Cryptography and Communications (2024) 16:879–887
https://doi.org/10.1007/s12095-024-00706-1

RESEARCH

An improvement on Weil bounds for character sums of polynomials over finite fields

Fengwei Li[1] · Fanhui Meng[2] · Ziling Heng[3] · Qin Yue[4]

Received: 7 September 2023 / Accepted: 28 February 2024 / Published online: 6 March 2024

Abstract
Let $\mathbb{F}_q$ be a finite field with q elements, where q is a power of a prime p. In this paper, we obtain an improvement on Weil bounds for character sums associated to a polynomial $f(x)$ over $\mathbb{F}_q$, which extends the results of Wan et al. (Des. Codes Cryptogr. **81**, 459–468, 2016) and Wu et al. (Des. Codes Cryptogr. **90**, 2813–2821, 2022).

Keywords Weil bound · Character sum

Mathematics Subject Classification (2010) 11T24

1 Introduction

Let $\mathbb{F}_q$ be a finite field with q elements, where $q = p^m$, p is a prime and m is a positive integer. The trace function from $\mathbb{F}_q$ onto $\mathbb{F}_p$ is defined by $\mathrm{Tr}_{q/p}(x) = x + x^p + \cdots + x^{p^{m-1}}$, $x \in \mathbb{F}_q$. The canonical additive character of $\mathbb{F}_q$ is defined as follows:

$$\psi_1 : \mathbb{F}_q \longrightarrow \mathbb{C}^*, \psi_1(x) = \zeta_p^{\mathrm{Tr}_{q/p}(x)},$$

✉ Fengwei Li
lfwzzu@126.com

Fanhui Meng
fanhuim99@126.com

Ziling Heng
zilingheng@chd.edu.cn

Qin Yue
yueqin@nuaa.edu.cn

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

2 School of Mathematics and Statistics, Zaozhuang University, Zaozhuang 277160, People's Republic of China

3 School of Science, Chang'an University, Xi'an 710064, People's Republic of China

4 Department of Mathematics, Nanjing University of Aeronautics and Astronautics, Nanjing 211100, People's Republic of China

where $\zeta_p = e^{\frac{2\pi\sqrt{-1}}{p}}$ denotes the p-th primitive root of unity. It is well-known that an arbitrary nontrivial additive character ψ of $\mathbb{F}_q$ can be expressed by $\psi = \psi_1(c)$, $c \in \mathbb{F}_q^*$.

Let $f(x)$ be a polynomial over $\mathbb{F}_q$ of degree n with $\gcd(n, p) = 1$. Define the character sum $S(f, \psi) = \sum_{x\in\mathbb{F}_q} \psi(f(x))$. A well-known result for $S(f, \psi)$ says that

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

The upper bound in (1.1) is called the Weil bound. In general, the bound is tight and cannot be improved except some special families of conditions.

For a positive integer $d \leq q = p^m$, the p-ary expansion of $d = d_0+d_1p+\ldots+d_{m-1}p^{m-1}$, the p-ary weight of d, denoted by $W_p(d)$, is equal to $\sum_{i=0}^{m-1} d_i$. In [6], let $f(x) = ax^d + g(x)$ be a polynomial defined over $\mathbb{F}_q$, where d is the only exponent in the support of $f(x)$ with p-ary weight equal to $\deg_p(f)$ and $\deg_p(f) = \max_{d\in supp(f)}\{W_p(d)\}$, Gillot obtained the Weil bound of $f(x)$ under the assumption $d = 1 + d_r p^r$ with $\gcd(p, d_r) = 1$ is

$$|\sum_{x\in\mathbb{F}_q} \psi(f(x))| \leq (W_p(d) - 1)^m\sqrt{q}.$$

Later, Gillot and Langevin [7] gave a further improvement on this bound.

