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 x n symmetric matrix A over GF(q) is said to be an alternate matrix if A has zero diagonal. Let A be an n x n alternate matrix over GF(q) and let C be an s x 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 x n matrices X of rank r over GF(q) such that XAX^T = C is determined.

A symmetric bilinear form on 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,...,x_p,y_1,...,y_p), n = 2p, for V_n is said to be a symplectic basis for V_n if f(x_i,y_j) = f(y_i,x_j) = 0 and f(x_i,y_i) = δ_{i,j}, for each i, j = 1, 2, ..., p. 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^r, 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 x 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^r, to the matrix equation XX^T = 0 and has enumerated the s x n matrices X of a given rank r over GF(q), q = 2^r, such that XX^T = 0. The author [3] has determined the number N(A,0,n,s) of s x n matrices X over GF(q), q = 2^r, such that XAX^T = 0.

An n x n symmetric matrix A over GF(2^r) 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 x n matrices X of rank r over GF(q), q = 2^r, 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 x n matrices X over GF(q), q = 2^r, 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^r 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.


Copyright © 1974, American Mathematical Society

201
2. Albert’s canonical forms and bilinear forms over \( \text{GF}(q) \). Let \( f \) be a symmetric bilinear form on \( V_n \times V_n \). For any subspace \( E \) of \( V_n \), define \( E^* = \{ y \in V_n | f(x,y) = 0 \text{ for all } x \in E \} \). 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 \( n - \text{dim } V_n^* \). \( f \) 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. Let \( F_p \) denote the \( 2p \times 2p \) matrix \( \begin{bmatrix} I_p & 0 \\ 0 & -I_p \end{bmatrix} \), where \( I_p \) denotes the \( p \times p \) identity matrix. Then \( F_p \) is an alternate matrix of rank \( 2p \). 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, \( f(\xi, \eta) = \xi F_p \eta^T \) for all \( \xi, \eta \) 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 \( \xi, \eta \) 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, \( f(\xi, \eta) = \xi \begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix} \eta^T \) for all \( \xi, \eta \) in \( V_n \) and, hence, \( k = 2p \).

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

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

\[
\text{dim } E^* = n - \text{dim } E + \text{dim}(E \cap V_n^*). 
\]

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

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 \( \text{GF}(q) \). Then there is a nonsingular matrix \( P \) such that \( P A P^T = F_p \).

**Theorem 2.4.** Let \( A \) be an \( n \times n \) alternate matrix of rank \( k \) over \( \text{GF}(q) \). Then there is a nonsingular matrix \( P \) such that \( P A P^T = \begin{bmatrix} I_k & 0 \\ 0 & -I_k \end{bmatrix} \) (\( k = 2p \)).

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

\[
|\text{Sp}_n(q)| = (q^n - 1)q^{n-1}(q^{n-2} - 1)q^{n-3} \cdots (q^2 - 1)q.
\]

Let \( f \) be a nondegenerate, alternating bilinear form of rank \( 2p \) on \( V_n \), \( n = 2p \). A basis \( (x_1, \ldots, x_p, y_1, \ldots, y_p) \) 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 \( i, j = 1, 2, \ldots, p \). Chevalley [6] has proved the existence of a symplectic basis for any \( n \)-dimensional vector space \( V_n \) on which a nondegenerate, alternating bilinear form has been defined. The following theorem is a corollary to the proof of this result.
THE MATRIX EQUATION XAXT = C

203

Theorem 2.5. Let f be a nondegenerate, alternating bilinear form on $V_n \times V_n$, $n = 2p$. If $x_1, \ldots, x_p, y_1, \ldots, y_\gamma$, $\gamma < p$, are independent vectors in $V_n$ such that $f(x_i, x_j) = 0$ for all $i, j = 1, 2, \ldots, p$, $f(y_i, y_j) = 0$ for all $i, j = 1, 2, \ldots, \gamma$, and $f(x_i, y_j) = \delta_{ij}$ for $i = 1, 2, \ldots, p$ and $j = 1, 2, \ldots, \gamma$, then there exist vectors $y_{p+1}, \ldots, y_\gamma$ in $V_n$ such that $(x_1, \ldots, x_p, y_1, \ldots, y_\gamma)$ 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 $[s]_n$ denote the $q$-binomial coefficient defined by $[s]_1 = 1$; $[s]_k = 0$, $k > n$; $[s]_k = (q)_n/(q)_k(q)_k$, $0 < k \leq n$, where $(q)_k = (q - 1)(q^2 - 1) \cdots (q^j - 1)$, $j > 0$. 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

$$L(s, t, m, r, r + \gamma) = \left[ m \atop \gamma \right] q^{r(m-r)} \prod_{i=0}^{\gamma-1} (q^s - q^{r+i}).$$

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 $PAP^T = F_p, n = 2p$. By Lemma 2.1, for any $s \times s$ symmetric matrix $C$, $N(A, C, n, s) = N(F_p, C, n, s)$. Let $X$ be any $s \times n$ matrix and let $XF_pX^T = (b_{ij})$. A simple calculation shows that

$$b_{ii} = \sum_{k=1}^{p} x_{ik+p} x_{ik} + \sum_{k=p+1}^{2p} x_{ik-p} x_{ik}$$

$$= \sum_{k=1}^{p} x_{ik+p} x_{ik} + \sum_{i=1}^{p} x_{ik} x_{ik+p} = 0.$$

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

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, $N(A, C, n, s) = N(F_p, F_\gamma, n, s)$. Thus, it suffices to find $N(F_p, F_\gamma, n, s)$.

