ISSN 1342-2812

Research Reports on Mathematical and Computing Sciences

Can low degree polynomials compute modulo functions over finite fields?

Akinori Kawachi, Hidetoki Tanaka, and Osamu Watanbe

March 2009, C–259

Department of Mathematical and Computing Sciences
Tokyo Institute of Technology

SERIES C: Computer Science

Can low degree polynomials compute modulo functions over finite fields?

Akinori Kawachi* Hidetoki Tanaka* Osamu Watanbe*

Abstract

In this paper, we examine the computational limitation of low degree polynomials over finite fields. We prove that no $o(\log n)$-degree polynomial of n variables over $\mathbb{Z}_q$ can compute the modulo function MOD_m over $\mathbb{Z}_q^n$, where q is a prime and m is coprime to q. Our main technical contribution is to estimate a correlation between low degree polynomials and modulo functions over prime field $\mathbb{Z}_q$ by computing the Gowers uniformity of exponential functions, which generalizes Viola and Wigderson's estimation over $\mathbb{Z}_2$.

1 Introduction

1.1 Background

A *low degree polynomial* is one of the most fundamental objects in the field of the theoretical computer science. It often plays important roles in a number of the areas such as error-correcting codes, circuit complexity, probabilistic checkable proofs, etc. In particular, the computational power of the low degree polynomial has attracted much attention in the complexity theory since the seminal works by Razborov [Raz87] and Smolensky [Smo87], which proved an exponential lower bound for AC^0 and $\mathsf{AC}^0[p]$ for any prime p. The remarkable point of their works is to approximate constant-depth circuits in AC^0 and $\mathsf{AC}^0[p]$ with low degree polynomials over the binary field. We can say that low degree polynomials over the binary field are close to constant-depth circuits as a computational model in some sense.

Their technique is called the *polynomial method*. Let C be a class of functions, e.g., AC^0. It gives a lower bound for the class C following two steps: (1) We show that any function in C has high *correlation* with some low degree polynomial and then (2) show some specific function, e.g., the parity function, has low correlation with every low degree polynomial. By these two steps, we can conclude that no function in C computes the specific function.

The polynomial method is based on two notions we call the correlation and $\mathbb{Z}_q$ polynomials in this paper. For the standard polynomial method, the binary field is only considered in the notions. However, we here define generalized ones over $\mathbb{Z}_q$ for our purpose. The correlation intuitively measures the distance between two functions.

Definition 1.1 (correlation)**.** Let $f, g : \mathbb{Z}_q^n \to \{1, -1\}$. The correlation between f and g is defined as:

$$\mathrm{Corr}(f,g) = \left| \mathop{\mathrm{E}}_{x\in\mathbb{Z}_q^n}[f(x)g(x)] \right| = \left| \Pr_{x\in\mathbb{Z}_q^n}[f(x) = g(x)] - \Pr_{x\in\mathbb{Z}_q^n}[f(x) \neq g(x)] \right|.$$

*Department of Mathematical and Computing Sciences, Tokyo Institute of Technology, Email: {kawachi,tanaka7,watanabe}@is.titech.ac.jp

Also, the correlation between a function f and a class C of functions is defined as:

$$\mathrm{Corr}(f, C) = \max_{g \in C} \mathrm{Corr}(f, g).$$

We introduce a sort of polynomials called $\mathbb{Z}_q$ *polynomials* to adjust their output to $\{1, -1\}$.

Definition 1.2 ($\mathbb{Z}_q$ polynomials)**.** Let $g : \mathbb{Z}_p^n \to \mathbb{Z}$ be an integer-valued polynomial of n variables. We then define a $\mathbb{Z}_q$ polynomial $f : \mathbb{Z}_p^n \to \{1, -1\}$ of input $\mathbb{Z}_p^n$ as

$$f(x_1, x_2, \ldots, x_n) = \begin{cases} 1 & \text{if } q \mid g(x_1, x_2, \ldots, x_n) \\ -1 & \text{if } q \nmid g(x_1, x_2, \ldots, x_n). \end{cases}$$

The degree of f is defined as that of g. We denote by $P_d^{(q)}[p]$ a set of degree-d $\mathbb{Z}_q$ polynomials of input $\mathbb{Z}_p^n$. We simply write it as $P_d^{(q)}$ if $p = q$.

For example in [Smo87], he proved for a prime q and an integer m coprime to q that (1) we have $\mathrm{Corr}(f, P^{(q)}_{\mathrm{polylog}n}[2]) \geq 1 - 1/n^{\omega(1)}$ for every $f \in \mathsf{AC}^0[q]$ and (2) $\mathrm{Corr}(\mathrm{MOD}_m, P^{(q)}_{\mathrm{polylog}n}[2]) \leq 1/(n^{1/2-o(1)})$ for the modulo function MOD_m over $\mathbb{Z}_2$. This implies that no function in AC^0 can compute MOD_m. A modulo function $\mathrm{MOD}_m : \mathbb{Z}_p^n \to \{1, -1\}$ is generally defined as follows. (Again, we give a general definition over $\mathbb{Z}_p$ for our purpose, although the case where $p = 2$ was only considered in [Smo87].)

$$\mathrm{MOD}_m(x_1, x_2, \ldots, x_n) = \begin{cases} 1 & \text{if } m \mid \sum_{j=1}^n x_j \\ -1 & \text{if } m \nmid \sum_{j=1}^n x_j. \end{cases}$$

After the lower bounds were proven for AC^0, researchers started to investigate a new technique to prove lower bounds for higher circuit classes such as ACC. For this new goal, they utilized the low degree polynomials and their correlation again.

For the investigation, they often discussed depth-3 circuits of the special form $\mathrm{MAJ} \circ \mathrm{MOD}_q \circ \mathrm{AND}_d$. This circuit consists of three levels. The bottom level has only AND_d, AND gate with at most d fan-in, the middle level has only MOD_q, and the top level is the majority gate MAJ. Interestingly, it is shown by Allender [All89] that every function in AC^0 can be computed by quasipolynomial-size circuits of this form with $d = \mathrm{polylog}n$.

To compare the computational power of AC^0 with that of ACC, Alon and Beigel discussed the hardness of the modulo function MOD_m, which is in ACC, against the depth-3 circuits [AB01]. They demonstrated that $\mathrm{MAJ} \circ \mathrm{MOD}_q \circ \mathrm{AND}_d$ of polynomial size cannot compute MOD_m if $d = O(1)$ and q is coprime to m. In what follows, we assume that q is always coprime to m. Their proof reduced proving the circuit lower bound to estimating upper bounds of the correlation between its depth-2 subcircuits $\mathrm{MOD}_q \circ \mathrm{AND}_d$ and the target function MOD_m by using the well-known discriminator lemma [HMP$^+$93]. The low degree polynomials then model the subcircuits, and thus the essential part of their proof was reduced to proof of $\mathrm{Corr}(\mathrm{MOD}_m, P_d^{(q)}[2]) = o(1)$. More precise bounds on the correlation were given by the results Bourgain [Bou05] and Green, Roy, and Straubing [GRS05], which proved exponentially small upper bounds. Viola and Wigderson also gave a simple proof for the bound of $\mathrm{Corr}(\mathrm{MOD}_m, P_d^{(2)})$ using properties of the Gowers uniformity [VW08]. The best known bound for general case is due to Chattopadhyay [Cha06]. He proved that $\mathrm{Corr}(\mathrm{MOD}_m, P_d^{(q)}[2]) \leq \exp\left(-\Omega(n/(q2^{q-1})^d)\right)$.

As mentioned above, a low degree polynomial was implicitly utilized as a computational model in the circuit complexity theory. Several recent works more explicitly analyzed the

hardness against the low degree polynomial as a computational model not only over the binary field but also general ones. For example, Viola and Wigderson gave the so-called XOR lemma, which generally provides how to amplify the hardness, for polynomials over the binary field [VW08]. Bogdanov constructed a pseudorandom generator that fools low degree polynomials over the field whose size is not so small [Bog05]. His result was improved by a number of intensive studies [BV07, Lov08, Vio08]. Recently, Kaufman and Lovett demonstrated that the average-case approximability of a polynomial over general finite fields by low degree polynomials can be reduced to the worst-case computability of a polynomial by low degree polynomials [KL08].

1.2 Our Results

As shown in the recent works, a low degree polynomial is actively studied as a computational model beyond the binary field. However, it was not clarified sufficiently how low degree polynomials themselves are powerful over general finite field.

In this paper, we discuss the computational limitation of the low degree polynomials over prime fields by following the line of studies initiated by Alon and Beigel [AB01]. Our main result is stated as follows:

Theorem 1.3. *Let q be any odd prime and let m be any integer coprime to q. Then, we have*

$$\mathrm{Corr}(\mathrm{MOD}_m, P_d^{(q)}) \leq \exp(-\Omega(n/q^d)).$$

Now we consider a function $\mathrm{MOD}_m^{(q)}$, that is a simple generalization of MOD_m.

Definition 1.4. $\mathrm{MOD}_m^{(q)}$ is a function $\mathbb{Z}_q^n \to \mathbb{Z}_m$ such that

$$\mathrm{MOD}_m^{(q)}(x_1, \ldots, x_n) := \sum_{j=1}^{n} x_j \mod m.$$

By a simple calculation, we directly obtain the following corollary related to $\mathrm{MOD}_m^{(q)}$.

Corollary 1.5. *Let q be an odd prime and $m < q$ be coprime to q. Then there is no $o(\log n/\log q)$-degree polynomial $\mathbb{Z}_q^n \to \mathbb{Z}_q$ can compute $\mathrm{MOD}_m^{(q)}$*

Proof. Assume that there is an $o(\log n/\log q)$-degree polynomial $p : \mathbb{Z}_q^n \to \mathbb{Z}_q$ that can compute $\mathrm{MOD}_m^{(q)}$. We construct an $o(\log n/\log q)$-degree $\mathbb{Z}_q$ polynomial p' from p such that $p'(x) = 1$ if $p(x) = 0$, and $p'(x) = -1$ if $p(x) \neq 0$. Then, p' can compute MOD_m, which contradicts that no $o(\log n/\log q)$-degree $\mathbb{Z}_q$ polynomial can compute MOD_m from Theorem 1.3. □

Therefore, polynomials over $\mathbb{Z}_q$ require at least $\Omega(\log n)$ degree to compute $\mathrm{MOD}_m^{(q)}$ over $\mathbb{Z}_q^n$ for a constant q.

Our approach is a generalization of Viola and Wigderson's work, which exploits properties of the Gowers uniformity [VW08]. The Gowers uniformity was originally introduced by Gowers [Gow98, Gow01] and independently by Alon, Kaufman, Krivelevich, Litsyn and Ron [AKK+03].

Many applications of the Gowers uniformity have already found in the theoretical computer science such as linearity testing in PCP [Sam07, ST06] and pseudorandom generators for low degree polynomials [Bog05, BV07]. We apply it to estimation of the correlation over a prime field by generalizing Viola and Wigderson's estimation over $\mathbb{Z}_2$.

The main technical issue of our result is to estimate the Gowers uniformity of an exponential function over a prime field. Viola and Wigderson also gave a similar estimation for the Gowers uniformity over $\mathbb{Z}_2$. The estimation for the case of $\mathbb{Z}_2$ was simply done by the property of $\mathbb{Z}_2$. Generalizing the underlying field, the estimation becomes complicated, as seen in Section 3. We then require several new calculation methods for a prime field, which may be of independent interest.

2 Gowers Uniformity

We present the definition of the Gowers uniformity and its properties. For the definition, we first introduce several notions. The conjugate of a complex number $a + ib$, where i is the imaginary unit, is denoted by $\overline{a + ib}$. For a complex number z and an integer j, we denote by $z^{\underline{j}}$ the complex number z if j is an even, and its conjugate $\bar{z}$ if j is an odd. A set $\{1, 2, \ldots, n\}$ is denoted by $[n]$. The definition of the Gowers uniformity is given as follows.

Definition 2.1 (Gowers uniformity over $\mathbb{Z}_q$ [Gow98, Gow01])**.** Let $d \geq 0$, $f : \mathbb{Z}_q^n \to \mathbb{C}$, $\oplus$ be the addition over $\mathbb{Z}_q$. Then the degree-d Gowers uniformity of f over $\mathbb{Z}_q$ is defined as

$$U_q^d(f) := \mathop{\mathrm{E}}_{x,y_1,\ldots,y_d \in \mathbb{Z}_q^n} \left[\prod_{S \subseteq [d]} f\left(x \oplus \bigoplus_{j \in S} y_j \right)^{\underline{|S|}} \right].$$

There are useful properties of the Gowers uniformity.

