Electronic Colloquium on Computational Complexity, Report No. 65 (2010)

Testing of exponentially large codes, by a new extension to Weil bound for character sums

Tali Kaufman [*]
The Weizmann Institute of Science
kaufmant@mit.edu

Shachar Lovett [†]
The Weizmann Institute of Science
shachar.lovett@weizmann.ac.il

April 13, 2010

Abstract

In this work we consider linear codes which are locally testable in a sublinear number of queries. We give the first general family of locally testable codes of exponential size. Previous results of this form were known only for codes of quasi-polynomial size (e.g. Reed-Muller codes). We accomplish this by showing that any affine invariant code $\mathcal{C}$ over $\mathbb{F}_{p^n}$ of size $p^{p^{\Omega(n)}}$ is locally testable using $poly(\log_p |\mathcal{C}|/n)$ queries. Previous general result for affine invariant codes were known only for sparse codes, i.e. codes of size $p^{O(n)}$. The main new ingredients used in our proof are a new extension of the Weil bound for character sums, and a Fourier-analytic approach for estimating the weight distribution of affine invariant codes.

[*] Research supported in part by a Koshland Fellowship.
[†] Research supported by the Israel Science Foundation (grant 1300/05).

ISSN 1433-8092

Contents

1 Introduction

We study in this work families of locally testable codes. Let $\mathbb{F}_N = \mathbb{F}_{p^n}$ be a finite field, where we think of p as either constant or small. A code is a family of functions $\mathcal{C} = \{f : \mathbb{F}_{p^n} \to \mathbb{F}_p\}$. All codes we consider in this work are linear[1]. The dimension of a code is $\dim(\mathcal{C}) = \log_p(|\mathcal{C}|)$.

A code is *locally testable* if there is a randomized algorithm, which when given as input a function $f : \mathbb{F}_{p^n} \to \mathbb{F}_p$, probes f in a small number of locations and determines (with high probability) whether $f \in \mathcal{C}$ or f is far[2] from all codewords of $\mathcal{C}$. A code is q-locally testable if the number of probes is at most q, where q is sublinear in the code length, i.e. $q = o(N)$.

Most of the study of locally testable codes has been focused on codes testable with constant query complexity (i.e. $q = O(1)$) or with poly-logarithmic query complexity (i.e. $q = (\log N)^{O(1)}$). They appear as low-degree tests in the $IP = PSPACE$, $MIP = NEXP$ and $PCP = NP$ theorems, and indeed the work of [15] (which was later partly derandomized by [8]) elucidates their role as the “combinatorial heart” of PCPs.

In general, there is a tradeoff between the rate of the code $\dim(\mathcal{C})/N$ and the query complexity of testing this code. A major open problem in this field is whether one can enjoy the best of both worlds: a code of constant rate which is locally testable with a constant query complexity.

One line of research focuses on constructing explicit codes which try to approach this optimal tradeoff. The best results to date are by Ben-Sasson and Sudan [6] and Dinur [13] (see also Meir [25]) which achieve an explicit binary code of rate $\frac{1}{(\log N)^{O(1)}}$ which is testable using a constant number of probes.

A second line of research focuses on characterization of general families of codes that are locally testable [9, 26, 1, 16, 19, 21, 17, 20, 14, 22]. Many results in this field apply only to *sparse* codes over binary fields $\mathbb{F}_{2^n}$, which are codes of dimension $O(\log N)$ [17, 20, 14, 22]. Another example is *Generalized Reed-Muller codes* which are the family of polynomials $f : \mathbb{F}_{p^n} \to \mathbb{F}_p$ of total degree at most d. These codes are testable using $p^{\frac{d}{p-1}} = exp(d)$ queries, while having dimension $O(n^d)$ [1, 16, 19]. Such codes can be locally testable with sublinear number of queries for $d \le O(\log n)$, which gives codes of quasi-logarithmic dimension $\dim(\mathcal{C}) \le (\log N)^{\log \log N}$.

Our work falls into the latter line of research. We exhibit a general family of codes of almost optimal dimension $\dim(\mathcal{C}) = N^{\Omega(1)}$ which are locally testable with sublinear query complexity. We achieve this by studying *affine invariant codes*. A code $\mathcal{C} = \{f : \mathbb{F}_{p^n} \to \mathbb{F}_p\}$ is affine invariant if it is invariant under affine transformation of the coordinates of input space. That is, if $f(x) \in \mathcal{C}$ then also $g(x) = f(ax + b) \in \mathcal{C}$ for any $a, b \in \mathbb{F}_{p^n}, a \neq 0$. Previous results [14] showed that sparse affine invariant codes (i.e., codes of size $p^{O(n)}$) are locally testable. We significantly extend this to codes of up to exponential size, i.e. of size at most $p^{p^{\Omega(n)}}$.

Theorem 1 (Main result)**.** *Let $\mathcal{C} = \{f : \mathbb{F}_{p^n} \to \mathbb{F}_p\}$ be a linear code which is affine invariant of dimension $\dim(\mathcal{C}) \le p^{\alpha n}$, where $\alpha > 0$ is an absolute constant. Then $\mathcal{C}$ is locally testable with query complexity $q = poly(\dim(\mathcal{C})/n) = o(p^n)$. In particular, any sparse affine invariant code (i.e. with $\dim(\mathcal{C}) = O(n)$) is locally testable with constant query complexity $q = O(1)$. The parameter α can be chosen to be any $\alpha < 1/32$ for large enough n.*

This generalizes previous works in several aspects: our result applies to codes of exponential size $exp(N^\alpha)$, while previous results apply only to codes of polynomial size $N^{O(1)}$ or quasi-polynomial

[1] A code $\mathcal{C} = \{f : \mathbb{F}_{p^n} \to \mathbb{F}_p\}$ is linear if for any $f(x), g(x) \in \mathcal{C}$ also $h(x) = \alpha f(x) + \beta g(x) \in \mathcal{C}$ where $\alpha, \beta \in \mathbb{F}_p$.

[2] If f has distance ϵ from $\mathcal{C}$, i.e. if $\min_{g \in \mathcal{C}} \Pr_{x \in \mathbb{F}_{p^n}}[f(x) \neq g(x)] = \epsilon$, we require the local test to reject f with probability at least $\Omega(\epsilon)$.

size $exp(\log N^{\log\log N})$. Previous results on sparse codes applied only to binary fields $\mathbb{F}_{2^n}$, while our result applies to any field of small characteristic. Note that a recent result of Ben-Sasson and Sudan [7, 27] shows that affine invariant codes that are testable with constant number of queries can not have exponential rate. Thus, our testing result of exponentially large codes can not be improved to testing with constant locality.

The main new ingredients in our work is a Fourier-analytic approach for estimating the weight distribution of affine invariant codes, and a new extension of the Weil bound for character sums of low-degree polynomials. We start by describing our new result for character sums for polynomials, and then discuss its relation to proving local testability of affine invariant codes. The proof of our new extension for the Weil bound relies on techniques borrowed from additive combinatorics. This demonstrates yet another connection between additive combinatorics and theoretical computer science. Such connections were used before to establish results regarding pseudorandom generators [10, 23, 28] and list-decoding of codes [18].

1.1 Character sums

Let $\mathbb{F}$ be a finite field. An additive character is a function $\chi : \mathbb{F} \to \mathbb{C}$ for which $\chi(x+y) = \chi(x)\chi(y)$ (and which is not the identically zero function). For example, if $\mathbb{F} = \mathbb{F}_q$ is a prime finite field then the additive characters are given by $\chi_a(x) = e^{\frac{2\pi i}{q}ax}$ for $a \in \mathbb{F}_q$. In the general case of $\mathbb{F} = \mathbb{F}_{p^n}$, the additive characters are given by $\chi_a(x) = e^{\frac{2\pi i}{p}\mathrm{Tr}(ax)}$, where $a \in \mathbb{F}_{p^n}$ and the Trace operator $\mathrm{Tr} : \mathbb{F}_{p^n} \to \mathbb{F}_p$ is defined as $\mathrm{Tr}(x) = \sum_{i=0}^{n-1} x^{p^i}$.

The Weil bound for character sums [29] is a general result regarding character sums of low-degree polynomials over a finite field $\mathbb{F}$. Let $f(x) \in \mathbb{F}[x]$ be a univariate polynomial of degree k. Let $\chi : \mathbb{F} \to \mathbb{C}$ be any additive character. Weil's bound states that either $\chi(f(x))$ is constant, or is distributed close to uniform when $x \in \mathbb{F}$ is uniformly chosen.

Theorem 2 (Weil bound [29])**.** *Let $f(x)$ be a univariate polynomial over $\mathbb{F}$ of degree $\leq |\mathbb{F}|^{1/2-\delta}$. Let $\chi : \mathbb{F} \to \mathbb{C}$ be any additive character. Then either $\chi(f(x))$ is constant for all $x \in \mathbb{F}$, or*

$$|\mathbb{E}_{x\in\mathbb{F}}[\chi(f(x))]| \leq |\mathbb{F}|^{-\delta}.$$

The Weil bound is very effective to polynomials of degree $k \ll \sqrt{|\mathbb{F}|}$, however it fails for polynomials of degree $k \geq \sqrt{|\mathbb{F}|}$. We establish a general result in fields of small characteristics $\mathbb{F}_{p^n}$ which allows to extend polynomials by a small number of monomials of larger degree, as long as they have small *weight degree.*

Definition 3 (Weight degree)**.** Let $t \in \{0, \dots, p^n - 1\}$. The weight degree of t is the hamming weight of the digits of t in base p. That is, let $t = \sum_{i=0}^{n-1} t_i p^i$ be the representation of t in base p, where $0 \leq t_i \leq p-1$. The weight degree of t is

$$\mathrm{wt}(t) = \sum_{i=0}^{n-1} t_i.$$

The weight degree of a monomial x^t is the weight degree of t, and the weight degree of a univariate polynomial $f(x)$ is the maximal weight degree of a monomial in it with a nonzero coefficient.

We prove the following extension of the Weil bound in case $f(x)$ is the sum of a low degree polynomial and a small number of monomials of bounded weight degree (but of arbitrary degree).

Theorem 4 (Extension of the Weil bound)**.** *Let $f(x) = g(x) + h(x)$ be a univariate polynomial over $\mathbb{F}_{p^n}$, where $g(x)$ is a polynomial of degree $\le |\mathbb{F}|^{1/2-\delta}$ and $h(x)$ is the sum of at most $k \ge 1$ monomials, each of weight degree at most d. Let $\chi : \mathbb{F}_{p^n} \to \mathbb{C}$ be an additive character. Then either $\chi(f(x))$ is constant for all $x \in \mathbb{F}_{p^n}$, or*

$$|\mathbb{E}_{x\in\mathbb{F}}[\chi(f(x))]| \le |\mathbb{F}_{p^n}|^{-\frac{\delta}{2d^2 2^d k}}.$$

Note that in order to get a meaningful bound, we need our parameters to obey $kd^2 2^d \le O(n)$. Note that for $d \le (1-\epsilon)\log_2(n)$ we may have $k = n^{O(1)}$. This can be compared to a relatively recent result of Bourgain [4] of a similar flavor. We state it below informally, as the exact formulation is somewhat complex, and we will not require it in the paper.

Theorem 5 (Bourgain's extension of Weil bound [4])**.** *Let $f(x) = g(x) + h(x)$ be a univariate polynomial over a prime finite field $\mathbb{F}_q$, where $g(x)$ is a polynomial of degree $\le |\mathbb{F}_q|^{1/2-\delta}$ and $h(x)$ is the sum of at most $k = O(1)$ monomials, each of degree at most $|\mathbb{F}_q|^{1-\epsilon}$. Let $\chi : \mathbb{F}_q \to \mathbb{C}$ be an additive character. Then either $\chi(f(x))$ is constant for all $x \in \mathbb{F}_q$, or*

$$\left|\mathbb{E}_{x\in\mathbb{F}_q}[\chi(f(x))]\right| \le |\mathbb{F}_q|^{-\Omega(1)}.$$

Comparing our result with the result of Bourgain, we note two important advantages of our work: first, we can handle non-prime finite fields; second, when $d \le O(\log n)$ is small enough, we may have $k = poly(n)$ monomials of high degree, while in the result of Bourgain one can take at most $k = O(1)$ such monomials. In contrast, the result of Bourgain does not assume a bound on the weight degree of the monomials. The two advantages of our work are crucial for the application to locally testing of exponentially large affine invariant codes. Bourgain's result was used in a similar fashion by Grigorescu, Kaufman and Sudan [14] to establish a similar result which holds only for sparse affine invariant codes, i.e. codes of polynomial size. Our new character sum result allows us to extend their techniques to handle exponentially large affine invariant codes.

1.2 Connection between character sums and affine invariant codes

Affine invariant codes can be characterized by trace codes. Let $S \subseteq \{0, \dots, p^n - 1\}$. The S-trace code over $\mathbb{F}_{p^n}$ is defined as the family of functions $f : \mathbb{F}_{p^n} \to \mathbb{F}_p$ given by

$$\mathcal{T}(S) = \left\{ \left(\mathrm{Tr}(\sum_{e\in S} a_e x^e) : F_{p^n} \to \mathbb{F}_p \right) : a_e \in \mathbb{F}_{p^n} \right\}.$$

where we recall that the Trace function $\mathrm{Tr} : \mathbb{F}_{p^n} \to \mathbb{F}_p$ is given by $\mathrm{Tr}(x) = \sum_{i=0}^{n-1} x^{p^i}$. For example, Generalized Reed-Muller codes $\mathrm{RM}(n, d)$, which are the family of functions $f : \mathbb{F}_p^n \to \mathbb{F}_p$ where f is an n-variate polynomial of total degree at most d, can be equivalently characterized as

$$\mathrm{RM}(n, d) = \mathcal{T}(\{e \in \{0, \dots, p^n - 1\} : \mathrm{wt}(e) \le d\}).$$

We define two important properties of trace codes.

Definition 6 (Shift closed)**.** Let $S \subseteq \{0, \dots, p^n - 1\}$. The set S is said to be *shift closed* if, for every $e \in S$, we also have that $ep^\ell \pmod{p^n} \in S$ for all $\ell = 1, \dots, n$.

The term *shift closed* comes from viewing elements $e \in S$ as vectors in $\mathbb{F}_p^n$, given by the representation of e in base p. In this case, $ep^\ell \pmod{p^n}$ corresponds to a cyclic shift of the vector by ℓ coordinates.

Definition 7 (Shadow closed)**.** Let $S \subseteq \{0, \ldots, p^n - 1\}$. The set S is said to be *shadow closed* if the following holds. For any $e \in S$, let $e = \sum_{i=0}^{n-1} e_i p^i$ be the representation of e in base p. Define the *support* of e to be the set of nonzero digits of e,

$$\text{support}(e) = \{0 \leq i \leq n-1 : e_i \neq 0\}.$$

Let e' be obtained from e by changing some of the non-zero digits of e, i.e.

$$e' = \sum_{i \in \text{support}(e)} e'_i p^i.$$

Then we should have that also $e' \in S$. That is, S is shadow closed if

$$\left\{ \sum_{i \in \text{support}(e)} e'_i p^i : e \in S, (e'_i)_{i \in \text{support}(e)} \in \mathbb{F}_p \right\} \subseteq S.$$

A set S is said to be *affine closed* if it is both shift closed and shadow closed. The following general result was established by Kafuman and Sudan [21]. They show that the class of affine invariant linear codes is equivalent to the class of trace codes of affine closed sets.

