Gauss sums and the number of solutions to the matrix equation $XAX^T = 0$ over GF($2^p$)

by

PHILIP G. BUCKHIREN (Clemson, S. C.)

1. Introduction. Let GF($q$) denote a finite field of order $q = p^r$, $p$ a prime. Let $A$ and $B$ be symmetric matrices of order $n$, rank $m$ and order $s$, rank $k$, respectively, over GF($q$). Carlitz [2] has determined the number $N_s(A, B)$ of solutions $X$ over GF($q$), for $p$ an odd prime, to the matrix equation

$$XAX^T = B$$

(1.1)

of arbitrary rank when $n = m$. Furthermore, Hodges [4] has determined the number $N_s(A, B, r)$ of $s \times n$ matrices $X$ of rank $r$ over GF($q$), $p$ an odd prime, which satisfy (1.1). Perkins [6], [7] has determined the number $N_s(A, B, r)$ of solutions $X$ over GF($q$), $q = 2^p$, to the matrix equation $XAX^T = 0$ and has enumerated the $s \times n$ matrices $X$ of given rank $r$ over GF($q$), $q = 2^p$, such that $XAX^T = 0$.

The purpose of this paper is to determine the number $N_s(A, 0)$ of solutions $X$ over GF($q$), $q = 2^p$, to the matrix equation $XAX^T = 0$. In determining this number, Gauss sums, as developed in Section 2, are used. Also needed are Albert’s canonical forms for symmetric matrices over fields of characteristic two ([1]).

Throughout the remainder of this paper, GF($q$) will denote a finite field of order $q = 2^p$ and $V_n$ will denote an $n$-dimensional vector space over GF($q$).

2. Gauss sums and alternating bilinear forms. For $a$ in GF($q$), let $t$ be the mapping from GF($q$) into GF($q$) defined by $t(a) = a + a^2 + \ldots + a^{q-1}$. Then $t$ maps onto the prime subfield of GF($q$). Hence, for each $a$ in GF($q$), $t(a) = m \cdot 1$ where $m = 0$ or 1. Let $\sigma$ be the map from GF($q$) onto the multiplicative subgroup $\{-1, 1\}$ of the reals defined by

$$\sigma(a) = (-1)^m \quad \text{where } t(a) = m \cdot 1.$$

(2.1)
Clearly, \( t(a + b) = t(a) + t(b) \) for all \( a, b \) in \( \text{GF}(q) \). It follows that \( e(a + b) = e(a) + e(b) \) for all \( a, b \) in \( \text{GF}(q) \) and that

\[
\sum_{\beta} e(a\beta) = \begin{cases} \frac{q}{2} & (a = 0), \\ 0 & (a \neq 0), \end{cases}
\]

where the summation in (2.2) extends over all \( \beta \) in \( \text{GF}(q) \). From (2.2), it follows that

\[
\sum_{\alpha, \beta} e(a\beta) = q,
\]

where the summation in (2.3) extends over all \( a, \beta \) in \( \text{GF}(q) \).

Perkins [7] has shown that

\[
\sum_{\alpha} e(\sigma(DB)) = \begin{cases} q - 1 & (D = 0), \\ 0 & (D \neq 0), \end{cases}
\]

where \( D \) is a symmetric matrix, where the sum extends over all upper triangular matrices \( B \), and where \( e(DB) \) denotes the trace of the matrix \( DB \).

