MATH. SCAND. 44 (1979), 5–16

EXPLICIT EVALUATION OF CERTAIN EXPONENTIAL SUMS

L. CARLITZ

1. Introduction.

Let $F = \mathrm{GF}\,(q)$ denote the finite field of order $q = p^n$, p prime, $n \geqq 1$. For $a \in F$ put

$$t(a) = a + a^p + \ldots + a^{p^{n-1}}$$

and

$$e(a) = e^{2\pi i t(a)/p} .$$

Define the exponential sums

$$S(a,b) = \sum_{x \in F} e(ax^3 + bx) \tag{1.1}$$

and

$$T(a,b) = \sum_{x \in F} e(ax^6 + bx^2) . \tag{1.2}$$

In an earlier paper [1] the writer proved that, for $p > 3$, $a \neq 0$,

$$\psi(3a)T(a,b)G = S^2(4a,b) + \psi(3a)S(a,b)G - q , \tag{1.3}$$

where $\psi(a) = +1, -1, 0$ according as a is a nonzero square, a non-square or the zero element of F, and G is the Gauss sum defined by

$$G = \sum_{x \in F} \psi(x)e(x) . \tag{1.4}$$

Since $|G| = q^{\frac{1}{2}}$, it follows from (1.3) that the two estimates

$$S(a,b) = O(q^{\frac{1}{2}}), \qquad T(a,b) = O(q^{\frac{1}{2}})$$

are equivalent.

The case $p = 3$ is of little interest. We have

$$S(a^3,b) = \begin{cases} q & (a+b=0) \\ 0 & (a+b \neq 0) , \end{cases}$$

Received May 29, 1978.

$$T(a^3, b) = \begin{cases} q & (a+b=0) \\ \psi(a+b)G & (a+b\neq 0) \end{cases}$$

The case $p=2$ is more interesting. Since $e(a)=e(a^2)$ it follows that

$$T(a^2, b^2) = S(a, b) .$$

Also it is clear from the definition of $e(a)$ that $S(a,b)$ is now a rational integer. It is proved in [1] that, for $q=2^n$,

$$S^2(a,b) = (1-e(bu_0))q \quad (n \text{ odd}) , \tag{1.5}$$

where u_0 is the unique solution of $au^3=1$. For n even we have

$$S^2(a,b) = \begin{cases} q & (au^3=1 \text{ not solvable}) \\ (1+e(bu_0)+e(bu_1)+e(bu_2))q & \end{cases} , \tag{1.6}$$

where u_0, u_1, u_2 are the three solutions of $au^3=1$. It is assumed throughout that $a\neq 0$. The coefficient of q in the second half of (1.6) is equal to 0 or 4. Thus $S(a,b)$ is evaluated except for sign.

The object of the present note is to determine the sign of $S(a,b)$. The cases n even and n odd require separate treatment. We show in particular that, for $n=2m$, $a \in F$, $a\neq 0$,

$$S(a,0) = \begin{cases} (-1)^{m+1}2^{m+1} \\ (-1)^m 2^m , \end{cases}$$

according as a is or is not a cube in F. For the general case, if $a=c^3$, $c \in F$, then

$$S(c^3, b) = \begin{cases} (-1)^{m+1}2^{m+1}e(u_0^3) \\ 0 \end{cases} ,$$

according as

$$\sum_{j=0}^{m-1} (bc^{-1})^{2^{2j}} = 0$$

is or is not satisfied; u_0 denote any solution of the equation $u^4+u=b^2c^{-2}$. If $a \neq c^3$, $c \in F$, then

$$S(a,b) = (-1)^m 2^m e(ax_0^3) ,$$

where x_0 is the unique solution of $a^2x^4+ax=b^2$.

