d'un nombre fini des cas, aient un facteur premier idéal de degré 1 dans $J$, il faut et il suffit que

$$G(x) = aN(H(x)),$$

où $H(x)$ est un polynôme à coefficients de $J$, $N$ est la norme dans $J$ et $a$ est un nombre rationnel.

La propriété des corps Baueriens exprimée dans ce théorème est caractéristique: pour les autres corps p.ex. $Q/2\cos(2\pi/7))$ (cf. [4], p. 335) le théorème est en défaut.

Travaux cités


Reçu par la Rédaction le 22. 8. 1968

Gauss sums over finite fields of order $2^n$*

by

L. Carlitz (Durham, North Carolina)

1. Introduction. Let $F = GF(q)$ denote the finite field of order $q$; we shall assume throughout the paper that $q = 2^n, n \geq 1$. For $a \in F$ put

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

so that $t(a) \in GF(2)$. Define

$$e(a) = (-1)^{|a|},$$

Let

$$Q(x) = Q(x_1, \ldots, x_n) = \sum_{1\leq i < j \leq n} a_{ij} x_i x_j \ (a_{ij} \in F)$$

denote a quadratic form over $F$. If

$$y_I = \sum_{j=1}^{n} a_{ij} x_j \ (e_{ij} \neq 0)$$

and

$$Q(x_1, \ldots, x_n) = Q(y_1, \ldots, y_n),$$

the quadratic forms $Q(x)$ and $Q(y)$ are equivalent. Dickson ([2], p. 197) has proved that if $Q(x)$ is not equivalent to a form in fewer than $m$ indeterminates then it is equivalent to either

$$y_1 y_2 + y_2 y_3 + \ldots + y_{n-1} y_n + y_n^2$$

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

$$y_1 y_2 + y_2 y_4 + \ldots + y_{n-2} y_n$$

or

$$y_1 y_2 + \ldots + y_{n-1} y_{n-1} + y_n y_{n+1}$$

* Supported in part by NSF grant GP-1855.
when \( m \) is even. In the latter case \( \beta \) is any number of \( F \) such that the polynomial
\[
\alpha x^2 + \beta y^2
\]
is irreducible over \( F[u, v] \). We shall say that \( Q(x) \) is of type \( \tau = +1 \) or \( -1 \) according as it is equivalent to (1.3) or (1.4). We remark that \( \tau = \sigma(\beta) \).

We now define the sum
(1.5) \[ S(Q) = \sum_{c_1, \ldots, c_m \in F} \sigma(Q(c_1, \ldots, c_m)). \]
However in the present situation it is of interest to consider a more general sum
(1.6) \[ S(Q, L) = \sum_{c_1, \ldots, c_m \in F} \sigma(Q(c_1, \ldots, c_m) + L(c_1, \ldots, c_m)), \]
where
\[ L(x) = L(x_1, \ldots, x_m) = \sum_{i=1}^{m} b_i x_i (b_i \in F), \]
is an arbitrary linear form over \( F \). For odd \( q \) there is no gain in generality in considering sums like (1.6); however, as we shall see, for even \( q \), (1.6) is indeed more general than (1.5).

It is convenient to first treat the sum \( S(Q) \). We assume that \( Q(x) \) is not equivalent to a quadratic form in fewer than \( m \) indeterminates. Then we show that
(1.7) \[ S(Q) = 0 \quad (m \text{ odd}), \]
(1.8) \[ S(Q) = 2^\frac{m+1}{2} \quad (m \text{ even}), \]
where \( \tau \) denotes the type of \( Q \). The corresponding results for \( S(Q, L) \) require some preliminaries and are contained in Theorems 6 and 7 below. It is not difficult to obtain these results when \( Q(x) \) is assumed to be in one of the normal forms (1.2), (1.3) or (1.4). To state the results for arbitrary \( Q(x) \) it is necessary to define first an invariant \( \delta(Q) \) when \( m \) is odd and an invariant \( \eta(Q) \) when \( m \) is even. In addition certain simultaneous invariants \( \zeta(Q, L), \omega(Q, L) \) for \( m \) even and odd, respectively, are also needed. For the first three invariants see Theorems 1 and 2 below, for \( \omega(Q, L) \) see (4.15). These invariants suggest certain geometric questions that we hope to discuss elsewhere.

As an application we determine the number of solutions in \( F \) of the equation
(1.9) \[ Q(x) + L(x) = a. \]
More generally we show that the weighted sum
(1.10) \[ \sum_{c_1, \ldots, c_m \in F} \sigma(\lambda_1 c_1 + \ldots + \lambda_m c_m) \quad (\lambda_i \in F), \]
where the summation is over all solutions of (1.9), can be expressed in terms of the Kloosterman sum
\[ K(a, b) = \sum_{c \in F} \sigma(ac + bc^{-1}). \]

2. Preliminaries on quadratic forms. If \( Q(x_1, \ldots, x_m) \) is equivalent to a form in \( r \) indeterminates but not in fewer than \( r \), then \( Q \) is of rank \( r \); if \( r = m \), \( Q \) is nonsingular.