Theorem 8 (Monomial extraction [21])**.** *Let $\mathcal{C} = \{f : \mathbb{F}_{p^n} \to \mathbb{F}_p\}$ be an affine invariant linear code. Then there exists an affine closed set $S \subseteq \{0, \ldots, p^n - 1\}$ such that $\mathcal{C} = \mathcal{T}(S)$. Moreover, for any affine closed set S the code $\mathcal{T}(S)$ is linear and affine invariant.*

Thus, to study affine invariant codes, we need to study trace codes. We now introduce two notions. The dual of a code $\mathcal{C} = \{f : \mathbb{F}_{p^n} \to \mathbb{F}_p\}$ is defined as

$$\mathcal{C}^\perp = \left\{ (g : \mathbb{F}_{p^n} \to \mathbb{F}_p) : \sum_{x \in \mathbb{F}_{p^n}} f(x)g(x) = 0 \quad \forall f \in \mathcal{C} \right\}.$$

The *affine closure* of a function $g : \mathbb{F}_{p^n} \to \mathbb{F}_p$ is the set of functions obtained by applying affine transformations on the coordinates of the input space of f, that is

$$\overline{\text{affine}}(g) = \left\{ (g(ax+b) : \mathbb{F}_{p^n} \to \mathbb{F}_p) : a, b \in \mathbb{F}_{p^n} \right\}.$$

It is easy to verify that if $\mathcal{C}$ is an affine invariant code, and $g \in \mathcal{C}^\perp$, then in fact $\overline{\text{affine}}(g) \subseteq \mathcal{C}^\perp$. An important case is when in fact $\overline{\text{affine}}(g)$ spans the entire code $\mathcal{C}^\perp$.

Definition 9 (Single orbit property)**.** Let $g \in \mathcal{C}^\perp$. We say that $\mathcal{C}$ has the *single orbit property* for g if the affine closure of g is a spanning set for $\mathcal{C}^\perp$, that is if

$$\mathcal{C} = \text{Span}(\overline{\text{affine}}(g))^\perp.$$

We will shortly see that the single orbit property is tightly connected to locally testing properties of the code $\mathcal{C}$. First, define the *weight* of $g : \mathbb{F}_{p^n} \to \mathbb{F}_p$ to be the number of coordinates where g evaluates to a nonzero value,

$$\text{wt}(g) = |\{x \in \mathbb{F}_{p^n} : g(x) \neq 0\}|.$$

The following result was established by Kaufman and Sudan [21]. If $\mathcal{C}$ is an affine invariant code which has the single orbit property for a codeword $g \in \mathcal{C}^\perp$ of small weight, then $\mathcal{C}$ can be locally tested[3].

[3] In fact, the local test for $\mathcal{C}$ is performed by computing $\sum f(ax+b)g(x)$ for a small random subset of $a, b \in \mathbb{F}_{p^n}$. Note that to perform each such test, we only need to query $f(x)$ only on $x \in \mathbb{F}_{p^n}$ for which $g(x) \neq 0$.

Theorem 10 (Theorem 2.9 in [21]). *Let $\mathcal{C} = \{f : \mathbb{F}_{p^n} \to \mathbb{F}_p\}$ be a linear code which is affine invariant. Assume there exists $g \in \mathcal{C}^\perp$ such that $\mathcal{C}$ has the single orbit property for g. Then $\mathcal{C}$ can be locally tested with $O(\mathrm{wt}(g)^2)$ queries.*

Hence, to show that $\mathcal{C}$ can be locally tested, it is sufficient to demonstrate that $\mathcal{C}^\perp$ is spanned by the orbit of a short codeword under the affine group.

Let $\mathcal{C} = \mathcal{T}(S)$ for some affine closed set $S \subseteq \{0, \ldots, p^n - 1\}$. The dual code of $\mathcal{C}$ is a dual-trace code $d\mathcal{T}(S)$, which can be verified (Claim 15) to be

$$d\mathcal{T}(S) = \left\{ (f : \mathbb{F}_{p^n} \to \mathbb{F}_p) : \sum_{x \in \mathbb{F}_{p^n}} f(x) x^e = 0 \quad \forall e \in S \right\}.$$

We need to establish that there exists $f \in d\mathcal{T}(S)$ of small weight such that $\mathrm{Span}(\overline{\mathrm{affine}}(f)) = d\mathcal{T}(S)$. Assume that this is false, i.e. that $\mathrm{Span}(\overline{\mathrm{affine}}(f)) \subsetneq d\mathcal{T}(S)$. Using the fact that S is affine invariant, we show (Corollary 32) that in fact $f \in d\mathcal{T}(S \cup \{e\})$ where $e \in \{0, \ldots, p^n - 1\} \setminus S$ has small weight.

Hence, in order to conclude the proof, we will show that for a suitably chosen weight ℓ, there exist codewords on weight ℓ in $d\mathcal{T}(S)$ which are not in any of $d\mathcal{T}(S \cup \{e\})$ for any $e \notin S$ which has small weight.

The main tool we develop in order to do so, is a tight estimate on the number of codewords of weight ℓ in dual-trace codes. We show the following result.

Lemma (Lemma 25, informal statement). *Let $S \subseteq \{0, \ldots, p^n - 1\}$ be affine closed of size $|S| \le p^{\Omega(n)}$. Then there exists $\ell_{\min} = poly(|S|)$ and $\ell_{\max} = p^{\Omega(n)}$, such that for any $\ell_{\min} \le \ell \le \ell_{\max}$ the following holds. The number of codewords in $d\mathcal{T}(S)$ of weight exactly ℓ is given by*

$$\frac{C(p, \ell)}{\ell!} p^{n\ell - |S'|}(1 + o(1))$$

where $S' = \{e \in S : (p, e) = 1\}$ is the set of elements in S which are co-prime to p, and where $C(p, \ell)$ is given by

$$C(p, \ell) = \left| \left\{ (v_1, \ldots, v_\ell) \in (\mathbb{F}_p \setminus \{0\})^\ell : v_1 + \ldots + v_\ell = 0 \right\} \right|.$$

Similar results were previously obtained over binary fields $\mathbb{F}_{2^n}$ using properties of Krawtchouk polynomials [17, 20]. Our technique is different, and relies on methods from additive combinatorics and Fourier analysis. In particular it allows us to extend the result to arbitrary fields and allows to obtain bounds for a wider range of values of ℓ. The proof of this lemma relies on the new extension of the Weil bound we establish.

Given the lemma, the proof of Theorem 1 can be easily concluded. Recall that we showed that in order to prove local testability of an affine invariant code $\mathcal{T}(S)$, we need to show that there is a short codeword whose affine closure linearly spans $d\mathcal{T}(S)$. We showed that any $f \in d\mathcal{T}(S)$ for which this does not occur, is in fact contained in some $d\mathcal{T}(S \cup \{e\})$ for some $e \notin S$ of small weight. Thus, to conclude the proof we need to show that there exist small weight codewords in

$$d\mathcal{T}(S) \setminus \bigcup_{e \notin S : e \text{ has small weight}} d\mathcal{T}(S \cup \{e\}).$$

To this end we apply the tight bounds we obtain for the number of codewords of weight ℓ in dual-trace codes. We first show that if $\mathcal{C}$ is affine invariant of size $|\mathcal{C}| \le p^{p^{O(n)}}$ then in fact $\mathcal{C} = d\mathcal{T}(S)$

where S is affine invariant of size $|S| \leq p^{O(n)}$, so our estimates for the number of codewords apply for $d\mathcal{T}(S)$. Fix a suitable weight ℓ. The number of codewords of weight ℓ in $d\mathcal{T}(S)$ is given by

$$W_\ell = \frac{C(p,\ell)}{\ell!} p^{n(\ell - |S'|)}(1+o(1)),$$

where we recall that $S' = \{e \in S : (e,p) = 1\}$. On the other hand, as S is affine closed and $e \notin S$, we can bound the number of codewords of weight ℓ in any of the codes $d\mathcal{T}(S \cup \{e\})$ by

$$\leq \frac{C(p,\ell)}{\ell!} p^{n(\ell - |S'|-1)}(1+o(1)) \approx p^{-n} W_\ell.$$

Thus to conclude we just need to verify that the number of distinct e of small weight is $\ll p^n$. This then can be verified by a routine calculation.

1.3 New extension to the Weil bound

We sketch in high level how we achieve the new extension to the Weil bound. Let $f(x) = g(x)+h(x)$ be a univariate polynomial over $\mathbb{F}_{p^n}$, where $\deg(g) \leq |\mathbb{F}_{p^n}|^{1/2-\delta}$ and $h(x)$ is the sum of k monomials, each of weight degree at most d. We need to prove that either $\mathrm{Tr}(f) : \mathbb{F}_{p^n} \to \mathbb{F}_p$ is a constant function, or that it is highly unbiased (note that proving the result for the Trace operator implies it immediately for all additive characters).

The analysis divides into two cases: either g has high weight-degree $\mathrm{wt}(g) \geq d+1$, or g has low weight-degree $\mathrm{wt}(g) \leq d$. The first case is the easier one, and both cases rely on an analysis of directional derivatives of polynomials. The directional derivative of a polynomial $f(x)$ in direction $y \in \mathbb{F}_{p^n}$ is given by $f_y(x) = f(x+y) - f(x)$, and iterated derivatives are defined as $f_{y_1,\ldots,y_k}(x) = (f_{y_1,\ldots,y_{k-1}})_{y_k}(x)$.

The case of high weight g The first case, where $\mathrm{wt}(g) \geq d+1$ is easy to analyze by taking enough derivatives that eliminate $h(x)$, and reducing to a theorem of Deligne [12], which is a multivariate analog of Weil's bound. Specifically, For any $y_1, \ldots, y_{d+1}$ one can verify that since $\mathrm{wt}(h) \leq d$ then

$$h_{y_1,\ldots,y_{d+1}} \equiv 0,$$

hence $f_{y_1,\ldots,y_{d+1}} \equiv g_{y_1,\ldots,y_{d+1}}$. An iterated application of the Cauchy-Schwarz inequality yields that

$$\left| \mathbb{E}_{x \in \mathbb{F}_{p^n}} [\omega^{\mathrm{Tr}(f(x))}] \right|^{2^{d+1}} \leq \left| \mathbb{E}_{x,y_1,\ldots,y_{d+1} \in \mathbb{F}_{p^n}} [\omega^{\mathrm{Tr}(f_{y_1,\ldots,y_{d+1}}(x))}] \right|$$

where $\omega = e^{\frac{2\pi i}{p}}$. Hence to prove that $\mathrm{Tr}(f(x))$ in unbiased for uniform x, it is sufficient to prove that $\mathrm{Tr}(f_{y_1,\ldots,y_{d+1}}(x))$ is unbiased for uniform $x, y_1, \ldots, y_{d+1}$. We then verify that as g is of weight degree at least $d+1$, it is not eliminated by taking generic $d+1$ derivatives, and we get that $f_{y_1,\ldots,y_{d+1}}(x)$ is a nonzero polynomial in the variables $x, y_1, \ldots, y_{d+1}$ of total degree at most $\deg(g) \leq |\mathbb{F}_{p^n}|^{1/2-\delta}$. Moreover, we can prove that $\mathrm{Tr}(f_{y_1,\ldots,y_{d+1}}(x))$ is not a constant function; hence by Deligne's theorem we deduce that

$$\left| \mathbb{E}_{x,y_1,\ldots,y_{d+1} \in \mathbb{F}_{p^n}} [\omega^{\mathrm{Tr}(f_{y_1,\ldots,y_{d+1}}(x))}] \right| \leq |\mathbb{F}|^{-\delta}$$

and the bound on the bias of $\mathrm{Tr}(f(x))$ follows.

The case of low weight g The harder case is handling g of small weight $\mathrm{wt}(g) \leq d$, since h cannot simply be eliminated by taking enough iterated derivatives, without eliminating f altogether. We solve this problem by taking a smaller number of derivatives, such that f is not eliminated, but instead is transformed into a special class of polynomials (p-multilinear polynomials). We then proceed to study this family of polynomials, and are able to bound the bias of such polynomials, given that they came from a polynomial $f = g + h$ where g has low degree and h is the sum of a small number of low weight degree monomials. Most of the technical challenges of the proof are in this part.

1.4 Paper organization

We prove our main result, Theorem 1, on the local testing properties of affine invariant codes in Section 2. The proof uses our new extension to the Weil bound, which we prove in Section 3. Both sections are written in a self-contained manner, so that readers that are interested in the details of only one of these results can read only the relevant section. We note that throughout the paper we do not attempt to optimize constants.

2 Testing of affine invariant codes

We study affine invariant codes in this section. We begin with some definitions and stating our main theorem formally. We then proceed to prove some properties of affine invariant codes, and then apply those to prove our main result, Theorem 1.

2.1 Basic codes definitions

Let $\mathbb{F} = \mathbb{F}_{p^n}$ be a finite field. A code is a set of functions $\mathcal{C} = \{f : \mathbb{F}_{p^n} \to \mathbb{F}_p\}$. A code is called *linear* if it forms a linear space, i.e. if $f(x), g(x) \in \mathcal{C}$ then also $h(x) = \alpha f(x) + \beta g(x) \in \mathcal{C}$ where $\alpha, \beta \in \mathbb{F}_p$. We will only consider linear codes in this paper. For a linear code $\mathcal{C}$, its dual is the set functions which are normal to all codewords of $\mathcal{C}$.

Definition 11 (Dual code)**.** Let $\mathcal{C} = \{f : \mathbb{F}_p^n \to \mathbb{F}_p\}$ be some linear code over $\mathbb{F}_p$. The dual code $\mathcal{C}^\perp$ is defined as

$$\mathcal{C}^\perp = \left\{(g : \mathbb{F}_p^n \to \mathbb{F}_p) : \sum_{x \in \mathbb{F}_p^n} f(x)g(x) = 0 \quad \forall f \in \mathcal{C}\right\}.$$

Note that the dual of the dual is the original code, i.e. $(\mathcal{C}^\perp)^\perp = \mathcal{C}$. We next define the weight and support of a codeword.

Definition 12 (Weight and support of codeword)**.** The *support* of a codeword $f : \mathbb{F}_p^n \to \mathbb{F}_p$ is the set of $x \in \mathbb{F}_p^n$ for which $f(x) \neq 0$,

$$\mathrm{support}(f) = \{x \in \mathbb{F}_{p^n} : f(x) \neq 0\}.$$

The *weight* of a codeword is the size of its support,

$$\mathrm{wt}(f) = |\mathrm{support}(f)| = |\{x \in \mathbb{F}_{p^n} : f(x) \neq 0\}|.$$

2.2 Trace codes

Definition 13 (trace codes)**.** Let $S \subseteq \{0, \ldots, p^n - 1\}$. The S-trace code is a code whose codewords are evaluations of functions $f : \mathbb{F}_{p^n} \to \mathbb{F}_p$ given by

$$\mathcal{T}(S) = \left\{ \left(\sum_{e \in S} \mathrm{Tr}(\alpha_e x^e) : \mathbb{F}_{p^n} \to \mathbb{F}_p \right) : \alpha_e \in \mathbb{F}_p \right\},$$

where the Trace function $\mathrm{Tr} : \mathbb{F}_{p^n} \to \mathbb{F}_p$ is given by $\mathrm{Tr}(x) = \sum_{i=0}^{n-1} x^{p^i}$.