For $n=2m+1$ it suffices to take $b=1$. We show that

$$S(1,1) = \left(\frac{2}{2m+1}\right)2^{m+1} ,$$

where $(2/2m+1)$ is the Jacobi symbol (quadratic character). If $e(b) = -1$, we may put $b = c^4 + c + 1$; then

$$S(1,b) = e(c^3+c)\left(\frac{2}{2m+1}\right)2^{m+1}.$$

Finally

$$S(1,b) = 0 \qquad (e(b) = +1).$$

For a fuller statement of the results see Theorems 1 and 2 below.

2.

We consider first the case n even. Then $3 \mid q-1$. Let χ denote a non-principal cubic character of the multiplicative group of the nonzero elements of F. Define

$$R(\chi) = \sum_{a \in F} \chi(a)e(a). \tag{2.1}$$

We have

$$\begin{aligned}|R(\chi)|^2 &= R(\chi)R(\bar{\chi}) = \sum_{a,b} \chi(a)\bar{\chi}(b)e(a+b) \\ &= \sum_{a,b} \chi(ab^2)e(a+b) = \sum_{a,b \neq 0} \chi(a)e(ab+b) \\ &= \sum_a \chi(a) \sum_b e((a+1)b),\end{aligned}$$

so that

$$|R(\chi)|^2 = q. \tag{2.2}$$

Similarly

$$\begin{aligned}R^2(\chi) &= \sum_{a,b} \chi(ab)e(a+b) = \sum_{a,b \neq 0} \chi(a)e(ab^2+b) \\ &= \sum_a \chi(a) \sum_b e((a+1)b^2)\end{aligned}$$

and therefore

$$R^2(\chi) = q. \tag{2.3}$$

Comparison of (2.2) and (2.3) gives

$$R(\chi) = R(\bar{\chi}), \tag{2.4}$$

so that $R(\chi)$ is a rational integer.

We now define the sums

$$(2.5)\qquad \begin{aligned} S_0 &= \tfrac{1}{3}\sum_{a\neq 0} e(a^3) \\ S_1 &= \tfrac{1}{3}\sum_{a\neq 0} e(ba^3) \qquad (\chi(b)=\omega) \\ S_2 &= \tfrac{1}{3}\sum_{a\neq 0} e(ca^3) \qquad (\chi(c)=\omega^2)\,, \end{aligned}$$

where $\omega=(1+\sqrt{-3})/2$. It is evident that S_0, S_1, S_2 are rational integers.

It follows from (2.1) and (2.5) that

$$(2.6)\qquad \begin{aligned} -1 &= S_0+S_1+S_2 \\ R(\chi) &= S_0+\omega S_1+\omega S_1+\omega^2 S_2 \\ R(\chi^2) &= S_0+\omega^2 S_1+\omega S_2 \end{aligned}$$

and

$$(2.7)\qquad \begin{aligned} 3S_0 &= -1+2R(\chi) \\ 3S_1 &= -1-R(\chi) \\ 3S_2 &= -1-R(\chi)\,. \end{aligned}$$

It is clear, by (2.3), that

$$(2.8)\qquad R(\chi) = \pm 2^m \qquad (n=2m)\,.$$

By (2.7) we have

$$(2.9)\qquad R(\chi) \equiv -1 \pmod 3\,,$$

so that (2.8) becomes

$$(2.10)\qquad R(\chi) = (-1)^{m-1}2^m\,.$$

It then follows from (2.7) that

$$(2.11)\qquad \begin{cases} 3S_0 = -1+(-1)^{m-1}2^{m+1} \\ 3S_1 = 3S_2 = -1+(-1)^m 2^m\,. \end{cases}$$

The sum

$$(2.12)\qquad S(a) = S(a,0) = \sum_x e(ax^3) \qquad (a\neq 0)$$

can now be evaluated. Clearly

$$S(a) = \begin{cases} 1+3S_0 & (\chi(a)=1) \\ 1+3S_1 & (\chi(a)\neq 1)\,. \end{cases}$$

Hence we have

(2.13)
$$S(a) = \begin{cases} (-1)^{m-1}2^{m+1} & (\chi(a)=1) \\ (-1)^m 2^m & (\chi(a)\neq 1)\,. \end{cases}$$

3.