Let
(2.1) \[ Q(x) = \sum_{1 \leq i < j \leq n} a_{ij} x_i x_j, \]
Put
(2.2) \[ \delta_{ij} (i < j), \quad \delta_{ii} (i > j), \quad \delta_{ii} (i = j), \]
(2.3) \[ \delta = \delta(Q) = \det(a_{ij}). \]
If
(2.4) \[ y_i = \sum_{j=1}^{m} a_{ij} x_j \quad (i = 1, 2, \ldots, m), \]
where
\[ c = \det(a_{ij}) \neq 0 \]
and
\[ Q(x) = \sum_{1 \leq i < j \leq m} b_{ij} y_i y_j, \]
then
(2.5) \[ \frac{\partial^2 Q(x)}{\partial x_i \partial x_j} = \sum_{k=1}^{m} \frac{\partial Q(x)}{\partial y_k} \frac{\partial y_k}{\partial x_i} \cdot \frac{\partial y_k}{\partial x_j}. \]
On the other hand
\[ \frac{\partial Q(x)}{\partial x_i} = \sum_{j=1}^{m} a_{ij} x_j, \quad \frac{\partial^2 Q(x)}{\partial x_i \partial x_j} = a_{ij}. \]
so that (2.4) reduces to

$$s_{ij} = \sum_{k=1}^{n} \delta_{ik} a_k a_j,$$

where

$$\delta_{ik} = \begin{cases} b_{ik} & (s < t), \\ b_{ji} & (s > t), \\ 0 & (s = t). \end{cases}$$

It therefore follows at once that

$$\delta(Q) = \delta(D),$$

that is to say, $\delta$ is a relative invariant of weight two.

If $m$ is odd it is easily seen that $\delta(Q)$ vanishes identically. For $m$ even, however, if

$$Q(x) = x_1 x_2 + x_3 x_4 + \ldots + x_{m-1} x_m$$

then it can be verified that $\delta(Q) = 1$.

When $m$ is odd we shall construct an invariant that does not vanish identically in the following way.

Some preliminaries are needed. If $B$ is a skew matrix of even order:

$$B = (b_{ij}) \quad (b_{ij} = b_{ji} = 0),$$

it is readily seen that $\det B$ is equal to the square of a polynomial in the $b_{ij}$. Indeed this can be stated quite explicitly. We have for example

$$\begin{vmatrix} . & b_{12} & \cdots & b_{1m} \\ . & b_{21} & \cdots & b_{2m} \\ \vdots & \vdots & \ddots & \vdots \\ . & b_{m1} & \cdots & b_{mm} \end{vmatrix} = b_{m1}^2,$$

$$\begin{vmatrix} . & b_{12} & b_{13} & b_{14} \\ . & b_{21} & b_{23} & b_{24} \\ . & b_{31} & b_{32} & b_{34} \\ . & b_{41} & b_{42} & b_{44} \end{vmatrix} = (b_{12} b_{44} + b_{13} b_{34} + b_{14} b_{24})^2,$$

$$\begin{vmatrix} . & b_{12} & b_{14} & b_{15} & b_{16} & b_{17} & b_{18} \\ . & b_{21} & b_{24} & b_{25} & b_{26} & b_{27} & b_{28} \\ . & b_{31} & b_{34} & b_{35} & b_{36} & b_{37} & b_{38} \\ . & b_{41} & b_{43} & b_{45} & b_{46} & b_{47} & b_{48} \\ . & b_{51} & b_{53} & b_{54} & b_{56} & b_{57} & b_{58} \\ . & b_{61} & b_{63} & b_{65} & b_{66} & b_{67} & b_{68} \\ . & b_{71} & b_{73} & b_{74} & b_{75} & b_{76} & b_{78} \\ . & b_{81} & b_{83} & b_{84} & b_{85} & b_{86} & b_{87} \end{vmatrix} = (b_{12} b_{15} b_{18} + b_{13} b_{16} b_{18} + b_{14} b_{17} b_{18} + b_{21} b_{25} b_{28} + b_{23} b_{26} b_{28} + b_{24} b_{27} b_{28} + b_{31} b_{35} b_{38} + b_{32} b_{36} b_{38} + b_{34} b_{37} b_{38} + b_{41} b_{45} b_{48} + b_{42} b_{46} b_{48} + b_{43} b_{47} b_{48} + b_{51} b_{55} b_{58} + b_{52} b_{56} b_{58} + b_{53} b_{57} b_{58} + b_{61} b_{65} b_{68} + b_{62} b_{66} b_{68} + b_{63} b_{67} b_{68} + b_{71} b_{75} b_{78} + b_{72} b_{76} b_{78} + b_{73} b_{77} b_{78})^3.$$

The general expression for $\det B$ can now be written down without any difficulty. Incidentally the number of terms is equal to $(2m)!/(2!)^m s!$, where $B$ is of order $2m$.

