ON THE EVALUATION OF A CLASS OF WEIL SUMS IN CHARACTERISTIC 2

ROBERT S. COULTER

Abstract. We consider a class of Weil sums involving polynomials of a particular shape. In all cases, explicit evaluations are obtained.

1. Introduction

Let p be a prime and $q = p^e$ for some integer e. We denote the finite field of q elements by $\mathbb{F}_q$ and the non-zero elements of $\mathbb{F}_q$ by $\mathbb{F}_q^*$. A Weil sum is an exponential sum of the form $\sum_{x \in \mathbb{F}_q} \chi\big(f(x)\big)$, where χ is a non-trivial additive character of $\mathbb{F}_q$ and $f \in \mathbb{F}_q[X]$. In this article we consider the evaluation of all Weil sums where $f(X) = aX^{p^\alpha+1} + L(X)$ and $p = 2$. Here, $a \in \mathbb{F}_q$, α is any natural number and $L \in \mathbb{F}_q[X]$ is any additive polynomial (by which it is meant that $L(x+y) = L(x)+L(y)$ for all $x, y \in \mathbb{F}_q$). A result from [4] reduces the problem to the case $\chi = \chi_1$, the canonical additive character, and $L(X) = bX$ for some $b \in \mathbb{F}_q$. Hence our objective in this paper is to explicitly determine the value of the sum

$$S_\alpha(a, b) = \sum_{x \in \mathbb{F}_q} \chi_1(ax^{p^\alpha+1} + bx)$$

for all $a, b \in \mathbb{F}_q$ and where $p = 2$. Carlitz explicitly determined $S_\alpha(a, b)$ with $\alpha = 1$ in [1] (for $p = 2$) and [2] (for p odd). For general α, the author has completed the evaluation of $S_\alpha(a, b)$ in odd characteristic in [3] and [4]. Here, we complete the evaluation of $S_\alpha(a, b)$ for all characteristics by considering the case $p = 2$. For the most part, this article uses methods similar to those developed in [3] and [4], which are generalisations of methods employed by Carlitz in [2].

If t is an integer dividing e then we denote by Tr_t the trace function mapping $\mathbb{F}_q$ onto $\mathbb{F}_{p^t}$. Formally,

$$Tr_t(x) = x + x^{p^t} + x^{p^{2t}} + \ldots + x^{p^{(e/t-1)t}}$$

for all $x \in \mathbb{F}_q$. The absolute trace function, Tr_1, is simply denoted Tr. The trace function satisfies $Tr_t(ax) = aTr_t(x)$, $Tr_t(x + y) = Tr_t(x) + Tr_t(y)$ and $Tr_t(x^{p^t}) = Tr_t(x)$ for all $x, y \in \mathbb{F}_q$ and $a \in \mathbb{F}_{p^t}$. The canonical additive character, χ_1, is given by

$$\chi_1(x) = \exp\big(2\pi i Tr(x)/p\big)$$

for all $x \in \mathbb{F}_q$. Due to the properties of the trace function, $\chi_1(x + y) = \chi_1(x)\chi_1(y)$ and $\chi_1(x^p) = \chi_1(x)$ for all $x, y \in \mathbb{F}_q$. Any additive character of $\mathbb{F}_q$ can be obtained from χ_1: for any $a \in \mathbb{F}_q$, $\chi_a(x) = \chi_1(ax)$ for all $x \in \mathbb{F}_q$. Finally, a polynomial $f \in \mathbb{F}_q[X]$ is called a permutation polynomial if it induces a permutation of $\mathbb{F}_q$.

1991 *Mathematics Subject Classification.* 11T24.
This work was partially supported by an Australian Research Council grant.

Throughout this article, unless otherwise stated, $q = 2^e$ for some integer e and $d = gcd(\alpha, e) = (\alpha, e)$. As $S_\alpha(0,0) = q$ and $S_\alpha(0,b) = 0$ for all $b \in \mathbb{F}_q^*$, we always assume $a \neq 0$. We note that, throughout this article, $\chi_a(x) = \pm 1$ for all $x \in \mathbb{F}_q$ and therefore $S_\alpha(a,b)$ is always an integer. The problem of evaluating $S_\alpha(a,b)$ splits into two distinct cases: e/d odd and e/d even.

2. Preliminary results

In this section, we provide some preliminary results. Our first result concerns greatest common divisors. For want of a reference, we provide a proof.

Lemma 2.1. *Let $d = (\alpha, e)$. Then*

$$(2^\alpha + 1, 2^e - 1) = \begin{cases} 1 & \text{if } e/d \text{ is odd,} \\ 2^d + 1 & \text{if } e/d \text{ is even.} \end{cases}$$

Proof. It is well known that

$$(2^{2\alpha} - 1, 2^e - 1) = 2^{(2\alpha, e)} - 1 = \begin{cases} 2^d - 1 & \text{if } e/d \text{ is odd,} \\ 2^{2d} - 1 & \text{if } e/d \text{ is even.} \end{cases}$$

Further, it is clear that $(2^\alpha + 1, 2^d - 1) = 1$ since $(2^\alpha + 1, 2^\alpha - 1) = 1$. Now

$$\begin{aligned} (2^{2\alpha} - 1, 2^e - 1) &= (2^\alpha - 1, 2^e - 1) \left(2^\alpha + 1, \frac{2^e - 1}{(2^\alpha - 1, 2^e - 1)} \right) \\ &= (2^d - 1) \left(2^\alpha + 1, (2^e - 1)/(2^d - 1) \right) \\ &= (2^d - 1)\, (2^\alpha + 1, 2^e - 1) \end{aligned}$$

from which we can derive the lemma. □

We require the following lemma from [4].

