ACTA ARITHMETICA
LXXXVI.3 (1998)

Further evaluations of Weil sums

by

Robert S. Coulter (St. Lucia, Qld.)

1. Introduction. Weil sums are exponential sums whose summation runs over the evaluation mapping of a particular function. Explicitly they have the form

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

where $\mathbb{F}_q$ denotes the finite field of q elements ($q = p^e$ for p a prime) and $f \in \mathbb{F}_q[X]$. In a recent article [2] the author gave explicit evaluations of all Weil sums with $f(X) = aX^{p^\alpha+1}$ and p odd. These were obtained mostly through generalising methods used by Carlitz in [1] who obtained explicit evaluations of Weil sums with $f(X) = aX^{p+1} + bX$, p odd.

In this article we complete the work begun in [2]. By generalising some of the methods employed by Carlitz in [1] we obtain explicit evaluations of the exponential sums

$$\sum_{x\in\mathbb{F}_q} \chi(ax^{p^\alpha+1} + bx)$$

with $b \neq 0$. Clearly the case $b = 0$ was dealt with in [2]. Further, we highlight our motivation for studying these Weil sums and obtain an alternative, but much longer, proof of when the polynomial $X^{p^\alpha+1}$ is planar (see [4, Theorem 3.3]). We conclude by extending our results to include the explicit evaluations of all Weil sums with $f(X) = aX^{p^\alpha+1} + L(X)$ where $L \in \mathbb{F}_q[X]$ is a linearised polynomial. Theorem 5.1 states the results of this paper in their broadest context.

Throughout this article $\mathbb{F}_q$ will denote the finite field of q elements with $q = p^e$ odd, α will denote a natural number and $d = \gcd(\alpha, e)$. Henceforth, we will use (α, e) as shorthand for $\gcd(\alpha, e)$. We denote the non-zero elements of $\mathbb{F}_q$ by $\mathbb{F}_q^*$. We shall denote by Tr the absolute trace function and use Tr_t to denote the trace function $\mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_{p^t}}$ where t divides e. The canonical additive

1991 *Mathematics Subject Classification*: Primary 11T24.

character of $\mathbb{F}_q$, denoted by χ_1, is given by

$$\chi_1(x) = e^{2\pi i \mathrm{Tr}(x)/p}$$

for all $x \in \mathbb{F}_q$. Note that $\chi_1(x^p) = \chi_1(x)$ and $\chi_1(-x) = \overline{\chi_1(x)}$ for all $x \in \mathbb{F}_q$. Any additive character χ_a of $\mathbb{F}_q$ can be obtained from χ_1 by $\chi_a(x) = \chi_1(ax)$ for all $x \in \mathbb{F}_q$. Due to this fact we only explicitly evaluate the Weil sums with $\chi = \chi_1$ as it is possible to evaluate the Weil sums for any non-trivial additive character simply by manipulating the results obtained (see Theorem 5.1). We denote by $S_\alpha(a, b)$ the Weil sum given by

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

If we now let g be a fixed primitive element of $\mathbb{F}_q$ then we can, for each $j = 0, \ldots, q-2$, define a multiplicative character λ_j of $\mathbb{F}_q$ by

$$\lambda_j(g^k) = e^{2\pi i jk/(q-1)}$$

for $k = 0, \ldots, q-2$. We shall use η to denote the quadratic character of $\mathbb{F}_q$, that is, $\eta = \lambda_{(q-1)/2}$.

As with the results obtained in [2] the results of the current paper split into two distinct cases. In this article the different scenarios that arise depend on whether the polynomial $a^{p^\alpha} X^{p^{2\alpha}} + aX$ is a permutation polynomial or not. A polynomial $f \in \mathbb{F}_q[X]$ is called a *permutation polynomial* if it induces a permutation of $\mathbb{F}_q$. Our two main results concerning the evaluation of $S_\alpha(a, b)$ are given in the following two theorems.

