Hard Functions for Low-degree Polynomials over Prime Fields

Andrej Bogdanov, Department of Computer Science and Engineering and Institute for Theoretical Computer Science and Communications, Chinese University of Hong Kong
Akinori Kawachi, Department of Mathematical and Computing Sciences, Graduate School of Information Science and Engineering, Tokyo Institute of Technology
Hidetoki Tanaka, Department of Mathematical and Computing Sciences, Graduate School of Information Science and Engineering, Tokyo Institute of Technology

In this paper, we present a new hardness amplification for low-degree polynomials over *prime fields*, namely, we prove that if some function is mildly hard to approximate by any low-degree polynomials then the sum of independent copies of the function is very hard to approximate by them. This result generalizes the XOR lemma for low-degree polynomials over the binary field given by Viola and Wigderson [VW08]. The main technical contribution is the analysis of the Gowers norm over prime fields. For the analysis, we discuss a generalized low-degree test, which we call the *Gowers test*, for polynomials over prime fields, which is a natural generalization of that over the binary field given by Alon, Kaufman, Krivelevich, Litsyn and Ron [AKK$^+$03]. This Gowers test provides a new technique to analyze the Gowers norm over prime fields. Actually, the rejection probability of the Gowers test can be analyzed in the framework of Kaufman and Sudan [KS08]. However, our analysis is self-contained and quantitatively better. By using our argument, we also prove the hardness of modulo functions for low-degree polynomials over prime fields.

Categories and Subject Descriptors: F.1.3 [**Computation by Abstract Devices**]: Complexity Measures and Classes

General Terms: Theory, Algorithms

Additional Key Words and Phrases: Hardness Amplification, Low-Degree Polynomials, Property Testing

ACM Reference Format:
Andrej Bogdanov, Akinori Kawachi, and Hidetoki Tanaka, 2013. Hard Functions for Low-degree Polynomials over Prime Fields. ACM 0, 0, Article 0 (2013), 15 pages.
DOI = 10.1145/0000000.0000000 http://doi.acm.org/10.1145/0000000.0000000

1. INTRODUCTION

Hardness amplification [Yao82] is a method for turning a function that is somewhat hard to compute into one that is very hard to compute against a given class of adversaries. The existence of many objects in average-case complexity and cryptography, such as hard on average NP problems and one-way functions, rely on unproven assumptions. In many cases, hardness amplification allows us to prove that if weakly hard versions of such objects exist, then strongly hard ones exist as well.

In settings where complexity lower bounds are known, applications of hardness amplification are not so common. Nevertheless, the method can sometimes be used to turn unconditional weak lower bounds into strong ones. Viola and Wigderson [VW08] showed an XOR lemma that amplifies the hardness of functions $f : \mathbb{F}_2^n \to \mathbb{F}_2$ against

A. Bogdanov is supported by grants RGC GRF CUHK410309 and CUHK410111. A. Kawachi is supported in part by KAKENHI No. 24106009 and 21300002.
Permission to make digital or hard copies of part or all of this work for personal or classroom use is granted without fee provided that copies are not made or distributed for profit or commercial advantage and that copies show this notice on the first page or initial screen of a display along with the full citation. Copyrights for components of this work owned by others than ACM must be honored. Abstracting with credit is permitted. To copy otherwise, to republish, to post on servers, to redistribute to lists, or to use any component of this work in other works requires prior specific permission and/or a fee. Permissions may be requested from Publications Dept., ACM, Inc., 2 Penn Plaza, Suite 701, New York, NY 10121-0701 USA, fax +1 (212) 869-0481, or permissions@acm.org.
© 2013 ACM 0000-0000/2013/-ART0 $10.00
DOI 10.1145/0000000.0000000 http://doi.acm.org/10.1145/0000000.0000000

low-degree polynomials over finite fields. There are many examples of weakly hard functions for this class of adversaries. The result of Viola and Wigderson allows us to turn these into functions of related complexity that are very hard to approximate (in terms of approximation accuracy) by polynomials of the same degree. Specifically, they take a function f that disagrees with every degree-d polynomial on a noticeable fraction of inputs and use it to construct a function f' such that no low-degree polynomial can noticeably outperform a constant function in predicting the value of f' at a random point.

Low-degree polynomials are fundamental objects in theoretical computer science, with applications in error-correcting codes, circuit complexity, probabilistically checkable proofs, and so on [Raz87; Smo87; BFL91; GLR$^+$91; FGL$^+$96]. In some cases results about polynomials over $\mathbb{F}_2$ can be easily extended to other finite fields, but in other cases different ideas are required for binary and non-binary fields. However, applications often require the use of polynomials over fields larger than $\mathbb{F}_2$.

For example, the "quadraticity test" of Gowers was first analyzed at large distances by Green and Tao [GT08] over non-binary fields. The extension over $\mathbb{F}_2$ by Samorodnitsky [Sam07] required additional ideas. In the other direction, Alon, Kaufman, Krivelevich, Litsyn and Ron [AKK$^+$03] gave an analysis of a low-degree test at small distances over $\mathbb{F}_2$. Kaufman and Ron [KR06] introduced substantial new ideas to generalize this test to other fields.

In this work, we generalize the XOR lemma of Viola and Wigderson [VW08] to arbitrary prime fields. Let $\mathbb{F}_q$ be a finite field of prime order q (identified with $\{0, ..., q-1\}$) and let $\delta(f, g) = \Pr_x[f(x) \neq g(x)]$ be the distance between f and g. In particular, we define $\delta_d(f) = \min_{p \text{ of degree } d} \delta(f, p)$, that is the distance between f and its nearest degree-d polynomial $p : \mathbb{F}_q^n \to \mathbb{F}_q$. (See Section 2 for precise definitions.) We then prove the following.

THEOREM 1.1. *Let q be any prime number, $t > 0$ be any integer, and $f : \mathbb{F}_q^n \to \mathbb{F}_q$ be any function. Let $f^{+t} : (\mathbb{F}_q^n)^t \to \mathbb{F}_q$ be the sum over $\mathbb{F}_q$ of t independent copies of f, namely, $f^{+t}(x_1, ..., x_t) = \sum_{i=1}^t f(x_i)$. If $\delta_d(f) \geq \frac{q}{(d+1)2^{d+1}}$,*

$$\delta_d\left(f^{+t}\right) > \frac{q-1}{q} - \frac{q-1}{q} \exp\left(-\frac{3t}{q^2(d+1)2^{2d+3}}\right).$$

Otherwise,

$$\delta_d\left(f^{+t}\right) > \frac{q-1}{q} - \frac{q-1}{q} \exp\left(-\frac{3t\delta_d(f)}{q^3 2^{d+2}}\right).$$

Since $\delta_d(f) \leq \delta_0(f) \leq (q-1)/q$, Theorem 1.1 allows us to construct functions that are arbitrarily close to having optimal hardness against degree-d polynomials over $\mathbb{F}_q$, by choosing $t = t(d, q, \varepsilon, \delta_d(f))$ sufficiently large. Specializing Theorem 1.1 to the case $q = 2$, we recover Theorem 1.2 of Viola and Wigderson.

