Designs, Codes and Cryptography (2022) 90:2813–2821
https://doi.org/10.1007/s10623-021-00987-0

Further improvement on index bounds

Yansheng Wu[1,2] · Yoonjin Lee[3] · Qiang Wang[4]

Received: 22 January 2021 / Revised: 15 August 2021 / Accepted: 20 November 2021 /
Published online: 4 January 2022

Abstract
In this paper we obtain further improvement of index bounds for character sums of polynomials over finite fields. We present some examples, which show that our new bound is an improved bound compared to both the Weil bound and the index bound given by Wan and Wang. As an application, we give an estimation of the number of all the solutions of some algebraic curves by using our result.

Keywords Index bound · Polynomial · Character sum · Weil bound

Mathematics Subject Classification 11T24

1 Introduction

Let p be a prime number and $\mathbb{F}_q$ be a finite field, where $q = p^m$ for some positive integer m. Let $\psi : \mathbb{F}_q \to \mathbb{C}^*$ be a nontrivial additive character and $f(x) \in \mathbb{F}_q[x]$. The following sums

$$\sum_{x \in \mathbb{F}_q} \psi(f(x))$$

are referred to as the *Weil sums* [6]. Throughout this paper, we always view a polynomial $f(x) \in \mathbb{F}_q[x]$ as a mapping over $\mathbb{F}_q$. In this sense the degree of a polynomial in $\mathbb{F}_q[x]$ should be controlled by $q - 1$ when we consider Weil sums.

This is one of several papers published in *Designs, Codes and Cryptography* comprising the "Special Issue: On Coding Theory and Combinatorics: In Memory of Vera Pless".

Y. Wu was sponsored by the National Natural Science Foundation of China (Grant No. 12101326) and the Natural Science Foundation of Jiangsu Province (Grant No. BK20210575). Y. Lee is a corresponding author and supported by the National Research Foundation of Korea (NRF) Grant funded by the Korea government (MEST)(NRF-2017R1A2B2004574) and also by the Basic Science Research Program through the National Research Foundation of Korea (NRF) funded by the Ministry of Education (Grant No. 2019R1A6A1A11051177). The research of Qiang Wang is partially supported by NSERC of Canada (RGPIN-2017-06410).

✉ Yoonjin Lee
yoonjinl@ewha.ac.kr

Extended author information available on the last page of the article

Given a polynomial $f(x) \in \mathbb{F}_q[x]$ of positive degree n with $\gcd(n, q) = 1$, we have

$$\left| \sum_{x \in \mathbb{F}_q} \psi(f(x)) \right| \leq (n-1)\sqrt{q}. \tag{1.1}$$

The upper bound in (1.1) is well known as the *Weil bound*.

The Weil bound for character sums has many applications in mathematics, theoretical computer science, and information theory etc. The Weil bound is trivial when the degree of the polynomial is bigger than $\sqrt{q}$. Some progress on improvement to the Weil bound has been made as follows.

(1) Using *Deligne's bound* for exponential sums in several variables, Gillot et al. [3,4] provided a new bound for $|\sum_{x \in \mathbb{F}_{q^m}} \psi(f(x))|$ such that for any $b \in \mathbb{F}_{q^m}^*$ the q-degree of $f(x) = bx^d + g(x) \in \mathbb{F}_{q^m}[x]$ only depends on the leading term bx^d; the *q-degree* of a nonzero polynomial f over $\mathbb{F}_{q^m}$ is defined by

$$\deg_q(f) = \max\{d_0 + d_1 + \cdots + d_{m-1} : d \in \mathrm{supp}(f)\},$$

where $d = d_0 + d_1 q + \cdots + d_{m-1} q^{m-1}$ denotes the q-ary expansion of d.

(2) Wan and Wang [7] obtained an index bound for character sums over finite fields; they used the the concept of index of a polynomial over a finite field, which was first introduced in the research of permutation polynomials [1]. This bound improved the Weil bound for high degree polynomials with small indices as well as polynomials with large indices that are generated by cyclotomic mapping of small indices.