THEOREM 1. *Let q be odd and suppose $f(X) = a^{p^\alpha} X^{p^{2\alpha}} + aX$ is a permutation polynomial over $\mathbb{F}_q$. Let x_0 be the unique solution of the equation $f(x) = -b^{p^\alpha}$, $b \neq 0$. The evaluation of $S_\alpha(a, b)$ partitions into the following two cases.*

(i) *If e/d is odd then*

$$S_\alpha(a, b) = \begin{cases} (-1)^{e-1}\sqrt{q}\,\eta(-a)\,\overline{\chi_1(ax_0^{p^\alpha+1})} & \text{if } p \equiv 1 \bmod 4, \\ (-1)^{e-1} i^{3e}\sqrt{q}\,\eta(-a)\,\overline{\chi_1(ax_0^{p^\alpha+1})} & \text{if } p \equiv 3 \bmod 4. \end{cases}$$

(ii) *If e/d is even then $e = 2m$, $a^{(q-1)/(p^d+1)} \neq (-1)^{m/d}$ and*

$$S_\alpha(a, b) = (-1)^{m/d} p^m\, \overline{\chi_1(ax_0^{p^\alpha+1})}.$$

THEOREM 2. *Let $q = p^e$ be odd and suppose $f(X) = a^{p^\alpha} X^{p^{2\alpha}} + aX$ is not a permutation polynomial over $\mathbb{F}_q$. Then for $b \neq 0$ we have $S_\alpha(a, b) = 0$ unless the equation $f(x) = -b^{p^\alpha}$ is solvable. If this equation is solvable, with some solution x_0 say, then*

$$S_\alpha(a, b) = -(-1)^{m/d} p^{m+d}\, \overline{\chi_1(ax_0^{p^\alpha+1})}.$$

Excluding the last section, the remainder of this paper will be devoted to proving the above two theorems. In the last section we extend the results of this paper and conclude by discussing planar functions and the relevance of the results of this paper to them.

2. Relevant results. The following lemma on greatest common divisors will prove a useful tool.

LEMMA 2.1 ([2, Lemma 2.6]). *Let $d = (\alpha, e)$ and p be odd. Then*

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

The next result will play an important part in the structure and results of this article.

LEMMA 2.2 ([2, Theorem 4.1]). *The equation*

$$a^{p^\alpha} x^{p^{2\alpha}} + ax = 0$$

is solvable for $x \in \mathbb{F}_q^*$ if and only if e/d is even with $e = 2m$ and

$$a^{(q-1)/(p^d+1)} = (-1)^{m/d}.$$

In such cases there are $p^{2d} - 1$ non-zero solutions.

We note that [2, Theorem 4.1] claims this result for e even only. However, the proof given in [2] does not rely on this assumption and in fact proves the more general result given above. We make the following observations in regard to Lemma 2.2. Let $f(X) = a^{p^\alpha} X^{p^{2\alpha}} + aX$. The polynomial f belongs to the well known class of polynomials called linearised (or affine) polynomials. These polynomials have been extensively studied (see [6] for some of their properties). In particular, a linearised polynomial is a permutation polynomial of $\mathbb{F}_q$ if and only if $x = 0$ is its only root in $\mathbb{F}_q$ (see [6, Theorem 7.9]). Lemma 2.2 thus tells us that f is a permutation polynomial of $\mathbb{F}_q$ with $q = p^e$ if and only if e/d is odd or e/d is even with $e = 2m$ and $a^{(q-1)/(p^d+1)} \neq (-1)^{m/d}$.

To end this section we recall the main results on $S_\alpha(a, b)$ obtained in [2].

THEOREM 2.3 ([2, Theorem 1]). *Let e/d be odd. Then*

$$S_\alpha(a, 0) = \begin{cases} (-1)^{e-1} \sqrt{q}\, \eta(a) & \text{if } p \equiv 1 \bmod 4, \\ (-1)^{e-1} i^e \sqrt{q}\, \eta(a) & \text{if } p \equiv 3 \bmod 4. \end{cases}$$

THEOREM 2.4 ([2, Theorem 2]). *Let e/d be even with $e = 2m$. Then*

$$S_\alpha(a,0) = \begin{cases} p^m & \text{if } a^{(q-1)/(p^d+1)} \neq (-1)^{m/d} \text{ and } m/d \text{ is even}, \\ -p^m & \text{if } a^{(q-1)/(p^d+1)} \neq (-1)^{m/d} \text{ and } m/d \text{ is odd}, \\ p^{m+d} & \text{if } a^{(q-1)/(p^d+1)} = (-1)^{m/d} \text{ and } m/d \text{ is odd}, \\ -p^{m+d} & \text{if } a^{(q-1)/(p^d+1)} = (-1)^{m/d} \text{ and } m/d \text{ is even}. \end{cases}$$

It should be clear by referring to Lemma 2.2 that the cases given in Theorems 2.3 and 2.4 differentiate between when the polynomial $a^{p^\alpha}X^{p^{2\alpha}} + aX$ is a permutation polynomial and when it is not.

