Can. J. Math., Vol. XXVI, No. 1, 1974, pp. 78–90

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

PHILIP G. BUCKHIESTER

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 [**6**] has determined the number $N(A, C, n, s)$ of solutions X over $GF(q)$, for p an odd prime, to the matrix equation

$$XAX^T = C, \tag{1.1}$$

where $n = m$. Furthermore, Hodges [**9**] has determined the number $N(A, C, n, s, r)$ of $s \times n$ matrices X of rank r over $GF(q)$, p an odd prime, which satisfy (1.1). Perkin [**10**] has enumerated the $s \times n$ matrices of given rank r over $GF(q)$, $q = 2^y$, such that $XX^T = 0$. Finally, the author [**3**] has determined the number of solutions to (1.1) in case $C = 0$, where $q = 2^y$.

An $n \times n$ symmetric matrix over $GF(2^y)$ is said to be an *alternate matrix* if A has 0 diagonal. Otherwise, A is said to be *nonalternate*. The author [**4**; **5**] has determined the number $N(A, C, n, s, r)$ of $s \times n$ matrices X of rank r over $GF(q)$, $q = 2^y$, which satisfy (1.1), in case A is an alternate matrix over $GF(q)$ and in case both A and C are symmetric, nonalternate matrices over $GF(q)$.

The purpose of this paper is to determine the number $N(A, C, n, s, r)$, in case A is a symmetric, nonalternate matrix over $GF(2^y)$ and C is an alternate matrix over $GF(2^y)$. In determining this number, Albert's canonical forms for symmetric matrices over fields of characteristic two are used [**1**]. These forms and other necessary preliminaries appear in Section 2. In Section 3, the number $N(A, C, n, s)$ is found, in case both A and C are nonsingular. Finally, in Section 4, the number $N(A, C, n, s, r)$, $0 \leqq r \leqq \min(s, n)$, is determined.

The difference equations obtained in Section 4 were solved by using methods due to Carlitz [**7**].

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, for any matrix M over $GF(q)$, $\mathscr{R}\mathscr{S}[M]$ will denote the row space of M.

For matrices $X_1, X_2, \ldots, X_k$, where X_i is $m_i \times n$, col $[X_1, \ X_2, \ldots, X_k]$

Received August 2, 1972 and in revised form, February 16, 1973.

https://doi.org/10.4153/CJM-1974-008-2 Published online by Cambridge University Press

will denote the $(m_1 + m_2 + \ldots + m_k) \times n$ matrix

$$\begin{bmatrix} X_1 \\ X_2 \\ \cdot \\ \cdot \\ \cdot \\ X_k \end{bmatrix}.$$

2. Notation and preliminaries. Let f be a symmetric bilinear form defined on $V_n \times V_n$. For any subspace E of V_n, define

$$E^* = \{x \in V_n | f(x, y) = 0 \text{ for all } y \text{ in } E\}.$$

Clearly, E^* is a subspace of V_n. If $V_n^* = \{0\}$, then f is said to be *nondegenerate*. A vector x in V_n such that $f(x, x) = 0$ is said to be an *isotropic vector*. If every x in V_n is isotropic, then f is said to be an *alternating bilinear form*. Otherwise, f is called *nonalternating*.

The following theorem, which appears in [**8**], will be needed in Sections 3 and 4.

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 nondegenerate, then $\dim E + \dim E^* = n$, for any subspace E of V_n.

Let I_k denote the $k \times k$ identity matrix over $GF(q)$. Albert [**1**] has proved the following theorems concerning symmetric matrices over $GF(q)$.

THEOREM 2.2. *Let C be an $s \times s$ alternate matrix over $GF(q)$. If C is nonsingular, then there is a nonsingular matrix P such that*

$$PCP^T = \begin{bmatrix} 0 & I_\gamma \\ I_\gamma & 0 \end{bmatrix}, \quad (s = 2\gamma).$$

If C has rank $k < s$, then there is a nonsingular matrix Q such that

$$QCQ^T = \begin{bmatrix} 0 & I_\gamma & 0 \\ I_\gamma & 0 & 0 \\ 0 & 0 & 0 \end{bmatrix}, \quad (k = 2\gamma).$$

THEOREM 2.3. *Let A be an $n \times n$ symmetric, nonalternate matrix over $GF(q)$. If A is nonsingular, then there is a nonsingular matrix P such that $PAP^T = I_n$. If A has rank $k < n$, then there is a nonsingular matrix Q such that*

$$QAQ^T = \begin{bmatrix} I_k & 0 \\ 0 & 0 \end{bmatrix}.$$

The following lemma, which appears in [**4**], will be needed in Sections 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 $N(A, C, n, s) = N(B, D, n, s)$. Furthermore, $N(A, C, n, s, r) = N(B, D, n, s, r)$, $0 \leqq r \leqq \min(s, n)$.*

For integers n and k, let $\begin{bmatrix} n \\ k \end{bmatrix}$ denote the q-binomial coefficient defined by

$$\begin{bmatrix} n \\ 0 \end{bmatrix} = 1; \begin{bmatrix} n \\ k \end{bmatrix} = 0, k > n; \begin{bmatrix} n \\ n \end{bmatrix} = 1; \begin{bmatrix} n \\ k \end{bmatrix} = \frac{(q)_n}{(q)_k(q)_{n-k}}, \quad 0 < k < n,$$

where $(q)_j = (q-1)\ldots(q^j - 1)$, $j > 0$. Brawley and Carlitz [**2**] have proved the following lemma.

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*

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

Let f be the bilinear form defined on $V_n \times V_n$ by $f(\xi, \eta) = \xi\eta^T$, for all ξ, η in V_n. It is immediate that f is a nondegenerate, nonalternating bilinear form. Let W denote the set of all isotropic vectors in V_n. Then W is a subspace of V_n and, further, $x = (x_1, \ldots, x_n)$ is in W if and only if

$$f(x, x) = xx^T = \sum_{i=1}^{n} x_i^2 = \left(\sum_{i=1}^{n} x_i\right)^2 = 0.$$

Thus, W consists of all vectors x such that $\sum_{i=1}^{n} x_i = 0$. Consequently, W is an $(n-1)$-dimensional subspace of V_n. Let u denote the vector $(1, 1, \ldots, 1)$ in V_n. Perkins [**10**] has proved the following theorem.

