EXPONENTIAL SUMS OVER GF($2^n$)

KENNETH S. WILLIAMS
EXPONENTIAL SUMS OVER $GF(2^n)$

KENNETH S. WILLIAMS

Let $F = GF(q)$ denote the finite field with $q = 2^n$ elements. For $f(X) \in F[X]$ we let

$$S(f) = \sum_{x \in F} e(f(x)).$$

A deep result of Carlitz and Uchiyama states that if $f(X) \neq g(X)^2 + g(X) + b, g(X) \in F[X], b \in F$, then

$$|S(f)| \leq (\deg f - 1)q^{1/2}.$$

This estimate is proved in an elementary way when $\deg f = 3, 4, 5$ or 6. In certain cases the estimate is improved.

If $a \in F'$ then $a^{2^n} = a$ and $a$ has a unique square root in $F'$ namely $a^{2^{n-1}}$. We let

$$(1.1) \quad t(a) = a + a^2 + a^3 + \cdots + a^{2^{n-1}},$$

so that $t(a) \in GF(2)$, that is $t(a) = 0$ or 1. We define

$$(1.2) \quad e(a) = (-1)^{t(a)},$$

so that $e(a)$ has the following easily verified properties: for $a_1, a_2 \in F$

$$e(a_1 + a_2) = e(a_1)e(a_2)$$

and

$$(1.3) \quad \sum_{x \in F} e(a_i x) = \begin{cases} q, & \text{if } a_i = 0, \\ 0, & \text{if } a_i \neq 0. \end{cases}$$

Let $X$ denote an indeterminate. For $f(X) \in F[X]$ we consider the exponential sum

$$(1.4) \quad S(f) = \sum_{x \in F} e(f(x)).$$

We note that $S(f)$ is a real number. Since $S(f) = e(f(0))S(f - f(0))$ it suffices to consider only those $f$ with $f(0) = 0$. This will be assumed throughout.

If $f(X) \in F[X](f(0) = 0)$ is such that

$$(1.5) \quad f(X) = g(X)^2 + g(X),$$

for some $g(X) \in F[X]$, then $f(X)$ is called exceptional over $F$, otherwise it is termed regular. Clearly $f$ can be exceptional only if $\deg f$ is even. If $f(X)$ is regular over $F$, Carlitz and Uchiyama [2] have proved (as a special case of a more general result) that

511
Their method appeals to a deep result of Weil [3] concerning the roots of the zeta function of algebraic function fields over a finite field. It is of interest therefore to prove (1.6) in a completely elementary way. That this is possible when $\deg f = 1$ follows from (1.3) and when $\deg f = 2$ from the recent work of Carlitz [1]. In this paper we show that (1.6) can also be proved in an elementary way when $\deg f = 3, 4, 5$ or 6. Moreover in some cases more precise information than that given by (1.6) is obtained. Unfortunately the method used does not appear to apply directly when $\deg f \geq 7$. The method depends on knowing $S(f)$ exactly, when $\deg f = 2$ and when $f$ is exceptional over $F$. These sums are evaluated in §2, 3 respectively.

2. $\deg f = 2$. In this section we evaluate $S(f)$, when $\deg f = 2$. This slightly generalizes a result of Carlitz [1]. We prove

**Theorem 1.** If $f(X) = a_2X^2 + a_1X \in F[X]$, then

$$ S(f) = \begin{cases} q, & \text{if } a_2^p = a_2, \\ 0, & \text{if } a_2^p \neq a_2. \end{cases} $$

**Proof.** We note that the result includes the case $a_2 = 0$ in view of (1.3). If $a_2 \neq 0$ then $S(f) = \sum_{x \in F} e((a_2 x^{2n})^3 + a_1 x^{2n} - (a_2 x^{2n})) = \sum_{x \in F} e(x^3 + a_1 x^{2n} - x^{2n})$, since $x \rightarrow a_2 x^{2n}$ is a bijection on $F$. By Carlitz's result [1]

$$ S(f) = \begin{cases} q, & \text{if } a_1 a_2^{2n-1} = 1, \\ 0, & \text{if } a_1 a_2^{2n-1} \neq 1. \end{cases} $$

This proves the theorem as $a_2 a_2^{2n-1} = 1$ is equivalent to $a_2^p = a_2$ in $F$.