Lemma 2.2 ([4, Lemma 4.2])**.** *Denote by χ_1 the canonical additive character of $\mathbb{F}_q$ with $q = p^e$, p any prime. Let $a \in \mathbb{F}_q$ be arbitrary and let d be some integer dividing e. Then*

$$\sum_{\beta \in \mathbb{F}_{p^d}} \chi_1(a\beta) = \begin{cases} p^d & \text{if } Tr_d(a) = 0, \\ 0 & \text{otherwise.} \end{cases}$$

Theorem 2.3 ([4, Theorem 5.1])**.** *Let $q = p^e$ and $L \in \mathbb{F}_q[X]$ be a linearised polynomial of the form*

$$L(X) = \sum_{i=0}^{e-1} b_i X^{p^i}$$

with $b_i \in \mathbb{F}_q$ for all i. Let χ_c be any additive character of $\mathbb{F}_q$ with $c \in \mathbb{F}_q$ and let $b = \sum_{i=0}^{e-1} (b_i c)^{p^{e-i}}$. Then

$$\sum_{x \in \mathbb{F}_q} \chi_c\big(a x^{p^\alpha + 1} + L(x)\big) = S_\alpha(ca, b).$$

Theorem 2.3 reduces the overall problem to that of evaluating $S_\alpha(a,b)$. Consequently, for the remainder of the paper, we consider $S_\alpha(a,b)$ only.

3. Solvability of the equation $a^{2^\alpha} x^{2^{2\alpha}} + ax = 0$

The next result is the characteristic 2 version of [3, Theorem 4.1]. As in odd characteristic, this theorem plays a central role in the evaluation of $S_\alpha(a, b)$.

Theorem 3.1. *Let g be a primitive element of $\mathbb{F}_q$. For any $a \in \mathbb{F}_q^*$ consider the equation $a^{2^\alpha} x^{2^{2\alpha}} + ax = 0$ over $\mathbb{F}_q$.*

(i) *If e/d is odd then there are 2^d solutions to this equation for any choice of $a \in \mathbb{F}_q^*$.*

(ii) *If e/d is even then there are two possible cases. If $a = g^{t(2^d+1)}$ for some t then there are 2^{2d} solutions to the equation. If $a \neq g^{t(2^d+1)}$ for any t then there exists one solution only, $x = 0$.*

Proof. We wish to solve the equation $x^{2^{2\alpha}-1} = a^{1-2^\alpha}$. Let $a = g^s$ for some integer s. Then we wish to solve for r in the equation

$$g^{r(2^{2\alpha}-1)} = g^{s(1-2^\alpha)}$$

where $x = g^r$. Equivalently, we need to find solutions r of the equation

$$r(2^{2\alpha} - 1) \equiv s(1 - 2^\alpha) \bmod (q - 1).$$

Again recall $iu \equiv v \bmod n$ has a solution i if and only if (u, n) divides v. If e/d is odd we have $(2^{2\alpha}-1, 2^e-1) = 2^d-1$ which divides $s(1-2^\alpha)$ regardless of the choice of s. Thus, for e/d odd, there are always solutions to the equation for any choice of $a \in \mathbb{F}_q^*$. It is obvious that there are 2^d solutions in this case. If e/d is even then $(2^{2\alpha} - 1, 2^e - 1) = 2^{2d} - 1$. This divides $s(1 - 2^\alpha)$ if and only if $s \equiv 0 \bmod (2^d + 1)$ because, by Lemma 2.1, $(2^d + 1, 1 - 2^\alpha) = 1$. If $s \not\equiv 0 \bmod (2^d + 1)$ then $x = 0$ is the only solution. □

4. Evaluating $S_\alpha(a, b)$ when e/d is odd

In this section we assume e/d is odd. The following theorem is a direct consequence of Lemma 2.1.

Theorem 4.1. *Let χ be any non-trivial additive character of $\mathbb{F}_q$. If e/d is odd then*

$$\sum_{x \in \mathbb{F}_q} \chi(ax^{2^\alpha+1}) = \begin{cases} q & \text{if } a = 0, \\ 0 & \text{otherwise.} \end{cases}$$

Note that the evaluation of $S_\alpha(a, 0)$ when e/d is odd is covered by the above theorem. We now consider $S_\alpha(a, b)$ for e/d odd.

Theorem 4.2. *Let $b \in \mathbb{F}_q^*$ and suppose e/d is odd. Then $S_\alpha(a, b) = S_\alpha(1, bc^{-1})$ where $c \in \mathbb{F}_q^*$ is the unique element satisfying $c^{2^\alpha+1} = a$. Further, $S_\alpha(1, b) = 0$ if $Tr_d(b) \neq 1$ and $S_\alpha(1, b) = \pm 2^{(e+d)/2}$ if $Tr_d(b) = 1$.*

Proof. Let e/d be odd. The polynomial $X^{2^\alpha+1}$ is a permutation polynomial over $\mathbb{F}_q$ and so there exists a unique $c \in \mathbb{F}_q^*$ such that $c^{2^\alpha+1} = a$. We have

$$\begin{aligned} S_\alpha(a,b) &= \sum_{x\in\mathbb{F}_q} \chi_1(ax^{2^\alpha+1} + bx) \\ &= \sum_{x\in\mathbb{F}_q} \chi_1\big((cx)^{2^\alpha+1} + bc^{-1}(cx)\big) \\ &= S_\alpha(1, bc^{-1}). \end{aligned}$$

So we need only be concerned with the sum $S_\alpha(1,b)$.

