PACIFIC JOURNAL OF MATHEMATICS
Vol. 40, No. 2, 1972

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

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

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

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

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

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

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

$$\sum_{x \in F} e(a_1 x) = \begin{cases} q, \text{ if } a_1 = 0 , \\ 0, \text{ if } a_1 \neq 0 . \end{cases} \tag{1.3}$$

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

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

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

$$f(X) = g(X)^2 + g(X) , \tag{1.5}$$

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

$$|S(f)| \leqq (\deg f - 1)q^{1/2} . \tag{1.6}$$

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 $\deg f \geqq 7$. 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*

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

Proof. We note that the result includes the case $a_2 = 0$ in view of (1.3). If $a_2 \neq 0$ then $S(f) = \sum_{x \in F} e((a_2^{2^{n-1}}x)^2 + a_1a_2^{-2^{n-1}}(a_2^{2^{n-1}}x)) = \sum_{x \in F} e(x^2 + a_1a_2^{-2^{n-1}}x)$, since $x \to a_2^{-2^{n-1}}x$ is a bijection on F. By Carlitz's result [1]

$$S(f) = \begin{cases} q, & \text{if } a_1a_2^{-2^{n-1}} = 1 , \\ 0, & \text{if } a_1a_2^{-2^{n-1}} \neq 1 . \end{cases}$$

This proves the theorem as $a_1a_2^{-2^{n-1}} = 1$ is equivalent to $a_1^2 = a_2$ in F.

We remark that $a_2X^2 + a_1X$ is exceptional over F precisely when $a_1^2 = a_2$.

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

$$t(f(x)) = t(g(x)^2 + g(x)) = g(x)^{2^n} + g(x) = 0 ,$$

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*

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

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

Proof. We have

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

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

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

By Theorem 1 we have

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

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

$$\begin{aligned} S(f)^2 &= q \sum_{\substack{t \in F \\ a_3t^4 - t = 0}} e(a_3t^3 + a_2t^2 + a_1t) \\ &= q\{1 + (-1)^n \sum_{\substack{t \in F \\ t^3 = 1/a_3}} e(a_2t^2 + a_1t)\} , \end{aligned}$$

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* $a_4 = a_2^2 + a_1^4$ *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

$$a_4 = r^2,\ a_3 = 0,\ a_2 = s^2 + r,\ a_1 = s ,$$

that is, if and only if,

$$a_4 = r^2 = (a_2 + s^2)^2 = a_2^2 + s^4 = a_2^2 + a_1^4 \text{ and } a_3 = 0 .$$

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) $a_3 = 0$

$$S(f) = \begin{cases} q, & \textit{if } a_4 = a_2^2 + a_1^4 , \\ 0, & \textit{if } a_4 \neq a_2^2 + a_1^4 . \end{cases}$$

(ii) $a_3 \neq 0$

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

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

$$K(f)^2 = 1 + (-1)^n \sum_{\substack{t \in F \\ t^3 = 1/a_3}} e(a_4t^4 + a_2t^2 + a_1t) .$$

(Thus in particular when f is regular we have $K(f) \leqq 2$ so the Carlitz-Uchiyama estimate $|S(f)| \leqq 3q^{1/2}$ can be improved to $|S(f)| \leqq 2q^{1/2}$).

Proof. (i) For $l \in F$ we define

$$T(l) = \sum_{x \in F} e((a_2^2 + a_1^4 + l)x^4 + a_2x^2 + a_1x) .$$

By Theorem 4 $(a_2^2 + a_1^4)X^4 + a_2X^2 + a_1X$ is exceptional over F so that by Theorem 2, $T(0) = q$. Now

$$\begin{aligned} T(l)^2 &= \sum_{x,y \in F} e((a_2^2 + a_1^4 + l)(x^4 + y^4) + a_2(x^2 + y^2) + a_1(x + y)) \\ &= \sum_{x,t \in F} e((a_2^2 + a_1^4 + l)t^4 + a_2t^2 + a_1t) , \end{aligned}$$

on setting $y = x + t$. Thus we have $T(l)^2 = qT(l)$, so that $T(l) = 0$ or q. But we have

$$\sum_{l \in F} T(l) = \sum_{x \in F} e((a_2^2 + a_1^4)x^4 + a_2x^2 + a_1x) \sum_{l \in F} e(lx^4) = q ,$$

that is,

$$\sum_{0 \neq l \in F} T(l) = 0 ,$$

giving $T(l) = 0$, when $l \neq 0$. This completes the proof of case (i).

