Bull. Aust. Math. Soc. **92** (2015), 32–43
doi:10.1017/S0004972715000301

A NOTE ON SOME CHARACTER SUMS OVER FINITE FIELDS

XIWANG CAO✉ and GUANGKUI XU

(Received 2 December 2014; accepted 28 February 2015; first published online 30 April 2015)

Abstract

In this paper, we present a decomposition of the elements of a finite field and illustrate the efficiency of this decomposition in evaluating some specific exponential sums over finite fields. The results can be employed in determining the Walsh spectrum of some Boolean functions.

2010 *Mathematics subject classification*: primary 11T23; secondary 11T71.

Keywords and phrases: finite field, exponential sum, Boolean function, Walsh spectrum.

1. Introduction

Let $n = 2m$ be a positive even integer and $\mathbb{F}_{2^n}$ the finite field of order 2^n. Let $\mathrm{Tr}_1^n(x) = \sum_{i=0}^{n-1} x^{2^i}$ be the trace function. The following exponential sums are useful in determining the Walsh spectrum of some Boolean functions (see Section 2 for the definitions).

$$p(\mu) = \sum_{a\in\mathbb{F}_{2^n}\setminus\mathbb{F}_2} \chi_n\Big(\mu\frac{a^{2^m}+a}{a^2+a}\Big), \quad q(\mu) = \sum_{a\in\mathbb{F}_{2^n}\setminus\mathbb{F}_{2^m}} \chi_n\Big(\mu\frac{a^2+a}{a^{2^m}+a}\Big),$$

$$q_s(\mu) = \sum_{a\in\mathbb{F}_{2^n}\setminus\mathbb{F}_{2^m}} \chi_n\Big(\mu\frac{(a^2+a)^{2^s}}{a^{2^m}+a}\Big), \quad r(l) = \sum_{a\in\mathbb{F}_{2^n}} \chi_n((a^{2^m}+a)L(a)).$$

Here, $\mu \in \mathbb{F}_{2^m}$, $\chi_n(x) = (-1)^{\mathrm{Tr}_1^n(x)}$, s is a positive integer with $\gcd(s, m) = d$ and $L(x) = \sum_{i=0}^{k} \alpha_i x^{2^{a_i}} \in \mathbb{F}_{2^m}[x]$ is a linearised polynomial with coefficients in $\mathbb{F}_{2^m}$. (See [1] for details.)

These sums form a subset of a much larger class of exponential sums, also known as Weil sums, of the form $\sum_{x\in\mathbb{F}_q} \chi_n(f(x))$, where $f(x) \in \mathbb{F}_q[X]$. The problem of explicitly evaluating Weil sums is usually difficult. Results giving estimates for the absolute value of a Weil sum are accessible and there are many examples (see for example [4–7, 9–14, 18]). We also refer the reader to [16] for an overview of the field.

The work of this paper is supported by the NUAA Fundamental Research Funds, No. 2013202.

For cryptographic systems, the method of confusion and diffusion is used as a fundamental technique to achieve security. Confusion is reflected in nonlinearity of certain Boolean functions describing the cryptographic transformation. For security of the system, high nonlinearity of these Boolean functions is desirable. The Walsh spectrum is used to measure this property of Boolean functions and its computation usually involves exponential sums over finite fields.

In this note, we will explicitly evaluate some of the related exponential sums. By using a new representation of elements of $\mathbb{F}_{2^{2m}}$, rather than polar decomposition, we show that all the aforementioned exponential sums can be reduced to exponential sums over a smaller subfield. The main contributions of the paper are to provide this new representation of elements of finite fields and to prove the following theorems.

THEOREM 1.1. *Let $k_m(\mu)$ denote the Kloosterman sum. For every $\mu \in \mathbb{F}_{2^m}^*$,*

$$p(\mu) = \sum_{a \in \mathbb{F}_{2^n} \setminus \mathbb{F}_2} \chi_n\left(\mu \frac{a^{2^m} + a}{a^2 + a}\right) = -2 - (1 + k_m(\mu))^2,$$

$$q(\mu) = \sum_{a \in \mathbb{F}_{2^n} \setminus \mathbb{F}_{2^m}} \chi_n\left(\mu \frac{a^2 + a}{a^{2^m} + a}\right) = -2^m \chi_m(\mu).$$

THEOREM 1.2. *Suppose that m is odd and $\gcd(s, m) = 1$ and let $(\frac{2}{m})$ denote the Jacobi symbol. Let $(2^s + 1)^{-1}$ denote the least positive integer s' satisfying $s'(2^s + 1) \equiv 1 \pmod{2^m - 1}$. Then:*
(1) $q_s(\mu) = -2^m$ if and only if $\mathrm{Tr}_1^m(\mu^{(2^s+1)^{-1}}) = 0$;
(2) if $\mathrm{Tr}_1^m(\mu^{(2^s+1)^{-1}}) = 1$, there is an $h \in \mathbb{F}_{2^m}$ such that $\mu^{(2^s+1)^{-1}} = h^{2^s} + h^{2^{m-s}} + 1$ and

$$q_s(\mu) = 2^m \left(\chi_m(h^{2^s+1} + h)\left(\frac{2}{m}\right) 2^{(m+1)/2} - 1\right).$$

THEOREM 1.3. *For every $L(x) = \sum_{i=0}^{k} \alpha_i x^{2^{a_i}} \in \mathbb{F}_{2^m}[x]$,*

$$r(l) = 2^m \sum_{u \in \mathbb{F}_{2^m}} \chi_m(uL(u)) = 2^m \sum_{u \in \mathbb{F}_{2^m}} \chi_m\left(\sum_{i=0}^{k} \alpha_i u^{2^{a_i}+1}\right).$$

The paper is organised as follows. Section 2 covers notation and preliminaries. In Section 3, we present the proof of Theorems 1.1–1.3. In Section 4, a generalisation of the new representation of the elements of finite fields of any extension degree is given and some more applications are proposed. In addition, we prove the following results.