Applying our argument, we show that addition modulo m is very hard to approximate by polynomials of degree d for every m coprime to q:

THEOREM 1.2. *Let $d \geq 0$ be any integer, q be any prime and m be any integer coprime to q, where $m < q$. Define $\mathsf{MOD}_m : \mathbb{F}_q^n \to \mathbb{Z}_m$ as $\mathsf{MOD}_m(x_1, ..., x_n) := x_1 + x_2 + \cdots + x_n \mod m$, where $+$ is the addition over $\mathbb{Z}$. Then, for every degree-d polynomial p,*

$$\delta(\mathsf{MOD}_m, p \bmod m) > \frac{m-1}{m} - \frac{m-1}{m} \exp\left(-\frac{1}{m^2 q} \cdot \left(\frac{q-1}{q}\right)^{d+1} \cdot \frac{n}{2^{d+2}}\right),$$

where $\delta(\mathsf{MOD}_m, p \bmod m) = \Pr_x[\mathsf{MOD}_m(x) \neq p(x) \bmod m]$.

Since $\delta(\mathsf{MOD}_m, c) \leq (m-1)/m$ for some constant c, this bound is asymptotically tight in m.

Hardness of modulo functions for low-degree polynomials for different settings of parameters has been studied in several works [AB01; Bou05; GRS05; Cha06; VW08]. Directly applying our hardness amplification to a function $f(x) = x \bmod m$, we would prove the hardness of another modulo function defined as $(x_1 \bmod m) + (x_2 \bmod m) + \cdots + (x_n \bmod m)$ over $\mathbb{F}_q^n$, similarly to Theorem 1.2. However, we then need an additional analysis for $\delta_d(f)$ to apply Theorem 1.1.

Our proof. We generalize the proof of Viola and Wigderson [VW08] over $\mathbb{F}_2$. Their argument makes use of the *Gowers d-norm* $\|\cdot\|_{U^d}$ [Gow98; Gow01] (see Section 2 for the definition). Starting from a function $f : \mathbb{F}_2^n \to \mathbb{F}_2$ that is mildly far from degree-d polynomials over $\mathbb{F}_2$, Viola and Wigderson reason as follows: (1) From the low-degree tests analysis of Alon et al. [AKK+03], we know that if f is mildly far from degree-d polynomials, then $\|(-1)^f\|_{U^{d+1}}$ is bounded away from one. (2) By the multiplicativity of the Gowers norm, $\|(-1)^{f^{+t}}\|_{U^{d+1}} = \|(-1)^f\|_{U^{d+1}}^t$, so $\|(-1)^{f^{+t}}\|_{U^{d+1}}$ is close to zero for t sufficiently large. (3) For any polynomial p of degree d, we have $\|(-1)^{f^{+t}-p}\|_{U^1} \leq \|(-1)^{f^{+t}}\|_{U^{d+1}}^{2^{d+1}}$ by a property of the Gowers norm, which is also close to zero from step (2). So $\|(-1)^{f^{+t}-p}\|_{U^1}$ must be close to zero as well. The last quantity simply measures the correlation between f^{+t} and p, so p must be far from all degree-d polynomials over $\mathbb{F}_2$.

Step (2) of this analysis extends easily to prime fields; step (3) requires some additional but standard technical tools (see Lemmas 4.2 and 4.3). However, step (1) relies on the analysis of the low-degree test of Alon et al., which was designed specifically for the binary field. Our main technical contribution is the extension of the analysis for this test (in fact, a slight variant of it) to arbitrary prime fields, described in Section 3. We believe that our presentation of this test is also simpler and more modular.

The test, which we call the Gowers test, works as follows: Given a function $f\colon \mathbb{F}_q^n \to \mathbb{F}_q$, choose a random set of points $x, y_1, \ldots, y_{d+1} \in \mathbb{F}_q^n$, and query f at all inputs of the form $x + a_1 y_1 + \cdots + a_{d+1} y_{d+1}$, where $(a_1, \ldots, a_{d+1})$ ranges over $\{0,1\}^{d+1}$. If the evaluations are consistent with a degree-d polynomial accept, otherwise reject. For two functions f, g, f is called δ-far from g if $\Pr_x[f(x) \neq g(x)] \geq \delta$. We show that if f is δ-far from every degree-d polynomial, then the Gowers test performs 2^{d+1} queries and rejects f with probability $\min\{\delta/q, 1/(d+1)2^{d+1}\}$ (See Theorem 3.2).

The Gowers test is a generalization for prime fields $\mathbb{F}_q$ of the low-degree test of Alon et al. over $\mathbb{F}_2$.[1] In analyses of [VW08] and ours, the distance of f from low-degree polynomials required in step (1) is obtained from the rejection probability of these tests. Alon et al. essentially showed their test performs 2^{d+1} queries and rejects f with $\Omega(\min\{2^d\delta, 1/(d2^d)\})$. Alon et al.'s test thus provides a better rejection probability than the Gowers test over $\mathbb{F}_2^n$ if δ is small. Since the hardness amplification is analyzed by the rejection probability of the tests, their test provides better hardness amplification than that of the Gowers test in the case $q = 2$.

Let us call the collection of queries $\{x + a_1 y_1 + \cdots + a_{d+1} y_{d+1}\colon (a_1, \ldots, a_{d+1}) \in \{0,1\}^{d+1}\}$ a *subcube* of $\mathbb{F}_q^n$. In the case $q = 2$, something special happens: With high probability, a subcube of $\mathbb{F}_q^n$ coincides with a rank $d+1$ affine subspace of $\mathbb{F}_q^n$. This fact plays a crucial property in the analysis of Bhattacharyya et al. [BKS+10], who obtain

[1] The original test of Alon et al. was actually for polynomials p evaluating 0 on the all-zero vector, i.e., $p(0, ..., 0) = 0$, but it can be naturally extended to a test for general polynomials.

tight lower bounds (within a constant factor) on the rejection probability of the Gowers test over $\mathbb{F}_2$.

The low-degree test of Kaufman and Ron [KR06] over general fields also works by choosing a random affine subspace of appropriate dimension and checking that the restriction of f on this space is a polynomial of degree d. Their work suggests that the proper way to generalize the Gowers test to larger fields is by viewing it as a random subspace test, and not a random subcube test. However, we do not see how the Kaufman-Ron test can be used to argue hardness amplification. Unlike the Gowers test, their test does not seem to be naturally related to the Gowers norm or any other measure on functions that is multiplicative and bounds the correlation with degree-d polynomials, and so we cannot proceed with steps (2) and (3) of the Viola-Wigderson argument. Jutla, Patthak, Rudra, and Zuckerman [JPRZ09] also proposed another low-degree test over prime fields, which can be viewed as a kind of random subspace tests. From a similar reason, we cannot apply their test to our analysis.

The Gowers test has higher query complexity than the Kaufman-Ron test.[2] However, its rejection probability is closely related to the Gowers norm over $\mathbb{F}_q$ (see Lemma 4.3), and we can conclude the proof.

Our analysis of the Gowers test is a generalization of the linearity test analysis of Blum, Luby, and Rubinfeld [BLR93]. Given a function $f\colon \mathbb{F}_q^n \to \mathbb{F}_q$ that the test accepts with high probability, they define a function $g\colon \mathbb{F}_q^n \to \mathbb{F}_q$ that is close to f, and then they argue that g must be linear. The linearity of g is proved using a self-reducibility argument, which relates evaluations of g at arbitrary inputs to evaluations at random inputs, where the identity $g(x) + g(y) = g(x + y)$ holds with high probability.

We proceed along the same lines: Given f, we define a function g that is close to f, and then argue that g must be a degree-d polynomial. To argue the second part, we use a self-reducibility argument that relates evaluations of g at arbitrary subcubes to evaluations at random subcubes. The main technical tool in the self-reduction argument is Claim 3.5, which to the best of our knowledge is a new identity about discrete derivatives in finite fields.

