Czechoslovak Mathematical Journal

Leonard Carlitz

Reduction formulas for certain multiple exponential sums

Czechoslovak Mathematical Journal, Vol. 20 (1970), No. 4, 616–627

Persistent URL: `http://dml.cz/dmlcz/100987`

Czechoslovak Mathematical Journal, 20 (95) 1970, Praha

REDUCTION FORMULAS
FOR CERTAIN MULTIPLE EXPONENTIAL SUMS[1]

L. CARLITZ, Durham

(Received July 18, 1969)

1. Introduction. Let $F = GF(q)$ denote the finite field of order $q = p^n$, where p is a prime and $n \geqq 1$. For $a \in F$ put

$$t(a) = a + a^2 + \ldots + a^{p^{n-1}},$$

so that $t(a) \in F$. Now put $e(a) = e^{2\pi i t(a)}$. We define the Kloosterman sum for F:

$$K(a) = K_1(a) = \sum_{x \neq 0} e(x + ax'), \tag{1.1}$$

where the summation is over all nonzero $x \in F$ and $xx' = 1$. Similarly we define the double sum

$$K_2(a) = \sum_{x \neq 0, y \neq 0} e(x + y + ax'y'), \tag{1.2}$$

where now the summation is over all nonzero $x, y \in F$.

The writer has proved [2] that, when $p = 2$,

$$K_1^2(a) = q + K_2(a). \tag{1.3}$$

No result of this kind is known for $p > 2$. Moreover the writer has been unable to obtain a reduction formula for the triple sum

$$K_3(a) = \sum_{x \neq 0, y \neq 0, z \neq 0} e(x + y + z + ax'y'z'). \tag{1.4}$$

In the present paper we consider sums of the following type:

$$S(Q, L) = \sum_{(x)} e\{L(x) + (Q(x))^{-1}\}, \tag{1.5}$$

where $L(x)$ is a linear form and $Q(x)$ a quadratic form in $x_1, x_2, \ldots, x_s$ with coef-

---

[1] Supported in part by NSF grant GP-7855.

ficients in F and the summation is over all x_j in F such that $Q(x) \neq 0$. We find that in general the sum $S(Q, L)$ can be expressed in terms of $K_1(a)$ or $K_2(a)$, where a is an explicit function of Q and L. More precisely for $p = 2$ and s even, $S(Q, L)$ reduces essentially to $K_2(a)$; for s odd it reduces to $K_1(a)$. These results are contained in Theorems 1 and 2 below. For $p > 2$ and s even we find that $S(Q, L)$ reduces essentially to $K_2(a)$; for s odd, on the other hand, we require a variant of $K_1(a)$, namely

$$K'(a) = \sum_{u \neq 0} e(u + au^{-2}) .$$

These results are contained in Theorems 3 and 4.

The cases $p = 2$ and $p > 2$ require separate treatment. For the former we make considerable use of a recent paper [3] on multiple Gauss sums over finite fields of order 2^n. For the latter case we use some of the results of an earlier paper [1] on weighted quadratic partitions over a finite field of odd order.

2. Preliminaries. We recall that

$$\sum_x e(ax) = \begin{cases} q & (a = 0) \\ 0 & (a \neq 0) , \end{cases} \tag{2.1}$$

where now the summation is over all $x \in F$. Let $N(u, v)$ denote the number of solutions $x_1, x_2, \ldots, x_s \in GF(q)$ of the system

$$Q(x) = u , \quad L(x) = v , \tag{2.2}$$

where u, v are fixed numbers of F. Then by (2.1) we have

$$q^2 N(u, v) = \sum_{c,d} \sum_{(x)} e\{c(Q(x) - u) + d(L(x) - v)\} =$$

$$= \sum_{c,d} e(-cu - dv) \sum_{(x)} e\{c\, Q(x) + d\, L(x)\} ,$$

where the outer summation is over all c, $d \in F$ and the inner summation is over all $x_1, x_2, \ldots, x_s$. Thus (1.5) becomes

$$q^2\, S(Q, L) = q^2 \sum_{\substack{u,v \\ u \neq 0}} e(u' + v)\, N(u, v) =$$

$$= \sum_{\substack{u,v \\ u \neq 0}} e(u' + v) \sum_{c,d} e(-cu - dv) \sum_{(x)} e\{c\, Q(x) + d\, L(x)\} =$$

$$= \sum_{u \neq 0} e(u') \sum_{c,d} e(-cu) \sum_{(x)} e\{c\, Q(x) + d\, L(x)\} \sum_v e((1 - d)\, v) .$$