For example, dual-BCH codes of weight t correspond to the special case

$$\mathrm{dBCH}(t) = \mathcal{T}(\{1, 2, \ldots, t\}).$$

Generalized Reed-Muller codes over $\mathbb{F}_p^n$ of total degree d are equivalent to

$$\mathrm{RM}(n, d) = \mathcal{T}(\{e \in \{0, \ldots, p^n - 1\} : \mathrm{wt}(e) \leq d\}).$$

The following fact gives some simple properties of the Trace operator. For a proof, see any standard Algebra textbook, e.g. [5].

Fact 14 (Facts on the trace operator)**.** *Let* $\mathrm{Tr}(x) = \sum_{i=0}^{n-1} x^{p^i}$ *be the trace operator over* $\mathbb{F}_{p^n}$*. Then*

1. *For any* $x \in \mathbb{F}_{p^n}$*,* $\mathrm{Tr}(x) \in \mathbb{F}_p$*. That is,* $\mathrm{Tr} : \mathbb{F}_{p^n} \to \mathbb{F}_p$*.*
2. *The trace operator is linear. That is, for any* $x, y \in \mathbb{F}_{p^n}$ *and* $a, b \in \mathbb{F}_p$ *we have*
$$\mathrm{Tr}(ax + by) = a\mathrm{Tr}(x) + b\mathrm{Tr}(y).$$
3. *The trace operator is invariant under the Frobenius map. That is, for any* $x \in \mathbb{F}_{p^n}$ *and* $0 \leq i \leq n - 1$ *we have*
$$\mathrm{Tr}(x^{p^i}) = \mathrm{Tr}(x).$$
4. *Let* $x \in \mathbb{F}_{p^n}$*, and assume that for any* $\alpha \in \mathbb{F}_{p^n}$ *we have* $\mathrm{Tr}(\alpha x) = 0$*. Then* $x = 0$*.*

We denote the dual codeword to $\mathcal{T}(S)$ by $d\mathcal{T}(S) = \mathcal{T}(S)^{\perp}$. The following claim characterizes dual-trace codes.

Claim 15 (Characterization of dual-trace codes)**.** Let $S \subseteq \{0, \ldots, p^n - 1\}$. Then

$$d\mathcal{T}(S) = \left\{ (g : \mathbb{F}_{p^n} \to \mathbb{F}_p) : \sum_{x \in \mathbb{F}_{p^n}} g(x) x^e = 0 \quad \forall e \in S \right\}.$$

Proof. Let $g : \mathbb{F}_{p^n} \to \mathbb{F}_p$ be a function such that $\sum g(x) x^e = 0$ for all $e \in S$. We first verify that $g \in d\mathcal{T}(S)$. To do so, we need to show that $\sum_x f(x) g(x) = 0$ for any $f \in \mathcal{T}(S)$. Let $f = \sum_{e \in S} \mathrm{Tr}(\alpha_e x^e) \in \mathcal{T}(S)$. Then we have

$$\begin{aligned}\sum_{x \in \mathbb{F}_{p^n}} f(x) g(x) &= \sum_{x \in \mathbb{F}_{p^n}} \sum_{e \in S} \mathrm{Tr}(\alpha_e x^e) g(x) \\ &= \sum_{e \in S} \mathrm{Tr}(\alpha_e \sum_{x \in \mathbb{F}_{p^n}} x^e g(x)) = 0,\end{aligned}$$

where we used the fact that Trace is a linear operator over $\mathbb{F}_{p^n}$, thus $\mathrm{Tr}(ax+by) = a\mathrm{Tr}(x)+b\mathrm{Tr}(y)$ for any $a, b \in \mathbb{F}_p$ and $x, y \in \mathbb{F}_{p^n}$. Thus, to prove the claim we need to establish that for any $g \in d\mathcal{T}(S)$ and any $e \in S$ we have $\sum g(x)x^e = 0$. Note that for any $\alpha_e \in \mathbb{F}_{p^n}$ we have $f(x) = \alpha_e x^e \in \mathcal{T}(S)$, thus we have

$$\sum_{x \in \mathbb{F}_{p^n}} \mathrm{Tr}(\alpha_e x^e g(x)) = 0.$$

Let $z = \sum_{x \in \mathbb{F}_{p^n}} g(x)x^e$. We obtained that for any $\alpha_e \in \mathbb{F}_{p^n}$ we have

$$\mathrm{Tr}(\alpha_e z) = 0.$$

This can only hold if $z = 0$, thus we conclude that we must have that $\sum_x g(x)x^e = 0$ for all $e \in S$. □

The next claim shows that if $S_1 \subseteq S_2$ then $\mathcal{T}(S_1) \subseteq \mathcal{T}(S_2)$ and $d\mathcal{T}(S_1) \supseteq d\mathcal{T}(S_2)$.

Claim 16 (Monotonicity of trace codes). Let $S_1 \subseteq S_2 \subseteq \{0, \dots, p^n - 1\}$. Then we have the following inclusions

1. $\mathcal{T}(S_1) \subseteq \mathcal{T}(S_2)$.
2. $d\mathcal{T}(S_1) \supseteq d\mathcal{T}(S_2)$.

Proof. The claim follows immediately from the definition of trace codes and of dual codes. □

We will consider in the following few claims only trace codes for $S \subseteq \{1, \dots, p^n - 1\}$, i.e. we disallow $0 \in S$. We will later also deal with sets containing 0. We now define irreducible degrees and reduced forms. We will see that it is enough to study trace codes over reduced form sets.

Definition 17 (Irreducible degrees and reduced form)**.** We define R as the set of co-prime elements to p,

$$R = \{1 \le e \le p^n - 1 : (e, p) = 1\}.$$

For $1 \le e \le p^n - 1$ define its *reduced form* $e' \in R$ as follows. Let $e = p^k m$ where $(p, m) = 1$. Then the reduced form of e is $e' = m$. For a subset $S \subseteq \{1, \dots, p^n - 1\}$ define its reduced form $S' \subseteq R$ as $S' = \{e' : e \in S\}$.

Claim 18 (Trace codes are defined over reduce form sets). Let $S \subseteq \{1, \dots, p^n - 1\}$. Let $S' \subseteq R$ be the reduced form of S. Then $d\mathcal{T}(S) = d\mathcal{T}(S')$ and $\mathcal{T}(S) = \mathcal{T}(S')$.

Proof. By Claim 15 we have that $g \in d\mathcal{T}(S)$ iff $\sum g(x)x^e = 0$ for all $e \in S$. For any $0 \le k \le n - 1$ we have

$$\left(\sum g(x)x^e\right)^{p^k} = \sum g(x)x^{ep^k} = \sum g(x)x^{ep^k \pmod{p^n}},$$

where we used the facts that $x \to x^{p^k}$ is a linear map over $\mathbb{F}_{p^n}$, and that for any $x \in \mathbb{F}_{p^n}$ we have $x^{p^n} = x$. Hence we get that $\sum g(x)x^e = 0$ iff $\sum g(x)x^{e'} = 0$ for any e' such that $e' = ep^k \pmod{p^n}$. This shows that $d\mathcal{T}(S) = d\mathcal{T}(S')$, since for every element $e \in S$ there is some $e' = ep^k \pmod{p^n} \in S'$ and vice versa. Since $d\mathcal{T}(S) = d\mathcal{T}(S')$ we also get by the uniqueness of dual codes that $\mathcal{T}(S) = d\mathcal{T}(S)^\perp = d\mathcal{T}(S')^\perp = \mathcal{T}(S')$. □

The next claim establishes the size of trace codes defined over reduced form sets $S \subseteq R$.

Claim 19 (Size of trace codes). Let $S \subseteq \{1, \dots, p^n - 1\}$. Let $S' \subseteq R$ be the reduced form of S. Then $|\mathcal{T}(S)| = p^{n|S'|}$.

Proof. By Claim 18 we know that $\mathcal{T}(S) = \mathcal{T}(S')$. The codewords of $\mathcal{T}(S')$ are functions of the form

$$f(x) = \sum_{e \in S'} \mathrm{Tr}(\alpha_e x^e),$$

where $\alpha_e \in \mathbb{F}_{p^n}$. The number of combinations of $\{\alpha_e : e \in S'\}$ is $|\mathbb{F}_{p^n}|^{|S'|} = p^{n|S'|}$. Hence to conclude we need to show any two such settings are distinct. Since the code is linear, it is enough to show that if the coefficients α_e are not all zero, then the codeword is not the all zeros codeword, i.e. there is some $x \in \mathbb{F}_{p^n}$ such that

$$\sum_{e \in S'} \mathrm{Tr}(\alpha_e x^e) \neq 0.$$

Let $p(x) = \sum_{e \in S'} \mathrm{Tr}(\alpha_e x^e)$, and note that

$$\begin{aligned} p(x) &= \sum_{e \in S'} \sum_{i=0}^{n-1} \alpha_e^{p^i} x^{ep^i} \\ &= \sum_{e \in S'} \sum_{i=0}^{n-1} \alpha_e^{p^i} x^{ep^i \pmod{p^n}}, \end{aligned}$$

where we used the facts that $\mathrm{Tr}(x) = \sum_{i=0}^{n-1} x^{p^i}$ as well as the identity $x^t = x^{t \pmod{p^n}}$ which holds for any t. Since $S' \subseteq R$ is a set of

all the monomials x^{ep^i} for $e \in S'$ are disjoint. Hence $p(x)$ is not the all zeros polynomial. As $\deg(p) \leq p^n - 1$ there must exist some $x \in \mathbb{F}_{p^n}$ such that $p(x) \neq 0$, and the codeword defined by f is not the all zeros codeword. □

2.3 Characterization of affine invariant codes by trace codes

We start by recalling *affine invariant codes*, which are codes that are closed under an affine transformation of the input space coordinates.

Definition 20 (Affine closure, and affine invariant codes)**.** Let $f : \mathbb{F}_{p^n} \to \mathbb{F}_p$ be a function. The *affine closure* of f is the set of functions

$$\overline{\text{affine}}(f) = \left\{ (f(ax+b) : \mathbb{F}_{p^n} \to \mathbb{F}_p) : a, b \in \mathbb{F}_{p^n} \right\}.$$

A code $\mathcal{C} = \{f : \mathbb{F}_{p^n} \to \mathbb{F}_p\}$ is called *affine invariant* if for any $f \in \mathcal{C}$, we have $\overline{\text{affine}}(f) \subseteq \mathcal{C}$. A codeword $f \in \mathcal{C}$ *affinely generates* $\mathcal{C}$ if

$$\mathcal{C} = \mathrm{Span}(\overline{\text{affine}}(f)).$$

We can characterize linear codes which are affine invariant as a special subfamily of trace codes. To this end we will require some definitions. We first define shift closure of a set, which is tightly related to the reduced form we previously defined.

Definition 21 (Shift closed)**.** Let $e \in \{0, \ldots, p^n - 1\}$. The *shift closure* of e is defined as the set

$$\overline{\text{shift}}(e) = \{ep^\ell \pmod{p^n} : \ell = 1, \ldots, n\}.$$

The shift closure of a set $S \subseteq \{0, \ldots, p^n - 1\}$ is defined as the union of the shift closures of its elements,

$$\overline{\text{shift}}(S) = \cup_{e \in S} \overline{\text{shift}}(e).$$

A set $S \subseteq \{0, \ldots, p^n - 1\}$ is said to be *shift closed* if $S = \overline{\text{shift}}(S)$.

The term *shift closed* comes from viewing elements $e \in S$ as vectors in $\mathbb{F}_p^n$, given by the representation of e in base p. In this case, $ep^\ell \pmod{p^n}$ corresponds to a cyclic shift of the vector by ℓ coordinates. The following claim shows that trace codes are invariant under shift closure.

Claim 22. Let $S \subseteq \{0, \dots, p^n - 1\}$. Then

$$d\mathcal{T}(S) = d\mathcal{T}(\overline{\text{shift}}(S)), \quad \mathcal{T}(S) = \mathcal{T}(\overline{\text{shift}}(S)).$$

Proof. The proof is identical to the proof of Claim 18. □

We next define the notion of shadow closed sets.

Definition 23 (Shadow closed)**.** Let $S \subseteq \{0, \dots, p^n - 1\}$. The set S is said to be *shadow closed* if the following holds. For any $e \in S$, let $e = \sum_{i=0}^{n-1} e_i p^i$ be the representation of e in base p. Define the *support* of e to be the set of nonzero digits of e,

$$\text{support}(e) = \{0 \le i \le n-1 : e_i \ne 0\}.$$

Let e' be obtained from e by changing some of the non-zero digits of e, i.e.

$$e' = \sum_{i \in \text{support}(e)} e'_i p^i.$$

Then we should have that also $e' \in S$. That is, S is shadow closed if

$$\left\{ \sum_{i \in \text{support}(e)} e'_i p^i : e \in S, (e'_i)_{i \in \text{support}(e)} \in \mathbb{F}_p \right\} \subseteq S.$$

Definition 24 (Affine closed)**.** A set $S \subseteq \{0, \dots, p^n - 1\}$ is *affine closed* if it is both shift closed and shadow closed.

We recall the following theorem of Kaufman and Sudan [21] that we presented in the introduction. It shows that affine invariant linear codes are equivalent to trace codes over affine closed sets.

Theorem (Theorem 8: Equivalence of affine invariant codes and trace codes of affine closed sets)**.** *Let $\mathcal{C} = \{f : \mathbb{F}_{p^n} \to \mathbb{F}_p\}$ be an affine invariant linear code. Then there exists an affine closed set $S \subseteq \{0, \dots, p^n - 1\}$ such that $\mathcal{C} = \mathcal{T}(S)$. Moreover, for any affine closed set S the code $\mathcal{T}(S)$ is linear and affine invariant.*

2.4 Weight distribution of affine invariant codes

Theorem 8 tells us that in order to study affine invariant codes, it suffices to study trace codes of affine closed sets. In this subsection we establish the following lemma, which gives a tight estimate on the number of codewords in $d\mathcal{T}(S)$ for affine closed sets S. For the statement of the lemma recall that $R = \{1 \le e \le p^n - 1 : (e, p) = 1\}$ is the set of elements co-prime to p.

Lemma 25 (Weight distribution of dual trace affine closed codes)**.** *There exist absolute constants $c, c' > 1$ such that the following is true. Let $S \subseteq \{0, \dots, p^n - 1\}$ be affine closed of size $|S| \le \frac{1}{c'} p^{n/c}$.*

Then there exists $\ell_{\min} = c'|S \cap R|^c$ and $\ell_{\max} = \frac{1}{c'}p^{n/c}$, such that for any $\ell_{\min} \le \ell \le \ell_{\max}$ the following holds. The number of codewords in $d\mathcal{T}(S)$ of weight exactly ℓ is given by

$$\frac{C(p,\ell)}{\ell!}p^{n\ell-|S\cap R|}(1+\epsilon)$$

where $C(p,\ell)$ is defined as

$$C(p,\ell) = \left|\left\{(v_1,\dots,v_\ell) \in (\mathbb{F}_p \setminus \{0\})^\ell : v_1+\ldots+v_\ell = 0\right\}\right|.$$

and $|\epsilon| \le p^{-n/2} \ll 1$. In particular, one can take $c = 8$ and $c' = 16$.

We start by showing a general bound on the weight degree of elements of affine closed sets, in terms of the size of the set.