The product

(3.1)
$$\begin{aligned} S(a)S(a,b) &= \sum_{x,y} e(ax^3+ay^3+by) \\ &= \sum_{x,y} e(a(x+y)^3+ay^3+by) \\ &= \sum_{x} e(ax^3) \sum_{y} e(ax^2y+axy^2+by)\,. \end{aligned}$$

The inner sum is equal to

$$\sum_{y} e((a^2x^4+ax+b^2)y)\,.$$

This sum vanishes unless

(3.2)
$$a^2x^4+ax = b^2\,.$$

There are two cases to consider according as $a=c^3$, $c \in \mathrm{GF}(q)$, or $a \neq c^3$). In the first case, (3.2) becomes

(3.3)
$$u^4+u = b^2c^{-2} \qquad (u=cx)\,.$$

This equation is solvable in GF (q) if and only if [2, p. 29]

(3.4)
$$\sum_{j=0}^{m-1} (bc^{-1})^{2^{2j}} = 0 \qquad (n=2m)\,.$$

When (3.4) is satisfied, the four solutions of (3.3) are given by

(3.5)
$$u_0,\ u_1 = u_0+1,\ u_0+\theta,\ u_0+\theta^2\,,$$

where u_0 is any solution of (3.3) and $\theta \in \mathrm{GF}(4)$, $\theta^2=\theta+1$.

Thus (3.1) becomes

(3.6)
$$S(c^3)S(c^3,b) = q\sum_{u_i} e(u_i^3)\,,$$

where the summation is over the four values (3.5). Now

$$\begin{aligned} t((u_0+1)^3) &= t(u_0^3)+t(u_0^2+u_0)+t(1) = t(u_0^3) \\ t((u_0+\theta)^3) &= t(u_0^3)+t(u_0^2\theta+u_0\theta^2)+t(1) = t(u_0^3)\,, \end{aligned}$$

so that (3.6) reduces to

$$S(c^3)S(c^3,b) = 4qe(u_0^3) = 2^{2m+2}e(u_0^3)\,. \tag{3.7}$$

Therefore, by the first of (2.13), we get

$$S(c^3,b) = (-1)^{m+1}2^{m+1}e(u_0^3) \tag{3.8}$$

provided (3.4) is satisfied. If (3.4) is not satisfied, $S(c^3,b)=0$.

Returning to (3.2), assume now that $a \neq c^3$, $c \in \mathrm{GF}\,(q)$. Then, by (3.2),

$$a^{2^{2j}}x^{2^{2j+2}} + x^{2^{2j}} = (a^{-1}b^2)^{2^{2j}} \qquad (j=0,1,\ldots,m-1)\,.$$

Multiply both sides by

$$a^{1+2^2+\ldots+2^{2j-2}} = a^{(2^{2j}-1)/3}$$

and add the resulting equations:

$$(a^{(2^{2m}-1)/3}+1)x = \sum_{j=0}^{m-1} (a^{-1}b^2)^{2^{2j}}a^{(2^{2j}-1)/3}\,. \tag{3.9}$$

Since $a \neq c^3$, the coefficient of x does not vanish; moreover it is easily verified that the value of x given by (3.9) satisfies (3.2). Let x_0 denote this value. Then (3.1) gives

$$S(a)S(a,b) = qe(ax_0^3) = 2^{2m}e(ax_0^3)\,. \tag{3.10}$$

Hence by the second of (2.13), (3.10) reduces to

$$S(a,b) = (-1)^m 2^m e(ax_0^3) \qquad (\chi(a) \neq 1)\,. \tag{3.11}$$

Summing up the results of section 2, 3, we state the following

THEOREM 1. *Let* $q=2^{2m}$, $a,b \in \mathrm{GF}\,(q)$, $a \neq 0$, $b \neq 0$,

$$S(a,b) = \sum_{x\in \mathrm{GF}(q)} e(ax^3+bx), \qquad S(a) = S(a,0)\,.$$

Then

$$S(a) = \begin{cases} (-1)^{m+1}2^{m+1} \\ (-1)^m 2^m\,, \end{cases}$$

according as a is or is not a cube in $\mathrm{GF}(q)$.

