TRANSACTIONS OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 189, 1974

RANK r SOLUTIONS TO THE MATRIX EQUATION $XAX^T = C$, A ALTERNATE, OVER GF(2^y)

BY
PHILIP G. BUCKHIESTER

ABSTRACT. Let GF(q) denote a finite field of characteristic two. Let V_n denote an n-dimensional vector space over GF(q). An $n \times n$ symmetric matrix A over GF(q) is said to be an alternate matrix if A has zero diagonal. Let A be an $n \times n$ alternate matrix over GF(q) and let C be an $s \times s$ symmetric matrix over GF(q). By using Albert's canonical forms for symmetric matrices over fields of characteristic two, the number $N(A, C, n, s, r)$ of $s \times n$ matrices X of rank r over GF(q) such that $XAX^T = C$ is determined.

A symmetric bilinear form on $V_n \times V_n$ is said to be alternating if $f(x, x) = 0$, for each x in V_n. Let f be such a bilinear form. A basis $(x_1, \ldots, x_\rho, y_1, \ldots, y_\rho)$, $n = 2\rho$, for V_n is said to be a symplectic basis for V_n if $f(x_i, x_j) = f(y_i, y_j) = 0$ and $f(x_i, y_j) = \delta_{ij}$, for each i, $j = 1, 2, \ldots, \rho$. In determining the number $N(A, C, n, s, r)$, it is shown that a symplectic basis for any subspace of V_n can be extended to a symplectic basis for V_n. Furthermore, the number of ways to make such an extension is determined.

1. Introduction. Let GF(q) denote a finite field of order $q = p^y$, p a prime. Let A and C be symmetric matrices of order n, rank m and order s, rank k, respectively, over GF(q). Carlitz [4] has determined the number $N(A, C, n, s)$ of $s \times n$ matrices X of arbitrary rank over GF(q), for p an odd prime, satisfying the matrix equation $XAX^T = C$ when $n = m$. Perkins [9], [10] has determined the number $N(I, 0, n, s)$ of solutions X over GF(q), $q = 2^y$, to the matrix equation $XX^T = 0$ and has enumerated the $s \times n$ matrices X of a given rank r over GF(q), $q = 2^y$, such that $XX^T = 0$. The author [3] has determined the number $N(A, 0, n, s)$ of $s \times n$ matrices X over GF(q), $q = 2^y$, such that $XAX^T = 0$.

An $n \times n$ symmetric matrix A over GF(2^y) is called an *alternate matrix* if A has 0 diagonal. Let A be such a matrix. The purpose of this paper is to determine the number $N(A, C, n, s, r)$ of $s \times n$ matrices X of rank r over GF(q), $q = 2^y$, such that $XAX^T = C$. In determining this number, Albert's canonical forms for symmetric matrices over fields of characteristic two are used [1]. These forms and the necessary theorems concerning them appear in §2. In §3, the number $N(A, C, n, s)$ of $s \times n$ matrices such that $XAX^T = C$, where A and C are of full rank, is determined. In §4, the requirement that A and C be of full rank is dropped, and $N(A, C, n, s, r)$ is determined.

The author wishes to express his appreciation to John D. Fulton, who suggested investigation of the symplectic group, which is used in §3 of this paper.

Throughout the remainder of this paper, GF(q) will denote a finite field of order $q = 2^y$ and V_n will denote an n-dimensional vector space over GF(q). Further, if M is any matrix over GF(q), RS[M] will denote the row space of M.

Presented to the Society, January 28, 1973; received by the editors July 10, 1972.

AMS (MOS) subject classifications (1970). Primary 15A24, 15A33; Secondary 15A63, 05A15.

2. **Albert's canonical forms and bilinear forms over** GF(q). Let f be a symmetric bilinear form on $V_n \times V_n$. For any subspace E of V_n, define $E^* = \{y \in V_n \mid f(x,y) = 0 \text{ for all } x \text{ in } E\}$. Clearly, E^* is a subspace of V_n. We say that f is *nondegenerate* if $V_n^* = \{0\}$. 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 GF(q) is a symmetric matrix with 0 diagonal. Let F_ρ denote the $2\rho \times 2\rho$ matrix $\left[\begin{smallmatrix} 0 & I_\rho \\ I_\rho & 0 \end{smallmatrix}\right]$, where I_ρ denotes the $\rho \times \rho$ identity matrix. Then F_ρ is an alternate matrix of rank 2ρ. Chevalley [6] 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, $f(\xi, \eta) = \xi F_\rho \eta^T$ for all ξ, η in V_n. Chevalley [6] 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 k on $V_n \times V_n$, then there exists a basis such that, relative to that basis, $f(\xi,\eta) = \xi\left[\begin{smallmatrix} F_\rho & 0 \\ 0 & 0 \end{smallmatrix}\right]\eta^T$ for all ξ, η in V_n and, hence, $k = 2\rho$.

The following theorem, which appears in [7], will be needed.