In [5], let $q = 2^m$, for some positive integer N, suppose that $f(x) = x^c + \sum_{i=1}^{N} \beta^i x^{a_i(2t-1)}$, where $\beta_i \in \mathbb{F}_q$, $t|m$, $\gcd(c, q-1) = 1$, and each a_i is a positive integer, Gangopadhyay obtained that

$$|\sum_{x\in\mathbb{F}_{2^m}} \psi(f(x))| \leq 2^{m-t+1},$$

which improved the Weil bound when $\deg(f(x)) \geq 2^{\frac{m}{2}-t+1} + 1$.

In [15], suppose that $f(x) = x^n$, where $p^{\frac{2}{m}} \leq n \leq p^{\frac{m}{2}+\frac{1}{2}}$, Shparlinski estimated the character sum $\left|\sum_{x\in\mathbb{F}_q} \psi(x^n)\right|$; later, Bourgain and Chang in [2] also obtained a nontrivial estimate of $\left|\sum_{x\in\mathbb{F}_q} \psi(x^n)\right|$ under the assumption $\gcd(n, \frac{q-1}{p^v-1}) < p^{-v}q^{1-\varepsilon}$, where $q = p^m$, $1 \leq v < m$,$v|m$, and $\varepsilon > 0$, which extended the results of Bourgain et al. in [3].

Furthermore, there are a lot of attentions on improving the Weil bound for the Artin-Schreier curves, that is $y^q - y = f(x)$ for $(x, y) \in \mathbb{F}_{q^m}^2$, because of their applications in coding theory and computer sciences, which are referred as [4, 9, 13, 14] and therein. About character sums for polynomials, there are a lot of papers to investigate them and presented their applications in cryptography radar and wireless communication systems. Wu et al. in [22] computed the cross correlation distributions of a p-ary m-sequence for several decimations with $d = \frac{q-1}{p^m}$ in case of $p = 2$ and $p = 3$. Li and Wu et al. in [10, 12, 20, 21] gave some low valued Walsh spectrums of monomial functions. Heng et al. in [8, 11] constructed two families of linear codes with a few weights based on special polynomials over finite fields and some near MDS codes which are optimal locally recoverable codes.

In [18], for character sums associated to a polynomial $f(x)$ over $\mathbb{F}_q$, Wan and Wang presented a new bound, which is called an index bound. They improved the Weil bound for high degree polynomials with small indices. The idea was to use monomial bounds over each cyclotomic cosets because each polynomial can be presented as a cyclotomic mapping. Recently, the index bound was slightly improved by Wu et al. in [19] by using the least index obtained from all possible conjugated exponents of the polynomial $f(x)$.

In this paper, let $\mathbb{F}_q$ be a finite field, where $q = p^m$ and p is a prime. Let ψ be an arbitrary nontrivial additive character of $\mathbb{F}_q$. For an arbitrary polynomial $f(x) \in \mathbb{F}_q[x]$, we investigate the Weil bound of character sum $\sum_{x\in\mathbb{F}_q} \psi(f(x))$ associated to $f(x)$ by considering all possible conjugated exponents of $f(x)$ and present an improved upper bound compared to the results of Wan et al. in [18] and Wu et al. in [19].

2 An improvement of Weil bound for character sums of polynomials

In this section, we always assume that $\mathbb{F}_q$ is a finite field, where $q = p^m$, p is a prime, and m is a positive integer. Let γ be a primitive element of $\mathbb{F}_q$, i.e., $\mathbb{F}_q^* = \langle\gamma\rangle$ and l, s two positive integers with $ls = q - 1$, then we define the cyclotomic cosets of order l in $\mathbb{F}_q$ as follows:

$$C_i = \gamma^i \langle\gamma^l\rangle, i = 0, 1, \ldots, l-1,$$

where $C_0 = \langle\gamma^l\rangle$ is a cyclic subgroup of $\mathbb{F}_q^*$ generated by γ^l.