Proposition 2.2 ([GT08, VW08])**.** *For every function $f : \mathbb{Z}_q^n \to \mathbb{C}$,*

1. $\left| \mathop{\mathrm{E}}_{x \in \mathbb{Z}_q^n} [f(x)] \right| = \sqrt{U_q^1(f)}$,
2. *for every k, $U_q^k(f) \leq \sqrt{U_q^{k+1}(f)}$,*
3. *for every $\mathbb{Z}_q$ polynomial p of degree at most d, $U_q^{d+1}(f \cdot p) = U_q^{d+1}(f)$,*
4. *for every function $f' : \mathbb{Z}_q^{n'} \to \mathbb{C}$, $U_q^k(f \cdot f') = U_q^k(f) \cdot U_q^k(f')$, where $(f \cdot f')(x, y) = f(x)f'(y)$.*

3 Overview

Our goal is to estimate of the correlation between the modulo function and $\mathbb{Z}_q$ polynomials, that is $\mathrm{Corr}(\mathrm{MOD}_m, P_d^{(q)})$.

Theorem 3.1. *For any prime $q \geq 3$, any integer m coprime to q,*

$$\mathrm{Corr}(\mathrm{MOD}_m, P_d^{(q)}) \leq \exp\left(-\alpha \cdot \frac{n}{q^d} \right),$$

where $\alpha > 0$ is a constant that depends on m only.

Since our proof of the above theorem is technically complicated and involved, we exhibit the overview of our proof to obtain intuitions in this section.

We first show the correlation $\mathrm{Corr}(\mathrm{MOD}_m, P_d^{(q)})$ is bounded by the Gowers uniformity of the exponential function $e_m^a(x) = \exp(2\pi iax/m)$ above by using the properties of the Gowers uniformity. This method is a straightforward extension of the proof of Viola and Wigderson [VW08], which is proven by Proposition 2.2.

Lemma 3.2 ([VW08])**.** *For any $a \in [m-1]$,*

$$\mathrm{Corr}(\mathrm{MOD}_m, P_d^{(q)}) \leq (m-1)\left(U_q^{d+1}(e_m^a)\right)^{n/2^{d+1}}.$$

Hence, our task is reduced to the estimation of the Gowers uniformity $U_q^{d+1}(e_m^a)$. Our next target is to prove the following lemma, which is the main technical lemma of our result.

Lemma 3.3. *Let $q \geq 3$ be a prime, m be coprime to q, and $a \in [m-1]$. Then for any even $k \geq 2$,*

$$U_q^k(e_m^a) \leq 1 - \alpha \cdot \left(\frac{2}{q}\right)^k,$$

where $\alpha > 0$ is a constant that depends on m only.

This lemma claims that the Gowers uniformity is sufficiently smaller than 1. By this lemma, the upper bound $(U_q^{d+1}(e_m^a))^{n/2^{d+1}}$ of the correlation becomes exponentially small. Note that it is sufficient for our purpose to only estimate the case where k is an even, which makes our analysis simpler. For an odd k, we can use the degree-$(k+1)$ Gowers uniformity instead of the degree-k Gowers uniformity since $U_q^k(e_m^a) \leq \sqrt{U_q^{k+1}(e_m^a)} \leq U_q^{k+1}(e_m^a)$ by Proposition 2.2.

Now we move to the proof of Lemma 3.3. By some inductive argument, the Gowers uniformity of e_m^a can be bounded as follows.

$$U_q^k(e_m^a) \leq 1 - \left(\frac{2}{q}\right)^k \left\{1 - \frac{1 + 2\sum_{j=1}^{r} \cos\left(2\pi a g_j(k)/m\right)}{q}\right\},$$

where $r = (q-1)/2$ and $g_1(k), g_2(k), \ldots,$ and $g_r(k)$ are recursive sequences defined as

$$g_1(k) = \begin{cases} 2g_1(k-2) + g_2(k-2) & \text{if } k \geq 4; \\ 0 & \text{if } k = 2, \end{cases}$$

for $1 < j < r$,

$$g_j(k) = \begin{cases} g_{j-1}(k-2) + 2g_j(k-2) + g_{j+1}(k-2) & \text{if } k \geq 4; \\ 0 & \text{if } k = 2, \end{cases}$$

and

$$g_r(k) = \begin{cases} g_{r-1}(k-2) + 3g_r(k-2) & \text{if } k \geq 4; \\ q & \text{if } k = 2. \end{cases}$$

If all the $g_1(k), \ldots, g_r(k)$ are divided by m, we only obtain a trivial upper bound 1 of $U_q^k(e_m^a)$. Hence we have to show that there is a $j \in [r]$ such that $g_j(k)$ is not divided by m. Once the assumption can be proven, we achieve our goal, as stated in the following lemma.

Lemma 3.4. *Let $q \geq 3$ be a prime, m be an integer coprime to q, $r = (q-1)/2$, and $g_1(k), \ldots, g_r(k)$ be sequences defined above. If there is a $j \in [r]$ such that $g_j(k)$ is not divided by m for any even $k \geq 2$,*

$$U_q^k(e_m^a) \leq 1 - \alpha \left(\frac{2}{q}\right)^k,$$

where $\alpha > 0$ is a constant that depends on m only.

Now we have to show the assumption that for every even k some $g_j(k)$ is not divided by m. These sequences look simple but it is not trivial to obtain the closed forms. Instead of directly calculating closed forms of $g_1(k), \ldots, g_r(k)$, we estimate the greatest common divisor (GCD for short) of $g_1(k), \ldots, g_r(k)$. We can show the GCD of $g_1(k), \ldots, g_r(k)$ is a power of q if $q \geq 3$ is a prime. More precisely, the following lemma holds:

Lemma 3.5. *Let $q \geq 3$ be a prime and $g_1(k), g_2(k) \ldots, g_r(k)$ be sequences defined above. Then, for any even $k \geq 2$,*

$$\gcd(g_1(k), g_2(k), \ldots, g_r(k)) = q^{\lfloor (k-2)/(q-1) \rfloor + 1}.$$

Since m is coprime to q, if the GCD has only a power of q as its factors, for every even k, there is a j such that $g_j(k)$ is not divided by m.

Now, we show how to estimate the GCD stated in the above lemma. For proving the relations, we show that $\gcd(g_1(k), \ldots, g_r(k))$ is multiplied by q for every increase of $q-1$ in k, namely

$$\gcd(g_1(k), \ldots, g_r(k)) = \begin{cases} q \cdot \gcd(g_1(k-(q-1)), \ldots, g_r(k-(q-1))) & \text{if } k \geq q+1; \\ q & \text{if } 2 \leq k \leq q. \end{cases} \tag{1}$$

It is easy to show the relation in the case where $2 \leq k \leq q$. To show the relation in the case where $k \geq q+1$, we take the following two steps.

Step 1: $\gcd(g_1(k), \ldots, g_r(k))$ is multiplied by *at least* a multiple of q every increase of $q-1$ in k. That is,

$$\gcd(g_1(k), \ldots, g_r(k)) = C \gcd(g_1(k-(q-1)), \ldots, g_r(k-(q-1))),$$

where C is a multiple of q.

Step 2: $\gcd(g_1(k), \ldots, g_r(k))$ is multiplied by *only* q every increase of $q-1$ in k. That is,

$$\gcd(g_1(k)/q, \ldots, g_r(k)/q) = \gcd(g_1(k-(q-1)), \ldots, g_r(k-(q-1))).$$

Now we introduce an $r \times r$ matrix A_r for analyzing the GCD of these sequences. The matrix A_r is defined as

$$\begin{bmatrix} g_1(k) \\ g_2(k) \\ \vdots \\ g_r(k) \end{bmatrix} = A_r \begin{bmatrix} g_1(k-2) \\ g_2(k-2) \\ \vdots \\ g_r(k-2) \end{bmatrix}.$$

Thus, we have

$$A_r = \begin{bmatrix} 2 & 1 & & & & 0 \\ 1 & 2 & 1 & & & \\ & \ddots & \ddots & \ddots & & \\ & & \ddots & \ddots & \ddots & \\ & & & 1 & 2 & 1 \\ 0 & & & & 1 & 3 \end{bmatrix}$$

by the definition of the sequences. By powering the matrix, we obtain

$$\begin{bmatrix} g_1(k) \\ g_2(k) \\ \vdots \\ g_r(k) \end{bmatrix} = (A_r)^{(q-1)/2} \begin{bmatrix} g_1(k-(q-1)) \\ g_2(k-(q-1)) \\ \vdots \\ g_r(k-(q-1)) \end{bmatrix}$$

and $(q-1)/2 = r$. In fact, we can obtain Equation (1) by transforming $(A_r)^r$ using basic row operations corresponding to the operations for the GCD. In the specific case of small q like $q = 5$, this transformation can be done by an adhoc manner. However, such a manner does not work for general q and thus we require a systematic manner to obtain Equation (1), which is the above mentioned two step analysis.

Now let us see the analysis of each step. Step 1 is proven by the following lemma.

Lemma 3.6. *If q is a prime, for any $k \geq q+1$*

$$\gcd(g_1(k), \ldots, g_r(k)) = C \gcd(g_1(k-(q-1)), \ldots, g_r(k-(q-1))),$$

where C is a multiple of q and $r = (q-1)/2$.

This lemma can be proven by calculating an explicit form of each entry of $(A_r)^r$ and showing that it is a multiple of $2r+1 = q$. Precisely, we show

$$(A_r)^r(i,j) = \begin{cases} \binom{2r}{r-(i-j)} - \binom{2r}{r-(i+j)} & \text{if } i+j \leq r, \\ \binom{2r}{r-(i-j)} + \binom{2r}{i+j-(r+1)} & \text{if } i+j \geq r+1, \end{cases}$$

and any $(A_r)^r(i,j)$ is a multiple of $2r+1$.

Step 2 is more involved. It is proven by the following two lemmas.

Lemma 3.7. *If $q(A_r)^{-r}$ is an integer matrix, for any $k \geq q+1$*

$$\gcd\left(\frac{g_1(k)}{q}, \frac{g_2(k)}{q}, \ldots, \frac{g_r(k)}{q}\right) = \gcd(g_1(k-(q-1)), g_2(k-(q-1)), \ldots, g_r(k-(q-1))).$$

Lemma 3.8. *If $q \geq 3$ is a prime, each entry of $q(A_r)^{-r}$ is an integer.*

Lemma 3.8 is technically hardest in our whole argument, and we will explain our approach for proving it later. Here we first explain why we consider the inverse matrix $q(A_r)^{-r}$ for our analysis.

To demonstrate the idea, we discuss one concrete example where $q = 5$ (and then $r = 2$). For a while let $q = 5$ and fixed. By the definition,

$$(A_2)^2 = \begin{bmatrix} 5 & 5 \\ 5 & 10 \end{bmatrix}.$$

This means

$$\begin{bmatrix} g_1(k) \\ g_2(k) \end{bmatrix} = 5 \begin{bmatrix} 1 & 1 \\ 1 & 2 \end{bmatrix} \begin{bmatrix} g_1(k-4) \\ g_2(k-4) \end{bmatrix}. \tag{2}$$

Hence, the GCD of $g_1(k)$ and $g_2(k)$ is the GCD of $g_1(k-4)$ and $g_2(k-4)$ times *at least* a multiple of 5. This is the analysis of Step 1, and this is indeed an example that Lemma 3.6 holds.