THEOREM 1.4. *Let q be an odd prime power, $L_1(x) = \sum_{i=0}^{s-1} \beta_i x^{q^{mi}} \in \mathbb{F}_{q^n}[x]$ and $L(x) = \mathrm{Tr}_m^n(x)$. Then*

$$\sum_{x \in \mathbb{F}_{q^n}} \chi_n(L_1(x)\mathrm{Tr}_m^n(x)) = \begin{cases} q^{(s-1)m} + q^{(s-1)m} G(\eta, \chi_m)\eta(s)\chi_n(L_1(\lambda_0)) & \text{if } L_1(\ker(\mathrm{Tr}_m^n)) \subseteq \ker(\mathrm{Tr}_1^n), \\ q^{(s-1)m} & \text{otherwise.} \end{cases}$$

https://doi.org/10.1017/S0004972715000301 Published online by Cambridge University Press

Here, $\chi_n(x)$ is the canonical additive character of $\mathbb{F}_{q^n}$, η is the quadratic character of $\mathbb{F}_{q^m}$ with $\eta(0)$ defined as 0, λ_0 is a fixed element satisfying $\mathrm{Tr}_m^n(\lambda_0) = 1$ and $G(\eta, \chi_m)$ is the Gaussian sum.

THEOREM 1.5. *Let $n = sm$, q be an odd prime power and $L(x) = \sum_{i=0}^{s-1} \alpha_i x^{q^{mi}} \in \mathbb{F}_{q^m}[x]$. If $\dim_{\mathbb{F}_{q^m}}(\ker(L)) = s - 1$ and $L(1) \neq 0$, then*

$$\sum_{x \in \mathbb{F}_{q^n}} \chi_n\Big(\sum_{i=0}^{s-1} \alpha_i x^{q^{mi}+1}\Big) = q^{(s-1)m}(1 + G(\eta, \chi_m)\eta(s/L(1))).$$

2. Notation and preliminaries

2.1. Boolean functions. Let n be a positive integer and $\mathbb{F}_{2^n}$ be the finite field with 2^n elements. A Boolean function on $\mathbb{F}_{2^n}$ is a $\{0, 1\}$-valued function from $\mathbb{F}_{2^n}$ to $\mathbb{F}_2$.

For any positive integer n and for any positive integer k dividing n, the trace function from $\mathbb{F}_{2^n}$ to $\mathbb{F}_{2^k}$, denoted by Tr_k^n, is the map

$$\mathrm{Tr}_k^n(x) = x + x^{2^k} + x^{2^{2k}} + \cdots + x^{2^{n-k}}.$$

In particular, the absolute trace over $\mathbb{F}_2$ is the function $\mathrm{Tr}_1^n(x) = \sum_{i=0}^{n-1} x^{2^i}$ corresponding to $k = 1$. Recall that, for every integer k dividing n, the trace function satisfies the transitivity property [16], that is, for all $x \in \mathbb{F}_{2^n}$,

$$\mathrm{Tr}_1^n(x) = \mathrm{Tr}_1^k(\mathrm{Tr}_k^n(x)). \tag{2.1}$$

2.2. Walsh transform of Boolean functions. Let f be a Boolean function from $\mathbb{F}_{2^n}$ to $\mathbb{F}_2$. For every element $a \in \mathbb{F}_{2^n}$, the *Walsh (Hadamard) transform* of f at the point a is defined by

$$W_f(a) = \sum_{x \in \mathbb{F}_{2^n}} (-1)^{f(x)+\mathrm{Tr}_1^n(ax)}.$$

The set $\{W_f(a) \mid a \in \mathbb{F}_{2^n}\}$ is called the *Walsh spectrum* of f.

The Walsh spectrum is a powerful mathematical tool to measure the nonlinearity of a Boolean function (see [2, 3] for details).

2.3. Polar decomposition. Let $n = 2m$. Denote the subgroup of $(2^m + 1)$th roots of unity in $\mathbb{F}_{2^n}$ by $\mathfrak{S}$, that is, $\mathfrak{S} = \{z \in \mathbb{F}_{2^n} \mid z^{2^m+1} = 1\}$. For every $x \in \mathbb{F}_{2^n}^* = \mathbb{F}_{2^n} \setminus \{0\}$, there is a unique polar decomposition of x as $x = yz$, where $y \in \mathbb{F}_{2^m}^*$ and $z \in \mathfrak{S}$. In fact, $y = x^{(2^m+1)2^{m-1}}$ and $z = x^{(2^m-1)2^{m-1}}$. Write $\overline{x} = x^{2^m}$. For every $x \in \mathbb{F}_{2^n}^*$, $x \in \mathbb{F}_{2^m}$ if and only if $x = \overline{x}$ and $x \in \mathfrak{S}$ if and only if $\overline{x} = x^{-1}$. It is evident that for every $x \in \mathbb{F}_{2^n}^*$, $x + \overline{x}, x\overline{x} \in \mathbb{F}_{2^m}$ and $x/\overline{x}, \overline{x}/x \in \mathfrak{S}$. Note that $x \mapsto \overline{x}$ is an isomorphism of the finite field $\mathbb{F}_{2^n}$.

https://doi.org/10.1017/S0004972715000301 Published online by Cambridge University Press

2.4. Kloosterman sums. For $a, b \in \mathbb{F}_{2^m}$, the Kloosterman sum is defined by

$$k_m(a,b) = \sum_{x \in \mathbf{F}_{2^m}^*} (-1)^{\mathrm{Tr}_m(ax+bx^{-1})}.$$

It is easy to check that $k_m(a,b) = k_m(ab,1) = k_m(1,ab)$. For simplicity, write $k_m(a) = k_m(a,1) = k_m(1,a)$. The Kloosterman sum $k_m(a,b)$ can be calculated recursively. That is, if we define

$$k_m^{(s)}(a) = \sum_{\gamma \in \mathbb{F}_{2^{ms}}^*} \chi^{(s)}(a\gamma + \gamma^{-1}), \quad a \in \mathbb{F}_{2^m},$$

where $\chi^{(s)}$ is the lifting of $\chi(x) = (-1)^{\mathrm{Tr}(x)}$ to $\mathbb{F}_{2^{ms}}$, then

$$k_m^{(s)}(a) = -k_m^{(s-1)}(a)k_m^{(1)}(a) - 2^m k_m^{(s-2)}(a),$$

where we put $k_m^{(0)}(a,b) = -2$ and $k_m^{(1)}(a) = k(a)$. (See [16, Ch. 5] for details.)