(3) Recently, there is an improvement on the Hasse-Weil bound in the characteristic two case by Cramer and Xing [2]. They used the algebraic geometry and the algebraic number theory. As an application, they also improved the Weil bound for character sums.

1.1 Main result and comparison with previous results

The concept of the *index* of a polynomial over a finite field was first introduced in [1].

A polynomial $f(x) \in \mathbb{F}_q[x]$ of degree $n \leq q-1$ can be written as the following form:

$$f(x) = a(x^n + a_{n-i_1} x^{n-i_1} + \cdots + a_{n-i_k} x^{n-i_k}) + b,$$

where $a, a_{n-i_j} \neq 0$, $j = 1, \ldots, k$. Let r be the lowest degree of x in $f(x) - b$. The index l of the polynomial $f(x)$ is defined by

$$l := \frac{q-1}{\gcd(n-r, n-r-i_1, \ldots, n-r-i_{k-1}, q-1)}.$$

In fact, any non-constant polynomial $f(x) \in \mathbb{F}_q[x]$ of degree $n \leq q-1$ can be written uniquely as $f(x) = a(x^r h(x^{(q-1)/l})) + b$.

By using the index of polynomials, Wan and Wang [7] found a new bound, which is called an *index bound*, for character sums of polynomials over finite fields as follows:

Theorem 1.1 [7, Theorem 1.1] *Let $f(x) = x^r h(x^{(q-1)/l}) + b \in \mathbb{F}_q[x]$ be any polynomial with index l. Let ξ be a primitive l-th root of unity in $\mathbb{F}_q$ and $n_0 = \sharp\{0 \leq i \leq l-1 \mid h(\xi^i) = 0\}$. Let $\psi : \mathbb{F}_q \to \mathbb{C}^*$ be a nontrivial additive character. Then*

$$\left| \sum_{x \in \mathbb{F}_q} \psi(f(x)) - \frac{q}{l} n_0 \right| \leq (l - n_0) \gcd\left(r, \frac{q-1}{l}\right) \sqrt{q}. \tag{1.2}$$

This theorem is sensitive to the form of $f(x)$. Replacing $f(x)$ with $f^*(x) = f(x)+d(x)$ such that $\sum_{x\in\mathbb{F}_q}\psi(d(x)) = 0$, and in particular, for $d(x)$ of the form $y^p - y$, leaves the left hand side unchanged but may lower the upper bound in the right hand side.

As mentioned before, we can view a polynomial as a mapping over $\mathbb{F}_q$ when we just consider the Weil sums. Then it is easy to extend the Frobenius mapping π over $\mathbb{F}_q$ to $\mathbb{F}_q[x]$ as follows:

$$\pi : \mathbb{F}_q[x] \to \mathbb{F}_q[x], \pi(a) = a^p, \pi(x) = x^p.$$

There is an equivalence relation between polynomials in $\mathbb{F}_q[x]$. Given two polynomials $f(x) = \sum_i a_i x^i$ and $g(x)$ in $\mathbb{F}_q[x]$, we write $f \sim g$ if there exists a vector $v = (v_0, v_1, \ldots, v_n) \in \mathbb{Z}_m^{n+1}$ such that

$$\pi^v(f) = \pi^{v_0}(a_0) + \pi^{v_1}(a_1 x) + \cdots + \pi^{v_n}(a_n x^n) = g.$$

The equivalence class of $f(x) \in \mathbb{F}_q[x]$ is denoted by $[f]$. For each polynomial $g(x)$ in the equivalence class $[f]$, we use l_g for the index of $g(x)$ and n_g for the degree of $g(x)$. For each equivalence class $[f]$, let l^* be defined by

$$l^* = \min\{l_g : g \in [f]\}.$$

Then there exists a polynomial $f^*(x) \in [f]$ such that $f^*(x) = x^{r^*} h^*(x^{(q-1)/l^*}) + b \in \mathbb{F}_q[x]$ and the index of $f^*(x)$ is exactly l^*. We call $f^*(x)$ the equivalent polynomial of $f(x)$ with the smallest index and $h^*(x)$ the associated polynomial of $f^*(x)$.

The following theorem is our main result, which provides a new formulation of index bounds in Theorem 1.1 for character sums of polynomials over finite fields.