Theorem 2.1. *If E is a subspace of V_n, then*

$$\dim E^* = n - \dim E + \dim(E \cap V_n^*).$$

From this theorem, it follows that if f is a nondegenerate bilinear form, then for any subspace E of V_n, $\dim E^* = n - \dim E$.

Albert [1] has proved the following theorems:

Theorem 2.2. *Every matrix congruent to an alternate matrix is an alternate matrix.*

Theorem 2.3. *Let A be any $n \times n$ nonsingular alternate matrix over* GF(q). *Then there is a nonsingular matrix P such that $PAP^T = F_\rho$.*

Theorem 2.4. *Let A be an $n \times n$ alternate matrix of rank k over* GF(q). *Then there is a nonsingular matrix P such that $PAP^T = \left[\begin{smallmatrix} F_\rho & 0 \\ 0 & 0 \end{smallmatrix}\right]$ $(k = 2\rho)$.*

The set of all $n \times n$ matrices P over GF(q) such that $PF_\rho P^T = F_\rho$, $2\rho = n$, forms a group, called the *symplectic group*. Denote this group by $\mathrm{Sp}_n(q)$. Dickson [8] has calculated the order of $\mathrm{Sp}_n(q)$ to be

$$|\mathrm{Sp}_n(q)| = (q^n - 1)q^{n-1}(q^{n-2} - 1)q^{n-3} \cdots (q^2 - 1)q. \tag{2.1}$$

Let f be a nondegenerate, alternating bilinear form of rank 2ρ on V_n, $n = 2\rho$. A basis $(x_1, \ldots, x_\rho, y_1, \ldots, y_\rho)$ for V_n is called a *symplectic basis* for V_n if $f(x_i, x_j) = 0$, $f(y_i, y_j) = 0$, and $f(x_i, y_j) = \delta_{ij}$ for all $i, j = 1, 2, \ldots, \rho$. Chevalley [6] has proved the existence of a symplectic basis for any n-dimensional vector space V_n on which a nondegenrate, alternating bilinear form has been defined. The following theorem is a corollary to the proof of this result.

Theorem 2.5. *Let f be a nondegenerate, alternating bilinear form on $V_n \times V_n$, $n = 2\rho$. If $x_1, \ldots, x_\rho, y_1, \ldots, y_\gamma$, $\gamma < \rho$, are independent vectors in V_n such that $f(x_i, x_j) = 0$ for all $i, j = 1, 2, \ldots, \rho$, $f(y_i, y_j) = 0$ for all $i, j = 1, 2, \ldots, \gamma$, and $f(x_i, y_j) = \delta_{ij}$ for $i = 1, 2, \ldots, \rho$ and $j = 1, 2, \ldots, \gamma$, then there exist vectors $y_{\gamma+1}, \ldots, y_\rho$ in V_n such that $(x_1, \ldots, x_\rho, y_1, \ldots, y_\rho)$ forms a symplectic basis for V_n.*

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

Lemma 2.1. *Let A and C be symmetric matrices of orders n and s, respectively, over* GF (q). *If there exist nonsingular matrices P and Q such that $PAP^T = B$ and $QCQ^T = D$, then $N(A, C, n, s) = N(B, D, n, s)$. Further, for each r, $0 \leq r \leq \min(n, s)$, $N(A, C, n, s, r) = N(B, D, n, s, r)$.*

Proof. Since $N(A, C, n, s) = \sum_{r=0}^{\min(n,s)} N(A, C, n, s, r)$, it suffices to prove only the second statement of the lemma. If X is an $s \times n$ matrix of rank r, then $XBX^T = D$ if and only if $YAY^T = C$ where $Y = Q^{-1}XP$. Since P and Q are nonsingular, the result follows.

For integers n and k, let $\left[{n \atop k}\right]$ denote the q-binomial coefficient defined by $\left[{n \atop 0}\right] = 1$; $\left[{n \atop k}\right] = 0$, $k > n$; $\left[{n \atop k}\right] = (q)_n/(q)_k(q)_{n-k}$, $0 < k \leq n$, where $(q)_j = (q-1)(q^2-1)\cdots(q^j-1), j > 0$. The following lemma, which appears in [2], will be needed in §4.

Lemma 2.2. *Let X be an $s \times t$ matrix of rank r over* GF(q). *The number of $s \times m$ matrices $[X, Y]$ of rank $r + \gamma$ over* GF(q) *is given by*

$$L(s, t, m, r, r+\gamma) = \begin{bmatrix} m-t \\ \gamma \end{bmatrix} q^{r(m-t-\gamma)} \prod_{i=0}^{\gamma-1} (q^s - q^{r+i}).$$