We remark that $a_2X^2 + a_1X$ is exceptional over $F$ precisely when $a_1^p = a_1$.

3. $f$ exceptional over $F$. In this section we evaluate $S(f)$, when $f$ is exceptional over $F$. We prove

**Theorem 2.** If $f(X) \in F[X]$ is exceptional over $F$ then $S(f) = q$.

**Proof.** As $f$ is exceptional over $F$ there exists $g(X) \in F[X]$ such that

$$ f(X) = g(X)^2 + g(X). $$

Hence for $x \in F$ we have

$$ t(f(x)) = t(g(x)^2 + g(x)) = g(x)^{2n} + g(x) = 0, $$
so that $e(f(x)) = 1$, giving $S(f) = q$.

4. deg $f = 3$. We prove

**Theorem 3.** If $f(X) = a_3X^3 + a_2X^2 + a_1X \in F[X]$, where $a_3 \neq 0$, then

$$|S(f)| = K(f)q^{1/2},$$

where $K(f) > 0$ is such that

$$K(f) = 1 + (-1)^n \sum_{t^3 = 1/a_3} e(a_2t^2 + a_1t).$$

(In particular if $t^3 = 1/a_3$ has 0, 1, 3 solutions $t$ in $F$ then $K(f) = 1$, $K(f) = 0$ or $\sqrt{2}$, $K(f) \leq 2$ respectively. Thus we have the Carlitz-Uchiyama estimate $|S(f)| \leq 2q^{1/2}$, and by arranging $K(f) = 2$ in the last of the three possibilities indicated we see that it is best possible).

**Proof.** We have

$$S(f) = \sum_{x,y \in F} e(a_3(x^3 + y^3) + a_2(x^2 + y^2) + a_1(x + y)),$$

so on changing the summation over $x, y$ into one over $x, t(x + y)$ we obtain

$$S(f) = \sum_{t \in F} e(a_3t^3 + a_2t^2 + a_1t) \sum_{x \in F} e(a_3tx^2 + a_2tx).$$

By Theorem 1 we have

$$\sum_{x \in F} e(a_3tx^2 + a_2tx) = \begin{cases} q, & \text{if } a_3t = (a_3t^3)^2, \\ 0, & \text{if } a_3t \neq (a_3t^3)^2, \end{cases}$$

so that, as $a_3 \neq 0$, this gives

$$S(f)^2 = q \sum_{a_3t^3 = 0} e(a_3t^3 + a_2t^2 + a_1t)$$

$$= q\{1 + (-1)^n \sum_{t^3 = 1/a_3} e(a_2t^2 + a_1t)}.$$

as $e(1) = (-1)^n$, which completes the proof of the theorem.

5. deg $f = 4$. We begin by giving necessary and sufficient conditions for $f(X) = a_4X^4 + a_3X^3 + a_2X^2 + a_1X \in F[X]$, where $a_4 \neq 0$, to be exceptional.

**Theorem 4.** $f(X) = a_4X^4 + a_3X^3 + a_2X^2 + a_1X \in F[X]$, where $a_4 \neq 0$, is exceptional over $F$ if and only if $a_4 = a_3^2 + a_1$ and $a_3 = 0$. 


Proof. \( f(X) \) is exceptional over \( F \) if and only if there exists \( rX^2 + sX \in F[X] \) such that
\[
a_4X^4 + a_3X^3 + a_2X^2 + a_1X = (rX^2 + sX)^2 + (rX^2 + sX).
\]
This is possible if and only if
\[
a_4 = r^2, \quad a_3 = 0, \quad a_2 = s^2 + r, \quad a_1 = s,
\]
that is, if and only if,
\[
a_4 = r^2 = (a_2 + s^2)^2 = a_2^2 + s^4 = a_2^2 + a_1^2 \quad \text{and} \quad a_3 = 0.
\]
We now evaluate \(|S(f)|\). We prove