THEOREM 2.4. *Let X be an $s \times n$ matrix over $GF(q)$. Then $(\mathscr{R}\mathscr{S}[X])^* \subseteq W$ if and only if u is in $\mathscr{R}\mathscr{S}[X]$.*

Let $M(I_n, 0, n, s, s)$ denote the number of $s \times n$ matrices X of rank s over $GF(q)$ such that $XX^T = 0$ and u is not in $\mathscr{R}\mathscr{S}[X]$. In determining the number $N(I_n, 0, n, s, s)$, Perkins [**10**] has determined $M(I_n, 0, n, s, s)$.

THEOREM 2.5. *The number of $s \times n$ matrices X of rank s over $GF(q)$ such that $XX^T = 0$ and such that u is not in $\mathscr{R}\mathscr{S}[X]$ is given by*

$$M(I_n, 0, n, s, s) = \begin{cases} \prod_{i=1}^{s} (q^{n-i} - q^{i-1}), & (n \text{ odd}) \\ \prod_{i=1}^{s} (q^{n-i} - q^{i}), & (n \text{ even}) \end{cases}$$

3. Determination of $N(A, C, n, s)$, A and C nonsingular. Let A be an $n \times n$ symmetric, nonalternate matrix of full rank over $GF(q)$ and let C be an

$s \times s$ alternate matrix of full rank over $GF(q)$. By Theorems 2.2 and 2.3, there exist nonsingular matrices P and Q such that $PAP^T = I_n$ and $QCQ^T = F_\gamma$, $s = 2\gamma$, where F_γ denotes the $2\gamma \times 2\gamma$ matrix

$$\begin{bmatrix} 0 & I_\gamma \\ I_\gamma & 0 \end{bmatrix}$$

over $GF(q)$. By Lemma 2.1, $N(A, C, n, s) = N(I_n, F_\gamma, n, 2\gamma)$, the number of $2\gamma \times n$ matrices X such that $XX^T = F_\gamma$. Thus, it suffices to find $N(I_n, F_\gamma, n, 2\gamma)$. Let f be the nonalternate, nondegenerate bilinear form on $V_n \times V_n$ defined by $f(\xi, \eta) = \xi I_n \eta^T = \xi\eta^T$, for each ξ, η in V_n. Let W be the $(n-1)$-dimensional subspace of V_n consisting of all isotropic vectors in V_n. Let $Z = \text{col}\,[X, Y]$ be an $s \times n$ matrix over $GF(q)$ such that $ZZ^T = F_\gamma$, $s = 2\gamma$, where each of X and Y is $\gamma \times n$. Then, rank $Z = 2\gamma$ and, therefore, rank $X = \gamma$. Furthermore

$$\begin{bmatrix} X \\ \\ Y \end{bmatrix} [X^T Y^T] = \begin{bmatrix} XX^T & XY^T \\ \\ YX^T & YY^T \end{bmatrix} = \begin{bmatrix} 0 & I_\gamma \\ \\ I_\gamma & 0 \end{bmatrix}. \tag{3.1}$$

Let $X = [x_1, \ldots, x_\gamma]^T$ and $Y = [y_1, \ldots, y_\gamma]^T$. From (3.1), it follows that $f(x_i, x_j) = f(y_i, y_j) = 0$ and $f(x_i, y_j) = \delta_{ij}$, for $i, j = 1, 2, \ldots, \gamma$. Thus $\mathscr{R}\mathscr{S}[X] \subseteq W$. If n is odd, then $f(u, u) = uu^T = 1$. Then u is not in W and, therefore, not in $\mathscr{R}\mathscr{S}[X]$. If n is even, then $f(u, u) = 0$, and u is an isotropic vector. However, u is not in $\mathscr{R}\mathscr{S}[X]$, as the following theorem shows.

THEOREM 3.1. *Suppose $Z = \text{col}\,[X, Y]$ is a $2\gamma \times n$ matrix over $GF(q)$ such that $ZZ^T = F_\gamma$, where each of X and Y is $\gamma \times n$. Then $u = (1, 1, \ldots, 1)$ is not in $\mathscr{R}\mathscr{S}[X]$.*

Proof. The proof of the theorem is given above in case n is odd. Suppose n is even and u is in $\mathscr{R}\mathscr{S}[X]$. Since rank $X = \gamma$, u may be represented uniquely as a linear combination of precisely k rows of X, for some k, $1 \leqq k \leqq \gamma$, say $u = \lambda_1 x_{i_1} + \ldots + \lambda_k x_{i_k}$, $\lambda_j \neq 0$, for each $j = 1, 2, \ldots, k$. Let

$$S = \langle x_1, \ldots, x_{i_1 - 1}, x_{i_1 + 1} \ldots, x_\gamma \rangle.$$

Since $f(x_{i_1}, y_{i_1}) = 1$, $f(x_j, y_{i_1}) = 0$, for $j \neq i_1$, and $f(y_j, y_{i_1}) = 0$, for $j = 1, 2, \ldots, \gamma$, it follows that y_{i_1} must be in $W \cap (S^* - (\mathscr{R}\mathscr{S}[X])^*) = (W \cap S^*) - (\mathscr{R}\mathscr{S}[X])^*$. Since u is in $\mathscr{R}\mathscr{S}[X]$, Theorem 2.4 implies that $(\mathscr{R}\mathscr{S}[X])^* \subseteq W$. Since $S \subseteq \mathscr{R}\mathscr{S}[X]$, $(\mathscr{R}\mathscr{S}[X])^* \subseteq S^*$. Thus $(\mathscr{R}\mathscr{S}[X])^* \subseteq W \cap S^*$. By Theorem 2.1, dim $(\mathscr{R}\mathscr{S}[X])^* = n - \gamma$. Further, since

$$u = \sum_{j=1}^{k} \lambda_j x_{i_j},\ \lambda_j \neq 0, \text{ for each } j = 1, 2, \ldots \gamma,$$

u is not in S. By Theorem 2.4, S^* is not a subspace of W. Therefore, dim $(W + S^*) = n$. Furthermore, by Theorem 2.1, dim $S^* = n - \dim S = n - (\gamma - 1)$. Hence,

$$\dim (W \cap S^*) = \dim W + \dim S^* - \dim (W + S^*) =$$
$$(n - 1) + [n - (\gamma - 1)] - n = n - \gamma = \dim (\mathscr{R}\mathscr{S}[X])^*.$$

https://doi.org/10.4153/CJM-1974-008-2 Published online by Cambridge University Press

Thus, $W \cap S^* = (\mathscr{R}\mathscr{S}[X])^*$ and, therefore, there exists no y_{i_1} in $(W \cap S^*) - (\mathscr{R}\mathscr{S}[X])^*$. It follows that u is not in $\mathscr{R}\mathscr{S}[X]$.

