PAPER Special Section on Foundations of Computer Science

# Estimating the Gowers Norm of Modulo Functions over Prime Fields

**Akinori KAWACHI**[†a)], *Nonmember*, **Hidetoki TANAKA**[†b)], *Student Member*, *and* **Osamu WATANABE**[†c)], *Fellow*

**SUMMARY** We show a technique for estimating an upper bound of the Gowers norm of modulo functions over prime fields, which reduces the estimation to the greatest common divisor of some periodic sequences. This estimation provides inapproximability of the modulo functions by low-degree polynomials over prime fields, which is a generalization of Viola and Wigderson's result in the case of the binary field.

***key words:*** *Gowers norm, Modulo functions*

## 1. Introduction

### 1.1 Background

The Gowers norm is a measure for analyzing functions from a viewpoint of derivatives over general groups. This measure was originally introduced by Gowers [1], [2] to give an alternative proof of Szemerédi's theorem.

**Definition 1** (Gowers norm): Let $d \geq 0$, $G$ be an additive group, and $\oplus$ be the addition over $G$. Then the degree $d$ Gowers norm $\|f\|_{U^d}$ of a function $f : G \to \mathbb{C}$ is defined as

$$\|f\|_{U^d} := \mathop{\mathrm{E}}_{\boldsymbol{x},\boldsymbol{y}_1,\ldots,\boldsymbol{y}_d \in G} \left[ \prod_{\substack{S \subseteq [d] \\ |S| \text{is even}}} v_f(\boldsymbol{x}, S) \cdot \prod_{\substack{S \subseteq [d] \\ |S| \text{is odd}}} \overline{v_f(\boldsymbol{x}, S)} \right]^{1/2^d}, \tag{1}$$

where $v_f(\boldsymbol{x}, S)$ is defined by

$$v_f(\boldsymbol{x}, S) := f\left( \boldsymbol{x} \oplus \bigoplus_{j \in S} \boldsymbol{y}_j \right)$$

and $\overline{v_f(\boldsymbol{x}, S)}$ is its conjugate.

**Remark.** Throughout this paper, for any fixed $n \geq 1$, we consider functions over $n$ variables. But for simplicity, we identify $n$-variate functions and functions on vectors consisting of $n$ elements.

Note that the Gowers norm is indeed a norm [1], [2], i.e., the Gowers norm takes a positive real, and satisfies the triangle inequality.

We state this general definition for the sake of completeness of our presentation; but for our target function, the Gowers norm can be expressed in a much simpler form (see (5) in Sect. 2), which is the actual target of our analysis.

There are many applications of the Gowers norm in complexity theory such as linearity testing in PCP [3], [4], pseudorandom generators for low-degree polynomials [5], [6], and hardness amplification for low-degree polynomials [7]. These results are shown by analyzing the Gowers norm over the binary field $\mathbb{Z}_2$. On the other hand, the Gowers norm over general groups are also important as well. The analysis of the Gowers norm is equivalent to a generalization of the Fourier analysis, known as the "higher-order Fourier analysis," which recently attracts much attention in mathematics, e.g., [8]. In this context, it is more natural to analyze the Gowers norm over general groups of important functions. The main technical contribution of this paper is to demonstrate some approach for analyzing the Gowers norm over general groups (see Sect. 1.2).

Let us see a typical example of using the Gowers norm. Viola and Wigderson [7] provided an elegant and simple proof for a correlation bound between the modulo function and low-degree polynomials over $\mathbb{Z}_2$ by estimating the Gowers norm of the modulo function. The correlation between a function $f$ and a class $C$ of functions is defined as

$$\mathrm{Corr}(f, C) := \min_{g \in C} \left| \Pr_x [f(x) = g(x)] - \Pr_x [f(x) \neq g(x)] \right|.$$

That is, if there is some function $g \in C$ that approximates $f$ well, then $\mathrm{Corr}(f, C)$ is close to 1, and otherwise, $\mathrm{Corr}(f, C)$ is close to 0. Let $\mathsf{MOD}_m$ be an $n$-variate modulo function defined by

$$\mathsf{MOD}_m(x_1, \ldots, x_n) := \begin{cases} -1, & \text{if } m \text{ divides } \sum_{i=1}^n x_i, \text{ and} \\ +1, & \text{otherwise.} \end{cases}$$

For any $D \subseteq \mathbb{Z}$, by $\mathsf{MOD}_m|_D$ we denote the $n$-variate function $\mathsf{MOD}_m$ whose domain is restricted to $D^n$. Let $P_d^{(2)}$ be the set of $n$-variate polynomials* of degree $d$ over $\mathbb{Z}_2$.

Manuscript received April 11, 2011.
Manuscript revised June 20, 2011.

[†]The authors are with Tokyo Institute of Technology, Tokyo, 152–8552 Japan.
a) E-mail: kawachi@is.titech.ac.jp
b) E-mail: tanaka7@is.titech.ac.jp
c) E-mail: watanabe@is.titech.ac.jp

DOI: 10.1587/transinf.E95.D.755

*Precisely speaking, for comparing with the function $\mathsf{MOD}_m$ that takes ±1 values, we assume that 1 and 0 values of polynomials are converted to −1 and +1 respectively. In other words, $P_d^{(2)}$ is the set of functions that are expressed as $\mathrm{sg}(p(x))$ with some $n$-variate degree-$d$ polynomial $p(x)$ mapping $\mathbb{Z}_2^n$ to $\mathbb{Z}_2$, where $\mathrm{sg}(v) := -1$ if $v = 1$ and +1 otherwise. In this paper, we will simply call such functions "polynomials."

Viola and Wigderson investigated the power of degree $d$ polynomials over $\mathbb{Z}_2$ for approximating $\mathsf{MOD}_m|_{\mathbb{Z}_2}$. They showed that $\mathrm{Corr}(\mathsf{MOD}_m|_{\mathbb{Z}_2}, P_d^{(2)}) \le \mathrm{e}^{-\Omega(n/4^d)}$ for any odd $m$; that is, no low-degree polynomial approximates the modulo function well. Their proof takes the following two steps: first the estimation of the correlation is reduced to that of the Gowers norm of this modulo function over the *binary* field $\mathbb{Z}_2$, and then, this Gowers norm is estimated. More concretely, in the second step, they showed that this Gowers norm over $\mathbb{Z}_2$ satisfies

$$\|\mathsf{MOD}_m|_{\mathbb{Z}_2}\|_{\mathrm{U}^k} \le m\left\{1-\alpha\left(\frac{1}{2}\right)^k\right\}^{\frac{n}{2^k}} \tag{2}$$

for some constant $\alpha > 0$ that depends only on $m$. This bound is not so difficult to show. On the other hand, it seems difficult to obtain similar bounds for the Gowers norm over more general fields. Indeed, there have been few results for the estimation over non-binary fields [9], especially, of important functions from computer-scientific viewpoints. The main purpose of this paper is to demonstrate some technical approach for such analysis.