$$\begin{aligned} S_\alpha^2(1,b) &= \sum_{w,y\in\mathbb{F}_q} \chi_1(w^{2^\alpha+1} + bw + y^{2^\alpha+1} + by) \\ &= \sum_{x,y\in\mathbb{F}_q} \chi_1\big((x+y)^{2^\alpha+1} + b(x+y) + y^{2^\alpha+1} + by\big) \\ &= \sum_{x\in\mathbb{F}_q} \Big(\chi_1(x^{2^\alpha+1} + bx) \sum_{y\in\mathbb{F}_q} \chi_1(x^{2^\alpha} y + xy^{2^\alpha})\Big) \\ &= \sum_{x\in\mathbb{F}_q} \Big(\chi_1(x^{2^\alpha+1} + bx) \sum_{y\in\mathbb{F}_q} \chi_1\big(y^{2^\alpha}(x^{2^{2\alpha}} + x)\big)\Big). \end{aligned}$$

The inner sum is zero unless $x^{2^{2\alpha}} + x = 0$, i.e., if $x \in \mathbb{F}_{2^d}$. So we can simplify to

$$\begin{aligned} S_\alpha^2(1,b) &= q \sum_{x\in\mathbb{F}_{2^d}} \chi_1(x^{2^\alpha+1} + bx) \\ &= q \sum_{x\in\mathbb{F}_{2^d}} \chi_1(x^2 + bx) \\ &= q \sum_{x\in\mathbb{F}_{2^d}} \chi_1(x^2)\ \chi_1(bx) \\ &= q \sum_{x\in\mathbb{F}_{2^d}} \chi_1(x)\ \chi_1(bx) \\ &= q \sum_{x\in\mathbb{F}_{2^d}} \chi_1\big(x(b+1)\big) \\ &= \begin{cases} 2^{e+d} & \text{if } Tr_d(1+b) = 0, \\ 0 & \text{if } Tr_d(1+b) \neq 0. \end{cases} \end{aligned}$$

As e/d is odd, $Tr_d(1) = 1$. The result follows. □

We make a few remarks concerning the trace function. These observations are used to prove the next result. There are 2^{e-d} distinct elements $a \in \mathbb{F}_q$ satisfying $Tr_d(a) = 0$. For any element $c \in \mathbb{F}_q$ it is clear that $Tr_d(c^{2^{2\alpha}} + c) = 0$. Furthermore, when e/d is odd the polynomial $X^{2^{2\alpha}} + X$ has 2^{e-d} distinct images as $x^{2^{2\alpha}} + x = y^{2^{2\alpha}} + y$ if and only if $x + y \in \mathbb{F}_{2^d}$. Hence, when e/d is odd, every $a \in \mathbb{F}_q$ which satisfies $Tr_d(a) = 0$ can be written in the form $a = c^{2^{2\alpha}} + c$ for a suitable choice of c. For e/d odd we also have $Tr_d(c^{2^{2\alpha}} + c + 1) = 1$. So every element $b \in \mathbb{F}_q$ satisfying $Tr_d(b) = 1$ can be written in the form $b = c^{2^{2\alpha}} + c + 1$ for a suitable choice of $c \in \mathbb{F}_q$.

Lemma 4.3. *Let $b \in \mathbb{F}_q^*$ satisfy $Tr_d(b) = 1$ and suppose e/d is odd. Then*
$$S_\alpha(1,b) = \chi_1(c^{2^\alpha+1} + c)S_\alpha(1,1)$$
where $b = c^{2^{2\alpha}} + c + 1$ for some $c \in \mathbb{F}_q$.

Proof. Let $c \in \mathbb{F}_q$ satisfy $b = c^{2^{2\alpha}} + c + 1$. We have
$$\begin{aligned}
S_\alpha(1,1) &= \sum_{x\in\mathbb{F}_q} \chi_1(x^{2^\alpha+1} + x)\\
&= \sum_{x\in\mathbb{F}_q} \chi_1\big((x + c^{2^\alpha})^{2^\alpha+1} + (x + c^{2^\alpha})\big)\\
&= \sum_{x\in\mathbb{F}_q} \chi_1(x^{2^\alpha+1} + x + x^{2^\alpha}c^{2^\alpha} + xc^{2^{2\alpha}} + c^{2^{2\alpha}+2^\alpha} + c^{2^\alpha})\\
&= \chi_1(c^{2^{2\alpha}+2^\alpha} + c^{2^\alpha}) \sum_{x\in\mathbb{F}_q} \chi_1\big(x^{2^\alpha+1} + x(1 + c + c^{2^{2\alpha}})\big)\\
&= \chi_1(c^{2^\alpha+1} + c)S_\alpha(1,b).
\end{aligned}$$
As $\chi_1(c^{2^\alpha+1} + c) = \pm 1$ we have the identity claimed. □

In Theorem 4.2 we failed to determine the sign of $S_\alpha(1,b)$ when $Tr_d(b) = 1$. Lemma 4.3 reduces this problem to determining the sign of $S_\alpha(1,1)$, which we shall now do. The method employed is a generalisation of the method used by Carlitz in [1]. We will need the following lemmas on two arithmetic functions.

Lemma 4.4. *Let n and d be any positive integers with n odd. Define $f_d(n)$ to be the arithmetic function*
$$f_d(n) = \sum_{s|n} \mu(n/s)\left[\left(\frac{2}{s}\right)2^{(s-1)/2}\right]^d,$$
where μ is the Möbius function and $\left(\frac{2}{s}\right)$ is the Jacobi symbol. If m is the product of distinct divisors of n then $f_d(n) \equiv 0 \bmod m$.