3. **Determination of $N(A, C, n, s)$, A and C of full rank.** Let A be an $n \times n$ nonsingular alternate matrix over GF(q). By Theorem 2.3, there exists a nonsingular matrix P such that $PAP^T = F_\rho$, $n = 2\rho$. By Lemma 2.1, for any $s \times s$ symmetric matrix C, $N(A, C, n, s) = N(F_\rho, C, n, s)$. Let X be any $s \times n$ matrix and let $XF_\rho X^T = (b_{ij})$. A simple calculation shows that

$$\begin{aligned} b_{ii} &= \sum_{k=1}^{\rho} x_{i,k+\rho} x_{i,k} + \sum_{k=\rho+1}^{2\rho} x_{i,k-\rho} x_{i,k} \\ &= \sum_{k=1}^{\rho} x_{i,k+\rho} x_{i,k} + \sum_{i=1}^{\rho} x_{i,k} x_{i,k+\rho} = 0. \end{aligned}$$

Thus, $XF_\rho X^T$ has 0 diagonal. It follows that if C is any $s \times s$ symmetric, nonalternate matrix, then $N(A, C, n, s) = N(F_\rho, C, n, s) = 0$.

Suppose C is an $s \times s$ alternate matrix of full rank. By Theorem 2.3, there exists a nonsingular matrix Q such that $QCQ^T = F_\gamma$, $s = 2\gamma$. By Lemma 2.1, $N(A, C, n, s) = N(F_\rho, F_\gamma, n, s)$. Thus, it suffices to find $N(F_\rho, F_\gamma, n, s)$.

For any $s \times n$ matrix X such that $XF_\rho X^T = F_\gamma$, $s = 2\gamma$ and $n = 2\rho$, rank $X = 2\gamma \leq 2\rho$. For P and Q in $\mathrm{Sp}_n(q)$, let

$$P = \begin{bmatrix} P_1 \\ R_1 \\ P_2 \\ R_2 \end{bmatrix} \quad \text{and} \quad Q = \begin{bmatrix} Q_1 \\ S_1 \\ Q_2 \\ S_2 \end{bmatrix},$$

where P_1, P_2, Q_1, and Q_2 are $\gamma \times n$ matrices and R_1, R_2, S_1, and S_2 are $(\rho - \gamma) \times n$ matrices. Define the relation $\sim$ on $\mathrm{Sp}_n(q)$ by $P \sim Q$ if and only if $P_1 = Q_1$ and $P_2 = Q_2$. Clearly, $\sim$ is an equivalence relation on $\mathrm{Sp}_n(q)$. For any P in $\mathrm{Sp}_n(q)$, let $[P]$ denote the equivalence class containing P.

Theorem 3.1. *Define the mapping ϕ from $\{[P] \mid P \in \mathrm{Sp}_n(q)\}$ into $\{X \mid XF_\rho X^T = F_\gamma\}$ by $\phi([P]) = X$, where X is the $s \times n$ matrix such that row i of X equals row i of P, for $i = 1, 2, \ldots, \gamma$, and row $\gamma + j$ of X equals row $\rho + j$ of P, for $j = 1, 2, \ldots, \gamma$. Then ϕ is a one-to-one mapping onto $\{X \mid XF_\rho X^T = F_\gamma\}$.*

Proof. By definition of $\sim$, ϕ is well defined and one-to-one. Let f be the bilinear form on $V_n \times V_n$ defined by $f(\xi,\eta) = \xi F_\rho \eta^T$ for all ξ, η in V_n. Then $\operatorname{rank} f = n - \dim V_n^* = \operatorname{rank} F_\rho = 2\rho = n$. Thus, $V_n^* = \{0\}$. Clearly, $f(\xi,\xi) = 0$ for all ξ in V_n. Hence, f is a nondegenerate, alternating bilinear form on $V_n \times V_n$. By Theorem 2.1, if E is any subspace of V_n, then $\dim E^* = n - \dim E$. For any P in $\mathrm{Sp}_n(q)$, $PF_\rho P^T = F_\rho$. Let $P = [{P_1 \atop P_2}]$, where each of P_1 and P_2 is $\rho \times n$. Then

$$\begin{bmatrix} P_1 \\ P_2 \end{bmatrix} F_\rho [P_1^T P_2^T] = \begin{bmatrix} P_1 F_\rho P_1^T & P_1 F_\rho P_2^T \\ P_2 F_\rho P_1^T & P_2 F_\rho P_2^T \end{bmatrix} = \begin{bmatrix} 0 & I_\rho \\ I_\rho & 0 \end{bmatrix}.$$

Hence, the rows of P form a symplectic basis for V_n. Let $X = [{X_1 \atop X_2}] = \phi([P])$, where X_1 and X_2 are $\gamma \times n$. Then