A statement similar to Theorem 3.2 can be derived by specializing the results of Kaufman and Sudan [KS08] on testing linear-invariant properties. Their result, which uses only generic properties of linear-invariant functions, implies the existence of a test that performs 2^{d+1} queries and rejects a function that is δ-far from all degree-d polynomials with probability $\min\{\delta/2, 1/((2^{d+2}+1)(2^{d+1}-1))\}$. In the case when δ is a constant independent of d, which is of interest in our application, their analysis gives a rejection probability of about $1/4^d$, while our analysis which relies on specific properties of polynomials improves the rejection probability to $1/d2^d$.

The reason why we assume prime fields in our results is that the characterization of polynomials used in the Gowers test makes sense only over prime fields (Theorem 2.3). We need to discover a new characterization of polynomials over non-prime fields connected to the Gowers norm for further generalization.

2. PRELIMINARIES

Notions and notation. We begin with basic notions and notation. Let q be a prime number. We denote by $\mathbb{F}_q$, a finite field of prime order q, identified with the set $\mathbb{Z}_q := \{0, ..., q-1\}$. Let $\mathbb{F}_q^*$ be a set of non-zero elements in $\mathbb{F}_q$, namely, $\mathbb{F}_q \setminus \{0\}$. First, we define multivariate polynomials over $\mathbb{F}_q$.

[2]The Kaufman-Ron test makes q^ℓ queries, where $\ell = \lceil (d+1)/(q - q/p) \rceil$ and $q = p^k$ for a prime p and integer k. Recently Haramaty, Shpilka, and Sudan [HSS11] gave a test with q^ℓ queries and optimal (up to constant factor) rejection probability of $\min\{\Omega(\delta_d(f)q^\ell), \Omega(1)\}$.

Definition 2.1 (*polynomial*). For an n-variate function $f : \mathbb{F}_q^n \to \mathbb{F}_q$ and an integer $d \geq 0$, if f can be written as

$$f(x) = \sum_{\alpha \in \mathbb{F}_q^n, \sum_{i=1}^n \alpha_i \leq d} C_\alpha \prod_{j=1}^n x_j^{\alpha_j},$$

where each $C_\alpha \in \mathbb{F}_q$, then we call f a degree-d polynomial.

For multivariate polynomials over prime fields $\mathbb{F}_q$, the so-called directional derivatives can be defined for well-known characterization of polynomials over $\mathbb{F}_q$.

Definition 2.2 (*directional derivative*). Let G, H be any additive groups. For a function $f : G \to H$ and an element $y \in G$, a derivative of f on y, denoted by $\Delta_y f$, is defined as

$$\Delta_y f(x) := f(x + y) - f(x).$$

A k-th derivative of f on vectors $y_1, \ldots, y_k \in G$ is recursively defined such that

$$\Delta_{y_1,\ldots,y_k} f(x) := \Delta_{y_1,\ldots,y_{k-1}} \left(\Delta_{y_k} f(x)\right).$$

The well-known characterization of degree-d polynomials over prime fields $\mathbb{F}_q$ with $(d+1)$-th derivatives is given by the following (folklore) theorem[3]. The Gowers test is derived from this characterization as shown in Section 3.

THEOREM 2.3 (CHARACTERIZATION OF POLYNOMIALS). *For a function $f : \mathbb{F}_q^n \to \mathbb{F}_q$, $\Delta_{y_1,\ldots,y_{d+1}} f(x) = 0$ for any $x, y_1, \ldots, y_{d+1} \in \mathbb{F}_q^n$ if and only if f is a degree-d polynomial.*

PROOF. We first prove the "if" part by a simple induction on d. When $d = 0$, it is obvious. Suppose that d-th derivatives of degree-$(d-1)$ polynomials on any d vectors are identical to zero. Since $\Delta_{y_1,\ldots,y_{d+1}} f = \Delta_{y_1,\ldots,y_d}(\Delta_{y_{d+1}} f))$, it suffices to show $\Delta_y f$ has degree $d-1$ for any degree-d polynomial f and any $y \in \mathbb{F}_q^n$. By linearity, we can assume f is a monomial as $f(x_1, ..., x_n) := \prod_{i=1}^n x_i^{d_i}$ without loss of generality. Then, we have $\Delta_y f(x) = f(x + y) - f(x) = \prod_{i=1}^n (x_i + y_i)^{d_i} - \prod_{i=1}^n x_i^{d_i}$. Since the term $\prod_{i=1}^n x_i^{d_i}$ of the maximum degree d is cancelled out in the righthand side, $\Delta_y f(x)$ has degree at most $d - 1$.

We next prove the "only if" part also by induction on d . Noting that the initial case $d = 0$ is trivial, we now assume the claim holds for d and suppose that $\Delta_{y_1,\ldots,y_{d+1}} f(x) = 0$. Therefore

$$\Delta_{y_1,\ldots,y_d}(\Delta_{y_{d+1}} f)(x) = 0.$$

By the inductive assumption, $\Delta_y f$ is a degree-$(d-1)$ polynomial g_y for every $y \in \mathbb{F}_q^n$. We have that

$$f(x + y) - f(x) = g_y(x)$$

for every x and y. Let e_i be the vector with 1 in coordinate i and 0 elsewhere. Let $y_{<i} = (y_1, \ldots, y_{i-1}, 0, \ldots, 0)$. Then by telescoping

$$f(y) - f(0) = \sum_{i=1}^n \big(f(y_{<i} + y_i e_i) - f(y_{<i})\big) = \sum_{i=1}^n \sum_{k=1}^{y_i} g_{e_i}(y_{<i} + k e_i)$$

[3]A proof of Theorem 2.3 appears in, e.g., Terence Tao's Weblog [Tao08].

since the underlying field has a prime order. We show $\sum_{k=1}^{y_i} g_{e_i}(y_{<i} + ke_i)$ has degree at most d for any degree-$(d-1)$ polynomial g_{e_i}. It suffices to consider the case that g_{e_i} is a monomial, namely, $g_{e_i}(y_1, ..., y_n) := \prod_{j=1}^{d_j} y_j^{d_j}$. In this case, we have

$$\sum_{k=1}^{y_i} g_{e_i}(y_{<i} + ke_i) = \prod_{j=1}^{i-1} y_{<i,j}^{d_j} \left(\sum_{k=1}^{y_i} k^{d_i} \right).$$

Since $\sum_{k=1}^{y_i} k^{d_i}$ is a polynomial of degree at most d_i+1 in y_i, the degree of $\sum_{k=1}^{y_i} g_{e_i}(y_{<i}+ ke_i)$ is at most $d+1$. □

Note that the characterization of Theorem 2.3 for degree-d polynomials does not hold over non-prime fields in general.

The distance is one of the central notions of this paper, which is formally defined as follows.

Definition 2.4 (*distance*). For functions $f, g : G \to H$, the distance between f and g is defined as $\delta(f, g) := \Pr_{x \in G}[f(x) \neq g(x)]$. The distance between a function f and the set of all the degree-d polynomials is defined as $\delta_d(f) := \min_{p \in \mathcal{P}_{d,n}} \delta(f, p)$, where $\mathcal{P}_{d,n}$ is the set of all degree-d n-variate polynomials.

Gowers uniformity. The Gowers norm is a measure for correlation between functions and low-degree polynomials over finite fields. This measure was originally introduced by Gowers [Gow98; Gow01] to give an alternative proof of Szemerédi's theorem. In this paper, we use a variant of the Gowers norm for technical convenience. We call it the Gowers uniformity here.