Let \( f \) be a symmetric bilinear form on \( V_n \times V_n \). Let \( V_n^* = \{ y \in V_n | f(x, y) = 0 \} \) for all \( x \) in \( V_n \). We say that \( f \) is nondegenerate if \( V_n^* = \{ 0 \} \). Clearly, \( V_n^* \) is a subspace of \( V_n \). The rank of \( f \) is defined to be \( n \)-dim \( V_n^* \). It is said to be an alternating bilinear form if \( f(x, x) = 0 \) for all \( x \) in \( V_n \). An alternating matrix over \( \text{GF}(q) \) is a symmetric matrix with 0 diagonal. Chevalley [3] has shown that for each nondegenerate alternating bilinear form \( f \) on \( V_n \times V_n \), there exists a basis for \( V_n \) such that, relative to that basis, \( f(\xi, \eta) = \xi \eta^T \) for all \( \xi, \eta \) in \( V_n \), where

\[
D = \begin{bmatrix} I_r & 0 \\ I_r & 0 \end{bmatrix},
\]

an alternating matrix of rank \( 2r \). Chevalley [3] has also shown that if \( f \) is a bilinear form of rank \( t \) on \( V_n \times V_n \) and if \( f(\xi, \eta) = \xi \eta^T \) for all \( \xi, \eta \) in \( V_n \), then the matrix rank of \( A \) is \( t \). It follows that if \( f \) is a nondegenerate alternating bilinear form of rank \( p \) on \( V_n \times V_n \), then there exists a basis such that, relative to that basis, \( f(\xi, \eta) = \xi \eta^T \) for all \( \xi, \eta \) in \( V_n \), where

\[
D = \begin{bmatrix} I_r & 0 \\ I_r & 0 \end{bmatrix},
\]

and, hence, \( p = 2r \).

Albert [1] has proved the following theorems:

**Theorem 2.1.** Every matrix congruent to an alternating matrix is an alternating matrix.

**Theorem 2.2.** Let \( D \) be an \( s \times s \) nonsingular alternate matrix over \( \text{GF}(q) \). Then there is a nonsingular matrix \( P \) such that

\[
P^T A P = \begin{bmatrix} I_r \\ I_r \end{bmatrix}.
\]

**Theorem 2.3.** Let \( D \) be an \( s \times s \) alternate matrix of rank \( p \) over \( \text{GF}(q) \). Then there is a nonsingular matrix \( P \) such that

\[
P^T A P = \begin{bmatrix} I_p \\ I_p \end{bmatrix} (p = 2r).
\]

**Theorem 2.4.** If \( A \) is an \( s \times s \) symmetric, nonalternate matrix of rank \( r \) over \( \text{GF}(q) \), then there is a nonsingular matrix \( P \) such that

\[
P^T A P = \begin{bmatrix} I_r \\ I_r \end{bmatrix}.
\]

Let \( D \) be an \( s \times s \) matrix over \( \text{GF}(q) \) and let \( g_D \) be the bilinear form defined by \( g_D(\xi, \eta) = \xi D \eta^T \). Define

\[
T(g_D) = \sum_{\xi, \eta} e[g_D(\xi, \eta)],
\]

where the summation extends over all \( \xi, \eta \) in \( V_n \).

**Theorem 2.5.** Let \( D \) be an \( s \times s \) alternate matrix over \( \text{GF}(q) \). If \( M = P D P^T \) for a nonsingular matrix \( P \), then \( T(g_M) = T(g_D) \). Furthermore, if \( D \) is of rank \( 2r \), then \( T(g_D) = q^{r(s-r)} \).

**Proof.** We have

\[
T(g_M) = \sum_{\xi, \eta} e[g_M(\xi, \eta)],
\]

\[
= q \sum_{\xi, \eta} e[\xi M \eta^T] = \sum_{\xi, \eta} e[(\xi P) D (\eta P)^T]
\]

\[
= q \sum_{\xi, \eta} e[D \eta^T] = \sum_{\xi, \eta} e[g_D(\eta, \eta)] = T(g_D),
\]

since \( P \) is nonsingular.