With $\bar{a}_{ij}$ defined by (2.2) put

$$\bar{Q}(u) = \begin{vmatrix} \bar{a}_{12} & \bar{a}_{13} & \cdots & \bar{a}_{1m} & u_1 \\ \bar{a}_{21} & \bar{a}_{23} & \cdots & \bar{a}_{2m} & u_2 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ \bar{a}_{m1} & \bar{a}_{m2} & \cdots & \bar{a}_{mm} & u_m \end{vmatrix}$$

(2.7)

For $m$ even, $\bar{Q}(u)$ vanishes identically. For $m$ odd, on the other hand, it is clear from the above that

$$\bar{Q}(u) = \left( \sum_{i=1}^{m} A_i u_i \right)^2,$$

(2.8)

where the $A_i$ are certain well-defined polynomials in $a_{ij}$. For example, for $m = 3$ we have

$$\bar{Q}(u) = (a_{12} u_1 + a_{13} u_2 + a_{15} u_3)^2,$$

while for $m = 5$

$$\bar{Q}(u) = \left( (a_{16} a_{66} + a_{17} a_{76} + a_{18} a_{86}) u_1 + + (a_{17} a_{67} + a_{18} a_{78} + a_{19} a_{89}) u_2 + + (a_{18} a_{68} + a_{19} a_{79} + a_{20} a_{89}) u_3 + + (a_{19} a_{69} + a_{20} a_{79} + a_{21} a_{89}) u_4 + + (a_{20} a_{79} + a_{21} a_{89}) u_5 \right)^2.$$

Again the mode of formation of the coefficients is clear.

We now define

$$\eta(Q) = \bar{Q}(A_1, A_2, \ldots, A_m),$$

where $Q(x)$ is an arbitrary quadratic form with $m$ odd. For example when $m = 3$ we have

$$\eta(Q) = a_{12} a_{23} + a_{13} a_{32} + a_{69} a_{96} + a_{69} a_{96} a_{69} a_{96} + a_{69} a_{96} + a_{69} a_{96} + a_{69} a_{96} a_{69} a_{96} + a_{69} a_{96} a_{69} a_{96} a_{69} a_{96}.$$

(2.9)

For

$$Q(x) = \alpha x_1 + \cdots + \alpha x_m + \alpha x_m,$$

(2.10)

we find that

$$A_1 = \ldots = A_{m-1} = 0, \quad A_m = 1$$

and therefore

$$\eta(Q) = 1.$$

(2.11)

Thus $\eta(Q)$ does not vanish identically.

To see how $\eta(Q)$ transforms when $Q(u)$ is subjected to a nonsingular linear transformation we assume that the $w_i$ in (2.7) transform contragrediently to the $u_i$. For brevity we replace (2.7) by

$$\bar{Q}(w) = \begin{vmatrix} \bar{A} \bar{w} \\ \bar{w}' \end{vmatrix},$$

(2.12)
where \( \mathcal{A} = (a_{ij}) \), \( u \) is the column vector \((u_1, \ldots, u_m)\) and \( u' \) is the corresponding row vector; similarly \( \mathcal{B} \) is the column vector \((b_1, \ldots, b_m)\) and \( y \) the column vector \((y_1, \ldots, y_m)\). Thus (2.4) becomes \( y = Cx \), where \( C = (c_{ij}) \), while

\[
C'v = u,
\]

where \( C' \) is the transpose of \( C \) and \( v = \text{col}(v_1, \ldots, v_m). \) Since \( \mathcal{A} = C'BC \),

where \( B = (b_{ij}) \), it follows from (2.12) that \( Q(u) = \begin{vmatrix} C'BO \ C'v \\ v' C \end{vmatrix} \).

Therefore

\[
Q(u) = \sigma Q'(v),
\]

where

\[
Q'(v) = B \begin{vmatrix} v' \end{vmatrix} = B_1|v|.
\]

Hence by (2.8) and (2.14)

\[
\sum_{i=1}^{m} A_i u_i = \sigma \sum_{i=1}^{m} B_i v_i,
\]

which, in view of (2.13) implies

\[
\sum_{i=1}^{m} A_i u_i = \sum_{i=1}^{m} B_i v_i.
\]

Now applying (2.9) we get

\[
\eta(Q) = \sigma^{\delta} \eta(Q),
\]

so that \( \eta(Q) \) is a relative invariant of weight two.

We shall also require, when \( m \) is even, a simultaneous invariant of the pair of forms \( Q(x), L(z) \), where

\[
L(z) = \sum_{i=1}^{m} b_i z_i.
\]

Put

\[
Q_i(x) = \frac{\partial Q(x)}{\partial x_i} = \sum_{j=1}^{m} a_{ij} x_j.
\]

We assume that \( \delta(Q) \neq 0 \), so that the system of equations

\[
Q_i(x) = a_i \quad (i = 1, 2, \ldots, m)
\]

has the unique solution \((a_1^*, a_2^*, \ldots, a_m^*)\). Now define

(2.18)

\[
\zeta(Q, L) = Q(a_1^*, a_2^*, \ldots, a_m^*).
\]

Applying the transformation (2.4), assume that \( L(z) \) becomes

\[
L_i(y) = \sum_{k=1}^{m} b_i y_k
\]

and let the system

\[
\frac{\partial Q_i(x)}{\partial x_i} = b_i \quad (i = 1, 2, \ldots, m)
\]

have the unique solution \((b_1^*, b_2^*, \ldots, b_m^*)\). Let \( a, b \) denote the column vectors \((a_1, a_2, \ldots, a_m), (b_1, b_2, \ldots, b_m) \) and similarly for \((a_1^*, a_2^*, \ldots, a_m^*)\). Then we have

(2.19)

\[
\bar{A}a^* = a, \quad \bar{B}b^* = b_1
\]

and moreover we have

(2.20)

\[
a = Cb.
\]

It now follows easily from (2.19) and (2.20) that

(2.21)

\[
b^* = Ca^*_L
\]

so that the \( a_i^* \) transform exactly like the \( a_i \). Consequently (2.18) yields

(2.22)

\[
\zeta(Q, L) = \zeta(Q_L, L). \]

Thus \( \zeta(Q, L) \) is an absolute invariant.