### 1.2 Our Result

We demonstrate some approach for analyzing the Gowers norm of the modulo function over prime fields $\mathbb{Z}_q$. Our target function is $\mathsf{MOD}_m$ the same function that has been studied in [7]; but here we analyze its Gowers norm over the finite field $\mathbb{Z}_q$ for any prime $q$ (hence, more precisely, our target is $\mathsf{MOD}_m|_{\mathbb{Z}_q}$). We show the following upper bound similar to the bound (2).

**Theorem 2** (Main theorem): For any prime $q \ge 3$ and any $m$ coprime to $q$, let $\|\mathsf{MOD}_m|_{\mathbb{Z}_q}\|_{\mathrm{U}^k}$ be the Gowers norm of $\mathsf{MOD}_m$ over $\mathbb{Z}_q$. Then, for all even $k \ge 2$, we have

$$\|\mathsf{MOD}_m|_{\mathbb{Z}_q}\|_{\mathrm{U}^k} \le m\left\{1-\alpha\left(\frac{2}{q}\right)^k\right\}^{\frac{n}{2^k}},$$

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

This, following [7], immediately yields the following correlation bound between $\mathsf{MOD}_m|_{\mathbb{Z}_q}$ and $P_d^{(q)}$.

**Corollary 3:** Let $q \ge 3$ be a prime and let $m$ be coprime to $q$. Then we have

$$\mathrm{Corr}(\mathsf{MOD}_m|_{\mathbb{Z}_q}, P_d^{(q)}) \le \mathrm{e}^{-\Omega(n/q^d)}.$$

**Remark.** We define the set $P_d^{(q)}$ of polynomials in the same way as $P_d^{(2)}$. That is, $P_d^{(q)}$ is the set of functions that are expressed as $\mathrm{sg}(p(x))$ with some degree-$d$ polynomial $p(x)$ mapping $\mathbb{Z}_q^n$ to $\mathbb{Z}_q$.

Although the function $\mathsf{MOD}_m$ has been studied in the literature as one of the typical functions for discussing complexity lower bounds, one may think that it is a rather technical target. On the other hand, our main result is obtained in fact by analyzing more basic functions that are defined by

$$\mathsf{e}_m^\ell(x) := \mathrm{e}^{2\pi i\ell x/m} \tag{3}$$

with parameters $m$ and $\ell \in [m-1]$. These functions form the Fourier basis over finite cyclic groups $\mathbb{Z}_m$. Hence, by applying our technique, we can prove an upper bound of the Gowers norm of any function over a finite cyclic group if we know its Fourier coefficients. Thus, our analysis could be useful for other applications of the Gowers norm over a finite cyclic group.

Note that a more recent result [10] also provides a different technique to estimate a variation of the Gowers norm of another version of modulo functions over prime fields. Their target function $\mathsf{MOD}'_m : \mathbb{Z}_q^n \to \mathbb{Z}_m$ is

$$\mathsf{MOD}'_m(x_1,\ldots,x_n) := \left(\sum_{i=1}^n x_i\right) \bmod m$$

for $m < q$, where the sum is computed in $\mathbb{Z}$. Due to this difference, a variation of the Gowers norm is analyzed. Also the technique is based on analysis of directional derivatives, which is totally different from ours.

### 1.3 Overview of Our Analysis

Here we explain briefly the outline of our analysis and the organization of this paper. For proving the main theorem, we first bound the Gowers norm of $\mathsf{MOD}_m$ over $\mathbb{Z}_q$ by

$$\|\mathsf{MOD}_m|_{\mathbb{Z}_q}\|_{\mathrm{U}^k} \le m\left(\max_{\ell\in[m-1]}\|\mathsf{e}_m^\ell\|_{\mathrm{U}^k}\right)^n \tag{4}$$

Then our task is reduced to give a good bound for the Gowers norm of each $\mathsf{e}_m^\ell$. For this task, we introduce a sequence of $q$-tuple $\boldsymbol{g}(k) := (g_1(k),\ldots,g_q(k))$ of numbers, and show that

$$\left(\|\mathsf{e}_m^\ell\|_{\mathrm{U}^k}\right)^{2^k} \le 1-\left(\frac{2}{q}\right)^k\left\{1-\frac{\sum_{j=1}^q \cos\left(\frac{2\pi}{m}\ell\cdot g_j(k)\right)}{q}\right\}$$

for all $\ell \in [m-1]$. This bound is useless if all $g_1(k),\ldots,g_q(k)$ were divided by $m$ because in this case, the lemma would yield only a trivial upper bound $\left(\|\mathsf{e}_m^\ell\|_{\mathrm{U}^k}\right)^{2^k} \le 1$. We will, however, show that this is not the case; that is, there is some $g_j(k)$ that is not divisible by $m$, which is the main technical lemma and the nontrivial part of our technique.

In Sect. 2, we explain our analysis following this outline, and in Sect. 3, we give the proof of the main technical lemma.

## 2. Proof of the Main Theorem

We follow the outline stated in Sect. 1.3 and prove the main theorem. Throughout this section, we fix any $n \ge 1$, any prime $q \ge 3$, and any $m$ that is coprime to $q$. Our target function is $\mathsf{MOD}_m|_{\mathbb{Z}_q}$, but we omit the subscript specifying

the domain for simplifying our notation. The Gowers norm we consider here is defined over the field $(\mathbb{Z}_q)^n$. Note that for any $n$-variate real valued function $f$, its degree $d$ Gowers norm is simply stated as

$$\|f\|_{\mathrm{U}^d} = \mathop{\mathrm{E}}_{\boldsymbol{x},\boldsymbol{y}_1,\ldots,\boldsymbol{y}_d\in\mathbb{Z}_q^n}\left[\prod_{S\subseteq[d]} f\left(\boldsymbol{x}\oplus\bigoplus_{j\in S}\boldsymbol{y}_j\right)\right]^{1/2^d}, \tag{5}$$

where by $\boldsymbol{x}\oplus\boldsymbol{y}$ we denote the component-wise $\mathbb{Z}_q$ addition of vectors.

First we prove the bound (4).