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

Hence, the range of ϕ is a subset of $\{X \mid XF_\rho X^T = F_\gamma\}$. In order to show that ϕ is onto, let X be an $s \times n$ matrix such that $XF_\rho X^T = F_\gamma$. Suppose $X = [{X_1 \atop X_2}]$, where each of X_1 and X_2 is $\gamma \times n$, $X_1 = [x_1, x_2, \ldots, x_\gamma]^T$, and $X_2 = [y_1, y_2, \ldots, y_\gamma]^T$. Then $f(x_i, x_j) = f(y_i, y_j) = 0$ and $f(x_i, y_j) = \delta_{ij}$ for $i, j = 1, 2, \ldots, \gamma$. We will show that the symplectic basis $(x_1, \ldots, x_\gamma, y_1, \ldots, y_\gamma)$ for the subspace $\mathrm{RS}[X]$ can be extended to a symplectic basis for the whole space. If $\rho = \gamma$, then $(x_1, \ldots, x_\gamma, y_1, \ldots, y_\gamma)$ forms a symplectic basis for V_n and no extension is necessary. Suppose $\rho - \gamma = \tau > 0$. If $(\mathrm{RS}[X])^* \subseteq \mathrm{RS}[X]$ then, for any z in $(\mathrm{RS}[X])^*$, $z = \sum_{i=1}^{\gamma} a_i x_i + \sum_{i=1}^{\gamma} b_i y_i$. Thus, for any $j = 1, 2, \ldots, \gamma$,

$$0 = f(z, x_j) = \sum_{i=1}^{\gamma} a_i f(x_i, x_j) + \sum_{i=1}^{\gamma} b_i f(y_i, x_j) = b_j.$$

Similarly, $a_j = 0$ for $j = 1, 2, \ldots, \gamma$. Thus, $z = 0$ and $(\mathrm{RS}[X])^* = \{0\}$. But $\dim(\mathrm{RS}[X])^* = 2\rho - \dim \mathrm{RS}[X] = 2\rho - 2\gamma = 2\tau > 0$. Hence, there exists z_1 in $(\mathrm{RS}[X])^* - \mathrm{RS}[X]$. Suppose $z_2, z_3, \ldots, z_k$, $k < \tau$, have been chosen such that z_i is in $(\mathrm{RS}[M_{i-1}])^* - \mathrm{RS}[M_{i-1}]$ for $i = 1, 2, \ldots, k$, where M_j denotes the $(s + j) \times n$ matrix

$$\begin{bmatrix} X \\ z_1 \\ \cdot \\ \cdot \\ \cdot \\ z_j \end{bmatrix}, \qquad \text{for } j = 0, 1, \ldots, k.$$

Suppose $(\mathrm{RS}[M_k])^* \subseteq \mathrm{RS}[M_k]$. Then if z is in $(\mathrm{RS}[M_k])^*$, $z = \sum_{i=1}^{\gamma} a_i x_i + \sum_{i=1}^{\gamma} b_i y_i + \sum_{i=1}^{k} c_i z_i$. As before, $b_j = f(z, x_j) = 0$ and $a_j = f(z, y_j) = 0$ for $j = 1, 2, \ldots, \gamma$. Hence, $z = \sum_{i=1}^{k} c_i z_i$. Since f is an alternating bilinear form, z_i is in $(\mathrm{RS}[M_k])^*$ for $i = 1, 2, \ldots, k$. Thus, $(\mathrm{RS}[M_k])^* = \langle z_1, z_2, \ldots, z_k \rangle$, which implies $\dim(\mathrm{RS}[M_k])^* = k$. But, $\dim(\mathrm{RS}[M_k])^* = 2\rho - \dim \mathrm{RS}[M_k] = 2\rho - (2\gamma + k)$. This implies $2\rho - 2\gamma - k = k$, or $2\tau = 2\rho - 2\gamma = 2k < 2\tau$, a contradiction. Hence, there exists z_{k+1} in $(\mathrm{RS}[M_k])^* - \mathrm{RS}[M_k]$. Thus, there exist vectors $z_1, \ldots, z_{\rho-\gamma}$ in V_n such that $f(z_k, z_j) = f(x_i, z_j) = f(y_i, z_j) = 0$ for $i = 1, 2, \ldots, \gamma$ and j, $k = 1, 2, \ldots, \rho - \gamma$. By Theorem 2.5, there exist vectors $\omega_1, \ldots, \omega_{\rho-\gamma}$ such that $(x_1, \ldots, x_\gamma, z_1, \ldots, z_{\rho-\gamma}, y_1, \ldots, y_\gamma, \omega_1, \ldots, \omega_{\rho-\gamma})$ forms a symplectic basis for V_n. Let $Z = [z_1, \ldots, z_{\rho-\gamma}]^T$, $W = [\omega_1, \ldots, \omega_{\rho-\gamma}]^T$, and $P^T = [X_1^T Z^T X_2^T W^T]$. Then P is in $\mathrm{Sp}_n(q)$ and $\phi([P]) = X$. Thus, ϕ is onto.

Consider any P in $\mathrm{Sp}_n(q)$. We seek the order of the equivalence class $[P]$. Let $P^T = [X^T Z^T Y^T W^T]$, where each of X and Y is $\gamma \times n$ and each of Z and W is $(\rho - \gamma) \times n$. Clearly, for any Q in $\mathrm{Sp}_n(q)$, Q is in $[P]$ if and only if $Q^T = [X^T R^T Y^T S^T]$. Let $X = [x_1, \ldots, x_\gamma]^T$ and $Y = [y_1, \ldots, y_\gamma]^T$. Then the order of $[P]$ is equal to the number of ways we can extend the symplectic basis $(x_1, \ldots, x_\gamma, y_1, \ldots, y_\gamma)$ for the subspace $\mathrm{RS}[{}^X_Y]$ to a symplectic basis $(x_1, \ldots, x_\rho, y_1, \ldots, y_\rho)$ for V_n.