By Theorem 2.3, if \( D \) is of rank \( 2r \), there is a nonsingular matrix \( P \) such that

\[
P D P^T = \begin{bmatrix} I_r & 0 \\ I_r & 0 \end{bmatrix}.
\]
Thus, \( T(g_B) = T(g_R) \), where

\[
R = \begin{bmatrix}
0 & I_r \\
I_r & 0
\end{bmatrix}.
\]

But

\[
R(e^{i \xi}, e^{i \eta}) = e^{i \eta} R e^{i \eta} = \sum_{k=1}^{r} e^{i \eta} \cdot \sum_{i=1}^{r} e^{i \xi}.
\]

Hence,

\[
T(g_B) = T(g_R) = \sum_{e \in \mathcal{A}} \sum_{e \in \mathcal{A}} g_{B} (e, \eta) = \sum_{e \in \mathcal{A}} \sum_{e \in \mathcal{A}} g_{R} (e, \eta) = \sum_{e \in \mathcal{A}} \sum_{e \in \mathcal{A}} g_{B} (e, \eta) = \sum_{e \in \mathcal{A}} \sum_{e \in \mathcal{A}} g_{R} (e, \eta) = \sum_{e \in \mathcal{A}} \sum_{e \in \mathcal{A}} g_{B} (e, \eta) = \sum_{e \in \mathcal{A}} \sum_{e \in \mathcal{A}} g_{R} (e, \eta).
\]

Thus, \( T(g_B) = q^{(t^2 - t)} q^{t^2 - t} = q^{t^2 - t} \). Define

\[
\mathcal{A} = \{ B \mid B \text{ is an } s \times s \text{ upper triangular matrix with 0 diagonal} \}
\]

and

\[
\mathcal{A} = \{ D \mid D \text{ is an } s \times s \text{ alternate matrix} \}.
\]

Let \( M(s, 2r) \) denote the number of \( s \times s \) upper triangular matrices \( B \) such that \( \text{rank}(B + B^T) = 2r \). Let \( K(s, 2r) \) denote the number of \( B \) in \( \mathcal{A} \) such that \( \text{rank}(B + B^T) = 2r \). Let \( I_0(s, t) \) denote the number of \( D \) in \( \mathcal{A} \) of rank \( t \).

MacWilliams [5] has found that

\[
I_0(s, t) = \begin{cases}
0 & \text{(if } t \text{ is odd)},
\prod_{i=1}^{r} \frac{q^{2i-1} - 1}{q^{2i-1} - 1} & \text{(if } t = 2r).
\end{cases}
\]

Theorem 2.8. The mapping \( \tau \) from \( \mathcal{A} \) into \( \mathcal{A} \) defined by \( \tau(B) = B + B^T \) is a one-to-one mapping onto \( \mathcal{A} \). For each \( r = 0, 1, \ldots, [s/2] \), where \([s/2]\) denotes the largest integer not exceeding \( s/2 \), define \( \mathcal{A}_0(r) = \{ B \in \mathcal{A} \mid \text{rank } (B + B^T) = 2r \} \) and define \( \mathcal{A}(r) = \{ D \in \mathcal{A} \mid \text{rank } D = 2r \} \). Then \( \tau \), the restriction of \( \tau \) to \( \mathcal{A}_0(r) \), is a one-to-one mapping onto \( \mathcal{A}(r) \) for each \( r = 0, 1, \ldots, [s/2] \).

Proof. Clearly, \( \tau \) has its range in \( \mathcal{A} \) and is onto. If \( B_1 \) and \( B_2 \) are in \( \mathcal{A} \) and if \( \tau(B_1) = \tau(B_2) \), then \( B_1 + B_2 = B_2 + B_2 \). Thus \( B_1 + B_2 = B_2 + B_2 \), from which it follows that \( B_1 + B_2 \) is upper triangular and lower triangular. Since \( B_1 + B_2 \) has 0 diagonal, \( B_1 + B_2 = 0 \). Thus \( B_1 = B_2 \).