Claim 26 (Weight degree bound on affine closed sets)*.* Let $S \subseteq \{0,\dots,p^n-1\}$ such that S is affine closed. Then for any $e \in S$,

$$\mathrm{wt}(e) \le \log_p |S \cap R| + 1.$$

Proof. Let $S' = S \cap R$. Let $e \in S$ be of weight $k \ge 1$. By taking some shift of e we may assume $e \in R$ (that is, $0 \in \mathrm{support}(e)$), hence $e \in S' = S \cap R$. Consider the set

$$E' = \left\{\sum_{i \in \mathrm{support}(e)} e'_i p^i : e'_i \in \mathbb{F}_p,\ e'_0 \ne 0\right\}.$$

Note that as S is shadow closed, we have $E' \subseteq S$. Moreover since $e'_0 \ne 0$ we have $E' \subseteq R$, hence $E' \subseteq S' = S \cap R$. Thus $|E'| \le |S'|$. On the other hand,

$$|E'| = (p-1)p^{\mathrm{wt}(e)-1}.$$

Hence we conclude that $\mathrm{wt}(e) \le \log_p(\frac{p}{p-1}|S'|) \le \log_p |S'| + 1$. □

We will need the following simple claim.

Claim 27 (Trace is not constant)*.* Let $f(x) = \sum_{e\in R} \alpha_e x^e$ be a nonzero polynomial. Then $\mathrm{Tr}(f(x)) : \mathbb{F}_{p^n} \to \mathbb{F}_p$ is not a constant function.

Proof. Assume for contradiction that $\mathrm{Tr}(f(x)) = a$ for all $x \in \mathbb{F}_{p^n}$. Let $q(x) = \mathrm{Tr}(f(x)) - a$. We have

$$q(x) = -a + \sum_{i=0}^{n-1}(\sum_{e\in R} \alpha_e x^e)^{p^i} = -a + \sum_{i=0}^{n-1}\sum_{e \in R}(\alpha_e)^{p^i} x^{ep^i \pmod{p^n}}.$$

Since $e \in R$ all the degrees $ep^i \pmod{p^n}$ are distinct and different from 0. Thus $q(x)$ is not the zero polynomial. Since $\deg(q) \le p^n - 1$ we have that there must be x such that $q(x) \ne 0$, hence $\mathrm{Tr}(f(x)) \ne a$. □

The next lemma is a general lemma, which estimates the number of elements in $d\mathcal{T}(S)$ where S is a relatively small set of elements of small weight degree. We will then show that the lemma can be applied to any affine invariant set S which is not too large.

Lemma 28 (Weight distribution of dual trace codes of reduced form sets)**.** *There exists an absolute constant $c > 1$ such that the following is true. Let $S \subseteq R$ be such that for any $e \in S$ its weight degree is at most $\mathrm{wt}(e) \le d$. There exist $\ell_{\min} = c|S|^2 d^2 2^d$ and $\ell_{\max} = p^{n/c}$, such that for any $\ell_{\min} \le \ell \le \ell_{\max}$ the following holds.*

1. *The number of codewords in $d\mathcal{T}(S)$ of weight exactly ℓ is given by*

$$\frac{(p-1)^\ell}{\ell!} p^{n\ell - |S|}(1+\epsilon).$$

where $|\epsilon| \le p^{-n/2} \ll 1$.

2. *The number of codewords in $d\mathcal{T}(S \cup \{0\})$ of weight exactly ℓ is given by*

$$\frac{C(p,\ell)}{\ell!} p^{n\ell - |S|}(1+\epsilon).$$

where $|\epsilon| \le p^{-n/2}$ and $C(p,\ell)$ is defined as

$$C(p,\ell) = \left| \left\{ (v_1, \ldots, v_\ell) \in (\mathbb{F}_p \setminus \{0\})^\ell : v_1 + \ldots + v_\ell = 0 \right\} \right|.$$

In particular, one can take $c = 8$.

Proof. We start by proving the estimate for $d\mathcal{T}(S)$. For any $v = (v_1, \ldots, v_\ell) \in \{1, \ldots, p-1\}^\ell$ define the sets

$$A_\ell(v) = \{(\alpha_1, \ldots, \alpha_\ell) \in \mathbb{F}_{p^n}^\ell : \sum_{i=1}^{\ell} v_i \alpha_i^e = 0 \quad \forall e \in S\}$$

and

$$B_\ell(v) = \{(\alpha_1, \ldots, \alpha_\ell) \in A_\ell(v) : \alpha_1, \ldots, \alpha_\ell \text{ are all distinct}\}.$$

Let $f : \mathbb{F}_p^n \to \mathbb{F}_p$ be a function $f \in d\mathcal{T}(S)$, such that f has weight exactly ℓ. Equivalently, there are distinct points $\alpha_1, \ldots, \alpha_\ell \in \mathbb{F}_{p^n}$ such that $\sum f(\alpha_i)\alpha_i^e = 0$ for all $e \in S$. We can identify f uniquely by the list of points $(\alpha_1, \ldots, \alpha_\ell)$ and the evaluation of f on these points $v = (f(\alpha_1), \ldots, f(\alpha_\ell)) \in \{1, \ldots, p-1\}^\ell$. Since the order of $\alpha_1, \ldots, \alpha_\ell$ does not matter, and they are all distinct, there are $\ell!$ elements in $\cup B_\ell(v)$ which correspond to f, (i.e. these elements correspond to all orderings of $\alpha_1, \ldots, \alpha_\ell$). Thus we obtain the following identity,

$$\text{Number of codewords in } d\mathcal{T}(S) \text{ of weight } \ell = \frac{1}{\ell!} \sum_{v \in \{1,\ldots,p-1\}^\ell} |B_\ell(v)|.$$

Hence, to conclude the proof we will show that $|B_\ell(v)| \approx p^{n(\ell - |S|)}$. In fact, we will first show that $|A_\ell(v)| \approx p^{n(\ell-|S|)}$ and then deduce the estimate for $|B_\ell(v)|$.

Fix some $v \in \{1, \ldots, p-1\}^\ell$. We will now show an estimate on $|A_\ell(v)|$, where the main tool we use is Fourier analysis. Let $\alpha = (\alpha_e : e \in S) \in \mathbb{F}_{p^n}^S$, and define $\phi_\alpha : \mathbb{F}_{p^n} \to \mathbb{F}_p$ by

$$\phi_\alpha(x) = \mathrm{Tr}(\sum_{e \in S} \alpha_e x^e).$$

Take any tuple $(x_1, \ldots, x_\ell) \in \mathbb{F}_{p^n}^\ell$, and consider

$$\mu(x_1, \ldots, x_\ell) = \mathbb{E}_{\alpha \in \mathbb{F}_{p^n}^S} \left[\omega^{v_1 \phi_\alpha(x_1) + \ldots + v_\ell \phi_\alpha(x_\ell)} \right],$$

where $\omega = e^{\frac{2\pi i}{p}}$ is a p-root of unity. We claim that if $(x_1, \ldots, x_\ell) \in A_\ell(v)$ then $\mu(x_1, \ldots, x_\ell) = 1$, and if $(x_1, \ldots, x_\ell) \notin A_\ell(v)$ then $\mu(x_1, \ldots, x_\ell) = 0$. To see that,

$$\begin{aligned}
\mu(x_1, \ldots, x_\ell) &= \mathbb{E}_{\alpha \in \mathbb{F}_{p^n}^S} \left[\omega^{\mathrm{Tr}(\sum_{e \in S} \alpha_e (v_1 x_1^e + \ldots + v_\ell x_\ell^e))}\right] \\
&= \prod_{e \in S} \mathbb{E}_{\alpha_e \in \mathbb{F}_{p^n}} \left[\omega^{\mathrm{Tr}(\alpha_e (v_1 x_1^e + \ldots + v_\ell x_\ell^e))}\right] \\
&= \prod_{e \in S} \mathbf{1}_{v_1 x_1^e + \ldots + v_\ell x_\ell^e = 0} = \mathbf{1}_{(x_1, \ldots, x_\ell) \in A_\ell(v)}.
\end{aligned}$$

Hence we have

$$\begin{aligned}
|\mathbb{F}_{p^n}|^{-\ell} |A_\ell(v)| &= \mathbb{E}_{x_1, \ldots, x_\ell \in \mathbb{F}_{p^n}} \left[\mu(x_1, \ldots, x_\ell)\right] \\
&= \mathbb{E}_{x_1, \ldots, x_\ell \in \mathbb{F}_{p^n}} \mathbb{E}_{\alpha \in \mathbb{F}_{p^n}^S} \left[\omega^{\mathrm{Tr}(\sum_{e \in S} \alpha_e (v_1 x_1^e + \ldots + v_\ell x_\ell^e))}\right] \\
&= \mathbb{E}_{\alpha \in \mathbb{F}_{p^n}^S} \prod_{i=1}^{\ell} \mathbb{E}_{x_i \in \mathbb{F}_{p^n}} \left[\omega^{\mathrm{Tr}(\sum_{e \in S} \alpha_e v_i x_i^e)}\right]
\end{aligned}$$

We partition the expectation to the cases where $\alpha = 0^S$ and $\alpha \neq 0^S$. When $\alpha = 0^S$ then for all $i = 1, \ldots, \ell$ we have that

$$\mathbb{E}_{x_i \in \mathbb{F}_{p^n}} \left[\omega^{\mathrm{Tr}(\sum_{e \in S} \alpha_e v_i x_i^e)}\right] = 1.$$

Consider now any $\alpha \neq 0^S$ and any $i = 1, \ldots, \ell$. As $v_i \in \mathbb{F}_p \setminus \{0\}$ then also $\alpha v_i \neq 0^S$. We will show that $\mathrm{Tr}(\sum_{e \in S} \alpha_e v_i x_i^e)$ has small bias . To this end we apply Theorem 4. Let $f(x) = g(x) + h(x)$ for $g(x) = 0$ and $h(x) = \sum_{e \in S} \alpha_e v_i x_i^e$. As $S \subseteq R$ and not all $\alpha_e = 0$, we have by Claim 27 that $\mathrm{Tr}(f)$ is not constant. Our condition on the set S was that $\mathrm{wt}(e) \leq d$ for any $e \in S$. Hence we get by Theorem 4 (for $\delta = 1/2$) that

$$\left|\mathbb{E}_{x \in \mathbb{F}_{p^n}} \left[\omega^{\mathrm{Tr}(\sum_{e \in S} \alpha_e v_i x^e)}\right]\right| \leq |\mathbb{F}_{p^n}|^{-\frac{1}{4|S|d^2 2^d}}.$$

Hence we deduce that

$$|A_\ell(v)| = |\mathbb{F}_{p^n}|^{\ell - |S|}(1 + \epsilon)$$

where $|\epsilon| \leq |\mathbb{F}_{p^n}|^{|S| - \ell \cdot \frac{1}{4|S|d^2 2^d}}$. Thus, if we take $\ell \geq 8|S|^2 d^2 2^d$ we get that $|\epsilon| \leq p^{-n|S|} \leq p^{-n} \ll 1$.

To conclude, we need to derive an estimate on $|B_\ell(v)|$. Let $C_\ell(v) = A_\ell(v) \setminus B_\ell(v)$. We will show that $|C_\ell(v)| \ll |B_\ell(v)|$, and hence $|B_\ell(v)| \approx |A_\ell(v)|$. To derive this, note that if $(\alpha_1, \ldots, \alpha_\ell) \in C_\ell(v)$, then $\alpha_1, \ldots, \alpha_\ell$ are not all distinct, that is, $\alpha_i = \alpha_j$ for some distinct $i < j$. Define $v^{(i,j)} \in \{1, \ldots, p-1\}^{\ell - 1}$ by "joining" α_i and α_j, i.e. $v_a^{(i,j)} = v_a$ for $1 \leq a < i$ and $i < a < j$, $v_i^{(i,j)} = v_i + v_j$, $v_a^{(i,j)} = v_{a+1}$ for $a > j$. Then we can identify uniquely $(\alpha_1, \ldots, \alpha_\ell) \in C_\ell(v)$ with $\alpha^{(i,j)} = (\alpha_1, \ldots, \alpha_{j-1}, \alpha_{j+1}, \ldots, \alpha_\ell) \in A_{\ell-1}(v^{(i,j)})$. Hence we get

$$|C_\ell(v)| \leq \sum_{i<j} |A_{\ell-1}(v^{i,j})| \leq \binom{\ell}{2} |A_{\ell-1}(\cdot)| \leq \ell^2 |\mathbb{F}_{p^n}|^{\ell - 1 - |S|}(1 + \epsilon) = \frac{\ell^2}{p^n} |A_\ell(v)|(1 + \epsilon).$$

Hence we get that

$$|B(v)| = |\mathbb{F}_{p^n}|^{\ell - |S|}(1 + \epsilon')$$

where $\epsilon' = \frac{\ell^2}{p^n} + \epsilon$. Thus if $\ell \leq p^{n/8}$ we get that $\frac{\ell^2}{p^n} \ll p^{-n/2}$. Hence we finished the proof of the first claim.

The proof of the second claim is completely analogous, except if we consider $d\mathcal{T}(S \cup \{0\})$, we have that additional requirement that $v_1 + \ldots + v_\ell = 0$. Thus one should not consider $A_\ell(v)$ for all $v \in (\mathbb{F}_p \setminus \{0\})^\ell$, but only those corresponding to $v \in C(p, \ell)$. Thus we have

$$\text{Number of codewords in } d\mathcal{T}(S \cup \{0\}) \text{ of weight } \ell = \frac{1}{\ell!} \sum_{v \in C(p,\ell)} |B_\ell(v)|.$$

and the proof follows by the estimates we proved on $|B_\ell(v)|$. □

We can now deduce Lemma 25 from Claim 26 and Lemma 28.

Proof of Lemma 25. Let $S \subseteq \{0, \ldots, p^n - 1\}$ be affine closed. We have that

$$d\mathcal{T}(S) = d\mathcal{T}((S \cap R) \cup \{0\}).$$

By Claim 26 the maximal weight of elements in S is at most

$$d \leq \log_p |S \cap R| + 1.$$

Applying Lemma 28, we get that for $\ell_{\min} = 16 \cdot |S \cap R|^4 \geq 8|S \cap R|^2 d^2 2^d$ and $\ell_{\max} = \frac{1}{16} p^{n/4}$, we get that for every $\ell_{\min} \leq \ell \leq \ell_{\max}$ the number of codewords of weight ℓ in $d\mathcal{T}(S) = d\mathcal{T}((S \cap R) \cup \{0\})$ is

$$\frac{C(p,\ell)}{\ell!} p^{n\ell - |S \cap R|}(1 + \epsilon)$$

where $|\epsilon| \leq p^{-n/2}$. □

2.5 Trace codes of exponential size are generated by a single orbit

We prove in this subsection that any affine invariant linear code of up to exponential size is generated by a single orbit of a dual codeword. Combining this with Theorem 10 we get that any such code is locally testable, which prove our main result, Theorem 1. We now state the main theorem we prove in this subsection.

Theorem 29 (Affine invariant codes are generated by a single orbit). *There exist absolute constants $0 < \alpha < 1$ and $c, c' \geq 1$ such that the following is true. Let $\mathcal{C} = \{f : \mathbb{F}_{p^n} \to \mathbb{F}_p\}$ be an affine invariant linear code, such that $\dim(\mathcal{C}) \leq \frac{1}{c'} p^{\alpha n}$. Then there exists $f \in \mathcal{C}^\perp$ such that*

$$\overline{\text{affine}}(f)^\perp = \mathcal{C}$$

and of weight

$$\text{wt}(f) \leq c'(\dim(\mathcal{C})/n)^c.$$

In particular, one may choose $\alpha = 1/16$, $c = 4$ and $c' = (2p)^8$.