For any $a_0, a_1, \cdots, a_{l-1} \in \mathbb{F}_q$ and a positive integer r, Wang [16] defined the r-th order cyclotomic mapping $f^r_{a_0,a_1,\cdots,a_{l-1}}$ of index l from $\mathbb{F}_q$ to itself:

$$f^r_{a_0,a_1,\cdots,a_{l-1}} = \begin{cases} 0 & \text{if } x = 1, \\ a_i x^r & \text{if } x \in C_i, i = 0, 1, \cdots, l-1. \end{cases}$$

It is shown that the r-th order cyclotomic mappings of index l produce the polynomials of the form $f(x) = x^r h(x^{\frac{q-1}{l}})$. More generally any nonconstant polynomial $f(x)$ with degree $\leq q-1$ over $\mathbb{F}_q$ such that $f(0) = a_0$ can be written uniquely as $f(x) = x^r h(x^{\frac{q-1}{l}}) + a_0$ with some positive integers r, l such that $l|(q-1)$. We call l the index of $f(x)$ (see [1, 17]).

Let $Gal(\mathbb{F}_q/\mathbb{F}_p)$ be the Galois group of $\mathbb{F}_q$ over $\mathbb{F}_p$, it is clear that

$$Gal(\mathbb{F}_q/\mathbb{F}_p) = \langle\sigma\rangle = \{1, \sigma, \sigma^2, \ldots, \sigma^{m-1}\},$$

where $\sigma : c \mapsto c^p$ is an automorphism of $\mathbb{F}_q$, which is called Frobenius automorphism of $\mathbb{F}_q$ over $\mathbb{F}_p$. A well-known fact is that $\sigma(c) = c$ if and only if $c \in \mathbb{F}_p$. We extend σ to a map $\tilde{\sigma}$ of $\mathbb{F}_q[x]$: $f(x) \mapsto (f(x))^p$, where $f(x)$ is an arbitrary polynomial over $\mathbb{F}_q$.

In the following, we always assume that

$$f(x) = a_{r_k}x^{r_k} + a_{r_{k-1}}x^{r_{k-1}} + \ldots + a_{r_1}x^{r_1} + a_0 \in \mathbb{F}_q[x], \tag{2.1}$$

where $q - 1 \geq r_k > r_{k-1} > \cdots > r_1 \geq 1$ and $a_{r_i} \neq 0, i = 1, 2, \ldots, k$. Denote $r = r_1$. Then

$$f(x) = x^r h(x^{\frac{q-1}{l}}) + a_0,$$

and the index l of $f(x)$ is

$$l = \frac{q-1}{\gcd(r_k - r, r_{k-1} - r, \cdots, r_2 - r, q-1)}.$$

Lemma 2.1 [18] *Let $f(x) = x^r h(x^{\frac{q-1}{l}}) \in \mathbb{F}_q[x]$ be a polynomial with the index l. Let $n_0 = \sharp\{i, 0 \leq i \leq l-1 : h(\zeta^i) = 0\}$, where ζ is a primitive l-th root of unity in $\mathbb{F}_q$. For a nontrivial additive character ψ of $\mathbb{F}_q$,*

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

Let $f(x)$ be given in (2.1). Define a transformation of $\mathbb{F}_q[x]$:

$$\begin{aligned} \mathbb{F}_q[x] &\longrightarrow \mathbb{F}_q[x] \\ \phi : f(x) &\longmapsto \phi(f(x)), \end{aligned} \tag{2.2}$$

where

$$\begin{aligned} \phi(f(x)) &= \tilde{\sigma}^{v_k}(a_{r_k}x^{r_k}) + \ldots + \tilde{\sigma}^{v_1}(a_{r_1}x^{r_1}) + \sigma^{v_0}(a_0) \\ &= a_{r_k}^{p^{v_k}} x^{r_k p^{v_k}} + \ldots + a_{r_1}^{p^{v_1}} x^{r_1 p^{v_1}} + a_0^{p^{v_0}}, \end{aligned}$$

$0 \le v_i \le m-1, i = 0, 1, 2, \ldots, k$.