Theorem 1.2 *Let $f(x) \in \mathbb{F}_q[x]$ be a polynomial of positive degree n with $\gcd(n, q) = 1$. Let $f^*(x)$ be the equivalent polynomial of $f(x)$ with the smallest index l^* and $h^*(x)$ the associated polynomial of $f^*(x)$. Let ξ be a primitive l^*-th root of unity in $\mathbb{F}_q$ and $n_0 = \sharp\{0 \le i \le l^* - 1 \mid h^*(\xi^i) = 0\}$. Let $\psi : \mathbb{F}_q \to \mathbb{C}^*$ be a nontrivial additive character. Then*

$$\left| \sum_{x\in\mathbb{F}_q} \psi(f(x)) - \frac{q}{l^*} n_0 \right| \le (l^* - n_0) \gcd\left(r^*, \frac{q-1}{l^*}\right)\sqrt{q}. \tag{1.3}$$

The following examples show that the upper bound in (1.3) is indeed an improved bound compared to both the Weil bound in (1.1) and the index bound in Theorem 1.1.

Example 1.3 Let $f(x) = x^{25} + ax^4 \in \mathbb{F}_{27}[x]$, where $a \in \mathbb{F}_{27}^*$. Obviously, the Weil bound is trivial because of the high degree. Since the index of f is 26, the index bound is also trivial. However, by Theorem 1.2, $l^* = \frac{26}{\gcd(25-12,26)} = 2$. If $a^3 = \pm 1$, then $\left| \sum_{x\in\mathbb{F}_{27}} \psi(x^{25} + ax^4) - \frac{27}{2} \right| \le \sqrt{27}$; otherwise, we have $\left| \sum_{x\in\mathbb{F}_{27}} \psi(x^{25} + ax^4) \right| \le 2\sqrt{27}$.

Example 1.4 Let $f(x) = x^{19} + ax^2 \in \mathbb{F}_{27}[x]$, where $a \in \mathbb{F}_{27}^*$. Obviously, the Weil bound and the index bound are both trivial. By Theorem 1.2, $l^* = 2$. If $a^3 = \pm 1$, then $\left| \sum_{x\in\mathbb{F}_{27}} \psi(x^{19} + ax^2) - \frac{27}{2} \right| \le \sqrt{27}$; otherwise, we have $\left| \sum_{x\in\mathbb{F}_{27}} \psi(x^{19} + ax^2) \right| \le 2\sqrt{27}$.

Similarly, we define

$$n^* = \min\{n_g : g \in [f]\}. \tag{1.4}$$

Then using the Weil bound, the same arguments derives

$$\left| \sum_{x \in \mathbb{F}_q} \psi(f(x)) \right| \leq (n^* - 1)\sqrt{q}. \tag{1.5}$$

The following examples show that the upper bound in (1.5) is also an improved bound when it is compared to the Weil bound in (1.1), the index bound in Theorem 1.1, and the upper bound in (1.3).

Example 1.5 Let $f(x) = x^{19} + ax^4 \in \mathbb{F}_{27}[x]$, where $a \in \mathbb{F}_{27}^*$. Obviously, the Weil bound, the index bound, and the upper bound in (1.3) are all trivial. However, by (1.4) and (1.5), we have $n^* = 5$ and $\left| \sum_{x \in \mathbb{F}_{27}} \psi(x^{19} + ax^4) \right| \leq 4\sqrt{27}$.

Example 1.6 Let $f(x) = x^{10} + ax^5 \in \mathbb{F}_{27}[x]$, where $a \in \mathbb{F}_{27}^*$. Obviously, the Weil bound, the index bound, and the upper bound in (1.3) are all trivial. However, by (1.4) and (1.5), we have $n^* = 5$ and $\left| \sum_{x \in \mathbb{F}_{27}} \psi(x^{10} + ax^5) \right| \leq 4\sqrt{27}$.

