, Bou05, GRS05, DMRS06, Vio06, VW09, Cha07, GR10]. The quantity of interest is the following (cf. [Gre04]):

$$C(n,d,p,q) := \frac{1}{2^n} \max_f \left| \sum_{x \in \{0,1\}^n} \omega_p^{f(x)} \cdot \omega_q^{\sum_i x_i} \right|,$$

*Email: fgreen@black.clarku.edu

†Supported by NSF grant CCF-0845003, REU supplement. Email: {dank,viola}@ccs.neu.edu

where the maximum is over n-variable degree-d polynomials f with coefficients in $\{0, 1, \ldots, p-1\}$, and $\omega_k = e^{2\pi \cdot i/k}$ is the k-th complex principal root of unity.

It seems natural to conjecture that for p and q fixed and coprime, $C(n, d, p, q)$ is exponentially small in n, even for some $d = n^{\Omega(1)}$. But current proofs only establish this for $d < \log n$, see [Vio09, Chapter 1].

We follow the lead of Green who settles the correlation between quadratic polynomials mod 3 and the mod 2 (a.k.a. parity) function:

Theorem 1.1 ([Gre04])**.** *For all n: $C(n, d = 2, p = 3, q = 2) = \left(\frac{\sqrt{3}}{2}\right)^{\lceil n/2 \rceil}$.*

Moreover, Green and Roy [GR10] determine all polynomials yielding the maximum value of C (listed in §2.2). We call such polynomials *optimal*. A surprising fact is that these polynomials are never symmetric – they are not invariant under permutation of the variables.

Later, Dueñez, Miller, Roy, and Straubing determine $C(n, d = 2, p, q = 2)$ for other values of p, *but only up to $n = 10$ variables* [DMRS06]. The corresponding optimal polynomials have exactly the same structure as those in 1.1, and in particular are not symmetric.

2 Our results

We perform brute-force search to obtain new correlation bounds for uncharted settings of parameters (described below). The code is available at `http://www.ccs.neu.edu/home/viola`.

We often find that *symmetric* polynomials yield the maximum correlation. This contrasts with the previous results mentioned in §1, which obtained non-symmetric polynomials, and gives hope that a general proof technique may be within reach. If one could prove that for the relevant setting of parameters some optimal polynomial is symmetric, then the conjecture mentioned in §1 would be proved, because it can be shown that for symmetric polynomials C is exponentially small in n for degree as high as n^α for some $\alpha \in (0, 1)$ depending on p and q only [CGT96].

The next definition is useful to state our results succinctly.

Definition 2.1. *Let s(n,d) be the homogeneous elementary symmetric polynomial over n variables and degree d.*

2.1 Polynomials mod $p = 2$ vs. the mod $q = 3$ function

We report below on our results for polynomials mod $p = 2$ vs. the mod $q = 3$ function. For concreteness, we mention this means that we are computing

$$C(n, d, 2, 3) := \frac{1}{2^n} \max_f \left| \sum_{x \in \{0,1\}^n} (-1)^{f(x)} \cdot \omega_3^{\sum_i x_i} \right|.$$

Each entry in the next tables contains the optimal polynomials and the associated value for $C(n, d, p, q)$. We set the constant term to 0. Its value does not affect C.

	d = 2	d = 3	d = 4	d = 5
n = 2	$s(2,1)$ $\sqrt{9}/2^2$ ≈ 0.7500			
n = 3	$s(3,1)$ $s(3,2)$ $\sqrt{27}/2^3$ ≈ 0.6495	$s(3,3)+s(3,1)$ $s(3,3)+s(3,2)$ $\sqrt{31}/2^3$ ≈ 0.6960		
n = 4	$s(4,2)$ $s(4,2)+s(4,1)$ $\sqrt{97}/2^4$ ≈ 0.6156	$s(4,3)+s(4,2)$ $\sqrt{121}/2^4$ ≈ 0.6875	$s(4,3)+s(4,2)$ $\sqrt{121}/2^4$ ≈ 0.6875	
n = 5	$s(5,2)+s(5,1)$ $\sqrt{363}/2^5$ ≈ 0.5954	$s(5,3)$ $s(5,3)+s(5,2)$ $\sqrt{381}/2^5$ ≈ 0.6100	$s(5,4)+s(5,3)+s(5,1)$ $\sqrt{441}/2^5$ ≈ 0.6563	$s(5,5)+s(5,4)+s(5,2)+s(5,1)$ $s(5,5)+s(5,3)+s(5,2)$ $\sqrt{463}/2^5$ ≈ 0.6724
n = 6	$s(6,2)$ $s(6,2)+s(6,1)$ $\sqrt{1351}/2^6$ ≈ 0.5743	$s(6,3)$ $\sqrt{1521}/2^6$ ≈ 0.6094		
n = 7	$s(7,2)$ $\sqrt{5043}/2^7$ ≈ 0.5548			
n = 8	$s(8,2)$ $s(8,2)+s(8,1)$ $\sqrt{18817}/2^8$ ≈ 0.5358			