Theorem 3.2. *Let f be a nondegenerate, alternating bilinear form defined on $V_n \times V_n$, $n = 2\rho$. Let W be a 2γ-dimensional subspace of V_n. If $(x_1, \ldots, x_\gamma, y_1, \ldots, y_\gamma)$ is a symplectic basis for W, then the number of ways to extend this basis for W to a symplectic basis for V_n is given by*

$$K(\rho, \gamma) = \prod_{i=0}^{\rho-\gamma-1} (q^{2\rho-2\gamma-i} - q^i) \prod_{i=\gamma}^{\rho-1} q^{\rho-i}.$$

Proof. If z is in $W \cap W^*$, then $z = \sum_{i=1}^{\gamma} a_i x_i + \sum_{i=1}^{\gamma} b_i y_i$. As in the proof of Theorem 3.1, $a_j = b_j = 0$ for each $j = 1, 2, \ldots, \gamma$. Hence $W \cap W^* = (0)$. Since $\dim W^* = 2\rho - 2\gamma$, there are $q^{2\rho-2\gamma} - 1$ vectors in $W^* - W$. Thus, there are $q^{2\rho-2\gamma}-1$ choices for $x_{\gamma+1}$. Suppose $x_{\gamma+1},\ldots,x_{\gamma+k}$, $k<\rho-\gamma$, have been chosen so that $x_{\gamma+i}$ is in $(W\oplus\langle x_{\gamma+1},\ldots,x_{\gamma+i-1}\rangle)^*-(W\oplus\langle x_{\gamma+1},\ldots,x_{\gamma+i-1}\rangle)$, $i=2,\ldots,k$. If z is in $(W\oplus\langle x_{\gamma+1},\ldots,x_{\gamma+k}\rangle)^*\cap(W\oplus\langle x_{\gamma+1},\ldots,x_{\gamma+k}\rangle)$, then $z=\sum_{i=1}^{\gamma}a_ix_i+\sum_{i=1}^{\gamma}b_iy_i+\sum_{i=1}^{k}c_ix_{\gamma+i}$. Again, $a_j=b_j=0$ for $j=1,2,\ldots,\gamma$. Since f is alternating, it follows that

$$(W\oplus\langle x_{\gamma+1},\ldots,x_{\gamma+k}\rangle)^*\cap(W\oplus\langle x_{\gamma+1},\ldots,x_{\gamma+k}\rangle)=\langle x_{\gamma+1},\ldots,x_{\gamma+k}\rangle.$$

Thus, it is necessary and sufficient that $x_{\gamma+k+1}$ be chosen from $(W\oplus\langle x_{\gamma+1},\ldots,x_{\gamma+k}\rangle)^*-\langle x_{\gamma+1},\ldots,x_{\gamma+k}\rangle$. Hence the number of choices for $x_{\gamma+k+1}$ is $q^{2\rho-2\gamma-k}-q^k$. Since this is true for any $k<\rho-\gamma$, it follows that the number of choices for $(x_{\gamma+1},\ldots,x_\rho)$ is $\prod_{i=0}^{\rho-\gamma-1}q^{2\rho-2\gamma-i}-q^i$. For a given choice of $(x_{\gamma+1},\ldots,x_\rho)$, we seek the number of choices for $(y_{\gamma+1},\ldots,y_\rho)$ such that $f(x_i,x_j)=f(y_i,y_j)=0$ and $f(x_i,y_j)=\delta_{ij}$ for $i,\ j=1,2,\ldots,\rho$. Let $R=\langle x_1,\ldots,x_\gamma,x_{\gamma+2},\ldots,x_\rho,y_1,\ldots,y_\gamma\rangle$ and $S=\langle x_1,\ldots,x_\rho,y_1,\ldots,y_\gamma\rangle$. Then $y_{\gamma+1}$ must be chosen in R^*-S^*. $R\subseteq S$ implies $S^*\subseteq R^*$. Further, $\dim R^*=2\rho-(\rho-1+\gamma)=\rho-\gamma+1$ and $\dim S^*=2\rho-(\rho+\gamma)=\rho-\gamma$. Hence $\dim R^*/S^*=1$ and $|R^*-S^*|=q^{\rho-\gamma}(q-1)$. Define the mapping $\bar f$ from R^*/S^* into $\mathrm{GF}(q)$ by $\bar f(z+S^*)=f(z,x_{\gamma+1})$. It is easy to see that $\bar f$ is well defined. Let z_0 be such that $R^*/S^*=\langle z_0+S^*\rangle$. Then, z_0 is R^*-S^* and so $\bar f(z_0+S^*)\neq 0$. Thus, since $\dim R^*/S^*=1$, $\bar f$ is one-to-one. Hence, there exists precisely one coset z_1+S^* such that $\bar f(z_1+S)=1$. For any u in S^*, $f(z_1+u,x_{\gamma+1})=1$. Thus, the number of choices for $y_{\gamma+1}$ is equal to $|S^*|=q^{\rho-\gamma}$. Having chosen $y_{\gamma+1},\ldots,y_{\gamma+k}$, $k<\rho-\gamma$, we define $R_1=\langle x_1,\ldots,x_{\gamma+k},x_{\gamma+k+2},\ldots,x_\rho,y_1,\ldots,y_{\gamma+k}\rangle$ and $S_1=\langle x_1,\ldots,x_\rho,y_1,\ldots,y_{\gamma+k}\rangle$. Then $y_{\gamma+k+1}$ must be chosen from $R_1^*-S_1^*$ and must be such that $f(y_{\gamma+k+1},x_{\gamma+k+1})=1$. An argument similar to the one above shows that the number of choices for $y_{\gamma+k+1}$ is equal to $|S_1^*|=q^{\rho-\gamma-k}$. Thus, for any one of the $\prod_{i=0}^{\rho-\gamma-1}(q^{2\rho-2\gamma-i}-q^i)$ choices for $(x_{\gamma+1},\ldots,x_\rho)$, there are precisely $\prod_{i=\gamma}^{\rho-1}q^{\rho-i}$ choices for $(y_{\gamma+1},\ldots,y_\rho)$. This completes the proof.

