

Gauss sums and the number of solutions to the matrix equation $XAX^T = 0$ over $\text{GF}(2^v)$

by

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

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

$$(1.1) \quad XAX^T = B$$

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

The purpose of this paper is to determine the number $N_s(A, 0)$ of solutions X over $\text{GF}(q)$, $q = 2^v$, 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, $\text{GF}(q)$ will denote a finite field of order $q = 2^v$ and V_n will denote an n -dimensional vector space over $\text{GF}(q)$.

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

$$(2.1) \quad e(a) = (-1)^m \quad \text{where } t(a) = m \cdot 1.$$

Clearly, $t(\alpha + \beta) = t(\alpha) + t(\beta)$ for all α, β in $\text{GF}(q)$. It follows that $e(\alpha + \beta) = e(\alpha) \cdot e(\beta)$ for all α, β in $\text{GF}(q)$ and that

$$(2.2) \quad \sum_{\beta} e(\alpha\beta) = \begin{cases} q & (\alpha = 0), \\ 0 & (\alpha \neq 0), \end{cases}$$

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

$$(2.3) \quad \sum_{\alpha, \beta} e(\alpha\beta) = q$$

where the summation in (2.3) extends over all α, β in $\text{GF}(q)$.

Perkins [7] has shown that

$$(2.4) \quad \sum_B e(\sigma(DB)) = \begin{cases} q^{\frac{s(s+1)}{2}} & (D = 0), \\ 0 & (D \neq 0), \end{cases}$$

where D is an $s \times s$ symmetric matrix, where the sum extends over all $s \times s$ upper triangular matrices B , and where $\sigma(DB)$ denotes the trace of the matrix DB .

Let f be a symmetric bilinear form on $V_n \times V_n$. Let $V_n^* = \{y \in V_n \mid f(x, y) = 0 \text{ for all } x \text{ in } V_n\}$. 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 $n - \dim V_n^*$. f is said to be an *alternating bilinear form* if $f(x, x) = 0$ for all x in V_n . An *alternate 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, $f(\xi, \eta) = \xi D \eta^T$ for all ξ, η in V_n , where

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

an alternate 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 $f(\xi, \eta) = \xi A \eta^T$ for all ξ, η in V_n , then the matrix rank of A is t . It follows that if f is a degenerate alternating bilinear form of rank p on $V_n \times V_n$, then there exists a basis such that, relative to that basis, $f(\xi, \eta) = \xi D \eta^T$ for all ξ, η in V_n where

$$D = \begin{bmatrix} 0 & I_r & \\ I_r & 0 & \\ & & 0 \end{bmatrix}$$

and, hence, $p = 2r$.

Albert [1] has proved the following theorems:

THEOREM 2.1. *Every matrix congruent to an alternate matrix is an alternate 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*

$$PAP^T = \begin{bmatrix} 0 & I_r \\ I_r & 0 \end{bmatrix}.$$

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*

$$PAP^T = \begin{bmatrix} 0 & I_r & \\ I_r & 0 & \\ & & 0 \end{bmatrix} \quad (p = 2r).$$

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*

$$PAP^T = \begin{bmatrix} I_r & 0 \\ 0 & 0 \end{bmatrix}.$$

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

$$(2.5) \quad T(g_D) = \sum_{\xi, \eta} e[g_D(\xi, \eta)],$$

where the summation extends over all ξ, η in V_s .

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

Proof. We have

$$\begin{aligned} T(g_M) &= \sum_{\xi, \eta} e[g_M(\xi, \eta)] \\ &= \sum_{\xi, \eta} e[\xi M \eta^T] = \sum_{\xi, \eta} e[(\xi P) D (\eta P)^T] \\ &= \sum_{\gamma, \delta} e[\gamma D \delta^T] = \sum_{\gamma, \delta} e[g_D(\gamma, \delta)] = T(g_D), \end{aligned}$$

since P is nonsingular.

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

$$PDP^T = \begin{bmatrix} 0 & I_r & \\ I_r & 0 & \\ & & 0 \end{bmatrix}.$$



Thus, $T(g_D) = T(g_R)$, where

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

But

$$g_R(\xi, \eta) = \xi R \eta^T = \sum_{i=1}^r \xi_i \eta_{r+i} + \sum_{i=1}^r \xi_{r+i} \eta_i.$$