For $x \in \mathbb{F}_q$, let $\mathrm{Tr}_{q/p}(x)$ be the absolute trace of x over $\mathbb{F}_p$, then $\mathrm{Tr}_{q/p}(\phi(f(x))) = \mathrm{Tr}_{q/p}(f(x))$. For convenience, let ψ be the canonical additive character of $\mathbb{F}_q$. Then

$$\begin{aligned} \sum_{x\in\mathbb{F}_q} \psi(f(x)) &= \sum_{x\in\mathbb{F}_q} \zeta_p^{\mathrm{Tr}_{q/p}(f(x))} \\ &= \sum_{x\in\mathbb{F}_q} \zeta_p^{\mathrm{Tr}_{q/p}(\phi(f(x)))} \\ &= \sum_{x\in\mathbb{F}_q} \psi(\phi(f(x))). \end{aligned} \tag{2.3}$$

In fact, for an arbitrary nontrivial additive character of $\mathbb{F}_q$, (2.3) holds. Hence, Wu et al. [19] obtained the following result, which is an improvement of Lemma 2.1.

Lemma 2.2 [19] *The notations are as above. Suppose that l^* is the least index of $\phi(f(x))$ and $\phi(f(x)) = x^{r^*}h(x^{\frac{q-1}{l^*}})$. Let $n_0 = \sharp\{i, 0 \le i \le l^*-1 : h(\zeta^i) = 0\}$, where ζ is a primitive l^* root of unity in $\mathbb{F}_q$. Then*

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

In this paper, we shall generalize Lemma 2.2 to get improved bound for character sums of $f(x)$. In order to investigate the bound for character sum of polynomial $f(x)$, we consider the set of all positive divisors of $q-1$:

$$D = \{d \in \mathbb{N} : d|(q-1)\}.$$

Let $f(x) = \sum_{i=1}^{k} a_{r_i}x^{r_i} + a_0$ be defined as (2.1). Fix a $d \in D$ and $ds = q-1$. Then by division algorithm,

$$\begin{aligned} r_i &= sq_0^{(d,i)} + r_0^{(d,i)}, \\ pr_i &= sq_1^{(d,i)} + r_1^{(d,i)}, \\ &\cdots \\ p^{m-1}r_i &= sq_{m-1}^{(d,i)} + r_{m-1}^{(d,i)}, \end{aligned} \tag{2.4}$$

where $0 \le r_0^{(d,i)}, \ldots, r_{m-1}^{(d,i)} \le s-1$.

Let

$$\begin{aligned} R_{d,i} &= \{r_0^{(d,i)}, r_1^{(d,i)}, \ldots, r_{m-1}^{(d,i)}\}, i = 1, 2, \ldots, k, \\ r^{(d,i)} &= \min\{\gcd(s, r_j^{(d,i)}) : 0 \le j \le m-1\}, i = 1, \ldots, k, \end{aligned}$$

and

$$T_d = \{r^{(d,i)} : i = 1, \ldots, k\}.$$

Without loss of generality, let $t = |T_d|$,

$$T_d = \{r^{(d,1)}, \ldots, r^{(d,t)}\}, \tag{2.5}$$

and $r^{(d,1)} < r^{(d,2)} < \cdots < r^{(d,t)}$.

By (2.5), there exists a transformation ϕ_d of $\mathbb{F}_q[x]$ defined as (2.2) such that

$$\phi_d(f(x)) = \sum_{j=1}^{t} x^{r^{(d,j)}} h_j(x^s) + b,$$

where $b \in \mathbb{F}_q$ and $h_j(x^s)$ is a polynomial of x^s over $\mathbb{F}_q$. In the following, we present our main result in Theorem 2.3.

Theorem 2.3 *Let $d \in D$ and $sd = q-1$. Let γ be a primitive element of the finite field $\mathbb{F}_q$ and $\zeta = \gamma^s$ be a fixed primitive d-th root of unity in $\mathbb{F}_q$. Let $f(x)$ be defined as (2.1) and T_d be given by (2.5). Let ϕ_d be the transformation of $\mathbb{F}_q[x]$ such that $\phi_d(f(x)) = \sum_{j=1}^{t} x^{r^{(d,j)}} h_j(x^s)+b$, where $b \in \mathbb{F}_q$ and $t = |T_d|$. Let*

$$I_d = \{i : 0 \le i \le d-1 \text{ and } h_j(\zeta^i) \ne 0 \text{ for some } j, 1 \le j \le t\}$$

and $n_{d,0} = d - |I_d|$. Then for each $d \in D$,

$$\left|\sum_{x\in\mathbb{F}_q} \psi(f(x))\right| \le (d - n_{d,0})\sqrt{q}(r^{(d,t)} - \frac{1}{d}) + \frac{q}{d} n_{d,0}.$$

