REDUCTION FORMULAS
FOR CERTAIN MULTIPLE EXPONENTIAL SUMS

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 $n \geq 1$. For $a \in F$ put

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

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

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

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

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

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

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

$$K_2^2(a) = q + K_2(a).$$

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

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

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

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

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

$$(2.1) \quad \sum_{x} e(ax) = \begin{cases} q & (a = 0) \\ 0 & (a \neq 0) \end{cases},$$

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

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

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

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

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

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

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

$$= \sum_{u, v} e(u' + v) \sum_{c, d} e(-cu - dv) \sum_{(x)} e\{cQ(x) + dL(x)\} =$$

$$= \sum_{u \neq 0} e(u') \sum_{c, d} e(-cu) \sum_{(x)} e\{cQ(x) + dL(x)\} \sum_{v} e(1 - dv).$$

617
By (2.1)
\[ \sum_v e((1 - d) v) = \begin{cases} q & (d = 1) \\ 0 & (d \neq 1) \end{cases}. \]

It follows that
\[ q S(Q, L) = \sum_{c, u} e(u' - cu) \sum_{v} e\{c Q(v) + L(v)\} = \]
\[ = \sum_{u \neq 0} e(u') \sum_{v} e(L(v)) + \sum_{c + 0, u \neq 0} e(u' - cu) \sum_{v} e\{c Q(v) + L(v)\}. \]

We now define the sum
\[ G(Q, L) = \sum_{v} e\{Q(v) + L(v)\}. \]

Then (2.3) becomes
\[ q S(Q, L) = - \sum_{v} e(L(v)) + \sum_{c + 0, u \neq 0} e(u' - cu) G(cQ, L). \]

Since
\[ \sum_{v} e(L(v)) = \begin{cases} q^s & (L(v) \equiv 0) \\ 0 & (L(v) \not\equiv 0) \end{cases}, \]

(2.5) may be replaced by
\[ q S(Q, L) = - \lambda q^s + \sum_{c + 0, u \neq 0} e(u' - cu) G(cQ, L), \]

where
\[ \lambda = \begin{cases} 1 & (L(v) \equiv 0) \\ 0 & (L(v) \not\equiv 0) \end{cases}. \]

3. The case \( p = 2 \). We may take
\[ Q(x) = \sum_{1 \leq i \neq j \leq s} a_{ij}x_i x_j \quad (a_{ij} \in F). \]

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 \cite[p. 197]{4}

\begin{equation}
(3.2) \quad y_1y_2 + y_3y_4 + \cdots + y_{s-2}y_{s-1} + y_s^2
\end{equation}

when $s$ is odd or to one of the forms

\begin{equation}
(3.3) \quad y_1y_2 + y_3y_4 + \cdots + y_{s-1}y_s
\end{equation}

or

\begin{equation}
(3.4) \quad y_1y_2 + \cdots + y_{s-3}y_{s-2} + y_{s-1}^2 + y_{s-1}y_s + \beta y^2_s
\end{equation}

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

\begin{equation}
\quad u^2 + uv + \beta v^2
\end{equation}

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

\begin{equation}
(3.5) \quad \tau = \tau(Q) = e(\beta).
\end{equation}

Moreover $\tau$ is invariant under nonsingular linear transformations.

In order to evaluate the sum

\begin{equation}
G(Q, L) = \sum_{(x)} e\{Q(x) + L(x)\},
\end{equation}

where

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

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

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

\begin{equation}
(3.8) \quad \delta = \delta(Q) = \det(\bar{a}_{ij}).
\end{equation}

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

\begin{equation}
(3.9) \quad \sum_{j=1}^s \bar{a}_{ij}x_j = b_i \quad (i = 1, \ldots, s)
\end{equation}

619
has a unique solution \((b_1^*, b_2^*, \ldots, b_s^*)\). We put

\[
\zeta(Q, L) = Q(b_1^*, b_2^*, \ldots, b_s^*).
\]

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

\[
\bar{Q}(u) = \begin{vmatrix}
\bar{a}_{12} & \bar{a}_{13} & \cdots & \bar{a}_{1s} & u_1 \\
\bar{a}_{21} & \bar{a}_{23} & \cdots & \bar{a}_{2s} & u_2 \\
\vdots & \vdots & \ddots & \vdots & \vdots \\
\bar{a}_{s1} & \bar{a}_{s2} & \cdots & \bar{a}_{ss} & u_s \\
u_1 & u_2 & u_3 & \cdots & u_s
\end{vmatrix},
\]

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

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

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

\[
\eta = \eta(Q) = Q(A_1, A_2, \ldots, A_s)
\]

and

\[
\omega(Q, L) = \frac{Q(b_1, b_2, \ldots, b_s)/\eta(Q)}{}.
\]