**Theorem 5.** If \( f(X) = a_4X^4 + a_3X^3 + a_2X^2 + a_1X \in F[X] \), where \( a_4 \neq 0 \), then \(|S(f)|\) is given as follows:

(i) \( a_3 = 0 \)
\[
S(f) = \begin{cases} q, & \text{if } a_4 = a_2^2 + a_1^2, \\ 0, & \text{if } a_4 \neq a_2^2 + a_1^2. \end{cases}
\]

(ii) \( a_3 \neq 0 \)
\[
|S(f)| = K(f)q^{1/2},
\]
where \( K(f) > 0 \) is such that
\[
K(f)^2 = 1 + (-1)^n \sum_{t \in F} e(a_4t^4 + a_2t^2 + a_1t).
\]
(Thus in particular when \( f \) is regular we have \( K(f) \leq 2 \) so the Carlitz-Uchiyama estimate \(|S(f)| \leq 3q^{1/2}\) can be improved to \(|S(f)| \leq 2q^{1/2}\)).

Proof. (i) For \( l \in F \) we define
\[
T(l) = \sum_{x \in F} e((a_2^2 + a_1^2 + b)x^4 + a_3x^2 + a_4x).
\]
By Theorem 4 \( (a_2^2 + a_1^2)X^4 + a_2X^2 + a_1X \) is exceptional over \( F \) so that by Theorem 2, \( T(0) = q \). Now
\[
T(l)^2 = \sum_{x,y \in F} e((a_2^2 + a_1^2 + b)^4 + a_2(x^4 + y^4) + a_4(x + y))
\]
\[
= \sum_{x,t \in F} e((a_2^2 + a_1^2 + b)t^4 + a_2t^2 + a_1t),
\]
on setting \( y = x + t \). Thus we have \( T(l)^2 = qT(l) \), so that \( T(l) = 0 \) or \( q \). But we have
\[
\sum_{l \in F} T(l) = \sum_{x \in F} e((a_2^2 + a_1^2)x^4 + a_3x^2 + a_4x) \sum_{l \in F} e(lx^4) = q,
\]
that is,
\[ \sum_{t \neq 0} T(l) = 0, \]
giving \( T(l) = 0 \), when \( l \neq 0 \). This completes the proof of case (i).

(ii) We have as before
\[ S(f)^2 = \sum_{t \neq 0} e(a_5 t^4 + a_3 t^3 + a_1 t) \sum_{x \in F} e(a_5 t x^4 + a_3 t x^3 + a_1 t) \cdot \]
Now by Theorem 1 we have
\[ \sum_{x \in F} e(a_5 t x^4 + a_3 t x^3 + a_1 t) = \begin{cases} q, & \text{if } a_3 t = (a_5 t)^2, \\ 0, & \text{if } a_3 t \neq (a_5 t)^2, \end{cases} \]
so that, as \( a_3 \neq 0 \), we obtain
\[ S(f)^2 = q \sum_{a_3 t \neq 0} e(a_5 t^4 + a_3 t^3 + a_1 t) = q \{ 1 + (-1)^{\sigma} \sum_{t \in \alpha} e(a_5 t^4 + a_3 t^3 + a_1 t) \}, \]
which completes the proof of the theorem.

6. \( \deg f = 5 \). We prove the Carlitz-Uchiyama estimate in an elementary way.

**Theorem 6.** If \( f(X) = a_5 X^5 + a_4 X^4 + a_3 X^3 + a_2 X^2 + a_1 X \in F[X] \), where \( a_5 \neq 0 \), then \(|S(f)| \leq 4q^{1/2}\).