By (2.1)

$$\sum_{v} e((1-d)\,v) = \begin{cases} q & (d = 1) \\ 0 & (d \neq 1) . \end{cases}$$

It follows that

$$\text{(2.3)} \qquad q\,S(Q, L) = \sum_{\substack{c,u \\ u \neq 0}} e(u' - cu) \sum_{(x)} e\{c\,Q(x) + L(x)\} =$$

$$= \sum_{u \neq 0} e(u') \sum_{(x)} e(L(x)) + \sum_{c \neq 0, u \neq 0} e(u' - cu) \sum_{(x)} e\{c\,Q(x) + L(x)\} .$$

We now define the sum

$$\text{(2.4)} \qquad G(Q, L) = \sum_{(x)} e\{Q(x) + L(x)\} .$$

Then (2.3) becomes

$$\text{(2.5)} \qquad q\,S(Q, L) = -\sum_{(x)} e(L(x)) + \sum_{c \neq 0, u \neq 0} e(u' - cu)\,G\{cQ, L\} .$$

Since

$$\sum_{(x)} e(L(x)) = \begin{cases} q^s & (L(x) \equiv 0) \\ 0 & (L(x) \not\equiv 0) , \end{cases}$$

(2.5) may be replaced by

$$\text{(2.6)} \qquad q\,S(Q, L) = -\lambda q^s + \sum_{c \neq 0, u \neq 0} e(u' - cu)\,G(cQ, L) ,$$

where

$$\text{(2.7)} \qquad \lambda = \begin{cases} 1 & (L(x) \equiv 0) \\ 0 & (L(x) \not\equiv 0) . \end{cases}$$

3. The case $p = 2$. We may take

$$\text{(3.1)} \qquad Q(x) = \sum_{1 \leqq i \leqq j \leqq s} a_{ij} x_i x_j \quad (a_{ij} \in F) .$$

If

$$y_i = \sum_{j=1}^{s} c_{ij} x_j \quad (c_{ij} \in F,\ |c_{ij}| \neq 0)$$

and

$$Q(x) = Q_1(y) ,$$

the quadratic forms $Q(x)$ and $Q_1(y)$ are *equivalent*. If $Q(x)$ is nonsingular, that is, if it is not equivalent to a form in fewer than s indeterminates, then it is equivalent to either [4, p. 197]

$$y_1y_2 + y_3y_4 + \dots + y_{s-2}y_{s-1} + y_s^2 \tag{3.2}$$

when s is odd or to one of the forms

$$y_1y_2 + y_3y_4 + \dots + y_{s-1}y_s \tag{3.3}$$

or

$$y_1y_2 + \dots + y_{s-3}y_{s-2} + y_{s-1}^2 + y_{s-1}y_s + \beta y_s^2 \tag{3.4}$$

when s is even. In the latter case β is any number of F such that the polynomial

$$u^2 + uv + \beta v^2$$

is irreducible in $F[u, v]$. We say that $Q(x)$ is of the type $\tau = +1$ or -1 according as it is equivalent to (3.3) or (3.4). It is easily seen that

$$\tau = \tau(Q) = e(\beta)\,. \tag{3.5}$$

Moreover τ is invariant under nonsingular linear transformations.

In order to evaluate the sum

$$G(Q, L) = \sum_{(x)} e\{Q(x) + L(x)\}\,,$$

where

$$L(x) = \sum_{i=1}^{s} b_ix_i \quad (b_i \in F)\,, \tag{3.6}$$

some additional notation is needed. For s even we define $\zeta(Q, L)$ in the following way. Put

$$\bar{a}_{ij} = \begin{cases} a_{ij} & (i < j) \\ a_{ji} & (i > j) \\ 0 & (i = j)\,, \end{cases} \tag{3.7}$$

$$\delta = \delta(Q) = \det(\bar{a}_{ij})\,. \tag{3.8}$$

Since $Q(x)$ is not equivalent to a form in fewer than s indeterminates it follows that $\delta \neq 0$. Then the system of equations