2.2 Polynomials mod $p = 3$ vs. the mod $q = 2$ function

We report below on our results for polynomials mod $p = 3$ vs. the mod $q = 2$ function. In order to make it easier to compare our results with the previous ones in the literature, in this setting we actually think of the variables as ranging over $\{-1, 1\}$ as opposed to $\{0, 1\}$. One can always switch between the two with a linear transformation, so this does not change C, but it does change the polynomials. For concreteness, we mention this means that we are

computing

$$C(n,d,3,2) := \frac{1}{2^n} \max_f \left| \sum_{x \in \{-1,1\}^n} \omega_3^{f(x)} \cdot \prod_i x_i \right|.$$

The results are listed up to multiplying a variable by -1, and up to adding a constant term – two operations that it is easy to see do not affect C.

	d = 3	d = 4
n = 3	$s(3,3)$ $\sqrt{48}/2^3$ ≈ 0.8660	
n = 4	$s(4,3)+s(4,2)+s(4,1)$ $s(4,3)-s(4,2)+s(4,1)$ $\sqrt{171}/2^4$ ≈ 0.8173	$s(4,4)$ $\sqrt{192}/2^4$ ≈ 0.8660
n = 5	$s(5,3)+s(5,1)$ $\sqrt{675}/2^5$ ≈ 0.8119	

For context, we mention that for any n and $d = 2$ the optimal polynomials are characterized [GR10]. Up to a constant term and permutation of the variables, the optimal polynomials are of the form

$$\pm x_1 x_2 \pm x_3 x_4 \pm \cdots \pm x_{n-1} x_n$$

if n is even, and

$$\pm x_1 x_2 \pm x_3 x_4 \pm \cdots \pm x_{n-2} x_{n-1} + x_n$$

if n is odd.

3 A property of optimal polynomials for parity

In this section we prove the following result:

Theorem 3.1. *For every even n, even d, and any odd p: $C(n-1,d,p,2) = C(n,d,p,2)$.*

Using this result we can show that for degree 4 there are cases in which symmetric polynomials are not optimal. Indeed, when restricted to symmetric polynomials, the values for $(8,4,3,2)$ and $(7,4,3,2)$ are respectively $\sqrt{36972}/2^8 \approx 0.7510$ and $\sqrt{9747}/2^7 \approx 0.7713$ (details of the simple computation omitted). These two values are different, hence incompatible with the above theorem.

We now proceed with the proof. We rely on two Lemmas below which are similar to Lemmas 3.4 and 3.5 in [Gre04].

Let

$$S(t,n) = \frac{1}{2^n} \sum_{x \in \{1,-1\}^n} \left(\prod_{i=1}^{n} x_i \right) \omega_m^{t(x)},$$

where t is a polynomial in $\mathbb{Z}_m[x_1, \ldots, x_n]$ and $\omega_m = e^{2\pi i/m}$.