3. Evaluating $S_\alpha(a,b)$ when $a^{p^\alpha}X^{p^{2\alpha}}+aX$ permutes $\mathbb{F}_q$. Throughout this section we assume that the polynomial $a^{p^\alpha}X^{p^{2\alpha}} + aX$ is a permutation polynomial of $\mathbb{F}_q$. Lemma 2.2 implies that either e/d is odd or that e/d is even with $e = 2m$ and $a^{(q-1)/(p^d+1)} \neq (-1)^{m/d}$.

THEOREM 3.1. *Suppose the polynomial $f(X) = a^{p^\alpha}X^{p^{2\alpha}} + aX$ is a permutation polynomial over $\mathbb{F}_q$. Then*

$$S_\alpha(a,b)S_\alpha(-a,0) = q\,\overline{\chi_1(ax_0^{p^\alpha+1})}$$

where x_0 is the unique solution to the equation

$$a^{p^\alpha}x^{p^{2\alpha}} + ax + b^{p^\alpha} = 0.$$

Proof. We have

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

The inner sum is zero unless $f(x) = -b^{p^\alpha}$. Since f is assumed to be a permutation polynomial there exists a unique x_0 satisfying $f(x_0) = -b^{p^\alpha}$.

So the inner sum is zero unless $x = x_0$ in which case it is q. Finally, we have

$$\begin{aligned}\chi_1(ax_0^{p^\alpha+1} + bx_0) &= \chi_1(x_0(ax_0^{p^\alpha} + b)) \\ &= \chi_1(x_0^{p^\alpha}(ax_0^{p^\alpha} + b)^{p^\alpha}) = \chi_1(x_0^{p^\alpha}(a^{p^\alpha}x_0^{p^{2\alpha}} + b^{p^\alpha})) \\ &= \chi_1(-ax_0^{p^\alpha+1}) = \overline{\chi_1(ax_0^{p^\alpha+1})}\,. \ \blacksquare\end{aligned}$$

Theorem 3.1 clearly outlines how to evaluate $S_\alpha(a, b)$ under the assumed conditions. The proof of Theorem 1 follows by combining Theorems 2.3 and 2.4 with Theorem 3.1. (Note that $i^{-e} = i^{3e}$.) In connection with Theorem 1 we have the following lemma.

LEMMA 3.2. *Let q, $f(X)$ and x_0 be as in Theorem* 1. *If e/d is odd then*

$$x_0 = -\frac{1}{2}\sum_{j=0}^{e/d-1}(-1)^j a^{-(p^{(2j+1)\alpha}+1)/(p^\alpha+1)} b^{p^{(2j+1)\alpha}}.$$

P r o o f. Let j be an integer and raise both sides of the equation $f(x_0) = -b^{p^\alpha}$ by $p^{2j\alpha}$. This gives the equations

$$a^{p^{(2j+1)\alpha}}x_0^{p^{(2j+2)\alpha}} + a^{p^{2j\alpha}}x_0^{p^{2j\alpha}} = -b^{p^{(2j+1)\alpha}}.$$

Now multiplying both sides by $(-1)^j a^{-(p^{(2j+1)\alpha}+1)/(p^\alpha+1)}$ yields the equations

$$\begin{aligned}(-1)^j a^{(p^{(2j+2)\alpha}-1)/(p^\alpha+1)}x_0^{p^{(2j+2)\alpha}} &+ (-1)^j a^{(p^{2j\alpha}-1)/(p^\alpha+1)}x_0^{p^{2j\alpha}} \\ &= -(-1)^j a^{-(p^{(2j+1)\alpha}+1)/(p^\alpha+1)} b^{p^{(2j+1)\alpha}}.\end{aligned}$$