$$\sum_{j=1}^{s} \bar{a}_{ij}x_j = b_i \quad (i = 1, \dots, s) \tag{3.9}$$

has a unique solution $(b_1^*, b_2^*, \ldots, b_s^*)$. We put

$$(3.10) \qquad \zeta(Q, L) = Q(b_1^*, b_2^*, \ldots, b_s^*) .$$

For s odd $\delta(Q)$ vanishes identically. Put

$$\bar{Q}(u) = \begin{vmatrix} \cdot & \bar{a}_{12} & \bar{a}_{13} & \ldots & \bar{a}_{1s} & u_1 \\ \bar{a}_{21} & \cdot & \bar{a}_{23} & \ldots & \bar{a}_{2s} & u_2 \\ \ldots & \ldots & \ldots & \ldots & \ldots & \ldots \\ \bar{a}_{s1} & \bar{a}_{s2} & \bar{a}_{s3} & \ldots & \cdot & u_s \\ u_1 & u_2 & u_3 & \ldots & u_s & \cdot \end{vmatrix} ,$$

where $\bar{a}_{ij}$ is defined by (3.7). Then for s odd we have

$$\bar{Q}(u) = \Big(\sum_{i=1}^{s} A_i u_i\Big)^2 ,$$

where the A_i are certain well-defined polynomials in $\bar{a}_{ij}$. We define

$$(3.11) \qquad \eta = \eta(Q) = Q(A_1, A_2, \ldots, A_s)$$

and

$$(3.12) \qquad \omega(Q, L) = \bar{Q}(b_1, b_2, \ldots, b_s)/\eta(Q) .$$

It is proved in [3] that when s is even, $\delta(Q)$ is a relative invariant of weight two; when s is odd $\eta(Q)$ is a relative invariant of weight two. On the other hand, $\zeta(Q, L)$ and $\omega(Q, L)$ are absolute simultaneous invariants in the respective cases.

Finally we have for s even and $Q(x)$ nonsingular

$$(3.13) \qquad G(Q, L) = q^{s/2}\, \tau(Q)\, e[\zeta(Q, L)] ,$$

while for s odd

$$(3.14) \qquad G(Q, L) = \begin{cases} q^{(s+1)/2}\, \tau(Q + zL) & (\omega(Q, L) = 1) \\ 0 & (\omega(Q, L) \neq 1) , \end{cases}$$

$Q + zL$ denotes a quadratic form in the $s + 1$ indeterminates $x_1, \ldots, x_s, z$.

We now substitute from (3.13) and (3.14) in (2.6). We first assume s even. It is evident from the definition that

$$(3.15) \qquad \tau(cQ) = \tau(Q) \qquad (c \neq 0) ,$$

while

$$(3.16) \qquad \zeta(cQ, L) = c^{-2}\, \zeta(Q, L) \quad (c \neq 0) .$$

Thus

$$G(cQ, L) = q^{s/2}\,\tau(Q)\, e[c^{-2}\,\zeta(Q, L)]$$

and (2.6) becomes

$$q\, S(Q, L) = -\lambda q^s + q^{s/2}\,\tau(Q) \sum_{c \neq 0, u \neq 0} e[u' + cu + c^{-2}\,\zeta(Q, L)]\,.$$

Since $e(c) = e(c^2)$ we have

$$\sum_{c \neq 0, u \neq 0} e[u' + cu + c^{-2}\,\zeta(Q, L)] = \sum_{c \neq 0, u \neq 0} e[u^{-2} + c^2u^2 + c^{-2}\,\zeta(Q, L)] =$$

$$= \sum_{c \neq 0, u \neq 0} e[u' + c'u' + c\,\zeta(Q, L)]\,;$$

at the last step we have replaced u^2 by u and c^2 by c'. Thus

$$q\, S(Q, L) = -\lambda q^s + q^{s/2}\,\tau(Q) \sum_{c \neq 0, u \neq 0} e[u + c'u' + c\,\zeta(Q, L)]\,.$$

Comparison with (1.2) gives

$$S(Q, L) = -\lambda q^{s-1} + q^{(s-2)/2}\,\tau(Q)\, K_2\, \zeta(Q, L)]\,. \tag{3.17}$$