By (3.1) and Theorem 3.1, if $Z = \text{col}\,[X, Y]$ is such that $ZZ^T = F_\gamma$, then the $\gamma \times n$ matrix X of rank γ is such that $XX^T = 0$ and such that u is not in $\mathscr{R}\mathscr{S}[X]$. The number of such matrices X is the number $M(I_n, 0, n, \gamma, \gamma)$, as given in Theorem 2.5. Given a $\gamma \times n$ matrix X of rank γ over $GF(q)$ such that $XX^T = 0$ and u is not in $\mathscr{R}\mathscr{S}[X]$, we seek the number of $\gamma \times n$ matrices Y over $GF(q)$ such that $XY^T = I_\gamma$ and $YY^T = 0$. In the argument given below it is shown that this number depends only on γ and n. Consequently, if we denote this number by $K(\gamma, n)$, it follows that

$$N(I_n, F_\gamma, n, 2\gamma) = K(\gamma, n)M(I_n, 0, n, \gamma, \gamma). \tag{3.2}$$

Thus, it suffices to determine the number $K(\gamma, n)$. Consider any $2\gamma \times n$ matrix $Z = \text{col}\,[X, Y]$ such that $ZZ^T = F_\gamma$. By (3.1), $\mathscr{R}\mathscr{S}[Z] \subseteq W$. Hence, as before, if n is odd u is not in W and, therefore, not in $\mathscr{R}\mathscr{S}[Z]$. The following theorem shows that this is also the case if n is even.

THEOREM 3.2. *If Z is a $2\gamma \times n$ matrix over $GF(q)$ such that $ZZ^T = F_\gamma$, where each of X and Y is $\gamma \times n$, then $u = (1, 1, \ldots, 1)$ is not in $\mathscr{R}\mathscr{S}[Z]$.*

Proof. The proof of the theorem is given above in case n is odd. Suppose n is even and let $Z = \text{col}\,[X, Y]$, where each of X and Y is $\gamma \times n$. By Theorem 3.1, u is not in $\mathscr{R}\mathscr{S}[X]$. Suppose u is in $\mathscr{R}\mathscr{S}$ col $[X, y_1]$. Since u is not in $\mathscr{R}\mathscr{S}[X]$, y_1 is in $\mathscr{R}\mathscr{S}$ col $[X, u]$. If $v = (v_1, \ldots, v_n)$ is any isotropic vector in V_n, then

$$0 = f(v, v) = vv^T = \sum_{i=1}^{n} v_i^2 = \left(\sum_{i=1}^{n} v_i\right)^2,$$

which implies $f(u, v) = uv^T = \sum_{i=1}^{n} v_i = 0$. Thus, if v is an isotropic vector in V_n, then u is in $\langle v \rangle^*$. It follows that $\mathscr{R}\mathscr{S}$ col $[X, u] \subseteq \langle x_1 \rangle^*$. Thus y_1 is in $\langle x_1 \rangle^*$ and $f(x_1, y_1) = 0$. Since $f(x_1, y_1) = 1$, it follows that u is not in $\mathscr{R}\mathscr{S}$ col $[X, y_1]$. Suppose u is not in $\mathscr{R}\mathscr{S}$ col $[X, y_1, \ldots, y_k]$, where $1 \leqq k < \gamma$ and u is in $\mathscr{R}\mathscr{S}$ col $[X, y_1, \ldots, y_{k+1}]$. Then y_{k+1} is in

$$\mathscr{R}\mathscr{S}\begin{bmatrix} X \\ y_1 \\ \cdot \\ \cdot \\ \cdot \\ y_k \\ u \end{bmatrix} \subseteq \langle x_{k+1} \rangle^*,$$

an impossibility since $f(x_{k+1}, y_{k+1}) = 1$. Hence, u is not in

$$\mathscr{R}\mathscr{S} \text{ col } [X, y_1, \ldots, y_{k+1}]$$

and the proof is complete.

We proceed to determine the number $K(\gamma, n)$. Let $X = [x_1, \ldots, x_\gamma]^T$ be a $\gamma \times n$ matrix of rank γ over $GF(q)$ such that $XX^T = 0$ and u is not in $\mathscr{R}\mathscr{S}[X]$. In order to choose a $\gamma \times n$ matrix $Y = [y_1, \ldots, y_\gamma]^T$ such that $XY^T = I_\gamma$ and $YY^T = 0$, y_1 must be chosen from

$$W \cap \left(\left(\mathscr{R}\mathscr{S}\begin{bmatrix} x_2 \\ \cdot \\ \cdot \\ \cdot \\ x_\gamma \end{bmatrix}\right)^* - (\mathscr{R}\mathscr{S}[X])^*\right)$$

$$= \left(W \cap \left(\mathscr{R}\mathscr{S}\begin{bmatrix} x_2 \\ \cdot \\ \cdot \\ \cdot \\ x_\gamma \end{bmatrix}\right)^*\right) - (\mathscr{R}\mathscr{S}[X])^*.$$

Let $T = W \cap (\mathscr{R}\mathscr{S}\operatorname{col}[x_2, \ldots, x_\gamma])^*$ and let $S = T \cap (\mathscr{R}\mathscr{S}[X])^* = W \cap (\mathscr{R}\mathscr{S}[X])^*$. Then y_1 must be chosen in $T - S$. Since u is not in $\mathscr{R}\mathscr{S}[X]$, Theorem 2.4 implies that neither $(\mathscr{R}\mathscr{S}[X])^*$ nor $(\mathscr{R}\mathscr{S}\operatorname{col}[x_2, \ldots, x_\gamma])^*$ is a subspace of W. Applying Theorem 2.1, we obtain $\dim S = \dim W + \dim (\mathscr{R}\mathscr{S}[X])^* - \dim (W + (\mathscr{R}\mathscr{S}[X])^*) = (n-1) + [n-\gamma] - n = n - \gamma - 1$ and $\dim T = (n-1) + [n-(\gamma-1)] - n = n - \gamma$. Thus, $\dim T/S = 1$. Define the mapping $\bar{f}$ from T/S into $GF(q)$ by $\bar{f}(z + S) = f(z, x_1)$ for each coset $z + S$ in T/S. Let z_0 be such that $T/S = \langle z_0 + S\rangle$. Then z_0 is in $T - S$ and, therefore, $\bar{f}(z_0 + S) = f(z_0, x_1) \neq 0$. It follows that $\bar{f}$ is a one-to-one mapping from T/S onto $GF(q)$. Hence, there exists precisely one coset $z_1 + S$ in T/S such that $\bar{f}(z_1 + S) = 1$. For any v in S, $f(v, x_1) = 0$ and, thus, $f(z_1 + v, x_1) = f(z_1, x_1) + f(v, x_1) = \bar{f}(z_1 + S) = 1$. Since y_1 must be such that $f(x_1, y_1) = 1$, the number of choices for y_1 is equal to $|z_1 + S| = |S| = q^{n-\gamma-1}$. Suppose $y_1, \ldots, y_k$, $k < \gamma$, have been chosen such that the following properties hold:

(i) $y_1, \ldots, y_k$ are independent vectors in V_n,

(ii) u is not in $T_k = \langle x_1, \ldots, x_\gamma, y_1, \ldots, y_k\rangle$,

(iii) $f(x_i, y_j) = \delta_{ij}$ and $f(y_l, y_j) = 0$, for $i = 1, 2, \ldots, \gamma$ and $j, l = 1, 2, \ldots, k$.

Then y_{k+1} must be chosen from $W \cap (S_k^* - (T_k^* \cup T_k)) = (W \cap S_k^*) - (T_k^* \cup T_k)$, where $S_k = \langle x_1, \ldots, x_k, x_{k+2}, \ldots, x_\gamma, y_1, \ldots, y_k\rangle$. However,

$$\begin{aligned}(W \cap S_k^*) \cap (T_k^* \cup T_k) &= (W \cap S_k^* \cap T_k^*) \cup (W \cap S_k^* \cap T_k) \\ &= (W \cap T_k^*) \cup (W \cap S_k^* \cap T_k).\end{aligned}$$

If z is in $S_k^* \cap T_k$, then

$$z = \sum_{i=1}^{\gamma} a_i x_i + \sum_{i=1}^{k} b_i y_i.$$

https://doi.org/10.4153/CJM-1974-008-2 Published online by Cambridge University Press

However, $0 = f(z, y_j) = a_j$ and $0 = f(z, x_j) = b_j$, for $j = 1, 2, \ldots, k$. Thus $z = \sum_{i=k+1}^{\gamma} a_i x_i$. Since x_i is in $S_k^* \cap T_k$ for $i = k + 1, \ldots, \gamma$, it follows that $S_k^* \cap T_k = \langle x_{k+1}, \ldots, x_\gamma \rangle$. Hence, $W \cap S_k^* \cap T_k = \langle x_{k+1}, \ldots, x_\gamma \rangle \subseteq W \cap T_k^*$ and, therefore, $(W \cap S_k^*) - (T_k^* \cup T_k) = (W \cap S_k^*) - (W \cap T_k^*)$. Since u is not in T_k and, therefore, not in S_k, it follows from Theorems 2.4 and 2.1 that

$$\dim (W \cap S_k^*) = (n - 1) + [n - (\gamma - 1 + k)] - n = n - \gamma - k$$

and

$$\dim (W \cap T_k^*) = (n - 1) + [n - (\gamma + k)] - n = n - \gamma - k - 1.$$

Let $J = W \cap S_k^*$ and $M = W \cap T_k^*$. Then $\dim J/M = 1$. As before, the mapping $\bar{f}$ from J/M into $GF(q)$ defined by $\bar{f}(z + M) = f(z, x_{k+1})$ is a one-to-mapping onto $GF(q)$. Since y_{k+1} must be such that $f(x_{k+1}, y_{k+1}) = 1$, it follows that the number of choices for y_{k+1} is equal to $|M| = q^{n-\gamma-k-1}$. As in the proof of Theorem 3.2, it can be shown that for any such y_{k+1}, u is not an element of $T_{k+1} = \langle x_1, \ldots, x_\gamma, y_1, \ldots, y_{k+1} \rangle$. Thus, the inductive argument is complete and it follows that

$$K(\gamma, n) = \prod_{i=1}^{\gamma} q^{n-\gamma-i}. \tag{3.3}$$

Together, (3.2) and (3.3) yield the number $N(I_n, F_\gamma, n, 2\gamma) = N(A, C, n, 2\gamma)$.

THEOREM 3.3. *Let A be an $n \times n$ symmetric, nonalternate matrix of full rank over $GF(q)$ and let C be an $s \times s$ alternate matrix of full rank over $GF(q)$, $s = 2\gamma$. Then the number of $s \times n$ matrices X over $GF(q)$ such that $XAX^T = C$ is given by*

$$N(A, C, n, s) = \prod_{i=1}^{\gamma} (q^{n-\gamma-i}) M(I_n, 0, n, \gamma, \gamma),$$

where $M(I_n, 0, n, \gamma, \gamma)$ is given in Theorem 2.5.

4. Determination of $N(A, C, n, s, r)$. Let A be an $n \times n$ symmetric, nonalternate matrix of full rank over $GF(q)$. Let C be an $s \times s$ alternate matrix of rank $2\gamma \leqq s$ over $GF(q)$. By Theorem 2.2, Theorem 2.3, and Lemma 2.1, $N(A, C, n, s, r) = N(I_n, G_\gamma, n, s, r)$, $0 \leqq r \leqq \min (s, n)$, where G_γ denotes the $s \times s$ matrix

$$\begin{bmatrix} 0 & I_\gamma & 0 \\ I_\gamma & 0 & 0 \\ 0 & 0 & 0 \end{bmatrix}$$

over $GF(q)$. Thus, it suffices to determine the number $N(I_n, G_\gamma, n, s, r)$ of $s \times n$ matrices M of rank r such that $MM^T = G_\gamma$. Let $M = \text{col}\ [X_1, Z]$ be any such matrix, where X_1 is $2\gamma \times n$ and Z is $(s - 2\gamma) \times n$. Then

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

https://doi.org/10.4153/CJM-1974-008-2 Published online by Cambridge University Press