**Lemma 4:** The bound (4) holds for all $\ell\in[m-1]$.

*Proof.* For any $\ell\in[m-1]$, define $u_\ell(x_1,\ldots,x_n)$ by

$$u_\ell(x_1,\ldots,x_n) := \mathsf{e}_m^\ell\left(\sum_{j=1}^n x_j\right).$$

Then it is easy to see that for every $(x_1,\ldots,x_n)\in\mathbb{Z}_q^n$, $\sum_{\ell=1}^{m-1} u_\ell(x_1,\ldots,x_n)$ is $m-1$ if $m$ divides $\sum_{i=1}^n x_i$ and $-1$ otherwise. This means that $\mathsf{MOD}_m(x_1,\ldots,x_n)\le\sum_{\ell=1}^{m-1}u(x_1,\ldots,x_n)$ in the domain $\mathbb{Z}_q^n$. Hence, by using (5), we have

$$\begin{aligned}\|\mathsf{MOD}_m\|_{\mathrm{U}^k} &= \mathop{\mathrm{E}}_{\boldsymbol{x},\boldsymbol{y}_1,\ldots,\boldsymbol{y}_k\in\mathbb{Z}_q^n}\left[\prod_{S\subseteq[k]}\mathsf{MOD}_m\left(\boldsymbol{x}\oplus\bigoplus_{j\in S}\boldsymbol{y}_j\right)\right]^{1/2^k}\\ &\le \mathop{\mathrm{E}}_{\boldsymbol{x},\boldsymbol{y}_1,\ldots,\boldsymbol{y}_k\in\mathbb{Z}_q^n}\left[\prod_{S\subseteq[k]}\sum_{\ell=1}^{m-1}u_\ell\left(\boldsymbol{x}\oplus\bigoplus_{j\in S}\boldsymbol{y}_j\right)\right]^{1/2^k}\\ &= \left\|\sum_{\ell=1}^{m-1}u_\ell\right\|_{\mathrm{U}^k}.\end{aligned}$$

On the other hand, by the triangle inequality, we have

$$\left\|\sum_{\ell=1}^{m-1}u_\ell\right\|_{\mathrm{U}^k}\le\sum_{\ell=1}^{m-1}\|u_\ell\|_{\mathrm{U}^k}\le m\cdot\max_{\ell\in[m-1]}\|u_\ell\|_{\mathrm{U}^k}.$$

Now consider $\|u_\ell\|_{\mathrm{U}^k}$ for any $\ell\in[m-1]$. Then we have

$$\begin{aligned}\|u_\ell\|_{\mathrm{U}^k} &= \mathop{\mathrm{E}}_{\boldsymbol{x},\boldsymbol{y}_1,\ldots,\boldsymbol{y}_k\in\mathbb{Z}_q^n}\left[\prod_{S\subseteq[k]}\mathsf{e}_m^\ell\left(\sum_{i=1}^n x_i\oplus\bigoplus_{j\in S}y_{j,i}\right)\right]^{\frac{1}{2^k}}\\ &= \mathop{\mathrm{E}}_{\boldsymbol{x},\boldsymbol{y}_1,\ldots,\boldsymbol{y}_k\in\mathbb{Z}_q^n}\left[\prod_{i=1}^n\prod_{S\subseteq[k]}\mathsf{e}_m^\ell\left(x_i\oplus\bigoplus_{j\in S}y_{j,i}\right)\right]^{\frac{1}{2^k}}\\ &= \mathop{\mathrm{E}}_{x,y_1,\ldots,y_k\in\mathbb{Z}_q}\left[\prod_{S\subseteq[k]}\mathsf{e}_m^\ell\left(x\oplus\bigoplus_{j\in S}y_j\right)\right]^{\frac{n}{2^k}} = \left(\|\mathsf{e}_m^\ell\|_{\mathrm{U}^k}\right)^n,\end{aligned}$$

where $x_i$ and $y_{j,i}$ denote respectively the $i$th coordinate of vector $\boldsymbol{x}$ and $\boldsymbol{y}_j$. The bound (4) follows. ■

Now our task is to give a good bound for $\|\mathsf{e}_m^\ell\|_{\mathrm{U}^k}$. For this, we introduce a sequence $\{\boldsymbol{g}(k)\}_{k\ge2}$ of $q$-tuples of $\mathbb{Z}_q$ elements. First define a $q\times q$ circulant matrix $D_q$ by

$$D_q=\begin{bmatrix}1&-1&&&\\&1&-1&&\\&&\ddots&\ddots&\\&&&1&-1\\-1&&&&1\end{bmatrix},$$

where empty entries represent 0 in the matrix. Then we define the $k$th $q$-tuple $\boldsymbol{g}(k)=(g_1(k),g_2(k),\ldots,g_q(k))$ inductively. Define $\boldsymbol{g}(2):=(0,\ldots,0,-q,q)$, and for any $k\ge3$, define

$$\boldsymbol{g}(k)^{\mathrm{T}} := D_q\boldsymbol{g}(k-1)^{\mathrm{T}},$$

where by $\boldsymbol{x}^{\mathrm{T}}$ we denote the transposition of a row vector $\boldsymbol{x}$. Note that the computation is over $\mathbb{Z}_q$.

By using this sequence, we now show the following bound for $\|\mathsf{e}_m^\ell\|_{\mathrm{U}^k}$.

**Lemma 5:** For all $\ell\in[m-1]$ and all $k\ge2$, we have

$$\left(\|\mathsf{e}_m^\ell\|_{\mathrm{U}^k}\right)^{2^k}\le1-\left(\frac{2}{q}\right)^k\left\{1-\frac{\sum_{j=1}^q\cos\left(\frac{2\pi}{m}\ell\cdot g_j(k)\right)}{q}\right\}.$$

*Proof.* By Definition 1, $\left(\|\mathsf{e}_m^\ell\|_{\mathrm{U}^k}\right)^{2^k}$ is expressed as

$$\mathop{\mathrm{E}}_{\substack{x\in\mathbb{Z}_q\\y_1,\ldots,y_k\in\mathbb{Z}_q}}\left[\prod_{\substack{S\subseteq[k]\\|S|\text{ is even}}}\mathsf{e}_m^\ell\left(x\oplus\bigoplus_{j\in S}y_j\right)\cdot\prod_{\substack{S\subseteq[k]\\|S|\text{ is even}}}\overline{\mathsf{e}_m^\ell\left(x\oplus\bigoplus_{j\in S}y_j\right)}\right].$$