Next let s be odd. Then we find, using (3.11) and (3.12) that

$$\eta(cQ) = c^s\,\eta(Q) \qquad (c \neq 0) \tag{3.18}$$

and

$$\omega(cQ, L) = c'\,\omega(Q, L) \;\; (c \neq 0)\,. \tag{3.19}$$

As noted above $\tau(Q)$ is unchanged by nonsingular linear transformations. Applying the transformation

$$y_i = cx_i \quad (i = 1, 2, \ldots, s) \quad (c \neq 0)$$

to the form

$$cQ(x_1, \ldots, x_s) + zL(x_1, \ldots, x_s)\,,$$

it is clear that

$$\tau(cQ + zL) = \tau(c'(Q + zL))\,.$$

Moreover, from the definition of τ, it is evident that

$$\tau(cQ) = \tau(Q) \quad (c \neq 0)\,.$$

Consequently

$$\tau(cQ + zL) = \tau(Q + zL)\,. \tag{3.20}$$

It follows at once from (3.14), (3.19) and (3.20) that

$$G(cQ, L) = \begin{cases} q^{(s+1)/2}\tau(Q + zL) & (\omega(Q, L) = c) \\ 0 & (\omega(Q, L) \neq c)\,. \end{cases} \tag{3.21}$$

Substituting from (3.21) in (2.6) we get

$$S(Q, L) = -\lambda q^{s-1} + q^{(s-1)/2}\,\tau(Q + zL) \sum_{u \neq 0} e\{u + u'\,\omega(Q, L)\}\,, \tag{3.22}$$

provided $\omega(Q, L) \neq 0$. If however $\omega(Q, L) = 0$ we get

$$S(Q, L) = -\lambda q^{s-1}\,. \tag{3.23}$$

We may evidently rewrite (3.22) in the form

$$S(Q, L) = -\lambda q^{s-1} + q^{(s-1)/2}\,\tau(Q + zL)\,K[\omega(Q, L)]\,. \tag{3.24}$$

We have therefore proved the following results.

Theorem 1. *Let*

$$Q(x) = \sum_{1 \leqq i \leqq j \leqq s} a_{ij}x_i x_j \quad (a_{ij} \in F) \tag{3.25}$$

denote a quadratic form that is not equivalent to a form in fewer than s indeterminates and let

$$L(x) = \sum_{i=1}^{s} b_i x_i \quad (b_i \in F) \tag{3.26}$$

denote an arbitrary linear form. Then for s even we have

$$S(Q, L) = -\lambda q^{s-1} + q^{(s-2)/2}\,\tau(Q)\,K_2[\zeta(Q, L)]\,,$$

where λ, $\tau(Q)$, $\zeta(Q, L)$ are defined by (2.7), (3.4), (3.5) *and* (3.10).

Theorem 2. *For $Q(x)$, $L(x)$ as above and s odd we have*

$$S(Q, L) = -\lambda q^{s-1} \quad (\omega(Q, L) = 0)$$

while

$$S(Q, L) = -\lambda q^{s-1} + q^{(s-1)/2}\,\tau(Q + zL)\,K_1[\omega(Q, L)] \quad (\omega(Q, L) \neq 0)\,,$$

where $\omega(Q, L)$ is defined by (3.11) *and* (3.12).

We remark that for nonsingular $Q(x)$ we have $\eta(Q) \neq 0$. Thus by (3.12) the vanishing of $\omega(Q, L)$ is equivalent to

$$\bar{Q}(b_1, b_2, \ldots, b_s) = 0 . \tag{3.27}$$

When $Q(x)$ is in one of the normal forms (3.2), (3.3), (3.4) the above results can be stated in a more explicit form. In particular if s is even and

$$Q(x) = x_1x_2 + x_3x_4 + \ldots + x_{s-1}x_s$$

we have $\delta(Q) = 1$ and

$$\zeta(Q, L) = b_1b_2 + b_3b_4 + \ldots + b_{s-1}b_s ,$$

while if

$$Q(x) = x_1x_2 + \ldots + x_{s-3}x_{s-2} + x_{s-1}^2 + x_{s-1}x_s + \beta x_s^2$$

then

$$\zeta(Q, L) = b_1b_2 + \ldots + b_{s-3}b_{s-2} + b_s^2 + b_sb_{s-1} + \beta b_{s-1}^2 .$$