Definition 2.5. For every function $f : \mathbb{F}_q^n \to \mathbb{F}_q$ and every integer $k \geq 0$, the degree-k Gowers uniformity $U_k(f)$ is defined as

$$U_k(f) := \mathop{\mathbb{E}}_{x, y_1, ..., y_k \in \mathbb{F}_q^n} \left[\omega_q^{\Delta_{y_1, ..., y_k} f(x)} \right],$$

where $\omega_q := \exp(2\pi i/q)$ and $\mathbb{E}[\cdot]$ is the expectation.

Let $f : \mathbb{F}_q^n \to \{\omega_q^a\}_{a \in \{0,...,q-1\}}$. Then, we can represent f as $f(x) := \omega_q^{2\pi i g(x)}$ for some function $g : \mathbb{F}_q^n \to \mathbb{F}_q$. The original degree-$k$ Gowers norm $\|f\|_{U^k}$ of f is defined by $\|f\|_{U^k} := (U_k(g))^{1/2^k}$. Our target is the functions of range $\mathbb{F}_q$ rather than those of range $\{\omega_q^a\}_{a \in \{0,...,q-1\}}$ and the test for such functions. So, it is necessary to modify the original Gowers norm to fit the definition to such functions.

Equivalently, we can define the Gowers uniformity inductively. For a function $f : \mathbb{F}_q^n \to \mathbb{F}_q$ and a vector $y \in \mathbb{F}_q^n$, let $T^y f$ be a shift of f on y such that $T^y f(x) = f(x + y)$. Then, we define

$$U_0(f) := \mathop{\mathbb{E}}_{x \in \mathbb{F}_q^n} \left[\omega_q^{f(x)} \right], \quad U_1(f) := \left| \mathop{\mathbb{E}}_{x \in \mathbb{F}_q^n} \left[\omega_q^{f(x)} \right] \right|^2,$$
$$U_k(f) := \mathop{\mathbb{E}}_{y \in \mathbb{F}_q^n} [U_{k-1}(T^y f - f)] \quad \text{for } k \geq 2. \tag{1}$$

The equivalence between two definitions of the Gowers uniformity can be easily verified from the relation $\mathbb{E}_{y_k}[U_{k-1}(T^{y_k} f - f)] = \mathbb{E}_{x, y_1, ..., y_{k-1}, y_k}[\omega_q^{\Delta_{x, y_1, ..., y_{k-1}} \{f(x+y_k) - f(x)\}}] = \mathbb{E}_{x, y_1, ..., y_{k-1}, y_k}[\omega_q^{\Delta_{x, y_1, ..., y_{k-1}, y_k} f(x)}] = U_k(f)$.

Remark 2.6. If $k \geq 1$, the degree-k Gowers uniformity $U_k(f)$ is a non-negative real number, namely $U_k(f) = |U_k(f)|$.

The Gowers uniformity has the following important properties.

PROPOSITION 2.7. *For any function $f : \mathbb{F}_q^n \to \mathbb{F}_q$, the following statements hold:*

(1) $|U_k(f)| \leq \sqrt{U_{k+1}(f)}$ *for any integer* $k \geq 0$
(2) $U_{d+1}(f - p) = U_{d+1}(f)$ *for any degree-*d *polynomial* $p : \mathbb{F}_q^n \to \mathbb{F}_q$
(3) $U_k(f^{+t}) = (U_k(f))^t$ *for any integers* $k \geq 0$ *and* $t > 0$,

where $f^{+t} : \left(\mathbb{F}_q^n\right)^t \to \mathbb{F}_q$ *is the sum of* t *independent copies of* f *defined as*

$$f^{+t}(x^{(1)}, \ldots, x^{(t)}) := f(x^{(1)}) + f(x^{(2)}) + \cdots + f(x^{(t)})$$

for an integer $t > 0$.

These properties can be shown by arguments used in [Gow98; Gow01] for the Gowers norm, and thus we omit proofs of them.

3. GOWERS TEST

Next, we consider a low-degree test for polynomials, which we call the Gowers test. The Gowers test is derived from the characterization of polynomials given in Theorem 2.3.

Definition 3.1 (*Gowers test*). The degree-d Gowers test for a function $f : \mathbb{F}_q^n \to \mathbb{F}_q$, denoted by $\mathsf{GT}_d(f)$, is the following procedure:

(1) Pick $x, y_1, \ldots, y_{d+1} \in \mathbb{F}_q^n$ uniformly and independently at random;
(2) Accept if and only if $\Delta_{y_1,\ldots,y_{d+1}} f(x) = 0$.

We denote by $\rho_d(f)$ the rejection probability of $\mathsf{GT}_d(f)$.

By Theorem 2.3, if f has degree at most d, $\mathsf{GT}_d(f)$ accepts with probability 1. Our question is how large the rejection probability is in the case when f is not a degree-d polynomial. An answer to this question is given in the following theorem, which estimates the rejection probability $\rho_d(f)$ of the Gowers test $\mathsf{GT}_d(f)$.

THEOREM 3.2. *Let f be any function $\mathbb{F}_q^n \to \mathbb{F}_q$. Then*

$$\rho_d(f) \geq \min\left\{\frac{\delta_d(f)}{q}, \frac{1}{(d+1)2^{d+1}}\right\}.$$

PROOF. The proof is immediately obtained from the following main lemma:

LEMMA 3.3. *Let $f : \mathbb{F}_q^n \to \mathbb{F}_q$ and $\epsilon < \frac{1}{(d+1)2^{d+1}}$. If $\rho_d(f) \leq \epsilon$, then $\delta_d(f) \leq q\epsilon$.*

From Lemma 3.3, Theorem 3.2 can be proven as follows. If $\rho_d(f) \geq 1/(d+1)2^{d+1}$, we are done. So, assume that $\rho_d(f) < 1/(d+1)2^{d+1}$. Let $\epsilon := \rho_d(f)$. By Lemma 3.3, $\delta_d(f) \leq q\epsilon = q\rho_d(f)$. Then we obtain $\rho_d(f) \geq \delta_d(f)/q$. Hence, the theorem follows.

Now, we prove the main lemma.

PROOF OF LEMMA 3.3. Our proof of this lemma is a generalization of the linearity test analysis of Blum, Luby, and Rubinfeld [BLR93], using ideas from the work of Alon et al. [AKK+03] on higher degree polynomials over $\mathbb{F}_2$. Namely, we construct a function g such that

(1). $g(x) = 0$ for all but at most $q\epsilon$ fraction of inputs x and
(2). $g(x) - f(x)$ is a degree-d polynomial.

We define

$$g(x) = \text{the plurality value of } \Delta_{y_1,\ldots,y_{d+1}} f(x), \text{ where } y_1,\ldots,y_{d+1} \in \mathbb{F}_q^n,$$

where if the plurality value is not unique, we define $g(x)$ as an arbitrary value from the plurality ones. Property (1) is almost immediate: If $g(x) \neq 0$, it follows that $\Pr_{y_1,\ldots,y_{d+1}}[\Delta_{y_1,\ldots,y_{d+1}} f(x) \neq 0] \geq 1/q$, so if $g(x) \neq 0$ for more than a $q\epsilon$ fraction of xs, it would follow that the Gowers test rejects with probability more than $(q\epsilon)/q = \epsilon$, a contradiction.