We next consider the analysis of Step 2. Here we want to prove the relation that $\gcd(g_1(k)/5, g_2(k)/5) = \gcd(g_1(k-4), g_2(k-4))$. First from (2), we have

$$\begin{bmatrix} g_1(k)/5 \\ g_2(k)/5 \end{bmatrix} = \begin{bmatrix} 1 & 1 \\ 1 & 2 \end{bmatrix} \begin{bmatrix} g_1(k-4) \\ g_2(k-4) \end{bmatrix} = \begin{bmatrix} g_1(k-4) + g_2(k-4) \\ g_1(k-4) + 2g_2(k-4) \end{bmatrix}.$$

Hence, we have

$$\gcd(g_1(k)/5, g_2(k)/5) = \gcd(g_1(k-4) + g_2(k-4), g_1(k-4) + 2g_2(k-4)). \tag{3}$$

For our goal, it suffices to show that the righthand side of this equation is equal to $\gcd(g_1(k-4), g_2(k-4))$. For computing the righthand side, we make use of the following basic properties of GCD. For any integers a, b, m, the following equations hold:

$$\gcd(a, b) = \gcd(a, b, ma) \qquad \text{and} \qquad \gcd(a, b) = \gcd(a, b + ma). \tag{4}$$

Intuitively, what we need is to express $g_1(k-4)$ and $g_2(k-4)$ by using $g_1(k-4) + g_2(k-4)$ and $g_1(k-4) + 2g_2(k-4)$. To derive this transformation, we consider the inverse of the matrix $\begin{bmatrix} 1 & 1 \\ 1 & 2 \end{bmatrix}$ in (2), that is, $\left(\frac{1}{5}(A_2)^2\right)^{-1}$ $(= 5(A_2)^{-2})$. Let a_{ij} be the (i, j)-entry of $\left(\frac{1}{5}(A_2)^2\right)^{-1}$. Then by the definition we have

$$\begin{bmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{bmatrix} \begin{bmatrix} 1 & 1 \\ 1 & 2 \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}.$$

Hence, we have

$$\begin{aligned} g_1(k-4) &= a_{11}(g_1(k-4) + g_2(k-4)) + a_{12}(g_1(k-4) + 2g_2(k-4)), \\ g_2(k-4) &= a_{21}(g_1(k-4) + g_2(k-4)) + a_{22}(g_1(k-4) + 2g_2(k-4)). \end{aligned}$$

Hence, if all entries of $\left(\frac{1}{5}(A_2)^2\right)^{-1}$ are integers, then by Equation (4), we have

$$\begin{aligned} &\gcd(g_1(k-4) + g_2(k-4),\ g_1(k-4) + 2g_2(k-4)) \\ &\quad = \gcd(g_1(k-4) + g_2(k-4),\ g_1(k-4) + 2g_2(k-4), \\ &\qquad\qquad a_{11}(g_1(k-4) + g_2(k-4)) + a_{12}(g_1(k-4) + 2g_2(k-4))) \\ &\quad = \gcd(g_1(k-4) + g_2(k-4),\ g_1(k-4) + 2g_2(k-4),\ g_1(k-4)) \\ &\quad = \gcd(g_1(k-4) + g_2(k-4),\ g_1(k-4) + 2g_2(k-4),\ g_1(k-4), \\ &\qquad\qquad a_{21}(g_1(k-4) + g_2(k-4)) + a_{22}(g_1(k-4) + 2g_2(k-4))) \\ &\quad = \gcd(g_1(k-4) + g_2(k-4),\ g_1(k-4) + 2g_2(k-4),\ g_1(k-4),\ g_2(k-4)) \\ &\quad = \gcd(g_1(k-4),\ g_2(k-4)). \end{aligned}$$

This is the motivation of introducing the inverse matrix. Coming back to the general case, as Lemma 3.7 states, if all entries of $q(A_r)^{-r}$ $(= (q^{-1}(A_r)^r)^{-1})$ are integers, then we can show the goal of Step 2 analysis.

Now the rest is to show all entries of $q(A_r)^{-r}$ are indeed integers, that is, Lemma 3.8. This is the technically hardest part in our argument. Instead of directly proving that $q(A_r)^{-r}$ is an integer matrix, we prove that each entry of $(q(A_r)^{-1})^r$ is a multiple of q^{r-1}. Note that if each entry of $(q(A_r)^{-1})^r$ is a multiple of q^{r-1} then $q(A_r)^{-r}$ is an integer matrix.

Note first that

$$(q(A_r)^{-1})(i,j) = \begin{cases} (-1)^{i+j+1}\,(2ij - qi) & \text{if } i < j, \\ (-1)^{i+j}\,(qj - 2ij) & \text{if } i \geq j. \end{cases}$$

Let $a_{ij} = q(A_r)^{-1}(i,j)$. Then,

$$(q(A_r)^{-1})^r(i,j) = \sum_{t_{r-1}=1}^{r} \sum_{t_{r-2}=1}^{r} \cdots \sum_{t_1=1}^{r} a_{it_1} a_{t_1 t_2} \dots a_{t_{r-2} t_{r-1}} a_{t_{r-1} j},$$

where

$$a_{uv} = \begin{cases} (-1)^{u+v+1}(2uv - qu) & \text{if } u < v, \\ (-1)^{u+v}(qv - 2uv) & \text{if } u \geq v. \end{cases}$$

Let

$$\xi_{uv} := (-1)^{u+v+1} 2uv, \quad \eta_{uv} := \begin{cases} (-1)^{u+v} qu & \text{if } u < v \\ (-1)^{u+v} qv & \text{if } u \geq v. \end{cases}$$

Expanding $a_{it_1} \dots a_{t_{r-1}j}$, we obtain a sum of products of ξ_{uv} and η_{uv}.

For example, if $r = 2$, the (i,j)-entry is written as

$$\begin{aligned} \sum_{t_1=1}^{2} a_{it_1} a_{t_1 j} &= a_{i1} a_{1j} + a_{i2} a_{2j} \\ &= (\xi_{i1} + \eta_{i1})(\xi_{1j} + \eta_{1j}) + (\xi_{i2} + \eta_{i2})(\xi_{2j} + \eta_{2j}) \\ &= \xi_{i1}\xi_{1_j} + \xi_{i1}\eta_{1j} + \cdots + \eta_{i2}\eta_{2j}. \end{aligned}$$

Let $b_{uv} \in \{q \min(u,v), 2uv\}$. The product $b_{it_1} \cdots b_{t_{r-1}j}$ then represents an absolute value of the term that consists of ξ_{uv} and η_{uv} obtained by expanding $a_{it_1} \dots a_{t_{r-1}j}$. In the above example, $b_{i1}b_{1j}$ corresponds to one of $|\xi_{i1}\xi_{1j}|, |\xi_{i1}\eta_{1j}|, |\eta_{i1}\xi_{1j}|, |\eta_{i1}\eta_{1j}|$.

Therefore, $(q(A_r)^{-1})(i,j)$ can be written as a linear combination of

$$\gamma := \sum_{t_{r-1}=1}^{r} \cdots \sum_{t_1=1}^{r} b_{it_1} \dots b_{t_{r-1}j}.$$

Now we show that the above summation is a multiple of q^{r-1}. If the number of $b_{uv} = q\min(u,v)$ in $\{b_{it_1}, \dots, b_{t_{r-1}j}\}$ is at least $r-1$, the degree on q of $b_{it_1} \dots b_{t_{r-1}j}$ is at least $r-1$. In this case, γ is a multiple of q^{r-1}. Hence we have to show that γ is a multiple of q^{r-1} in the case where the number of $b_{uv} = q\min(u,v)$ in $\{b_{it_1}, \dots, b_{t_{r-1}j}\}$ is at most $r-2$. Then let k be the number of $b_{uv} = 2uv$. Note that $k \geq 2$ and the number of $b_{uv} = q\min(u,v)$ is $r-k$.

Now we use properties of a power sum stated in the following claim.

Claim 3.9. *If k is an even such that $k < 2r$ and $2r+1$ is a prime, $\sum_{t=1}^{r} t^k$ is a multiple of $2r+1$.*

$\sum_{t_w=1}^{r} t_w^{2l}$ is a multiple of $2r+1 = q$ from Claim 3.9, where $l < r$. If γ is a multiple of $\sum_{t_w=1}^{r} t_w^{2l}$, where $w \in [r-1]$ and $l < r$, the degree on q of γ is at least the degree on q of $b_{it_1} \dots b_{t_{r-1}j}$ plus 1.

Actually, we can show that γ is a multiple of

$$\sum_{t_{w_1}=1}^{r} t_{w_1}^{2l_1} \sum_{t_{w_2}=1}^{r} t_{w_2}^{2l_2} \cdots \sum_{t_{w_{k-1}}=1}^{r} t_{w_{k-1}}^{2l_{k-1}}, \tag{5}$$

where $\{t_{w_1}, t_{w_2}, \dots, t_{w_{k-1}}\}$ is a subset of $\{t_1, \dots, t_{r-1}\}$ and $l_1, \dots, l_{k-1} < r$. From Claim 3.9, Term (5) is a multiple of q^{k-1}. Now the degree on q of $b_{it_1} \dots b_{t_{r-1}j}$ is $r-k$. Hence the degree on q of γ is at least $k-1+r-k = r-1$. Therefore, γ is a multiple of q^{r-1}, which concludes Lemma 3.8.

By Lemmas 3.6, 3.7 and 3.8, we can prove our main technical lemma, Lemma 3.5. The details of the estimation are exhibited in Section 4.

4 Estimation of Gowers Uniformity

Let $e_m^a(x)$ be a function on the m-th root of unity, that is $e_m^a(x) = \exp(2\pi iax/m)$. We estimate the degree-k Gowers uniformity over $\mathbb{Z}_q$ of e_m^a, where $q \geq 3$ is a prime and m is coprime to q. We have shown the overview of the estimation in Section 3. In this section, we estimate the Gowers uniformity $U_q^d(e_m^a)$ in detail.

The following is our main lemma.

Lemma 4.1. *Let $q \geq 3$ be a prime, m be coprime to q, and $a \in [m-1]$. Then for any even $k \geq 2$,*

$$U_q^k(e_m^a) \leq 1 - \alpha \cdot \left(\frac{2}{q}\right)^k,$$

where $\alpha > 0$ is a constant that depends on m only.

If Lemma 4.1 holds, the following theorem is derived from Lemma 3.2

Theorem 4.2. *For any prime $q \geq 3$, any integer m coprime to q,*

$$\mathrm{Corr}(\mathrm{MOD}_m, P_d^{(q)}) \leq \exp\left(-\alpha \cdot \frac{n}{q^d}\right),$$

where $\alpha > 0$ is a constant that depends on m only.

4.1 Sequences $g_j(k)$ and Their GCD

First, we introduce sequences $g_1(k), g_2(k), \dots, g_r(k)$. They play an important role for proving the main lemma. These recursive sequences are very simple. However it is not trivial how to obtain closed forms of $g_1(k), \dots, g_r(k)$.

Definition 4.3. For an integer $q \geq 3$, we define sequences $g_1(k), g_2(k), \ldots, g_r(k), g_{r+1}(k)$, where $k \geq 2$ and $r = \lfloor q/2 \rfloor$, as

$$g_1(k) = \begin{cases} g_1(k-1) + g_2(k-1) & \text{if } k \text{ is an even and } k \geq 4 \\ g_1(k-1) & \text{if } q \text{ is an odd, } k \text{ is an odd, and } k \geq 3 \\ 2g_1(k-1) & \text{if } q \text{ is an even, } k \text{ is an odd, and } k \geq 3 \\ 0 & \text{if } k = 2 \text{ and } q > 3 \\ q & \text{if } k = 2 \text{ and } q = 3, \end{cases}$$

for $1 < j < r$,

$$g_j(k) = \begin{cases} g_j(k-1) + g_{j+1}(k-1) & \text{if } k \text{ is an even and } k \geq 4 \\ g_{j-1}(k-1) + g_j(k-1) & \text{if } k \text{ is an odd and } k \geq 3 \\ 0 & \text{if } k = 2, \end{cases}$$

$$g_r(k) = \begin{cases} g_r(k-1) + g_{r+1}(k-1) & \text{if } k \text{ is an even and } k \geq 4 \\ g_{r-1}(k-1) + g_r(k-1) & \text{if } k \text{ is an odd and } k \geq 3 \\ q & \text{if } k = 2, \end{cases}$$

and

$$g_{r+1}(k) = \begin{cases} 0 & \text{if } k \text{ is an even} \\ 2g_r(k-1) & \text{if } k \text{ is an odd,} \end{cases}$$

where $g_0(k) = 0$ for any integer k in the case where $q = 3$, namely $r = \lfloor 3/2 \rfloor = 1$.

If we only consider the case where k is an even, we use the next definition, that is equivalent to Definition 4.3 if k is an even.

Definition 4.4. For an integer $q \geq 3$, we define sequences $g_1(k), g_2(k), \ldots, g_r(k)$, where $k \geq 2$ is an even and $r = \lfloor q/2 \rfloor$, such that if $q > 3$,

$$g_1(k) = \begin{cases} 2g_1(k-2) + g_2(k-2) & \text{if } k \geq 4 \text{ and } q \text{ is an odd} \\ 3g_1(k-2) + g_2(k-2) & \text{if } k \geq 4 \text{ and } q \text{ is an even} \\ 0 & \text{if } k = 2, \end{cases}$$

for $1 < j < r$,

$$g_j(k) = \begin{cases} g_{j-1}(k-2) + 2g_j(k-2) + g_{j+1}(k-2) & \text{if } k \geq 4 \\ 0 & \text{if } k = 2, \end{cases}$$

and

$$g_r(k) = \begin{cases} g_{r-1}(k-2) + 3g_r(k-2) & \text{if } k \geq 4 \\ q & \text{if } k = 2, \end{cases}$$

and if $q = 3$,

$$g_1(k) = \begin{cases} 3g_1(k-2) & \text{if } k \geq 4 \\ q(=3) & \text{if } k = 2. \end{cases}$$

We can show that $g_1(k), \ldots, g_r(k)$ appear in the estimation of $U_q^k(e_m^a)$. It is important to show divisibility of $g_1(k), \ldots, g_r(k)$ for the estimation of $U_q^k(e_m^a)$. More specifically, if some $g_j(k)$ is not divided by m, the estimation of $U_q^k(e_m^a)$ is finished, that is stated in the following lemma.