If s is odd and

$$Q(x) = x_1x_2 + \ldots + x_{s-2}x_{s-1} + x_s^2$$

we get

$$\omega(Q, L) = b_s^2 .$$

Thus if

$$L(x) = \sum_{i=1}^{s-1} b_ix_i$$

but not all $b_1, \ldots, b_{s-1}$ vanish it follows that

$$S(Q, L) = 0 .$$

4. The case $p > 2$. We now take

$$Q(x) = \sum_{i,j=1}^{s} a_{ij}x_ix_j \quad (a_{ij} \in F,\ a_{ij} = a_{ji}) \tag{4.1}$$

and put

$$\delta(Q) = \det(a_{ij}) , \tag{4.2}$$

the discriminant of Q. Then by a nonsingular transformation

$$y_i = \sum_{j=1}^{s} c_{ij}x_j \quad (i = 1, 2, \ldots, s) ,$$

$Q(x)$ becomes

$$Q_0(y) = \sum_{i=1}^{s} a_i y_i^2 \quad (a_i \in F)\,. \tag{4.3}$$

Let

$$L(x) = \sum_{i=1}^{s} b_i x_i \quad (b_i \in F)\,. \tag{4.4}$$

It is convenient to now define

$$G(Q, L) = \sum_{(x)} e\{Q(x) + 2L(x)\}\,. \tag{4.5}$$

Then

$$G(Q_0, L) = \prod_{i=1}^{s} \sum_{x_i \in F} e(a_i x_i^2 + 2b_i x_i)\,. \tag{4.6}$$

If $a \neq 0$ and b is arbitrary we have

$$\sum_x e(ax^2 + 2bx) = e(-a'b^2) \sum_x e(a(x + a'b)^2) = e(-a'b^2) \sum_x e(ax^2)\,.$$

We recall that

$$G(a) = \sum_x e(ax^2) = \psi(a)\, G(1) \quad (a \neq 0) \tag{4.7}$$

where $\psi(a) = +1$ or -1 according as a is or is not a square in F. It is convenient to put $\psi(0) = 0$. We have also

$$G^2(1) = \psi(-1)\, q\,. \tag{4.8}$$

It follows from (4.6) and (4.7) that, if $\delta(Q_0) = a_1 a_2 \ldots a_s \neq 0$,

$$G(Q_0, L) = e(-\omega)\, \psi(\delta(Q_0))\, G^s(1)\,, \tag{4.9}$$

where

$$\omega = \omega(Q_0, L) = \sum_{i=1}^{s} a_i' b_i^2\,. \tag{4.10}$$

This result may be put in invariantive form. If $\delta(Q) \neq 0$ we have

$$G(Q, L) = e(-\omega(Q, L)\, \psi(\delta(Q))\, G^s(1)\,, \tag{4.11}$$

where

$$\omega(Q, L) = Q'(b_1, b_2, \ldots, b_s) \tag{4.12}$$

and $Q'(x)$ denotes the quadratic form inverse to $Q(x)$. We omit the proof of (4.11). The proof is similar to that of [1, §5].

For the application we require $G(cQ, L)$ with $c \neq 0$. Clearly

$$\delta(cQ) = c^s\,\delta(Q)\,,$$

while

$$\omega(cQ, L) = c' \,.\, \omega(Q, L) \quad (c \neq 0)\,.$$

Thus (4.11) becomes

$$G(cQ, L) = e(-c' \,.\, \omega(Q, L))\,\psi(c^s\,\delta(Q))\,G^s(1)\,. \tag{4.13}$$

Substituting from (4.13) in (2.6) we get

$$q\,S(Q, L) = -\lambda q^s + \psi(\delta(Q))\,G^s(1) \sum_{c \neq 0, u \neq 0} \psi(c^s)\,e(u + cu' + c'\,\omega(Q, L))\,. \tag{4.14}$$

If $s = 2t$, (4.14) reduces to

$$\begin{aligned} S(Q, L) &= -\lambda q^{s-1} + \psi((-1)^t\,\delta(Q))\,q^{t-1} \sum_{c \neq 0, u \neq 0} e(u + c + c'u'\,\omega(Q, L) = \\ &= -\lambda q^{s-1} + \psi((-1)^t\,\delta(Q))\,q^{t-1}K_2(\omega(Q, L))\,. \end{aligned} \tag{4.15}$$