Hence,

$$\begin{aligned} T(g_D) &= T(g_R) = \sum_{\xi, \eta} e[g_R(\xi, \eta)] \\ &= \sum_{\substack{\xi_1, \dots, \xi_s \in \text{GF}(q) \\ \eta_1, \dots, \eta_s \in \text{GF}(q)}} e \left[\sum_{i=1}^r \xi_i \eta_{r+i} + \sum_{i=1}^r \xi_{r+i} \eta_i \right] \\ &= \sum_{\substack{\xi_1, \dots, \xi_s \in \text{GF}(q) \\ \eta_1, \dots, \eta_s \in \text{GF}(q)}} \left[\prod_{i=1}^r e(\xi_i \eta_{r+i}) \right] \cdot \left[\prod_{i=1}^r e(\xi_{r+i} \eta_i) \right] \\ &= \sum_{\substack{\xi_{2r+1}, \dots, \xi_s \\ \eta_{2r+1}, \dots, \eta_s}} \left[\prod_{i=1}^r \sum_{\xi_i, \eta_{r+i}} e(\xi_i \eta_{r+i}) \right] \cdot \left[\prod_{i=1}^r \sum_{\xi_{r+i}, \eta_i} e(\xi_{r+i} \eta_i) \right] \\ &= \sum_{\substack{\xi_{2r+1}, \dots, \xi_s \\ \eta_{2r+1}, \dots, \eta_s}} \left[\prod_{i=1}^r q \right] \cdot \left[\prod_{i=1}^r q \right] \quad \text{by (2.3)}. \end{aligned}$$

Thus, $T(g_D) = q^{(s-2r)} \cdot q^{(s-2r)} \cdot q^{2r} = q^{2(s-r)}$. Define

$$(2.6) \quad \mathcal{B}_0 = \{B \mid B \text{ is an } s \times s \text{ upper triangular matrix with } 0 \text{ diagonal}\}$$

and

$$(2.7) \quad \mathcal{A} = \{D \mid D \text{ is an } s \times s \text{ alternate matrix}\}.$$

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{B}_0 such that $\text{rank}(B + B^T) = 2r$. Let $L_0(s, t)$ denote the number of D in \mathcal{A} of rank t .

MacWilliams [5] has found that

$$(2.8) \quad L_0(s, t) = \begin{cases} 0 & (\text{if } t \text{ is odd}), \\ \prod_{i=1}^r \frac{q^{2i-2} - 1}{q^{2i} - 1} \prod_{i=0}^{2r-1} (q^{s-i} - 1) & (\text{if } t = 2r). \end{cases}$$

THEOREM 2.6. *The mapping τ from \mathcal{B}_0 into \mathcal{A} defined by $\tau(B) = B + B^T$ is a one-to-one mapping onto \mathcal{A} . For each $r = 0, 1, \dots, [s/2]$, where $[s/2]$ denotes the largest integer not exceeding $s/2$, define $\mathcal{B}_0(r) = \{B \in \mathcal{B}_0 \mid \text{rank}(B + B^T) = 2r\}$ and define $\mathcal{A}(r) = \{D \in \mathcal{A} \mid \text{rank } D = 2r\}$. Then τ_r , the restriction of τ to $\mathcal{B}_0(r)$, is a one-to-one mapping onto $\mathcal{A}(r)$ for each $r = 0, 1, \dots, [s/2]$.*

Proof. Clearly, τ has its range in \mathcal{A} and is onto. If B_1 and B_2 are in \mathcal{B}_0 and if $\tau(B_1) = \tau(B_2)$, then $B_1 + B_1^T = B_2 + B_2^T$. Thus $B_1 + B_2 = B_1^T + B_2^T$, 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 $r = 0, 1, \dots, [s/2]$, it is clear that τ_r is one-to-one. Choose any D in $\mathcal{A}(r)$. Since τ is onto, there is a B in \mathcal{B}_0 such that $\tau(B) = B + B^T = D$. Since D is in $\mathcal{A}(r)$, $\text{rank}(B + B^T) = \text{rank } D = 2r$. Thus, $B \in \mathcal{B}_0(r)$, and it follows that τ_r is onto $\mathcal{A}(r)$.

Since $K(s, 2r)$ is the number of elements in $\mathcal{B}_0(r)$ and $L_0(s, 2r)$ is the number of elements in $\mathcal{A}(r)$, Theorem 2.6 yields

$$(2.9) \quad K(s, 2r) = L_0(s, 2r) \quad \text{for each } r = 0, 1, \dots, [s/2].$$

LEMMA 2.1. $M(s, 2r) = q^s L_0(s, 2r)$, for each $r = 0, 1, \dots, [s/2]$.

Proof. If B is any matrix from $\mathcal{B}_0(r)$ and if $C = B + D$, where D is any $s \times s$ diagonal matrix, then $B + B^T = C + C^T$ from which it follows that $\text{rank}(C + C^T) = 2r$. Thus, $M(s, 2r) = q^s K(s, 2r) = q^s L_0(s, 2r)$ 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 $XCX^T = 0$ if and only if $YAY^T = 0$ 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 $\text{GF}(q)$ such that $XX^T = 0$.