Lemma 4.5. *Let $m \geq 2$ be an integer, $q \geq 3$ be an odd, $g_1(k), \ldots, g_r(k)$ be the sequences defined in Definition 4.4 with q, and $r = (q-1)/2$. If there is a $j \in [r]$ such that $g_j(k)$ is not divided by m for any even $k \geq 2$,*

$$U_q^k(e_m^a) \leq 1 - \alpha \left(\frac{2}{q}\right)^k,$$

where $\alpha > 0$ is a constant that depends on m only.

Proof. From the definition,

$$U_q^k(e_m^a) = \frac{1}{q^{k+1}} \sum_{x, y_1, \ldots, y_k \in \mathbb{Z}_q} e_m \left(\sum_{S \subseteq [k]} (-1)^{|S|} a \left(x \oplus \bigoplus_{j \in S} y_j \right) \right).$$

Bounding $e_m(\cdot)$ by 1 on inputs $y_1, ..., y_k$ over $\mathbb{Z}_q^k \setminus \{1, q-1\}^k$, we then obtain the following inequality.

$$\begin{aligned}
&U_q^k(e_m^a) \\
&\leq \frac{1}{q^{k+1}} \left\{ \sum_{\substack{x \in \mathbb{Z}_q \\ y_1, \ldots, y_k \in \{1, q-1\}}} e_m \left(a \sum_{S \subseteq [k]} (-1)^{|S|} \left(x \oplus \bigoplus_{j \in S} y_j \right) \right) + (q^{k+1} - 2^k q) \right\} \\
&= 1 - \left(\frac{2}{q}\right)^k + \frac{1}{q^{k+1}} \left\{ \sum_{\substack{x \in \mathbb{Z}_q \\ y_1, \ldots, y_k \in \{1, q-1\}}} e_m \left(a \sum_{S \subseteq [k]} (-1)^{|S|} \left(x \oplus \bigoplus_{j \in S} y_j \right) \right) \right\} \\
&= 1 - \left(\frac{2}{q}\right)^k \left\{ 1 - \frac{1}{2^k q} \sum_{\substack{x \in \mathbb{Z}_q \\ y_1, \ldots, y_k \in \{1, q-1\}}} e_m \left(a \sum_{S \subseteq [k]} (-1)^{|S|} \left(x \oplus \bigoplus_{j \in S} y_j \right) \right) \right\}. \qquad (6)
\end{aligned}$$

In the case where $y_1, \ldots, y_k \in \{1, q-1\}$, $\sum_{S \subseteq [k]} (-1)^{|S|} \left(x \oplus \bigoplus_{j \in S} y_j \right)$ is equal to one of the sequences $g_1(k), \ldots, g_r(k)$ up to its sign. Specifically, the following claim holds.

Claim 4.6. *Let $q \geq 3$ be an integer, $k \geq 2$ be an even, and $y_1, \ldots, y_k \in \{1, q-1\}$. Now let x be a random variable uniformly chosen at random from $\mathbb{Z}_q$. Then*

$$\begin{aligned}
&\sum_{S \subseteq [k]} (-1)^{|S|} \left(x \oplus \bigoplus_{j \in S} y_j \right) \\
&= g_1(k),\ g_2(k),\ \ldots,\ g_r(k),\ -g_1(k),\ -g_2(k),\ \ldots,\ -g_r(k),\ \text{or } 0,
\end{aligned}$$

with each probability $1/q$.

Now we prove the lemma using this claim.

$$\begin{aligned}
&\sum_{x\in\mathbb{Z}_q} e_m\left(a\sum_{S\subseteq[k]}(-1)^{|S|}\left(x\oplus\bigoplus_{j\in S}y_j\right)\right)\\
&=1+\sum_{j=1}^{r}\exp\left(\frac{2\pi ia}{m}g_j(k)\right)+\sum_{j=1}^{r}\exp\left(-\frac{2\pi ia}{m}g_j(k)\right)\\
&=1+2\sum_{j=1}^{r}\cos\left(\frac{2\pi a}{m}g_j(k)\right).
\end{aligned}$$

Note that $e_m(0)=1$. Combining these equations and Inequality (6), we obtain

$$U_q^k(e_m^a)\le 1-\left(\frac{2}{q}\right)^k\left\{1-\frac{1+2\sum_{j=1}^{r}\cos\left(2\pi a g_j(k)/m\right)}{q}\right\}.$$

Note that the number of $y_1,\ldots,y_k\in\{1,q-1\}$ is 2^k. Now there is a $j_0\in[r]$ such that $g_{j_0}(k)$ is not divided by m. Then $\cos\left(2\pi a g_{j_0}(k)/m\right)<1$. Let $\delta:=\cos\left(2\pi a g_{j_0}(k)/m\right)$. We bound $\cos\left(2\pi a g_{j'}(k)/m\right)$ by 1 for all $j'\neq j_0$. Note that $2r+1=q$. Now,

$$\begin{aligned}
1-\frac{1+2\sum_{j=1}^{r}\cos(2\pi a g_{j_0}(k)/m)}{q}&\ge 1-\frac{1+2(r-1)+2\delta}{q}\\
&=1-\frac{q+2\delta-2}{q}\\
&=\frac{2-2\delta}{q}>0.
\end{aligned}$$

Hence the lemma follows. □

From now on, we give the proof of Claim 4.6. For proving Claim 4.6, we show the following claim.

Claim 4.7. *Let $k\ge 2$ be an integer, $q\ge 3$ be an odd, $r=(q-1)/2$, and $\mathbf{G}(k)$ and $\mathbf{G}^R(k)$ be ordered sequences*

$$\begin{aligned}
\mathbf{G}(k)&=-g_1(k),g_2(k),\ldots,(-1)^j g_j(k),\ldots,(-1)^r g_r(k),\\
\mathbf{G}^R(k)&=(-1)^r g_r(k),\ldots,(-1)^j g_j(k),\ldots,g_2(k),-g_1(k).
\end{aligned}$$

For any $y_1,\ldots,y_k\in\{1,q-1\}$, there are an integer $l=l(y_1,\ldots,y_k,q)$ and a permutation $\sigma=\sigma(y_1,\ldots,y_k,q)$ such that

$$\left(\sum_{S\subseteq[k]}(-1)^{|S|}\left(x\oplus\bigoplus_{j\in S}y_j\right)\right)_{x\in\mathbb{Z}_q}=\begin{cases}(-1)^l\sigma\left(-\mathbf{G}^R(k),g_{r+1}(k),\mathbf{G}(k)\right) & \text{if } k \text{ is an even}\\ (-1)^l\sigma\left(\mathbf{G}(k),(-1)^{r+1}g_{r+1}(k),\mathbf{G}^R(k)\right) & \text{if } k \text{ is an odd,}\end{cases}$$

where the lefthand side $\left(\sum_{S\subseteq[k]}(-1)^{|S|}\left(x\oplus\bigoplus_{j\in S}y_j\right)\right)_{x\in\mathbb{Z}_q}$ denotes a q-tuple

$$\left(\sum_{S\subseteq[k]}(-1)^{|S|}\left(0\oplus\bigoplus_{j\in S}y_j\right),\sum_{S\subseteq[k]}(-1)^{|S|}\left(1\oplus\bigoplus_{j\in S}y_j\right),\ldots,\sum_{S\subseteq[k]}(-1)^{|S|}\left((q-1)\oplus\bigoplus_{j\in S}y_j\right)\right),$$

and

$$\left(-\mathbf{G}^R(k), g_{r+1}(k), \mathbf{G}(k)\right) = \left((-1)^{r+1}g_r(k), \dots, g_1(k), g_{r+1}(k), -g_1(k), \dots, (-1)^r g_r(k)\right)$$
$$\left(\mathbf{G}(k), (-1)^{r+1}g_{r+1}(k), \mathbf{G}^R(k)\right) = \left(-g_1(k), \dots, (-1)^r g_r(k), (-1)^{r+1}g_{r+1}(k), (-1)^r g_r(k), \dots, -g_1(k)\right).$$

If the above claim holds, Claim 4.6 follows, since there are an integer l and a permutation σ' such that

$$\left(\sum_{S\subseteq[k]} (-1)^{|S|}\left(x \oplus \bigoplus_{j\in S} y_j\right)\right)_{x\in\mathbb{Z}_q}$$
$$= (-1)^l \sigma'\left(g_1(k), \dots, g_j(k), \dots, g_r(k), -g_1(k), \dots, -g_j(k), \dots, -g_r(k), 0\right),$$

if k is an even and $y_1, \dots, y_k \in \{1, q-1\}$. Hence it suffices to prove the claim.

Proof of Claim 4.7. Let

$$\mathcal{S}_{y_1,y_2,\dots,y_k}(x) := \sum_{S\subseteq[k]} (-1)^{|S|}\left(x \oplus \bigoplus_{j\in S} y_j\right).$$

We prove this claim by the induction on k. In the base case where $k = 2$,

$$\left(\mathcal{S}_{y_1,y_2}(x)\right)_{x\in\mathbb{Z}_q} = \left(x - (x\oplus y_1) - (x\oplus y_2) + (x\oplus y_1\oplus y_2)\right)_{x\in\mathbb{Z}_q}.$$

If $(y_1, y_2) = (1, 1)$

$$\left(\mathcal{S}_{1,1}(x)\right)_{x\in\mathbb{Z}_q} = \left(x - 2(x\oplus 1) + (x\oplus 2)\right)_{x\in\mathbb{Z}_q} = (0, \dots, 0, -q, q),$$

if $(y_1, y_2) = (q-1, q-1)$

$$\left(\mathcal{S}_{q-1,q-1}(x)\right)_{x\in\mathbb{Z}_q} = \left(x - 2\{x\oplus(q-1)\} + \{x\oplus(q-2)\}\right)_{x\in\mathbb{Z}_q} = (-q, q, 0, \dots, 0),$$

and if $(y_1, y_2) = (1, q-1)$ or $(q-1, 1)$

$$\left(\mathcal{S}_{1,q-1}(x)\right)_{x\in\mathbb{Z}_q} = \left(\mathcal{S}_{q-1,1}(x)\right)_{x\in\mathbb{Z}_q} = \left(2x - (x\oplus 1) - \{x\oplus(q-1)\}\right)_{x\in\mathbb{Z}_q} = (-q, 0, \dots, 0, q).$$

Hence there are an integer l and a permutation σ such that

$$\begin{aligned}\left(\mathcal{S}_{y_1,y_2}(x)\right)_{x\in\mathbb{Z}_q} &= \left(x - (x\oplus y_1) - (x\oplus y_2) + (x\oplus y_1\oplus y)\right)_{x\in\mathbb{Z}_q}\\ &= (-1)^l\sigma\left((-1)^{r-1}q, 0, \dots, 0, (-1)^r q\right).\end{aligned}$$

That is

$$(-1)^l\sigma\left(-\mathbf{G}^R(2), g_{r+1}(2), \mathbf{G}(2)\right).$$

The statement is true in the base case.