If we now add these equations with $0 \le j \le e/d - 1$ we obtain

$$\begin{aligned}&-\sum_{j=0}^{e/d-1}(-1)^j a^{-(p^{(2j+1)\alpha}+1)/(p^\alpha+1)} b^{p^{(2j+1)\alpha}} \\ &\qquad = x_0 + (-1)^{e/d-1}a^{(p^{(2e/d)\alpha}-1)/(p^\alpha+1)}x_0^{p^{(2e/d)\alpha}} \qquad (1) \\ &\qquad = x_0 + (-1)^{e/d-1}a^{(q^{2\alpha/d}-1)/(p^\alpha+1)}x_0^{q^{2\alpha/d}} \\ &\qquad = x_0(1 + a^{(q^{\alpha/d}-1)(q^{\alpha/d}+1)/(p^\alpha+1)}). \qquad (2)\end{aligned}$$

Since e/d is odd $p^\alpha + 1$ must divide $q^{\alpha/d} + 1$. Therefore $q - 1$ divides $(q^{\alpha/d} - 1)(q^{\alpha/d} + 1)/(p^\alpha + 1)$ and so $a^{(q^{\alpha/d}-1)(q^{\alpha/d}+1)/(p^\alpha+1)} = 1$. Thus the right hand side of (2) simplifies to $2x_0$ and so

$$x_0 = -\frac{1}{2}\sum_{j=0}^{e/d-1}(-1)^j a^{-(p^{(2j+1)\alpha}+1)/(p^\alpha+1)} b^{p^{(2j+1)\alpha}}.$$

We claim this determines the unique solution x_0 satisfying $f(x_0) = -b^{p^\alpha}$. $\blacksquare$

Determining x_0 with e/d even appears to be a more difficult task. By using a similar method to the proof just given, but summing over j for $0 \le j \le m/d-1$, we can arrive at a similar point in the proof. We will find the right hand side of (1) equal to $x_0(1-(-1)^{m/d}a^{(q^{\alpha/d}-1)/(p^\alpha+1)})$. However, it is unclear whether this method then leads to a solution as it is not certain that $a^{(q^{\alpha/d}-1)/(p^\alpha+1)} \neq (-1)^{m/d}$ even though $a^{(q-1)/(p^d+1)} \neq (-1)^{m/d}$.

4. Evaluating $S_\alpha(a,b)$ when $a^{p^\alpha}X^{p^{2\alpha}}+aX$ does not permute $\mathbb{F}_q$. We now assume that the polynomial $f(X) = a^{p^\alpha}X^{p^{2\alpha}}+aX$ is not a permutation polynomial. It is immediate from this assumption that there exist solutions $x \in \mathbb{F}_q^*$ satisfying $f(x) = 0$. That is, there are $x \in \mathbb{F}_q$ satisfying $x^{p^{2\alpha}-1} = -a^{1-p^\alpha}$. The method of evaluation, although slightly more involved, is similar to that used in the previous section.

THEOREM 4.1. *Suppose the polynomial $f(X) = a^{p^\alpha}X^{p^{2\alpha}}+aX$ is not a permutation polynomial over $\mathbb{F}_q$. Then $S_\alpha(a,b) = 0$ unless the equation*

$$f(x) = -b^{p^\alpha} \tag{3}$$

is solvable. If it is solvable then

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

where x_0 is any solution to (3) and $c \in \mathbb{F}_q^*$ satisfies $f(c) = 0$.

Proof. As in the proof of Theorem 3.1 we have

$$S_\alpha(a,b)S_\alpha(-a,0) = \sum_{x\in\mathbb{F}_q}\chi_1(ax^{p^\alpha+1}+bx)\sum_{y\in\mathbb{F}_q}\chi_1(y^{p^\alpha}(f(x)+b^{p^\alpha})). \tag{4}$$

The inner sum is zero (and so too is $S_\alpha(a,b)$) unless $f(x) = -b^{p^\alpha}$ has a solution. Suppose that this equation is solvable. Dividing through by a^{p^α} we have

$$x^{p^{2\alpha}} + a^{1-p^\alpha}x + (ba^{-1})^{p^\alpha} = 0.$$

Let $c \in \mathbb{F}_q^*$ satisfy $f(c) = 0$ so that $c^{p^{2\alpha}-1} = -a^{1-p^\alpha}$. Our equation becomes