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

$$PAP^T = \begin{bmatrix} I_\rho & 0 \\ 0 & 0 \end{bmatrix}.$$

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

$$C = \begin{bmatrix} I_\rho & 0 \\ 0 & 0 \end{bmatrix}.$$

Consider the equation

$$(3.1) \quad XCX^T = 0.$$



Let $X = [X_1, X_2]$, where X_1 is $s \times \rho$ and X_2 is $s \times (n - \rho)$. Then, (3.1) becomes

$$0 = X C X^T = [X_1, X_2] \begin{bmatrix} I_\rho & 0 \\ 0 & 0 \end{bmatrix} \begin{bmatrix} X_1 \\ X_2 \end{bmatrix} = X_1 X_1^T.$$

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

This proves the following theorem.

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

$$N_s(A, 0) = q^{s(n-\rho)} N_s(I_\rho, 0).$$

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

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

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

$$R = \begin{bmatrix} 0 & I_\rho \\ I_\rho & 0 \\ & & 0 \end{bmatrix}.$$

Thus, it suffices to find $N_s(R, 0)$. Since R is symmetric, $XR X^T$ is symmetric. Hence, by (2.4), $\sum_B e(\sigma(XR X^T B)) = q^{\frac{s(s+1)}{2}}$ if and only if $XR X^T = 0$, and $\sum_B e(\sigma(XR X^T B)) = 0$ otherwise, where the summation extends over all $s \times s$ upper triangular matrices B . Thus

$$(4.1) \quad \sum_B \sum_X e(\sigma(XR X^T B)) = \sum_X \sum_B e(\sigma(XR X^T B)) = N_s(R, 0) q^{\frac{s(s+1)}{2}}.$$

A simple calculation shows that

$$(4.2) \quad \sigma(XR X^T B) = \sum_{k=1}^{\rho} \left[\sum_{j=1}^s \sum_{i=1}^s x_{i, \rho+k} b_{ji} x_{jk} \right] + \sum_{k=\rho+1}^{2\rho} \left[\sum_{j=1}^s \sum_{i=1}^s x_{i, k-\rho} b_{ji} x_{jk} \right].$$

Let g_B be the bilinear form defined by $g_B(x, y) = x B y^T$ for all x, y in V_s .

Then, $g_B(x, y) = \sum_{i=1}^s \sum_{j=1}^s x_i b_{ij} y_j$. Thus, (4.2) becomes

$$(4.3) \quad \sigma(XR X^T B) = \sum_{k=1}^{\rho} g_B(x_k, x_{\rho+k}) + \sum_{k=\rho+1}^{2\rho} g_B(x_k, x_{k-\rho}).$$

Hence,

$$\begin{aligned} \sum_B \sum_X e(\sigma(XR X^T B)) &= \sum_B \sum_X e \left[\sum_{k=1}^{\rho} g_B(x_k, x_{\rho+k}) + \sum_{k=\rho+1}^{2\rho} g_B(x_k, x_{k-\rho}) \right] \\ &= \sum_B \sum_X \left[\prod_{k=1}^{\rho} e(g_B(x_k, x_{\rho+k})) \right] \left[\prod_{k=\rho+1}^{2\rho} e(g_B(x_k, x_{k-\rho})) \right] \\ &= \sum_B \sum_X \prod_{k=1}^{\rho} e(g_B(x_k, x_{\rho+k})) \cdot e(g_B(x_{\rho+k}, x_k)). \end{aligned}$$

Thus, (4.1) becomes

$$(4.4) \quad N_s(R, 0) q^{\frac{s(s+1)}{2}} = \sum_B \sum_X \prod_{k=1}^{\rho} e(g_B(x_k, x_{\rho+k})) \cdot e(g_B(x_{\rho+k}, x_k)).$$

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

$$\begin{aligned} (4.5) \quad N_s(R, 0) q^{\frac{s(s+1)}{2}} &= \sum_B \sum_{x_1^T} \dots \sum_{x_n^T} \left[\prod_{k=1}^{\rho} e(g_B(x_k, x_{\rho+k})) \cdot e(g_B(x_{\rho+k}, x_k)) \right] \\ &= \sum_B \sum_{x_{2\rho+1}^T} \dots \sum_{x_n^T} \left[\prod_{k=1}^{\rho} \sum_{x_k^T} \sum_{x_{\rho+k}^T} e(g_B(x_k, x_{\rho+k})) e(g_B(x_{\rho+k}, x_k)) \right]. \end{aligned}$$