2.5. A decomposition of elements of $\mathbb{F}_{2^n}$ related to an affine subspace. Let $n = 2m$ and set

$$E = \{\lambda \in \mathbb{F}_{2^n} \mid \lambda^{2^m} + \lambda = 1\}.$$

Then E is an affine subspace of $\mathbb{F}_{2^n}/\mathbb{F}_2$. For every $x \in \mathbb{F}_{2^n}^* \setminus \mathbb{F}_{2^m}$, there is a unique pair $(u,\lambda) \in \mathbb{F}_{2^m}^* \times E$ such that $x = u\lambda$. If $x \in \mathbb{F}_{2^m}$, we just write $x = u$. We claim that this decomposition is unique. Define a map $\tau : \mathbb{F}_{2^n} \to \mathbb{F}_{2^m}^* \times E$; if there are $u_1, u_2 \in \mathbb{F}_{2^m}^*$ and $\lambda_1, \lambda_2 \in E$ satisfying $u_1\lambda_1 = u_2\lambda_2$, then

$$1 = \overline{\lambda_1} + \lambda_1 = (u_2/u_1)(\overline{\lambda_2} + \lambda_2) = u_2/u_1,$$

which implies that $u_1 = u_2$ and $\lambda_1 = \lambda_2$. Counting the image number of the map τ leads to the desired statement. Under this decomposition, the following two facts are easily verified.

Fact (i). Suppose that $x \in \mathbb{F}_{2^n} \setminus \mathbb{F}_{2^m}$ and $x = u\lambda$, $u \in \mathbb{F}_{2^m}^*$, $\lambda \in E$. Then $\mathrm{Tr}_1^n(x) = \mathrm{Tr}_1^m(u)$.

Proof. By (2.1), $\mathrm{Tr}_1^n(x) = \mathrm{Tr}_1^m(\mathrm{Tr}_n^m(u\lambda)) = \mathrm{Tr}_1^m(u(\lambda + \overline{\lambda})) = \mathrm{Tr}_1^m(u)$. □

Fact (ii). The map $\sigma : E \to \mathbb{F}_{2^m}$ given by $\lambda \mapsto \lambda\overline{\lambda}$ is two-to-one. The image set is precisely the set of elements in $\mathbb{F}_{2^m}$ of trace one.

Proof. It is obvious that there are two elements $\lambda_1, \lambda_2 \in E$ satisfying $\lambda_1\overline{\lambda_1} = \lambda_2\overline{\lambda_2} = a$ for some $a \in \mathbb{F}_{2^m}$ if and only if λ_1, λ_2 are the two distinct roots of the equation

$$X^2 + X + a = 0. \tag{2.2}$$

Now (2.2) has two distinct roots in $\mathbb{F}_{2^n} \setminus \mathbb{F}_{2^m}$ if and only if $\mathrm{Tr}_1^m(a) = 1$. Moreover, for any $a \in \mathbb{F}_{2^m}$ with trace one, λ is a root of the equation (2.2) if and only if $\overline{\lambda}$ is also a root of the equation. Thus, $\lambda + \overline{\lambda} = 1$ and $\lambda \in E$. □

In the next section, we will show that this new representation of elements in $\mathbb{F}_{2^{2m}}$ is an effective tool in evaluating some exponential sums over finite fields.

https://doi.org/10.1017/S0004972715000301 Published online by Cambridge University Press

3. Proof of Theorems 1.1–1.3

3.1. The evaluation of $p(\mu)$. For the first exponential sum, we compute

$$p(\mu)=\sum_{a\in\mathbb{F}_{2^n}\setminus\mathbb{F}_2}\chi_n\Big(\mu\frac{a^{2^m}+a}{a^2+a}\Big)=2^m-2+\sum_{a\in\mathbb{F}_{2^n}\setminus\mathbb{F}_{2^m}}\chi_n\Big(\mu\frac{a^{2^m}+a}{a^2+a}\Big).$$

For any $a\in\mathbb{F}_{2^n}\setminus\mathbb{F}_{2^m}$, let $a=u\lambda$, where $u\in\mathbb{F}_{2^m}^*$, $\lambda\in E$. Then

$$\begin{aligned}\sum_{a\in\mathbb{F}_{2^n}\setminus\mathbb{F}_{2^m}}\chi_n\Big(\mu\frac{a^{2^m}+a}{a^2+a}\Big)&=\sum_{u\in\mathbb{F}_{2^m}^*,\lambda\in E}\chi_n\Big(\mu\Big(\frac{1}{\lambda}+\frac{1}{\lambda+u}\Big)\Big)\\&=\sum_{u\in\mathbb{F}_{2^m}^*,\lambda\in E}\chi_m\Big(\mu\Big(\frac{1}{\lambda\overline{\lambda}}+\frac{1}{\lambda\overline{\lambda}+u^2+u}\Big)\Big).\end{aligned}$$

By Fact (ii),

$$\begin{aligned}\sum_{u\in\mathbb{F}_{2^m}^*,\lambda\in E}\chi_m\Big(\mu\Big(\frac{1}{\lambda\overline{\lambda}}+\frac{1}{\lambda\overline{\lambda}+u^2+u}\Big)\Big)&=2\sum_{v\in\mathbb{F}_{2^m},\mathrm{Tr}_1^m(v)=1}\chi_m\Big(\frac{\mu}{v}\Big)\sum_{u\in\mathbb{F}_{2^m}^*}\chi_m\Big(\frac{\mu}{v+u^2+u}\Big)\\&=2\sum_{v\in\mathbb{F}_{2^m},\mathrm{Tr}_1^m(v)=1}\chi_m\Big(\frac{\mu}{v}\Big)\Big(\chi_m\Big(\frac{\mu}{v}\Big)+2\sum_{u\in\mathbb{F}_{2^m}^*\setminus\{v\},\mathrm{Tr}_1^m(u)=1}\chi_m\Big(\frac{\mu}{u}\Big)\Big).\end{aligned}$$