Thus, the $2\gamma \times n$ matrix X_1 must be such that $X_1X_1^T = F_\gamma$. The number of such matrices X_1 is the number $N(I_n, F_\gamma, n, 2\gamma)$, given in Theorem 3.3. Further, since rank $X_1 = 2\gamma$, rank $M = 2\gamma + \tau$ for some τ, $0 \leqq \tau \leqq \min(s, n) - 2\gamma$. Given a $2\gamma \times n$ matrix X_1 such that $X_1X_1^T = F_\gamma$, the number of $s \times n$ matrices $M = \text{col}\,[X_1, Z]$ of rank $2\gamma + \delta$ such that $MM^T = G_\gamma$ depends only on γ, n, s, and δ. Thus, if we denote this number by $\Phi(2\gamma, n, s, \delta)$, it follows that

$$(4.2)\qquad N(I_n, G_\gamma, n, s, 2\gamma + \tau) = N(I_n, F_\gamma, n, 2\gamma) \cdot \Phi(2\gamma, n, s, \tau).$$

Suppose n is odd and let $X_1 = \text{col}\,[X, Y]$ be a $2\gamma \times n$ matrix over $GF(q)$ such that $X_1X_1^T = F_\gamma$, where each of $X = [x_1, \ldots, x_\gamma]^T$ and $Y = [y_1, \ldots.., y_\gamma]^T$ is $\gamma \times n$. Then, if f is the nonalternate, nondegenerate bilinear form defined by $f(\xi, \eta) = \xi\eta^T$, for all ξ, η in V_n, we have $f(x_i, x_j) = f(y_i, y_j) = 0$ and $f(x_i, y_j) = \delta_{ij}$, for $i, j = 1, 2, \ldots, \gamma$. Suppose $M = \text{col}\,[X_1, Z]$ is an $s \times n$ matrix of rank $2\gamma + \tau$ over $GF(q)$ such that $MM^T = G_\gamma$. By (4.1), $\mathscr{R}\mathscr{S}[M] \subseteq W$. Since n is odd, u is not an isotropic vector and, therefore, is not in $\mathscr{R}\mathscr{S}[M]$. Furthermore, if $Z = \text{col}\,[Z_1, z_{s-2\gamma}]$, where $Z_1 = [z_1, \ldots, z_{s-1-2\gamma}]^T$ is $(s - 1 - 2\gamma) \times n$, then the $(s-1) \times n$ matrix $D = \text{col}\,[X_1, Z_1]$ has rank $2\gamma + \tau$ or $2\gamma + \tau - 1$ and is such that

$$DD^T = \begin{bmatrix} 0 & I_\gamma & 0 \\ I_\gamma & 0 & 0 \\ 0 & 0 & 0 \end{bmatrix}.$$

Since $MM^T = G_\gamma$, it is clear that $z_{s-2\gamma}$ must be in $W \cap (\mathscr{R}\mathscr{S}[D])^*$. If rank $D = 2\gamma + \tau$, then $z_{s-2\gamma}$ is in $W \cap (\mathscr{R}\mathscr{S}[D])^* \cap \mathscr{R}\mathscr{S}[D]$. If v is in this subspace, then

$$v = \sum_{i=1}^{\gamma} a_i x_i + \sum_{i=1}^{\gamma} b_i y_i + \sum_{i=1}^{s-1-2\gamma} c_i z_i,$$

for some a_i, b_i, c_i in $GF(q)$. However, $0 = f(v, x_j) = b_j$ and $0 = f(v, y_j) = a_j$, for $j = 1, 2, \ldots, \gamma$. Hence,

$$v = \sum_{i=1}^{s-1-2\gamma} c_i z_i.$$

Clearly, $\mathscr{R}\mathscr{S}[Z_1] \subseteq W \cap (\mathscr{R}\mathscr{S}[D])^* \cap \mathscr{R}\mathscr{S}[D]$. Thus, in order that rank $D = 2\gamma + \tau$, it is necessary and sufficient that $z_{s-2\gamma}$ be in $\mathscr{R}\mathscr{S}[Z_1]$. Since $\dim \mathscr{R}\mathscr{S}\ \text{col}\,[X_1, Z_1] = 2\gamma + \tau$, it is clear that $\dim \mathscr{R}\mathscr{S}[Z_1] \geqq \tau$. If $\dim \mathscr{R}\mathscr{S}[Z_1] > \tau$, then for some i, $1 \leqq i \leqq s - 1 - 2\gamma$, z_i is in

$$\mathscr{R}\mathscr{S}\ \text{col}\,[X_1, z_1, \ldots, z_{i-1}] - \langle z_1, \ldots, z_{i-1}\rangle.$$

But z_i is in $(\mathscr{R}\mathscr{S}\ \text{col}\,[X_1, z_1, \ldots, z_{i-1}])^*$, whose intersection with

$$\mathscr{R}\mathscr{S}\ \text{col}\,[X_1, z_1, \ldots, z_{i-1}] \quad \text{is} \quad \langle z_1, \ldots, z_{i-1}\rangle.$$

Thus $\dim \mathscr{R}\mathscr{S}[Z_1] = \tau$ and the number of choices for $z_{s-2\gamma}$ is q^τ. If rank $D = 2\gamma + \tau - 1$, then $z_{s-2\gamma}$ must be in $W \cap (\mathscr{R}\mathscr{S}[D])^* - \mathscr{R}\mathscr{S}[D]$. Since u is not in $\mathscr{R}\mathscr{S}[D]$, it follows from Theorem 2.4 that $(\mathscr{R}\mathscr{S}[D])^*$ is not a subspace of W. Hence,

$$\dim (W \cap (\mathscr{R}\mathscr{S}[D])^*) = (n-1) + [n - (2\gamma + \tau - 1)] - n = n - 2\gamma - \tau.$$

Furthermore, $W \cap (\mathscr{R}\mathscr{S}[D])^* \cap \mathscr{R}\mathscr{S}[D] = \mathscr{R}\mathscr{S}[Z_1]$, which, by an argument similar to the one used above, can be shown to be of dimension $\tau - 1$. Thus, the number of choices for $z_{s-2\gamma}$ is $q^{n-2\gamma-\tau} - q^{\tau-1}$. Hence, we obtain the difference equation

$$(4.3) \quad \Phi(2\gamma, n, s, \tau) = q^\tau \Phi(2\gamma, n, s-1, \tau) + (q^{n-2\gamma-\tau} - q^{\tau-1}) \times \Phi(2\gamma, n, s-1, \tau-1), \quad (n \text{ odd}),$$

with initial condition $\Phi(2\gamma, n, s, 0) = 1$, for $s \geqq 2\gamma$, and $\Phi(2\gamma, n, 2\gamma, \tau) = 0$, for $\tau \neq 0$. It is easily seen that the solution to the recurrence in (4.3) is given by

$$(4.4) \qquad \Phi(2\gamma, n, s, \tau) = \begin{bmatrix} s - 2\gamma \\ \tau \end{bmatrix} \prod_{j=0}^{\tau-1} (q^{n-2\gamma-j-1} - q^j), \quad (n \text{ odd}),$$

where $\begin{bmatrix} s - 2\gamma \\ \tau \end{bmatrix}$ is the q-binomial coefficient as defined in Section 2.