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

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

while for \(s\) odd

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

\(Q + zL\) 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

\[
\tau(cQ) = \tau(Q) \quad (c \neq 0),
\]

while

\[
\zeta(cQ, L) = c^{-2} \zeta(Q, L) \quad (c \neq 0).
\]
Thus
\[ G(cQ, L) = q^{s/2} \tau(Q) e[\xi^{-2} \zeta(Q, L)] \]
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
\[ (3.17) \quad S(Q, L) = -\lambda q^{s-1} + q^{(s-2)/2} \tau(Q) K_2 \zeta(Q, L) . \]

Next let \( s \) be odd. Then we find, using (3.11) and (3.12) that
\[ (3.18) \quad \eta(cQ) = c^s \eta(Q) \quad (c \neq 0) \]
and
\[ (3.19) \quad \omega(cQ, L) = c' \omega(Q, L) \quad (c \neq 0) . \]
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 \( \tau \), it is evident that
\[ \tau(cQ) = \tau(Q) \quad (c \neq 0) . \]
Consequently
\[ (3.20) \quad \tau(cQ + zL) = \tau(Q + zL) . \]
It follows at once from (3.14), (3.19) and (3.20) that

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

Substituting from (3.21) in (2.6) we get

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

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

\[
S(Q, L) = -\lambda q^{s-1}.
\]

We may evidently rewrite (3.22) in the form

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

We have therefore proved the following results.

**Theorem 1.** Let

\[
Q(x) = \sum_{1 \leq i \leq j \leq s} a_{ij} x_i x_j \quad (a_{ij} \in F)
\]

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

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

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 \(\lambda, \tau(Q), \zeta(Q, L)\) 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

$$Q(b_1, b_2, \ldots, b_s) = 0.$$  

(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

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

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

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

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

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

and put

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

the discriminant of $Q$. Then by a nonsingular transformation

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

we have $\eta(Q) = 0$ and

$$\omega(Q, L) = \sum_{i=1}^{s-1} b_i y_i,$$  

(4.1) 

and

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

(4.2)
\(Q(x)\) becomes

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

Let

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

It is convenient to now define

\[(4.5)\quad G(Q, L) = \sum_{(x)} e\{Q(x) + 2L(x)\}.\]

Then

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

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

\[(4.7)\quad G(a) = \sum_{x} e(ax^2) = \psi(a) G(1) \quad (a \neq 0)\]

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

\[(4.8)\quad G^2(1) = \psi(-1) q.\]

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

\[(4.9)\quad G(Q_0, L) = e(-\omega) \psi(\delta(Q_0)) G^t(1),\]

where

\[(4.10)\quad \omega = \omega(Q_0, L) = \sum_{i=1}^{s} a_i b_i^2.\]

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

\[(4.11)\quad G(Q, L) = e(-\omega(Q, L) \psi(\delta(Q)) G^t(1),\]

where

\[(4.12)\quad \omega(Q, L) = Q'(b_1, b_2, \ldots, b_s)\]

624
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

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

Thus (4.11) becomes

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

Substituting from (4.13) in (2.6) we get

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

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

$$(4.15) \quad S(Q, L) = -\lambda q^{t-1} + \psi(-1)^T \delta(Q) \sum_{c+0, u+0} e(u + c + c' u' \omega(Q, L)) =$$

$$= -\lambda q^{t-1} + \psi(-1)^T \delta(Q) q^{t-1} K_2(\omega(Q, L)).$$

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

$$(4.16) \quad S(Q, L) = -\lambda q^{t-1} + \psi(-1)^T \delta(Q) q^{t-1} G(1).$$

$$\sum_{c+0, u+0} \psi(c) e(u + c + u' c' \omega(Q, L)).$$

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

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

Thus (4.16) becomes

$$(4.17) \quad S(Q, L) = -\lambda q^{t-1} - \psi(-1)^{t+1} \delta(Q) q'(\omega(Q, L) = 0).$$

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

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

It is known [1] that the sum

$$(4.19) \quad L(a) = \sum_{c} \psi(c) e(c + ac').$$
satisfies
\[(4.20)\]
\[L(a) = 0 \quad (\psi(a) = -1),\]
\[(4.21)\]
\[L(a^2) = G(1)(e(2a) + e(-2a)) \quad (a \neq 0).\]

Substituting from (4.20), (4.21) in (4.18) we get
\[L_2(a) = \sum_{u+0} e(u) \sum_{u' = v^2} G(1) e(2v) = G(1) \sum_{v+0} e(2v + av^2) = G(1) \sum_{v \neq 0} e(v + 4av^2).\]

Hence if we put
\[(4.22)\]
\[K'(a) = \sum_{v \neq 0} e(v + av^2)\]
we get
\[(4.23)\]
\[S(Q, L) = -\lambda q^{s-1} + \psi((-1)^{t+1} \delta(Q)) q^t K'(4\omega(Q, L)).\]

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 \(\delta(Q) = \text{det}(a_{ij})\) 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


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