Since

$$\begin{aligned}\chi_m\Big(\frac{\mu}{v}\Big)+2\sum_{u\in\mathbb{F}_{2^m}^*\setminus\{v\},\mathrm{Tr}_1^m(u)=1}\chi_m\Big(\frac{\mu}{u}\Big)&=\chi_m\Big(\frac{\mu}{v}\Big)-2\chi_m\Big(\frac{\mu}{v}\Big)+2\sum_{u\in\mathbb{F}_{2^m},\mathrm{Tr}_1^m(u)=1}\chi_m\Big(\frac{\mu}{u}\Big)\\&=\chi_m\Big(\frac{\mu}{v}\Big)-2\chi_m\Big(\frac{\mu}{v}\Big)+\sum_{u\in\mathbb{F}_{2^m}}\chi_m\Big(\frac{\mu}{u}\Big)(1-\chi_m(u))\\&=-\chi_m\Big(\frac{\mu}{v}\Big)-\sum_{u\in\mathbb{F}_{2^m}}\chi_m(u+\mu/u)\\&=-1-\chi_m\Big(\frac{\mu}{v}\Big)-k_m(\mu),\end{aligned}$$

it follows that

$$\begin{aligned}\sum_{a\in\mathbb{F}_{2^n}\setminus\mathbb{F}_{2^m}}\chi_n\Big(\mu\frac{a^{2^m}+a}{a^2+a}\Big)&=-2(1+k_m(\mu))\sum_{v\in\mathbb{F}_{2^m},\mathrm{Tr}_1^m(v)=1}\chi_m\Big(\frac{\mu}{v}\Big)-2\sum_{v\in\mathbb{F}_{2^m},\mathrm{Tr}_1^m(v)=1}1\\&=-(1+k_m(\mu))^2-2^m.\end{aligned}$$

Therefore,

$$p(\mu)=\sum_{a\in\mathbb{F}_{2^n}\setminus\mathbb{F}_2}\chi_n\Big(\mu\frac{a^{2^m}+a}{a^2+a}\Big)=-2-(1+k_m(\mu))^2.$$

https://doi.org/10.1017/S0004972715000301 Published online by Cambridge University Press

3.2. The evaluation of $q(\mu)$. It is evident that

$$q(\mu) = \sum_{a\in\mathbb{F}_{2^n}\setminus\mathbb{F}_{2^m}} \chi_n\Big(\mu\frac{a^2+a}{a^{2^m}+a}\Big) = \sum_{u\in\mathbb{F}_{2^m}^*,\lambda\in E} \chi_n(\mu(u\lambda^2+\lambda))$$
$$= \sum_{u\in\mathbb{F}_{2^m}^*,\lambda\in E} \chi_m(\mu(u+1)) = -2^m\chi_m(\mu).$$

3.3. The evaluation of $q_s(\mu)$. It is easy to see that

$$q_s(\mu) = \sum_{a\in\mathbb{F}_{2^n}\setminus\mathbb{F}_{2^m}} \chi_n\Big(\mu\frac{(a^2+a)^{2^s}}{a^{2^m}+a}\Big) = \sum_{u\in\mathbb{F}_{2^m}^*,\lambda\in E} \chi_m(\mu(u^{2^{s+1}-1}+u^{2^s-1}))$$
$$= 2^m \sum_{u\in\mathbb{F}_{2^m}^*} \chi_m(\mu(u^{(2^s-1)(2^s+1)}+u^{2^s-1})).$$

If m is odd and $\gcd(s,m)=1$, then $\gcd(2^s+1, 2^m-1) = \gcd(2^s-1, 2^m-1) = 1$ and

$$q_s(\mu) = \sum_{a\in\mathbb{F}_{2^n}\setminus\mathbb{F}_{2^m}} \chi_n\Big(\mu\frac{(a^2+a)^{2^s}}{a^{2^m}+a}\Big) = 2^m \sum_{u\in\mathbb{F}_{2^m}^*} \chi_m(\mu(u^{(2^s-1)(2^s+1)}+u^{2^s-1}))$$
$$= 2^m \sum_{u\in\mathbb{F}_{2^m}^*} \chi_m(\mu(u^{2^s+1}+u)).$$

The last exponential sum is a special case of

$$C_m^{(s)}(a,b) = \sum_{x\in\mathbf{F}_{2^m}} \chi_m(ax^{2^s+1}+bx), \quad a,b\in\mathbb{F}_{2^m}.$$

Lemma 3.1 [15]. *If m is odd and $\gcd(s,m)=1$, then*

$$C_m^{(s)}(1,1) = \Big(\frac{2}{m}\Big)2^{(m+1)/2} = \begin{cases} 2^{(m+1)/2} & \text{if } m\equiv\pm1 \pmod 8,\\ -2^{(m+1)/2} & \text{if } m\equiv\pm3 \pmod 8,\end{cases}$$

where $(\frac{2}{m})$ is the Jacobi symbol.

If m is odd and $\gcd(s,m)=1$, then $x\mapsto x^{2^s+1}$ is a permutation on $L =: \mathbb{F}_{2^m}$.