Let $\mathcal{C} = \mathcal{T}(S)$ be an affine invariant code where $S \subseteq \{0, \ldots, p^n - 1\}$ is affine closed. We start by showing that if some $f \in \mathcal{C}^\perp = d\mathcal{T}(S)$ does not generate $d\mathcal{T}(S)$, then in fact $f \in d\mathcal{T}(S \cup \{e\})$ where $e \in \{1, \ldots, p^n - 1\} \setminus S$ has small weight (Corollary 32). From this and the exact estimates for the weight distribution for dual trace codes we derive Theorem 29. Before proving Corollary 32 we will require two technical claims.

Claim 30. Let $S \subseteq \{0, \ldots, p^{n-1}\}$ be affine closed. Let $f \in d\mathcal{T}(S)$ be a codeword which does not affinely generate $d\mathcal{T}(S)$, i.e.

$$\overline{\text{affine}}(f) \subsetneq d\mathcal{T}(S).$$

Then

$$\overline{\text{affine}}(f) = d\mathcal{T}(T)$$

for some affine closed $T \supsetneq S$.

Proof. The code $\overline{\text{affine}}(f)$ is an affine invariant code which is a proper subset of $d\mathcal{T}(S)$. By Theorem 8 we know that $\overline{\text{affine}}(f) = d\mathcal{T}(T)$ for some affine closed $T \subseteq \{0, \ldots, p^n - 1\}$. Since $d\mathcal{T}(T) \subsetneq d\mathcal{T}(S)$ we must have that $T \supsetneq S$. □

Claim 31. Let $S \subsetneq T \subseteq \{0, \ldots, p^n - 1\}$ such that both S and T are affine closed. Then there exist an element $e \in (T \setminus S) \cap R$ such that

$$\text{wt}(e) \le \log_p |S \cap R| + 2.$$

Proof. Let $S' = S \cap R$ and $T' = T \cap R$. We have $S' \subsetneq T'$ as otherwise, if $S' = T'$, we would have $S = \overline{\text{affine}}(S') = \overline{\text{affine}}(T') = T$.

Let $k = \lfloor \log_p |S'| \rfloor + 2$. We argue there is $e \in T' \setminus S'$ of weight at most k. Otherwise, let $e \in S' \setminus T'$ such that $\text{wt}(e) > k$. Consider the set

$$E = \overline{\text{shadow}}(e) \cap R = \left\{ \sum_{i \in \text{support}(e)} e'_i p^i : e'_i \in \mathbb{F}_p,\ e'_0 \neq 0 \right\},$$

where we use the fact that since $e \in R$ then $0 \in \text{support}(e)$. Note that by definition, $E \subseteq T'$, since T is affine closed hence in particular shadow closed.

Let $e' \in E \subseteq T'$ such that $\text{wt}(e') = k$ (by setting $\text{wt}(e) - k$ digits of e in base p to zero). Consider the set

$$E' = \overline{\text{shadow}}(e') \cap R = \left\{ \sum_{i \in \text{support}(e')} e''_i p^i : e''_i \in \mathbb{F}_p,\ e''_0 \neq 0 \right\}.$$

Note that since $|E'| = (p-1)p^{\text{wt}(e')-1} = (p-1)p^{k-1} > |S'|$ we cannot have that $e' \in S'$. Hence we found an element $e' \in T' \setminus S'$ such that $\text{wt}(e') \le k$. □

Corollary 32. *Let $S \subseteq \{0, \ldots, p^{n-1}\}$ be affine closed. Let $f \in d\mathcal{T}(S)$ be a codeword which does not affinely generate $d\mathcal{T}(S)$, i.e.*

$$\overline{\text{affine}}(f) \subsetneq d\mathcal{T}(S).$$

Then there must exist $e \in R \setminus S$ of weight $\text{wt}(e) \le \log_p |S \cap R| + 2$ such that

$$f \in d\mathcal{T}(S \cup \{e\}).$$

Proof. By Claim 30 we have $\overline{\text{affine}}(f) = d\mathcal{T}(T)$ where $T \supsetneq S$. By Claim 31 there is $e \in (T \setminus S) \cap R \subseteq R \setminus S$ such that $\text{wt}(e) \le \log_p |S \cap R| + 2$. Hence we conclude sicne

$$f \in d\mathcal{T}(T) \subseteq d\mathcal{T}(S \cup \{e\}).$$

□

We are now ready to prove Theorem 29.

Proof of Theorem 29. Let $\mathcal{C}$ be a linear affine invariant code. By theorem 8 we have $\mathcal{C} = \mathcal{T}(S)$ where $S \subseteq \{0, \ldots, p^n - 1\}$ is affine closed. By Claims 16, 18 and 19 we have that

$$|\mathcal{C}| = \mathcal{T}((S \cap R) \cup \{0\}) \leq |\mathcal{T}(S \cap R)| = p^{n|S \cap R|}.$$

Hence we need to prove there is a codeword $f \in d\mathcal{T}(S)$ of weight $|S \cap R|^c$ whose affine closure spans $d\mathcal{T}(S)$. Let ℓ be an appropriate weight to be determined later. We now count the number of codewords in $d\mathcal{T}(S)$ of weight exactly ℓ. To this end we apply Lemma 25. The number of codewords in $d\mathcal{T}(S)$ of weight ℓ (as long as ℓ is in the permissible range) is given by

$$W_\ell = \frac{C(p, \ell)}{\ell!} p^{n\ell - |S \cap R|}(1 + p^{-\Omega(n)}).$$

Let $f \in d\mathcal{T}(S)$ be such that $\overline{\text{affine}}(f) \subsetneq d\mathcal{T}(S)$. By Corollary 32 we know that there exists some $e \in R \setminus S$ of weight $\text{wt}(e) \leq k$, where $k \leq \log_p(|S \cap R|) + 2$, such that $f \in d\mathcal{T}(S \cup \{e\})$. Let E be the set of all such possible e,

$$E = \{e \in R \setminus S : \text{wt}(e) \leq k\}.$$

Fix some $e \in E$. Let $S_e = \overline{\text{affine}}(S \cup \{e\})$. Note that as $e \in R \setminus S$ we have $|S_e \cap R| \geq |S \cap R| + 1$. Hence for ℓ in the permissible range for S_e we get that the number of codewords of weight ℓ in $d\mathcal{T}(S_e)$ is given by

$$\frac{C(p, \ell)}{\ell!} p^{n\ell - |S_e \cap R|}(1 + p^{-\Omega(n)}) \leq p^{-n} W_\ell (1 + p^{-\Omega(n)}),$$

So, as long as $|E| \ll p^n$, we can deduce that there must exist some $f \in d\mathcal{T}(S)$ of weight ℓ which is not in any of $d\mathcal{T}(S \cup \{e\})$ for any $e \in E$ (in fact, almost all $f \in d\mathcal{T}(S)$ of weight ℓ will do). This will establish the theorem. Thus, we need to bound $|E|$. The following is a simple bound which is sufficient for our needs.

$$|E| \leq \sum_{i=1}^{k} \binom{n}{i} p^i \leq p^{3n/4}$$

as long as $k \leq n/4$.

To conclude we need to show that we can choose ℓ such that $\ell \leq |S \cap R|^c$ for some absolute constant $c > 0$, as long as $|S \cap R| \leq p^{\alpha n}$ for some absolute constant $\alpha > 0$. The bounds on $\ell_{\min}$ and $\ell_{\max}$ that are required for the application Lemma 25 are stricter for S_e than for S, and are given by

$$\begin{aligned}
&|S_e| \leq \tfrac{1}{16} p^{n/4}, \\
&\ell_{\min} \geq 16 |S_e \cap R|^4, \\
&\ell_{\max} \leq \tfrac{1}{16} p^{n/4}.
\end{aligned}$$

To verify them we need to give an upper bound on $|S_e|$ and $|S_e \cap R|$. As $S_e = S \cup \overline{\text{affine}}(\{e\})$ we have

$$\begin{aligned}
&|S_e| \leq |S| + |\overline{\text{affine}}(\{e\})| = |S| + np^k, \\
&|S_e \cap R| \leq |S \cap R| + |\overline{\text{affine}}(\{e\}) \cap R| \leq |S \cap R| + p^k.
\end{aligned}$$

Note that $p^k = p^2|S \cap R|$. Thus, the bounds for applying Lemma 25 are satisfied if we make sure that

$$\begin{aligned} &|S| \leq \tfrac{1}{32p^2n}p^{n/4}, \\ &\ell_{\min} \geq (2p)^8|S \cap R|^4, \\ &\ell_{\max} \leq \tfrac{1}{16}p^{n/4}. \end{aligned}$$

Notice that as long as $|S| \leq \frac{1}{16p^3}p^{n/16}$ we have that all the conditions are satisfied (for large enough n) and that $\ell_{\min} \leq \ell_{\max}$. Hence we may choose $\ell = \ell_{\min}$ to conclude the proof. □

3 Extension of the Weil bound

In this section we prove our new extension to the Weil bound for character sums, which is one of the key technical ingredients in our proof of the local testability of affine invariant codes. As this result may be of independent interest, this section is self-contained, and the interested reader may read this section without relying on Section 2.

We recall several definitions and theorems from the introduction, for the sake of self containment. Let $\mathbb{F} = \mathbb{F}_{p^n}$ be a finite field. An additive character $\chi : \mathbb{F} \to \mathbb{C}$ is a mapping such that $\chi(x+y) = \chi(x)\chi(y)$ and χ is not identically zero. The following is a classical result by Weil.

Theorem (Weil bound - Theorem 2)**.** *Let $f(x)$ be a univariate polynomial over $\mathbb{F}$ of degree $|\mathbb{F}|^{1/2-\delta}$. Let $\chi : \mathbb{F} \to \mathbb{C}$ be an additive character. Then either $\chi(f(x))$ is constant or*

$$|\mathbb{E}_{x \in \mathbb{F}}[\chi(f(x))]| \leq |\mathbb{F}|^{-\delta}.$$

The *weight degree* of a monomial x^t is defined as follows. Let $t = \sum_{i=0}^{n-1} a_i p^i$ be the representation of t in base p, where $0 \leq a_i \leq p-1$. The weight degree of x^t is defined to be $wt(x^t) = \sum a_i$. The weight degree of a polynomial $f(x)$ is the maximal weight of a monomial in f.

Note 33. We note that the weight degree of a polynomial can be equivalently defined also as a *derivative degree*, defined as follows. The directional derivative of $f(x)$ in direction $y \in \mathbb{F}_{p^n}$ is defined as $f_y(x) = f(x+y) - f(x)$. Define iterative derivatives in directions $y_1, \ldots, y_k$ as $f_{y_1,\ldots,y_k} = (f_{y_1,\ldots,y_{k-1}})_{y_k}$. The *derivative degree* of f is the minimal d such that for any $d+1$ derivatives $y_1, \ldots, y_{d+1} \in \mathbb{F}$, $f_{y_1,\ldots,y_{d+1}}(x) \equiv 0$. It can be verified that the derivative degree of a polynomial is exactly its weight degree. We do not prove this here, and will not require this fact in the proof.

We prove an extension of the Weil bound in case f is the sum of a low degree polynomial and a small number of monomials of bounded weight (but of arbitrary degree).

Theorem (Extension of the Weil bound - Theorem 4)**.** *Let $f(x) = g(x) + h(x)$ be a univariate polynomial over $\mathbb{F}_{p^n}$, where $g(x)$ is a polynomial of degree $|\mathbb{F}|^{1/2-\delta}$ and $h(x)$ is the sum of at most $k \geq 1$ monomials, each of weight degree at most d. Let $\chi : \mathbb{F}_{p^n} \to \mathbb{C}$ be an additive character. Then either $\chi(f(x))$ is constant or*

$$|\mathbb{E}_{x \in \mathbb{F}}[\chi(f(x))]| \leq |\mathbb{F}|^{-\frac{\delta}{2kd^2 2^d}}.$$

3.1 Technical claims

In this subsection we provide some technical claims that will be needed for the proof of Theorem 4.

3.1.1 The trace operator

The trace operator $Tr : \mathbb{F}_{p^n} \to \mathbb{F}_p$ is defined as $Tr(x) = \sum_{i=0}^{n-1} x^{p^i}$. We give in this subsection some simple properties of the Trace operator.

Claim 34 (Characterization of additive characters)*.* Let $\chi : \mathbb{F}_{p^n} \to \mathbb{C}$ be an additive character. Then there exists $a \in \mathbb{F}_{p^n}$ such that $\chi(x) \equiv \omega^{\mathrm{Tr}(ax)}$ where $\omega = e^{2\pi i/p}$.

Proof. We first prove that $\chi(x) = \omega^{\ell(x)}$ where $\ell : \mathbb{F}_{p^n} \to \mathbb{F}_p$ is a linear map. Note that we must have $\chi(0) = 1$ since $\chi(0) = \chi(0+0) = \chi(0)^2$, and we cannot have $\chi(0) = 0$ as this will imply that $\chi \equiv 0$. Thus, we get that the image of χ is a p-th root of unity since $\chi(x)^p = \chi(px) = \chi(0) = 1$. Thus we can write $\chi(x) = \omega^{\ell(x)}$ for some mapping $\ell : \mathbb{F}_{p^n} \to \mathbb{F}_p$. The mapping ℓ is linear since

$$\omega^{\ell(x+y)} = \chi(x+y) = \chi(x)\chi(y) = \omega^{\ell(x)+\ell(y)}.$$

Now we argue that any linear mapping $\ell : \mathbb{F}_{p^n} \to \mathbb{F}_p$ can be represented as $\ell(x) \equiv \mathrm{Tr}(ax)$ for some $a \in \mathbb{F}_{p^n}$. This is proved by a counting argument. Each linear map $\ell : \mathbb{F}_{p^n} \to \mathbb{F}_p$ can be uniquely identified by its image on a basis for $\mathbb{F}_{p^n}$ as a linear space over $\mathbb{F}_p$. Thus, the number of such linear mappings is at most p^n. On the other hand, for each $a \in \mathbb{F}_{p^n}$ the mapping $x \to Tr(ax)$ is linear (since Trace is a linear mapping), and the total number of theses mappings is the number of distinct $a \in \mathbb{F}_{p^n}$, that is p^n. To conclude we just need to show that for any distinct $a \neq b \in \mathbb{F}_{p^n}$ the mappings $\mathrm{Tr}(ax)$ and $\mathrm{Tr}(bx)$ are distinct. Equivalently, since Trace is a linear mapping, we need to show that $Tr((a-b)x) \not\equiv 0$. This is clear however because the Trace mapping is not identically zero and $a - b \neq 0$ is invertible. □

Claim 35 (Trace of a p-power is unbiased)*.* For every $c \neq 0$ and $0 \leq L \leq n-1$ we have

$$\mathbb{E}_{x\in\mathbb{F}_{p^n}}[\omega^{\mathrm{Tr}(cx^{p^L})}] = 0.$$

Proof. We have $Tr(cx^{p^L}) = Tr(c^{p^{n-L}}x)$, so it suffices to prove the claim for $L = 0$. Let $\ell : \mathbb{F}_{p^n} \to \mathbb{F}_p$ defined as $\ell(x) = Tr(cx)$. The mapping ℓ is linear, and as it is not identically zero, its output is uniform over $\mathbb{F}_p$. Thus we have that $\mathbb{E}_{x\in\mathbb{F}_{p^n}}[\omega^{\ell(x)}] = 0$. □

3.1.2 Reduced forms

We define in this subsection reduced forms of polynomials. We show that for studying character sums it is the sufficient to restrict to reduced polynomials. We start by considering univariate polynomials, and then generalize the definitions and claims to multivariate polynomials.