Lemma 3.2. *If n is even, there exists a polynomial $e' \in \mathbb{Z}_m[x_1, ..., x_n]$ such that all of the monomials of e' are of even degree and,*

$$|S(t,n)| \leq |S(e',n)|.$$

Proof. Let $t(x) = e(x) + k(x)$ where $e, k \in \mathbb{Z}_m[x_1, \ldots, x_n]$ are polynomials such that all of the monomials of e are of even degree and the monomials of k are of odd degree. Then

$$\begin{aligned}
S(t,n) &= \frac{1}{2^n} \sum_{x \in \{1,-1\}^n} \left(\prod_{i=1}^{n} x_i \right) \omega_m^{t(x)} \\
&= \frac{1}{2^n} \sum_{x \in \{1,-1\}^n} \left(\prod_{i=1}^{n} x_i \right) \omega_m^{e(x)+k(x)} \\
&= \frac{1}{2^n} \sum_{x \in \{1,-1\}^n} \left(\prod_{i=1}^{n} x_i \right) \omega_m^{e(x)-k(x)} \\
&= \frac{1}{2} \cdot \frac{1}{2^n} \sum_{x \in \{1,-1\}^n} \left(\prod_{i=1}^{n} x_i \right) \omega_m^{e(x)} (\omega_m^{k(x)} + \omega_m^{-k(x)}) \\
&= \frac{1}{2} \cdot \frac{1}{2^n} \sum_{x \in \{1,-1\}^n} \left(\prod_{i=1}^{n} x_i \right) \omega_m^{e(x)} (\omega_m^{x_1 k(x)} + \omega_m^{-x_1 k(x)}),
\end{aligned}$$

where in the third equality we made the substitution $x_i \mapsto -x_i$, and in the last we used the fact that $\omega_m^{k(x)} + \omega_m^{-k(x)} = \omega_m^{x_1 k(x)} + \omega_m^{-x_1 k(x)}$ for $x_1 \in \{1, -1\}$. Now by the triangle inequality,

$$\begin{aligned}
|S(t,n)| &\leq \frac{1}{2} \cdot \frac{1}{2^n} \left| \sum_{x \in \{1,-1\}^n} \left(\prod_{i=1}^{n} x_i \right) \omega_m^{e(x)} (\omega_m^{x_1 k(x)} + \omega_m^{-x_1 k(x)}) \right| \\
&\leq \frac{1}{2} \cdot \frac{1}{2^n} \left| \sum_{x \in \{1,-1\}^n} \left(\prod_{i=1}^{n} x_i \right) \omega_m^{e(x)+x_1 k(x)} \right| + \frac{1}{2} \cdot \frac{1}{2^n} \left| \sum_{x \in \{1,-1\}^n} \left(\prod_{i=1}^{n} x_i \right) \omega_m^{e(x)-x_1 k(x)} \right|
\end{aligned}$$

Note that both $e + x_1 k$ and $e - x_1 k$ contain only even degree monomials. Let e' be the $e + x_1 k$ or $e - x_1 k$ that gives the larger sum. Then, $|S(t,n)| \leq |S(e',n)|$. □

Observe that if $deg(t) = d$ where d is even, then $deg(x_1 k) \leq d$. Hence the theorem above implies that if d is even and n is even, there are polynomials e' with $deg(e') = deg(t)$ consisting of only even-degree terms such that $|S(e',n)|$ is an upper bound on $|S(t,n)|$. The next Lemma implies furthermore that there are such e' where $|S(e',n)|$ is actually equal to the maximal value for $n - 1$.

Lemma 3.3. *Let n be even, and let a polynomial $t \in \mathbb{Z}_m[x_1, ..., x_n]$ be given consisting only of terms of even degree. Then there is a polynomial $t' \in \mathbb{Z}_m[x_2, ..., x_n]$ of only even degree terms, and a polynomial $k \in \mathbb{Z}_m[x_2, ..., x_n]$ of only odd degree terms such that,*

$$S(t, n) = S(t' + k, n - 1).$$

Conversely, given any polynomial $t' \in \mathbb{Z}_m[x_2, ..., x_n]$ of only even degree terms and a $k \in \mathbb{Z}_m[x_2, ..., x_n]$ of only odd degree terms, there is a polynomial $t \in \mathbb{Z}_m[x_1, x_2, ..., x_n]$ of only even degree terms such that the above equality holds.