**Proof.** As before we have
\[ S(f)^2 = \sum_{x \in F} e(a_5 t^3 + \cdots + a_1 t) \sum_{x \in F} e(a_5 t x^4 + a_3 t x^3 + (a_5 t^4 + a_3 t^3) x). \]
By Theorem 5 we have
\[ \sum_{x \in F} e(a_5 t x^4 + a_3 t x^3 + (a_5 t^4 + a_3 t^3) x) = \begin{cases} q, & \text{if } a_3 t = (a_5 t)^3 + (a_5 t^4 + a_3 t^3)^4, \\ 0, & \text{if } a_3 t \neq (a_5 t)^3 + (a_5 t^4 + a_3 t^3)^4, \end{cases} \]
and as \( a_3 t^4 = a_3 t^8 + a_3 t^2 + a_3 t + a_3 t = 0 \) has at most 16 solutions \( t \) in \( F \) we have
\[ |S(f)|^2 \leq 16 q, \quad |S(f)| \leq 4q^{1/2}. \]

7. \( \deg f = 6 \). We begin by giving necessary and sufficient conditions for \( f(X) = a_6 X^6 + \cdots + a_1 X \in F[X] \), where \( a_6 \neq 0 \), to be excep-
ATIONAL OVER $F$.

**Theorem 7.** $f(X) = a_6 X^6 + a_5 X^5 + a_4 X^4 + a_3 X^3 + a_2 X^2 + a_1 X \in F[X]$, where $a_6 \neq 0$, is exceptional over $F$ if and only if $a_6 = a_5^2$, $a_5 = 0$, $a_4 = a_2^2 + a_1^2$.

**Proof.** $f(X)$ is exceptional over $F$ if and only if there exists $r X^3 + s X^2 + t X \in F[X]$ such that

$$a_6 X^6 + \cdots + a_5 X = (r X^3 + s X^2 + r X)^2 + (r X^3 + s X^2 + t X)$$

This is possible if, and only if, we can solve the equations

$$a_6 = r^2, a_5 = 0, a_4 = s^2, a_3 = r, a_2 = t^2 + s, a_1 = t,$$

that is if, and only if,

$$a_6 = a_5^2, a_5 = 0, a_4 = s^2 = (a_2 + t^2)^2 = a_2^2 + t^2 = a_2^2 + a_1^2.$$

We now evaluate $|S(f)|$. We prove

**Theorem 8.** If $f(X) = a_6 X^6 + a_5 X^5 + a_4 X^4 + a_3 X^3 + a_2 X^2 + a_1 X \in F[X]$, where $a_6 \neq 0$, then $|S(f)|$ is given as follows:

(i) $a_5 = 0, a_6 = a_2^2$

$$S(f) = \begin{cases} q, & \text{if } a_4 = a_2^2 + a_1^2, \\ 0, & \text{if } a_4 \neq a_2^2 + a_1^2. \end{cases}$$

(ii) $a_5 = 0, a_6 \neq a_2^2$

$$|S(f)| \leq \sqrt{1 + n_1(f)} q^{1/2},$$

where $n_1(f)$ denotes the number of solutions $t \in F$ of

$$t^2 = \frac{1}{a_6 + a_5^2}.$$

(iii) $a_5 \neq 0$

$$|S(f)| \leq \sqrt{1 + n_2(f)} q^{1/2},$$

where $n_2(f)$ denotes the number of solutions $t \in F$ of

$$(7.1) \quad a_5^2 t^{15} + (a_6^2 + a_5^2) t^7 + (a_6 + a_5^2) t + a_5 = 0.$$

(Thus in particular when $f$ is regular we have

$$|S(f)| \leq \sqrt{1 + 15} q^{1/2} = 4q^{1/2},$$

which improves the Carlitz-Uchiyama estimate $|S(f)| \leq 5 q^{1/2}$.)
Proof. (i) For \( l \in F \) we define

\[
T(l) = \sum_{x \in F} e(a_2^2 x^6 + (a_2^2 + a_1^4 + l)x^4 + a_2 x^3 + a_3 x^2 + a_3 x) .
\]