Moreover, if d runs over all positive factors of $q-1$, then

$$\left|\sum_{x\in\mathbb{F}_q} \psi(f(x))\right| \le \min_{d\in D}\{(d - n_{d,0})\sqrt{q}(r^{(d,t)} - \frac{1}{d}) + \frac{q}{d} n_{d,0}\}.$$

Proof Take a $d \in D$ and $ds = q-1$, let

$$\phi_d(f(x)) = \sum_{j=1}^{t} x^{r^{(d,j)}} h_j(x^s) + b,$$

$C_0 = \langle \gamma^d \rangle$ be a subgroup of $\mathbb{F}_q^*$ of index d, and $\mathbb{F}_q^* = \cup_{i=0}^{d-1} \gamma^i C_0$.

Let

$$I_d = \{i : 0 \le i \le d-1 \text{ and } h_j(\zeta^i) \ne 0 \text{ for some } j, 1 \le j \le t\}$$

be a subset of $\{0, 1, \ldots, d-1\}$. Then

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

$$= 1 + \sum_{i=0}^{d-1}\sum_{x\in C_0}\psi(\phi_d(f(\gamma^i x)) - b)$$

$$= 1 + \frac{1}{d}\sum_{i=0}^{d-1}\sum_{x\in\mathbb{F}_q^*}\psi(\phi_d(f(\gamma^i x^d)) - b)$$

$$= 1 + \frac{1}{d}\sum_{i=0}^{d-1}(\sum_{x\in\mathbb{F}_q^*}\psi(\sum_{j=1}^{t} x^{dr^{(d,j)}}\gamma^{ir^{(d,j)}}h_j(\zeta^i)))$$

$$= 1 + \frac{1}{d}\sum_{i\in I_d}(\sum_{x\in\mathbb{F}_q^*}\psi(\sum_{j=1}^{t} x^{dr^{(d,j)}}\gamma^{ir^{(d,j)}}h_j(\zeta^i))) + \frac{q-1}{d}n_{d,0}$$

$$= \frac{1}{d}\sum_{i\in I_d}(\sum_{x\in\mathbb{F}_q}\psi(\sum_{j=1}^{t} x^{dr^{(d,j)}}\gamma^{ir^{(d,j)}}h_j(\zeta^i))) + \frac{q}{d}n_{d,0}.$$

Furthermore,

$$\begin{aligned}
&\left|\sum_{x\in\mathbb{F}_q}\psi(\phi_d(f(x)) - b)\right| \\
&\leq \frac{1}{d}\sum_{i\in I_d}\left|(\sum_{x\in\mathbb{F}_q}\psi(\sum_{j=1}^{t} x^{dr^{(d,j)}}\gamma^{ir^{(d,j)}}h_j(\zeta^i)))\right| + \frac{q}{d}n_{d,0} \\
&\leq \frac{d-n_{d,0}}{d}\{\gcd(dr^{(d,t)}, q-1) - 1\}\sqrt{q} + \frac{q}{d}n_{d,0} \\
&\leq (d-n_{d,0})\sqrt{q}(r^{(d,t)} - \frac{1}{d}) + \frac{q}{d}n_{d,0}, \qquad (2.6)
\end{aligned}$$

note that

$$\psi(\phi_d(f(x)) - b) = \psi(-b)\psi(\phi_d(f(x))),$$

where $|\psi(-b)| = 1$. Recall that $\sum_{x\in\mathbb{F}_q}\psi(f(x)) = \sum_{x\in\mathbb{F}_q}\psi(\phi(f(x)))$, then

$$\left|\sum_{x\in\mathbb{F}_q}\psi(f(x))\right| \leq (d-n_{d,0})\sqrt{q}(r^{(d,t)} - \frac{1}{d}) + \frac{q}{d}n_{d,0}.$$

Moreover, if d runs over all positive divisors of $q-1$, then

$$\left|\sum_{x\in\mathbb{F}_q}\psi(f(x))\right| \leq \min_{d\in D}\{(d-n_{d,0})\sqrt{q}(r^{(d,t)} - \frac{1}{d}) + \frac{q}{d}n_{d,0}\}.$$

□

In fact, we may obtain an improved upper bound than one in (2.6). In Theorem 2.3, if $d \in D$ is fixed and $|T_d| = 1$, then a generalized form of Lemma 2.2 in [19] is obtained immediately.