Lemma 3.2 [8]. *If m is odd and $\gcd(s,m)=1$, then:*
(1) $C_m^{(s)}(a,b) = C_m^{(s)}(1, b/a^{(2^s+1)^{-1}})$;
(2) $C_m^{(s)}(1,a) = C_m^{(s)}(1,a^2)$ *for all* $a\in L$;
(3) $C_m^{(s)}(1,a) = 0$ *if and only if* $\mathrm{Tr}_1^m(a) = 0$;
(4) *if* $\mathrm{Tr}_1^m(a) = 1$, *then there is an* $h\in L$ *such that* $a = h^{2^s}+h^{2^{m-s}}+1$ *and*

$$C_m^{(s)}(1,a) = \chi_m(h^{2^s+1}+h)C_m^{(s)}(1,1) = \chi_m(h^{2^s+1}+h)\Big(\frac{2}{m}\Big)2^{(m+1)/2}.$$

https://doi.org/10.1017/S0004972715000301 Published online by Cambridge University Press

LEMMA 3.3. *For a positive integer l, let*

$$T_l(x) = x + x^2 + x^4 + \cdots + x^{2^{l-1}}.$$

Then, for every positive integer k and every $h \in \mathbb{F}_{2^m}$,

$$\mathrm{Tr}_1^m(u^3 + u) = \mathrm{Tr}_1^m(h^{2^k+1} + h) \quad \text{and} \quad \chi(u^3 + u) = \chi(h^{2^k+1} + h),$$

where $u = T_k(h)$. Moreover, if k is odd, then

$$\mathrm{Tr}_1^m(u^3) = \mathrm{Tr}_1^m(h^{2^k+1}).$$

PROOF. Since $u = T_k(h)$, $\mathrm{Tr}_1^m(u) = k\mathrm{Tr}_1^m(h)$ and

$$\begin{aligned}
\mathrm{Tr}_1^m(u^3) &= \mathrm{Tr}_1^m((T_k(h))^3) = \mathrm{Tr}_1^m(T_k(h)T_k(h^2)) \\
&= \mathrm{Tr}_1^m\Big(\Big(h + \sum_{i=1}^{k-1} h^{2^i}\Big)\Big(\sum_{i=1}^{k-1} h^{2^i} + h^{2^k}\Big)\Big) \\
&= \mathrm{Tr}_1^m\Big(\sum_{i=1}^{k-1} h^{2^i+1} + \sum_{i=1}^{k-1} h^{2^i} + h^{2^k+1} + \sum_{i=1}^{k-1} h^{2^i+2^k}\Big) \\
&= \mathrm{Tr}_1^m(h^{2^k+1}) + (k-1)\mathrm{Tr}_1^m(h) + \mathrm{Tr}_1^m\Big(\sum_{i=1}^{k-1} h^{2^i+1} + \sum_{i=1}^{k-1} h^{2^i+2^k}\Big).
\end{aligned}$$

Since

$$\mathrm{Tr}_1^m\Big(\sum_{i=1}^{k-1} h^{2^i+2^k}\Big) = \mathrm{Tr}_1^m(h^{1+2^{k-1}} + h^{1+2^{k-2}} + \cdots + h^{1+2}) = \mathrm{Tr}_1^m\Big(\sum_{i=1}^{k-1} h^{2^i+1}\Big),$$

we see that $\mathrm{Tr}_1^m(u^3 + u) = \mathrm{Tr}_1^m(h^{2^k+1} + h)$ and thus $\chi(u^3 + u) = \chi(h^{2^k+1} + h)$. □

Using Lemma 3.2(3) and (4), we also obtain the following result.

THEOREM 3.4. *Suppose that k and m are odd and* $\gcd(k, m) = 1$. *Then, for every $v \in \mathbb{F}_{2^m}$,*

$$C_m^{(k)}(1, v^{2^k} + v + 1) = C_m^{(1)}(1, v^2 + v + 1). \tag{3.1}$$

Consequently,

$$C_m^{(k)}(1, T_k(v)) = C_m^{(1)}(1, v). \tag{3.2}$$

PROOF. Let $h \in \mathbb{F}_{2^m}$ with $a = h^{2^k} + h^{2^{m-k}} + 1$, where h is the same element as in Lemma 3.2(4). Then

$$C_m^{(k)}(1, a) = \chi(h^{2^k+1} + h)\Big(\frac{2}{m}\Big)2^{(m+1)/2}.$$

Put $\rho(a) = u^2 + u^{2^{m-1}} + 1$. By Lemma 3.2(4) with $k = 1$,

$$C_m^{(1)}(1, \rho(a)) = \chi(u^3 + u)\Big(\frac{2}{m}\Big)2^{(m+1)/2}.$$

https://doi.org/10.1017/S0004972715000301 Published online by Cambridge University Press

Thus, we obtain

$$C_m^{(k)}(1,a) = C_m^{(1)}(1,\rho(a)). \tag{3.3}$$

Substituting h^{2^k} for h, we have $a = h + h^{2^{2k}} + 1$ and $\rho(a) = T_k(h^{2^{k+1}}) + T_k(h^{2^{k-1}}) + 1$. Thus, $a = h + h^{2^k} + (h + h^{2^k})^{2^k} + 1 = T_k(h + h^2) + (T_k(h + h^2))^{2^k} + 1 = v + v^{2^k} + 1$ and $\rho(a) = T_k(h^{2^{k+1}} + h^{2^{k-1}}) + 1 = (T_k(h + h^2) + T_k(h + h^2)^2)^{2^{k-1}} + 1 = (v + v^2 + 1)^{2^{k-1}}$, where $v = T_k(h + h^2)$. From (3.3) and Lemmas 3.3 and 3.2(2),

$$C_m^{(k)}(1, v + v^{2^k} + 1) = C_m^{(1)}(1, (v + v^2 + 1)^{2^{k-1}}) = C_m^{(1)}(1, v + v^2 + 1).$$

Since k is odd, T_k is a permutation on $\mathbb{F}_{2^m}$. For $v \in \mathbb{F}_{2^m}$, $v + v^{2^k} + 1$ and $v + v^2 + 1$ are invariant under the transformation $v \mapsto v + 1$, so that

$$C_m^{(k)}(1, v + v^{2^k} + 1) = C_m^{(1)}(1, v + v^2 + 1).$$

For the proof of (3.2), notice that when $\mathrm{Tr}_1^m(v) = 0$, $C_m^{(k)}(1, T_k(v)) = C_m^{(1)}(1, v) = 0$. If $\mathrm{Tr}_1^m(v) = 1$, then $T_k(v^2 + v + 1) = v + v^{2^k} + 1$ shows that (3.2) is equivalent to (3.1). This completes the proof. □

Remark 3.5. (1) Lemma 3.1 is a direct consequence of (3.2) by taking $v = 1$ and utilising [4].
(2) Lemma 3.2 gives an explicit determination of $\sum_{u \in \mathbb{F}_{2^m}^*} \chi_m(\mu(u^{2^s+1} + u))$ and its spectrum.