Proof. It is readily established that $f_d(p) \equiv 0 \bmod p$ for any odd prime p and all positive integers d. Suppose that, for some odd integer n and m the product of distinct divisors of n, we have $f_d(n) \equiv 0 \bmod m$ for all d. Consider $f_d(np)$ for some prime p. We have
$$\begin{aligned}
f_d(np) &= \sum_{s|n, r|p} \mu(np/rs)\left[\left(\frac{2}{sr}\right)2^{(sr-1)/2}\right]^d\\
&= -f_d(n) + \sum_{s|n} \mu(n/s)\left[\left(\frac{2}{sp}\right)2^{(sp-1)/2}\right]^d.
\end{aligned}$$

To begin with,

$$\begin{aligned} f_d(np) &\equiv \sum_{s|n} \mu(n/s) \left[\left(\frac{2}{p}\right)\left(\frac{2}{s}\right)(2^{(s-1)/2})^{p+1} 2^{(p-s)/2} \right]^d \bmod m \\ &\equiv \left[\left(\frac{2}{p}\right) 2^{(p-1)/2} \right]^d \sum_{s|n} \mu(n/s) \left[\left(\frac{2}{s}\right) 2^{(s-1)/2} \right]^{pd} \bmod m \\ &\equiv \left[\left(\frac{2}{p}\right) 2^{(p-1)/2} \right]^d f_{pd}(n) \bmod m \\ &\equiv 0 \bmod m. \end{aligned}$$

If $(n,p) = p$ then we are done. If $(n,p) = 1$ then we also have

$$\begin{aligned} f_d(np) &\equiv -f_d(n) + \sum_{s|n} \mu(n/s) \left[\left(\frac{2}{s}\right) 2^{(p-1)/2} 2^{(sp-1)/2)} \right]^d \bmod p \\ &\equiv -f_d(n) + \sum_{s|n} \mu(n/s) \left[\left(\frac{2}{s}\right) (2^{(p-1)/2})^{s+1} 2^{(s-1)/2)} \right]^d \bmod p \\ &\equiv -f_d(n) + f_d(n) \bmod p \\ &\equiv 0 \bmod p. \end{aligned}$$

Hence, $f_d(np) \equiv 0 \bmod mp$. The lemma follows by induction. □

Lemma 4.5. *Let n and d be any positive integers with n odd. Define $g_d(n)$ to be the arithmetic function*

$$g_d(n) = \sum_{s|n} \mu(n/s) 2^{sd}.$$

If m is the product of distinct divisors of n then $g_d(n) \equiv 0 \bmod m$.

Proof. It is easily established that $g_d(p) \equiv 0 \bmod p$ for any odd prime p and all possible d. Suppose $g_d(n) \equiv 0 \bmod m$ for all d. Consider $g_d(np)$. We have $g_d(np) = g_{dp}(n) - g_d(n)$. Clearly, $g_d(np) \equiv 0 \bmod m$. If $(n,p) = p$ then we are done. If $(n,p) = 1$ then

$$\begin{aligned} g_d(np) &\equiv -g_d(n) + \sum_{s|n} \mu(n/s) 2^{spd} \bmod p \\ &\equiv -g_d(n) + \sum_{s|n} \mu(n/s) 2^{sd} \bmod p \\ &\equiv 0 \bmod p. \end{aligned}$$

Hence, $g_d(np) \equiv 0 \bmod mp$ and the lemma is established. □

Theorem 4.6. *Let e/d be odd. Then $S_\alpha(1,1) = \left(\frac{2}{e/d}\right)^d 2^{(e+d)/2}$*

Proof. By Theorem 4.2, $S_\alpha(1,1) = \varepsilon_{e/d} 2^{(e+d)/2}$. We need to prove $\varepsilon_{e/d} = \left(\frac{2}{e/d}\right)^d$ for all odd e/d. Let

$$N(q) = \#\{(x,y) \in \mathbb{F}_q \times \mathbb{F}_q \mid x^{2^\alpha+1} + x = y^{2^d} + y\}$$

and, for $t \geq 1$, let

$$N'(2^{td}) = \#\{(x,y) \in \mathbb{F}_{2^{td}} \times \mathbb{F}_{2^{td}} \mid x^{2^\alpha+1} + x = y^{2^d} + y \text{ and } x \text{ not in any proper subfield of } \mathbb{F}_{2^{td}} \text{ containing } \mathbb{F}_{2^d}\}.$$

From these definitions it is clear that

$$N(q) = \sum_{s|(e/d)} N'(2^{sd}).$$

By the Möbius Inversion Formula,

$$N'(q) = \sum_{s|(e/d)} \mu\big((e/d)/s\big) N(2^{sd}).$$

Furthermore, in regards to $N'(2^{td})$, if (x,y) is such a solution then $(x^{2^{id}}, y^{2^{id}})$, $0 \leq i \leq t-1$, are also distinct solutions. Hence, $N'(2^{td}) \equiv 0 \bmod t$ and, in particular, $N'(q) \equiv 0 \bmod e/d$. Also, it is easily seen that $N'(2^d) = N(2^d) = 2^{d+1}$. Now

$$\begin{aligned} qN(q) &= \sum_{a\in\mathbb{F}_q}\sum_{x\in\mathbb{F}_q}\left(\chi_1\big(a(x^{2^\alpha+1}+x)\big)\sum_{y\in\mathbb{F}_q}\chi_1\big(y^{2^d}(a^{2^d}+a)\big)\right) \\ &= q\sum_{a\in\mathbb{F}_{2^d}}\sum_{x\in\mathbb{F}_q}\chi_1(ax^{2^\alpha+1}+ax). \end{aligned}$$

As e/d is odd, $X^{2^\alpha+1}$ is a permuation polynomial over $\mathbb{F}_q$. Hence

$$\begin{aligned} N(q) &= q + \sum_{a\in\mathbb{F}_{2^d}^*}\sum_{x\in\mathbb{F}_q}\chi_1(ax^{2^\alpha+1}+ax) \\ &= q + \sum_{\left\{\substack{\gamma\in\mathbb{F}_{2^d}^* \\ \gamma^{2^\alpha+1}=a}\right\}}\sum_{x\in\mathbb{F}_q}\chi_1\big((\gamma x)^{2^\alpha+1}+(a\gamma^{-1})\gamma x\big) \\ &= q + \sum_{\gamma\in\mathbb{F}_{2^d}^*}\sum_{x\in\mathbb{F}_q}\chi_1(x^{2^\alpha+1}+\gamma^{2^\alpha}x) \\ &= q + \sum_{\gamma\in\mathbb{F}_{2^d}^*} S_\alpha(1,\gamma). \end{aligned}$$

However, $S_\alpha(1,\gamma) = 0$ unless $Tr_d(\gamma) = 1$. For $\gamma \in \mathbb{F}_{2^d}^*$, $Tr_d(\gamma) = \gamma$ as e/d is odd. So $N(q) = q + S_\alpha(1,1) = 2^e + \varepsilon_{e/d}2^{(e+d)/2}$, where $\varepsilon_{e/d} = \pm 1$.