By Theorem 3.1, $N(F_\rho,F_\gamma,n,s)=|\mathrm{Sp}_n(q)|/\|[P]\|$. Since, for any P in $\mathrm{Sp}_n(q)$, $\|[P]\|=K(\rho,\gamma)$, we have determined $N(F_\rho,F_\gamma,n,s)$.

Theorem 3.3. *Let A and C be nonsingular alternate matrices over $\mathrm{GF}(q)$ of orders $n=2\rho$ and $s=2\gamma$, respectively. The number $N(A,C,n,s)$ of $s\times n$ matrices X over $\mathrm{GF}(q)$ such that $XAX^T=C$ is*

$$N(A,C,n,s)=|\mathrm{Sp}_n(q)|/K(\rho,\gamma),$$

where $|\mathrm{Sp}_n(q)|$ is given by (2.1) and $K(\rho,\gamma)$ is given in Theorem 3.2. If D is any $s\times s$ nonalternate matrix over $\mathrm{GF}(q)$, then $N(A,D,n,s)=0$.

4. Determination of $N(A,C,n,s,r)$. Let A be an $n\times n$ nonsingular alternate matrix, $n=2\rho$, over $\mathrm{GF}(q)$ and let C be an $s\times s$ alternate matrix of rank $2\gamma<s$. By Theorem 2.3, Theorem 2.4, and Lemma 2.1, $N(A,C,n,s,r)=N(F_\rho,G_\gamma,n,s,r)$, where $G_\gamma=\left[\begin{smallmatrix}F_\gamma&0\\0&0\end{smallmatrix}\right]$. Let $X=\left[\begin{smallmatrix}X_1\\X_2\end{smallmatrix}\right]$ be any $s\times n$ matrix such that $XF_\rho X^T=G_\gamma$, where X_1 is $2\gamma\times n$ and X_2 is $(s-2\gamma)\times n$. Then

$$\begin{bmatrix} X_1 \\ X_2 \end{bmatrix} F_\rho [X_1^T X_2^T] = \begin{bmatrix} X_1 F_\rho X_1^T & X_1 F_\rho X_2^T \\ X_2 F_\rho X_1^T & X_2 F_\rho X_2^T \end{bmatrix} = \begin{bmatrix} F_\gamma & 0 \\ 0 & 0 \end{bmatrix}. \tag{4.1}$$

Hence, X_1 is such that $X_1 F_\rho X_1^T = F_\gamma$. The number $N(F_\rho, F_\gamma, n, 2\gamma)$ of such $2\gamma \times n$ matrices X_1 is given in Theorem 3.3. Let $X_1 = [x_1, \ldots, x_\gamma, y_1, \ldots, y_\gamma]^T$. By (4.1), in order that $X = [{X_1 \atop X_2}]$ be such that $XF_\rho X^T = G_\gamma$, $X_2 = [z_1, \ldots, z_{s-2\gamma}]^T$ must be such that $f(x_i, z_j) = f(y_i, z_j) = f(z_k, z_j) = 0$, for $i = 1, 2, \ldots, \gamma$ and $k, j = 1, 2, \ldots, s - 2\gamma$, where $f(\xi, \eta) = \xi F_\rho \eta^T$ for all ξ, η in V_n.