Next, we assume that the statement holds in the case of $k-1$ and prove that it holds in the case of k. Note that

$$\begin{aligned}\mathcal{S}_{y_1,\dots,y_k}(x) &= \sum_{S\subseteq[k]} (-1)^{|S|}\left(x \oplus \bigoplus_{j\in S} y_j\right)\\ &= \sum_{S\subseteq[k-1]} (-1)^{|S|}\left(x \oplus \bigoplus_{j\in S} y_j\right) - \sum_{S\subseteq[k-1]} (-1)^{|S|}\left(x \oplus y_k \oplus \bigoplus_{j\in S} y_j\right)\\ &= \mathcal{S}_{y_1,\dots,y_{k-1}}(x) - \mathcal{S}_{y_1,\dots,y_{k-1}}(x\oplus y_k). \qquad (7)\end{aligned}$$

Table 1: $\mathcal{S}_{y_1,\ldots,y_k}(x)$ in the case where $y_k = 1$ and k is an odd

x	$\mathcal{S}_{y_1,\ldots,y_{k-1}}(x)$	$-\mathcal{S}_{y_1,\ldots,y_{k-1}}(x \oplus y_k)$	$\mathcal{S}_{y_1,\ldots,y_k}(x)$
0	$(-1)^{r+1}g_r(k-1)$	$(-1)^{r+1}g_{r-1}(k-1)$	$(-1)^{r+1}g_r(k)$
$\vdots$	$\vdots$	$\vdots$	$\vdots$
$r-j$	$(-1)^{j+1}g_j(k-1)$	$(-1)^{j+1}g_{j-1}(k-1)$	$(-1)^{j+1}g_j(k)$
$\vdots$	$\vdots$	$\vdots$	$\vdots$
$r-1$	$g_1(k-1)$	$-g_{r+1}(k-1) = 0$	$g_1(k)$
r	$g_{r+1}(k-1) = 0$	$g_1(k-1)$	$g_1(k)$
$\vdots$	$\vdots$	$\vdots$	$\vdots$
$r+j-1$	$(-1)^{j-1}g_{j-1}(k-1)$	$(-1)^{j+1}g_j(k-1)$	$(-1)^{j+1}g_j(k)$
$\vdots$	$\vdots$	$\vdots$	$\vdots$
$2r-1$	$(-1)^{r-1}g_{r-1}(k-1)$	$(-1)^{r+1}g_r(k-1)$	$(-1)^{r+1}g_r(k)$
$2r$	$(-1)^{r}g_r(k-1)$	$(-1)^{r+2}g_r(k-1)$	$(-1)^{r+2}g_{r+1}(k)$

Table 2: $\mathcal{S}_{y_1,\ldots,y_k}(x)$ in the case where $y_k = q-1$ and k is an odd

x	$\mathcal{S}_{y_1,\ldots,y_{k-1}}(x)$	$-\mathcal{S}_{y_1,\ldots,y_{k-1}}(x \oplus y_k)$	$\mathcal{S}_{y_1,\ldots,y_k}(x)$
0	$(-1)^{r+1}g_r(k-1)$	$(-1)^{r+1}g_r(k-1)$	$(-1)^{r+1}g_{r+1}(k)$
1	$(-1)^{r}g_{r-1}(k-1)$	$(-1)^{r+2}g_r(k-1)$	$(-1)^{r}g_r(k)$
$\vdots$	$\vdots$	$\vdots$	$\vdots$
$r-j+1$	$(-1)^{j}g_{j-1}(k-1)$	$(-1)^{j+2}g_j(k-1)$	$(-1)^{j}g_j(k)$
$\vdots$	$\vdots$	$\vdots$	$\vdots$
$r-1$	$g_1(k-1)$	$g_2(k-1)$	$g_2(k)$
r	$g_{r+1}(k-1) = 0$	$-g_1(k-1)$	$-g_1(k)$
$r+1$	$-g_1(k-1)$	$-g_{r+1}(k-1) = 0$	$-g_1(k)$
$\vdots$	$\vdots$	$\vdots$	$\vdots$
$r+j$	$(-1)^{j}g_j(k-1)$	$(-1)^{j}g_{j-1}(k-1)$	$(-1)^{j}g_j(k)$
$\vdots$	$\vdots$	$\vdots$	$\vdots$
$2r$	$(-1)^{r}g_r(k-1)$	$(-1)^{r}g_{r-1}(k-1)$	$(-1)^{r}g_r(k)$

First, we consider the case where k is an odd. Since $k-1$ is an even, by the induction hypothesis, there are an integer l' and a permutation σ' such that

$$\left(\mathcal{S}_{y_1,\ldots,y_{k-1}}(x)\right)_{x\in\mathbb{Z}_q} = (-1)^{l'}\sigma'\left(-\mathbf{G}^R(k-1), g_{r+1}(k-1), \mathbf{G}(k-1)\right).$$

Now we omit $(-1)^{l'}$ and σ'. From the induction hypothesis, we can build Tables 1 and 2. Table 1 is for the case where $y_k = 1$, and Table 2 is for the case where $y_k = q-1$. The first columns of these tables show the q-tuple $\left(\mathcal{S}_{y_1,\ldots,y_{k-1}}(x)\right)_{x\in\mathbb{Z}_q}$, and the second columns of these tables show the q-tuple $\left(-\mathcal{S}_{y_1,\ldots,y_{k-1}}(x\oplus y_k)\right)_{x\in\mathbb{Z}_q}$. By using Equation (7), we can calculate $\left(\mathcal{S}_{y_1,\ldots,y_k}(x)\right)_{x\in\mathbb{Z}_q}$ from $\left(\mathcal{S}_{y_1,\ldots,y_{k-1}}(x)\right)_{x\in\mathbb{Z}_q}$ and $\left(-\mathcal{S}_{y_1,\ldots,y_{k-1}}(x\oplus y_k)\right)_{x\in\mathbb{Z}_q}$, that is the third columns of these tables. Multiplying $(-1)^{l''}$ for some l'' to $\mathcal{S}_{y_1,\ldots,y_k}(x)$'s column and shift it in these tables, we obtain $(\mathbf{G}(k), (-1)^{r+1}g_{r+1}(k), \mathbf{G}^R(k))$. Therefore the statement follows in the case where k is an odd.

Table 3: $\mathcal{S}_{y_1,\ldots,y_k}(x)$ in the case where $y_k = 1$ and k is an even

x	$\mathcal{S}_{y_1,\ldots,y_{k-1}}(x)$	$-\mathcal{S}_{y_1,\ldots,y_{k-1}}(x \oplus y_k)$	$\mathcal{S}_{y_1,\ldots,y_k}(x)$
0	$-g_1(k-1)$	$-g_2(k-1)$	$-g_1(k)$
$\vdots$	$\vdots$	$\vdots$	$\vdots$
$j-1$	$(-1)^j g_j(k-1)$	$(-1)^{j+2} g_{j+1}(k-1)$	$(-1)^j g_j(k)$
$\vdots$	$\vdots$	$\vdots$	$\vdots$
$r-1$	$(-1)^r g_r(k-1)$	$(-1)^{r+2} g_{r+1}(k-1)$	$(-1)^r g_r(k)$
r	$(-1)^{r+1} g_{r+1}(k-1)$	$(-1)^{r+1} g_r(k)$	$(-1)^{r+1} g_r(k)$
$\vdots$	$\vdots$	$\vdots$	$\vdots$
$2r-j$	$(-1)^{j+1} g_{j+1}(k-1)$	$(-1)^{j+1} g_j(k-1)$	$(-1)^{j+1} g_j(k)$
$\vdots$	$\vdots$	$\vdots$	$\vdots$
$2r-1$	$g_2(k-1)$	$g_1(k-1)$	$g_1(k)$
$2r$	$-g_1(k-1)$	$g_1(k-1)$	$0 = g_{r+1}(k)$

Table 4: $\mathcal{S}_{y_1,\ldots,y_k}(x)$ in the case where $y_k = q-1$ and k is an even

x	$\mathcal{S}_{y_1,\ldots,y_{k-1}}(x)$	$-\mathcal{S}_{y_1,\ldots,y_{k-1}}(x \oplus y_k)$	$\mathcal{S}_{y_1,\ldots,y_k}(x)$
0	$-g_1(k-1)$	$g_1(k-1)$	$0 = g_{r+1}(k)$
1	$g_2(k-1)$	$g_1(k-1)$	$g_1(k)$
$\vdots$	$\vdots$	$\vdots$	$\vdots$
j	$(-1)^{j+1} g_{j+1}(k-1)$	$(-1)^{j+1} g_j(k-1)$	$(-1)^{j+1} g_j(k)$
$\vdots$	$\vdots$	$\vdots$	$\vdots$
r	$(-1)^{r+1} g_{r+1}(k-1)$	$(-1)^{r+1} g_r(k-1)$	$(-1)^{r+1} g_r(k)$
$r+1$	$(-1)^r g_r(k-1)$	$(-1)^{r+2} g_{r+1}(k-1)$	$(-1)^r g_r(k)$
$\vdots$	$\vdots$	$\vdots$	$\vdots$
$2r-j+1$	$(-1)^j g_j(k-1)$	$(-1)^{j+2} g_{j+1}(k-1)$	$(-1)^j g_j(k)$
$\vdots$	$\vdots$	$\vdots$	
$2r$	$-g_1(k-1)$	$-g_2(k-1)$	$-g_1(k)$

Next, we consider the case where k is an even. The argument for this even case is the same as for the odd case, except we use Tables 3 and 4 instead of Tables 1 and 2. Multiplying $(-1)^{l''}$ for some l'' to $\mathcal{S}_{y_1,\ldots,y_k}(x)$'s column and shift it in these tables, we obtain $(-\mathbf{G}^R(k), g_{r+1}(k), \mathbf{G}(k))$. Therefore the statement follows in the case where k is an even. □

The remaining task is to prove the assumption in Lemma 4.5, i.e., that some $g_j(k)$ is not divided by m for any even k. To show this, it is sufficient to prove the following lemma, which is a technical lemma on GCD of the sequences.

Lemma 4.8. *Let $q \geq 3$ be a prime and $g_1(k), g_2(k) \ldots, g_r(k)$ be sequences defined in Definition 4.4 with q, where $r = (q-1)/2$. Then, for any even $k \geq 2$,*

$$\gcd(g_1(k), g_2(k), \ldots, g_r(k)) = q^{\lfloor (k-2)/(q-1) \rfloor + 1}.$$

Proof. If we show

$$\gcd(g_1(k),\dots,g_r(k)) = \begin{cases} q\cdot\gcd(g_1(k-(q-1)),\dots,g_r(k-(q-1))) & \text{if } k\geq q+1 \\ q & \text{if } 2\leq k\leq q-1, \end{cases}$$

the lemma follows by the induction on k.

If $2\leq k\leq q-1$, we can prove that $g_1(k),\dots,g_{r-k/2}(k)$ are all 0, $g_{r-k/2+1}(k)=q$, and $g_{r-k/2+2}(k),\dots,g_r(k)$ are all multiples of q by the induction on k. Hence

$$\gcd(g_1(k),\dots,g_r(k)) = q,$$

for $2\leq k\leq q$.

In the case where $k\geq q+1$, we take the following two steps as stated in Section 3.

Step 1: $\gcd(g_1(k),\dots,g_r(k)) = C\cdot\gcd(g_1(k-(q-1)),\dots,g_r(k-(q-1)))$, where C is a multiple by q.

Step 2: $\gcd(g_1(k)/q,\dots,g_r(k)/q) = \gcd(g_1(k-(q-1)),\dots,g_r(k-(q-1)))$.

For proving these steps, we analyze the $r\times r$ matrix A_r introduced in Section 3. Recall that

$$\begin{bmatrix} g_1(k)\\ g_2(k)\\ \vdots\\ g_r(k)\end{bmatrix} = A_r \begin{bmatrix} g_1(k-2)\\ g_2(k-2)\\ \vdots\\ g_r(k-2)\end{bmatrix},$$

where

$$A_r = \begin{bmatrix} 2 & 1 & & & & & 0\\ 1 & 2 & 1 & & & & \\ & \ddots & \ddots & \ddots & & & \\ & & \ddots & \ddots & \ddots & & \\ & & & 1 & 2 & 1 & \\ 0 & & & & 1 & 3 & \end{bmatrix}.$$

Then,

$$\begin{bmatrix} g_1(k)\\ g_2(k)\\ \vdots\\ g_r(k)\end{bmatrix} = (A_r)^{(q-1)/2} \begin{bmatrix} g_1(k-(q-1))\\ g_2(k-(q-1))\\ \vdots\\ g_r(k-(q-1))\end{bmatrix}.$$

Now, $(A_r)^{(q-1)/2} = (A_r)^r$ since $r=(q-1)/2$.

We can achieve these two steps using $(A_r)^r$. Step 1 can be proven by the following lemma.

Lemma 4.9. *If q is a prime, for any $k\geq q+1$*

$$\gcd(g_1(k),\dots,g_r(k)) = C\cdot\gcd(g_1(k-(q-1)),\dots,g_r(k-(q-1))),$$

where C is a multiple of q and $r=(q-1)/2$.

Step 2 can be proven by the following two lemmas.

Lemma 4.10. *If $q(A_r)^{-r}$ is an integer matrix, for any $k \geq q+1$*

$$\gcd\left(\frac{g_1(k)}{q}, \frac{g_2(k)}{q}, \ldots, \frac{g_r(k)}{q}\right) = \gcd(g_1(k-(q-1)), g_2(k-(q-1)), \ldots, g_r(k-(q-1))).$$

Lemma 4.11. *If $q \geq 3$ is a prime, any entry of $q(A_r)^{-r}$ is an integer.*

By these lemmas, we can show

$$\gcd(g_1(k), \ldots, g_r(k)) = q \cdot \gcd(g_1(k-(q-1)), \ldots, g_r(k-(q-1)))$$

for any $k \geq q+1$. Therefore

$$\gcd(g_1(k), \ldots, g_r(k)) = q^{\lfloor (k-2)/(q-1) \rfloor + 1}.$$

□

The following corollary can be proven from Lemma 4.8.

Corollary 4.12. *Let q be a prime, m be coprime to q, $r = (q-1)/2$, and $g_1(k), \ldots, g_r(k)$ be sequences defined in Definition 4.4 with q. Then there is a $j \in [r]$ such that $g_j(k)$ is not divided by m for any even $k \geq 2$.*

Proof. We assume $m \mid g_j(k)$ for all $j \in [r]$. Then m is the common divisor of $g_1(k), \ldots, g_r(k)$. By Lemma 4.8, $q^{\lfloor (k-2)/(q-1) \rfloor + 1}$ is a multiple of m. However m is coprime to q. It is a contradiction. □

By Lemma 4.5 and Corollary 4.12, we obtain Lemma 4.1.