For any $s \times n$ matrix $X$ such that $XF_pX^T = F_p, s = 2\gamma$ and $n = 2p$, rank $X = 2\gamma \leq 2p$. For $P$ and $Q$ in $Sp_n(q)$, let
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 $\mathbb{S}_p(q)$ by $P \sim Q$ if and only if $P_1 = Q_1$ and $P_2 = Q_2$. Clearly, $\sim$ is an equivalence relation on $\mathbb{S}_p(q)$. For any $P$ in $\mathbb{S}_p(q)$, let $[P]$ denote the equivalence class containing $P$.

**Theorem 3.1.** Define the mapping $\phi$ from $\{[P] \mid P \in \mathbb{S}_p(q)\}$ into $\{X \mid XF_pX^T = E_p\}$ 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 $\phi$ is a one-to-one mapping onto $\{X \mid XF_pX^T = E_p\}$.

**Proof.** By definition of $\sim$, $\phi$ is well defined and one-to-one. Let $f$ be the bilinear form on $V_s \times V_\rho$ defined by $f(\xi, \eta) = \xi F_p \eta^T$ for all $\xi, \eta$ in $V_\rho$. Then rank $f = n - \dim V_\rho^* = \dim E_p = 2\rho = n$. Thus, $V_\rho^* = \{0\}$. Clearly, $f(\xi, \xi) = 0$ for all $\xi$ in $V_\rho$. Hence, $f$ is a nondegenerate, alternating bilinear form on $V_s \times V_\rho$. By Theorem 2.1, if $E$ is any subspace of $V_\rho$, then dim $E^* = n - \dim E$. For any $P$ in $\mathbb{S}_p(q)$, $P F_p P^T = E_p$. Let $P = [A_2]$, where each of $P_1$ and $P_2$ is $\rho \times n$. Then

$$
\begin{bmatrix}
P_1 & P_2
\end{bmatrix} F_p [P_1^T P_2^T] =
\begin{bmatrix}
P_1 F_p P_1^T & P_1 F_p P_2^T \\
P_2 F_p P_1^T & P_2 F_p P_2^T
\end{bmatrix} =
\begin{bmatrix}
0 & I_p \\
I_p & 0
\end{bmatrix}.
$$

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

$$
X F_p X^T =
\begin{bmatrix}
X_1 & X_2
\end{bmatrix} F_p \left[\begin{bmatrix}
X_1^T \\
X_2^T
\end{bmatrix}\right] =
\begin{bmatrix}
X_1 F_p X_1^T & X_1 F_p X_2^T \\
X_2 F_p X_1^T & X_2 F_p X_2^T
\end{bmatrix} =
\begin{bmatrix}
0 & I_p \\
I_p & 0
\end{bmatrix} = E_p.
$$

Hence, the range of $\phi$ is a subset of $\{X \mid XF_pX^T = E_p\}$. In order to show that $\phi$ is onto, let $X$ be an $s \times n$ matrix such that $XF_pX^T = E_p$. Suppose $X = \left[\frac{X_1}{X_2}\right]$, 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 $f(x_i, y_j) = f(y_i, y_j) = 0$ 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 $\text{RS}[X]$ 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 $V_\rho$ and no extension is necessary. Suppose $\rho - \gamma = \tau > 0$. If $(\text{RS}[X])^* \subseteq \text{RS}[X]$ then, for any $z$ in $(\text{RS}[X])^*$, $z = \sum_{i=1}^{\gamma} a_i x_i + \sum_{i=1}^{\gamma} b_i y_i$. Thus, for any $j = 1, 2, \ldots, \gamma$,

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

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

$$
\begin{bmatrix}
X \\
z_1 \\
\vdots \\
z_k
\end{bmatrix},
$$

for $j = 0, 1, \ldots, k$.

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

Consider any $P$ in $Sp_n(q)$. 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 $Sp_n(q)$, $Q$ 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 $RS[\gamma]$ to a symplectic basis $(x_1, \ldots, x_p, y_1, \ldots, y_p)$ for $V_\nu$.