3.4. The evaluation of $r(l)$. A direct computation shows that

$$\begin{aligned} r(l) &= 2^m + \sum_{a \in \mathbb{F}_{2^n} \setminus \mathbb{F}_{2^m}} \chi_n((a^{2^m} + a)L(a)) = 2^m + \sum_{\lambda \in E, u \in \mathbb{F}_{2^m}^*} \chi_n(uL(\lambda u)) \\ &= 2^m + \sum_{\lambda \in E, u \in \mathbb{F}_{2^m}^*} \chi_m(uL(u(\lambda + \overline{\lambda}))) = 2^m + \sum_{\lambda \in E, u \in \mathbb{F}_{2^m}^*} \chi_m(uL(u)) \\ &= 2^m \sum_{u \in \mathbb{F}_{2^m}} \chi_m(uL(u)) = 2^m \sum_{u \in \mathbb{F}_{2^m}} \chi_m\Big(\sum_{i=0}^{k} \alpha_i u^{2^{a_i}+1}\Big). \end{aligned}$$

4. Extensions

In the previous section, we provided a representation of elements in finite fields of characteristic two. It is shown that this decomposition leads to an effective recursive method for computing some exponential sums by reducing the computation to a smaller subfield. By a slight modification, this method generalises to finite fields of any characteristic. Let $n = sm$ and $L(x) = \sum_{i=0}^{s-1} \alpha_i x^{q^{mi}} \in \mathbb{F}_{q^n}[x]$ be a linearised polynomial with coefficients in $\mathbb{F}_{q^n}$. Denote

$$E_a = \{x \in \mathbb{F}_{q^n} : L(x) = a\}, \quad a \in \mathbb{F}_{q^m}.$$

It is easily seen that E_a is an affine subspace of $\mathbb{F}_{q^{sm}}$ (viewed as an $\mathbb{F}_{q^m}$-vector space) and, for $a, b \in \mathbb{F}_{q^m}^*$,

$$E_a \cap E_b = \emptyset \text{ for } a \neq b \quad \text{and} \quad E_a = aE_1 = \{a\lambda : \lambda \in E_1\}.$$

https://doi.org/10.1017/S0004972715000301 Published online by Cambridge University Press

Furthermore, if $\dim_{\mathbb{F}_{q^m}}(\ker(L)) = s-1$, then $\mathbb{F}_{q^n} = \bigcup_{a\in\mathbb{F}_{q^m}} E_a$ since the cardinality of the right-hand side is $q^m q^{m(s-1)} = q^n$. This is an alternative explanation of the new decomposition proposed in Section 2.

PROPOSITION 4.1. *With the notation as above, if* $\dim_{\mathbb{F}_{q^m}}(\ker(L)) = s-1$, *then, for every* $x \in \mathbb{F}_{q^n} \setminus \ker(L)$, *there is a unique decomposition*

$$x = u\lambda, \quad u \in \mathbb{F}_{q^m},\ \lambda \in E_1.$$

PROOF. After the previous remarks, we only need to prove the uniqueness of the decomposition. If there are elements $x \in \mathbb{F}_{q^n} \setminus \ker(L)$, $u_1, u_2 \in \mathbb{F}_{p^m}$, $\lambda_1, \lambda_2 \in E_1$ satisfying

$$x = u_1\lambda_1 = u_2\lambda_2,$$

then

$$0 \neq L(x) = u_1 L(\lambda_1) = u_2 L(\lambda_2).$$

But $L(u_1) = L(u_2) = 1$, so we have $u_1 = u_2$ and then $\lambda_1 = \lambda_2$. □

In order to apply Proposition 4.1, we need to find linearised polynomials whose kernel has dimension $s-1$. We have the following lemma.

LEMMA 4.2 [17]. *Let* $n = sm$, $\{\alpha_1, \alpha_2, \ldots, \alpha_s\}$ *be a basis of* $\mathbb{F}_{q^{sm}}$ *viewed as a vector space over* $\mathbb{F}_{q^m}$ *and* $L(x) = \sum_{i=0}^{s-1} a_i x^{q^{mi}} \in \mathbb{F}_{q^n}[x]$ *be a linearised polynomial over* $\mathbb{F}_{q^n}$. *Then there exist s elements* $\beta_1, \beta_2, \ldots, \beta_s \in \mathbb{F}_{q^n}$ *such that*

$$L(x) = \mathrm{Tr}_m^n(\beta_1 x)\alpha_1 + \mathrm{Tr}_m^n(\beta_2 x)\alpha_2 + \cdots + \mathrm{Tr}_m^n(\beta_s x)\alpha_s.$$

Moreover, $\dim_{\mathbb{F}_{q^m}}(\ker(L)) = k$ *if and only if* $\mathrm{rank}_{\mathbb{F}_{q^m}}\{\beta_1, \beta_2, \ldots, \beta_s\} = s-k$ *for* $0 \le k \le s$. *Furthermore, every d-dimensional subspace of* $\mathbb{F}_{q^m}^s$ *can be obtained in this way.*

By Lemma 4.2, it is easy to find a linearised polynomial whose kernel has dimension $s-1$. In particular, if $L(x) = \mathrm{Tr}_m^n(x)$, then $\dim_{\mathbb{F}_{q^m}}(\ker(L)) = s-1$.