Suppose n is even and suppose $X_1 = \operatorname{col}[X, Y]$ is a $2\gamma \times n$ matrix over $GF(q)$ such that $X_1X_1^T = F_\gamma$. Given the matrix X_1, let $J_1(2\gamma, n, s, \delta)$ denote the number of $s \times n$ matrices $M = \operatorname{col}[X_1, Z]$ of rank $2\gamma + \delta$ over $GF(q)$ such that $MM^T = G_\gamma$ and such that u is in $\mathscr{R}\mathscr{S}[M]$, and let $J_2(2\gamma, n, s, \delta)$ denote the number of $s \times n$ matrices $M = \operatorname{col}[X_1, Z]$ of rank $2\gamma + \delta$ over $GF(q)$ such that $MM^T = G_\gamma$ and such that u is not in $\mathscr{R}\mathscr{S}[M]$. The use of this notation is justified below as we show that the numbers J_1 and J_2 depend only on γ, n, s, and δ. Furthermore,

$$(4.5) \quad \Phi(2\gamma, n, s, \tau) = J_1(2\gamma, n, s, \tau) + J_2(2\gamma, n, s, \tau), \quad (n \text{ even}).$$

Let $M = \operatorname{col}[X_1, Z]$ be an $s \times n$ matrix of rank $2\gamma + \tau$ over $GF(q)$ such that $MM^T = G_\gamma$. Since n is even, u is isotropic and, therefore, may or may not be in $\mathscr{R}\mathscr{S}[M]$. Let $Z = \operatorname{col}[Z_1, z_{s-2\gamma}]$, where $Z_1 = [z_1, \ldots, z_{s-1-2\gamma}]^T$ is $(s-1-2\gamma) \times n$. Suppose u is not in $\mathscr{R}\mathscr{S}[M]$. Then the $(s-1) \times n$ matrix $D = \operatorname{col}[X_1, Z_1]$ has rank $2\gamma + \tau$ or $2\gamma + \tau - 1$ and is such that u is not in $\mathscr{R}\mathscr{S}[D]$. In order to determine a difference equation in $J_2(2\gamma, n, s, \tau)$, we seek expressions $Q(2\gamma, n, s, \tau)$ and $R(2\gamma, n, s, \tau)$ such that

$$(4.6) \quad J_2(2\gamma, n, s, \tau) = Q(2\gamma, n, s, \tau) J_2(2\gamma, n, s-1, \tau) + R(2\gamma, n, s, \tau) \times J_2(2\gamma, n, s-1, \tau-1), \quad (n \text{ even}).$$

If rank $D = 2\gamma + \tau$, then $z_{s-2\gamma}$ must be in $W \cap (\mathscr{R}\mathscr{S}[D])^* \cap \mathscr{R}\mathscr{S}[D] = \mathscr{R}\mathscr{S}[Z_1]$, a subspace of dimension τ. Further, since u is not in $\mathscr{R}\mathscr{S}[D]$, any $z_{s-2\gamma}$ in $\mathscr{R}\mathscr{S}[Z_1]$ will be such that u is not in $\mathscr{R}\mathscr{S}[M]$. Hence, $Q(2\gamma, n, s, \tau) = q^\tau$. If rank $D = 2\gamma + \tau - 1$, then $z_{s-2\gamma}$ must be in $W \cap (\mathscr{R}\mathscr{S}[D])^* - \mathscr{R}\mathscr{S}[D]$. Since u is not in $\mathscr{R}\mathscr{S}[D]$, u is not in $\mathscr{R}\mathscr{S}[M]$ if and only if $z_{s-2\gamma}$ is not in $\mathscr{R}\mathscr{S} \operatorname{col}[D, u] - \mathscr{R}\mathscr{S}[D]$. Hence, it is necessary and sufficient that $z_{s-2\gamma}$ be

https://doi.org/10.4153/CJM-1974-008-2 Published online by Cambridge University Press

in $T - (S \cap T)$, where $T = (W \cap (\mathscr{R}\mathscr{S}[D])^*) - \mathscr{R}\mathscr{S}[D]$ and $S = \mathscr{R}\mathscr{S}\,\mathrm{col}\,[D, u] - \mathscr{R}\mathscr{S}[D]$. Since u is not in $\mathscr{R}\mathscr{S}[D]$,

$$\dim (W \cap (\mathscr{R}\mathscr{S}[D])^*) = (n-1) + [n - (2\gamma + \tau - 1)] - n = n - 2\gamma - \tau.$$

Further, $W \cap (\mathscr{R}\mathscr{S}[D])^* \cap \mathscr{R}\mathscr{S}[D] = \mathscr{R}\mathscr{S}[Z_1]$, a subspace of dimension $\tau - 1$. Thus, $|T| = q^{n-2\gamma-\tau} - q^{\tau-1}$. Next,

$$T \cap S = (W \cap (\mathscr{R}\mathscr{S}[D])^* \cap \mathscr{R}\mathscr{S}\,\mathrm{col}\,[D, u]) - \mathscr{R}\mathscr{S}[D].$$

Suppose v is in $W \cap (\mathscr{R}\mathscr{S}[D])^* \cap \mathscr{R}\mathscr{S}\,\mathrm{col}\,[D, u]$. Then

$$v = \sum_{i=1}^{\gamma} a_i x_i + \sum_{i=1}^{\gamma} b_i y_i + \sum_{i=1}^{s-1-2\gamma} c_i z_i + du,$$

for scalars a_i, b_i, c_i, and d in $GF(q)$. Since x_j and y_j are isotropic, for $j = 1, 2, \ldots, \gamma, f(u, x_j) = f(u, y_j) = 0, j = 1, 2, \ldots, \gamma$. Thus, $0 = f(v, x_j) = b_j$ and $0 = f(v, y_j) = a_j$, for $j = 1, 2, \ldots, \gamma$. Hence,

$$v = \sum_{i=1}^{s-1-2\gamma} c_i z_i + du.$$

Moreover, since n is even,

$$\langle z_1, \ldots, z_{s-1-2\gamma}, u \rangle \subseteq W \cap (\mathscr{R}\mathscr{S}[D])^* \cap \mathscr{R}\mathscr{S}\,\mathrm{col}\,[D, u].$$