The results of this section may be summarized in the following two theorems.

**Theorem 1.** For \( m \) even, \( \delta(Q) \) is a relative invariant of weight two. For \( m \) odd, \( \eta(Q) \) is a relative invariant of weight two.

**Theorem 2.** For \( m \) even and \( \delta(Q) \neq 0 \), \( \zeta(Q, L) \) is a simultaneous absolute invariant.

We note that if

\[
Q_1(x) = x_1 z_1 + x_2 z_2 + \ldots + x_m z_m
\]

then

(2.23)

\[
\zeta(Q_1, L) = a_1 a_2 + a_2 a_3 + \ldots + a_{m-1} a_m
\]

but if

\[
Q_1(x) = x_1 x_2 + \ldots + x_{m-1} x_m + a_1 a_{m-1} x_m + \beta a_m^z
\]

then

(2.24)

\[
\zeta(Q_1, L) = a_1 a_2 + \ldots + a_{m-1} a_m + a_m + a_m a_{m-1} + \beta a^z_{m-1}.
\]
Remark. For even, \( Q(x) \) is nonsingular if and only if \( \delta(Q) \neq 0 \); for odd, \( Q(x) \) is nonsingular if and only if \( \eta(Q) \neq 0 \).

3. Evaluation of \( S(Q) \). We shall make frequent use of the formula

\[
\sum_{a \in \mathbb{F}} e(a) = \begin{cases} q & \text{(a = 0)}, \\ 0 & \text{(a = 0)}, \end{cases}
\]

where the summation is over all \( \beta \in \mathbb{F} \). In what follows we shall usually indicate summations in this way.

It follows at once from the definition

\[
S(Q) = \sum_{a \in \mathbb{F}} e(Q(c_1, \ldots, c_n))
\]

that if \( Q_2 \) is equivalent to \( Q \) then

\[
S(Q_2) = S(Q).
\]

However, as we shall see, the converse is in general not true.

In view of (3.2) we may assume that \( Q \) is in normal form. We assume \( Q \) nonsingular. Hence we may put

\[
Q = x_1 x_2 + \ldots + x_{m-1} x_m + x_m^2 \quad (m \text{ odd})
\]

or, when \( m \) is even,

\[
Q = \begin{cases} x_1 x_2 + \ldots + x_{m-1} x_m, \\ x_1 x_2 + \ldots + x_{m-1} x_m + x_m^2, \\ x_1 x_2 + \ldots + x_{m-1} x_m + x_m^2 + \beta x_m^2, \end{cases}
\]

according as \( Q \) is of type \( +1 \) or \( -1 \).

Since by (3.1)

\[
\sum_{a \in \mathbb{F}} e(a) = 0,
\]

it follows at once from (3.3) that

\[
S(Q) = 0 \quad (m \text{ odd}).
\]

In the next place, by (3.1),

\[
\sum_{a \in \mathbb{F}} e(ab) = q.
\]

Hence for \( Q \) of type \( +1 \) we have

\[
S(Q) = q^{m/2} \quad (\tau = +1).
\]

For \( Q \) of type \( -1 \) we have

\[
S(Q) = q^{(m-1)/2} \sum_{a \in \mathbb{F}} e(a^2 + ab + \beta b^2).
\]

Now since \( x^2 + xy + \beta y^2 \) is irreducible in \( F[x, y] \) it follows that the equation

\[
x^2 + xy + \beta y^2 = 0
\]

has the single solution \( (0, 0) \). On the other hand the number of solutions of

\[y^2 + xy + \beta y^2 = a \quad (a \neq 0),\]

is independent of \( a \) and is therefore equal to \( q+1 \). It follows that

\[
\sum_{a \in \mathbb{F}} e(a^2 + ab + \beta b^2) = 1 + (q+1) \sum_{a \in \mathbb{F}} e(a) = -q.
\]

Thus (3.7) becomes

\[
S(Q) = -q^{m/2}.
\]

We may now state

**Theorem 3.** Let

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

be a nonsingular quadratic form over \( F \). Then

\[
S(Q) = \begin{cases} 0 & \text{(m odd),} \\ \tau q^{m/2} & \text{(m even),} \end{cases}
\]

where \( \tau \) denotes the type of \( Q \).

Suppose now that \( Q \) is of rank \( r \leq m \). If \( r \) is odd it follows at once that \( S(Q) = 0 \). If \( r \) is even and \( Q \) is equivalent to \( Q_1(x_1, \ldots, x_r) \) of type \( r \), then by (3.9)

\[
S(Q) = \tau q^{m/2} - q^{m-r} = q^{m-r}.
\]

In particular this establishes the invariance of \( r \) and \( \tau \). Moreover if \( Q_1(x_1, \ldots, x_r) \) also satisfies

\[
S(Q_1) = \tau q^{m-r} - q^{m-r} = q^{m-r}.
\]

it follows that \( Q \) and \( Q_1 \) are equivalent.