Definition 36 (Reduced form: univariate polynomials)**.** Let $m(x) = ax^t$ be a monomial. We say m is *reduced* if $p \nmid t$. If $t = p^k r$ for $p \nmid r$ we define the *reduced form* of $m(x)$ to be $m(x)^{p^{n-k}} \equiv a^{p^{n-k}} x^r$. A constant term $c \in \mathbb{F}_{p^n}$ is reduced if $c \in \mathbb{F}_p$, otherwise its reduced form is $\mathrm{Tr}(c) \in \mathbb{F}_p$. We say a polynomial is reduced if all its monomials are reduced, and the reduced form of a polynomial is the sum of the reduced forms of its monomials.

Claim 37 (Equivalence of reduced form: univariate polynomials)*.* Let $f(x)$ be a univariate polynomial over $\mathbb{F}$. Let $f'(x)$ be its reduced form. Then

1. $\mathrm{Tr}(f(x)) \equiv \mathrm{Tr}(f'(x))$.

2. $deg(f') \leq deg(f)$.

3. $wt(f') \leq wt(f)$.

Proof. For a monomial $m(x) = ax^t$ with $t = p^k r$, $p \nmid r$, let $m'(x) = a^{p^{n-k}} x^r$ be its reduced form. Note that $m'(x) = m(x)^{p^{n-k}}$. Since $\mathrm{Tr}(x) = \mathrm{Tr}(x^p)$ we have that $\mathrm{Tr}(m(x)) = \mathrm{Tr}(m'(x))$ for all $x \in \mathbb{F}$. Note that $wt(m') = wt(m)$ and $\deg(m') = r \leq t = \deg(m)$. For a general polynomial $f(x) = \sum m_i(x)$ we have that $f'(x) = \sum m'_i(x)$. Hence we get that $\mathrm{Tr}(f) \equiv \mathrm{Tr}(f')$, and since cancelations among the m'_i can only reduce the degree and weight degree of f', we get that $deg(f') \leq deg(f)$ and $wt(f') \leq wt(f)$. □

Claim 38 (Trace of reduced non-constant polynomial is non-constant: univariate polynomials). Let $f(x)$ be a non-constant reduced univariate polynomial. Then $\mathrm{Tr}(f(x))$ is not constant.

Proof. Assume for contradiction that $\mathrm{Tr}(f(x)) \equiv c$ for some $c \in \mathbb{F}_p$. Let $f(x) = a_0 + \sum_{i \in I} a_i x^i$ where $a_0 \in \mathbb{F}_p$, $a_i \in \mathbb{F}_{p^n}$ for $i \in I$ and $I \subseteq \{0, \ldots, p^n - 1\}$ is nonempty such that $p \nmid i$ for all $i \in I$. Define $g(x) = \mathrm{Tr}(f(x)) - c$. We have that

$$g(x) = -c + \mathrm{Tr}(f(x)) = (a_0 - c) + \sum_{i \in I} \sum_{j=0}^{n-1} a_i^{p^j} x^{ip^j} = (a_0 - c) + \sum_{i \in I} \sum_{j=0}^{n-1} a_i^{p^j} x^{ip^j \pmod{p^n}}.$$

Notice that all the monomials in this representation are distinct, since all $i \in I$ are not divisible by p. Thus this is a non-zero polynomial of degree at most $p^n - 1$, and so it cannot evaluate to zero on all elements of $\mathbb{F}_{p^n}$. □

We now generalize some of the definitions and claims to multivariate polynomials. When we refer to the degree of a multivariate polynomial we always mean is its total degree. The weight degree of a monomial $x_1^{e_1} \ldots x_s^{e_s}$ is the sum of the weight degrees of the variables, that is $wt(x_1^{e_1} \ldots x_s^{e_s}) = wt(x_1^{e_1}) + \ldots + wt(x_s^{e_s})$. The weight degree of a multivariate polynomial is the maximal weight degree of its monomials.

Note 39. As in the univariate case, the weight degree of a multivariate degree is equivalent to its derivative degree, which is defined in an analogous way to the univariate case.

Definition 40 (Reduced form: multivariate polynomials)**.** Let $m(x_1, \ldots, x_s) = ax_1^{e_1} \ldots x_s^{e_s}$ be a monomial. We say m is *reduced* if $p \nmid gcd(e_1, \ldots, e_s)$ (that is, at least one e_i is co-prime to p). If $e_i = p^k r_i$ where $p \nmid gcd(r_1, \ldots, r_s)$ we define the *reduced form* of $m(x_1, \ldots, x_s)$ to be $a^{p^{n-k}} x_1^{r_1} \ldots x_s^{r_s}$. We say a polynomial is reduced if all its monomials are reduced, and the reduced form of a polynomial is the sum of the reduced forms of its monomial.

Claim 41 (Equivalence of reduced form: multivariate polynomials). Let $f(x_1, \ldots, x_s)$ be a multivariate polynomial over $\mathbb{F}$. Let $f'(x_1, \ldots, x_s)$ be its reduced form. Then

1. $\mathrm{Tr}(f(x_1, \ldots, x_s)) \equiv \mathrm{Tr}(f'(x_1, \ldots, x_s))$.
2. $deg(f') \leq deg(f)$.
3. $wt(f') \leq wt(f)$.

Proof. The proof is identical to the proof of Claim 41 for the univariate case. □

Claim 42 (Trace of reduced non-constant polynomial is non-constant: multivariate polynomials). Let $f(x_1, \ldots, x_s)$ be a non-constant reduced multivariate polynomial. Then $\mathrm{Tr}(f(x_1, \ldots, x_s))$ is not constant.

Proof. The proof is very similar to the proof of Claim 38 for the univariate case. If f is not a constant polynomial, that is if I is not empty, then for any $c \in \mathbb{F}_p$ the polynomial $\mathrm{Tr}(f(x_1, \ldots, x_s)) - c$ is a non-zero polynomial of individual degree at most $p^n - 1$ in each variable, and such a polynomial cannot evaluate to zero on all points in $(\mathbb{F}_{p^n})^s$. □

3.1.3 Properties of derivatives

Let $f(x)$ be a univariate polynomial. For every $s \geq 1$ define the s-iterated derivative polynomial of f, $\Delta f(x; y_1, \ldots, y_s)$, to be the multivariate polynomial in variables $x, y_1, \ldots, y_s \in \mathbb{F}$ defined as

$$\Delta f(x; y_1, \ldots, y_s) = f_{y_1,\ldots,y_s}(x) = \sum_{I \subseteq [s]} (-1)^{|I|+s} f(x + \sum_{i \in I} y_i).$$

Derivatives play a crucial role in the proof of Theorem 4. We study in this subsection some of their properties, and prove some structural results on polynomials of the form $\Delta f(x; y_1, \ldots, y_s)$.

Claim 43 (Derivation maintains degree). Let $m(x) = x^t$ be a monomial. Then for any k, all the monomials appearing in $\Delta m(x; y_1, \ldots, y_k)$ have total degree t (or $\Delta m(x; y_1, \ldots, y_k) \equiv 0$).

Proof. The polynomial $\Delta m(x; y_1, \ldots, y_k)$ is a linear combination of $(x + \sum_{i \in I} y_i)^t$ for subsets $I \subseteq [k]$, each of which is homogeneous of degree t. □

We show that the character sum of a polynomial can be bounded by a character sum of its iterated derivatives polynomial.

Claim 44 (Bias can be bounded by bias of derivatives). For any univariate polynomial $f(x)$ and $s \geq 1$

$$\left|\mathbb{E}_{x \in \mathbb{F}}[\omega^{\mathrm{Tr}(f(x))}]\right| \leq \left(\mathbb{E}_{x, y_1, \ldots, y_s \in \mathbb{F}}[\omega^{\mathrm{Tr}(\Delta f(x; y_1, \ldots, y_s))}]\right)^{1/2^s}$$

Proof. Consider first the case $s = 1$. We have

$$\left|\mathbb{E}_{x \in \mathbb{F}}[\omega^{\mathrm{Tr}(f(x))}]\right|^2 = \mathbb{E}_{x, x' \in \mathbb{F}}[\omega^{\mathrm{Tr}(f(x))} \overline{\omega^{\mathrm{Tr}(f(x'))}}] =$$
$$\mathbb{E}_{x, x' \in \mathbb{F}}[\omega^{\mathrm{Tr}(f(x)) - \mathrm{Tr}(f(x'))}] = \mathbb{E}_{x, y \in \mathbb{F}}[\omega^{\mathrm{Tr}(f(x+y)) - \mathrm{Tr}(f(x))}] =$$
$$\mathbb{E}_{x, y \in \mathbb{F}}[\omega^{\mathrm{Tr}(f(x+y) - f(x))}] = \mathbb{E}_{x, y \in \mathbb{F}}[\omega^{\mathrm{Tr}(\Delta f(x; y))}].$$

Hence

$$\left|\mathbb{E}_{x \in \mathbb{F}}[\omega^{\mathrm{Tr}(f(x))}]\right| \leq \left(\mathbb{E}_{x, y \in \mathbb{F}}[\omega^{\mathrm{Tr}(\Delta f(x; y))}]\right)^{1/2}.$$

For $s > 1$ we prove the result by induction. By the base case of $s = 1$ and the Cauchy-Schwartz inequality, we have that

$$\left|\mathbb{E}_{x \in \mathbb{F}}[\omega^{\mathrm{Tr}(f(x))}]\right|^{2^s} \leq \left(\mathbb{E}_{x, y_1 \in \mathbb{F}}[\omega^{\mathrm{Tr}(\Delta f(x; y_1))}]\right)^{2^{s-1}} \leq \mathbb{E}_{y_1 \in \mathbb{F}}\left[\left(\mathbb{E}_{x \in \mathbb{F}}[\omega^{\mathrm{Tr}(\Delta f(x; y_1))}]\right)^{2^{s-1}}\right].$$

For every value of $y_1 \in \mathbb{F}$ we have by the $s - 1$ case that

$$\left(\mathbb{E}_{x \in \mathbb{F}}[\omega^{\mathrm{Tr}(\Delta f(x; y_1))}]\right)^{2^{s-1}} \leq \mathbb{E}_{x, y_2, \ldots, y_s \in \mathbb{F}}[\omega^{\mathrm{Tr}(\Delta f(x; y_1, \ldots, y_s))}],$$

hence we get that

$$\left|\mathbb{E}_{x \in \mathbb{F}}[\omega^{\mathrm{Tr}(f(x))}]\right|^{2^s} \leq \mathbb{E}_{x, y_1, y_2, \ldots, y_s \in \mathbb{F}}[\omega^{\mathrm{Tr}(\Delta f(x; y_1, \ldots, y_s))}].$$

□

We now define a special family of multivariate polynomials that will play an important role in the proof. Such polynomials arise when taking d-iterated derivatives from a polynomial of weight degree d.

Definition 45 (p-multilinear polynomials)**.** A multivariate polynomial $f(x_1, \ldots, x_s)$ over $\mathbb{F}_{p^n}$ is p-multilinear if all its monomials are of the form $x_1^{p^{i_1}} \ldots x_s^{p^{i_s}}$. In particular, if it is nonzero it has weight degree s.

Claim 46 (Structure of derivatives of monomials). Let $m(x) = x^t$ be a monomial of weight degree d. The d-iterated derivatives polynomial $\Delta m(x; y_1, \ldots, y_d)$ of m is given as follows. Let $t = \sum_{j=1}^{k} a_{\ell_j} p^{\ell_j}$ where $1 \leq a_{\ell_1}, \ldots, a_{\ell_k} \leq p-1$ and $\sum a_\ell = d$. Let $\mathcal{S}$ be the family of all partitions of $\{1, \ldots, d\}$ into k subsets of sizes $a_{\ell_1}, \ldots, a_{\ell_s}$, that is

$$\mathcal{S} = \{(S_1, \ldots, S_k) : S_1 \uplus \ldots \uplus S_k = \{1, \ldots, d\}, |S_1| = a_{\ell_1}, \ldots, |S_k| = a_{\ell_k}\}.$$

Then we have

$$\Delta m(x; y_1, \ldots, y_d) = c \sum_{(S_1, \ldots, S_k) \in \mathcal{S}} \prod_{j=1}^{k} \prod_{i \in S_j} (y_i)^{p^{\ell_j}}.$$

where $c = \prod_{j=1}^{k} a_{\ell_j}! \neq 0$ in $\mathbb{F}$. In particular, Δm is a non-zero p-multilinear polynomial in $y_1, \ldots, y_d$ which does not depend on x.

Proof. We have

$$\Delta m(x; y_1, \ldots, y_d) = \sum_{I \subseteq [d]} (-1)^{d+|I|} m(x + \sum_{i \in I} y_i) = \sum_{I \subseteq [d]} (-1)^{d+|I|} (x + \sum_{i \in I} y_i)^t.$$

Substituting $t = \sum a_{\ell_j} p^{\ell_j}$, and using the linearity of the Frobenius map $x \to x^{p^{\ell_j}}$ we get that

$$\Delta m(x; y_1, \ldots, y_d) = \sum_{I \subseteq [d]} (-1)^{d+|I|} \prod_{j=1}^{k} (x^{p^{\ell_j}} + \sum_{i \in I} (y_i)^{p^{\ell_j}})^{a_{\ell_j}}.$$

Since $\sum a_{\ell_j} = d$ we get that Δm is a degree-d polynomial in the Frobenius images of $x, y_1, \ldots, y_d$, i.e. in the monomials $\{x^{p^j}, (y_1)^{p^j}, \ldots, (y_d)^{p^j} : 0 \leq j \leq n-1\}$.

We first claim that Δm does not depend on x, and is p-linear in $y_1, \ldots, y_d$. That is, all the monomials of Δm consist of a product $(y_1)^{p^{j_1}} \ldots (y_d)^{p^{j_d}}$, where $0 \leq j_1, \ldots, j_d \leq n-1$. Otherwise, there exists some monomial in Δm which does not depend on at least one of $y_1, \ldots, y_d$. This is because all monomials of Δm are products of d Frobenius images of $x, y_1, \ldots, y_d$, and by the pigeonhole principle, if either a single variable y_i has two images appearing, or an image of x appears in the monomial, then there must exists a variable y_j not participating in the monomial.

Assume w.l.o.g that Δm contains monomials in which y_1 does not participate. Substituting $y_1 = 0$ in the definition of Δm, since $\Delta f(x; 0) = f(x) - f(x) \equiv 0$ for any polynomial f, we get that

$$\Delta m(x; 0, y_2, \ldots, y_d) \equiv 0.$$

Hence, if there exist monomials in $\Delta m(x; y_1, \ldots, y_d)$ which do not depend on y_1, they are left intact by the substitution $y_1 = 0$, while all monomials depending on y_1 vanish. Thus since $\Delta m(x; 0, y_2, \ldots, y_d) \equiv 0$ all the monomials in $\Delta m(x; y_1, \ldots, y_d)$ must depend on y_1.