Theorem 4.1. *For a given $2\gamma \times n$ matrix X_1 over* GF(q) *such that $X_1 F_\rho X_1^T = F_\gamma$, the number of $s \times n$ matrices $X = [{X_1 \atop X_2}]$ of rank $2\gamma + \tau$ over* GF(q) *such that $XF_\rho X^T = G_\gamma$ is given by*

$$R(2\gamma, n, s, 2\gamma + \tau) = \begin{bmatrix} s - 2\gamma \\ \tau \end{bmatrix} \prod_{j=0}^{\tau-1} (q^{n-2\gamma-j} - q^j), \tag{4.2}$$

where $[{s-2\gamma \atop \tau}]$ is the q-binomial coefficient as defined in §2.

Proof. Let $Z = [z_1, \ldots, z_{s-1-2\gamma}]^T$ be an $(s - 1 - 2\gamma) \times n$ matrix over GF(q) such that $X_1 F_\rho Z^T = 0$ and $ZF_\rho Z^T = 0$. Let D denote the $(s - 1) \times n$ matrix $[{X_1 \atop Z}]$. If rank $D = 2\gamma + \tau$, then in order that $X_2 = [{Z \atop z_{s-2\gamma}}]$ be as required by the theorem, it is necessary and sufficient that $z_{s-2\gamma}$ be chosen from $(\mathrm{RS}[D])^* \cap \mathrm{RS}[D] = \mathrm{RS}[Z]$. Since rank $D = 2\gamma + \tau$, $\dim \mathrm{RS}[Z] \geq \tau$. If $\dim \mathrm{RS}[Z] > \tau$, then there exists z_i, $1 \leq i \leq s - 1 - 2\gamma$, such that z_i is in $\mathrm{RS}[M_{i-1}] - \langle z_1, \ldots, z_{i-1} \rangle$, where

$$M_j = \begin{bmatrix} X_1 \\ z_1 \\ \cdot \\ \cdot \\ \cdot \\ z_j \end{bmatrix}, \qquad j = 0, 1, \ldots, s - 1 - 2\gamma.$$

But z_i must be chosen from $(\mathrm{RS}[M_{i-1}])^*$, whose intersection with $\mathrm{RS}[M_{i-1}]$ is $\langle z_1, \ldots, z_{i-1} \rangle$. Thus, $\dim \mathrm{RS}[Z] = \tau$ and the number of choices for $z_{s-2\gamma}$ is q^τ. If Z is such that rank $D = 2\gamma + \tau - 1$, then $z_{s-2\gamma}$ must be chosen from $(\mathrm{RS}[D])^* - \mathrm{RS}[D] = (\mathrm{RS}[D])^* - \mathrm{RS}[Z]$. Since $\dim(\mathrm{RS}[D])^* = n - (2\gamma + \tau - 1)$ and $\dim \mathrm{RS}[Z] = \tau - 1$, the number of choices for such a $z_{s-2\gamma}$ is $q^{n-2\gamma-\tau+1} - q^{\tau-1}$. Thus, we obtain the difference equation

$$\begin{aligned} R(2\gamma, n, s, 2\gamma + \tau) &= q^\tau R(2\gamma, n, s - 1, 2\gamma + \tau) \\ &\quad + (q^{n-2\gamma-\tau+1} - q^{\tau-1}) R(2\gamma, n, s - 1, 2\gamma + \tau - 1), \end{aligned}$$

with initial conditions $R(2\gamma, n, s, 2\gamma) = 1$, for all $s \geq 2\gamma$, and $R(2\gamma, n, 2\gamma, 2\gamma + \tau) = 0$, for $\tau \neq 0$. By using a method due to Carlitz [5], one may derive

$R(2\gamma, n, s, 2\gamma + \tau)$ as given in (4.2) as the solution to this recurrence. It is easily seen that (4.2) is the solution to this recurrence.

Together, Theorems 3.3 and 4.1 yield the number $N(A, C, n, s, r)$, A nonsingular.

Theorem 4.2. *Let A be an $n \times n$ nonsingular alternate matrix, $n = 2\rho$, over* $\mathrm{GF}(q)$ *and let C be an $s \times s$ alternate matrix of rank 2γ. Then*

$$N(A, C, n, s, 2\gamma + \tau) = N(F_\rho, F_\gamma, n, 2\gamma) \cdot R(2\gamma, n, s, 2\gamma + \tau),$$
$$0 \le \tau \le \min(s, n) - 2\gamma,$$

where $N(F_\rho, F_\gamma, n, 2\gamma)$ is given in Theorem 3.3 *and $R(2\gamma, n, s, 2\gamma + \tau)$ is given in Theorem* 4.1.