4.2 Step 1

First, we give an explicit formula of $(A_r)^r$. Since eigenvalues and eigenvectors of A_r are complicated, we predict an explicit formula of $(A_r)^r$ and then prove its correctness by the induction.

Lemma 4.13.

$$(A_r)^r(i,j) = \begin{cases} \binom{2r}{r-(i-j)} - \binom{2r}{r-(i+j)} & \text{if } i+j \leq r, \\ \binom{2r}{r-(i-j)} + \binom{2r}{i+j-(r+1)} & \text{if } i+j \geq r+1. \end{cases}$$

Proof Sketch. We can prove that

$$(A_r)^l(i,j) = \binom{2l}{l-(i-j)} - \binom{2l}{l-(i+j)} + \binom{2l}{2r+l+1-(i+j)}$$

for any integer $l \in [r]$ by the induction on l. Hence

$$(A_r)^r(i,j)\binom{2r}{r-(i-j)} - \binom{2r}{r-(i+j)} + \binom{2r}{3r+1-(i+j)}.$$

Note that $\binom{2r}{3r+1-(i+j)} = \binom{2r}{2r-\{3r+1-(i+j)\}} = \binom{2r}{i+j-(r+1)}$. If $i+j \leq r$, the third term becomes 0, since $i+j-(r+1) < 0$. If $i+j \geq r+1$, the second term becomes 0, since $r-(i+j) < 0$. Therefore the claim follows. □

Using the above claim, we achieve Step 1.

Lemma 4.14 (Restated Lemma 4.9)**.** *If q is a prime, for any $k \geq q+1$*

$$\gcd(g_1(k), \ldots, g_r(k)) = C \cdot \gcd(g_1(k-(q-1)), \ldots, g_r(k-(q-1))),$$

where C is a multiple of q and $r = (q-1)/2$.

Proof. Recall that

$$\begin{bmatrix} g_1(k) \\ \vdots \\ g_r(k) \end{bmatrix} = (A_r)^r \begin{bmatrix} g_1(k-(q-1)) \\ \vdots \\ g_r(k-(q-1)) \end{bmatrix}.$$

Hence it is sufficient to show $(2r+1) \mid (A_r)^r(i,j)$ for any $i, j \in [r]$.

In the case where $i + j \leq r$,

$$\begin{aligned}
(A_r)^r(i,j) &= \binom{2r}{r-(i-j)} - \binom{2r}{r-(i+j)} \\
&= \frac{2r(2r-1)\ldots(r+i+j+1)}{(r-i-j)!} \left\{ \frac{(r+i+j)\ldots(r+i-j+1)}{(r-i+j)\ldots(r-i-j+1)} - 1 \right\} \\
&= \frac{2r(2r-1)\ldots(r+i+j+1)}{(r-i+j)!} \\
&\quad \cdot \{(r+i+j)\ldots(r+i-j+1) - (r-i+j)\ldots(r-i-j+1)\}.
\end{aligned}$$

Let $s := r+i$ and $t := r-i$. Then,

$$\begin{aligned}
&(r+i+j)(r+i+j-1)\ldots(r+i-j+1) - (r-i+j)(r-i+j-1)\ldots(r-i-j+1) \\
&= (s+j)(s+j-1)\ldots(s-j+1) - (t+j)(t+j-1)\ldots(t-j+1).
\end{aligned}$$

By substituting s with $-t-1$, the first term becomes

$$\begin{aligned}
&\{(-t-1)+j\}\{(-t-1)+j-1\}\ldots\{(-t-1)-j+1\} \\
&= (t+1-j)(t+1-j+1)\ldots(t+1+j-1) \\
&= (t+j)\ldots(t-j+2)(t-j+1).
\end{aligned}$$

That means

$$\{(-t-1)+j\}\ldots\{(-t-1)-j+1\} - (t+j)\ldots(t-j+1) = 0.$$

By the factor theorem, $(s+j)\ldots(s-j+1) - (t+j)\ldots(t-j+1)$ is divided by $s-(-t-1) = 2r+1$. Hence, there is an integer M such that

$$\begin{aligned}
(A_r)^r(i,j) &= \frac{2r(2r-1)\ldots(r+i+j+1)}{(r-i+j)!}(2r+1)M \\
&= \binom{2r}{r-i-j} \frac{(2r+1)M}{(r-i+j)\ldots(r-i-j+1)}.
\end{aligned}$$

Since all the factors of the denominator in this formula is smaller than $2r+1$ and $2r+1$ is a prime, $2r+1$ remains as a factor in this formula. Therefore $(A_r)^r(i,j)$ is divided by $2r+1$ in this case.

In the case where $i+j \geq r+1$,

$$\begin{aligned}(A_r)^r(i,j) &= \binom{2r}{r-(i-j)} + \binom{2r}{i+j-(r+1)} \\ &= \frac{2r(2r-1)\dots(3r+2-i-j)}{(i+j-r-1)!}\left\{\frac{(3r+1-i-j)\dots(r+i-j+1)}{(r-i+j)\dots(i+j-r)}+1\right\} \\ &= \frac{2r(2r-1)\dots(r+i+j+1)}{(r-i+j)!} \\ &\qquad \cdot\{(3r+1-i-j)\dots(r+i-j+1)+(r-i+j)\dots(i+j-r)\}.\end{aligned}$$

Let $s := 2r-j+1$. Then,

$$\begin{aligned}&(3r+1-i-j)\dots(r+i+j+1)+(r-i+j)\dots(i+j-r) \\ &= \{2r-j+1+(r-i)\}\dots\{2r-j+1-(r-i)\}+\{j+(r-i)\}\dots\{j-(r-i)\} \\ &= \{s+(r-i)\}\dots\{s-(r-i)\}+\{j+(r-i)\}\dots\{j-(r-i)\}.\end{aligned}$$

By substituting s with $-j$, the first term becomes

$$\{-j+(r-i)\}\dots\{-j-(r-i)\} = -\{j-(r-i)\}\dots\{j+(r-i)\}.$$

That means

$$\{(-j)+(r-i)\}\dots\{(-j)-(r-i)\}+\{j+(r-i)\}\dots\{j-(r-i)\} = 0.$$

By the factor theorem, $\{s+(r-i)\}\dots\{s-(r-i)\}+\{j+(r-i)\}\dots\{j-(r-i)\}$ is divided by $s-(-j) = 2r+1$. Hence, there is an integer M such that

$$\begin{aligned}(A_r)^r(i,j) &= \frac{2r(2r-1)\dots(3r+2-i-j)}{(r-i+j)!}(2r+1)M \\ &= \binom{2r}{i+j-(r+1)}\frac{(2r+1)M}{(r-i+j)\dots(i+j-r)}.\end{aligned}$$

Since all the factors of the denominator in this formula is smaller than $2r+1$ and $2r+1$ is a prime, $2r+1$ remains as a factor in this formula. Therefore $(A_r)^r$ is also divided by $2r+1$ in this case. □

4.3 Step 2

Now we define the integral elementary row operation, that is restricted elementary row operations for computing the GCD.

Definition 4.15 (Integral Elementary Row Operations)**.** For a matrix A, these four operations are called the integral elementary row operations (IERO):

1. Row-swapping of the i-th row and the j-th row: swapping the i-th row and the j-th row.
2. Row-adding to the i-th row from the j-th row times m: adding the j-th row multiplied by a non-zero integer m to the i-th row.
3. Row-inserting from the i-th row times m: inserting a new row at bottom that is the i-th row multiplied by a non-zero integer m.

4. Row-deleting of the i-th row: deleting the i-th row which all entries are 0.

Observation 4.16. *Let $x_1, \ldots, x_n, y_1, \ldots, y_n$ be integers and A be an $n \times n$ matrix. we assume that*

$$\begin{bmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{bmatrix} = A \begin{bmatrix} y_1 \\ y_2 \\ \vdots \\ y_n \end{bmatrix}.$$

Then, the GCD of $x_1, x_2, \ldots,$ and x_n is equal to the GCD of $y_1, y_2, \ldots,$ and y_n if A is reduced to the $r \times r$ identity matrix I_r by the IERO.

We confirm the observation. Let $\mathbf{a}_1, \ldots, \mathbf{a}_n$ be row vectors of A and a_{ij} be the (i,j)-entry of A. The row-swapping of $\mathbf{a}_i$ and $\mathbf{a}_j$, that is

$$\begin{bmatrix} \vdots \\ \mathbf{a}_i \\ \vdots \\ \mathbf{a}_j \\ \vdots \end{bmatrix} \begin{bmatrix} \vdots \\ y_i \\ \vdots \\ y_j \\ \vdots \end{bmatrix} \longrightarrow \begin{bmatrix} \vdots \\ \mathbf{a}_j \\ \vdots \\ \mathbf{a}_i \\ \vdots \end{bmatrix} \begin{bmatrix} \vdots \\ y_j \\ \vdots \\ y_i \\ \vdots \end{bmatrix},$$

means

$$\gcd(x_1, \ldots, x_i, \ldots, x_j, \ldots, x_n) = \gcd(x_1, \ldots, x_j, \ldots, x_i, \ldots, x_n).$$

The row-adding to $\mathbf{a}_i$ from $\mathbf{a}_j$ times m, that is

$$\begin{bmatrix} \vdots \\ \sum_{t=1}^n a_{it} y_t \\ \vdots \\ \sum_{t=1}^n a_{jt} y_t \\ \vdots \end{bmatrix} = \begin{bmatrix} \vdots \\ \mathbf{a}_i \\ \vdots \\ \mathbf{a}_j \\ \vdots \end{bmatrix} \begin{bmatrix} \vdots \\ y_i \\ \vdots \\ y_j \\ \vdots \end{bmatrix} \longrightarrow \begin{bmatrix} \vdots \\ \mathbf{a}_i + m\mathbf{a}_j \\ \vdots \\ \mathbf{a}_j \\ \vdots \end{bmatrix} \begin{bmatrix} \vdots \\ y_i \\ \vdots \\ y_j \\ \vdots \end{bmatrix} = \begin{bmatrix} \vdots \\ \sum_{t=1}^n a_{it} y_t + m \sum_{t=1}^n a_{jt} y_t \\ \vdots \\ \sum_{t=1}^n a_{jt} y_t \\ \vdots \end{bmatrix},$$

means

$$\gcd(x_1, \ldots, x_i, \ldots, x_j, \ldots, x_n) = \gcd(x_1, \ldots, x_i + mx_j, \ldots, x_j, \ldots, x_n).$$

The row-inserting from $\mathbf{a}_i$ times m, that is

$$\begin{bmatrix} \vdots \\ \mathbf{a}_i \\ \vdots \end{bmatrix} \begin{bmatrix} \vdots \\ y_i \\ \vdots \end{bmatrix} \longrightarrow \begin{bmatrix} \vdots \\ \mathbf{a}_i \\ \vdots \\ m\mathbf{a}_i \end{bmatrix} \begin{bmatrix} \vdots \\ y_i \\ \vdots \\ y_i \end{bmatrix},$$

means

$$\gcd(x_1, \ldots, x_i, \ldots, x_n) = \gcd(x_1, \ldots, x_i, \ldots, x_n, mx_i).$$

The row-deleting of $\mathbf{a}_i = \mathbf{0}$, that is

$$\begin{bmatrix} \vdots \\ \mathbf{a}_{i-1} \\ \mathbf{0} \\ \mathbf{a}_{i+1} \\ \vdots \end{bmatrix} \begin{bmatrix} \vdots \\ y_{i-1} \\ y_i \\ y_{i+1} \\ \vdots \end{bmatrix} \longrightarrow \begin{bmatrix} \vdots \\ \mathbf{a}_{i-1} \\ \mathbf{a}_{i+1} \\ \vdots \end{bmatrix} \begin{bmatrix} \vdots \\ y_{i-1} \\ y_{i+1} \\ \vdots \end{bmatrix},$$

means

$$\gcd(x_1, \ldots, x_{i-1}, 0, x_{i+1}, \ldots, x_n) = \gcd(x_1, \ldots, x_{i-1}, x_{i+1}, \ldots, x_n).$$

Hence these operations correspond to operations of the GCD. If we can convert A to I_n, that is

$$\begin{bmatrix} \mathbf{a}_1 \\ \mathbf{a}_2 \\ \vdots \\ \mathbf{a}_n \end{bmatrix} \begin{bmatrix} y_1 \\ y_2 \\ \vdots \\ y_n \end{bmatrix} \to \cdots \to \begin{bmatrix} 1 & & & 0 \\ & 1 & & \\ & & \ddots & \\ 0 & & & 1 \end{bmatrix} \begin{bmatrix} y_1 \\ y_2 \\ \vdots \\ y_n \end{bmatrix},$$

$$\gcd(x_1, \ldots, x_n) = \gcd(y_1, \ldots, y_n).$$

Therefore we have to show that $\frac{1}{q}(A_r)^r$ can be converted to I_r by the IERO.