We have thus proved that $\Delta m(x; y_1, \ldots, y_d)$ does not depend on x, and is p-linear in $y_1, \ldots, y_d$. To conclude we need to compute the exact form of $\Delta m(x; y_1, \ldots, y_d)$. Any monomial depending on all $y_1, \ldots, y_d$ must come from the term corresponding for $I = \{1, \ldots, d\}$,

$$(x + \sum_{i \in [d]} y_i)^t = \prod_{j=1}^{k} (x^{p^{\ell_j}} + \sum_{i \in [d]} (y_i)^{p^{\ell_j}})^{a_{\ell_j}}.$$

The individual degree of each y_i is some p^{ℓ_j}, and there are exactly a_{ℓ_j} variables among $y_1, \ldots, y_d$ which has individual degree p^{ℓ_j}. Since the number of variables d is exactly the sum $\sum a_{\ell_j}$, all the monomials depending on all of $y_1, \ldots, y_d$ must be of the form $\prod_{j=1}^{k} \prod_{i \in S_j} (y_i)^{p^{\ell_j}}$, where $(S_1, \ldots, S_k) \in \mathcal{S}$ is a partition of $\{1, \ldots, d\}$ into sets of sizes $a_{\ell_1}, \ldots, a_{\ell_k}$. The coefficient of the monomial $\prod_{j=1}^{k} \prod_{i \in S_j} (y_i)^{p^{\ell_j}}$ is equal to the number of times this monomial appears in the last term, which is exactly $\prod_{j=1}^{k} a_{\ell_j}!$. □

Claim 47 (Derivative of reduced monomial is nonzero). Let $m(x)$ be a nonzero reduced monomial of weight degree d. Then $\Delta m(x; y_1, \ldots, y_d)$ is a nonzero reduced polynomial.

Proof. Let $m(x) = x^t$ for $t = \sum a_{\ell_j} p^{\ell_j}$. Since m is reduced we must have $a_0 \neq 0$. By Claim 46 we know that

$$\Delta m(x; y_1, \ldots, y_d) = c \sum_{(S_1, \ldots, S_k) \in \mathcal{S}} \prod_{j=1}^{k} \prod_{i \in S_j} (y_i)^{p^{\ell_j}}.$$

Thus any monomial of $\Delta m(x; y_1, \ldots, y_d)$ contains at least one variable of degree 1, thus it is reduced. □

Claim 48 (Derivative of distinct reduced monomials is distinct). Let $m'(x), m''(x)$ be two distinct monomials of weight degree d. Then $\Delta m'(x; y_1, \ldots, y_d)$ and $\Delta m''(x; y_1, \ldots, y_d)$ are nonzero polynomials which do not share any common monomial.

Proof. Let $m'(x) = x^{t'}$ and $m''(x) = x^{t''}$ for $t' \neq t''$. By Claim 46 we have that $\Delta m'(x; y_1, \ldots, y_d)$ is a nonzero polynomial such that all its monomials have total degree exactly t'. Similarly $\Delta m''(x; y_1, \ldots, y_d)$ is a nonzero polynomial such that all its monomials have total degree exactly t''. Since $t' \neq t''$ the polynomials $\Delta m'(x; y_1, \ldots, y_d)$ and $\Delta m''(x; y_1, \ldots, y_d)$ contain no common monomial. □

Claim 49 (High derivative vanishes). Let $f(x)$ be a polynomial of weight degree at most $d - 1$. Then $\Delta m(x; y_1, \ldots, y_d) \equiv 0$.

Proof. It is enough to prove the claim for monomials. Let $m(x) = x^t$ be some monomial, and let $d' = wt(m) \leq d - 1$ be its weight degree. By Claim 46 we have that $\Delta m(x; y_1, \ldots, y_{d'})$ does not depend on x, thus

$$\Delta m(x; y_1, \ldots, y_{d'}, y_{d'+1}) = \Delta m(x + y_{d'+1}; y_1, \ldots, y_{d'}) - \Delta m(x; y_1, \ldots, y_{d'}) \equiv 0.$$

□

Lemma 50 (Highest non-vanishing derivative). *Let $f(x)$ be a nonzero reduced polynomial of weight degree d. Then $\Delta f(x; y_1, \ldots, y_d)$ is a nonzero reduced polynomial which does not depend on x and is p-linear in $y_1, \ldots, y_d$.*

Proof. Let $f(x) = \sum c_t x^t$. Let $m(x) = c_t x^t$ be some monomial of f. If $wt(m) \leq d-1$ then by Claim 49 we have $\Delta m(x; y_1, \dots, y_d) \equiv 0$. Thus it is enough to consider just the monomials of weight degree exactly d. By Claim 47 the derivative polynomial of each reduced monomial of weight degree d is a reduced polynomial, and these polynomials for two distinct monomials contain no shared monomials, and so cannot cancel each other. Thus the derivative polynomial $\Delta f(x; y_1, \dots, y_d)$ is a nonzero reduced polynomial. By Claim 46 is does not depend on x, and it is p-linear in $y_1, \dots, y_d$. □

Lemma 51 (General non-vanishing derivatives)**.** *Let $f(x)$ be a nonzero reduced polynomial of weight degree d. For any $k \leq d$ the polynomial $\Delta f(x; y_1, \dots, y_k)$ is a nonzero reduced polynomial in $x, y_1, \dots, y_k$.*

Proof. Let $f(x) = \sum c_t x^t$. Let $m(x) = c_t x^t$ be some monomial of f. Observe that all monomials in the polynomial $\Delta m(x; y_1, \dots, y_k)$ have the same total degree t. Thus, if $m(x)$ is reduced then so is $\Delta m(x; y_1, \dots, y_k)$, since if $x^{e_0} y_1^{e_1} \dots y_k^{e_k}$ is a monomial of $\Delta m(x; y_1, \dots, y_k)$ which is not reduced, then $p \mid gcd(e_0, \dots, e_k)$. However $t = e_0 + \ldots + e_k$ and since $m(x)$ is reduced we have that $p \nmid t$. Contradiction, hence $\Delta m(x; y_1, \dots, y_k)$ must be reduced. Hence, we get that if $f(x)$ is a reduced polynomial, then $\Delta f(x; y_1, \dots, y_k)$ is also reduced. To conclude we need to prove that $\Delta f(x; y_1, \dots, y_k)$ is nonzero. Assume by contradiction it is zero; then so is $\Delta f(x; y_1, \dots, y_d) = \sum_{I \subseteq \{k+1, \dots, d\}} (-1)^{|I|+d-k} \Delta f(x + \sum_{i \in I} y_i; y_1, \dots, y_k)$. However by Lemma 50 we know that if f is a nonzero reduced polynomial, then $\Delta f(x; y_1, \dots, y_d)$ is nonzero. Hence also $\Delta f(x; y_1, \dots, y_k)$ must be nonzero. □

3.1.4 Additional claims

We give in this subsection some more claims we will require. The first is the Schwarz-Zippel lemma.

Claim 52 (Schwarz-Zippel). Let $f(x_1, \dots, x_s)$ be a polynomial over $\mathbb{F}$ of total degree e. Then

$$\Pr_{x_1, \dots, x_s \in \mathbb{F}} [f(x_1, \dots, x_s) = 0] \leq \frac{e}{|\mathbb{F}|}.$$

The second result we will need is a theorem of Deligne [12] which is a multivariate analog of Weil's bound.

Theorem 53 (Deligne theorem [12])**.** *Let $f(x_1, \dots, x_s)$ be a multivariate polynomial over $\mathbb{F}$ of degree $|\mathbb{F}|^{1/2-\delta}$. Let $\chi : \mathbb{F} \to \mathbb{C}$ be an additive character. Then either $\chi(f(x_1, \dots, x_s))$ is constant or*

$$|\mathbb{E}_{x_1, \dots, x_s \in \mathbb{F}} [\chi(f(x))]| \leq |\mathbb{F}|^{-\delta}.$$

3.2 The case of high weight g

In this subsection we prove Theorem 4 in the case that g has high weight degree, $\mathrm{wt}(g) \geq d+1$. This is captured by the following lemma, which we prove in this subsection. This is the easier case for Theorem 4.

Lemma 54 (The case of high weight g)**.** *Let $f(x) = g(x) + h(x)$ be a nonzero reduced univariate polynomial over $\mathbb{F}_{p^n}$, where $g(x)$ is a polynomial of degree $|\mathbb{F}|^{1/2-\delta}$ and weight degree at least $d+1$, and $h(x)$ has weight degree at most d. Then*

$$\left| \mathbb{E}_{x \in \mathbb{F}} [\omega^{\mathrm{Tr}(f(x))}] \right| \leq |\mathbb{F}|^{-\frac{\delta}{2^{d+1}}}.$$

Proof. The polynomial f is nonzero reduced and of weight degree at least $d+1$. By Lemma 51 we know that $\Delta f(x; y_1, \ldots, y_{d+1})$ is nonzero and reduced. However, since $\mathrm{wt}(h) \leq d$ we have that $\Delta h(x; y_1, \ldots, y_{d+1}) \equiv 0$ by Claim 49, hence we get that $\Delta f(x; y_1, \ldots, y_{d+1}) = \Delta g(x; y_1, \ldots, y_{d+1})$. Also, since derivation cannot increase total degree, we have that $\deg(\Delta f(x; y_1, \ldots, y_{d+1})) \leq \deg(g) \leq |\mathbb{F}|^{1/2-\delta}$.

So, we have that $f'(x, y_1, \ldots, y_{d+1}) = \Delta f(x; y_1, \ldots, y_{d+1})$ is a nonzero reduced polynomial of degree at most $|\mathbb{F}|^{1/2-\delta}$. By Claim 42 we have that $\mathrm{Tr}(f')$ is a non-constant function. Thus by Deligne's Theorem (Theorem 53) we get that is must be highly unbiased, that is

$$\left|\mathbb{E}_{x, y_1, \ldots, y_{d+1} \in \mathbb{F}}[\omega^{\mathrm{Tr}(f'(x, y_1, \ldots, y_{d+1}))}]\right| \leq |\mathbb{F}|^{-\delta}.$$

To conclude we apply Claim 44 to get that

$$\left|\mathbb{E}_{x \in \mathbb{F}}[\omega^{\mathrm{Tr}(f(x))}]\right| \leq \left|\mathbb{E}_{x, y_1, \ldots, y_{d+1} \in \mathbb{F}}[\omega^{\mathrm{Tr}(f'(x, y_1, \ldots, y_{d+1}))}]\right|^{\frac{1}{2^{d+1}}} \leq |\mathbb{F}|^{-\frac{\delta}{2^{d+1}}}.$$

□

3.3 The case of low weight g

In this subsection we prove Theorem 4 in the case that g has low weight degree, $\mathrm{wt}(g) \leq d$. This is captured by the following lemma, which we prove in this subsection. This is the harder case for Theorem 4.

Lemma 55 (The case of low weight g)**.** *Let $f(x) = g(x) + h(x)$ be a nonzero reduced univariate polynomial over $\mathbb{F}_{p^n}$, where $g(x)$ is a polynomial of degree $|\mathbb{F}|^{1/2-\delta}$ and weight degree at most d, and $h(x)$ has weight degree d and is the sum of k monomials. Then*

$$\mathbb{E}_{x \in \mathbb{F}}[\omega^{\mathrm{Tr}(f(x))}] \leq |\mathbb{F}|^{-\frac{\delta}{d^2 2^d k} + O(1/n)}.$$

To prove Lemma 55 we require some claims.

Claim 56 (Structure of derivative of g). Let $g(x)$ be a polynomial of degree at most $|\mathbb{F}|^{1/2-\delta}$ and weight degree at most d. For $L = \lceil n(1/2 - \delta) \rceil$ there exists a p-multilinear polynomial $u(y_2, \ldots, y_d)$ such that

$$\mathrm{Tr}(\Delta g(x; y_1, \ldots, y_d)) \equiv Tr(y_1^{p^L} \cdot u(y_2, \ldots, y_d)).$$

and such that $\deg(u) \leq p^{2L} \leq |\mathbb{F}|^{1-2\delta+2/n}$.

Proof. By linearity, it suffices to show that for every monomial $m(x)$ appearing in g, there exists a p-multilinear polynomial $u_m(y_2, \ldots, y_d)$ such that $\mathrm{Tr}(\Delta m(x; y_1, \ldots, y_d)) \equiv Tr(y_1^{p^L} \cdot u_m(y_2, \ldots, y_d))$ and $\deg(u_m) \leq p^{2L}$.

Let $m(x) = cx^t$ be such a monomial. If $wt(m) < d$ we have by Claim 49 that $\Delta m(x; y_1, \ldots, y_d) \equiv 0$. Otherwise assume that $\mathrm{wt}(m) = d$. By Claim 46 we know that $\Delta m(x; y_1, \ldots, y_d)$ does not depend on x and is p-multilinear in $y_1, \ldots, y_d$. Moreover, if $t = \sum_{j=1}^{k} a_{\ell_j} p^{\ell_j}$ where $1 \leq a_{\ell_j} \leq p-1$ we know that

$$\Delta m(x; y_1, \ldots, y_d) = \sum_{j=1}^{k} y_1^{p^{\ell_j}} w_j(y_2, \ldots, y_d)$$

where $w_j(y_2,\dots,y_d)$ is a homogeneous p-multilinear polynomial of total degree $t-p^{\ell_j}$. Since $t \le |\mathbb{F}|^{1/2-\delta}$ we have that $\ell_1,\dots,\ell_k \le n(1/2-\delta) \le L$. Thus, taking $u_m(y_2,\dots,y_d)$ to be

$$u_m(y_2,\dots,y_d) = \sum_{j=1}^{k} w_j(y_2,\dots,y_d)^{p^{L-\ell_j}}$$

we get that

$$Tr(y_1^{p^L} \cdot u_m(y_2,\dots,y_d)) \equiv \sum_{j=1}^{k} Tr(y_1^{p^L} w_j(y_2,\dots,y_d)^{p^{L-\ell_j}}) \equiv$$

$$\sum_{j=1}^{k} Tr(y_1^{p^{\ell_j}} w_j(y_2,\dots,y_d)) = \mathrm{Tr}(\Delta m(x;y_1,\dots,y_d)).$$

To conclude we need to bound $\deg(u_m)$. Since $\deg(w_j) \le \deg(m) \le p^{n(1/2-\delta)}$ and $L-\ell_j \le L$ we get that $\deg(u_m) \le \deg(m)\cdot p^L \le p^{2L}$. □

Claim 57 (Structure of derivative of h). Let $h(x)$ be a polynomial of weight degree d which is the sum of k monomials. For every $0 \le L \le n-1$ there exists a p-multilinear polynomial $v(y_2,\dots,y_d)$ such that

$$\mathrm{Tr}(\Delta h(x;y_1,\dots,y_d)) \equiv Tr(y_1^{p^L} \cdot v(y_2,\dots,y_d)).$$

and the number of distinct total degrees of monomials appearing in v is at most kd.

Proof. By linearity, it suffices to show that for every monomial $m(x)$ appearing in h, there exists a p-multilinear polynomial $v_m(y_2,\dots,y_d)$ such that $\mathrm{Tr}(\Delta m(x;y_1,\dots,y_d)) \equiv Tr(y_1^{p^L} \cdot v_m(y_2,\dots,y_d))$ and the monomials appearing in v_m have at most d distinct total degrees.