We now prove property (2). We begin by showing that for *all* x, $g(x)$ not only agrees with the plurality value of $\Delta_{y_1,\ldots,y_{d+1}} f(x)$, but in fact with a vast majority:

CLAIM 3.4. *For all* $x \in \mathbb{F}_q^n$, $\Pr_{y_1,\ldots,y_{d+1}}[g(x) = \Delta_{y_1,\ldots,y_{d+1}} f(x)] \geq 1 - (d+1)\epsilon$.

PROOF OF CLAIM 3.4. First note that we use shorthand notation $\Delta_{\mathbf{y}} f = \Delta_{y_1,\ldots,y_{d+1}} f$ for $\mathbf{y} = (y_1,\ldots,y_{d+1}) \in (\mathbb{F}_q^n)^{d+1}$. Fix x and let $\mathbf{y} = (y_1,\ldots,y_{d+1})$ and $\mathbf{z} = (z_1,\ldots,z_{d+1})$ be independent random $(d+1)$-tuples of random points in $\mathbb{F}_q^n$. Then

$$\begin{aligned}\Pr[\Delta_{\mathbf{y}} f(x) = \Delta_{\mathbf{z}} f(x)] &= \sum_{t \in \mathbb{F}_q} \Pr[\Delta_{\mathbf{y}} f(x) = \Delta_{\mathbf{z}} f(x) = t] \\ &= \sum_{t \in \mathbb{F}_q} \Pr[\Delta_{\mathbf{y}} f(x) = t]^2 \leq \max_{t \in \mathbb{F}_q} \Pr[\Delta_{\mathbf{y}} f(x) = t] = \Pr[\Delta_{\mathbf{y}} f(x) = g(x)]\end{aligned}$$

so it is sufficient to show that $\Pr[\Delta_{\mathbf{y}} f(x) = \Delta_{\mathbf{z}} f(x)] \geq 1 - (d+1)\epsilon$, or $\Pr[\Delta_{\mathbf{y}} f(x) \neq \Delta_{\mathbf{z}} f(x)] \leq (d+1)\epsilon$. To do so, we define the hybrid distributions $\mathbf{w}_0,\ldots,\mathbf{w}_{d+1}$, where $\mathbf{w}_i = (z_1,\ldots,z_i,y_{i+1},\ldots,y_{d+1})$ and $\mathbf{w}_0 = (y_1,\ldots,y_{d+1})$. Then

$$\begin{aligned}\Pr[\Delta_{\mathbf{y}} f(x) \neq \Delta_{\mathbf{z}} f(x)] &= \Pr[\exists i, 1 \leq i \leq d+1 \colon \Delta_{\mathbf{w}_{i-1}} f(x) \neq \Delta_{\mathbf{w}_i} f(x)] \\ &\leq \sum_{i=1}^{d+1} \Pr[\Delta_{\mathbf{w}_{i-1}} f(x) \neq \Delta_{\mathbf{w}_i} f(x)] = (d+1) \cdot \Pr[\Delta_{\mathbf{w}_0} f(x) \neq \Delta_{\mathbf{w}_1} f(x)]\end{aligned}$$

The last equality follows from the symmetry of the derivatives; that is, for every i:

$$\begin{aligned}\Pr[\Delta_{z_1,\ldots,z_{i-1},z_i,y_{i+1},\ldots,y_{d+1}} f(x) &= \Delta_{z_1,\ldots,z_{i-1},y_i,y_{i+1},\ldots,y_{d+1}} f(x)] \\ &= \Pr[\Delta_{z_i,z_1,\ldots,z_{i-1},y_{i+1},\ldots,y_{d+1}} f(x) = \Delta_{y_i,z_1,\ldots,z_{i-1},y_{i+1},\ldots,y_{d+1}} f(x)] \\ &= \Pr[\Delta_{z_1,z_2,\ldots,z_{d+1}} f(x) = \Delta_{y_1,z_2,\ldots,z_{d+1}} f(x)].\end{aligned}$$

It remains to show that $\Pr[\Delta_{\mathbf{w}_0} f(x) \neq \Delta_{\mathbf{w}_1} f(x)] \leq \epsilon$:

$$\begin{aligned}\Pr[\Delta_{\mathbf{w}_0} f(x) \neq \Delta_{\mathbf{w}_1} f(x)] &= \Pr[\Delta_{y_1,y_2,\ldots,y_{d+1}} f(x) \neq \Delta_{z_1,y_2,\ldots,y_{d+1}} f(x)] \\ &= \Pr[\Delta_{y_1,y_2,\ldots,y_{d+1}} f(x) - \Delta_{z_1,y_2,\ldots,y_{d+1}} f(x) \neq 0] \\ &= \Pr[\Delta_{y_2,\ldots,y_{d+1}} f(x+y_1) - \Delta_{y_2,\ldots,y_{d+1}} f(x+z_1) \neq 0] \\ &= \Pr[\Delta_{y_1-z_1,y_2,\ldots,y_{d+1}} f(x+z_1) \neq 0] \\ &= \Pr_{x',\mathbf{y}'}[\Delta_{\mathbf{y}'} f(x') \neq 0] = \epsilon.\end{aligned}$$

□

We will also make use of the following identity. For $a \in \{0,1\}^{d+1}$, let $|a| = a_1 + \cdots + a_{d+1}$.

CLAIM 3.5. *For all* $x, y_1, \ldots, y_{d+1}, z_1, \ldots, z_{d+1} \in \mathbb{F}_q^n$,

$$\Delta_{z_1,\ldots,z_{d+1}} f(x) = \sum_{a \in \{0,1\}^{d+1}} (-1)^{|a|} \Delta_{y_1 - a_1 z_1, \ldots, y_{d+1} - a_{d+1} z_{d+1}} f\left(x + \sum_{i=1}^{d+1} a_i z_i\right).$$

PROOF OF CLAIM 3.5. By induction on d. For $d = 1$, a calculation shows that

$$\Delta_{z_1} f(x) = \Delta_{y_1} f(x) - \Delta_{y_1 - z_1} f(x + z_1). \tag{2}$$

The inductive step is obtained by iterating this identity. Suppose that we know the identity holds for $d-1$, namely

$$\Delta_{z_2,\ldots,z_{d+1}} f(x) = \sum_{a \in \{0,1\}^{d+1}} (-1)^{|a|} \Delta_{y_2 - a_2 z_2, \ldots, y_{d+1} - a_{d+1} z_{d+1}} f\left(x + \sum_{i=2}^{d+1} a_i z_i\right).$$

Applying (2) to the function $\Delta_{z_2,\ldots,z_{d+1}} f$ we have

$$\Delta_{z_1,\ldots,z_{d+1}} f(x) = \Delta_{y_1} \Delta_{z_2,\ldots,z_{d+1}} f(x) - \Delta_{y_1 - z_1} \Delta_{z_2,\ldots,z_{d+1}} f(x + z_1).$$

Using the inductive hypothesis on $\Delta_{z_2,\ldots,z_{d+1}} f$ and linearity of derivatives, we obtain the desired formula. □

We are now in a position to prove that $g - f$ is a polynomial of degree d. By Claim 3.4, we have that

$$\Pr_{y_1,\ldots,y_{d+1}}\left[g\left(x + \sum_{i=1}^{d+1} a_i z_i\right) \neq \Delta_{y_1 - a_1 z_1, \ldots, y_{d+1} - a_{d+1} z_{d+1}} f\left(x + \sum_{i=1}^{d+1} a_i z_i\right)\right] \leq (d+1)\epsilon$$

for all $x, z_1, \ldots, z_{d+1} \in \mathbb{F}_q^n$, and $a \in \{0,1\}^{d+1}$. Taking a union bound over all $a \in \{0,1\}^{d+1}$ it follows that

$$\Pr_{y_1,\ldots,y_{d+1}}\left[\exists a \colon g\left(x + \sum_{i=1}^{d+1} a_i z_i\right) \neq \Delta_{y_1 - a_1 z_1, \ldots, y_{d+1} - a_{d+1} z_{d+1}} f\left(x + \sum_{i=1}^{d+1} a_i z_i\right)\right]$$
$$\leq 2^{d+1} \cdot (d+1)\epsilon < 1.$$