If $a=c^3$, $c \in \mathrm{GF}\,(q)$, *then*

$$S(c^3,b) = \begin{cases} (-1)^{m+1}2^{m+1}e(u_0^3) \\ 0 \end{cases},$$

according as

$$\sum_{j=0}^{m-1} (bc^{-1})^{2^{2j}} = 0$$

is or is not satisfied; u_0 *denotes any solution of* $u^4+u=b^2c^{-2}$.

If $a \neq c^3$, $c \in \mathrm{GF}(q)$, *then*

$$S(a,b) = (-1)^m 2^m e(ax_0^3) ,$$

where x_0 *is the unique solution of* $a^2x^4+ax=b^2$ *given by* (3.9).

4.

Let $q=2^n$, $n=2m+1$. In this case the sum

$$\sum_{x \in \mathrm{GF}(q)} e(ax^3) = \sum_x e(ax) = 0 \qquad (a \neq 0) .$$

Also, if $a \neq 0$, then $a=c^3$, $c \in \mathrm{GF}(q)$, so that

$$\sum_x e(ax^3+bx) = \sum_x e(c^3x^3+bx) = \sum_x e(x^3+bc^{-1}x) .$$

Hence there is no loss in restricting the discussion to

$$S(1,b) = \sum_x e(x^3+bx) . \tag{4.1}$$

In particular put

$$S = S(1,1) = \sum_x e(x^3+x) . \tag{4.2}$$

Then

$$\begin{aligned} S^2 &= \sum_{x,y} e(x^3+y^3+x+y) \\ &= \sum_{x,y} e((x+y)^3+y^3+(x+y)+y) \\ &= \sum_x e(x^3+x) \sum_y e(x^2y+xy^2) . \end{aligned} \tag{4.3}$$

The inner sum is equal to

$$\sum_y e((x^4+x)y^2) = 0$$

unless

$$x^4+x = 0 . \tag{4.4}$$

The four solutions of (4.4) constitute the GF (2^2). Since $q=2^{2m+1}$, the only solutions of (4.4) that lie in GF (q) are $x=0$ and $x=1$. Hence (4.3) gives

$$S^2 = 2q = 2^{2m+2} , \tag{4.5}$$

so that $S \neq 0$.

In (4.2) replace x by $x+c^2$. We get

$$\begin{aligned} S &= \sum_x e((x+c^2)^3+x+c^2) \\ &= e(c^6+c^2) \sum_x e(x^3+c^2x^2+c^4x+x) \\ &= e(c^3+c) \sum_x e(x^3+(c^4+c+1)x) . \end{aligned}$$

Thus

$$S(1, c^4+c+1) = e(c^3+c)S . \tag{4.6}$$

Let b denote any number of GF (q) such that $e(b) = -1$, that is, any number that satisfies

$$b+b^2+b^{2^2}+\ldots+b^{2^{2m}} = 1 . \tag{4.7}$$

Exactly half the numbers of GF (q) satisfy (4.7). Then $b = a+1$, where $e(a) = +1$, so that $a = c_1^2+c_1$, $c_1 \in$ GF (q). Since either c_1 or c_1+1 is equal to c^2+c, we get $a = c^4+c$, $c \in$ GF (q). Hence $b = c^4+c+1$, that is, every solution of (4.7) is of this form and the corresponding sum $S(1,b)$ satisfies (4.6).