Since $\dim \mathscr{R}\mathscr{S}[Z_1] = \tau - 1$ and u is not in $\mathscr{R}\mathscr{S}[Z_1]$, $\dim \langle z_1, \ldots, z_{s-1-2\gamma}, u \rangle = \tau$ and, therefore, $|W \cap (\mathscr{R}\mathscr{S}[D])^* \cap \mathscr{R}\mathscr{S}\,\mathrm{col}\,[D, u]| = q^\tau$. Also, since $W \cap (\mathscr{R}\mathscr{S}[D])^* \cap \mathscr{R}\mathscr{S}\,\mathrm{col}\,[D, u] = \langle z_1, \ldots, z_{s-1-2\gamma}, u \rangle$, $W \cap (\mathscr{R}\mathscr{S}[D])^* \cap \mathscr{R}\mathscr{S}\,\mathrm{col}\,[D, u] \cap \mathscr{R}\mathscr{S}[D] = \mathscr{R}\mathscr{S}[Z_1]$. Consequently, $|T \cap S| = q^\tau - q^{\tau-1}$. Since $|T| = q^{n-2\gamma-\tau} - q^{\tau-1}$, it follows that $R(2\gamma, n, s, \tau) = q^{n-2\gamma-\tau} - q^\tau$. The difference equation in (4.6) becomes

$$(4.7)\quad J_2(2\gamma, n, s, \tau) = q^\tau J_2(2\gamma, n, s-1, \tau) + (q^{n-2\gamma-\tau} - q^\tau) \times J_2(2\gamma, n, s-1, \tau-1), \quad (n \text{ even}),$$

with initial conditions $J_2(2\gamma, n, s, 0) = 1$, for $s \geqq 2\gamma$, and $J_2(2\gamma, n, s, \tau) = 0$, for $\tau \neq 0$. It is easily seen that the solution to the recurrence in (4.7) is given by

$$(4.8)\qquad J_2(2\gamma, n, s, \tau) = \begin{bmatrix} s - 2\gamma \\ \tau \end{bmatrix} \prod_{j=1}^{\tau} (q^{n-2\gamma-j} - q^j), \quad (n \text{ even}).$$

Next, suppose u is in $\mathscr{R}\mathscr{S}[M]$. We seek expressions $B(2\gamma, n, s, \tau)$, $C(2\gamma, n, s, \tau)$, $E(2\gamma, n, s, \tau)$, and $F(2\gamma, n, s, \tau)$ such that

$$\begin{aligned}(4.9)\quad J_1(2\gamma, n, s, \tau) = {} & B(2\gamma, n, s, \tau) J_1(2\gamma, n, s-1, \tau) \\ & + C(2\gamma, n, s, \tau) J_1(2\gamma, n, s-1, \tau-1) \\ & + E(2\gamma, n, s, \tau) J_2(2\gamma, n, s-1, \tau) \\ & + F(2\gamma, n, s, \tau) J_2(2\gamma, n, s-1, \tau-1).\end{aligned}$$

https://doi.org/10.4153/CJM-1974-008-2 Published online by Cambridge University Press

Suppose D has rank $2\gamma + \tau$ and u is in $\mathscr{R}\mathscr{S}[D]$. Then, $z_{s-2\gamma}$ must be in $W \cap (\mathscr{R}\mathscr{S}[D])^* \cap \mathscr{R}\mathscr{S}[D] = \mathscr{R}\mathscr{S}[Z_1]$, a subspace of dimension τ. Thus, $B(2\gamma, n, s, \tau) = q^\tau$. Suppose D has rank $2\gamma + \tau - 1$ and u is in $\mathscr{R}\mathscr{S}[D]$. Then, $z_{s-2\gamma}$ must be in $W \cap (\mathscr{R}\mathscr{S}[D])^* - \mathscr{R}\mathscr{S}[D]$. Since u is in $\mathscr{R}\mathscr{S}[D]$, $(\mathscr{R}\mathscr{S}[D])^* \subseteq W$ and, thus, $W \cap (\mathscr{R}\mathscr{S}[D])^* - \mathscr{R}\mathscr{S}[D] = (\mathscr{R}\mathscr{S}[D])^* - \mathscr{R}\mathscr{S}[Z_1]$. It follows that $C(2\gamma, n, s, \tau) = q^{n-2\gamma-\tau+1} - q^{\tau-1}$. If D has rank $2\gamma + \tau$ and u is not in $\mathscr{R}\mathscr{S}[D]$, then for any $z_{s-2\gamma}$ in $\mathscr{R}\mathscr{S}[D]$, u is not in $\mathscr{R}\mathscr{S}[M]$. Therefore, $E(2\gamma, n, s, \tau) = 0$. Finally, suppose rank $D = 2\gamma + \tau - 1$ and u is not in $\mathscr{R}\mathscr{S}[M]$. Then, $z_{s-2\gamma}$ must be in

$$(W \cap (\mathscr{R}\mathscr{S}[D])^* \cap \mathscr{R}\mathscr{S} \operatorname{col}[D, u]) - \mathscr{R}\mathscr{S}[D] = \langle z_1, \ldots, z_{s-1-2\gamma}, u \rangle - \mathscr{R}\mathscr{S}[Z_1].$$

Hence, $F(2\gamma, n, s, \tau) = q^\tau - q^{\tau-1}$. The difference equation in (4.9) becomes

$$(4.10) \quad \begin{aligned} J_1(2\gamma, n, s, \tau) = {} & q^\tau J_1(2\gamma, n, s-1, \tau) \\ & + (q^{n-2\gamma-\tau+1} - q^{\tau-1})\, J_1(2\gamma, n, s-1, \tau-1) \\ & + (q^\tau - q^{\tau-1}) J_2(2\gamma, n, s-1, \tau-1), \quad (n \text{ even}), \end{aligned}$$

with initial condition $J_1(2\gamma, n, s, 0) = 0$, for all s, and $J_1(2\gamma, n, 2\gamma, \tau) = 0$, for all τ. This initial condition follows immediately from Theorem 3.2 and from the definition of $J_1(2\gamma, n, s, \delta)$. From (4.5), (4.7), and (4.10), a difference equation in $\Phi(2\gamma, n, s, \tau)$ is obtained, namely,