Corollary 2.4 *Let $f(x)$ be defined as (2.1), d, s two positive integers with $ds = q-1$, and $T_d = \{r^{(d,1)}\}$ with $r^{(d,1)} > 0$. Let ϕ_d be the transformation of $\mathbb{F}_q[x]$ such that $\phi_d(f(x)) =$*

$x^{r^{(d,1)}}h(x^s)$. *Let* γ *be a primitive element of the finite field* $\mathbb{F}_q$ *and* $\zeta = \gamma^s$ *be a fixed primitive* d*-th root of unity in* $\mathbb{F}_q$. *Let* $I_d = \{i : 0 \le i \le d-1 \text{ and } h(\zeta^i) = 0\}$ *and* $n_{d,0} = |I_d|$. *Then*

$$\left|\sum_{x\in\mathbb{F}_q}\psi(f(x)) - \frac{q}{d}n_{d,0}\right| \le (d - n_{d,0})(r^{(d,1)} - \frac{1}{d})\sqrt{q}.$$

Remark 2.5 *In Theorem 2.3, the Weil bound of character sum associated to an arbitrary polynomial* $f(x)$ *depends on* $d \in D$, $n_{d,0}$, *and* $r^{(d,t)}$. *The Weil bound in Theorem 2.3 is much better than the ones of Lemmas 2.1 and 2.2. In fact, the bound for character sum of* $f(x)$ *in Lemma 2.2 presented by Wu et al. in* [19] *is a special case of Corollary 2.4.*

In the following, we give some examples to show that the Weil bound for character sums of $f(x)$ in Theorem 2.3 is indeed an improved bound compared to the bounds in (1.1), Lemmas 2.1 and 2.2.

Example 2.6 *Let* $q = 5^2$ *and* $f(x) = x^{19} + x^{11} + x^5 \in \mathbb{F}_q[x]$. *The Weil bound in* (1.1) *is trivial because of the high degree. The bound in Lemma 2.1 is also trivial since the index of* $f(x)$ *is* 12.

In Lemma 2.2, the least index of $\phi(f(x))$ *is*

$$d^* = \frac{24}{\gcd(23-5, 11-5, 24)} = 4$$

and $\phi(f(x)) = x^5((x^6)^3 + x^6 + 1)$. *Then the bound for character sums of* $f(x)$ *in Lemma 2.2 is*

$$|\sum_{x\in\mathbb{F}_q}\psi(f(x))| \le 20.$$

In Theorem 2.3, $D = \{d : d|24\} = \{2, 3, 4, 6, 8, 12\}$.

(i) *For* $d = 2$, *we have* $R_{2,1} = \{1, 5\}$ *and* $R_{2,2} = R_{2,3} = \{7, 11\}$. *Let* $T_2 = \{1, 7\}$, *there exists the transformation* ϕ_2 *of* $\mathbb{F}_q[x]$ *such that* $\phi_2(f(x)) = x^7((x^{12})^4 + x^{12}) + x(x^{12})^2$, *then* $|\sum_{x\in\mathbb{F}_q}\psi(f(x))| \le 10$.

(ii) *For* $d = 3$, *we have* $R_{3,1} = R_{3,2} = R_{3,3} = \{1, 5\}$. *Let* $T_3 = \{5\}$, *there exists the transformation* ϕ_3 *of* $\mathbb{F}_q[x]$ *such that* $\phi_3(f(x)) = x^5((x^6)^{15} + (x^6) + 1)$, *then* $|\sum_{x\in\mathbb{F}_q}\psi(f(x))| \le 20$.