(ii) We have as before

$$S(f)^2 = \sum_{t \in F} e(a_4 t^4 + a_3 t^3 + a_2 t^2 + a_1 t) \sum_{x \in F} e(a_3 t x^2 + a_3 t^2 x) .$$

Now by Theorem 1 we have

$$\sum_{x \in F} e(a_3 t x^2 + a_3 t^2 x) = \begin{cases} q, \text{ if } a_3 t = (a_3 t^2)^2 , \\ 0, \text{ if } a_3 t \neq (a_3 t^2)^2 , \end{cases}$$

so that, as $a_3 \neq 0$, we obtain

$$\begin{aligned} S(f)^2 &= q \sum_{\substack{t \in F \\ a_3 t^4 - t = 0}} e(a_4 t^4 + a_3 t^3 + a_2 t^2 + a_1 t) \\ &= q\{1 + (-1)^n \sum_{\substack{t \in F \\ t^3 = 1/a_3}} e(a_3 t^4 + a_2 t^2 + a_1 t)\} , \end{aligned}$$

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* $|S(f)| \leqq 4q^{1/2}$.

Proof. As before we have

$$S(f)^2 = \sum_{t \in F} e(a_5 t^5 + \cdots + a_1 t) \sum_{x \in F} e(a_5 t x^4 + a_3 t x^2 + (a_5 t^4 + a_3 t^2) x) .$$

By Theorem 5 we have

$$\sum_{x \in F} e(a_5 t x^4 + a_3 t x^2 + (a_5 t^4 + a_3 t^2) x) = \begin{cases} q, \text{ if } a_5 t = (a_3 t)^2 + (a_5 t^4 + a_3 t^2)^4 , \\ 0, \text{ if } a_5 t \neq (a_3 t)^2 + (a_5 t^4 + a_3 t^2)^4 , \end{cases}$$

and as $a_5^2 t^{16} + a_3^2 t^8 + a_3^2 t^2 + a_5 t = 0$ has at most 16 solutions t in F we have

$$|S(f)|^2 \leqq 16\, q, \ |S(f)| \leqq 4\, q^{1/2} .$$

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-

tional over F.

THEOREM 7. *$f(X) = a_6X^6 + a_5X^5 + a_4X^4 + a_3X^3 + a_2X^2 + a_1X \in F[X]$, where $a_6 \neq 0$, is exceptional over F if and only if $a_6 = a_3^2$, $a_5 = 0$, $a_4 = a_2^2 + a_1^4$.*

Proof. $f(X)$ is exceptional over F if and only if there exists $rX^3 + sX^2 + tX \in F[X]$ such that

$$a_6X^6 + \cdots + a_1X = (rX^3 + sX^2 + rX)^2 + (rX^3 + sX^2 + tX) .$$

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,

$$a_6 = a_3^2,\ a_5 = 0,\ a_4 = s^2 = (a_2 + t^2)^2 = a_2^2 + t^4 = a_2^2 + a_1^4 .$$

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

THEOREM 8. *If $f(X) = a_6X^6 + a_5X^5 + a_4X^4 + a_3X^3 + a_2X^2 + a_1X \in F[X]$, where $a_6 \neq 0$, then $|S(f)|$ is given as follows:*

(i) $a_5 = 0$, $a_6 = a_3^2$

$$S(f) = \begin{cases} q, & \text{if } a_4 = a_2^2 + a_1^4 , \\ 0, & \text{if } a_4 \neq a_2^2 + a_1^4 . \end{cases}$$

(ii) $a_5 = 0$, $a_6 \neq a_3^2$

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

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

$$t^6 = \frac{1}{a_6 + a_3^2} .$$

(iii) $a_5 \neq 0$

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

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

$$a_5^4t^{15} + (a_6^2 + a_3^4)t^7 + (a_6 + a_3^2)t + a_5 = 0 . \tag{7.1}$$

(Thus in particular when f is regular we have

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

which improves the Carlitz-Uchiyama estimate $|S(f)| \leqq 5\, q^{1/2}$).

Proof. (i) For $l \in F$ we define

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

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

$$\begin{aligned} T(l)^2 &= \sum_{x, y \in F} e(a_3^2(x^6 + y^6) + (a_2^2 + a_1^4 + l)(x^4 + y^4) + a_3(x^3 + y^3) \\ &\quad + a_2(x^2 + y^2) + a_1(x + y)) \\ &= \sum_{x, t \in F} e(a_3^2(x^4 t^2 + x^2 t^4 + t^6) + (a_2^2 + a_1^4 + l)t^4 + a_3(x^2 t + x t^2 \\ &\quad + t^3) + a_2 t^2 + a_1 t) , \end{aligned}$$

on setting $y = x + t$. Thus we have

$$\begin{aligned} T(l)^2 &= \sum_{t \in F} e(a_3^2 t^6 + (a_2^2 + a_1^4 + l)t^4 + a_3 t^3 + a_2 t^2 + a_1 t) \\ &\quad \sum_{x \in F} e((a_3^2 t^2)x^4 + (a_3^2 t^4 + a_3 t)x^2 + (a_3 t^2)x) . \end{aligned}$$