This proves

**Theorem 4.** The quadratic form \( Q(x) \) is of odd rank if and only if \( S(Q) = 0 \). If

\[
S(Q) = \tau q^k \quad (m/2 \leq k \leq m)
\]

then \( Q \) is of rank \( r = 2(m-k) \) and type \( \tau \). Moreover two forms \( Q, Q_1 \) of even rank are equivalent if and only if \( S(Q) = S(Q_1) \).

Thus for forms of even rank \( S(Q) \) furnishes a criterion for equivalence. For odd rank however this is not the case.
The following corollary of Theorem 1 may be noted.

**Theorem 5.** If $Q_1(x_1, \ldots, x_m)$ is nonsingular of type $t_1$, and $Q_2(y_1, \ldots, y_m)$ is nonsingular of type $t_2$, then
\[ Q_1(x_1, \ldots, x_m) + Q_2(y_1, \ldots, y_m) \]
is nonsingular of type $t_1 t_2$.

4. **Evaluation of $S(Q, L)$**. We shall require several preliminary results.

**Lemma 1.**
\[ \sum_{ab} e(\lambda a + \mu b) = q e(ab). \] (4.1)

**Proof.** The sum is equal to
\[ \sum_{ab} e((\lambda + b)(\mu + a) + ab) = e(ab) \sum_{ab} e(\lambda \mu) \]
and (4.1) follows at once.

**Lemma 2.** Let $x^2 + xy + \beta y^2$ be irreducible over $F$. Then
\[ \sum_{ab} e((\lambda + b)(\mu + a) + ab) = -q e(b^2 + ab + \beta a^2). \] (4.2)

**Proof.** Replacing $\lambda, \mu$ by $\lambda + b, \mu + a$, the sum becomes
\[ \sum_{ab} e((\lambda + b)(\mu + a) + b^2 + ab + \beta a^2) = -q e(b^2 + ab + \beta a^2) \]
by (3.8).

Define
\[ R(a) = \sum_{\lambda} e(\lambda^2 + a\lambda). \] (4.3)

**Lemma 3.**
\[ R(a) = \begin{cases} q & (a = 1), \\ 0 & (a \neq 1). \end{cases} \] (4.4)

**Proof.** We have
\[ R^2(a) = \sum_{\lambda, \mu} e((\lambda + \mu)^2 + (a + a\mu)) = q \sum_{\lambda} e(\lambda^2 + a\lambda), \]
so that
\[ R(a) = q R(a). \] (4.5)
Hence $R(a) = 0$ or $q$. On the other hand
\[ \sum_a R(a) = \sum_a \sum_{\lambda} e(\lambda^2 + a\lambda) = \sum_{\lambda} e(\lambda^2) \sum_{a} e(a\lambda). \]

By (3.1) this reduces to
\[ \sum_{a} R(a) = q. \] (4.6)

We now show that
\[ R(1) = q. \] (4.7)
Indeed
\[ s(\lambda + 1) = \lambda^2 + 1 = 0, \quad e(\lambda + 1) = 1, \]
and (4.7) follows at once. Finally combining (4.5), (4.6) and (4.7) we get (4.4).

We now assume that $Q(x)$ is in normal form (3.3) or (3.4) and that
\[ L(x) = a_1 x_1 + \ldots + a_n x_n. \]
If $m$ is even and $Q$ is of type $+1$, then it is evident that
\[ S(Q, L) = \prod_{i=1}^{m} \sum_{a_i} e(\lambda a_i + a_{i-1} + a_i + a_{i-1} + a_i). \]

Applying Lemma 1 we get
\[ S(Q, L) = q^{m/2} e(a_1 a_2 + \ldots + a_{n-1} a_n). \] (4.9)
If $m$ is even and $Q$ is of type $-1$, then
\[ S(Q, L) = \prod_{i=1}^{m} \sum_{a_i} e(\lambda a_i + a_{i-1} + a_i + a_{i-1} + a_i). \]

Applying Lemmas 1 and 2 we get
\[ S(Q, L) = -q^{m/2} e(a_1 a_2 + \ldots + a_{n-1} a_n + a_n a_{n-1} + \beta a_n). \] (4.10)
If $m$ is odd we have
\[ S(Q, L) = \prod_{i=1}^{m} \sum_{a_i} e(\lambda a_i + a_{i-1} + a_i + a_{i-1} + a_i) \sum_{\lambda} e(\lambda^2 + a_n \lambda). \]

Applying Lemmas 1 and 3 we get
\[ S(Q, L) = \begin{cases} q^{(m+1)/2} e(a_1 a_2 + \ldots + a_{n-1} a_n) & (a_m = 1), \\ 0 & (a_m \neq 1). \end{cases} \] (4.11)

By means of (4.9), (4.10) and (4.11) we have evaluated $S(Q, L)$ when $Q$ is assumed to be in normal form. We shall now express these results in an invariant form.
We first consider the case \( m \) even. Comparing (2.23) with (4.9) we get

\[
S(Q, L) = q^{m+1} \eta(Q) \mu(L)
\]

when \( Q \) is of type \(+1\); comparing (2.24) with (4.10) we get

\[
S(Q, L) = -q^{m-1} \eta(Q) \mu(L)
\]

when \( Q \) is of type \(-1\). We may therefore state

**Theorem 6.** If \( m \) is even and \( Q(x) \) is nonsingular we have

\[
(4.12) \quad S(Q, L) = q^{m+1} \eta(Q) \mu(L). \]

When \( m \) is odd let \( Q_0(x) = x_1 x_2 + \ldots + x_{m-1} x_{m} + x_m \).