$$(4.11) \quad \begin{aligned} \Phi(2\gamma, n, s, \tau) = {} & q^\tau \Phi(2\gamma, n, s-1, \tau) \\ & + (q^{n-2\gamma-\tau+1} - q^{\tau-1})\, \Phi(2\gamma, n, s-1, \tau-1) \\ & - q^{n-2\gamma-\tau}(q-1) J_2(2\gamma, n, s-1, \tau-1), \quad (n \text{ even}), \end{aligned}$$

with initial condition $\Phi(2\gamma, n, s, 0) = 1$, for $s \geqq 2\gamma$, and $\Phi(2\gamma, n, 2\gamma, \tau) = 0$, for $\tau \neq 0$, where $J_2(2\gamma, n, s-1, \tau-1)$ is given in (4.8). It is easily seen that the solution to the recurrence in (4.11) is given by

$$(4.12) \quad \begin{aligned} \Phi(2\gamma, n, s, \tau) = {} & \begin{bmatrix} s - 2\gamma \\ \tau \end{bmatrix} \\ & \times \left\{ (q^\tau - 1) \prod_{i=1}^{\tau-1} (q^{n-2\gamma-i} - q^i) + \prod_{i=1}^{\tau} (q^{n-2\gamma-i} - q^i) \right\}, \quad (n \text{ even}). \end{aligned}$$

Combining (4.2), (4.4), and (4.12), we obtain the number $N(I_n, G_\gamma, n, s, 2\gamma + \tau)$.

THEOREM 4.1. *Let A be an $n \times n$ symmetric, nonalternate matrix of full rank over $GF(q)$, and let C be an $s \times s$ alternate matrix of rank 2γ over $GF(q)$. The number of $s \times n$ matrices X of rank $2\gamma + \tau$ over $GF(q)$ such that $XAX^T = C$ is $N(A, C, n, s, 2\gamma + \tau) = N(I_n, F_\gamma, n, 2\gamma)\Phi(2\gamma, n, s, \tau)$, where $N(I_n, F_\gamma, n, 2\gamma)$ is given in Theorem 3.3 and $\Phi(2\gamma, n, s, \tau)$ is given in (4.4) in case n is odd, and in (4.12) in case n is even.*

Suppose A is an $n \times n$ symmetric, nonalternate matrix of rank ρ over $GF(q)$ and C is an $s \times s$ alternate matrix of rank 2γ over $GF(q)$. By Theorem

2.2, Theorem 2.3, and Lemma 2.1, $N(A, C, n, s, r) = N(R_\rho, G_\gamma, n, s, r)$, $0 \leqq r \leqq \min(s, n)$, where R_ρ is the $n \times n$ matrix

$$\begin{bmatrix} I_\rho & 0 \\ 0 & 0 \end{bmatrix}$$

over $GF(q)$. If $X = [X_1X_2]$ is any $s \times n$ matrix of rank r over $GF(q)$ such that $XR_\rho X^T = G_\gamma$, where X_1 is $s \times \rho$ and X_2 is $s \times (n - \rho)$, then

$$(4.13) \qquad [X_1X_2]\begin{bmatrix} I_\rho & 0 \\ 0 & 0 \end{bmatrix}\begin{bmatrix} X_1{}^T \\ \\ X_2{}^T \end{bmatrix} = X_1X_1{}^T = G_\gamma.$$

Further, rank $X = r$ implies rank $X_1 \geqq r - (n - \rho)$. For any τ, $\max(r - n + \rho - 2\gamma, 0) \leqq \tau \leqq \min[\min(s, \rho) - 2\gamma, r - 2\gamma]$, the number $N(I_\rho, G_\gamma, \rho, s, 2\gamma + \tau)$ of $s \times \rho$ matrices X_1 of rank $2\gamma + \tau$ over $GF(q)$ such that $X_1X_1{}^T = G_\gamma$ is given in Theorem 4.1. Consider any such matrix X_1. By (4.13), any $s \times (n - \rho)$ matrix X_2 such that $X = [X_1X_2]$ has rank r yields $XR_\rho X^T = G_\gamma$. The number of such matrices X_2 is the number $L(s, \rho, n, 2\gamma + \tau, r)$, given in Lemma 2.2. Thus, we have determined the number $N(A, C, n, s, r) = N(R_\rho, G_\gamma, n, s, r)$, in case rank $A = \rho \leqq n$.

THEOREM 4.2. *Suppose A is an $n \times n$ symmetric, nonalternate matrix of rank ρ over $GF(q)$ and C is an $s \times s$ alternate matrix of rank 2γ over $GF(q)$. The number of $s \times n$ matrices X of rank r, $2\gamma \leqq r \leqq \min(s, n)$, over $GF(q)$ such that $XAX^T = C$ is given by*

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

where $N(I_\rho, G_\gamma, \rho, s, 2\gamma + \tau)$ is given in Theorem 4.1, $L(s, \rho, n, 2\gamma + \tau, r)$ is given in Lemma 2.2, where $h(r, n, \rho, \gamma) = \max(r - n + \rho - 2\gamma, 0)$, and where $d(s, \rho, \gamma, r) = \min[\min(s, \rho) - 2\gamma, r - 2\gamma]$.

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. Buckhiester, *Gauss sums and the number of solutions to the matrix equation $XAX^T = 0$ over $GF(2^y)$*, Acta Arith. *23* (1973), 271–278.
4. ——— *Rank r solutions to the matrix equation $XAX^T = C$, A alternate, over $GF(2^y)$*, Trans. Amer. Math. Soc. (to appear).
5. ——— *Rank r solutions to the matrix equation $XAX^T = C$, A and C nonalternate, over $GF(2^y)$*, Math. Nachr. (to appear).
6. L. Carlitz, *Representations by quadratic forms in a finite field*, Duke Math. J. *21* (1954), 123–137.
7. ——— *The number of solutions of certain matric equations over a finite field*, Math. Nachr. (to appear).

8. Dai Zong-duo (Tai Tsung-Tuo), *On transitivity of subspaces in orthogonal geometry over fields of characteristic 2*, Chinese Math. Acta. *16* (1966), 569–584.

9. J. H. Hodges, *A symmetric matrix equation over a finite field*, Math. Nachr. *30* (1965), 221–228.

10. 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.

Clemson University,
Clemson, South Carolina

https://doi.org/10.4153/CJM-1974-008-2 Published online by Cambridge University Press