Therefore, there must exist values for $y_1, \ldots, y_{d+1}$ such that

$$g\left(x + \sum_{i=1}^{d+1} a_i z_i\right) = \Delta_{y_1 - a_1 z_1, \ldots, y_{d+1} - a_{d+1} z_{d+1}} f\left(x + \sum_{i=1}^{d+1} a_i z_i\right)$$

for all $x, z_1, \ldots, z_{d+1}$ in $\mathbb{F}_q^n$ and $a \in \{0,1\}^{d+1}$. But then by Claim 3.5,

$$\begin{aligned}
\Delta_{z_1,\ldots,z_{d+1}} g(x) &= \sum_{a \in \{0,1\}^{d+1}} (-1)^{|a|} g\left(x + \sum_{i=1}^{d+1} a_i z_i\right) \\
&= \sum_{a \in \{0,1\}^{d+1}} (-1)^{|a|} \Delta_{y_1 - a_1 z_1, \ldots, y_{d+1} - a_{d+1} z_{d+1}} f\left(x + \sum_{i=1}^{d+1} a_i z_i\right) \\
&= \Delta_{z_1,\ldots,z_{d+1}} f(x),
\end{aligned}$$

and so $\Delta_{z_1,\ldots,z_{d+1}}(f - g)(x) = 0$ for all $x, z_1, \ldots, z_{d+1}$, namely, $f - g$ is a degree-d polynomial. Therefore, Lemma 3.3 follows.

Remark 3.6. Lemma 4.5 in [TZ08] provides a similar result to Lemma 3.3. This lemma shows if $\rho_d(f)$ approaches to 0 then f also approaches to some degree-$(d-1)$ polynomial, as Lemma 3.3 claims. The main difference between their lemma and ours is precise estimation for distance to degree-$(d-1)$ polynomials. For our purpose, we need to estimate how close f is to such polynomials with the parameters n, d, and q, but this lemma only guarantees that the distance converges to 0 as ε approaches to 0.

4. HARDNESS AMPLIFICATION

Our goal is to construct a hard function for low-degree polynomials (in other words, a function far from low-degree polynomials) from a mildly hard function for low-degree polynomials (in other words, a function mildly far from low-degree polynomials). Recall that, for a function $f : \mathbb{F}_q^n \to \mathbb{F}_q$ and an integer $t > 0$, a function $f^{+t} : (\mathbb{F}_q^n)^t \to \mathbb{F}_q$ is defined as

$$f^{+t}(x^{(1)}, \ldots, x^{(t)}) := f(x^{(1)}) + f(x^{(2)}) + \cdots + f(x^{(t)}).$$

We prove that f^{+t} is very hard for low-degree polynomials if f is mildly hard for low-degree polynomials. Recall that $\delta_d(f) \leq \frac{q-1}{q}$ for any function f. Hence our goal is to prove $\delta_d(f^{+t}) \geq \frac{q-1}{q} - \epsilon$ for some small ϵ.

THEOREM 4.1. *Let f be any function and $t > 0$ be any integer. Then*

$$\delta_d\left(f^{+t}\right) > \frac{q-1}{q} - \frac{q-1}{q} \exp\left(-\frac{3t}{q^2 \cdot 2^{d+2}} \cdot \rho_d(f)\right).$$

Note that our main theorem (Theorem 1.1) in Section 1 immediately follows from this theorem and the lower bound of the rejection probability of the Gowers test (Theorem 3.2).

PROOF. We first state two lemmas on relations between the distance from degree-d polynomials and the Gowers uniformity and between the Gowers uniformity and the rejection probability of the Gowers test.

LEMMA 4.2 (DISTANCE TO UNIFORMITY). *For any function $f : \mathbb{F}_q^n \to \mathbb{F}_q$ and any integer d,*

$$\delta_d(f) \geq \frac{q-1}{q} - \frac{q-1}{q} \mathop{\mathbb{E}}_{a \in \mathbb{F}_q^*} \left[(U_{d+1}(af))^{1/2^{d+2}}\right].$$

LEMMA 4.3 (UNIFORMITY TO TEST). *For any function $f : \mathbb{F}_q^n \to \mathbb{F}_q$ and any integer $d \geq 0$,*

$$U_{d+1}(f) < 1 - \frac{3}{q^2}\rho_d(f).$$

(Recall that $\rho_d(f)$ is the rejection probability of the Gowers test $\mathsf{GT}_d(f)$.)

We first assume that these lemmas hold in order to prove Theorem 4.1. (The proofs of these lemmas are given later.)

Note that the distance $\delta_d(f)$ is lower bounded by $\frac{q-1}{q}$ minus the term involved with $\mathbb{E}_{a \in \mathbb{F}_q^*}\left[(U_{d+1}(af))^{1/2^{d+2}}\right]$ in Lemma 4.2. One can easily see that the expectation is not required in the binary case, as in [VW08]. Hence, our analysis needs some technical tricks for the general case.

We can prove Theorem 4.1 using these two lemmas, Proposition 2.7 and Theorem 3.2. By Lemma 4.2 and the averaging principle, there is an $\alpha \in \mathbb{F}_q^*$ such that

$$\delta_d(f^{+t}) \geq \frac{q-1}{q} - \frac{q-1}{q}\left(U_{d+1}(\alpha f^{+t})\right)^{1/2^{d+2}}.$$

By the property of the Gowers uniformity (Proposition 2.7 (3)),

$$\left(U_{d+1}(\alpha f^{+t})\right)^{1/2^{d+2}} = \left(U_{d+1}(\alpha f)\right)^{t/2^{d+2}}.$$

Then, by Lemma 4.3,

$$\left(U_{d+1}(\alpha f)\right)^{t/2^{d+2}} < \left(1 - \frac{3}{q^2}\rho_d(f)\right)^{t/2^{d+2}} < \exp\left(-\frac{3}{q^2}\cdot\frac{t}{2^{d+2}}\rho_d(f)\right).$$

Note that $\rho_d(\alpha f) = \rho_d(f)$ since $\Delta_{y_1,\ldots,y_{d+1}}(\alpha f(x)) = 0$ if and only if $\Delta_{y_1,\ldots,y_{d+1}} f(x) = 0$, for all $x, y_1, \ldots, y_{d+1} \in \mathbb{F}_q$ and all $\alpha \in \mathbb{F}_q^*$. Therefore

$$\delta_d\left(f^{+t}\right) > \frac{q-1}{q} - \frac{q-1}{q}\exp\left(-\frac{3t}{q^2\cdot 2^{d+2}}\cdot\rho_d(f)\right).$$

Therefore, Theorem 4.1 follows if Lemmas 4.2 and 4.3 hold. We finally prove these lemmas below.