Proof. Let $t(x) = t_2'(x) + x_1 k_2(x)$, where $t_2' \in \mathbb{Z}_m[x_2, \ldots, x_n]$ and $k_2 \in \mathbb{Z}_m[x_2, \ldots, x_n]$ only depend on $x_2, \ldots, x_n$. Then, performing the sum over x_1,

$$\begin{aligned} S(t,n) &= \frac{1}{2^n} \sum_{x \in \{1,-1\}^n} \left(\prod_i x_i \right) \omega_m^{t_2'(x) + x_1 k_2(x)} \\ &= \frac{1}{2^n} \sum_{x \in \{1,-1\}^{n-1}} \left(\prod_{i=2}^{n} x_i \right) \omega_m^{t_2'(x)} (\omega_m^{k_2(x)} - \omega_m^{-k_2(x)}) \\ &= \frac{1}{2^{n-1}} \sum_{x \in \{1,-1\}^{n-1}} \left(\prod_{i=2}^{n} x_i \right) \omega_m^{t_2'(x) + k_2(x)}, \end{aligned}$$

where in the third equality we used the transformation $x_i \mapsto -x_i$. This establishes both implications, since we can work forwards or backwards in the chain of equalities, and t_2 and k_2 are completely general polynomials of $n - 1$ variables (consisting of even and odd degree monomials, respectively). □

This shows that for n even, as we range over all possible sums $S(t_2' + k_2, n - 1)$ we also range over all possible sums $S(t, n)$ where t has only even monomials. In particular, all optimal values for the sum for $n - 1$ are in 1-1 correspondence with all optimal values for the sum for n, in the case that d is even (since when d is odd, the proof of the first theorem increases the degree). Furthermore, this tells us that as n increases, the optimal value must decrease in "steps," not for all values of n.

References

[AB01] Noga Alon and Richard Beigel. Lower bounds for approximations by low degree polynomials over Z_m. In *16th Conference on Computational Complexity (CCC)*, pages 184–187. IEEE, 2001.

[BK10] Joppe Bos and Marcelo Kaihara. Playstation 3 computing breaks 2^{60} barrier: 112-bit prime ECDLP solved, 2010.

[Bou05] Jean Bourgain. Estimation of certain exponential sums arising in complexity theory. *C. R. Math. Acad. Sci. Paris*, 340(9):627–631, 2005.

[CGT96] Jin-Yi Cai, Frederic Green, and Thomas Thierauf. On the correlation of symmetric functions. *Mathematical Systems Theory*, 29(3):245–258, 1996.

[Cha07] Arkadev Chattopadhyay. Discrepancy and the power of bottom fan-in in depth-three circuits. In *48th Symposium on Foundations of Computer Science (FOCS)*, pages 449–458. IEEE, 2007.

[DMRS06] Eduardo Dueñez, Steven J. Miller, Amitabha Roy, and Howard Straubing. Incomplete quadratic exponential sums in several variables. *J. Number Theory*, 116(1):168–199, 2006.

[GR10] Frederic Green and Amitabha Roy. Uniqueness of optimal mod 3 circuits for parity. *Journal of Number Theory*, 130:961 – 975, 2010.

[Gre04] Frederic Green. The correlation between parity and quadratic polynomials mod 3. *J. Comput. System Sci.*, 69(1):28–44, 2004.

[GRS05] Frederic Green, Amitabha Roy, and Howard Straubing. Bounds on an exponential sum arising in Boolean circuit complexity. *C. R. Math. Acad. Sci. Paris*, 341(5):279–282, 2005.

[Rad09] Stanislaw Radziszowski. Small ramsey numbers, 2009. Dynamic Survey.

[Smo87] Roman Smolensky. Algebraic methods in the theory of lower bounds for Boolean circuit complexity. In *19th Symposium on the Theory of Computing (STOC)*, pages 77–82. ACM, 1987.

[Vio06] Emanuele Viola. New correlation bounds for GF(2) polynomials using Gowers uniformity. *Electronic Colloquium on Computational Complexity*, Technical Report TR06-097, 2006. www.eccc.uni-trier.de/.

[Vio09] Emanuele Viola. On the power of small-depth computation. *Foundations and Trends in Theoretical Computer Science*, 5(1):1–72, 2009.

[VW09] Emanuele Viola and Avi Wigderson. One-way multiparty communication lower bound for pointer jumping with applications. *Combinatorica*, 29(6):719–743, 2009.

[Wil07] Ryan Williams. *Algorithms and Resource Requirements for Fundamental Problems*. PhD thesis, Carnegie Mellon University, 2007.