The p-cyclotomic coset modulo $q - 1$ containing i is defined by

$$C_i = \{ip^j \pmod{q-1} : 0 \leq j < l_i\},$$

where l_i is the smallest positive integer such that $p^{l_i} i \equiv i \pmod{q-1}$, and is the cardinality of C_i. The smallest integer in C_i is called the *coset leader* of C_i. By [5, Lemma 6], we also find an infinite family of polynomials, which shows that the upper bound in (1.5) is an improved bound.

Proposition 1.7 *Let $q = p^m$, s be an integer with $p < s < \sqrt{q}$, and $\gcd(s, p) = 1$. Let $f(x) = x^{sp^{m-1}} + ax^r \in \mathbb{F}_q[x]$, where $a \in \mathbb{F}_q^*$ and $r < s$. Then $\gcd(sp^{m-1} - q + 1, q) = 1$, $n^* = s$, and $\left| \sum_{x \in \mathbb{F}_q} \psi(f(x)) \right| \leq (s-1)\sqrt{q}$.*

The rest of this paper is organized as follows. In Sect. 2, we prove Theorem 1.2. Our main idea of improving the index bound in [7] is to replace the polynomial over finite fields by using the equivalent polynomial with the smallest index. Those equivalent polynomials are obtained by applying Frobenius automorphisms on individual monomials. In Sect. 3, as an application, we count the number of solutions of some algebraic curves by using our main result.

2 Proof of Theorem 1.2 and corollaries

Let $q = p^m$ as before and $\mathbb{F}_p$ be a subfield of $\mathbb{F}_q$. Let π be the *Frobenius automorphism* of $\mathbb{F}_q$ over $\mathbb{F}_p$, which is defined by $\pi : \mathbb{F}_q \to \mathbb{F}_q, \pi(a) = a^p$. We note that $\pi(a) = a$ if and only if $a \in \mathbb{F}_p$.

Now, we are ready to give the proof of Theorem 1.2.

Proof of Theorem 1.2 We write $f(x) = a_0 + a_1x + \cdots + a_nx^n$ and $\psi = \psi_1(c)$ for some nonzero $c \in \mathbb{F}_q$, where ψ_1 is the *canonical* additive character of $\mathbb{F}_q$. Let $\mathrm{Tr}_{q/p}$ be the trace function from $\mathbb{F}_q$ to $\mathbb{F}_p$. For each $v = (v_0, v_1, \ldots, v_n) \in \mathbb{Z}_m^{n+1}$,

$$\begin{aligned}
&\sum_{x\in\mathbb{F}_q} \psi_1(\pi^v(cf(x)))\\
&= \sum_{x\in\mathbb{F}_q} \psi_1(\pi^{v_0}(ca_0) + \pi^{v_1}(ca_1x) + \cdots + \pi^{v_n}(ca_nx^n))\\
&= \sum_{x\in\mathbb{F}_q} \psi_1((ca_0)^{p^{v_0}} + (ca_1x)^{p^{v_1}} + \cdots + (ca_nx^n)^{p^{v_n}})\\
&= \sum_{x\in\mathbb{F}_q} \zeta_p^{\mathrm{Tr}_{q/p}((ca_0)^{p^{v_0}} + (ca_1x)^{p^{v_1}} + \cdots + (ca_nx^n)^{p^{v_n}})}\\
&= \sum_{x\in\mathbb{F}_q} \zeta_p^{\mathrm{Tr}_{q/p}(ca_0 + ca_1x + \cdots + ca_nx^n)}\\
&= \sum_{x\in\mathbb{F}_q} \psi(f(x)).
\end{aligned}$$

Note that $f(x)$ and $cf(x)$ have the same indices. Taking a vector $v \in \mathbb{Z}_m^{n+1}$ such that $f^*(x) = \pi^v(cf(x))$, the result follows from Theorem 1.1. □

Using the concept of the p-cyclotomic cosets, for binomial polynomials, we obtain the following corollary, which is a simple version of Theorem 1.2. This also improves and corrects an error in Corollary 1.2 in [7].