We now proceed by induction on e/d. Firstly, suppose $e/d = p$, an odd prime. We have $N'(2^e) \equiv 0 \bmod p$. However,

$$\begin{aligned} N'(2^e) &= N(2^e) - N(2^d) \\ &= 2^e + \varepsilon_{e/d}2^{(e+d)/2} - 2^{d+1} \\ &= (2^{e/d})^d - 2^{d+1} + \varepsilon_{e/d}(2^{((e/d)+1)/2})^d \\ &\equiv (2^p)^d - 2^{d+1} + \varepsilon_p(2^{(p+1)/2})^d \bmod p \\ &\equiv -2^d + 2^d\varepsilon_p\left(\frac{2}{p}\right)^d \bmod p. \end{aligned}$$

Simplifying yields $\varepsilon_{e/d} = \left(\frac{2}{e/d}\right)^d$ if e/d is prime. Now suppose $e/d = p^r$ for p an odd prime and $r > 1$. We have $N'(2^{p^r d}) \equiv 0 \bmod p^r$, in which case $N'(2^{p^r d}) \equiv 0 \bmod p$ also holds. Further,

$$\begin{aligned} N'(2^{p^r d}) &= N(2^{p^r d}) - N(2^{p^{r-1} d}) \\ &= 2^{p^r d} + \varepsilon_{p^r}(2^{(p^r+1)/2})^d - 2^{p^{r-1} d} - \varepsilon_{p^{r-1}}(2^{(p^{r-1}+1)/2})^d. \end{aligned}$$

As $2^{p^r d} \equiv 2^{p^{r-1} d} \bmod p$, we can simplify to the equation

$$\varepsilon_{p^r}\left(\frac{2}{p^r}\right)^d = \varepsilon_{p^{r-1}}\left(\frac{2}{p^{r-1}}\right)^d.$$

As $\varepsilon_p = \left(\frac{2}{p}\right)^d$, induction on r shows $\varepsilon_{p^r} = \left(\frac{2}{p^r}\right)^d$.

It remains to deal with the general case. Let $e/d = n$ be some odd number and m the product of distinct divisors of n. Assume that $\varepsilon_s = \left(\frac{2}{s}\right)^d$ for all proper divisors of n. As before, we have $N'(2^e) \equiv 0 \bmod e/d$, which implies $N'(2^e) \equiv 0 \bmod m$. Also,

$$\begin{aligned} N'(2^e) &= \sum_{s|(e/d)} \mu\big((e/d)/s\big) N(2^{sd}) \\ &= \sum_{s|(e/d)} \mu\big((e/d)/s\big) 2^{sd} + \sum_{s|(e/d)} \mu\big((e/d)/s\big)\varepsilon_s (2^{(s+1)/2})^d \\ &= g_d(n) + \sum_{s|n} \mu(n/s)\varepsilon_s(2^{(s+1)/2})^d \\ &\equiv \sum_{s|n} \mu(n/s)\varepsilon_s(2^{(s+1)/2})^d \bmod m, \end{aligned}$$

where the last step follows from Lemma 4.5. Hence

$$\sum_{s|n} \mu(n/s)\varepsilon_s(2^{(s+1)/2})^d \equiv 0 \bmod m.$$

Dividing by 2^d yields

$$\begin{aligned} 0 &\equiv \sum_{s|n} \mu(n/s)\varepsilon_s(2^{(s-1)/2})^d \bmod m \\ &\equiv \varepsilon_n(2^{(n-1)/2})^d + \sum_{\substack{s|n \\ s<n}} \mu(n/s)\left[\left(\frac{2}{s}\right)2^{(s-1)/2}\right]^d \bmod m \\ &\equiv \varepsilon_n(2^{(n-1)/2})^d + f_d(n) - \left(\frac{2}{n}\right)^d (2^{(n-1)/2})^d \bmod m. \end{aligned}$$

By Lemma 4.4, we have

$$\varepsilon_n(2^{(n-1)/2})^d \equiv \left(\frac{2}{n}\right)^d (2^{(n-1)/2})^d \bmod m$$

from which $\varepsilon_n = \left(\frac{2}{n}\right)^d$. Therefore, by induction, $\varepsilon_{e/d} = \left(\frac{2}{e/d}\right)^d$ for all e/d odd. $\square$

5. Evaluating $S_\alpha(a,b)$ when e/d is even

Throughout this section we assume e/d is even. Our first result determines the absolute value of $S_\alpha(a,0)$ for this case.