By Theorem 7 \( a_2^2 X^6 + (a_2^2 + a_1^4)X^4 + a_3 X^3 + a_3 X^2 + a_3 X \) is exceptional over \( F \) so that by Theorem 2, \( T(0) = q \). Now

\[
T(l) = \sum_{x, y \in F} e(a_2^2 (x^6 + y^6) + (a_2^2 + a_1^4 + l)(x^4 + y^4) + a_2(x^3 + y^3)
+ a_3(x^2 + y^2) + a_3(x + y))
= \sum_{x, t \in F} e(a_2^2 (x^6 t + x^4 t^2 + t^6) + (a_2^2 + a_1^4 + l)t^4 + a_2(x^6 t + x^4 t^2
+ t^6) + a_3 t^4 + a_3 t) ,
\]
on setting \( y = x + t \). Thus we have

\[
T(l) = \sum_{x, t \in F} e(a_2^2 (x^6 t + (a_2^2 + a_1^4 + l)t^4 + a_2 t^4 + a_3 t^4 + a_3 t))
\sum_{x, t \in F} e((a_2^2 t^6) x^4 + (a_2^2 t^4 + a_3 t)t^3 + (a_2^2 t^3) x) .
\]

Now as \( a_0 = a_1^2 \) and \( a_0 \neq 0 \) we have \( a_3 \neq 0 \). Hence for \( t \neq 0 \) by Theorem 4 \( (a_2^2 t^6)X^4 + (a_2^2 t^4 + a_3 t + a_3 t)X^2 + (a_2^2 t^3)X \) is exceptional as \( a_2^2 t^3 \neq 0 \) and

\[
(a_2^2 t^4 + a_3 t)^3 = a_2^2 t^3 + a_2^2 t^3 = a_2^2 t^2 .
\]

Thus for \( t \neq 0 \) by Theorem 2

\[
\sum_{x \in F} e((a_2^2 t^6) x^4 + (a_2^2 t^4 + a_3 t)x^2 + (a_2^2 t^3) x) = q .
\]

This is clearly true for \( t = 0 \) as well so that \( T(l) = qT(l) \), giving \( T(l) = 0 \) or \( q \). But we have

\[
\sum_{i \in F} T(l) = \sum_{x \in F} e(a_2^2 x^6 + (a_2^2 + a_1^4) x^4 + a_2 x^3 + a_3 x^2 + a_3 x) \sum_{i \in F} e(i x^4) = q ,
\]
that is

\[
\sum_{0 \neq i \in F} T(l) = 0 ,
\]
giving \( T(l) = 0 \), when \( l \neq 0 \). This completes the proof of case (i).

(ii) As before we have

\[
S(f)^2 = \sum_{i \in F} e((a_0 t^6 + a_1 t^4 + a_2 t^3 + a_3 t))
\times \sum_{x \in F} e((a_0 t^6 + a_2 t^3 + a_3 t) x^3 + (a_2 t^3) x) .
\]

By Theorems 1 and 5 we have

\[
\sum_{x \in F} e((a_0 t^6 + a_2 t^3 + a_3 t) x^3 + (a_2 t^3) x)
= \begin{cases} q, & \text{if } a_0 t^2 = (a_0 t^4 + a_3 t)^2 + (a_2 t^3)^4 , \\ 0, & \text{if } a_0 t^2 \neq (a_0 t^4 + a_3 t)^2 + (a_2 t^3)^4 . \end{cases}
\]
Thus

\[ S(f)^2 = q \sum_{t \in \mathbb{F}} e(a_6 t^6 + a_7 t^7 + a_5 t^5 + a_4 t^4 + a_1 t) , \]

where the dash (') denotes that the sum is over those \( t \) such that

\[ (a_6 + a_7^2) t^6 + (a_6 + a_7^2) t^2 = 0 . \]

For \( t \neq 0 \) this becomes

\[ t^6 = \frac{1}{a_6 + a_7^2} , \]

as \( a_6 + a_7^2 \neq 0 \) in view of \( a_6 \neq a_7^2 \). This completes case (ii).