Next let $e(b) = +1$. Then

$$\begin{aligned} S^2(1,b) &= \sum_{x,y} e(x^3+y^3+bx+by) \\ &= \sum_{x,y} e(x^3+x^2y+xy^2+bx) \\ &= \sum_x e(x^3+bx) \sum_y e(x^2y+xy^2) \\ &= \sum_x e(x^3+bx) \sum_y e((x^4+x)y^2) \\ &= q(1+e(b+1)) = 0 . \end{aligned}$$

Thus

$$S(1,b) = 0 \qquad (e(b) = +1) . \tag{4.8}$$

Hence, in view of (4.6), it will suffice to evaluate S. Indeed, by (4.5),

$$S = \varepsilon \cdot 2^{m+1} \qquad (\varepsilon = \pm 1) . \tag{4.9}$$

To determine ε let $N = N(q)$ denote the number of solutions $x, y \in$ GF (q) of

$$x^3+x = y^2+y; \tag{4.10}$$

also let $N' = N'(q)$ denote the number of solutions $x, y \in \mathrm{GF}(q)$ of (4.10) such that x is not in any proper subfield of $\mathrm{GF}(q)$. If (x, y) is such a solution then

$$(x^{2^j}, y^{2^j}) \qquad (j=0,1,\ldots,2m)$$

are also such solutions and are all distinct. Hence we have

$$N'(2^{2m+1}) \equiv 0 \pmod{2m+1}\,. \tag{4.11}$$

Also clearly $N'(2)=4$.

As for $N(q)$, we have

$$\begin{aligned} qN(q) &= \sum_a \sum_{x,y} e(a(x^3+x+y^2+y)) \\ &= q^2 + \sum_{a \neq 0} \sum_x e(a(x^3+x)) \sum_y e(a(y^2+y))\,. \end{aligned}$$

The sum on the extreme right is equal to

$$\sum_y e((a+a^2)y^2) = 0 \qquad (a+a^2 \neq 0)\,.$$

Hence

$$N(q) = q+S\,. \tag{4.12}$$

It is clear from the definition of $N(q)$ and $N'(q)$ that

$$N(2^{2m+1}) = \sum_{d \mid 2m+1} N'(2^d)\,.$$

Hence, by the Möbius inversion formula,

$$N'(2^{2m+1}) = \sum_{d \mid 2m+1} \mu\left(\frac{2m+1}{d}\right) N(2^d)\,. \tag{4.13}$$

By (4.9) and (4.12) we have

$$N(2^n) = 2^n + \varepsilon_n \cdot 2^{(n+1)/2} \qquad (\varepsilon_n = \pm 1); \tag{4.14}$$

the fuller notation ε_n is needed for what follows.

To begin with we take $2m+1=p$, where p is prime. Then (4.13) becomes

$$\begin{aligned} N'(2^p) &= N(2^p) - N(2) \\ &= 2^p + \varepsilon_p \cdot 2^{(p+1)/2} - 4\,. \end{aligned}$$

Thus, by (4.11),

$$\varepsilon_p \cdot 2^{(p-1)/2} \equiv 1 \pmod{p}\,,$$

so that $\varepsilon_p = (2/p)$, the Legendre symbol.

Next let $2m+1 = p^r$. Then

$$N'(2^{p^r}) = 2^{p^r} + \varepsilon_{p^r} \cdot 2^{(p^r+1)/2} - 2^{p^{r-1}} - \varepsilon_{p^{r-1}} \cdot 2^{(p^{r-1}+1)/2} ,$$

so that, by (4.11),

$$\varepsilon_{p^r} \cdot 2^{(p^r-1)/2} \equiv \varepsilon_{p^{r-1}} \cdot 2^{(p^{r-1}-1)/2} \pmod p .$$

It follows that

$$\varepsilon_{p^r} = \left(\frac{2}{p}\right)^r = \left(\frac{2}{p^r}\right). \tag{4.15}$$

We shall show that generally

$$\varepsilon_{2m+1} = \left(\frac{2}{2m+1}\right), \tag{4.16}$$

the Jacobi symbol. The following lemma will be used.