For $s = 2t + 1$, on the other hand, we have

$$\begin{aligned} S(Q, L) &= -\lambda q^{s-1} + \psi((-1)^t\,\delta(Q))\,q^{t-1}\,G(1)\,. \\ &\quad .\sum_{c \neq 0, u \neq 0} \psi(c)\,e(u + c + u'c'\,\omega(Q, L))\,. \end{aligned} \tag{4.16}$$

If $\omega(Q, L) = 0$ the sum on the right reduces to

$$\sum_{c \neq 0, u \neq 0} \psi(c)\,e(u + c) = -\sum_{c \neq 0} \psi(c)\,e(c) = -G(1)\,.$$

Thus (4.16) becomes

$$S(Q, L) = -\lambda q^{s-1} - \psi((-1)^{t+1}\,\delta(Q))\,q^t(\omega(Q, L) = 0)\,. \tag{4.17}$$

If however $\omega(Q, L) \neq 0$ we consider the sum

$$L_2(a) = \sum_{c \neq 0, u \neq 0} \psi(c)\,e(u + c + au'c') = \sum_{u \neq 0} e(u) \sum_{c \neq 0} \psi(c)\,e(c + au'c')\,. \tag{4.18}$$

It is known [1] that the sum

$$L(a) = \sum_{c} \psi(c)\,e(c + ac') \tag{4.19}$$

satisfies

$$L(a) = 0 \quad (\psi(a) = -1)\,, \tag{4.20}$$

$$L(a^2) = G(1)\,(e(2a) + e(-2a) \quad (a \neq 0)\,. \tag{4.21}$$

Substituting from (4.20), (4.21) in (4.18) we get

$$L_2(a) = \sum_{u \neq 0} e(u) \sum_{au' = v^2} G(1)\, e(2v) = G(1) \sum_{v \neq 0} e(2v + av'^2) = G(1) \sum_{v \neq 0} e(v + 4av'^2)\,.$$

Hence if we put

$$K'(a) = \sum_{v \neq 0} e(v + av'^2) \tag{4.22}$$

we get

$$S(Q, L) = -\lambda q^{s-1} + \psi((-1)^{t+1}\,\delta(Q))\, q^t K'(4\omega(Q, L))\,. \tag{4.23}$$

We may now state the following results.

Theorem 3. *Let*

$$Q(x) = \sum_{i,j=1}^{s} a_{ij} x_i x_j \quad (a_{ij} \in F,\ a_{ij} = a_{ji})$$

be a nonsingular quadratic form and let

$$L(x) = \sum_{i=1}^{s} b_i x_i \quad (b_i \in F)$$

be an arbitrary linear form. Then for $s = 2t$ *we have*

$$S(Q, L) = \sum_{(x)} e(Q(x) + 2L(x)) = -\lambda q^{s-1} + \psi((-1)^t\,\delta(Q))\, q^{t-1} K_2(\omega(Q, L))\,,$$

where $\delta(Q) = \det(a_{ij})$ *and* $\omega(Q, L)$ *is defined by* (4.12).

Theorem 4. *For* $Q(x)$, $L(x)$ *as above and* $s = 2t + 1$ *we have*

$$S(Q, L) = -\lambda q^{s-1} - \psi((-1)^{t+1}\,\delta(Q))\, q^t \quad (\omega(Q, L) = 0)\,,$$

while

$$S(Q, L) = -\lambda q^{s-1} + \psi((-1)^{t+1}\,\delta(Q))\, q^t\, K'(4\omega(Q, L))\,,$$

where $K'(a)$ *is defined by* (4.22).

References

[1] *L. Carlitz:* Weighted quadratic partitions over a finite field, Canadian Journal of Mathematics, vol. *5* (1953), pp. 317—323.

[2] *L. Carlitz:* A note on exponential sums, Pacific Journal of Mathematics, vol. *30* (1969), pp. 35—37.

[3] *L. Carlitz:* Gauss sums over finite fields of order 2^n, Acta Arithmetica, vol. *15* (1969), pp. 247—265.

[4] *L. E. Dickson:* Linear Groups with an Exposition of the Galois Theory, New York, 1958.

Author's address: Duke University, Department of Mathematics, Durham, North Carolina, U.S.A.