Since $\mathsf{e}_m^\ell(x)=\mathrm{e}^{2\pi i\ell x/m}$, we have $\overline{\mathsf{e}_m^\ell(x)}=\mathsf{e}_m^\ell(-x)$ and $\mathsf{e}_m^\ell(z)\cdot\mathsf{e}_m^\ell(z')=\mathsf{e}_m^\ell(z+z')$; hence, we can simplify the above to derive

$$\left(\|\mathsf{e}_m^\ell\|_{\mathrm{U}^k}\right)^{2^k}=\frac{1}{q^{k+1}}\sum_{x,y_1,\ldots,y_k\in\mathbb{Z}_q}\mathsf{e}_m^\ell\left(\sum_{S\subseteq[k]}(-1)^{|S|}\left(x\oplus\bigoplus_{j\in S}y_j\right)\right).$$

Let

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

Note that $\mathsf{e}_m^\ell(x)=\cos\left(\frac{2\pi}{m}\ell\cdot x\right)+i\sin\left(\frac{2\pi}{m}\ell\cdot x\right)$; hence, from the fact that the Gowers norm is positive real, we have

$$\left(\|\mathsf{e}_m^\ell\|_{\mathrm{U}^k}\right)^{2^k}=\frac{1}{q^{k+1}}\sum_{x,y_1,\ldots,y_k\in\mathbb{Z}_q}\cos\left(\frac{2\pi}{m}\ell\cdot Q_{x,y_1,\ldots,y_k}\right).$$

Bounding $\cos(\cdot)$ by the trivial 1 on inputs $y_1,\ldots,y_k$ in $\mathbb{Z}_q^k\setminus\{1,q-1\}^k$, we then obtain the following bound.

$$\left(\|\mathsf{e}_m^\ell\|_{\mathrm{U}^k}\right)^{2^k}$$

$$\le \frac{1}{q^{k+1}}\left\{\sum_{\substack{x\in\mathbb{Z}_q\\ \forall y_i\in\{1,q-1\}}}\cos\left(\frac{2\pi}{m}\ell\cdot Q_{x,y_1,\ldots,y_k}\right)+(q^{k+1}-2^k q)\right\}$$

$$= 1-\left(\frac{2}{q}\right)^k+\frac{1}{q^{k+1}}\left\{\sum_{\substack{x\in\mathbb{Z}_q\\ \forall y_i\in\{1,q-1\}}}\cos\left(\frac{2\pi}{m}\ell\cdot Q_{x,y_1,\ldots,y_k}\right)\right\}$$

$$= 1-\left(\frac{2}{q}\right)^k\left\{1-\frac{1}{2^k q}\sum_{\substack{x\in\mathbb{Z}_q\\ \forall y_i\in\{1,q-1\}}}\cos\left(\frac{2\pi}{m}\ell\cdot Q_{x,y_1,\ldots,y_k}\right)\right\}. \quad (6)$$

Now for any $y_1,\ldots,y_k\in\{1,q-1\}$, we can claim (see Claim 6 below) that sequence $(Q_{x,y_1,\ldots,y_k})_{x\in[q-1]}$ is a permutation of sequence $\boldsymbol{g}(k)$. Hence we have

$$\sum_{x\in\mathbb{Z}_q}\cos\left(\frac{2\pi}{m}\ell\cdot Q_{x,y_1,\ldots,y_k}\right)=\sum_{j=1}^{q}\cos\left(\frac{2\pi}{m}\ell\cdot g_j(k)\right).$$

Then the bound of the lemma follows from this and the above bound (6). ■

**Claim 6:** For any integer $k\ge 2$, consider any $y_1,\ldots,y_k\in\{1,q-1\}$. Then sequence $(Q_{x,y_1,\ldots,y_k})_{x\in[q-1]}$ is a permutation of sequence $\boldsymbol{g}(k)$.

*Proof.* Let $\{\{\cdot\}\}$ denotes a multiset. For the claim, we show by induction on $k$ that

$$\left\{\left\{Q_{0,y_1,\ldots,y_k},\ldots,Q_{q-1,y_1,\ldots,y_k}\right\}\right\}=\left\{\left\{g_1(k),\ldots,g_q(k)\right\}\right\}$$

holds for all $k\ge 2$ and $y_1,\ldots,y_k\in\{1,q-1\}$.

For the base case, i.e., $k=2$, noting that

$$Q_{x,y_1,y_2}=x-(x\oplus y_1)-(x\oplus y_2)+(x\oplus y_1\oplus y_2),$$

we obtain

$$\left\{\left\{Q_{0,y_1,y_2},\ldots,Q_{q-1,y_1,y_2}\right\}\right\}=\{\{0,\ldots,0,q,-q\}\}.$$

For showing the inductive step for $k\ge 3$, we first note that $Q_{x,y_1,\ldots,y_k}$ can be expressed as

$$Q_{x,y_1,\ldots,y_k}=Q_{x,y_1,\ldots,y_{k-1}}-Q_{x\oplus y_k,y_1,\ldots,y_{k-1}}.$$

Then for the case $y_k=1$, by the induction hypothesis, we have

$$\begin{aligned}&\left\{\left\{Q_{0,y_1,\ldots,y_k},\ldots,Q_{q-1,y_1,\ldots,y_k}\right\}\right\}\\&=\left\{\left\{g_1(k-1)-g_2(k-1),\ldots,g_q(k-1)-g_1(k-1)\right\}\right\}\\&=\left\{\left\{g_1(k),\ldots,g_q(k)\right\}\right\}.\end{aligned}$$

Similarly, for the case $y_k=q-1$, we have

$$\begin{aligned}&\left\{\left\{Q_{0,y_1,\ldots,y_k},\ldots,Q_{q-1,y_1,\ldots,y_k}\right\}\right\}\\&=\left\{\left\{g_2(k-1)-g_1(k-1),\ldots,g_1(k-1)-g_q(k-1)\right\}\right\}\\&=\left\{\left\{-g_1(k),\ldots,-g_q(k)\right\}\right\}=\left\{\left\{g_1(k),\ldots,g_q(k)\right\}\right\},\end{aligned}$$

where the last equality can be proved also by induction. ■

Here for using the bound of Lemma 5 to derive the desired bound, it suffices to show that some $g_j(k)$ is not divisible by $m$, which is immediate from the following lemma that will be proved in the next section.

**Lemma 7** (Main lemma): For any even $k\ge 2$, we have

$$\gcd(\boldsymbol{g}(k))=q^{\lfloor(k-2)/(q-1)\rfloor+1},$$

where $\gcd(\boldsymbol{g}(k))$ is the greatest common divisor (GCD) of the numbers in the $q$-tuple $\boldsymbol{g}(k)=(g_1(k),\ldots,g_q(k))$.