LEMMA. *We have*

$$\sum_{rs=2m+1} \mu(r)\left(\frac{2}{s}\right)2^{(s-1)/2} \equiv 0 \pmod M , \tag{4.17}$$

where M denotes the product of the distinct prime divisors of $2m+1$.

PROOF. Let $f(2m+1)$ denote the left member of (4.17). It is easily seen that $f(2m+1)$ is a factorable function of $2m+1$. For $2m+1$ equal to a prime power p^r we have

$$\begin{aligned} f(p^r) &= \left(\frac{2}{p^r}\right)2^{(p^r-1)/2} - \left(\frac{2}{p^{r-1}}\right)2^{(p^{r-1}-1)/2} \\ &\equiv \left(\frac{2}{p^r}\right)\left(\frac{2}{p}\right)^r - \left(\frac{2}{p^{r-1}}\right)\left(\frac{2}{p}\right)^{r-1} \equiv 0 \pmod p . \end{aligned}$$

This completes the proof of the lemma.

We shall now prove (4.16). By (4.13) and (4.14),

$$N'(2^{2m+1}) = \sum_{rs=2m+1} \mu(r)2^s + \sum_{rs=2m+1} \mu(r)\varepsilon_s \cdot 2^{(s+1)/2} . \tag{4.18}$$

It is well known that

$$\sum_{rs=2m+1} \mu(r)2^s \equiv 0 \pmod{2m+1} .$$

Hence (4.18) implies

$$\sum_{rs=2m+1} \mu(r)\varepsilon_s \cdot 2^{(s+1)/2} \equiv 0 \pmod M . \tag{4.19}$$

Assume that

$$\varepsilon_s = \left(\frac{2}{s}\right) \tag{4.20}$$

for all *proper* divisors of $2m+1$. Then (4.19) becomes

$$\sum_{\substack{rs=2m+1\\ s<2m+1}} \mu(r)\left(\frac{2}{s}\right)2^{(s+1)/2} + \varepsilon_{2m+1}\cdot 2^{m+1} \equiv 0 \pmod{M}\,.$$

By (4.17),

$$\sum_{\substack{rs=2m+1\\ s<2m+1}} \mu(r)\left(\frac{2}{s}\right)2^{(s+1)/2} + \left(\frac{2}{2m+1}\right)2^{m+1} \equiv 0 \pmod{M}$$

and therefore

$$\varepsilon_{2m+1} = \left(\frac{2}{2\mathrm{m}+1}\right).$$

Thus (4.9) becomes

$$S = \left(\frac{2}{2m+1}\right)2^{m+1} \qquad (q=2^{2m+1}) \tag{4.21}$$

and (by 4.6),

$$S(1,c^4+c+1) = e(c^3+c)\left(\frac{2}{2m+1}\right)2^{m+1}\,. \tag{4.22}$$

We may now state

THEOREM 2. *Let* $q=2^{2m+1}$, $b\neq 0$,

$$S(1,b) = \sum_{x\in \mathrm{GF}(q)} e(x^3+bx)\,.$$

Then

$$S(1,1) = \left(\frac{2}{2m+1}\right)2^{m+1}\,,$$

where $(2/2m+1)$ *is the Jacobi symbol. If* $e(b)=-1$, *put* $b=c^4+c+1$; *then*

$$S(1,b) = e(c^3+c)\left(\frac{2}{2m+1}\right)2^{m+1}\,.$$

Finally

$$S(1,b) = 0 \qquad (e(b) = +1)\,.$$

REFERENCES

1. L. Carlitz, *A note on exponential sums*, Math. Scand. 42 (1978), 39–48.
2. L. E. Dickson, *Linear Groups with an Exposition of the Galois Field Theory*, Dover, New York, 1958.

DUKE UNIVERSITY
DURHAM, N.C. 27706
U.S.A.