(iii) As before we have

\[ S(f)^2 = \sum_{t \in \mathbb{F}} e(a_6 t^6 + \cdots + a_1 t) \sum_{t \in \mathbb{F}} e((a_6 t^6 + a_7 t)x^6 + (a_6 t^7 + a_5 t)x^5 + \cdots) . \]

By Theorems 1 and 5 we have

\[ \sum_{t \in \mathbb{F}} e((a_6 t^6 + a_7 t)x^6 + (a_6 t^7 + a_5 t)x^5 + (a_4 t^4 + a_3 t^3)X) = \begin{cases} q, & \text{if } a_6 t^6 + a_7 t = (a_6 t^6 + a_7 t)^2 + (a_5 t^4 + a_3 t^3)X \\ 0, & \text{if } a_6 t^6 + a_7 t \neq (a_6 t^6 + a_7 t)^2 + (a_5 t^4 + a_3 t^3)X \end{cases} . \]

Thus

\[ S(f)^2 = q \sum_{t \in \mathbb{F}} e(a_6 t^6 + \cdots + a_1 t) , \]

where the dagger (\(^\dagger\)) denotes that the sum is over those \( t \) such that

\[ a_5 t^6 + (a_5 + a_7) t^5 + (a_6 + a_7^2) t^2 + a_2 t = 0 . \]

For \( t \neq 0 \) this becomes (7.1) which completes the proof of case (iii).

7. Conclusion. We conclude by remarking that the elementary method of this paper does not work when \( \deg f(X) = 7 \), since in this case we have

\[ S(f)^2 = \sum_{t \in \mathbb{F}} e(a_6 t^6 + \cdots + a_1 t) \sum_{x \in \mathbb{F}} e(g_t(x)) , \]

where

\[ g_t(X) = (a_7 t)X^7 + (a_7 t)X^6 + (a_5 t^5 + a_7 t^5 + a_7 t)X^4 + (a_4 t^4)X^3 + (a_4 t^3 + a_7 t^3 + a_7 t^2)X^2 + (a_4 t^2 + a_7 t^2 + a_7 t)X \]

has a nonzero coefficient of \( X^5 \) for \( t \neq 0 \).
REFERENCES


Received August 6, 1970.

Carleton University
Louis I. Alpert and L. V. Toralballa, *An elementary definition of surface area in $E^{n+1}$ for smooth surfaces* ................................................................. 261
Eamon Boyd Barrett, *A three point condition for surfaces of constant mean curvature* ................................................................. 269
Jan-Erik Björk, *On the spectral radius formula in Banach algebras* .... 279
Peter Botta, *Matrix inequalities and kernels of linear transformations* ...... 285
Bennett Eisenberg, *Baxter’s theorem and Varberg’s conjecture* .......... 291
Heinrich W. Guggenheimer, *Approximation of curves* ......................... 301
A. Hedayat, *An algebraic property of the totally symmetric loops associated with Kirkman-Steiner triple systems* ............................................. 305
Richard Howard Herman and Michael Charles Reed, *Covariant representations of infinite tensor product algebras* ................................. 311
Domingo Antonio Herrero, *Analytic continuation of inner function-operators* ................................................................. 327
Franklin Lowenthal, *Uniform finite generation of the affine group* .... 341
Stephen H. McCleary, *0-primitive ordered permutation groups* ........ 349
Malcolm Jay Sherman, *Disjoint maximal invariant subspaces* ............. 373
Mitsuru Nakai, *Radon-Nikodým densities and Jacobians* .................... 375
Mitsuru Nakai, *Royden algebras and quasi-isometries of Riemannian manifolds* ................................................................. 397
Russell Daniel Rupp, Jr., *A new type of variational theory sufficiency theorem* ................................................................. 415
Helga Schirmer, *Fixed point and coincidence sets of biconnected multifunctions on trees* ................................................................. 445
Murray Silver, *On extremal figures admissible relative to rectangular lattices* ................................................................. 451
James DeWitt Stein, *The open mapping theorem for spaces with unique segments* ................................................................. 459
Arne Stray, *Approximation and interpolation* ........................................ 463
Donald Curtis Taylor, *A general Phillips theorem for $C^*$-algebras and some applications* ................................................................. 477
Florian Vasilescu, *On the operator $M(Y) = TYS^{-1}$ in locally convex algebras* ................................................................. 489
Philip William Walker, *Asymptotics for a class of weighted eigenvalue problems* ................................................................. 501
Kenneth S. Williams, *Exponential sums over $GF(2^n)$* ........................ 511