Corollary 2.1 *Let $f(x) = x^n + ax^r \in \mathbb{F}_q[x]$, where $a \in \mathbb{F}_q^*$ and $1 \le r < n \le q-1$. Let C_r be the p-cyclotomic coset modulo $q-1$ containing r. Suppose that $r^* = rp^k$ for some integer k with $0 \le k \le m-1$ such that*

$$l^* = \frac{q-1}{\gcd(n-r^*, q-1)} = min\left\{\frac{q-1}{\gcd(n-j, q-1)} : j \in C_r\right\}.$$

Let $t = \gcd(n, r, q-1)$. Let $\psi : \mathbb{F}_q \to \mathbb{C}^*$ be a nontrivial additive character. If $x^{n-r^*} + a^{p^k}$ has a solution in $\mathbb{F}_q^*$, then

$$\left|\sum_{x\in\mathbb{F}_q} \psi(x^n + ax^r) - \frac{q}{l^*}\right| \le (l^* - 1)t\sqrt{q}; \tag{2.1}$$

otherwise, we have

$$\left|\sum_{x\in\mathbb{F}_q} \psi(x^n + ax^r)\right| \le l^*t\sqrt{q}. \tag{2.2}$$

Proof By Theorem 1.2, we have

$$l^* = \min\left\{\frac{q-1}{\gcd(i-j, q-1)} : i \in C_n, j \in C_r\right\}.$$

Suppose that $i = np^\alpha$ and $j = rp^\beta$ such that $l^* = \frac{q-1}{\gcd(i-j,q-1)}$. Then $i - j = p^\alpha(n - rp^{\beta-\alpha})$; hence, using Theorem 1.2, the result follows immediately since $\gcd(p, q-1) = 1$. In particular, $n_0 = 1$ if there exists a solution for $x^{n-r^*} + a^{p^k}$. □

In the following corollary, we present some special classes of polynomials for illustration of our main result.

Corollary 2.2 *Let Q be the least prime factor of $q-1$, $n=\frac{q-1}{Q}$, and α be a positive integer. Let $f(x)=x^{n+p^\alpha}+ax\in\mathbb{F}_q[x]$, where $a\in\mathbb{F}_q^*$ and $1<n+p^\alpha\le q-1$. If $x^n+a^{p^\alpha}$ has a solution in $\mathbb{F}_q^*$, then*

$$\left|\sum_{x\in\mathbb{F}_q}\psi(x^{n+p^\alpha}+ax)-\frac{q}{Q}\right|\le(Q-1)\sqrt{q};$$

otherwise, we have

$$\left|\sum_{x\in\mathbb{F}_q}\psi(x^{n+p^\alpha}+ax)\right|\le Q\sqrt{q}.$$

Proof For each integer i with $0\le i\le m-1$, $\gcd(n+p^\alpha-p^i,q-1)$ is a divisor of $q-1$. Since Q is the least prime factor of $q-1$, $\gcd(n,q-1)$ is the largest integer in the set $\{\gcd(n+p^\alpha-p^i,q-1):i=0,1,\ldots,m-1\}$. Hence, we have $l^*=Q$; thus, the result follows from Corollary 2.1. □

Let $n=p_1^{\alpha_1}p_2^{\alpha_2}\cdots p_h^{\alpha_h}$ be the prime factorization, where $p_1,\ldots,p_h$ are distinct primes and α_i are positive integers for $1\le i\le h$. We denote $\mathrm{rad}(n)=p_1p_2\cdots p_h$ and $v_{p_i}(n)=\alpha_i$ for $1\le i\le h$, where v_T denotes the T-adic valuation.

Corollary 2.3 *Let p be an odd prime number and n be an odd positive integer such that $\gcd(n,p-1)=1$ and $2rad(n)=rad(p+1)$. Let $f(x)=x^{n+p}+ax\in\mathbb{F}_{p^2}[x]$, where $a\in\mathbb{F}_{p^2}^*$ and $1<n+p\le p^2-1$. Let $s=\frac{p^2-1}{\gcd(n,p+1)}$. If x^n+a^p has a solution in $\mathbb{F}_{p^2}$, then*

$$\left|\sum_{x\in\mathbb{F}_{p^2}}\psi(x^{n+p}+ax)-\frac{p^2}{s}\right|\le(s-1)p;$$

otherwise, we have

$$\left|\sum_{x\in\mathbb{F}_{p^2}}\psi(x^{n+p}+ax)\right|\le sp.$$

Proof We note that $\gcd(n+p-1,p^2-1)=1$ and $\gcd(n,p^2-1)=\gcd(n,p+1)>1$. Hence, we have $l^*=s<l=p^2-1$. The result thus follows immediately from Corollary 2.1. □