$$x^{p^{2\alpha}} - c^{p^{2\alpha}-1}x + (ba^{-1})^{p^\alpha} = 0$$

and dividing by $c^{p^{2\alpha}}$ we obtain

$$(c^{-1}x)^{p^{2\alpha}} - (c^{-1}x) = -(ba^{-1}c^{-p^\alpha})^{p^\alpha}.$$

If this equation is solvable then there are p^{2d} solutions given by $x = x_0 + c\beta$ where x_0 is any solution of (3) and $\beta \in \mathbb{F}_{p^{2d}}$. To see that there can only be p^{2d} solutions suppose x_0 and x_1 are solutions of $f(x) = -b^{p^\alpha}$. Then we must have $f(x_0) = f(x_1)$ and $f(x_0 - x_1) = 0$. This implies that $x_0 - x_1 = \beta c$ for

some $\beta \in \mathbb{F}_{p^{2d}}$. Thus we have accounted for all solutions of (3). Returning to (4) we find

$$S_\alpha(a,b)S_\alpha(-a,0) = q \sum_{\beta\in\mathbb{F}_{p^{2d}}} \chi_1(a(x_0+\beta c)^{p^\alpha+1} + b(x_0+\beta c)). \tag{5}$$

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

$$\begin{aligned}
&\mathrm{Tr}(a(x_0+\beta c)^{p^\alpha+1} + b(x_0+\beta c))\\
&= \mathrm{Tr}(ax_0^{p^\alpha+1} + bx_0) + \mathrm{Tr}(a\beta^{p^\alpha+1}c^{p^\alpha+1}) + \mathrm{Tr}(a\beta c x_0^{p^\alpha} + a\beta^{p^\alpha}c^{p^\alpha}x_0 + b\beta c)\\
&= \mathrm{Tr}(ax_0^{p^\alpha+1} + bx_0) + \mathrm{Tr}(a\beta^{p^\alpha+1}c^{p^\alpha+1}) + \mathrm{Tr}(\beta^{p^\alpha}c^{p^\alpha}(a^{p^\alpha}x_0^{p^{2\alpha}} + ax_0 + b^{p^\alpha}))\\
&= \mathrm{Tr}(ax_0^{p^\alpha+1} + bx_0) + \mathrm{Tr}(a\beta^{p^\alpha+1}c^{p^\alpha+1}).
\end{aligned}$$

Combining this identity with (5) we obtain

$$\begin{aligned}
S_\alpha(a,b)S_\alpha(-a,0) &= q \sum_{\beta\in\mathbb{F}_{p^{2d}}} \chi_1(a(x_0+\beta c)^{p^\alpha+1} + b(x_0+\beta c))\\
&= q \sum_{\beta\in\mathbb{F}_{p^{2d}}} \chi_1(ax_0^{p^\alpha+1} + bx_0)\chi_1(a\beta^{p^\alpha+1}c^{p^\alpha+1})\\
&= q\chi_1(ax_0^{p^\alpha+1} + bx_0) \sum_{\beta\in\mathbb{F}_{p^{2d}}} \chi_1(a\beta^{p^\alpha+1}c^{p^\alpha+1}).
\end{aligned}$$

Finally, we note that, as in the proof of Theorem 3.1, $\chi_1(ax_0^{p^\alpha+1} + bx_0) = \overline{\chi_1(ax_0^{p^\alpha+1})}$. ∎

To complete the evaluation it is clear we must now consider the partial sum

$$\sum_{\beta\in\mathbb{F}_{p^{2d}}} \chi_1(a(\beta c)^{p^\alpha+1}).$$

Related to this partial sum is the following result.

LEMMA 4.2. *Denote by χ_1 the canonical additive character of $\mathbb{F}_q$ with $q = p^e$. Let $a \in \mathbb{F}_q$ be arbitrary and let d be some integer dividing e. Then*

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

Proof. Let μ_1 be the canonical additive character of $\mathbb{F}_{p^d}$. Then for any $x \in \mathbb{F}_q$ we have the following identity (see [6, p. 191]):

$$\chi_1(x) = \mu_1(\mathrm{Tr}_d(x)).$$

Now $\mathrm{Tr}_d(a\beta) = \beta\mathrm{Tr}_d(a)$ for all $\beta \in \mathbb{F}_{p^d}$. Let $t = \mathrm{Tr}_d(a)$. Then $t \in \mathbb{F}_{p^d}$ and for all $\beta \in \mathbb{F}_{p^d}$ we have $\mu_1(t\beta) = \mu_t(\beta)$ where μ_t is some character of $\mathbb{F}_{p^d}$. If we now recall that for any character τ of $\mathbb{F}_{p^d}$,

$$\sum_{\beta\in\mathbb{F}_{p^d}} \tau(\beta) = \begin{cases} p^d & \text{if } \tau \text{ is the trivial character,} \\ 0 & \text{otherwise,} \end{cases}$$

then the result follows. ∎

The previous lemma can be used to evaluate our partial sum.