*Proof of Theorem 2.* Recall that the bound of Lemma 5. We have

$$\left(\|\mathsf{e}_m^\ell\|_{\mathrm{U}^k}\right)^{2^k}\le 1-\left(\frac{2}{q}\right)^k\left\{1-\frac{\sum_{j=1}^{q}\cos\left(\frac{2\pi}{m}\ell\cdot g_j(k)\right)}{q}\right\}.$$

Then by Lemma 7, for all even $k\ge 2$, there is some $g_j(k)$ that is not divisible by $m$; for this $j$, we have

$$\delta:=\cos\left(\frac{2\pi}{m}\ell g_j(k)\right)<1.$$

Note that $1-\delta>0$ is determined only by $q$ and $m$. Hence, using the trivial bound 1 for the other $\cos(\cdot)$ terms, we obtain

$$\left(\|\mathsf{e}_m^\ell\|_{\mathrm{U}^k}\right)^{2^k}\le 1-\left(\frac{2}{q}\right)^k\left(1-\frac{q-1+\delta}{q}\right).$$

Then by using $\alpha$ defined by

$$\alpha:=1-\frac{q-1+\delta}{q}=\frac{1-\delta}{q}>0,$$

the bound of the theorem is derived. ■

## 3. Proof of Main Lemma

For proving Lemma 7, we estimate the GCD of another tuple rather than that of $\boldsymbol{g}(k)$ directly. Let $r=(q-1)/2$. We define an $r\times r$ matrix $A_r$ by

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

Then define an $r$-tuple $\boldsymbol{a}(2)=(a_1(2),a_2(2),\ldots,a_r(2)):=(0,\ldots,0,q)$, and for each even $k\ge 4$, define the $k$th $r$-tuple inductively by

$$\boldsymbol{a}(k)^{\mathrm{T}}:=A_r\boldsymbol{a}(k-2)^{\mathrm{T}}. \quad (7)$$

It can be shown (see Claim 9 at the end of this proof) that $\gcd(\boldsymbol{g}(k))=\gcd(\boldsymbol{a}(k))$ for any even $k\ge 2$. Thus, for our lemma, it suffices to show that

$$\gcd(\boldsymbol{a}(k)) = q^{\lfloor (k-2)/(q-1) \rfloor + 1} \tag{8}$$

holds for every even $k \geq 2$. We prove this by induction on $k$.

For the case that $2 \leq k \leq q-1$, it is easy to see that (i) $a_1(k), \ldots, a_{r-k/2}(k)$ are all 0, (ii) $a_{r-k/2+1}(k) = q$, and (iii) $a_{r-k/2+2}(k), \ldots, a_r(k)$ are all multiples of $q$. Thus, we have $\gcd(\boldsymbol{a}(k)) = q$ for $2 \leq k \leq q$, which proves (8).

For the case that $k \geq q+1$, for using the induction hypothesis to prove (8) it suffices to show that

$$\gcd(\boldsymbol{a}(k)) = q \cdot \gcd(\boldsymbol{a}(k-(q-1))).$$

This follows from two claims of the following lemma, whose proof will be shown in the following two subsections.

**Lemma 8:** For any even $k \geq q+1$, we have

(a) $\gcd(\boldsymbol{a}(k)) = Q \cdot \gcd(\boldsymbol{a}(k-(q-1))$ for some $Q$ that is multiple of $q$, and
(b) $\gcd(a_1(k)/q, \ldots, a_r(k)/q) = \gcd(\boldsymbol{a}(k-(q-1))$.

Finally we complete the proof by showing the following claim.

**Claim 9:** For any even $k \geq 2$, we have $\gcd(\boldsymbol{g}(k)) = \gcd(\boldsymbol{a}(k))$.

*Proof.* Let $\{\{\boldsymbol{g}(k)\}\}$ to denote $\left\{\left\{g_1(k), \ldots, g_q(k)\right\}\right\}$. For the claim it suffices to show that

$$\{\{\boldsymbol{g}(k)\}\} = \{\{0, \pm a_1(k), \pm a_2(k), \ldots, \pm a_r(k)\}\}$$

holds for every even $k \geq 2$.

But for proving this relation inductively, we consider more detailed relation between two sequences. Here we introduce a variation of mod $q$ addition/subtraction for calculating indices of $q$-tuples. For any $i, j \in [q]$, we define

$$i \overset{q}{+} j := \begin{cases} i+j, & \text{if } i+j \leq q, \text{ and} \\ i+j-q, & \text{if } i+j \geq q+1; \text{ and} \end{cases}$$

$$i \overset{q}{-} j := \begin{cases} i-j, & \text{if } i-j \geq 1, \text{ and} \\ i-j+q, & \text{if } i-j \leq 0. \end{cases}$$

Then we show that for any even $k \geq 2$, we have

$$\begin{aligned} &\exists h \in [q],\ \exists s \in \{+1, -1\} \\ &\quad g_h(k) = 0, \\ &\quad g_{h \overset{q}{+} i}(k) = s \cdot (-1)^i \cdot a_i(k) \qquad (\forall i \in [r]), \\ &\quad g_{h \overset{q}{-} i}(k) = s \cdot (-1)^{i+1} \cdot a_i(k) \qquad (\forall i \in [r]). \end{aligned} \tag{9}$$

Recall that $q = 2r+1$. In the rest of the proof we show this relation by induction on $k$.

First consider the base case, i.e., the case $k = 2$. Recall that $\boldsymbol{g}(2) = (0, \ldots, 0, -q, q)$. By letting $h = r$, we have $g_h(2) = 0$,

$$\begin{aligned} g_{h \overset{q}{+} i}(2) &= 0 = -a_i(2) \qquad (\forall i \in [r-1]), \\ g_{h \overset{q}{-} i}(2) &= 0 = a_i(2) \qquad (\forall i \in [r-1]), \end{aligned}$$

$g_{h \overset{q}{+} r}(2) = -q = -a_r(2)$, and $g_{h \overset{q}{-} r}(2) = g_q(2) = q = a_r(2)$. Hence the relation (9) holds by choosing $s = -1$ and $+1$ respectively for even and odd $r$.

For the induction step, assume that (9) holds for some even $k-2 \geq 2$ with some $h'$ and $s'$, and derive the relation (9) for $k$. (Since the argument is symmetric, we explain for the case $s' = +1$.) It turns out that (9) holds for $k$ with $h = h' \overset{q}{-} 1$ and $s = -1$.