For any \( r = 0, 1, \ldots, [s/2] \), it is clear that \( \tau \) is one-to-one. Choose any \( D \in \mathcal{A}(r) \). Since \( \tau \) is onto, there is a \( B \in \mathcal{A} \) such that \( \tau(B) = B + B^T = D \). Since \( D \) is in \( \mathcal{A}(r) \), \( \text{rank } (B + B^T) = 2r \). Thus, \( B \in \mathcal{A}_0(r) \), and it follows that \( \tau \) is onto \( \mathcal{A}(r) \).

Since \( K(s, 2r) \) is the number of elements in \( \mathcal{A}_0(r) \) and \( I_0(s, 2r) \) is the number of elements in \( \mathcal{A}(r) \), Theorem 2.6 yields

\[
K(s, 2r) = I_0(s, 2r) \quad \text{for each } r = 0, 1, \ldots, [s/2].
\]

Lemma 2.1. \( M(s, 2r) = q^{r} L_0(s, 2r) \), for each \( r = 0, 1, \ldots, [s/2] \).

Proof. If \( B \) is any matrix from \( \mathcal{A}_0(r) \), then \( B + B^T = C + C^T \) from which it follows that \( \text{rank } (C + C^T) = 2r \). Thus, \( M(s, 2r) = q^{r} K(s, 2r) = q^{r} L_0(s, 2r) \) by (2.9).

The following lemma will be needed in Sections 3 and 4.

Lemma 2.2. Let \( A \) be any \( n \times n \) symmetric matrix. If there is a nonsingular matrix \( P \) such that \( PAP^T = C \), then \( N_s(A, 0) = N_s(C, 0) \).

Proof. Clearly \( XX^T = 0 \) if and only if \( YY^T = 0 \) where \( Y = XP \).

Since \( P \) is nonsingular, the result follows.

3. Determination of \( N_s(A, 0) \), \( A \) a nonalternate symmetric matrix.

Perkins [7] has found the number \( N_s(I_n, 0) \) of \( s \times n \) matrices \( X \) over \( GF(q) \) such that \( XX^T = 0 \).

Let \( A \) be any \( n \times n \) nonalternate symmetric matrix of rank \( q \). By Theorem 2.4, there is a nonsingular matrix \( P \) such that

\[
PAP^T = \begin{bmatrix} I_q & 0 \\ 0 & 0 \end{bmatrix}.
\]

By Lemma 2.2, \( N_s(A, 0) = N_s(C, 0) \), where

\[
C = \begin{bmatrix} I_q & 0 \\ 0 & 0 \end{bmatrix}.
\]

Consider the equation

\[
XX^T = 0.
\]
Let $X = [X_1, X_2]$, where $X_1$ is $s \times q$ and $X_2$ is $s \times (n-q)$. Then, (3.1) becomes

$$0 = XDX^T = [X_1, X_2] \begin{bmatrix} I_q & 0 \\ 0 & 0 \end{bmatrix} \begin{bmatrix} X_1 \\ X_2 \end{bmatrix} = X_1X_1^T.$$  

Thus, if $X_1X_2^T = 0$ and $X_2$ is any $s \times (n-q)$ matrix, then $X = [X_1, X_2]$ satisfies (3.1). The number of ways to choose $X_2$ is $q^{(n-q)}$.

This proves the following theorem.

**Theorem 3.1.** Let $A$ be an $n \times n$ nonalternate symmetric matrix of rank $q$. Then the number of $s \times s$ matrices $X$ over GF($q$) such that $XAX^T = 0$ is

$$N_s(A, 0) = q^{(n-q)} N_s(I_1, 0).$$

4. **Determination of $N_s(A, 0)$, A alternate.** Let $A$ be an $n \times n$ alternate matrix of rank $t$. By Theorem 2.3, there is a nonsingular matrix $P$ such that