By (2.11) we have \( \eta(Q_0) = 1 \). If the transformation

\[
y_i = \sum_{j=1}^{m} c_{ij} x_j \quad (i = 1, 2, \ldots, m)
\]

carries \( Q_0(x) \) into \( Q(y) \), it follows from (2.15) that

\[
e^b \eta(Q) = 1. \]

In the next place consider \( Q(a_1, a_2, \ldots, a_m) \) as defined by (2.7). In particular by a simple calculation we get

\[
Q_0(a_1, a_2, \ldots, a_m) = a_1^2.
\]

By (2.8) we have

\[
Q(a_1, a_2, \ldots, a_m) = \left( \sum_{i=1}^{m} a_i^2 \right)^2.
\]

By (2.15) and (2.20)

\[
\sum_{i=1}^{m} a_i b_i = e \sum_{i=1}^{m} b_i a_i.
\]

It follows that

\[
(4.15) \quad \omega(Q, L) = Q(a_1, a_2, \ldots, a_m) \eta(Q)
\]

is an absolute invariant which reduces to \( a_1^2 \) when \( Q = Q_0 \).

It remains to give an invariante description of the coefficient

\[
e(a_1 a_2 + \ldots + a_{m-1} a_{m-1})
\]

occurring in the right member of (4.11). To do this we consider the quadratic form \( Q(x) + L(x) \) in the \( m+1 \) indeterminates \( x_1, \ldots, x_m, t \). When \( Q = Q_0 \) we find that

\[
Q_0(x) + L(x) = x_1 x_2 + \ldots + x_{m-1} x_m + x_m + \sum_{i=1}^{m} b_i x_i
\]

\[
= (x_1 + a_1 t)(x_2 + a_1 t) + \ldots + (x_{m-1} + a_{m-1} t)(x_m + a_{m-1} t) + x_m^2 + a_m x_m t + (a_1 a_2 + \ldots + a_{m-2} a_{m-1}) t^2.
\]

We may assume that \( a_m = 1 \). It follows that

\[
\tau(Q_0 + L) = e(a_1 a_2 + \ldots + a_{m-2} a_{m-1}).
\]

We may now state

**Theorem 7.** If \( m \) is odd and \( Q(x) \) is nonsingular, then

\[
(4.16) \quad S(Q, L) = \begin{cases} 
q^{m+1} \eta(Q) \mu(L) & \text{if } \tau(Q, L) = 1, \\
0 & \text{if } \tau(Q, L) \neq 1,
\end{cases}
\]

where \( \omega(Q, L) \) is defined by (4.15).

5. Number of solutions. As an application of the results of § 4 we shall now determine the number of solutions of the equation

\[
Q(x_1, \ldots, x_m) + L(x_1, \ldots, x_m) = a,
\]

where \( Q(x) \) is nonsingular and \( L(x) \) is arbitrary. If we let \( N \) denote the number of solutions of (5.1) then by (3.3)

\[
qN = \sum_{y_1, \ldots, y_m} \sum_{\gamma} e(ab + bQ(y)) + bL(c)
\]

\[
= q^{m-1} \sum_{b \neq 0} e(bQ(c) + bL(c)).
\]

Hence

\[
N = q^{m-1} \sum_{b \neq 0} e(ab) S(bQ, bL).
\]

We consider first the case \( m \) even. It is clear from the definition of \( \tau(Q) \) that

\[
(5.3) \quad \tau(bQ) = \tau(Q) \quad (b \neq 0).
\]

Also it follows from the definition of \( \xi(Q, L) \) that

\[
(5.4) \quad \xi(bQ, bL) = b \xi(Q, L) \quad (b \neq 0).
\]

Thus by (4.12), (5.3) and (5.4)

\[
\sum_{b \neq 0} e(ab) S(bQ, bL) = q^{m+1} \tau(Q) \sum_{b \neq 0} e[(a + \xi(Q, L)) b].
\]
It is convenient to define
\[
L(a) = \sum_{b \neq 0} e(ab) = \begin{cases} 1 & (a = 0), \\ -1 & (a \neq 0). \end{cases}
\]
Then clearly
\[
\sum_{b \neq 0} e(ab) S(bQ, bL) = q^{s^2} \tau(Q) \zeta(a + \zeta(Q, L)).
\]
Substituting from (5.6) in (5.2) we obtain
\[
N = q^{s^2} + q^{s^2} \tau(Q) \zeta(a + \zeta(Q, L))\]

**Theorem 8.** For \(m\) even and \(Q(x)\) nonsingular the number of solutions of (5.1) is given by
\[
N = q^{n-1} + q^{n-2} \zeta(Q) \zeta(a + \zeta(Q, L))\]

Turning now to the case \(m\) odd it is clear from (5.3) that
\[
\tau(bQ + mL) = \tau(Q + L) \quad (b \neq 0).
\]
Also it is evident from the definition that \(e(bQ, bL) = e(bQ, L) \quad (b \neq 0).\)
Thus (4.16) gives
\[
S(bQ, bL) = \begin{cases} q^{s^2} \zeta(Q + L) & (bQ, L) = 1, \\ 0 & (bQ, L) \neq 1. \end{cases}
\]
and therefore
\[
\sum_{b \neq 0} e(ab) S(bQ, bL) = q^{s^2} \zeta(Q + L) \zeta(a + \zeta(Q, L)).
\]
Substituting in (5.2) we get