Lemma 5.1. *Let e/d be even so that $e = 2m$ for some integer m. Then*

$$S_\alpha(a,0) = \pm\begin{cases} 2^{m+d} & \text{if } a = g^{t(2^d+1)} \text{ for some integer } t,\\ 2^m & \text{if } a \neq g^{t(2^d+1)} \text{ for any integer } t.\end{cases}$$

Proof. We have

$$\begin{aligned} S_\alpha^2(a,0) &= \sum_{w,y\in\mathbb{F}_q} \chi_1(aw^{2^\alpha+1} + ay^{2^\alpha+1}) \\ &= \sum_{x,y\in\mathbb{F}_q} \chi_1\big(a(x+y)^{2^\alpha+1} + ay^{2^\alpha+1}\big) \\ &= \sum_{x\in\mathbb{F}_q}\Big(\chi_1(ax^{2^\alpha+1})\sum_{y\in\mathbb{F}_q}\chi_1(ax^{2^\alpha}y + axy^{2^\alpha})\Big) \\ &= \sum_{x\in\mathbb{F}_q}\Big(\chi_1(ax^{2^\alpha+1})\sum_{y\in\mathbb{F}_q}\chi_1\big((a^{2^\alpha}x^{2^{2\alpha}} + ax)y^{2^\alpha}\big)\Big). \end{aligned}$$

The inner sum is zero unless $a^{2^\alpha}x^{2^{2\alpha}} + ax = 0$, in which case the inner sum is q. If $a \neq g^{t(2^d+1)}$ for any integer t then by Theorem 3.1 we have $S_\alpha(a,0) = \pm 2^m$.

Now suppose $a = g^{t(2^d+1)}$ for some integer t. Let x_0 be any non-zero solution of the equation $a^{2^\alpha}x^{2^{2\alpha}} + ax = 0$. Then there are 2^{2d} solutions of this equation given by βx_0, $\beta \in \mathbb{F}_{2^{2d}}$, see Theorem 3.1. We have

$$S_\alpha^2(a,0) = q\sum_{\beta\in\mathbb{F}_{2^{2d}}}\chi_1(ax_0^{2^\alpha+1}\beta^{2^\alpha+1}).$$

For any non-zero $\beta \in \mathbb{F}_{2^{2d}}$ we have $\beta^{2^\alpha+1} = \delta^{2^d+1} = \gamma \in \mathbb{F}_{2^d}$. Further, every non-zero $\gamma \in \mathbb{F}_{2^d}$ occurs 2^d+1 times. Therefore

$$\begin{aligned} \sum_{\beta\in\mathbb{F}_{2^{2d}}}\chi_1(ax_0^{2^\alpha+1}\beta^{2^\alpha+1}) &= 1 + (2^d+1)\sum_{\gamma\in\mathbb{F}_{2^d}^*}\chi_1(ax_0^{2^\alpha+1}\gamma) \\ &= 1 + (2^d+1)\begin{cases} 2^d-1 & \text{if } Tr_d(ax_0^{2^\alpha+1}) = 0,\\ -1 & \text{if } Tr_d(ax_0^{2^\alpha+1}) \neq 0,\end{cases} \\ &= \begin{cases} 2^{2d} & \text{if } Tr_d(ax_0^{2^\alpha+1}) = 0,\\ -2^d & \text{if } Tr_d(ax_0^{2^\alpha+1}) \neq 0.\end{cases} \end{aligned}$$

The middle step follows from Lemma 2.2. Now $a^{2^\alpha}x_0^{2^{2\alpha}} = ax_0$ and so $(ax_0^{2^\alpha+1})^{2^\alpha} = ax_0^{2^\alpha+1}$. Thus $ax_0^{2^\alpha+1} \in \mathbb{F}_{2^d}$ and since e/d is even we have $Tr_d(ax_0^{2^\alpha+1}) = 0$. This completes the proof. □

It remains to determine the sign.

Theorem 5.2. *Let e/d be even so that $e = 2m$ for some integer m. Then*

$$S_\alpha(a,0) = \begin{cases} (-1)^{m/d}2^m & \text{if } a \neq g^{t(2^d+1)} \text{ for any integer } t,\\ -(-1)^{m/d}2^{m+d} & \text{if } a = g^{t(2^d+1)} \text{ for some integer } t.\end{cases}$$

Proof. Let N denote the number of solutions $(x, y) \in \mathbb{F}_q \times \mathbb{F}_q$ of the equation
$$ax^{2^\alpha+1} = y^{2^d} - y. \tag{1}$$
We have
$$\begin{aligned} qN &= \sum_{w\in\mathbb{F}_q} \sum_{x,y\in\mathbb{F}_q} \chi_1\big(w(ax^{2^\alpha+1} - y^{2^d} + y)\big) \\ &= q^2 + \sum_{w\in\mathbb{F}_q^*} \sum_{x\in\mathbb{F}_q} \Big(\chi_1(awx^{2^\alpha+1}) \sum_{y\in\mathbb{F}_q} \chi_1\big(w(y - y^{2^d})\big)\Big) \\ &= q^2 + \sum_{w\in\mathbb{F}_q^*} \sum_{x\in\mathbb{F}_q} \Big(\chi_1(awx^{2^\alpha+1}) \sum_{y\in\mathbb{F}_q} \chi_1\big(y^{2^d}(w^{2^d} - w)\big)\Big). \end{aligned}$$
The inner sum is zero unless $w^{2^d} = w$, i.e., $w \in \mathbb{F}_{2^d}$. Simplifying yields
$$N = q + \sum_{w\in\mathbb{F}_{2^d}^*} \sum_{x\in\mathbb{F}_q} \chi_1(awx^{2^\alpha+1}).$$
For $w \in \mathbb{F}_{2^d}^*$, the equation $wz_w^{2^\alpha+1} = 1$ is solvable for $z_w \in \mathbb{F}_q$ if $(2^\alpha+1, q-1) = 2^d+1$ divides $(q-1)/(2^d-1)$. If e/d is even then this is always true and so
$$\begin{aligned} N &= q + \sum_{w\in\mathbb{F}_{2^d}^*} \sum_{x\in\mathbb{F}_q} \chi_1(awx^{2^\alpha+1}) \\ &= q + \sum_{w\in\mathbb{F}_{2^d}^*} \sum_{x\in\mathbb{F}_q} \chi_1\big(aw(z_w x)^{2^\alpha+1}\big) \\ &= q + \sum_{w\in\mathbb{F}_{2^d}^*} \sum_{x\in\mathbb{F}_q} \chi_1(ax^{2^\alpha+1}) \\ &= q + (2^d - 1)S_\alpha(a, 0). \end{aligned}$$
Let us return to (1). If (x, y) is a solution with $x \neq 0$ then (wx, y) is also a solution where $w^{2^d+1} = 1$. Therefore the solutions of this equation with $x \neq 0$ occur in batches of size $2^d + 1$. In addition there are 2^d solutions when $x = 0$. So according to this counting argument
$$\begin{aligned} N &\equiv 2^d \bmod (2^d + 1) \\ &\equiv -1 \bmod (2^d + 1). \end{aligned}$$
Combining with our previous identity for N and simplifying we deduce
$$S_\alpha(a, 0) \equiv 1 \bmod (2^d + 1).$$
For d dividing m,
$$2^m \bmod (2^d + 1) = \begin{cases} -1 & \text{if } m/d \text{ odd,} \\ 1 & \text{if } m/d \text{ even.} \end{cases}$$
Suppose first that $a \neq g^{t(2^d+1)}$ for any integer t. By Lemma 5.1, $S_\alpha(a, 0) = \epsilon 2^m$ where $\epsilon = \pm 1$. As $S_\alpha(a, 0) \equiv 1 \bmod (2^d + 1)$,
$$\epsilon = \begin{cases} -1 & \text{if } m/d \text{ odd,} \\ 1 & \text{if } m/d \text{ even} \end{cases}$$