(iii) *For* $d = 4$, *we have* $R_{4,1} = \{1, 5\}$ *and* $R_{4,2} = R_{4,3} = \{3, 7\}$. *Let* $T_4 = \{1, 3\}$, *there exists the transformation* ϕ_4 *of* $\mathbb{F}_q[x]$ *such that* $\phi_4(f(x)) = x^3((x^8)^2 + (x^8)) + x((x^8)^3)$, *then* $|\sum_{x\in\mathbb{F}_q}\psi(f(x))| \le 15$. *Similarly, for other* $d \in D$, *the bounds of* $f(x)$ *are larger than the above cases. Hence by Theorem 2.3, the bound for character sums of* $f(x)$ *is*

$$\left|\sum_{x\in\mathbb{F}_q}\psi(f(x))\right| \le \min\{10, 15, 20\} = 10.$$

Example 2.7 *Let* $f(x) = x^{19} + ax^4 \in \mathbb{F}_{27}[x]$, *where* $a \in \mathbb{F}_{27}^*$. *The bounds given by* (1.1), *Lemmas 2.1 and 2.2 are all trivial. Another upper bound for exponential sums of* $f(x)$ *presented by Wu et al. in* [19, Example 1.5] *is* $|\sum_{x\in\mathbb{F}_{27}}\psi(f(x))| \le 4\sqrt{27}$.

In Theorem 2.3, take $d = 2$, *we have* $R_{2,1} = \{4, 12, 10\}$, $R_{2,2} = \{6, 5, 2\}$, *and* $T_2 = \{4, 2\}$, *there exists the map* ϕ_2 *of* $\mathbb{F}_{27}[x]$ *such that* $\phi_2(f(x)) = x^2((x^s)^{13}) + cx^4$, *by Theorem 2.3,* $|\sum_{x\in\mathbb{F}_{27}}\psi(f(x))| \le 2\sqrt{27}$.

Example 2.8 *Let* $f(x) = x^{10} + ax^5 \in \mathbb{F}_{27}[x]$*, where* $a \in \mathbb{F}_{27}^*$*. The bounds given by* (1.1)*, Lemmas 2.1 and 2.2 are all trivial. Another upper bound for exponential sums of* $f(x)$ *presented by Wu et al. in* [19, Example 1.6] *is* $|\sum_{x\in\mathbb{F}_{27}} \psi(f(x))| \le 4\sqrt{27}$.

In Theorem 2.3, take $d = 2$*, we have* $R_{2,1} = \{5, 2, 4\}$*,* $R_{2,2} = \{10, 4, 6\}$*, and* $T_2 = \{4\}$*, there exists the map* ϕ_2 *of* $\mathbb{F}_q[x]$ *such that* $\phi_2(f(x)) = x^4((x^s)^2 + c(x^s)^2)$*, by Theorem 2.3,* $|\sum_{x\in\mathbb{F}_q} \psi(f(x))| \le 2\sqrt{27}$.

From the above examples one sees that the bound we obtained is indeed an improvement compared to that Wan and Wu et al. in [18] and [19].

3 Concluding remarks

This paper mainly studied the Weil bounds for character sums associated to an arbitrary polynomial $f(x)$ over a finite field $\mathbb{F}_q$. The result of Theorem 2.3 presented an improved upper bound than the results of Wan and Wu et al. in [18] and [19], respectively.

Acknowledgements The authors are very grateful to the reviewers and the Editor for their valuable suggestions that much improved the quality of this paper.

Author Contributions F. Li and F. Meng wrote the main manuscript text and Z. Heng and Q. Yue gave examples. All authors reviewed the manuscript.

Funding The paper was supported by National Natural Science Foundation of China under Grants 12171420, 62172219, 12271059, Natural Science Foundation of Shandong Province under Grant ZR2021MA046, Natural Science Research Start up Foundation of Recruiting Talents of Nanjing University of Posts and Telecommunications (Grant No.NY223199), and the Fundamental Research Funds for the Central Universities, CHD, under Grant 300102122202.