COROLLARY 4.3. *Let $c \in \mathbb{F}_q^*$ satisfy $f(c) = 0$. Then*

$$\sum_{\beta\in\mathbb{F}_{p^{2d}}} \chi_1(a(\beta c)^{p^\alpha+1}) = p^{2d}.$$

Proof. We have

$$\begin{aligned}\sum_{\beta\in\mathbb{F}_{p^{2d}}} \chi_1(a(\beta c)^{p^\alpha+1}) &= \sum_{\beta\in\mathbb{F}_{p^{2d}}} \chi_1(ac^{p^\alpha+1}\beta^{p^d+1}) \\ &= 1 + (p^d+1)\sum_{\gamma\in\mathbb{F}_{p^d}^*} \chi_1(ac^{p^\alpha+1}\gamma)\end{aligned}$$

as $\beta^{p^d+1} = \gamma \in \mathbb{F}_{p^d}$ for all $\beta \in \mathbb{F}_{p^{2d}}$ and each non-zero element $\gamma \in \mathbb{F}_{p^d}$ occurs p^d+1 times. Recall $\mathrm{Tr}_d(x^{p^d}) = \mathrm{Tr}_d(x)$ for all $x \in \mathbb{F}_q$. As $(ac^{p^\alpha+1})^{p^\alpha} = -ac^{p^\alpha+1}$ we have

$$\begin{aligned}0 &= \mathrm{Tr}_d(ac^{p^\alpha+1}) - \mathrm{Tr}_d(ac^{p^\alpha+1}) = \mathrm{Tr}_d(ac^{p^\alpha+1}) - \mathrm{Tr}_d((ac^{p^\alpha+1})^{p^\alpha}) \\ &= \mathrm{Tr}_d(ac^{p^\alpha+1}) + \mathrm{Tr}_d(ac^{p^\alpha+1}) = 2\mathrm{Tr}_d(ac^{p^\alpha+1}).\end{aligned}$$

Thus $\mathrm{Tr}_d(ac^{p^\alpha+1}) = 0$. The result now follows from the previous lemma. ∎

Having calculated the value of the partial sum we are now able to prove Theorem 2 by joint application of Theorem 2.4 and Corollary 4.3 with Theorem 4.1.

We note that, for the case $\alpha = 1$, Theorem 2 differs from that given by Carlitz in [1] by a factor of $-p$. There Carlitz claims (top of page 329) that since ac^{p+1} is non-zero then

$$\sum_{v\in\mathbb{F}_p^*} \chi_1(vac^{p+1}) = -1.$$

However, this is true if and only if $\mathrm{Tr}(ac^{p+1}) \neq 0$ (see Lemma 4.2). As was shown in the proof of Corollary 4.3, we actually have $\mathrm{Tr}(ac^{p+1}) = 0$. On page 337 of his paper Carlitz makes a similar claim depending on whether $ax_0^{p+1} + bx_0$ is or is not zero. This too should be examining $\mathrm{Tr}(ax_0^{p+1} + bx_0)$ rather than $ax_0^{p+1} + bx_0$. In either of those cases an error of a $-p$ multiple results.

5. Concluding remarks. As $\chi_1(x^p) = \chi_1(x)$ the results of this article can be extended to include all Weil sums with the polynomial of the form

$aX^{p^\alpha+1} + L(X)$ where L is 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. If we let $b \in \mathbb{F}_q$ satisfy $b = \sum_{i=0}^{e-1} b_i^{p^{e-i}}$ then we have