or simply $\epsilon = (-1)^{m/d}$. Now suppose $a = g^{t(2^d+1)}$ for some integer t. Then, by Lemma 5.1, $S_\alpha(a,0) = \kappa 2^{m+d}$, with $\kappa = \pm 1$, whereby $\kappa = -\epsilon$. This completes the proof. □

Finally, we consider $S_\alpha(a,b)$ when e/d is even.

Theorem 5.3. *Let $b \in \mathbb{F}_q^*$ and suppose e/d is even so that $e = 2m$ for some integer m. Let $f(X) = a^{2^\alpha} X^{2^{2\alpha}} + aX$. There are two cases.*

(i) *If $a \neq g^{t(2^d+1)}$ for some integer t then f is a permutation polynomial. Let $x_0 \in \mathbb{F}_q$ be the unique element satisfying $f(x_0) = b^{2^\alpha}$. Then*

$$S_\alpha(a,b) = (-1)^{m/d} 2^m \chi_1(a x_0^{2^\alpha+1}).$$

(ii) *If $a = g^{t(2^d+1)}$ then $S_\alpha(a,b) = 0$ unless the equation $f(x) = b^{2^\alpha}$ is solvable. If the equation is solvable, with solution x_0 say, then*

$$S_\alpha(a,b) = \begin{cases} -(-1)^{m/d} 2^{m+d} \chi_1(a x_0^{2^\alpha+1}) & \text{if } Tr_d(a) = 0, \\ (-1)^{m/d} 2^m \chi_1(a x_0^{2^\alpha+1}) & \text{if } Tr_d(a) \neq 0. \end{cases}$$

Proof. We have

$$\begin{aligned} S_\alpha(a,b) S_\alpha(a,0) &= \sum_{w,y\in\mathbb{F}_q} \chi_1(aw^{2^\alpha+1} + bw)\ \chi_1(ay^{2^\alpha+1}) \\ &= \sum_{x,y\in\mathbb{F}_q} \chi_1\big(a(x+y)^{2^\alpha+1} + b(x+y)\big)\ \chi_1(ay^{2^\alpha+1}) \\ &= \sum_{x,y\in\mathbb{F}_q} \chi_1\big(a(x+y)^{2^\alpha+1} + b(x+y) + ay^{2^\alpha+1}\big) \\ &= \sum_{x\in\mathbb{F}_q} \Big(\chi_1(ax^{2^\alpha+1} + bx) \sum_{y\in\mathbb{F}_q} \chi_1(ax^{2^\alpha} y + axy^{2^\alpha} + by)\Big) \\ &= \sum_{x\in\mathbb{F}_q} \Big(\chi_1(ax^{2^\alpha+1} + bx) \sum_{y\in\mathbb{F}_q} \chi_1\big(y^{2^\alpha}(a^{2^\alpha} x^{2^{2\alpha}} + ax + b^{2^\alpha})\big)\Big) \\ &= \sum_{x\in\mathbb{F}_q} \bigg(\chi_1(ax^{2^\alpha+1} + bx) \sum_{y\in\mathbb{F}_q} \chi_1\Big(y^{2^\alpha}\big(f(x) + b^{2^\alpha}\big)\Big)\bigg). \end{aligned}$$

Again there are two cases depending on whether f is a permutation polynomial or not.

Suppose f is a permutation polynomial. Then, by Theorem 3.1, e/d is even and $a \neq g^{t(2^d+1)}$. The inner sum is zero unless $f(x) = b^{2^\alpha}$. By assumption there exists a unique x_0 satisfying $f(x_0) = b^{2^\alpha}$. Hence the inner sum is zero unless $x = x_0$ in which case it is q. Simplifying yields

$$S_\alpha(a,b) S_\alpha(a,0) = q \chi_1(a x_0^{2^\alpha+1} + b x_0).$$

Since $f(x_0) = b^{2^\alpha}$ we have

$$\begin{aligned} Tr(a x_0^{2^\alpha+1} + b x_0) &= Tr(a^{2^\alpha} x_0^{2^{2\alpha}} x_0^{2^\alpha} + b^{2^\alpha} x_0^{2^\alpha}) \\ &= Tr\big(x_0^{2^\alpha}(b^{2^\alpha} + a x_0) + b^{2^\alpha} x_0^{2^\alpha}\big) \\ &= Tr(a x_0^{2^\alpha+1}). \end{aligned}$$

So $\chi_1(ax_0^{2^\alpha+1}+bx_0)=\chi_1(ax_0^{2^\alpha+1})$. We can complete the proof for this case by applying Theorem 5.2.