**Theorem 9.** For \(m\) odd and \(Q(x)\) nonsingular the number of solutions of (5.1) is given by
\[
N = q^{n-1} + q^{n-2} \zeta(Q) \zeta(a + \zeta(Q, L)),
\]
provided \(\omega(Q, L) \neq 0.\) If however \(\omega(Q, L) = 0\) then we have
\[
N = q^{n-1}.
\]
It may be of interest to state these results when the linear form \(L(x)\) is identically zero. We find that (5.7) reduces to
\[
N = q^{n-1} + q^{n-2} \zeta(Q) \quad (m \text{ even}),
\]
Since \(\omega(Q, 0) = 0, (5.8)\) does not apply and we have only
\[
N = q^{n-1} \quad (m \text{ odd}).
\]
It is not difficult to prove (5.7)' and (3.9)' directly.

6. **Weighted sums.** Let \(\lambda_1, \ldots, \lambda_n\) be arbitrary elements of \(GF(q)\) and consider the sum
\[
N(\lambda) = N(\lambda; Q, L) = \sum \text{e}(\lambda c_1 + \ldots + \lambda_n c_n),
\]
where the summation is extended over all solutions of
\[
Q(x_1, \ldots, x_n) + L(x_1, \ldots, x_n) = a.
\]
As above we assume that \(Q(x)\) is nonsingular while \(L(x)\) is arbitrary. Clearly
\[
qN(\lambda) = \sum_{c_1, \ldots, c_n} \sum e(ab + Q(c) + bL(c) + A(c)),
\]
where for brevity we put
\[
A(c) = \lambda_1 c_1 + \ldots + \lambda_n c_n.
\]
We rewrite (6.3) in the form
\[
N(\lambda) = q^{-1} \sum_{c_1, \ldots, c_n} e(A(c)) + q^{-1} \sum_{c_1} e(ab) \sum_{c_1, \ldots, c_n} e(bQ(c) + bL(c) + A(c)).
\]
Put
\[
A(\lambda) = \sum_{c_1, \ldots, c_n} e(A(c)) = \begin{cases} q^{n} \quad (\lambda_1 = \ldots = \lambda_n = 0), \\ 0 \quad (\text{otherwise}). \end{cases}
\]
Then it is evident that
\[
N(\lambda) = q^{-1} A(\lambda) + q^{-1} \sum_{c_1} e(ab) S(bQ, bL + A).
\]
For \(m\) even we have, by (5.3) and (6.4),
\[
S(bQ, bL + A) = q^{s^2} \tau(Q) \zeta[b\zeta(Q, L + b^{-1}A)].
\]
To evaluate \(\zeta(Q, L + b^{-1}A)\) let
\[
\sum_{j=1}^{m} a_j c_j = a_i, \quad \sum_{j=1}^{m} \overline{a_j} d_j = \lambda_i \quad (i = 1, 2, \ldots, m).
\]
Then
\[
\zeta(Q, L + b^{-1}A) = Q(a_1 + b^{-1}d_1, \ldots, a_m + b^{-1}d_m) = \zeta(Q, L) + b^{-1}Q + b^{-1}d_i \zeta(Q, A),
\]
where
\[
\xi = \sum_{j=1}^{m} b_j a_j \lambda_i, \quad \langle b\overline{a} \rangle = I.
\]
Hence
\[ S(bQ, bL + A) = q^{m+2} \tau(Q) \sigma(b \zeta(Q, L) + \xi + b^{-1} \zeta(Q, A)) \]
and (6.5) becomes
\[ N(\lambda) = q^{-1} N(\lambda) + q^{m-n-3} \tau(Q) \sigma(\xi) \sum_{a+b \zeta(Q, L) + b^{-1} \zeta(Q, A)} \]
If we define the Kloosterman sum
\[ K(a, b) = \sum_{c \neq b} \sigma(ac + bd^{-1}) \]
then it is clear that
\[ N(\lambda) = q^{-1} N(\lambda) + q^{m-n-3} \tau(Q) \sigma(\xi) K(a + \zeta(Q, L), \zeta(Q, A)) \]
This proves
\[ \text{Theorem 10. For } m \text{ even and } Q(x) \text{ nonsingular the sum } N(\lambda) \text{ satisfies (6.8) with } \lambda, \xi \text{ defined by (6.4), (6.6), respectively.} \]
For odd \( m \) we have by (4.16)
\[ S(bQ, bL + A) = q^{m+1} \tau(Q + t(bL + A)) \]
provided \( \omega(bQ, bL + A) = 1 \) and 0 otherwise. It is easily verified that
\[ \omega(bQ, bL + A) = b \omega(Q, L) + b^{-1} \omega(Q, A) \]
The following theorem now follows at once.
\[ \text{Theorem 11. For } m \text{ odd and } Q(x) \text{ nonsingular we have} \]
\[ N(\lambda) = q^{-1} N(\lambda) + q^{m-n-3} \tau(Q) \sigma(\xi) \sum_{b \neq 0} \omega(b \zeta(Q, L) + b^{-1} \omega(Q, A), \]
where the summation on the right is over all \( b \) such that
\[ b \omega(Q, L) + b^{-1} \omega(Q, A) = 1 \]
Remark. Equation (6.10) has two solutions if
\[ \omega(Q, L) \omega(Q, A) \neq 0, \quad \sigma(\omega(Q, L) \omega(Q, A)) = 1; \]
one solution if just one of \( \omega(Q, L), \omega(Q, A) = 0 \); otherwise there are no solutions.
For results corresponding to Theorems 10 and 11 when \( q \) is odd see [1].