Let $m(x) = cx^t$ be such a monomial. If $wt(m) < d$ we have by Claim 49 that $\Delta m(x;y_1,\dots,y_d) \equiv 0$. Otherwise assume that $\mathrm{wt}(m) = d$. By Claim 46 we know that $\Delta m(x;y_1,\dots,y_d)$ does not depend on x and is p-multilinear in $y_1,\dots,y_d$. Moreover, if $t = \sum_{j=1}^{k} a_{\ell_j} p^{\ell_j}$ where $1 \le a_{\ell_j} \le p-1$ we know that

$$\Delta m(x;y_1,\dots,y_d) = \sum_{j=1}^{k} y_1^{p^{\ell_j}} w_j(y_2,\dots,y_d)$$

where $w_j(y_2,\dots,y_d)$ is a homogeneous p-multilinear polynomial of total degree $t-p^{\ell_j}$. Let

$$v_m(y_2,\dots,y_d) = \sum_{j=1}^{k} w_j(y_2,\dots,y_d)^{p^{L-\ell_j+n}}$$

where we reduce individual powers of $y_2,\dots,y_d$ modulo p^n (that is, we replace each y_i^e with $y_i^{e \bmod p^n}$, which are equivalent as functions over the field $\mathbb{F}_{p^n}$). Thus we get that

$$Tr(y_1^{p^L} \cdot v_m(y_2,\dots,y_d)) \equiv \sum_{j=1}^{k} Tr(y_1^{p^L} w_j(y_2,\dots,y_d)^{p^{L-\ell_j+n}}) \equiv$$

$$\sum_{j=1}^{k} Tr(y_1^{p^{\ell_j}} w_j(y_2,\dots,y_d)) = \mathrm{Tr}(\Delta m(x;y_1,\dots,y_d)).$$

To conclude we need to bound the number of distinct total degrees of monomials appearing in v_m. Each polynomial w_j is homogeneous, and so also $w_j^{p^{L-\ell_j+n}}$ is homogenous, hence contributing a unique total degree to monomials in v_m. As the number of distinct w_j is bounded by $k \leq d$ we get the required bound. □

Claim 58 (Covering argument for a single element). Let $0 \leq e \leq p^n - 1$ such that $\mathrm{wt}(e) = d$. For $0 \leq s \leq n-1$ define $e_s = e \cdot p^s \bmod p^n$, such that also $0 \leq e_s \leq p^n - 1$. For $a \leq n$ let

$$S = \{0 \leq s \leq n-1 : e_s \geq p^{n-a}\}.$$

Then $|S| \leq a \cdot d$.

Proof. For every $0 \leq e \leq p^n - 1$ let $\vec{e} \in \{0, \dots, p-1\}^n$ denote the vector corresponding to the base-p representation of e, that is $e = \sum_{i=0}^{n-1} \vec{e}(i) p^i$. Observe that $\vec{e}_s$ is just the cyclic shift of $\vec{e}$ by s coordinates, that is $\vec{e}_s(i) = \vec{e}(i - s \pmod n)$. Note that the weight of e is just the hamming weight of $\vec{e}$, and that $e_s \geq p^{n-a}$ if and only if the vector $\vec{e}_s$ contains some nonzero entry in the indices $n-a \leq i \leq n-1$. As $\vec{e}$ contains only d nonzero entries, there are at most $a \cdot d$ cyclic shift of $\vec{e}$ such that some of these entries moves to indices $i \in \{n-a, \dots, n-1\}$. Thus we get that $|S| \leq a \cdot d$. □

Claim 59 (Covering argument for sum of monomials). Let $h(y_1, \dots, y_b)$ be a polynomial over $\mathbb{F}_{p^n}$ of weight degree at most d, such that the number of distinct total degrees of its monomial is z. Let $h_s(y_1, \dots, y_b) = h(y_1, \dots, y_b)^{p^s}$ reducing each individual degree of $y_1, \dots, y_b$ modulo p^n. Then for every a there exists $0 \leq s \leq a$ such that

$$\deg(h_s) < p^{n - \lfloor \frac{a}{dz} \rfloor}.$$

Proof. Let $q = \lfloor \frac{a}{dz} \rfloor$. Let $\{e_1, \dots, e_z\}$ be the set of total degrees occurring in monomials of h. The number of $0 \leq s \leq n-1$ such that $(e_i \cdot p^s \bmod p^n) \geq p^{n-q}$ is bounded by $d \cdot q \leq a/z$ by Claim 58. Thus, there are at most a values for s such that for some e_i we have $e_i \cdot p^s \bmod p^n \geq p^{n-q}$. Since there are $a+1$ possible values for $0 \leq s \leq a$, by the pigeonhole principle there exists a value for which for all $i = 1, \dots, k$,

$$(e_i \cdot p^s \bmod p^n) < p^{n-q}$$

hence we get that $\deg(h_s) < p^{n-q}$. □

Claim 60 (Structure of derivative of f). Let $f(x) = g(x) + h(x)$ be a nonzero reduced univariate polynomial over $\mathbb{F}_{p^n}$, where $g(x)$ is a polynomial of degree $|\mathbb{F}|^{1/2-\delta}$ and weight degree at most d, and $h(x)$ has weight degree d and is the sum of k monomials. Then there exists $M \in \{0, \dots, n-1\}$ and a p-multilinear polynomial $r(y_2, \dots, y_d)$ such that

$$\mathrm{Tr}(\Delta f(x; y_1, \dots, y_d)) \equiv \mathrm{Tr}(y_1^{p^M} \cdot r(y_2, \dots, y_d))$$

and $\deg(r) \leq |\mathbb{F}|^{1 - \frac{2\delta}{d^2 k + 1} + 3/n}$.

Proof. Let $L = \lceil n(1/2 - \delta) \rceil$. By Claim 56 there is a p-multilinear polynomial $u(y_2, \dots, y_d)$ such that $\mathrm{Tr}(\Delta g(x; y_2, \dots, y_d)) \equiv Tr(y_1^{p^L} \cdot u(y_2, \dots, y_d))$ and $\deg(u) \leq p^{2L}$. By Claim 57 there is a p-multilinear polynomial $v(y_2, \dots, y_d)$ such that $\mathrm{Tr}(\Delta h(x; y_2, \dots, y_d)) \equiv Tr(y_1^{p^L} \cdot v(y_2, \dots, y_d))$ and the number of distinct total degrees of monomials in v is bounded by kd.

For s define $r_s(y_2,\dots,y_d) = p^s(u(y_2,\dots,y_d) + v(y_2,\dots,y_d))$ where individual degrees of $y_2,\dots,y_d$ are reduced modulo p^n, and set $a = \alpha n$ to be determined later. We will show there exists $0 \le s \le n-2L-a$ such that $\deg(r_s) \le p^{n-a}$. This will establish the result as for every s,

$$\mathrm{Tr}(\Delta f(x; y_1,\dots,y_d)) \equiv \mathrm{Tr}(y_1^{p^{L+s}} r_s(y_2,\dots,y_d)).$$

First, notice that since $\deg(u) \le p^{2L}$ we have that for any $0 \le s \le n-2L-a$ we have that

$$\deg(u^{p^s}) \le \deg(u)\cdot p^s \le p^{2L+s} \le p^{n-a}.$$

We now move to consider v. By Claim 59 we have that there exists $0 \le s \le n-2L-a$ such that if we let $v_s(y_2,\dots,y_d) = v(y_2,\dots,y_d)^{p^s}$ reducing individual degrees modulo p^n, we have that

$$\deg(v_s) \le p^{n-\lfloor\frac{n-2L-a}{d^2k}\rfloor}.$$

Combining the two bounds, we get that

$$\deg(r_s) \le \max(p^{n-a}, p^{n-\lfloor\frac{n-2L-a}{d^2k}\rfloor}).$$

Setting $a = \lfloor\frac{n-2L-d^2k}{d^2k+1}\rfloor$ to optimize the bound we get that

$$\deg(r_s) \le p^{n-a} \le p^{n(1-\frac{2\delta}{d^2k+1})+3}.$$

□

We are now ready to prove Lemma 55.

Proof of Lemma 55. We will bound the bias of $\mathrm{Tr}(f(x))$ by the bias of $\mathrm{Tr}(\Delta f(x;y_1,\dots,y_d))$. By Claim 44 we have that

$$\left|\mathbb{E}_{x\in\mathbb{F}}[\omega^{\mathrm{Tr}(f(x))}]\right| \le \left|\mathbb{E}_{x,y_1,\dots,y_d\in\mathbb{F}}[\omega^{\mathrm{Tr}(f(x;y_1,\dots,y_d))}]\right|^{1/2^d}.$$

To bound the bias of $\mathrm{Tr}(\Delta f(x;y_1,\dots,y_d))$, we apply Claim 60. We have

$$\mathrm{Tr}(\Delta f(x;y_1,\dots,y_d)) \equiv \mathrm{Tr}(y_1^{p^M}\cdot r(y_2,\dots,y_d))$$

where $\deg(r) \le |\mathbb{F}|^{1-\frac{2\delta}{d^2k+1}+3/n}$. Moreover since f is nonzero and reduced, then by Lemma 50 $\Delta f(x;y_1,\dots,y_d)$ is nonzero, hence $r(y_2,\dots,y_d)$ must also be nonzero.

Whenever $y_2,\dots,y_d$ are such that $r(y_2,\dots,y_d)\ne 0$, we have that $\mathbb{E}_{y_1\in\mathbb{F}}[\omega^{\mathrm{Tr}(y_1^{p^M}\cdot r(y_2,\dots,y_d))}] = 0$ by Claim 35. The probability that $r(y_2,\dots,y_d)=0$ is bounded by Claim 52 by

$$\Pr_{y_2,\dots,y_d\in\mathbb{F}}[r(y_2,\dots,y_d)=0] \le \frac{\deg(r)}{|\mathbb{F}|} \le |\mathbb{F}|^{-\frac{2\delta}{d^2k+1}+3/n}.$$

Combining the results, we get that

$$\left|\mathbb{E}_{x\in\mathbb{F}}[\omega^{\mathrm{Tr}(f(x))}]\right| \le |\mathbb{F}|^{-\frac{2\delta}{(d^2k+1)2^d}+\frac{3}{2^dn}} \le |\mathbb{F}|^{-\frac{\delta}{d^22^dk}+O(1/n)}.$$

□

References

[1] Noga Alon, Tali Kaufman, Michael Krivelevich, Simon Litsyn and Dana Ron, *Testing Low Degree Polynomials Over GF(2)*, Proceedings of 7th International Workshop on Randomization and Computation,(RANDOM), Lecture Notes in Computer Science 2764, 188-199, 2003. Also, IEEE Transactions on Information Theory, Vol. 51(11), 4032-4039, 2005.

[2] Sanjeev Arora and Madhu Sudan. *Improved low degree testing and its applications.* Combinatorica, 23(3): 365-426, 2003.

[3] L. Babai and L. Fortnow and C. Lund, *Non-Deterministic Exponential Time has Two-Prover Interactive Protocols*, Computational Complexity, volume 1, number 1, 3–40, 1991.

[4] J. Bourgain, *Mordell's exponential sum estimate revisited*, J. Amer. Math. Soc., 18(2):477-499 (electronic), 2005.

[5] G. Birkhoff and S. MacLane, *A Survey of Modern Algebra.* third edition, MacMillan, New York, 1965.

[6] Eli Ben-Sasson, Madhu Sudan, *Simple PCPs with poly-log rate and query complexity*, STOC 2005: 266-275.

[7] Eli Ben-Sasson, Madhu Sudan, *Limits on the rate of locally testable affine-invariant codes*, Manuscript, November 2009.

[8] E. Ben-Sasson, M. Sudan, S. Vadhan, A. Wigderson. *Randomness-efficient Low Degree Tests and Short PCPs via Epsilon-Biased Sets* 35th Annual ACM Symposium, STOC 2003, pp. 612-621, 2003.

[9] Blum, M., Luby, M., Rubinfeld, R., *Self-Testing/Correcting with Applications to Numerical Problems*, In J. Comp. Sys. Sci. Vol. 47, No. 3, December 1993.

[10] Andrej Bogdanov and Emanuele Viola, *Pseudorandom bits for polynomials*,In the Proceedings of the 48^{th} Annual IEEE Symposium on Foundations of Computer Science (FOCS '07), pages 41–51, 2007.

[11] L. Carlitz and S. Uchiyama, *Bounds for exponential sums*, Duke Math. J., 24:37-41, 1957.

[12] P. Deligne, *Aplications de la formule des traces aux sommes trigonometriques*, in SGA $4\frac{1}{2}$ Springer Lecture Notes in Math 569, 1978.

[13] Irit Dinur,*The PCP theorem by gap amplification*, J. ACM 54(3): 12 (2007).

[14] Elena Grigorescu, Tali Kaufman and Madhu Sudan, *Succinct Representation of Codes with Applications to Testing*, manuscript.

[15] Oded Goldreich, Madhu Sudan, *Locally testable codes and PCPs of almost-linear length*, J. ACM 53(4): 558-655 (2006).

[16] Charanjit S. Jutla, Anindya C. Patthak, Atri Rudra and David Zukcerman , *Testing low-degree polynomials over prime fields*, Proceedings of the 45th Annual Symposium on Foundations of Computer Science (FOCS), pp. 423-432, 2004.

[17] Tali Kaufman and Simon Litsyn, *Almost Orthogonal Linear Codes are Locally Testable*, FOCS 2005: 317-326.

[18] Tali Kaufman and Shachar Lovett, *The List-Decoding Size of Reed-Muller Codes*, ICS 2010.

[19] Tali Kaufman and Dana Ron, *Testing polynomials over general fields*, Proceedings of the 45th Annual Symposium on Foundations of Computer Science (FOCS), pp. 413-422, 2004.

[20] Tali Kaufman and Madhu Sudan, *Sparse random linear codes are locally decodeable and testable*, FOCS 2007, pp. 590–600.

[21] Tali Kaufman and Madhu Sudan, *Algebraic Property Testing: The Role of Invariance*, Proceedings of the 40th ACM Symposium on Theory of Computing (STOC), 2008.

[22] Swastik Kopparty and Shubhangi Saraf, *Local List-Decoding and Testing of Random Linear Codes from High-Error*, to appear in the Proceedings of STOC 2010.

[23] Shachar Lovett, *Unconditional pseudorandom generators for low degree polynomials*, In the Proceedings of the 40^{th} annual ACM symposium on Theory of computing (STOC '08), pages 557–562, 2008.

[24] F. J. MacWilliams and N. J. A. Sloan, *The Theory of Error Correcting Codes*, North Holland, Amsterdam, 1977.

[25] Or Meir, *Combinatorial Construction of Locally Testable Codes*, proceedings of STOC 2008, pages 285-294.

[26] Ronitt Rubinfeld and Madhu Sudan, *Robust characterizations of polynomials with applications to program testing*, SIAM Journal on Computing, 25(2):252-271, April 1996.

[27] Madhu Sudan *Invariance in Property Testing* ECCC, TR10-051, 2010.

[28] Emanuele Viola, *The sum d of small-bias generators fools polynomials of degree d*, Computational Complexity 18(2):209–217, 2009.

[29] A. Weil, *Sur les courbes algebriques et les varietes qui s'en deduisent*, Actualities Sci. et Ind. no. 1041. Hermann, Paris, 1948.

ECCC ISSN 1433-8092

http://eccc.hpi-web.de