$$\begin{aligned}
\sum_{x\in\mathbb{F}_q} \chi_1(ax^{p^\alpha+1} + L(x)) &= \sum_{x\in\mathbb{F}_q} \chi_1(ax^{p^\alpha+1})\chi_1(L(x)) \\
&= \sum_{x\in\mathbb{F}_q} \chi_1(ax^{p^\alpha+1})\chi_1\Big(\sum_{i=0}^{e-1} b_i x^{p^i}\Big) \\
&= \sum_{x\in\mathbb{F}_q} \chi_1(ax^{p^\alpha+1}) \prod_{i=0}^{e-1} \chi_1(b_i x^{p^i}) \\
&= \sum_{x\in\mathbb{F}_q} \chi_1(ax^{p^\alpha+1}) \prod_{i=0}^{e-1} \chi_1(b_i^{p^{e-i}} x) \\
&= \sum_{x\in\mathbb{F}_q} \chi_1(ax^{p^\alpha+1})\chi_1\Big(x\sum_{i=0}^{e-1} b_i^{p^{e-i}}\Big) = S_\alpha(a,b).
\end{aligned}$$

We have thus shown

THEOREM 5.1. *Let $L \in \mathbb{F}_q[X]$ 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

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

We end with some relevant observations concerning planar functions. Planar functions were introduced by Dembowski and Ostrom in [5] to describe projective planes possessing a collineation group with particular properties. A polynomial $f \in \mathbb{F}_q[X]$ is *planar* if and only if the polynomial $f(X+a) - f(X)$ is a permutation polynomial over $\mathbb{F}_q$ for every $a \in \mathbb{F}_q^*$. Recently, in [3], it was discussed how bent polynomials (as defined there) are the multivariate equivalent of planar polynomials. This gave the following new definition for a planar polynomial: A polynomial $f \in \mathbb{F}_q[X]$ is planar if and only if the Weil sum

$$\sum_{x\in\mathbb{F}_q} \chi(f(x) + \lambda x)$$

has absolute value $q^{1/2}$ for all non-trivial additive characters χ of $\mathbb{F}_q$ and all $\lambda \in \mathbb{F}_q$. One well known class of planar polynomials is the Dembowski–Ostrom polynomials of the form $f(X) = X^{p^\alpha+1} + L(X)$ where L is a linearised polynomial. In [4] it was shown that these are planar if and only if $e/(\alpha, e)$ was odd. It was with this result in mind that an investigation of $S_\alpha(a, b)$ was undertaken. As

$$\chi_1(ax^{p^\alpha+1} + bx) = \chi_a(x^{p^\alpha+1} + (b/a)x)$$

for all $a \neq 0$, a closer inspection of the results obtained in this article reveals that we have obtained an alternative proof of when $X^{p^\alpha+1}$ is planar: the polynomial $a^{p^\alpha} X^{p^{2\alpha}} + aX$ must be a permutation polynomial for all $a \neq 0$. Theorem 2.2 shows that this can occur if and only if e/d is odd. Compare this polynomial with the polynomial $X^{p^\alpha} + X$ which was required to be a permutation polynomial in the proof given in [4]. We note that Theorem 5.1 also concurs with the fact that $X^{p^\alpha+1} + L(X)$ is a planar polynomial if and only if $X^{p^\alpha+1}$ is planar. This is apparent as ultimately the choice of b, whether it be zero or non-zero, does not alter the method of reasoning involved in this new proof of the planarity of $X^{p^\alpha+1}$. So the addition of a linearised polynomial L will not alter the absolute value of the exponential sums involved.

References

[1] L. Carlitz, *Evaluation of some exponential sums over a finite field*, Math. Nachr. 96 (1980), 319–339.

[2] R. S. Coulter, *Explicit evaluations of some Weil sums*, Acta Arith. 83 (1998), 241–251.

[3] R. S. Coulter and R. W. Matthews, *Bent polynomials over finite fields*, Bull. Austral. Math. Soc. 56 (1997), 429–437.

[4] —, —, *Planar functions and planes of Lenz–Barlotti class II*, Des. Codes Cryptogr. 10 (1997), 167–184.

[5] P. Dembowski and T. G. Ostrom, *Planes of order n with collineation groups of order n^2*, Math. Z. 103 (1968), 239–258.

[6] R. Lidl and H. Niederreiter, *Finite Fields*, Encyclopedia Math. Appl. 20, Addison-Wesley, Reading, 1983 (now distributed by Cambridge Univ. Press).

Centre for Discrete Mathematics and Computing
Department of Computer Science and Electrical Engineering
The University of Queensland
St. Lucia, Queensland 4072
Australia
E-mail: shrub@csee.uq.edu.au

Received on 19.8.1997
and in revised form on 28.4.1998 (3247)