Finally, let A be an $n \times n$ alternate matrix of rank $2\rho \le n$ and let C be an $s \times s$ alternate matrix of rank $2\gamma \le s$. By Theorem 2.3, Theorem 2.4, and Lemma 2.1, $N(A, C, n, s, r) = N(G_\rho, G_\gamma, n, s, r)$, $0 \le r \le \min(s, n)$, where $G_\rho = \left[\begin{smallmatrix} F_\rho & 0 \\ 0 & 0 \end{smallmatrix}\right]$ and $G_\gamma = \left[\begin{smallmatrix} F_\gamma & 0 \\ 0 & 0 \end{smallmatrix}\right]$. Let X be an $s \times n$ matrix of rank r over $\mathrm{GF}(q)$ such that $XG_\rho X^T = G_\gamma$. If $X = [X_1 X_2]$, where X_1 is $s \times 2\rho$ and X_2 is $s \times (n - 2\rho)$, then

$$[X_1 X_2]\begin{bmatrix} F_\rho & 0 \\ 0 & 0 \end{bmatrix}\begin{bmatrix} X_1^T \\ X_2^T \end{bmatrix} = X_1 F_\rho X_1^T = G_\gamma. \tag{4.3}$$

Further, rank $X = r$ implies rank $X_1 \ge r - (n - 2\rho)$. For any τ,

$$\max(r - n + 2\rho - 2\gamma, 0) \le \tau \le \min[\min(s, 2\rho) - 2\gamma, r - 2\gamma],$$

the number $N(F_\rho, G_\gamma, 2\rho, s, 2\gamma + \tau)$ of $s \times 2\rho$ matrices X_1 of rank $2\gamma + \tau$ over $\mathrm{GF}(q)$ such that $X_1 F_\rho X_1^T = G_\gamma$ is given in Theorem 4.2. Consider any such matrix X_1. By (4.3), any $s \times (n - 2\rho)$ matrix X_2 such that $X = [X_1 X_2]$ has rank r yields $XG_\rho X^T = G_\gamma$. The number of such matrices X_2 is the number $L(s, 2\rho, n, 2\gamma + \tau, r)$, given in Lemma 2.2. Thus, we have determined the number $N(A, C, n, s, r)$.

Theorem 4.3. *Let A be an $n \times n$ alternate matrix of rank 2ρ over* $\mathrm{GF}(q)$. *If C is an $s \times s$ nonalternate matrix over* $\mathrm{GF}(q)$, *then $N(A, C, n, s) = N(A, C, n, s, r) = 0$ for all r. If C is an $s \times s$ alternate matrix of rank 2γ over* $\mathrm{GF}(q)$ *and $2\gamma \le r \le \min(s, n)$, then the number $N(A, C, n, s, r)$ of $s \times n$ matrices X of rank r over* $\mathrm{GF}(q)$ *such that $XAX^T = C$ is given by*

$$N(A, C, n, s, r) = \sum_{\tau = h(r, n, \rho, \gamma)}^{d(s, \rho, \gamma, r)} N(F_\rho, G_\gamma, 2\rho, s, 2\gamma + \tau) \cdot L(s, 2\rho, n, 2\gamma + \tau, r)$$

where $N(F_\rho, G_\gamma, 2\rho, s, 2\gamma + \tau)$ is given in Theorem 4.2, *$L(s, 2\rho, n, 2\gamma + \tau, r)$ is given in Lemma* 2.2, *where $h(r, n, \rho, \gamma) = \max(r - n + 2\rho - 2\gamma, 0)$, and where $d(s, \rho, \gamma, r) = \min[\min(s, 2\rho) - 2\gamma, r - 2\gamma]$.*

Determination of the number $N(A, C, n, s, r)$, where A is an $n \times n$ symmetric, nonalternate matrix, will appear in a later communication.

REFERENCES

1. A. A. Albert, *Symmetric and alternate matrices in an arbitrary field*. I, Trans. Amer. Math. Soc. **43** (1938), 386–436.

2. J. Brawley and L. Carlitz, *Enumeration of matrices with prescribed row and column sums*, Linear Algebra and Appl. (to appear).

3. P. G. Buckhiester, *Gauss sums and the number of solutions to the matrix equations $XAX^T = 0$ over* GF(2^y), Acta Arith. **23** (1973), 271–278.

4. L. Carlitz, *Representations by quadratic forms in a finite field*, Duke Math. J. **21** (1954), 123–137. MR **15**, 604.

5.———, *The number of solutions of certain matric equations over a finite field*, Math. Nachr. (to appear).

6. C. Chevalley, *The algebraic theory of spinors*, Columbia University Press, New York, 1954. MR **15**, 678.

7. Dai Zong-duo (Tai Tsung-tuo), *On transitivity of subspaces in orthogonal geometry over fields of characteristic* 2, Acta Math. Sinica **16** (1966), 545–560 = Chinese Math. Acta **8** (1966), 569–584. MR **35** #209.

8. L. E. Dickson, *Linear groups*, Leipzig; reprint, Dover, New York, 1958. MR **21** #3488.

9. J. C. Perkins, *Rank r solutions to the matrix equation $XX^T = 0$ over a field of characteristic two*, Math. Nachr. **48** (1971), 69–76.

10.———, *Gauss sums and the matrix equation $XX^T = 0$ over fields of characteristic two*, Acta. Arith. **19** (1971), 205–214.

DEPARTMENT OF MATHEMATICAL SCIENCES, CLEMSON UNIVERSITY, CLEMSON, SOUTH CAROLINA 29631

Current address: Department of Mathematics, Valdosta State College, Valdosta, Georgia 31601