Example 2.4 We present more polynomials $x^n+ax^r\in\mathbb{F}_{p^m}[x]$ where $a\in\mathbb{F}_{p^m}^*$ to illustrate our main result for small primes $p\le5$ as listed in Tables 1, 2 and 3. In the tables, $*$ indicates that the bound is trivial.

3 An application

In this section, as an application of Theorem 1.2, we give an estimation of the number of solutions for some algebraic curves.

Table 1 $p = 2$

m	n	r	Weil bound	Index bound	Our bound
4	13	4	$*$	$*$	12
6	41	5	$*$	56	24
6	43	25	$*$	56	24
6	53	25	$*$	$*$	24
8	57	12	$*$	$*$	80
8	63	3	$*$	$*$	80

Table 2 $p = 3$

m	n	r	Weil bound	Index bound	Our bound
2	7	1	$*$	$*$	6
3	19	2	$*$	$*$	$6\sqrt{3}$
4	44	28	$*$	45	18
4	46	18	$*$	$*$	36
5	154	11	$*$	$*$	$18\sqrt{3}$
6	107	9	$*$	$*$	189
6	122	18	$*$	378	108

Table 3 $p = 5$

m	n	r	Weil bound	Index bound	Our bound
2	14	10	$*$	$*$	20
2	19	11	$*$	15	10
3	33	10	$*$	$*$	$20\sqrt{5}$
3	77	3	$*$	$*$	$10\sqrt{5}$
4	42	10	$*$	$*$	150
4	314	50	$*$	$*$	100

Let $f(x) \in \mathbb{F}_{q^m}[x]$ be a polynomial and N_{f,q^m} be the number of solutions $(x, y) \in \mathbb{F}_{q^m}^2$ of an *Artin–Schreier* equation $y^q - y = f(x)$. Then

$$N_{f,q^m} = \sum_{\psi_m} \sum_{x \in \mathbb{F}_{q^m}} \psi_m(f(x)),$$

where the outer sum runs over all additive characters ψ of $\mathbb{F}_q$ and $\psi_m(x) = \psi(\mathrm{Tr}_{q^m/q}(x))$.

If $f(x)$ has degree n and $\gcd(n, q) = 1$, then we have the well known Weil bound:

$$\left| N_{f,q^m} - q^m \right| \leq (q-1)(n-1)\sqrt{q^m}. \tag{3.1}$$

By Theorem 1.2, we have the following corollary.

Corollary 3.1 *Let $f(x) \in \mathbb{F}_{q^m}[x]$ be a polynomial of degree n with $\gcd(n, q) = 1$. Let N_{f,q^m} be the number of solutions $(x, y) \in \mathbb{F}_{q^m}^2$ of an Artin–Schreier equation $y^q - y = f(x)$. Then we get*

$$\left| N_{f,q^m} - q^m - \frac{(q-1)q^m n_0}{l^*} \right| \leq (q-1)(l^* - n_0) \gcd\left(r^*, \frac{q^m - 1}{l^*}\right)\sqrt{q^m}.$$

Example 3.2 Let $f(x) = x^{13} + ax \in \mathbb{F}_{16^2}[x]$ with $a \in \mathbb{F}_{16^2}^*$. Let $N_{f,16^2}$ be the number of solutions $(x, y) \in \mathbb{F}_{16^2}^2$ of an Artin–Schreier equation $y^{16} - y = f(x)$. Note that the 2-cyclotomic coset C_{13} modulo 255 is given by $C_{13} = \{13, 26, 52, 67, 104, 134\}$. By Corollary 3.1, $l^* = \frac{255}{\gcd(52-1,255)} = 5$. Then we get

$$\left| N_{f,16^2} - 16^2 \right| \leq 15 \cdot 5 \cdot 16,$$

except the case when $x^{51} + a$ has a solution in $\mathbb{F}_{16^2}$, in which case, we have

$$\left| N_{f,16^2} - 16^2 - \frac{15 \cdot 16}{5} \right| \leq 15 \cdot 4 \cdot 16.$$

By Magma program, $N_{f,16^2} = 1024$ if $a^5 = 1$ and $N_{f,16^2} = 256$ otherwise. Despite that the above bounds are not close to the reality for $a^5 \neq 1$, our bounds are still an improvement of (3.1) and the above second bound is pretty good when $a^5 = 1$.