$$PAP^T = \begin{bmatrix} 0 & I_q \\ I_q & 0 \end{bmatrix}, \quad t = 2q.$$  

By Lemma 2.2, $N_s(A, 0) = N_s(P, 0)$ where

$$P = \begin{bmatrix} 0 & I_q \\ I_q & 0 \end{bmatrix}.$$  

Thus, it suffices to find $N_s(P, 0)$. Since $P$ is symmetric, $XDX^T$ is symmetric. Hence, by (2.4), \( \sum_B e(\sigma(XDX^TB)) = q^{q-1} \) if and only if $XDX^T = 0$, and \( \sum_B e(\sigma(XDX^TB)) = 0 \) otherwise, where the summation extends over all $s \times s$ upper triangular matrices $B$. Thus

$$\sum_B \sum_X e(\sigma(XDX^TB)) = \sum_X \sum_B e(\sigma(XDX^TB)) = N_s(P, 0)q^{q-1}.$$  

A simple calculation shows that

$$\sigma(XDX^TB) = \sum_{k=1}^{s} \left[ \sum_{j=1}^{q} \sum_{i=1}^{s} x_{i+k} b_{ij} x_{i+j} \right] + \sum_{k=q+1}^{s} \left[ \sum_{j=1}^{q} \sum_{i=k-q}^{s} x_{i+k-q} b_{ij} x_{i+k-q} \right].$$

Let $g_B$ be the bilinear form defined by $g_B(x, y) = xBy^T$ for all $x, y$ in $V_s$. Then, $g_B(x, y) = \sum_{j=1}^{q} \sum_{i=1}^{s} x_i b_{ij} y_j$. Thus, (4.2) becomes

$$\sigma(XDX^TB) = \sum_{k=1}^{s} g_B(x_k, x_{k+q}) + \sum_{k=q+1}^{s} g_B(x_k, x_{k-q}).$$

Hence,

$$\sum_X \sum_B e(\sigma(XDX^TB)) = \sum_X \sum_B e\left( \sum_{k=1}^{s} g_B(x_k, x_{k+q}) + \sum_{k=q+1}^{s} g_B(x_k, x_{k-q}) \right)$$

$$= \sum_B \sum_X \left[ \sum_{k=1}^{s} e\left( g_B(x_k, x_{k+q}) \right) + \sum_{k=q+1}^{s} e\left( g_B(x_k, x_{k-q}) \right) \right]$$

$$= \sum_B \sum_X \left[ \prod_{k=1}^{s} e\left( g_B(x_k, x_{k+q}) \right) + \prod_{k=q+1}^{s} e\left( g_B(x_k, x_{k-q}) \right) \right].$$

Thus, (4.1) becomes

$$N_s(P, 0)q^{q-1} = \sum_B \sum_X \left[ \prod_{k=1}^{s} e\left( g_B(x_k, x_{k+q}) \right) + \prod_{k=q+1}^{s} e\left( g_B(x_k, x_{k-q}) \right) \right].$$

Let $X = [x_1^T, \ldots, x_n^T]$, where $x_k = (x_{1k}, \ldots, x_{nk}), 1 \leq k \leq n$. Furthermore, let $\sum_{x_k^T}$ indicate a sum extending over all vectors $x_k$ in $V_s$. Then (4.4) becomes

$$N_s(R, 0)q^{\frac{n(n+1)}{2}} = \sum_B \sum_{x_1} \cdots \sum_{x_n} \left[ \prod_{k=1}^{s} e\left( g_B(x_k, x_{k+q}) \right) + \prod_{k=q+1}^{s} e\left( g_B(x_k, x_{k-q}) \right) \right].$$