The following two results are applications of the new decomposition.

THEOREM 4.3. *Let* q *be an odd prime power,* $L_1(x) = \sum_{i=0}^{s-1} \gamma_i x^{q^{mi}} \in \mathbb{F}_{q^n}[x]$ *and* $L(x) = \mathrm{Tr}_m^n(x)$. *Then*

$$\sum_{x\in\mathbb{F}_{q^n}} \chi_n(L_1(x)\mathrm{Tr}_m^n(x)) = \begin{cases} q^{(s-1)m} + q^{(s-1)m} G(\eta, \chi_m)\eta(s)\chi_n(L_1(\lambda_0)) & \text{if } L_1(\ker(\mathrm{Tr}_m^n)) \subseteq \ker(\mathrm{Tr}_1^n), \\ q^{(s-1)m} & \text{otherwise.} \end{cases}$$

Here, $\chi_n(x)$ *is the canonical additive character of* $\mathbb{F}_{q^n}$, η *is the quadratic character of* $\mathbb{F}_{q^m}$ *with* $\eta(0)$ *defined as* 0, λ_0 *is a fixed element satisfying* $\mathrm{Tr}_m^n(\lambda_0) = 1$ *and* $G(\eta, \chi_m)$ *is the Gaussian sum.*

https://doi.org/10.1017/S0004972715000301 Published online by Cambridge University Press

PROOF. Note that

$$\sum_{x\in\mathbb{F}_{q^n}}\chi_n(L_1(x)\mathrm{Tr}_m^n(x)) = \sum_{x\in\ker(L)}\chi_n(L_1(x)\mathrm{Tr}_m^n(x)) + \sum_{x\in\mathbb{F}_{q^n}\setminus\ker(L)}\chi_n(L_1(x)\mathrm{Tr}_m^n(x)).$$

For the first sum, since $\dim_{\mathbb{F}_{q^m}}(\ker(L)) = s-1$,

$$\sum_{x\in\ker(L)}\chi_n(L_1(x)\mathrm{Tr}_m^n(x)) = q^{(s-1)m}.$$

For the second sum, we use the decomposition $x = u\lambda$, $u\in\mathbb{F}_{q^m}$, $\lambda\in E_1$:

$$L_1(x)\mathrm{Tr}_m^n(x) = uL_1(\lambda)u\mathrm{Tr}_m^n(\lambda) = u^2L_1(\lambda)$$

and

$$\sum_{x\in\mathbb{F}_{q^n}\setminus\mathbb{F}_{q^m}}\chi_n(L_1(x)\mathrm{Tr}_m^n(x)) = \sum_{u\in\mathbb{F}_{q^m}}\chi_n(u^2)\sum_{\lambda\in E_1}\chi_n(L_1(\lambda)).$$

Here, $\sum_{u\in\mathbb{F}_{q^m}}\chi_n(u^2) = \sum_{u\in\mathbb{F}_{q^m}}\chi_m(su^2) = G(\eta,\chi_m)\eta(s)$ by [16, Theorem 5.33] since $\chi_m(x)$ is the canonical additive character of $\mathbb{F}_{q^m}$. For the sum $\sum_{\lambda\in E_1}\chi_n(L_1(\lambda))$, let λ_0 be a fixed element in E_1. Then $E_1 = \lambda_0 + E_0 = \{\lambda_0 + x : x\in E_0\}$. Thus, $\sum_{\lambda\in E_1}\chi_n(L_1(\lambda)) = \chi_n(L_1(\lambda_0))\sum_{x\in E_0}\chi_n(L_1(x))$. If there is an element $x_0\in\mathbb{F}_{q^n}$ such that $\mathrm{Tr}_m^n(x_0) = 0$ and $\mathrm{Tr}_1^n(L_1(x_0)) \neq 0$, then

$$\chi_n(L_1(x_0))\sum_{x\in E_0}\chi_n(L_1(x)) = \sum_{x\in E_0}\chi_n(L_1(x_0+x)) = \sum_{x\in E_0}\chi_n(L_1(x)),$$

which implies that $\sum_{\lambda\in E_1}\chi_n(L_1(\lambda)) = 0$; if $\mathrm{Tr}_1^n(L_1(x)) = 0$ for every $x\in E_0$, then $\sum_{\lambda\in E_1}\chi_n(L_1(\lambda)) = q^{(s-1)m}\chi_n(L_1(\lambda_0))$. The desired result follows. □

THEOREM 4.4. *Let $n = sm$, q be an odd prime power and $L(x) = \sum_{i=0}^{s-1}a_ix^{q^{mi}}\in\mathbb{F}_{q^m}[x]$. If $\dim_{\mathbb{F}_{q^m}}(\ker(L)) = s-1$ and $L(1)\neq 0$, then*

$$\sum_{x\in\mathbb{F}_{q^n}}\chi_n\Big(\sum_{i=0}^{s-1}a_ix^{q^{mi}+1}\Big) = q^{(s-1)m}(1+G(\eta,\chi_m)\eta(s/L(1))).$$

PROOF. It is obvious that

$$\sum_{x\in\mathbb{F}_{q^n}}\chi_n\Big(\sum_{i=0}^{s-1}a_ix^{q^{mi}+1}\Big) = \sum_{x\in\mathbb{F}_{q^n}}\chi_n(xL(x)) = \sum_{x\in\ker(L)}\chi_n(xL(x)) + \sum_{x\in\mathbb{F}_{q^n}\setminus\ker(L)}\chi_n(xL(x)).$$

The first sum is equal to $q^{(s-1)m}$. Using the new decomposition,

$$\sum_{x\in\mathbb{F}_{q^n}\setminus\ker(L)}\chi_n(xL(x)) = \sum_{u\in\mathbb{F}_{q^m},\lambda\in E_1}\chi_n(u\lambda L(u\lambda)) = \sum_{u\in\mathbb{F}_{q^m},\lambda\in E_1}\chi_n(u^2\lambda).$$

https://doi.org/10.1017/S0004972715000301 Published online by Cambridge University Press