Recall the definition of $\boldsymbol{g}(k)$. We have

$$\boldsymbol{g}(k)^{\mathrm{T}} = (D_q)^2 \boldsymbol{g}(k-2)^{\mathrm{T}},$$

where

$$(D_q)^2 = \begin{bmatrix} 1 & -2 & 1 & & \\ & \ddots & \ddots & \ddots & \\ & & 1 & -2 & 1 \\ 1 & & & 1 & -2 \\ -2 & 1 & & & 1 \end{bmatrix}.$$

Hence for any $j \in [q]$, we have

$$g_j(k) = g_j(k-2) - 2g_{j \overset{q}{+} 1}(k-2) + g_{j \overset{q}{+} 2}(k-2).$$

For obtaining the relation between $\boldsymbol{g}(k)$ and $\boldsymbol{a}(k)$, we replace all $g_{j'}(k-2)$'s with $a_{i'}(k-2)$'s by using the relation (9) for $k-2$, $h'$, and $s = +1$. First since $h = h' \overset{q}{-} 1$, we have

$$\begin{aligned} g_h(k) &= g_{h' \overset{q}{-} 1}(k-2) - 2g_{h'}(k-2) + g_{h' \overset{q}{+} 1}(k-2) \\ &= (-1)^2 a_1(k-2) + 0 + (-1)^1 a_1(k-2) = 0, \end{aligned}$$

which is the first equation of (9) for $k$ and $h$. For showing the second equation, we note that $h \overset{q}{+} (r+1) = h \overset{q}{-} r$. Also we use the following recurrence relation for $\boldsymbol{a}(k)$:

$$\begin{aligned} a_1(k) &= 2a_1(k-2) + a_2(k-2), \\ a_i(k) &= a_{i-1}(k-2) + 2a_i(k-2) + a_{i+1}(k-2) \\ &\qquad\qquad (\forall i \in \{2, \ldots, r-1\}), \\ a_r(k) &= a_{r-1}(k-2) + 3a_r(k-2). \end{aligned}$$

Then we derive

$$\begin{aligned} g_{h \overset{q}{+} 1}(k) &= g_{h'}(k-2) - 2g_{h' \overset{q}{+} 1}(k-2) + g_{h' \overset{q}{+} 2}(k-2) \\ &= 0 - 2(-1)^1 a_1(k-2) + (-1)^2 a_2(k-2) \\ &= (-1) \cdot (-1)^1 a_1(k), \text{ and} \\ g_{h \overset{q}{+} r}(k) &= g_{h' \overset{q}{+} (r-1)}(k-2) - 2g_{h' \overset{q}{+} r}(k-2) + g_{h' \overset{q}{+} (r+1)}(k-2) \\ &= (-1)^{r-1} a_{r-1}(k-2) \\ &\qquad -2(-1)^r a_r(k-2) + (-1)^{r+1} a_r(k-2) \\ &= (-1) \cdot (-1)^r \left(a_{r-1}(k-2) + 3a_r(k-2)\right) \\ &= (-1) \cdot (-1)^r a_r(k). \end{aligned}$$

For any $i \in \{2, \ldots, r-1\}$, we have

$$\begin{aligned} g_{h \overset{q}{+} i}(k) &= g_{h' \overset{q}{+} (i-1)}(k-2) - 2g_{h' \overset{q}{+} i}(k-2) + g_{h' \overset{q}{+} i+1}(k-2) \\ &= (-1)^{i-1} a_{i-1}(k-2) \\ &\qquad -2(-1)^i a_i(k-2) + (-1)^{i+1} a_{i+1}(k-2) \\ &= (-1) \cdot (-1)^i a_i(k). \end{aligned}$$

Thus, the second equation holds for $k$ with $h$ and $s = -1$. The third equation can be shown similarly. ■

### 3.1 Proof of the Part (a) of Lemma 8

Before the proof, we give an explicit expression of $(A_r)^r$.

**Lemma 10:**

$$[(A_r)^r]_{i,j} = \begin{cases} \binom{2r}{r-(i-j)} - \binom{2r}{r-(i+j)}, & \text{if } i+j \le r, \\ \binom{2r}{r-(i-j)} + \binom{2r}{i+j-(r+1)}, & \text{if } i+j \ge r+1, \end{cases}$$

where $[M]_{i,j}$ denotes the $(i,j)$-entry of the matrix $M$.

*Proof.* First we show that

$$[(A_r)^\ell]_{i,j} = \binom{2\ell}{\ell-(i-j)} - \binom{2\ell}{\ell-(i+j)} + \binom{2\ell}{2r+\ell+1-(i+j)} \tag{10}$$

holds for any integer $\ell \in [r]$ by induction on $\ell$.

For the case $\ell = 1$, we can calculate

$$\begin{aligned} &\binom{2}{1-(i-j)} - \binom{2}{1-(i+j)} + \binom{2}{2r+2-(i+j)} \\ &= \begin{cases} 3, & \text{if } i=j=r, \\ 2, & \text{if } i=j<r, \\ 1, & \text{if } i-j=1 \text{ or } j-i=1, \\ 0, & \text{if } i-j>2 \text{ or } j-i>2, \end{cases} \end{aligned}$$

from which it is easy to see that $(A_r)^1$ $(= A_r)$ satisfies (10).

For the case $\ell \ge 2$, we note that

$$\begin{aligned} [(A_r)^\ell]_{i,j} &= \sum_{k=1}^{r} [(A_r)^{\ell-1}]_{i,k}[A_r]_{k,j} \\ &= \begin{cases} 2[(A_r)^{\ell-1}]_{i,1} + [(A_r)^{\ell-1}]_{i,2}, & \text{if } j=1; \\ [(A_r)^{\ell-1}]_{i,j-1} + 2[(A_r)^{\ell-1}]_{i,j} + [(A_r)^{\ell-1}]_{i,j+1}, & \text{if } 1<j<r; \\ [(A_r)^{\ell-1}]_{i,r-1} + 3[(A_r)^{\ell-1}]_{i,r}, & \text{if } j=r. \end{cases} \end{aligned}$$

Then by using the induction hypothesis, it is again easy to show (10).