Using the IERO, we can achieve Step 2 if $q(A_r)^{-r}$ is an integer matrix.

Lemma 4.17 (Restated Lemma 4.10)**.** *If $q(A_r)^{-r}$ is an integer matrix, for any $k \geq q+1$*

$$\gcd\left(\frac{g_1(k)}{q}, \frac{g_2(k)}{q}, \ldots, \frac{g_r(k)}{q}\right) = \gcd(g_1(k-(q-1)), g_2(k-(q-1)), \ldots, g_r(k-(q-1))).$$

Proof. Recall that

$$\begin{bmatrix} \frac{g_1(k)}{q} \\ \vdots \\ \frac{g_r(k)}{q} \end{bmatrix} = \frac{1}{q}(A_r)^r \begin{bmatrix} g_1(k-(q-1)) \\ \vdots \\ g_r(k-(q-1)) \end{bmatrix}.$$

By Observation 4.16, if $\frac{1}{q}(A_r)^r$ is reduced to the $r \times r$ identity matrix I_r by the IERO, the lemma holds. Now we show the existence of the reduction.

Let a_{ij} be (i,j)-th entry of $q(A_r)^{-r}$ and α_{ij} be (i,j)-th entry of $\frac{1}{q}(A_r)^r$. Note that $(q(A_r)^{-r}) \cdot (\frac{1}{q}(A_r)^r) = I_r$. If the matrix including $(q(A_r)^{-r}) \cdot (\frac{1}{q}(A_r)^r)$ is created from $\frac{1}{q}(A_r)^r$ by the IERO, the lemma follows, because the matrix can be reduced by the IERO as follows:

$$\begin{bmatrix} & * & \\ & & \\ & & \\ (q(A_r)^{-r}) \cdot \left(\frac{1}{q}(A_r)^r\right) & & \end{bmatrix} = \begin{bmatrix} & * & \\ & & \\ 1 & & 0 \\ & \ddots & \\ 0 & & 1 \end{bmatrix} \to \cdots \to \begin{bmatrix} 1 & & 0 \\ & \ddots & \\ 0 & & 1 \end{bmatrix}.$$

Now we show how to create $(q(A_r)^{-r}) \cdot (\frac{1}{q}(A_r))$. The i-th row vector of the matrix is

$$\left(\sum_{t=1}^{r} a_{it}\alpha_{t1}, \sum_{t=1}^{r} a_{it}\alpha_{t2}, \ldots, \sum_{t=1}^{r} a_{it}\alpha_{tr} \right). \tag{8}$$

It can be created by the IERO. First, we create

$$(a_{i1}\alpha_{11}, a_{i1}\alpha_{12}, \ldots, a_{i1}\alpha_{1r})$$

by the row-inserting from the first row times a_{i1}. Then, we convert the row to

$$(a_{i1}\alpha_{11} + a_{i2}\alpha_{21}, a_{i1}\alpha_{12} + a_{i2}\alpha_{22}, \ldots, a_{i1}\alpha_{1r} + a_{i2}\alpha_{2r})$$

by the row-adding to the new row from the second row times a_{i2}. For each $t \in [r]$, repeating the row-adding to the new row from the t-th row times a_{it}, we can create the wanted the i-th row vector (8). By creating the i-th row for each $i \in [r]$, we can create the matrix. Therefore the lemma follows. □

Next, we show any entry of $q(A_r)^{-r}$ is an integer. Instead of showing that $q(A_r)^{-r}$ is an integer matrix directly, we prove that its r-th power $(q(A_r)^{-1})^r$ is a multiple of q^{r-1}. Note that $(q(A_r)^{-1})^r = q^{r-1} \cdot q(A_r)^{-r}$. For it, we show an explicit formula of $(A_r)^{-1}$ in the following lemma.

Lemma 4.18. *Let B be an $r \times r$ matrix defined as*

$$B(i,j) = \begin{cases} (-1)^{i+j+1}\dfrac{2ij - qi}{q} & \text{if } i < j, \\ (-1)^{i+j}\dfrac{qj - 2ij}{q} & \text{if } i \geq j. \end{cases}$$

Then $A_r \cdot B = I_r$, i.e., $B = (A_r)^{-1}$.

Proof Sketch. We just calculate $A_r \cdot B$. □

Now we prove that any entry of $q(A_r)^{-r}$ is an integer.

Lemma 4.19 (Restated Lemma 4.11)**.** *If $q \geq 3$ is a prime, any entry of $q(A_r)^{-r}$ is an integer.*

Proof. If $q = 3$, the lemma clearly follows, since $3(A_1)^{-1}(1,1) = 3 \cdot 1/3 = 1$. We only consider the case where $q \geq 5$. Since $(q(A_r)^{-1})^r = q^{r-1} \cdot q(A_r)^{-r}$, it is sufficient to show that every entry of $(q(A_r)^{-1})^r$ is a multiple of q^{r-1}. Then, the following claims hold.

Claim 4.20. *For any integers α and β such that $1 \leq \alpha \leq \beta \leq r-1$, if*

$$\sum_{t_\beta=1}^{r} \sum_{t_{\beta-1}=1}^{r} \cdots \sum_{t_\alpha=1}^{r} t_\beta \min(t_\beta, t_{\beta-1}) \min(t_{\beta-1}, t_{\beta-2}) \ldots \min(t_{\alpha+1}, t_\alpha) t_\alpha$$

is a multiple of $2r+1$, then any entry of $\left(q(A_r)^{-1}\right)^r$ is a multiple of q^{r-1}.

Claim 4.21. *For any integers α and $\beta \geq \alpha$, there are constants $\theta_2, \theta_4, \ldots, \theta_d$ such that*

$$\sum_{t_\beta=1}^{r} \sum_{t_{\beta-1}=1}^{r} \cdots \sum_{t_\alpha=1}^{r} t_\beta \min(t_\beta, t_{\beta-1}) \min(t_{\beta-1}, t_{\beta-2}) \ldots \min(t_{\alpha+1}, t_\alpha) t_\alpha = \sum_{t_\beta=1}^{r} \sum_{\substack{2 \leq i \leq d \\ i:\ even}} \theta_i t_\beta^i, \tag{9}$$

where $d \leq 2(\beta - \alpha + 1)$.

Claim 4.22. *Let $l < r$ be an integer. If $2r+1$ is a prime, $\sum_{t=1}^{r} t^{2l}$ is a multiple of $2r+1$.*

Now we use these claims for proving this lemma. Let α and β be integers such that $1 \le \alpha \le \beta \le r-1$. From Claim 4.21, Equation (9) holds with $d \le 2(\beta-\alpha+1) \le 2(r-1-1+1) < 2r$. The righthand side of (9) is

$$\sum_{\substack{2 \le i \le d \\ i:\ \text{even}}} \left(\theta_i \sum_{t_\beta=1}^{r} t_\beta^i \right).$$

Each term $\theta_i \sum_{t_\beta=1}^{r} t_\beta^i$ is a multiple of $2r+1$ from Claim 4.22, since each i is an even and $i \le d < 2r$. Hence (9) is also a multiple of $q = 2r+1$. Therefore any entry of $(q(A_r)^{-1})^r$ is a multiple of q^{r-1} from Claim 4.20. □

From now on, we prove Claims 4.20 and 4.21. Claim 4.22 is easily obtained from basic properties of a power sum (see e.g., [GKP89]).

Proof of Claim 4.20. Let $a_{ij} = q(A_r)^{-1}(i,j)$. Then,

$$(q(A_r)^{-1})^r(i,j) = \sum_{t_{r-1}=1}^{r} \sum_{t_{r-2}=1}^{r} \cdots \sum_{t_1=1}^{r} a_{it_1} a_{t_1t_2} \dots a_{t_{r-2}t_{r-1}} a_{t_{r-1}j}. \tag{10}$$

Note that each a_{uv} is $(-1)^{u+v+1}(2uv - qu)$ if $u < v$, and $(-1)^{u+v}(qv - 2uv)$ if $u \ge v$. Let $\xi_{uv} := (-1)^{u+v+1}2uv$, and let $\eta_{uv} := (-1)^{u+v}qu$ if $u < v$ and $\eta_{uv} := (-1)^{u+v}qv$ if $u \ge v$. Then the righthand side of (10) is

$$\begin{aligned}
&\sum_{t_{r-1}=1}^{r} \cdots \sum_{t_1=1}^{r} (\xi_{it_1} + \eta_{it_1})(\xi_{t_1t_2} + \eta_{t_1t_2}) \dots (\xi_{t_{r-2}t_{r-1}} + \eta_{t_{r-2}t_{r-1}})(\xi_{t_{r-1}j} + \eta_{t_{r-1}j}) \\
&= \sum_{t_{r-1}=1}^{r} \cdots \sum_{t_1=1}^{r} \xi_{it_1}\xi_{t_1t_2} \dots \xi_{t_{r-1}j} + \eta_{it_1}\xi_{t_1t_2} \dots \xi_{t_{r-1}j} + \cdots + \eta_{it_1}\eta_{t_1t_2} \dots \eta_{t_{r-1}j} \\
&= \sum_{t_{r-1}=1}^{r} \cdots \sum_{t_1=1}^{r} \tau_{it_1}^{(\phi_1)} \tau_{t_1t_2}^{(\phi_2)} \cdots \tau_{t_{r-2}t_{r-1}}^{(\phi_{r-1})} \tau_{t_{r-1}j}^{(\phi_r)},
\end{aligned}$$

where $\tau_{uv}^{(\phi)}$ be ξ_{uv} if $\phi = 0$ and η_{uv} if $\phi = 1$.

It is obvious that $(q(A_r)^{-1})^r(i,j)$ is a multiple of q^{r-1} if

$$\gamma^{(\phi_1,\dots,\phi_r)} := \sum_{t_{r-1}=1}^{r} \cdots \sum_{t_1=1}^{r} |\tau_{it_1}^{(\phi_1)}||\tau_{t_1t_2}^{(\phi_2)}| \cdots |\tau_{t_{r-2}t_{r-1}}^{(\phi_{r-1})}||\tau_{t_{r-1}j}^{(\phi_r)}|$$

is a multiple of q^{r-1}. Below, we show that so is $\gamma^{(\phi_1,\dots,\phi_r)}$ for every $\phi_1, \dots, \phi_r$.

If $|\{i : \phi_i = 1\}| \ge r-1$, that is, $\gamma^{(\phi_1,\dots,\phi_r)}$ contains at least $r-1$ terms of the form $|\eta_{u,v}| = q\min(u,v)$, then $\gamma^{(\phi_1,\dots,\phi_r)}$ is clearly a multiple of q^{r-1}. Therefore, we arbitrarily fix $\phi_1, \dots, \phi_r$ so that $\gamma^{(\phi_1,\dots,\phi_r)}$ only contains at most $r-2$ terms of the form $|\eta_{u,v}|$.

Let $k := |\{i : \phi_i = 0\}|$, that is, the number of $|\xi_{u,v}| = 2uv$ in $\gamma^{(\phi_1,\dots,\phi_r)}$. Note that $k \ge 2$. Then the term $\gamma^{(\phi_1,\dots,\phi_r)}$ with fixed $\phi_1, \dots, \phi_r$ is denoted by

$$\gamma := \sum_{t_{r-1}=1}^{r} \cdots \sum_{t_1=1}^{r} b_{it_1} \cdots b_{t_{r-1}j},$$

where $b_{uv} \in \{2uv, q\min(u,v)\}$.

For ease of notation, we denote i and j by t_0 and t_r. Suppose that $s_1, ..., s_k \in \{0, ..., r\}$ indicate the locations of the terms of the form $2uv$, i.e., $b_{t_{s_i}t_{s_i+1}} = 2t_{s_i}t_{s_i+1}$ for every i.