PROOF OF LEMMA 4.2. Let p be a degree-d polynomial satisfying $\delta_d(f) = \delta(f,p)$. By Proposition 2.7, for all $a \in \mathbb{F}_q^*$

$$U_1\left(a(f-p)\right) = U_1(af - ap) \leq \left(U_{d+1}(af-ap)\right)^{1/2^{d+1}} = \left(U_{d+1}(af)\right)^{1/2^{d+1}}$$

since ap is a degree-d polynomial. Hence

$$\mathop{\mathbb{E}}_{a\in\mathbb{F}_q^*}\left[\left(U_{d+1}(af)\right)^{1/2^{d+2}}\right] \geq \mathop{\mathbb{E}}_{a\in\mathbb{F}_q^*}\left[\left(U_1\left(a(f-p)\right)\right)^{1/2}\right].$$

Now we provide a lower bound of $\mathbb{E}_{a\in\mathbb{F}_q^*}\left[\left(U_1\left(a(f-p)\right)\right)^{1/2}\right]$.

By the definition and the triangle inequality,

$$\begin{aligned}
&\mathop{\mathbb{E}}_{a\in\mathbb{F}_q^*}\left[\left(U_1\left(a(f-p)\right)\right)^{1/2}\right] \\
&= \mathop{\mathbb{E}}_{a\in\mathbb{F}_q^*}\left|\mathop{\mathbb{E}}_{x\in\mathbb{F}_q^n}\left[\omega_q^{a(f(x)-p(x))}\right]\right| = \frac{1}{q-1}\sum_{a=1}^{q-1}\left|\sum_{j=0}^{q-1}\omega_q^{aj}\Pr_x\left[f(x)-p(x)=j\right]\right| \\
&\geq \frac{1}{q-1}\left|\sum_{a=1}^{q-1}\sum_{j=0}^{q-1}\omega_q^{aj}\Pr_x\left[f(x)-p(x)=j\right]\right| \\
&= \frac{1}{q-1}\left|\sum_{a=1}^{q-1}\omega_q^{0}\Pr_x\left[f(x)-p(x)=0\right] + \sum_{a=1}^{q-1}\sum_{j=1}^{q-1}\omega_q^{aj}\Pr_x\left[f(x)-p(x)=j\right]\right|.
\end{aligned}$$

The first term is

$$\sum_{a=1}^{q-1}\omega_q^0\Pr_x\left[f(x)-p(x)=0\right] = (q-1)\Pr_x\left[f(x)=p(x)\right] = q-1-(q-1)\delta_d(f).$$

The second term is

$$\sum_{a=1}^{q-1}\sum_{j=1}^{q-1}\omega_q^{aj}\Pr_x\left[f(x)-p(x)=j\right]=\sum_{j=1}^{q-1}\Pr_x\left[f(x)-p(x)=j\right]\sum_{a=1}^{q-1}\omega_q^{aj}$$
$$=-\sum_{j=1}^{q-1}\Pr_x\left[f(x)-p(x)=j\right]=-\delta_d(f)$$

since $\sum_{a=1}^{q-1}\omega_q^{aj}=-1$ if $j\in\mathbb{F}_q^*$. Hence

$$\mathop{\mathbb{E}}_{a\in\mathbb{F}_q^*}\left[\left(U_1\left(a(f-p)\right)\right)^{1/2}\right]\geq\frac{1}{q-1}\left|q-1-q\delta_d(f)\right|$$
$$=\left|1-\frac{q}{q-1}\delta_d(f)\right|\geq 1-\frac{q}{q-1}\delta_d(f).$$

The last inequality is derived from the reverse triangle inequality.

Therefore

$$\delta_d(f)\geq\frac{q-1}{q}-\frac{q-1}{q}\mathop{\mathbb{E}}_{a\in\mathbb{F}_q^*}\left[\left(U_1\left(a(f-p)\right)\right)^{1/2}\right]$$
$$\geq\frac{q-1}{q}-\frac{q-1}{q}\mathop{\mathbb{E}}_{a\in\mathbb{F}_q^*}\left[\left(U_{d+1}(af)\right)^{1/2^{d+2}}\right].$$

□

PROOF OF LEMMA 4.3. From the definition,

$$U_{d+1}(f)=\mathop{\mathbb{E}}_{x,y_1,\ldots,y_{d+1}}\left[\omega_q^{\Delta_{y_1,\ldots,y_{d+1}}f(x)}\right]=\sum_{j=0}^{q-1}\omega_q^j\Pr_{x,y_1,\ldots,y_{d+1}}\left[\Delta_{y_1,\ldots,y_{d+1}}f(x)=j\right]$$
$$=\Pr_{x,y_1,\ldots,y_{d+1}}\left[\Delta_{y_1,\ldots,y_{d+1}}f(x)=0\right]+\sum_{j=1}^{q-1}\omega_q^j\Pr_{x,y_1,\ldots,y_{d+1}}\left[\Delta_{y_1,\ldots,y_{d+1}}f(x)=j\right].$$

Now, we have $\mathrm{Im}(U_{d+1}(f))=i\sum_{j=1}^{q-1}\sin\left(\frac{2\pi j}{q}\right)\Pr\left[\Delta_{y_1,\ldots,y_{d+1}}f(x)=j\right]=0$ since the Gowers uniformity $U_{d+1}(f)$ is a real number. So, recalling that $\rho_d(f)=\Pr_{x,y_1,\ldots,y_{d+1}}\left[\Delta_{y_1,\ldots,y_{d+1}}f(x)\neq 0\right]$,

$$U_{d+1}(f)=1-\rho_d(f)+\sum_{j=1}^{q-1}\cos\left(\frac{2\pi j}{q}\right)\Pr_{x,y_1,\ldots,y_{d+1}}\left[\Delta_{y_1,\ldots,y_{d+1}}f(x)=j\right]$$
$$\leq 1-\rho_d(f)+\cos\left(\frac{2\pi}{q}\right)\sum_{j=1}^{q-1}\Pr_{x,y_1,\ldots,y_{d+1}}\left[\Delta_{y_1,\ldots,y_{d+1}}f(x)=j\right]$$
$$=1-\rho_d(f)+\cos\left(\frac{2\pi}{q}\right)\rho_d(f)$$
$$<1-\frac{3}{q^2}\rho_d(f).$$

□

Thus, the proof of Theorem 4.1 is completed.

5. HARDNESS OF MOD_M

Let m, n be integers, and let q be a prime. The function $\mathsf{MOD}_m : \mathbb{F}_q^n \to \mathbb{Z}_m$ is defined as

$$\mathsf{MOD}_m(x) := x_1 + x_2 + \cdots + x_n \mod m,$$

where $1 < m < q$ and $+$ is the addition over $\mathbb{Z}$. In this section, we estimate the distance between MOD_m and low-degree polynomials.

Since the range of MOD_m is $\mathbb{Z}_m$, we define the distance δ_d between MOD_m and degree-d polynomials as follows:

$$\delta_d(\mathsf{MOD}_m) := \min_{p \in \mathcal{P}_{d,n}} \Pr_{x \in \mathbb{F}_q^n}[\mathsf{MOD}_m(x) \neq (p(x) \bmod m)].$$

Namely, we identify a standard polynomial (from $\mathbb{F}_q^n$ to $\mathbb{F}_q$) modulo m as a polynomial from $\mathbb{F}_q^n$ to $\mathbb{Z}_m$ here. Also, we modify the definition of the Gowers uniformity $U_d(f)$ for such functions $f : \mathbb{F}_q^n \to \mathbb{Z}_m$:

$$U_d(f) := \mathop{\mathbb{E}}_{x, y_1, \ldots, y_d \in \mathbb{F}_q^n} \left[\omega_m^{\Delta_{y_1, \ldots, y_d} f(x)} \right]. \tag{3}$$

It is easy to see the same properties given in Proposition 2.7 hold for this definition as before.