**Theorem 3.2.** Let $f$ be a nondegenerate, alternating bilinear form defined on $V_n \times V_n, n = 2p$. Let $W$ be a $2\gamma$-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 $V_\nu$ is given by

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

**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 $\dim W^* = 2p - 2\gamma$, there are $q^{2p-2\gamma} - 1$ vectors in $W^* - W$. Thus, there
are \(q^{2p-2y} - 1\) choices for \(x_{y+1}\). Suppose \(x_{y+1}, \ldots, x_{y+k}, k < \rho - \gamma\), have been chosen so that \(x_{y+i}\) is in \((W \oplus \langle x_{y+1}, \ldots, x_{y+i-1} \rangle)^* - (W \oplus \langle x_{y+1}, \ldots, x_{y+i-1} \rangle), i = 2, \ldots, k\). If \(z\) is in \((W \oplus \langle x_{y+1}, \ldots, x_{y+k} \rangle)^* \cap (W \oplus \langle x_{y+1}, \ldots, x_{y+k} \rangle),\) then

\[
z = \sum_{i=1}^{y} a_i x_i + \sum_{i=1}^{y} b_i y_i + \sum_{i=1}^{k} c_i x_{y+i}.
\]

Again, \(a_j = b_j = 0\) for \(j = 1, 2, \ldots, y\). Since \(f\) is alternating, it follows that

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

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

By Theorem 3.1, \(N(F_p, F_n, n) = |Sp_n(q)|/|\langle P \rangle|\). Since, for any \(P\) in \(Sp_n(q), |\langle P \rangle| = K(\rho, \gamma)\), we have determined \(N(F_p, F_n, n)\).

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

\[
N(A, C, n, s) = |Sp_n(q)|/|\langle P \rangle|/K(\rho, \gamma),
\]

where \(|Sp_n(q)|\) 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 \(\mathbb{F}_q\), 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, \(n = 2p\), over \(\mathbb{F}_q\) 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, \(N(A, C, n, s, r) = N(G_r, G_s, n, s, r)\), where \(G_r = \langle F_r \rangle\). Let \(X = [x_{ij}]\) be any \(s \times n\) matrix such that \(X F_p X^T = G_r\), where \(X_1 = 2\gamma \times n\) and \(X_2 = (s - 2\gamma) \times n\). Then
THE MATRIX EQUATION $XAX^T = C$

(4.1) $\begin{bmatrix} X_1 \\ X_2 \end{bmatrix} F_p [X_1^T X_2^T] = \begin{bmatrix} X_1 F_p X_1^T & X_1 F_p X_2^T \\ X_2 F_p X_1^T & X_2 F_p X_2^T \end{bmatrix} = \begin{bmatrix} F_r \\ 0 \end{bmatrix}$.

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

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

(4.2) $R(2\gamma, n, s, 2\gamma + \tau) = \sum_{\tau} \binom{s - 2\gamma}{\tau} (q^{n-2\gamma-\tau} - q^\tau),$

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

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

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

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

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...
Let $A$ be an $n \times n$ nonsingular alternate matrix, $n = 2p$, over $GF(q)$ and let $C$ be an $s \times s$ alternate matrix of rank $2\gamma$. Then

$$N(A, C, n, s, 2\gamma + \tau) = N(F_p, F_\gamma, n, 2\gamma) \cdot R(2\gamma, n, s, 2\gamma + \tau),$$

$$0 \leq \tau \leq \min(s, n) - 2\gamma,$$

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

$$\left[ \begin{array}{cc} X_1 & X_2 \end{array} \right] \left[ \begin{array}{cc} F_p & 0 \\ 0 & 0 \end{array} \right] \left[ \begin{array}{c} X_1^T \\ X_2^T \end{array} \right] = X_1 F_p X_1^T = G_\gamma.$$ 

Further, rank $X = r$ implies rank $X_1 \geq r - (n - 2p)$. For any $\tau$,

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

the number $N(F_p, G_\gamma, 2p, s, 2\gamma + \tau)$ of $s \times 2p$ matrices $X_1$ of rank $2\gamma + \tau$ over $GF(q)$ such that $X_1 F_p X_1^T = G_\gamma$ is given in Theorem 4.2. Consider any such matrix $X_1$. By (4.3), any $s \times (n - 2p)$ matrix $X_2$ such that $X = [X_1 X_2]$ has rank $r$ yields $XG_pX^T = G_\gamma$. The number of such matrices $X_2$ is the number $L(s, 2p, n, 2\gamma + \tau, r)$, 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 $2p$ over $GF(q)$. If $C$ is an $s \times s$ nonalternate matrix over $GF(q)$, 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 $2\gamma$ over $GF(q)$ and $2\gamma \leq r \leq \min(s, n)$, then 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 given by

$$N(A, C, n, s, r) = \sum_{\tau=(s,p,\gamma)} d(s, p, \gamma) N(F_p, G_\gamma, 2p, s, 2\gamma + \tau) \cdot L(s, 2p, n, 2\gamma + \tau, r),$$

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


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

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

License or copyright restrictions may apply to redistribution; see http://www.ams.org/journal-terms-of-use