The following corollary is obtained from Corollary 2.2.

Corollary 3.3 *Let Q be the least prime factor of $q^m - 1$ and $n = \frac{q^m-1}{Q}$. Let α and r be two positive integers, and $f(x) = x^{n+p^\alpha} + ax \in \mathbb{F}_{q^m}[x]$, where $a \in \mathbb{F}_{q^m}^*$ and $1 < n + p^\alpha \leq q^m - 1$. Let N_{f,q^m} be the number of solutions $(x, y) \in \mathbb{F}_{q^m}^2$ of an Artin–Schreier equation $y^q - y = f(x)$. If $x^n + a^{p^\alpha}$ has a solution in $\mathbb{F}_{q^m}$, then we get*

$$\left| N_{f,q^m} - q^m - \frac{(q-1)q^m}{Q} \right| \leq (q-1)(Q-1)\sqrt{q^m};$$

otherwise, we have

$$\left| N_{f,q^m} - q^m \right| \leq (q-1)Q\sqrt{q^m}.$$

The following corollary is obtained from Proposition 1.7.

Corollary 3.4 *Let s be an integer with $p < s < \sqrt{q^m}$ and $\gcd(s, p) = 1$. Let $f(x) = x^{sq^m/p} + ax^r \in \mathbb{F}_{q^m}[x]$, where $a \in \mathbb{F}_{q^m}^*$ and $r < s$. Let N_{f,q^m} be the number of solutions $(x, y) \in \mathbb{F}_{q^m}^2$ of an Artin–Schreier equation $y^q - y = f(x)$. Then*

$$\left| N_{f,q^m} - q^m \right| \leq (q-1)(s-1)\sqrt{q^m}.$$

Acknowledgements The authors thank the anonymous reviewers for their helpful suggestions.

References

1. Akbary A., Ghioca D., Wang Q.: On permutation polynomials of prescribed shape. Finite Fields Appl. **15**(2), 195–206 (2009).
2. Cramer R., Xing C.: An improvement to the Hasse-Weil bound and applications to character sums, cryptography and coding. Adv. Math. **309**, 238–253 (2017).
3. Gillot V.: Bounds for exponential sums over finite fields. Finite Fields Appl. **1**(4), 421–436 (1995).
4. Gillot V., Langevin P.: Estimation of some exponential sum by means of q-degree. Glasg. Math. J. **52**(2), 315–324 (2010).

5. Li C.: Hermitian LCD codes from cyclic codes. Des. Codes Cryptogr. **86**(10), 2261–2278 (2018).
6. Lidl R., Niederreiter H.: Finite Fields. Cambridge University Press, Cambridge (2008).
7. Wan D., Wang Q.: Index bounds for character sums of polynomials over finite fields. Des. Codes Cryptogr. **81**(3), 459–468 (2016).

Authors and Affiliations

Yansheng Wu[1,2] · Yoonjin Lee[3] · Qiang Wang[4]

✉ Yoonjin Lee
yoonjinl@ewha.ac.kr

Yansheng Wu
yanshengwu@njupt.edu.cn

Qiang Wang
wang@math.carleton.ca

1 School of Computer Science, Nanjing University of Posts and Telecommunications, Nanjing 210023, People's Republic of China

2 Shanghai Key Laboratory of Trustworthy Computing, East China Normal University, Shanghai 200062, People's Republic of China

3 Department of Mathematics, Ewha Womans University, Seoul 03760, Republic of Korea

4 School of Mathematics and Statistics, Carleton University, Ottawa, ON K1S 5B6, Canada