Since $\lambda \in E_1$, we have $L(\lambda) = 1$ and

$$s = \mathrm{Tr}_m^n(1) = \mathrm{Tr}_m^n(L(\lambda)) = L(1)\mathrm{Tr}_m^n(\lambda).$$

Thus,

$$\chi_n(u^2\lambda) = \chi_m(\mathrm{Tr}_m^n(u^2\lambda)) = \chi_m(u^2\mathrm{Tr}_m^n(\lambda)) = \chi_m(u^2 s/L(1)).$$

By [16, Theorem 5.33] again,

$$\sum_{u\in\mathbb{F}_{q^m},\lambda\in E_1} \chi_n(u^2\lambda) = \sum_{\lambda\in E_1}\sum_{u\in\mathbb{F}_{q^m}} \chi_m(u^2 s/L(1)) = q^{(s-1)m}G(\eta,\chi_m)\eta(s/L(1)).$$

This completes the proof. □

Remark 4.5.

(1) The determination of the quadratic Gaussian sum is well known and the exponential sums evaluated in Proposition 4.4 have been extensively studied (see for example [4–7, 9, 11–14, 18]), but our approach is different.

(2) Under the restrictions of Theorem 4.4, Lemma 4.2 implies that $L(x) = a\mathrm{Tr}_m^n(x)$ for an element $a \in \mathbb{F}_{q^m}$. Thus, the exponential sum in question is

$$\sum_{x\in\mathbb{F}_{q^n}} \zeta_p^{\mathrm{Tr}_1^m(a\mathrm{Tr}_m^n(x)^2)}, \tag{4.1}$$

where ζ_p is a primitive pth root of unity. To the authors' knowledge, the exponential sum in (4.1) has not been investigated before. A more challenging problem is to calculate the following exponential sum:

$$\sum_{x\in\mathbb{F}_{q^n}} \zeta_p^{\mathrm{Tr}_1^m(a\mathrm{Tr}_m^n(x)^r)},$$

where $r \geq 3$ is a positive integer.

References

[1] X. Cao and L. Hu, 'Two Boolean functions with five-valued Walsh spectra and high nonlinearity', *Int. J. Found. Comput. Sci.*, to appear.

[2] C. Carlet, 'Boolean functions for cryptography and error correcting codes', in: *Boolean Models and Methods in Mathematics, Computer Science, and Engineering* (eds. Y. Crama and P. L. Hammer) (Cambridge University Press, Cambridge, 2010), 257–397.

[3] C. Carlet and C. Ding, 'Highly nonlinear mappings', *J. Complexity* **20** (2004), 205–244.

[4] L. Carlitz, 'Explicit evaluation of certain exponential sums', *Math. Scand.* **44** (1979), 5–16.

[5] P. Charpin, T. Helleseth and V. Zinoviev, 'The coset distribution of triple-error-correcting binary primitive BCH codes', *IEEE Trans. Inform. Theory* **52**(4) (2006), 1727–1732.

[6] P. Charpin, T. Helleseth and V. Zinoviev, 'Divisibility properties of classical binary Kloosterman sums', *Discrete Math.* **309** (2009), 3975–3984.

[7] R. S. Coulter, 'On the evaluation of a class of Weil sums in characteristic 2', *New Zealand J. Math.* **28** (1999), 171–184.

[8] J. Dillon and H. Dobbertin, 'New cyclic difference sets with Singer parameters', *Finite Fields Appl.* **10**(3) (2004), 342–389.

https://doi.org/10.1017/S0004972715000301 Published online by Cambridge University Press

[9] K. Feng and J. Luo, 'Weight distribution of some reducible cyclic codes', *Finite Fields Appl.* **14** (2008), 390–409.
[10] T. Helleseth, 'Crosscorrelation of m-sequences, exponential sums and Dickson polynomials', *IEICE Trans. Fundam. Electron. Commun. Comput. Sci.* **E93-A**(11) (2010), 2212–2219.
[11] T. Helleseth and V. A. Zinoviev, 'On $\mathbf{Z}_4$-linear Goethals codes and Kloosterman sums', *Des. Codes Cryptogr.* **17** (1999), 246–262.
[12] X. Hou, 'Explicit evaluation of certain exponential sums of binary quadratic functions', *Finite Fields Appl.* **13** (2007), 843–868.
[13] A. Johansen and T. Helleseth, 'A family of m-sequences with five-valued cross correlation', *IEEE Trans. Inform. Theory* **55**(2) (2009), 880–887.
[14] A. Johansen, T. Helleseth and A. Kholosha, 'Further results on m-sequences with five-valued cross correlation', *IEEE Trans. Inform. Theory* **55**(12) (2009), 5792–5802.
[15] J. Lahtonen, G. McGuire and H. W. Ward, 'Gold and Kasami–Welch functions, quadratic forms, and bent functions', *Adv. Math. Commun.* **1**(2) (2007), 243–250.
[16] R. Lidl and H. Niederriter, *Finite Fields*, Encyclopedia of Mathematics and its Applications, 20 (Addison-Wesley, Reading, MA, 1983).
[17] S. Ling and L. Qu, 'A note on linearized polynomials and the dimension of their kernels', *Finite Fields Appl.* **18** (2012), 56–62.
[18] X. Zhang, X. Cao and R. Feng, 'A method of evaluation of exponential sum of binary quadratic functions', *Finite Fields Appl.* **18** (2012), 1089–1103.

XIWANG CAO, Department of Mathematics,
Nanjing University of Aeronautics and Astronautics, Nanjing 210016, PR China
e-mail: xwcao@nuaa.edu.cn

GUANGKUI XU, Department of Mathematics,
Nanjing University of Aeronautics and Astronautics, Nanjing 210016, PR China
and
Department of Mathematics, Huainan Normal University, Huainan 232038, PR China
e-mail: xuguangkuiy@163.com

https://doi.org/10.1017/S0004972715000301 Published online by Cambridge University Press