Now by (10), we have

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

Note that $\binom{2r}{3r+1-(i+j)} = \binom{2r}{2r-\{3r+1-(i+j)\}} = \binom{2r}{i+j-(r+1)}$. If $i+j \le r$, the third term becomes 0, since $i+j-(r+1) < 0$. If $i+j \ge r+1$, the second term becomes 0, since $r-(i+j) < 0$. Therefore the lemma follows. ■

*Proof of Part (a) of Lemma 8.* Since $r = (q-1)/2$, we have

$$\boldsymbol{a}(k)^{\mathrm{T}} = (A_r)^r \boldsymbol{a}(k-(q-1))^{\mathrm{T}}. \tag{11}$$

Hence it is sufficient to show that $2r+1$ divides $[(A_r)^r]_{i,j}$ for every $i, j \in [r]$.

In the case of $i+j \le r$, we have

$$\begin{aligned} [(A_r)^r]_{i,j} &= \binom{2r}{r-i+j} - \binom{2r}{r-i-j} \\ &= \binom{2r}{r-i-j}\left(\frac{\binom{2r}{r-i+j}}{\binom{2r}{r-i-j}} - 1\right). \end{aligned}$$

Here since

$$\begin{aligned} \frac{\binom{2r}{r-i+j}}{\binom{2r}{r-i-j}} &= \frac{(r-i-j)!}{(r-i+j)!} \cdot \frac{(r+i+j)!}{(r+i-j)!} \\ &= \frac{(r+i+j)\cdots(r+i-j+1)}{(r-i+j)\cdots(r-i-j+1)}, \end{aligned}$$

by using a polynomial $F_t(x)$ defined by

$$F_t(x) := \frac{(x+j)\cdots(x-j+1)}{(t+j)\cdots(t-j+1)} - 1,$$

we have

$$[(A_r)^r]_{i,j} = \binom{2r}{r-i-j} \cdot F_{r-i}(r+i).$$

Then by using the fact that

$$\begin{aligned} F_t(-t-1) &= \frac{(-t-1+j)\cdots(-t-1-j+1)}{(t+j)\cdots(t-j+1)} - 1 \\ &= (-1)^{2j}\frac{(t+1-j)\cdots(t+1+j-1)}{(t+j)\cdots(t-j+1)} - 1 \\ &= 1 - 1 = 0, \end{aligned}$$

we can show $x-(-t-1)$ divides $F_t(x)$. In particular, $F_{r-i}(r+i)$ is divided by $2r+1$ $(= (r+i)-(-t-1))$, and thus, $2r+1$ divides $[A_r^r]_{i,j}$ for any $i$ and $j$.

In the case of $i+j \ge r+1$, we have

$$\begin{aligned} [(A_r)^r]_{i,j} &= \binom{2r}{r-i+j} + \binom{2r}{i+j-r-1} \\ &= \binom{2r}{i+j-r-1}\left(\frac{\binom{2r}{r-i+j}}{\binom{2r}{i+j-r-1}} + 1\right). \end{aligned}$$

Here again by using

$$\frac{\binom{2r}{r-i+j}}{\binom{2r}{i+j-r-1}} = \frac{\{2r-j+1+(r-i)\}\cdots\{2r-j+1-(r-i)\}}{\{j+(r-i)\}\cdots\{j-(r-i)\}},$$

we can restate $[(A_r)^r]_{i,j}$ as

$$[(A_r)^r]_{i,j} = \binom{2r}{i+j-r-1} \cdot G(2r-j+1),$$

where $G(x)$ is a polynomial defined by

$$G(x) := \frac{\{x+(r-i)\}\cdots\{x-(r-i)\}}{\{j+(r-i)\}\cdots\{j-(r-i)\}} + 1.$$

Then from the fact that $G(-j) = 0$, we can show that $x-(-j)$ divides $G(x)$. In particular, $2r+1$ $(= (2r-j+1)-(-j))$ divides $G(2r-j+1)$, and thus, it divides $[(A_r)^r]_{i,j}$ for all $i$ and $j$. ■

### 3.2 Proof of the Part (b) of Lemma 8

We first observe the following property on the GCD of tuples.

**Lemma 11:** Let $\boldsymbol{x} = (x_1, \ldots, x_r)$, $\boldsymbol{y} = (y_1, \ldots, y_r)$, and $\boldsymbol{z} = (z_1, \ldots, z_r)$ are vectors denoting $r$-tuples of integers such that $\boldsymbol{y}^{\mathrm{T}} = U\boldsymbol{x}^{\mathrm{T}}$ and $\boldsymbol{z}^{\mathrm{T}} = (VU)\boldsymbol{x}^{\mathrm{T}}$ hold for some $r \times r$ integer matrices $U$ and $V$. Then we have

$$\gcd(y_1, \ldots, y_r) = \gcd(y_1, \ldots, y_r, z_1, \ldots, z_r). \tag{12}$$

In particular, if $UV$ is the identity matrix $I_r$, then we have

$$\gcd(y_1, \ldots, y_r) = \gcd(x_1, \ldots, x_r). \tag{13}$$

*Proof.* First Note that

$$\boldsymbol{z}^{\mathrm{T}} = (VU)\boldsymbol{x}^{\mathrm{T}} = V(U\boldsymbol{x}^{\mathrm{T}}) = V\boldsymbol{y}^{\mathrm{T}}.$$

Hence, we have that $\gcd(\boldsymbol{z}) = c \cdot \gcd(\boldsymbol{y})$, since any common divisor of $\boldsymbol{y}$ is also one of $\boldsymbol{z}$. Then (12) follows, since

$$\gcd(\boldsymbol{y}, \boldsymbol{z}) = \gcd(\gcd(\boldsymbol{y}), \gcd(\boldsymbol{z})) = \gcd(\boldsymbol{y}).$$

If furthermore $UV = I_r$, then since $\boldsymbol{z} = \boldsymbol{x}$, we have

$$\gcd(\boldsymbol{y}) = \gcd(\boldsymbol{y}, \boldsymbol{x}) = \gcd(\gcd(\boldsymbol{x}), \gcd(\boldsymbol{y})) = \gcd(\boldsymbol{x}),$$

where the last equality holds since $\boldsymbol{y}^{\mathrm{T}} = U\boldsymbol{x}^{\mathrm{T}}$ by an integer matrix $U$. ■

*Proof of Part (b) of Lemma 8.* For the proof, we compute the GCD of $(a_1(k)/q, \ldots, a_r(k)/q)$. For simplicity, let us write $(a_1(k)/q, \ldots, a_r(k)/q)$ as $\boldsymbol{a}(k)/q$.