Now as $a_6 = a_3^2$ and $a_6 \neq 0$ we have $a_3 \neq 0$. Hence for $t \neq 0$ by Theorem 4 $(a_3^2 t^2)X^4 + (a_3^2 t^4 + a_3 t + a_3 t)X^2 + (a_3 t^2)X$ is exceptional as $a_3^2 t^2 \neq 0$ and

$$(a_3^2 t^4 + a_3 t)^2 + (a_3 t^2)^4 = a_3^4 t^8 + a_3^2 t^2 + a_3^4 t^8 = a_3^2 t^2 .$$

Thus for $t \neq 0$ by Theorem 2

$$\sum_{x \in F} e((a_3^2 t^2)x^4 + (a_3^2 t^4 + a_3 t)x^2 + (a_3 t^2)x) = q .$$

This is clearly true for $t = 0$ as well so that $T(l)^2 = qT(l)$, giving $T(l) = 0$ or q. But we have

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

that is

$$\sum_{0 \neq l \in F} T(l) = 0 ,$$

giving $T(l) = 0$, when $l \neq 0$. This completes the proof of case (i).
(ii) As before we have

$$\begin{aligned} S(f)^2 &= \sum_{t \in F} e(a_6 t^6 + a_4 t^4 + a_3 t^3 + a_2 t^2 + a_1 t) \\ &\quad \times \sum_{x \in F} e((a_6 t^2)x^4 + (a_6 t^4 + a_3 t)x^2 + (a_3 t^2)x) . \end{aligned}$$

By Theorems 1 and 5 we have

$$\begin{aligned} &\sum_{x \in F} e((a_6 t^2)x^4 + (a_6 t^4 + a_3 t)x^2 + (a_3 t^2)x) \\ &= \begin{cases} q, \text{ if } a_6 t^2 = (a_6 t^4 + a_3 t)^2 + (a_3 t^2)^4 , \\ 0, \text{ if } a_6 t^2 \neq (a_6 t^4 + a_3 t)^2 + (a_3 t^2)^4 . \end{cases} \end{aligned}$$

Thus

$$S(f)^2 = q \sum_{t \in F}{}' e(a_6t^6 + a_4t^4 + a_3t^3 + a_2t^2 + a_1t) ,$$

where the dash (′) denotes that the sum is over those t such that

$$(a_6 + a_3^2)^2t^8 + (a_6 + a_3^2)t^2 = 0 .$$

For $t \neq 0$ this becomes

$$t^6 = \frac{1}{a_6 + a_3^2} ,$$

as $a_6 + a_3^2 \neq 0$ in view of $a_6 \neq a_3^2$. This completes case (ii).

(iii) As before we have

$$S(f)^2 = \sum_{t \in F} e(a_6t^6 + \cdots + a_1t) \sum_{x \in F} e((a_6t^2 + a_5t)x^4 + (a_6t^4 + a_3t)x^2 + (a_5t^4 + a_3t^2)x) .$$

By Theorems 1 and 5 we have

$$\sum_{x \in F} e((a_6t^2 + a_5t)x^4 + (a_6t^4 + a_3t)x^2 + (a_5t^4 + a_3t^2)x) = \begin{cases} q, \text{ if } a_6t^2 + a_5t = (a_6t^4 + a_3t)^2 + (a_5t^4 + a_3t^2)^4 , \\ 0, \text{ if } a_6t^2 + a_5t \neq (a_6t^4 + a_3t)^2 + (a_5t^4 + a_3t^2)^4 . \end{cases}$$

Thus

$$S(f)^2 = q \sum_{t \in F}{}^{\dagger} e(a_6t^6 + \cdots + a_1t) ,$$

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

$$a_5^4t^{16} + (a_6^2 + a_3^4)t^8 + (a_6 + a_3^2)t^2 + a_5t = 0 .$$

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

$$S(f)^2 = \sum_{t \in F} e(a_7t^7 + \cdots + a_1t) \sum_{x \in F} e(g_t(x)) ,$$

where

$$g_t(X) = (a_7t)X^6 + (a_7t^2)X^5 + (a_7t^3 + a_6t^2 + a_5t)X^4 + (a_7t^4)X^3 + (a_7t^5 + a_6t^4 + a_3t)X^2 + (a_7t^6 + a_5t^4 + a_3t^2)X$$

has a *nonzero* coefficient of X^5 for $t \neq 0$.

REFERENCES

1. L. Carlitz, *Gauss sums over finite fields of order* 2^n, Acta Arithmetica, **15** (1969), 247–265.
2. L. Carlitz and S. Uchiyama, *Bounds for exponential sums*, Duke Math. J., **24** (1957), 37–41.
3. A. Weil, *On the Riemann hypothesis in function fields*, Proc. Nat. Acad. of Sci., **27** (1941), 345–347.

Received August 6, 1970.

CARLETON UNIVERSITY