Next, consider

$$\sum_{x} \sum_{y} e\left( g_B(x, \eta) \right) e\left( g_B(\xi, y) \right)$$

$$= \sum_{x} \sum_{y} e\left[ \xi y_B^T + \eta B x^T \right] = \sum_{x} e\left[ \xi y_B^T + \xi x^T B y^T \right]$$

$$= \sum_{x} e\left[ \xi (B + B^T) x^T \right] = \sum_{x} e\left[ g_{B+B^T}(x, \eta) \right]$$

$$= T(g_{B+B^T}), \quad \text{where } T(g_B) \text{ is as defined in (2.5).}$$

Thus, (4.5) becomes

$$N_s(R, 0)q^{\frac{n(n+1)}{2}} = \sum_B \sum_{x_1} \cdots \sum_{x_n} \left[ \prod_{k=1}^{s} T\left( g_{B+B^T} \right) \right].$$
Since \( M(s, 2r) \) denotes the number of \( s \times s \) upper triangular matrices such that \( \operatorname{rank} (B + B^t) = 2r \), it follows from Theorem 2.5 that

\[
N_s(R, 0) q^{s(s+1)} = q^{s(n-2r)} \sum_{\sigma=0}^{[s/2]} M(s, 2r) (q^{2s-r})^{\sigma}.
\]

From Lemma 2.1, it follows that

\[
N_s(R, 0) q^{s(s+1)/2} = q^{s(n-2r)} \sum_{\sigma=0}^{[s/2]} q^{\sigma} L_\sigma(s, 2r) (q^{2s-r})^{\sigma}
\]

This completes the proof of the following theorem.

**Theorem 4.1.** Let \( A \) be an \( n \times n \) alternate matrix of rank \( 2 \phi \) over \( GF(q) \). The number \( s \times n \) matrices \( X \) over \( GF(q) \) such that \( XAX^t = 0 \) is

\[
N_s(A, 0) = \frac{q^{s(n+1)}}{q^{s(s+1)/2}} \sum_{\sigma=0}^{[s/2]} L_\sigma(s, 2r) q^{-2\sigma}
\]

where \( L_\sigma(s, 2r) \) is given by \( (2.8) \).

**References**


**Acta Arithmetica**

**XXIII** (1973)

**Slowly growing sequences and discrepancy modulo one**

by

R. C. Baker (London)

§ 1. Introduction. Let \( y_1, y_2, \ldots, y_k \ldots \) be numbers in the interval \( [0, 1) \) and let \( \alpha \) be any number in \( [0, 1) \). We say that \( y_1, y_2, \ldots \) is a uniformly distributed sequence if for any \( [a, b) \) \( (0 \leq a < b \leq 1) \), the number \( k \) of \( y_1, y_2, \ldots, y_k \) falling in \( [a, b) \) satisfies

\[
k' = (b - a)k + o(k) \quad \text{as} \quad k \to \infty.
\]

One can prove [3] that if \( (1.1) \) is true for all \( a \) and \( b \) \( (0 \leq a < b \leq 1) \), it holds uniformly in \( a \) and \( b \) : that is, the discrepancy \( D(k) \) of the sequence \( (y_k)_{k=1}^{\infty} \), defined by

\[
D(k) = \sup_{0 \leq a < b \leq 1} \frac{1}{k} \left| \frac{k'}{k} - (b - a) \right|
\]

(1.2)

satisfies \( \lim_{k \to \infty} D(k) = 0 \).

The behaviour of \( D(k) \) is closely related to that of the exponential sums

\[
s(k, h) = \left| \sum_{j=1}^{k} e^{2\pi i y_j h} \right| \quad (k \geq 1, h \geq 1).
\]

(1.3)

It can be shown that

\[
\lim_{k \to \infty} D(k) = 0 \quad \text{iff} \quad \lim_{k \to \infty} \frac{s(k, h)}{k} = 0 \quad \text{for all} \quad h \geq 1
\]

(1.4)

and, more precisely,

\[
\frac{1}{2\pi} \sup_{h \geq 1} \frac{s(k, h)}{h} \leq kD(k) \leq 150 \left( \frac{k}{m+1} + \frac{m}{h} \right)
\]

(1.5)

for all integers \( m \geq 1 \) ([7], Theorem III and [1], p. 14).

Now suppose that

\[
\lambda_1 \leq \lambda_2 \leq \ldots \leq \lambda_n \leq \ldots
\]

(1.6)