Next, consider

$$\begin{aligned} \sum_{\xi} \sum_{\eta} e(g_B(\xi, \eta)) e(g_B(\eta, \xi)) &= \sum_{\xi, \eta} e[\xi B \eta^T + \eta B \xi^T] = \sum_{\xi, \eta} e[\xi B \eta^T + \xi B^T \eta^T] \\ &= \sum_{\xi, \eta} e[\xi (B + B^T) \eta^T] = \sum_{\xi, \eta} e[g_{B+B^T}(\xi, \eta)] \\ &= T(g_{B+B^T}), \quad \text{where } T(g_D) \text{ is as defined in (2.5)}. \end{aligned}$$

Thus, (4.5) becomes

$$\begin{aligned} (4.6) \quad N_s(R, 0) q^{\frac{s(s+1)}{2}} &= \sum_B \sum_{x_{2\rho+1}^T} \dots \sum_{x_n^T} \left[\prod_{k=1}^{\rho} T(g_{B+B^T}) \right] \\ &= q^{s(n-2\rho)} \sum_B [T(g_{B+B^T})]^{\rho}. \end{aligned}$$

Since $M(s, 2r)$ denotes the number of $s \times s$ upper triangular matrices such that $\text{rank}(B+B^T) = 2r$, it follows from Theorem 2.5 that

$$(4.7) \quad N_s(R, 0) q^{\frac{s(s+1)}{2}} = q^{s(n-2r)} \sum_{r=0}^{[s/2]} M(s, 2r) (q^{2(s-r)})^c.$$

From Lemma 2.1, it follows that

$$(4.8) \quad N_s(R, 0) q^{\frac{s(s+1)}{2}} = q^{s(n-2r)} \sum_{r=0}^{[s/2]} q^s L_0(s, 2r) (q^{2(s-r)})^c.$$

This completes the proof of the following theorem.

THEOREM 4.1. *Let A be an $n \times n$ alternate matrix of rank $2r$ over $\text{GF}(q)$. The number of $s \times n$ matrices X over $\text{GF}(q)$ such that $XA X^T = 0$ is*

$$N_s(A, 0) = \frac{q^{s(n+1)}}{q^{\frac{s(s+1)}{2}}} \sum_{r=0}^{[s/2]} L_0(s, 2r) q^{-2er}$$

where $L_0(s, 2r)$ is given by (2.8).

References

- [1] A. A. Albert, *Symmetric and alternate matrices in an arbitrary field, I*, AMS Trans. 43 (1938), pp. 386-436.
- [2] L. Carlitz, *Representations by quadratic forms in a finite field*, Duke Math. J. 21 (1954), pp. 123-137.
- [3] C. Chevalley, *The algebraic theory of spinors*, New York 1954.
- [4] J. H. Hodges, *A symmetric matrix equation over a finite field*, Math. Nachr. 30 (1965), pp. 221-228.
- [5] J. MacWilliams, *Orthogonal matrices over finite fields*, Amer. Math. Monthly 76 (1969), pp. 152-164.
- [6] J. C. Perkins, *Rank r solutions to the matrix equation $XX^T = 0$ over a field of characteristic two*, Math. Nachr. 48 (1971), pp. 69-76.
- [7] — *Gauss sums and the matrix equation $XX^T = 0$ over fields of characteristic two*, Acta Arith. 19 (1971), pp. 205-214.

CLEMSON UNIVERSITY
Clemson, South Carolina

Received on 18. 2. 1972

(257)

Slowly growing sequences and discrepancy modulo one

by

R. C. BAKER (London)

§ 1. Introduction. Let $y_1, y_2, \dots, y_k \dots$ be numbers in the interval

$$[0, 1) = \{x: 0 \leq x < 1\}.$$

We say that y_1, y_2, \dots is a *uniformly distributed sequence* if for any $[a, b)$ ($0 \leq a < b \leq 1$), the number k' of y_1, \dots, y_k falling in $[a, b)$ satisfies

$$(1.1) \quad k' = (b-a)k + o(k) \quad \text{as } k \rightarrow \infty.$$

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

$$(1.2) \quad D(k) = \sup_{0 \leq a < b \leq 1} \left| \frac{k'}{k} - (b-a) \right|,$$

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

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

$$(1.3) \quad s(k, h) = \left| \sum_{j=1}^k e^{2\pi i y_j h} \right| \quad (k \geq 1, h \geq 1).$$

It can be shown that

$$(1.4) \quad \lim_{k \rightarrow \infty} D(k) = 0 \quad \text{iff } \lim_{k \rightarrow \infty} \frac{s(k, h)}{h} = 0 \quad \text{for all } h \geq 1$$

and, more precisely,

$$(1.5) \quad \frac{1}{2\pi} \sup_{h \geq 1} \frac{s(k, h)}{h} \leq kD(k) \leq 150 \left(\frac{k}{m+1} + \sum_{h=1}^m \frac{s(k, h)}{h} \right)$$

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

Now suppose that

$$(1.6) \quad \lambda_1 \leq \lambda_2 \leq \dots \leq \lambda_n \leq \dots$$