Then, we have

$$\gamma = \sum_{t_{r-1}=1}^{r} \cdots \sum_{t_1=1}^{r} \cdots 2t_{s_1}t_{s_1+1}\{q\min(t_{s_1+1}, t_{s_1+2}) \cdots q\min(t_{s_2-1}, t_{s_2})\}2t_{s_2}t_{s_2+1} \cdots$$
$$\cdots 2t_{s_{k-1}}t_{s_{k-1}+1}\{q\min(t_{s_{k-1}+1}, t_{s_{k-1}+2}) \cdots q\min(t_{s_k-1}, t_{s_k})\}2t_{s_k}t_{s_k+1} \cdots .$$

Recall that the number of the terms of the form $q\min(u,v)$ is $r-k$ in γ. Thus, moving all the factors q into head, we have

$$\gamma = q^{r-k} \sum_{t_{s_k+1}=1}^{r} \cdots \sum_{t_{s_1}=1}^{r} \cdots 2t_{s_1}t_{s_1+1}\{\min(t_{s_1+1}, t_{s_1+2}) \cdots \min(t_{s_2-1}, t_{s_2})\}2t_{s_2}t_{s_2+1} \cdots$$
$$\cdots 2t_{s_{k-1}}t_{s_{k-1}+1}\{\min(t_{s_{k-1}+1}, t_{s_{k-1}+2}) \cdots \min(t_{s_k-1}, t_{s_k})\}2t_{s_k}t_{s_k+1} \cdots .$$

To apply the assumption of the claim to γ, transforming the above expression to

$$\gamma = q^{r-k} \sum_{t_{r-1}=1}^{r} \cdots \sum_{t_1=1}^{r} \cdots 2t_{s_1} \left(\sum_{t_{s_1+1}=1}^{r} \cdots \sum_{t_{s_2}=1}^{r} t_{s_1+1}\min(t_{s_1+1}, t_{s_1+2}) \cdots \min(t_{s_2-1}, t_{s_2})t_{s_2} \right) 2t_{s_2+1} \cdots$$
$$\cdots 2t_{s_{k-1}} \left(\sum_{t_{s_{k-1}+1}=1}^{r} \cdots \sum_{t_{s_k}=1}^{r} t_{s_{k-1}+1}\min(t_{s_{k-1}+1}, t_{s_{k-1}+2}) \cdots \min(t_{s_k-1}, t_{s_k})t_{s_k} \right) 2t_{s_k+1} \cdots .$$

By the assumption of the claim that $\sum_{t_\beta} \cdots \sum_{t_\alpha} t_\beta \min(t_\beta, t_{\beta-1}) \min(t_{\beta-1}, t_{\beta-2}) \ldots \min(t_{\alpha+1}, t_\alpha)t_\alpha$ is a multiple of $q = 2r+1$, since we can apply this assumption to the $k-1$ locations parenthesized in the above expression, γ is a multiple of $q^{r-k} \cdot q^{k-1} = q^{r-1}$. □

Proof of Claim 4.21. Induction on β. In the base case where $\beta = \alpha$, the lefthand side of (9) is $\sum_{t_\beta=1}^{r} t_\beta^2$. Note that $2(\beta - \alpha + 1) = 2$ in this case. Hence the statement follows in the base case.

In the inductive case, we assume that there are constants $\theta_d, \theta_{d-2}, \ldots, \theta_2$ such that

$$\sum_{t_{\beta-1}=1}^{r} \sum_{t_{\beta-2}=1}^{r} \cdots \sum_{t_\alpha=1}^{r} t_{\beta-1}\min(t_{\beta-1}, t_{\beta-2}) \ldots \min(t_{\alpha+1}, t_\alpha)t_\alpha = \sum_{t_{\beta-1}=1}^{r} \sum_{\substack{2 \le i \le d \\ i:\text{ even}}} \theta_i t_{\beta-1}^i,$$

where $d \le 2(\beta - 1 - \alpha + 1) = 2(\beta - \alpha)$. We show from this inductive hypothesis the statement holds.

Then

$$\sum_{t_{\beta-2}=1}^{r} \cdots \sum_{t_\alpha=1}^{r} \min(t_{\beta-1}, t_{\beta-2}) \ldots \min(t_{\alpha+1}, t_\alpha)t_\alpha = \sum_{\substack{1 \le i \le d-1 \\ i:\text{ odd}}} \theta_{i+1} t_{\beta-1}^i.$$

Let $X_{t_{\beta-1}}$ be the above summation $\sum_{i:\text{ odd}} \theta_{i+1} t_{\beta-1}^i$. It therefore suffices to show that there are constants $\theta'_1, \theta'_3, ..., \theta'_{d+1}$ such that

$$\sum_{t_{\beta-1}=1}^{r} \min(t_\beta, t_{\beta-1}) X_{t_{\beta-1}} = \sum_{\substack{1 \le i \le d+1 \\ i:\text{ odd}}} \theta'_i t_\beta^i, \tag{11}$$

since

$$\sum_{t_\beta=1}^{r}\sum_{t_{\beta-1}=1}^{r} t_\beta \min(t_\beta, t_{\beta-1})X_{t_{\beta-1}} = \sum_{t_\beta=1}^{r}\sum_{t_{\beta-1}=1}^{r}\cdots\sum_{t_\alpha=1} t_\beta \min(t_\beta, t_{\beta-1})\ldots\min(t_{\alpha+1}, t_\alpha)t_\alpha$$
$$= \sum_{t_\beta=1}^{r}\sum_{\substack{2\le i\le d+2\\ i:\text{ even}}} \theta'_{i-1}t_\beta^i$$

and then $d+2 \le 2(\beta-\alpha+1)$ if Equation (11) holds, which completes the induction.

Now, we show that Equation (11) holds. For simplification, we denote $t_{\beta-1}$ by t and t_β by z. Then the lefthand side of (11) is

$$\sum_{t=1}^{r}\min(z,t)X_t = \sum_{t=1}^{z} tX_t + \sum_{t=z+1}^{r} zX_t$$
$$= \sum_{t=1}^{z} tX_t - \sum_{t=1}^{z} zX_t + \sum_{t=1}^{r} zX_t.$$

Therefore, it is sufficient to show that the above expression has an odd degree on z and the maximum degree is at most $d+1$.

The last term $\sum_{t=1}^{r} zX_t$ obviously is of degree 1 on z. For the remaining two terms, we use the following claim, that presents implicit forms of the power sum. This claim is also obtained from basic properties of a power sum (see e.g., [GKP89]).

Claim 4.23. *Let i be a positive integer. There are constants $c_0, c_1, \ldots, c_{i+1}$ such that if i is an even*

$$\sum_{t=1}^{z} t^i = \frac{1}{2}z^i + \sum_{j=0}^{i/2} c_{2j+1}z^{2j+1},$$

and if i is an odd

$$\sum_{t=1}^{z} t^i = \frac{1}{2}z^i + \sum_{j=0}^{(i+1)/2} c_{2j}z^{2j}.$$

From this claim, the two terms can be written as

$$\sum_{t=1}^{z} tX_t = \sum_{\substack{1\le i\le d-1\\ i:\text{ odd}}}\sum_{t=1}^{z}\theta_{i+1}t^{i+1} = \sum_{\substack{1\le i\le d-1\\ i:\text{ odd}}}\theta_{i+1}\left(\frac{1}{2}z^{i+1} + \sum_{j=0}^{(i+1)/2} c_{2j+1}z^{2j+1}\right)$$

and

$$\sum_{t=1}^{z} zX_t = \sum_{\substack{1\le i\le d-1\\ i:\text{ odd}}}\sum_{t=1}^{z}\theta_{i+1}zt^{i} = \sum_{\substack{1\le i\le d-1\\ i:\text{ odd}}}\theta_{i+1}\left(\frac{1}{2}z^{i+1} + \sum_{j=0}^{(i+1)/2} c_{2j}z^{2j+1}\right).$$

Therefore, we have for the two terms

$$\sum_{t=1}^{z} tX_t - \sum_{t=1}^{z} zX_t = \sum_{\substack{1\le i\le d-1\\ i:\text{ odd}}}\theta_{i+1}\left(\sum_{j=0}^{(i+1)/2}(c_{2j+1}-c_{2j})z^{2j+1}\right).$$

The righthand side of the above expression only has terms of odd degree and the maximum degree is at most $d+1$. Therefore, for some constants $\theta'_1, \theta'_3 ..., \theta'_{d+1}$ Equation (11) holds, which completes the inductive case. □

5 Open Problem

We have shown that the correlation $\mathrm{Corr}(\mathrm{MOD}_m, P_d^{(q)})$ is exponentially small for a prime q and an integer m coprime to q. An obvious open problem is to extend the parameter q from primes to general integers.

In the estimation of $U_q^k(e_m^a)$, we have proven

$$\gcd(g_1(k), g_2(k), \ldots, g_r(k)) = q^{\lfloor (k-2)/(q-1) \rfloor + 1}$$

for an odd prime q, where $r = \lfloor q/2 \rfloor$. We conjecture by using computer programs that the following holds:

$$\gcd(g_1(k), g_2(k), \ldots, g_r(k)) = \begin{cases} \text{a power of } p & \text{if } q \text{ is a power of a prime } p \\ q & \text{otherwise.} \end{cases}$$

If we resolve this conjecture, we can prove the case where q is a power of some prime and the most general case.

References

[AB01] Noga Alon and Richard Beigel. Lower bounds for approximations by low degree polynomials over $\mathbb{Z}_m$. In *Proceedings of the 16 th IEEE Conference on Computational Complexity*, pages 184–187, 2001.

[AKK+03] Noga Alon, Tali Kaufman, Michael Krivelevich, Simon Litsyn, and Dana Ron. Testing low-degree polynomials over GF(2). In *Proceedings of RANDOM-APPROX*, pages 188–199, 2003.

[All89] Eric Allender. A note on the power of threshold circuits. In *30th Annual Symposium on Foundations of Computer Science*, pages 514–519, 1989.

[Bog05] Andrej Bogdanov. Pseudorandom generators for low degree polynomials. In *Proceedings of the 37th annual ACM symposium on Theory of computing*, pages 21–30, 2005.

[Bou05] Jean Bourgain. Estimation of certain exponential sums arising in complexity theory. *Comptes Rendus Mathematique*, 340(9):627–631, 2005.

[BV07] Andrej Bogdanov and Emanuele Viola. Pseudorandom bits for polynomial. In *48th Annual IEEE Symposium on Foundations of Computer Science*, pages 41–51, 2007.

[Cha06] Arkadev Chattopadhyay. An improved bound on correlation between polynomials over $\mathbb{Z}_m$ and MOD_q. Technical Report TR06-107, Electronic Colloquium on Computational Complexity, 2006.

[GKP89] Ronald Graham, Donald Knuth, and Oren Patashnik. *Concrete Mathematics: A Foundation for Computer Science*. Addison-Wesley Publishing Company, 1989.

[Gow98] Timothy Gowers. A new proof of Szemerédi's theorem for arithmetic progressions of length four. *Geometric and Functional Analysis*, 8(3):529–551, 1998.

[Gow01] Timothy Gowers. A new proof of Szemerédi's theorem. *Geometric and Functional Analysis*, 11(3):465–588, 2001.

[GRS05] Frederic Green, Amitabha Roy, and Howard Straubing. Bounds on an exponential sum arising in Boolean circuit complexity. *Comptes Rendus Mathematique*, 341(5):279–282, 2005.

[GT08] Ben Green and Terence Tao. An inverse theorem for the Gowers $U^3(G)$ norm. *Proceedings of the Edinburgh Mathematical Society (Series 2)*, 51(1):73–153, 2008.

[HMP+93] András Hajnal, Wolfgang Maass, Pavel Pudlák, Mario Szegedy, and György Turán. Threshold circuits of bounded depth. *Journal of Computer and System Sciences*, 46(2):129–154, 1993.

[KL08] Tali Kaufman and Shachar Lovett. Worst case to average case reductions for polynomials. In *49th Annual IEEE Symposium on Foundations of Computer Science*, pages 166–175, 2008.

[Lov08] Shachar Lovett. Unconditional pseudorandom generators for low degree polynomials. In *Proceedings of the 40th annual ACM symposium on Theory of computing*, pages 557–562, 2008.

[Raz87] Alexander Razborov. Lower bounds on the size of bounded depth circuits over a complete basis with logical addition. *Mathematical notes of the Academy of Sciences of the USSR*, 41(4):333–338, 1987.

[Sam07] Alex Samorodnitsky. Low degree tests at large distances. In *Proceedings of the 39th annual ACM symposium on Theory of computing*, pages 506–515, 2007.

[Smo87] Roman Smolensky. Algebraic methods in the theory of lower bounds for Boolean circuit complexity. In *Proceedings of the 19th annual ACM symposium on Theory of computing*, pages 77–82, 1987.

[ST06] Alex Samorodnitsky and Luca Trevisan. Gowers uniformity, influence of variables, and PCPs. In *Proceedings of the 38th annual ACM symposium on Theory of computing*, pages 11–20, 2006.

[Vio08] Emanuele Viola. The sum of d small-bias generators fools polynomials of degree d. In *Proceedings of the 2008 IEEE 23rd Annual Conference on Computational Complexity*, pages 124–127, 2008.

[VW08] Emanuele Viola and Avi Wigderson. Norms, XOR Lemmas, and lower bounds for polynomials and protocols. *Theory of Computing*, 4(1):137–168, 2008.