7. Kloosterman sums. We conclude with a few properties of the sum
\[ K(a, b) = \sum_{c \neq 0} \sigma(ac + bd^{-1}) \]
Clearly
\[ K(a, b) = K(b, a) \]
and
\[ K(a, 0) = k(a), \]
with \( k(a) \) defined by (5.5). Also it is evident that
\[ K(a, b) = K(ab, 1) \quad (ab \neq 0) \]
This implies
\[ K(a, b) = K(b, c) \quad (ab = c \neq 0) \]
It follows at once from (7.1) that \( K(a, b) \) is an odd integer. Also since
\[ \sum_{a \neq 0} K(a, 1) = \sum_{a \neq 0} \sigma(b^{-1}) \sum_{a \neq 0} \sigma(ab) = 0, \]
we have
\[ \sum_{a \neq 0} K(a, 1) = 1 \]
Thus it is clear that, for \( q > 2, K(a, 1) \) takes on both positive and negative values.
Since
\[ K(a, 1) = \sum_{b \neq 0} \sigma(ab + b^{-1}) = \sum_{b \neq 0} \sigma(a b^2 + b^{-1}) = \sum_{b \neq 0} \sigma(ab + b^{-1}) \]
it follows that
\[ K(a, 1) = K(a^2, 1) = \ldots = K(a^{n-1}, 1) \]
If \( n \) is prime and \( a \neq 1 \), the numbers \( a, a^2, \ldots, a^{n-1} \) are distinct. Hence
\[ K(1, 1) = 1 \pmod{n} \quad \text{(n prime).} \]
In the next place
\[ \sum_{a \neq 0} K^2(a, 1) = \sum_{a \neq 0} \sum_{b \neq 0} \sigma(ab + b^{-1} + e^{-1}) \]
\[ = \sum_{b \neq 0} \sigma(b^{-1} + e^{-1}) \sum_{a \neq 0} \sigma(ab + b^{-1}) = q(q - 1) \]
and therefore
\[ \sum_{a \neq 0} K^2(a, 1) = q^2 - q - 1. \]
To evaluate the sum of the cubes take
\[ \sum_{a \neq 0} K^3(a, b) = \sum_{a \neq 0} \sum_{b \neq 0} \sigma(a(x + y + z) + b(x^{-1} + y^{-1} + z^{-1})) = q^2 N, \]
where \( N \) denotes the number of nonzero solutions of the system

\[
\begin{align*}
x + y + z &= 0, \\
\frac{1}{x} + \frac{1}{y} + \frac{1}{z} &= 0.
\end{align*}
\]

This number is equal to the number of nonzero solutions of

\[x^2 + xy + y^2 = 0.\]

For \( q = 2^n, n \) odd, \( x^2 + xy + y^2 \) is irreducible in \( F[x, y] \), so that \( N = 0 \).

For \( n \) even, on the other hand, we have \( N = 2(q-1) \). Thus

\[
\sum_{a,b}^2 K^2(a, b) = \begin{cases} 2q^2(q-1) & \text{(n even)}, \\
0 & \text{(n odd)}.\end{cases}
\]

Since \( K(0, 0) = q-1 \) and

\[
\sum_{a,b}^2 K^2(a, 0) = \sum_{b \in F} K^2(0, b) = -(q-1),
\]

it follows that

\[
\sum_{a,b}^2 K^2(a, b) = \begin{cases} q^2 + q - 1 & \text{(n even)}, \\
-(q-1)^2 + 2(q-1) & \text{(n odd)}\end{cases}
\]

and therefore

\[
\sum_{a,b}^2 K^3(a, 1) = \begin{cases} (q+1)^2 & \text{(n even)}, \\
-(q^2 - 2q - 1) & \text{(n odd)}\end{cases}
\]

For the sum of the fourth powers we have

\[
\sum_{a,b}^2 K^4(a, b) = q^2 M,
\]

where \( M \) is the number of nonzero solutions of

\[
\begin{align*}
x + y + z + t &= 0, \\
\frac{1}{x} + \frac{1}{y} + \frac{1}{z} + \frac{1}{t} &= 0.
\end{align*}
\]

This system is equivalent to

\[
(x+y)(x+z)(y+z) = 0,
\]

\[xyz(x+y+z) \neq 0.\]

We find that

\[
M = (q-1)^3 - (q-1)(q-2)(q-3) = (q-1)(3q-5),
\]

so that

\[
\sum_{a,b}^2 K^4(a, b) = q^2(q-1)(3q-5).
\]

Finally

\[
\sum_{a,b}^2 K^4(a, 1) = 2q^3 - 2q^2 - 3q - 1,
\]

so that

\[
K(a, 1) = O(q^{3k}) \quad (a \neq 0).
\]

References