Now suppose f is not a permutation polynomial. We have

$$S_\alpha(a,b)S_\alpha(a,0)=\sum_{x\in\mathbb{F}_q}\Big(\chi_1(ax^{2^\alpha+1}+bx)\sum_{y\in\mathbb{F}_q}\chi_1\big(y^{2^\alpha}(a^{2^\alpha}x^{2^{2\alpha}}+ax+b^{2^\alpha})\big)\Big). \quad (2)$$

The inner sum is zero (and so too is $S_\alpha(a,b)$) unless $f(x)=b^{2^\alpha}$ has a solution. If there exists a solution then, overall, there are 2^{2d} solutions given by $x=x_0+c$ where x_0 is any solution of $f(x)=b^{2^\alpha}$ and $c\in\mathbb{F}_{2^{2d}}$. To see that there can only be 2^{2d} solutions suppose x_1 and x_2 are solutions of $f(x)=b^{2^\alpha}$. Then we must have $f(x_1)=f(x_2)$ and $f(x_2-x_1)=0$. This implies that $x_2-x_1=c$ for some $c\in\mathbb{F}_{2^{2d}}$. Thus we have accounted for all solutions of $f(x)=b^{2^\alpha}$. Returning to (2) we obtain

$$S_\alpha(a,b)S_\alpha(a,0)=q\sum_{c\in\mathbb{F}_{2^{2d}}}\chi_1\big(a(x_0+c)^{2^\alpha+1}+b(x_0+c)\big). \quad (3)$$

For any x of the form $x=x_0+c$ we have

$$\begin{aligned}Tr(ax^{2^\alpha+1}+bx)&=Tr\big(a(x_0+c)^{2^\alpha+1}+b(x_0+c)\big)\\&=Tr(ax_0^{2^\alpha+1}+bx_0)+Tr(ac^{2^\alpha+1})\\&\qquad+Tr(acx_0^{2^\alpha}+ac^{2^\alpha}x_0+bc)\\&=Tr(ax_0^{2^\alpha+1}+bx_0)+Tr(ac^{2^\alpha+1})\\&\qquad+Tr\big(c^{2^\alpha}(a^{2^\alpha}x_0^{2^{2\alpha}}+ax_0+b^{2^\alpha})\big)\\&=Tr(ax_0^{2^\alpha+1}+bx_0)+Tr(ac^{2^\alpha+1}).\end{aligned}$$

Applying this identity to (3) yields

$$\begin{aligned}S_\alpha(a,b)S_\alpha(a,0)&=q\sum_{c\in\mathbb{F}_{2^{2d}}}\chi_1(ax_0^{2^\alpha+1}+bx_0)\ \chi_1(ac^{2^\alpha+1})\\&=q\ \chi_1(ax_0^{2^\alpha+1}+bx_0)\sum_{c\in\mathbb{F}_{2^{2d}}}\chi_1(ac^{2^\alpha+1}).\end{aligned}$$

Since $(2^\alpha+1,2^{2d}-1)=2^d+1$ the polynomial $X^{(2^\alpha+1)/(2^d+1)}$ is a permutation polynomial over $\mathbb{F}_{2^{2d}}$. So, by a change of variable, we have

$$S_\alpha(a,b)S_\alpha(a,0)=q\ \chi_1(ax_0^{2^\alpha+1}+bx_0)\sum_{\beta\in\mathbb{F}_{2^{2d}}}\chi_1(a\beta^{2^d+1}). \quad (4)$$

We note that, as in the proof of the first part of this theorem, $\chi_1(ax_0^{2^\alpha+1}+bx_0)=\chi_1(ax_0^{2^\alpha+1})$. Any $\beta\in\mathbb{F}_{2^{2d}}$ satisfies $\beta^{2^d+1}\in\mathbb{F}_{2^d}$ and every element of $\mathbb{F}_{2^d}^*$ will occur 2^d+1 times in this way. Thus the sum in (4) evaluates to

$$\begin{aligned}\sum_{\beta\in\mathbb{F}_{2^{2d}}}\chi_1(a\beta^{2^d+1})&=1+\sum_{\beta\in\mathbb{F}_{2^{2d}}^*}\chi_1(a\beta^{2^d+1})\\&=1+(2^d+1)\sum_{\gamma\in\mathbb{F}_{2^d}^*}\chi_1(a\gamma)\\&=\begin{cases}2^{2d} & \text{if } Tr_d(a)=0,\\ -2^d & \text{otherwise.}\end{cases}\end{aligned}$$

We have shown

$$S_\alpha(a,b)S_\alpha(a,0) = \begin{cases} 2^{e+2d}\chi_1(ax_0^{2^\alpha+1}) & \text{if } Tr_d(a) = 0, \\ -2^{e+d}\chi_1(ax_0^{2^\alpha+1}) & \text{otherwise,} \end{cases}$$

and dividing by $S_\alpha(a,0)$ we obtain the results claimed. □

It is interesting to note that the results for odd and even characteristic are very similar when e/d is even but very different when e/d is odd. The proofs of each of the cases reflect this relationship.

References

1. L. Carlitz, *Explicit evaluation of certain exponential sums*, Math. Scand. **44** (1979), 5–16.
2. ———, *Evaluation of some exponential sums over a finite field*, Math. Nachr. **96** (1980), 319–339.
3. R.S. Coulter, *Explicit evaluations of some Weil sums*, Acta Arithmetica **83** (1998), 241–251.
4. ———, *Further evaluations of Weil sums*, Acta Arithmetica (to appear).

Centre for Discrete Mathematics and Computing, Department of Computer Science and Electrical Engineering, The University of Queensland, St. Lucia, Queensland 4072, Australia.

E-mail address: shrub@csee.uq.edu.au