Recall first that $r = (q-1)/2$ and that $\boldsymbol{a}(k)^{\mathrm{T}} = (A_r)^r \boldsymbol{a}(k-(q-1))^{\mathrm{T}}$ by definition (7). Hence, we have

$$(\boldsymbol{a}(k)/q)^{\mathrm{T}} = \frac{1}{q}(A_r)^r \boldsymbol{a}(k-(q-1))^{\mathrm{T}}.$$

Also recall that for proving the part (a) of Lemma 8, we indeed proved that $(A_r)^r/q$ is an integer matrix. On the other hand, we can show (Claim 12) that $q(A_r)^{-r}$ is also an integer matrix. Then since

$$q(A_r)^{-r} \cdot \frac{1}{q}(A_r)^r \;=\; I_r,$$

by Lemma 11, we have

$$\gcd(\boldsymbol{a}(k)/q) = \gcd(\boldsymbol{a}(k-(q-1))).$$

■

**Claim 12:** $q(A_r)^{-r}$ is an integer matrix.

*Proof.* We denote the adjugate matrix of a matrix $A$ by $\mathrm{Adj}(A)$. By Cramer's rule, we have

$$q(A_r)^{-r} = \left(\frac{1}{q}(A_r)^r\right)^{-1} = \frac{\mathrm{Adj}(\frac{1}{q}(A_r)^r)}{\det(\frac{1}{q}(A_r)^r)} = \frac{\mathrm{Adj}(\frac{1}{q}(A_r)^r)}{(\det A_r)^r/q^r}.$$

Note that $\mathrm{Adj}(\frac{1}{q}(A_r)^r)$ is an integer matrix, since $\frac{1}{q}(A_r)^r$ is an integer matrix and every cofactor of the matrix is also an integer. Then for the claim it suffices to show that $\det(A_r) = q$.

We show that $\det(A_r) = q$ by induction on $r$. For the case $r = 2$, we have

$$\det(A_2) = \begin{vmatrix} 2 & 1 \\ 1 & 3 \end{vmatrix} = 5,$$

and for the case $r = 3$, we have

$$\det(A_3) = \begin{vmatrix} 2 & 1 & 0 \\ 1 & 2 & 1 \\ 0 & 1 & 3 \end{vmatrix} = 7.$$

Now for the induction step, consider any $r > 4$. By using the cofactor expansion along the 1st row, we get

$$\begin{aligned}
&\det(A_r) \\
&= \begin{vmatrix} 2 & 1 & & & & & \\ 1 & 2 & 1 & & & & \\ & 1 & 2 & 1 & & & \\ & & \ddots & \ddots & \ddots & & \\ & & & 1 & 2 & 1 & \\ & & & & 1 & 3 \end{vmatrix} \\
&= 2 \begin{vmatrix} 2 & 1 & & & & \\ 1 & 2 & 1 & & & \\ & \ddots & \ddots & \ddots & & \\ & & 1 & 2 & 1 & \\ & & & 1 & 3 \end{vmatrix} - \begin{vmatrix} 1 & 1 & & & & & \\ & 2 & 1 & & & & \\ & 1 & 2 & 1 & & & \\ & & \ddots & \ddots & \ddots & & \\ & & & 1 & 2 & 1 & \\ & & & & 1 & 3 \end{vmatrix} \\
&= 2\det(A_{r-1}) - \det(A_{r-2}).
\end{aligned}$$

The last equation follows from the cofactor expansion along the 1st column. By the induction hypothesis, we have

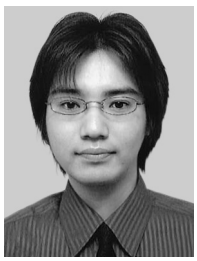
$$\det(A_r) = 2\det(A_{r-1}) - \det(A_{r-2}) = 2(q-2) - (q-4) = q.$$

Hence $\det(A_r) = q$ for every integer $q$. ■

#### References

[1] T. Gowers, "A new proof of Szemerédi's theorem for arithmetic progressions of length four," Geometric and Functional Analysis, vol.8, no.3, pp.529–551, 1998.
[2] T. Gowers, "A new proof of Szemerédi's theorem," Geometric and Functional Analysis, vol.11, no.3, pp.465–588, 2001.
[3] A. Samorodnitsky, "Low degree tests at large distances," Proc. 39th Annual ACM Symposium on Theory of Computing, pp.506–515, 2007.
[4] A. Samorodnitsky and L. Trevisan, "Gowers uniformity, influence of variables, and PCPs," Proc. 38th Annual ACM Symposium on Theory of Computing, pp.11–20, 2006.
[5] A. Bogdanov, "Pseudorandom generators for low degree polynomials," Proc. 37th Annual ACM Symposium on Theory of Computing, pp.21–30, 2005.
[6] A. Bogdanov and E. Viola, "Pseudorandom bits for polynomial," 48th Annual IEEE Symposium on Foundations of Computer Science, pp.41–51, 2007.

[7] E. Viola and A. Wigderson, "Norms, XOR Lemmas, and lower bounds for polynomials and protocols," Theory of Computing, vol.4, no.1, pp.137–168, 2008.
[8] H. Hatami and S. Lovett, "Higher-order Fourier analysis of $\mathbb{F}_p^n$ and the complexity of systems of linear forms," Tech. Rep. TR10-181, Electronic Colloquium on Computational Complexity, 2010.
[9] B. Green and T. Tao, "The distribution of polynomials over finite fields, with applications to the Gowers norms," Contributions to Discrete Mathematics, vol.4, no.2, pp.1–36, 2009.
[10] A. Bogdanov, A. Kawachi, and H. Tanaka, "Hard functions for low-degree polynomials over prime fields," Proc. 36th International Symposium on Mathematical Foundations of Computer Science, pp.120–131, 2011.



**Akinori Kawachi** is an assistant professor of Department of Mathematical and Computing Sciences, Tokyo Institute of Technology. Received B.E., M.Info., and Ph.D. degrees from Kyoto University in 2000, 2002, and 2004, respectively. His research interests are computational complexity, quantum computing, and foundations of cryptography.

**Hidetoki Tanaka** is a Ph.D. student of Department of Mathematical and Computing Sciences, Tokyo Institute of Technology. Received B.E. from Ritsumeikan University in 2007 and M.Sc. from Tokyo Institute of Technology in 2009. His research interests are computational complexity and GPU computing. Members of EATCS, and LA.

**Osamu Watanabe** received in 1980 B.Sc., in 1982 M.Sc., and Dr. of Engineering in 1986, all from Tokyo Institute of Technology. Presently, he is with Tokyo Institute of Technology, a Professor at Department of Information and Computing Sciences. His current interests are randomness in computation, design and analysis of randomized algorithms, and computational complexity. Members of IPSJ (fellow), EATCS, and LA.