We prove the hardness of MOD_m for low-degree polynomials in the following theorem.

THEOREM 5.1. *Let $d \geq 0$ be any integer, q be any prime, and m be any integer coprime to q, where $m < q$. Then,*

$$\delta_d(\mathsf{MOD}_m) > \frac{m-1}{m} - \frac{m-1}{m} \exp\left(-\frac{1}{m^2 q} \cdot \left(\frac{q-1}{q} \right)^{d+1} \cdot \frac{n}{2^{d+2}} \right).$$

PROOF. By the almost same proof as that of Lemma 4.2, we have, for $\mathsf{MOD}_m : \mathbb{F}_q^n \to \mathbb{Z}_m$ and any integer d,

$$\delta_d(\mathsf{MOD}_m) \geq \frac{m-1}{m} - \frac{m-1}{m} \mathop{\mathbb{E}}_{a \in \mathbb{F}_q^*} \left[\left(U_{d+1}(a\mathsf{MOD}_m) \right)^{1/2^{d+2}} \right].$$

Therefore, from the averaging argument, there is an $\alpha \in \mathbb{F}_q^*$ such that

$$\delta_d(\mathsf{MOD}_m) \geq \frac{m-1}{m} - \frac{m-1}{m} \left(U_{d+1}(\alpha\mathsf{MOD}_m) \right)^{1/2^{d+2}}.$$

Let $f : \mathbb{F}_q \to \mathbb{Z}_m$ be the 1-variable function defined by $f(x) = x \bmod m$. Then, we have $U_{d+1}(\alpha\mathsf{MOD}_m)^{1/2^{d+2}} = U_{d+1}(\alpha f)^{n/2^{d+2}}$ since the same properties as those in Proposition 2.7 hold even for the Gowers uniformity of Equation (3) , as stated above. So, we now estimate an upper bound of $U_{d+1}(\alpha f)$ by using the following claim.

CLAIM 5.2. *For any function f, the following properties hold:*

1. *If $y_i = 0$ for some i, then $\omega_m^{\Delta_{y_1, \ldots, y_{d+1}} f} \equiv 1$.*
2. *If ω_m^f is not a constant function and $y_i \neq 0$ for all i, then $\omega_m^{\Delta_{y_1, \ldots, y_{d+1}} f}$ is not a constant function.*

PROOF. We first show property 1. By the symmetry of derivatives, we can suppose that $y_{d+1} = 0$ without loss of generality. Then, for any x,

$$\Delta_{y_1, \ldots, y_d, y_{d+1}} f(x) = \Delta_{y_1, \ldots, y_d} \left(f(x+0) - f(x) \right) = 0.$$

Thus, $\omega_m^{\Delta_{y_1,\ldots,y_{d+1}} f(x)} = 1$ for any x.

We next prove property 2. We show the following statement: "If ω_m^f is not a constant, then $\omega_m^{\Delta_y f}$ is not a constant function for every nonzero $y \in \mathbb{F}_q^*$." Repeatedly applying this statement, we obtain property 2.

We prove its contrapositive. Suppose $\omega_m^{\Delta_y f(x)}$ is a constant function for some nonzero $y \in \mathbb{F}_q$. Then it must be that for every $x \in \mathbb{F}_q$:

$$f((x+y) \bmod q) - f(x \bmod q) \equiv c \mod m.$$

Plugging in $x := x+y, x+2y, \ldots, x+(q-1)y$, we obtain

$$\begin{aligned} f((x+2y) \bmod q) - f((x+y) \bmod q) &\equiv c \mod m, \\ f((x+3y) \bmod q) - f((x+2y) \bmod q) &\equiv c \mod m, \\ &\vdots \\ f((x+qy) \bmod q) - f((x+(q-1)y) \bmod q) &\equiv c \mod m. \end{aligned}$$

If we add these equations, on the left hand side we obtain zero, and on the right hand side we obtain $qc \mod m$, which equals zero only if $c = 0$. If $c = 0$, then f is a constant function since we have $\Delta_y f(x) \equiv 0 \bmod m$. □

By Claim 5.2, we have for some nonzero $0 < \alpha' < m$

$$\begin{aligned} &\mathop{\mathbb{E}}_{x,y_1,\ldots,y_{d+1}} \left[\omega_m^{\alpha \Delta_{x,y_1,\ldots,y_{d+1}} f(x)} \right] \\ &\leq \frac{1}{q^{d+2}} \left\{ \left(q^{d+2} - (q-1)^{d+1} \cdot q\right) \cdot 1 + (q-1)^{d+1} \left| (q-1) \cdot 1 + \omega_m^{\alpha'} \right| \right\} \\ &< 1 - \frac{1}{m^2 q} \left(\frac{q-1}{q} \right)^{d+1}. \end{aligned}$$

From this estimation, the theorem immediately follows.

REFERENCES

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.

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.

László Babai, Lance Fortnow, and Carsten Lund. Non-deterministic exponential time has two-prover interactive protocols. *Computational Complexity*, 1(1):3–40, 1991.

Arnab Bhattacharyya, Swastik Kopparty, Grant Schoenebeck, Madhu Sudan, and David Zuckerman. Optimal testing of Reed-Muller codes. In *Proceedings of the 51st Annual IEEE Symposium on Foundations of Computer Science*, 2010.

Manuel Blum, Michael Luby, and Ronitt Rubinfeld. Self-testing/Correcting with Applications to Numerical Problems. *Journal of Computer and System Sciences*, (3):549–595, 1993.

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

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.

Uriel Feige, Shafi Goldwasser, László Lovász, Shmuel Safra, and Mario Szegedy. Interactive proofs and the hardness of approximating cliques. *Journal of the ACM*, 43(2):268–292, 1996.

Peter Gemmell, Richard J. Lipton, Ronitt Rubinfeld, Madhu Sudan, and Avi Wigderson. Self-testing/correcting for polynomials and for approximate functions. In *Proceedings of the 23th Annual ACM Symposium on Theory of Computing*, pages 32–42, 1991.

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

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

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.

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.

Elad Haramaty, Amir Shpilka, and Madhu Sudan. Optimal testing of multivariate polynomials over small prime fields. In *52nd Annual Symposium on Foundations of Computer Science*, pages 629–637, 2011.

Charanjit S. Jutla, Anindya C. Patthak, Atri Rudra, and David Zuckerman. Testing low-degree polynomials over prime fields. *Random Structures and Algorithms*, 35(2):163–193, 2009.

Tali Kaufman and Dana Ron. Testing polynomials over general fields. *SIAM Journal on Computing*, 36(3):779–802, 2006.

Tali Kaufman and Madhu Sudan. Algebraic property testing: the role of invariance. In *Proceedings of the 40th Annual ACM Symposium on Theory of Computing*, pages 403–412, 2008.

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.

Alex Samorodnitsky. Low degree tests at large distances. In *Proceedings of the 39th Annual ACM Symposium on Theory of Computing*, pages 506–515, 2007.

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.

Terence Tao. Some notes on non classical polynomials in finite characteristic, 2008.

Terence Tao and Tamar Ziegler. The inverse conjecture for the gowers norm over finite fields via the correspondence principle, 2008.

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

Andrew C.-C. Yao. Theory and applications of trapdoor functions (extended abstract). In *Proceedings of the 23rd Annual IEEE Symposium on Foundations of Computer Science*, pages 80–91, 1982.