Declarations

Competing interests The authors declare no competing interests.

References

1. Akbary, A., Ghioca, D., Wang, Q.: On permutation polynomials of prescribed shape. Finite Fields Appl. **15**, 195–206 (2009)
2. Bourgain, J., Chang M.C.: A Gauss sum estimate in arbitrary finite fields. C. R. Math. Acad. Sci. Paris, Ser. I, vol. 342, no. 9, pp. 643–646, (2006)
3. Bourgain, J., Glibichuk, A.A., Konyagin, S.V.: Estimates for the number of sums and products and for exponential sums in fields of prime order. J. Lond. Math. Soc. **73**(2), 380–398 (2016)
4. Cramer, R., Xing, C.: An improvement to the Hasse-Weil bound and applications to character sums. Adv. Math. **309**, 238–253 (2017)
5. Gangopadhyay, S.: A note on character sums with polynomial arguments. Finite Fields Appl. **9**(4), 449–457 (2003)
6. Gillot, V.: Bounds for exponential sums over finite fields. Finite Fields Appl. **1**(4), 421–436 (1995)
7. Gillot, V., Langevin, P.: Estimation of some exponential sum by means of q-degree. Glasg. Math. J. **52**(2), 315–324 (2010)
8. Heng, Z., Wang, X., Li, X.: Constructions of cyclic codes and extended primitive cyclic codes with their applications. Finite Fields Appl. **89**, 102208 (2023)
9. Kaufman, T., Lovett, S.: New Extension of the Weil Bound for Character Sums with Applications to Coding. In: Proc. 2011 IEEE 52nd Annual symposium on foundations of computer science (FOCS), Palm Springs, California, USA, pp. 788–796, 2011

10. Li, F.: Several classes of exponential sums and three-valued Walsh spectrums over finite fields. Finite Fields Appl. **87**, 102142 (2023)
11. Li, X., Heng, Z.: Constructions of near MDS codes which are optimal locally recoverable codes. Finite Fields Appl. **88**, 102184 (2023)
12. Li, F., Wu, Y., Yue, Q.: Evalutions on Moisio's type exponential sums. Scientia Sinica Mathe. **51**(10), 1627–1634 (2021)
13. Mullen, G.L., Wan, D., Wang, Q.: An index bound on value sets of polynomial maps over finite fields. Appl. Algebra Number Theory, pp. 23–27. Cambridge University Press, United Kingdom (2014)
14. Rojas-Leon, A., Wan, D.: Improvements of the Weil bound for Artin-Schreier curves. Math. Ann. **351**, 417–442 (2011)
15. Shparlinski, I.E.: Bounds of Gauss sums in finite fields. Proc. Am. Math. Soc. **132**(10), 2817–2824 (2004)
16. Wang, Q.: Cyclotomic mapping permutation polynomials over finite fields. In: Sequences subsequences, and consequences (international workshop, SSC 2007, Los Angeles, May 31-June 2, 2007). Lecture Notes in Computer Science, vol. 4893, pp. 119–128. Springer, Berlin (2007)
17. Wang, Q.: Cyclotomy and permutation polynomials of large indices. Finite Fields Appl. **22**, 57–69 (2013)
18. Wan, D., Wang, Q.: Index bounds for character sums of polynomials over finite fields. Des. Codes Cryptogr. **81**, 459–468 (2016)
19. Wu, Y., Lee, J., Wang, Q.: Further improvement on index bounds. Des. Codes Cryptogr. **90**, 2813–2821 (2022)
20. Wu, Y., Yue, Q., Li, F.: Three families of monomial functions with three-valued Walsh spectrum. IEEE Trans. Inf. Theory **65**(5), 3304–3314 (2019)
21. Wu, Y., Yue, Q., Li, F.: More functions with three-valued Walsh transformation from linear combinations. IEEE Commun. Lett. **23**(4), 564–567 (2019)
22. Wu, Y., Yue, Q., Shi, X., Zhu, X.: Binary and ternary sequences with a few cross correlations. Cryptogr. Commun. **12**, 511–525 (2020)