Can. J. Math., Vol. XXIX, No. 1, 1977, pp. 169–179

REPRESENTATIONS BY HERMITIAN FORMS IN A FINITE FIELD OF CHARACTERISTIC TWO

JOHN D. FULTON

1. Introduction. Throughout this paper, we let $q = 2^w$, w a positive integer, and for $u = 1$ or 2, we let $GF(q^u)$ denote the finite field of cardinality q^u. Let $^-$ denote the involutory field automorphism of $GF(q^2)$ with $GF(q)$ as fixed subfield, where $\bar{a} = a^q$ for all a in $GF(q^2)$. Moreover, let $| \quad |$ denote the norm (multiplicative group homomorphism) mapping of $GF(q^2)$ onto $GF(q)$, where $|a| = a \cdot \bar{a} = a^{q+1}$.

Let l denote any primitive element of $GF(q^2)$ over $GF(q)$. Then $GF(q^2) = \{a + bl\colon a, b \in GF(q)\}$, $\overline{a + bl} = a + bl^q$, and $|a + bl| = a^2 + (l + l^q)ab + l^{q+1}b^2$.

Let $\mathscr{V}_c$ denote the c-dimensional vector space of c-tuples $\chi = (x_1, x_2, \ldots, x_c)$ over $GF(q^2)$. If $h(\cdot, \cdot)$ is a Hermitian scalar product on $\mathscr{V}_c \times \mathscr{V}_c$ and if $\mathscr{B}$ is any ordered basis for $\mathscr{V}_c$, then there exist elements h_{ij} in $GF(q^2)$ such that

$$(1.1) \qquad h(\chi, \chi) = \sum_i^c \sum_j^c h_{ij} x_i \bar{x}_j = \chi H \chi^*,$$

where $H = (h_{ij})$ is the $c \times c$ Hermitian matrix of the Hermitian form defined by $h(\cdot, \cdot)$ on $\mathscr{V}_c$ relative to $\mathscr{B}$ and where for any $a \times b$ matrix X over $GF(q^2)$, X^* denotes the conjugate, transpose of X.

Let vector spaces $\mathscr{V}_n$ and $\mathscr{V}_m$ have ordered bases $\mathscr{B}$ and $\mathscr{B}_1$, respectively. Let Hermitian form $h(\cdot, \cdot)$ of rank k on $\mathscr{V}_n$ have matrix A relative to $\mathscr{B}$ and let Hermitian form $h_1(\cdot, \cdot)$ of rank s on $\mathscr{V}_m$ have matrix B relative to $\mathscr{B}_1$. We seek the number of $m \times n$ matrices X of prescribed rank r such that for all $\eta \in \mathscr{V}_m$,

$$(1.2) \qquad \eta B \eta^* = h_1(\eta, \eta) = h(\eta X, \eta X) = \eta X A X^* \eta^*.$$

That is, we seek the number of $m \times n$ matrices X of rank r over $GF(q^2)$ such that

$$(1.3) \qquad XAX^* = B,$$

where A is $n \times n$, Hermitian of rank k and where B is $m \times m$, Hermitian of rank s.

Hodges [**11**] has solved the problem of this paper for finite fields $GF(q^2)$ of odd cardinality q^2. It should be pointed out here that the methods used in our

Received April 22, 1976 and in revised form, July 21, 1976.

https://doi.org/10.4153/CJM-1977-017-5 Published online by Cambridge University Press

paper apply as well to the odd cardinality q^2 case as to the even and rely more heavily on the classical theory of Hermitian forms than does the paper by Hodges. Had q^2 been odd, we would have chosen l in the second paragraph of this section to be equal to $g^{(q+1)/2}$, where g is any generator of the cyclic multiplicative group of $GF(q^2)$. In that case, $\overline{a + bl} = a + bl^q = a - bl$ and $|a + bl| = a^2 - vb^2$ for all a, $b \in GF(q^2)$ and for $l^2 = v$. We will point out other minor alterations in this paper which will apply to the determination of rank r solutions X to (1.3) over $GF(q^2)$, q^2 odd.

Carlitz and Hodges [**7**] have found the number of $m \times n$ matrices X of *all ranks* over $GF(q^2)$, q^2 odd, which satisfy (1.3), but did not find the number of *specified rank* as did Hodges and as is done in our paper for q^2 even. Wan and Yang [**16**] have employed partitioned matrices with many blocks to find all $m \times n$ matrices X of *full rank* m which are solutions to (1.3). Our paper relies more heavily on the classical theory of Hermitian forms than does that of Wan and Yang for the full rank case. Finally, we establish in Section 4, recurrence relations whose solution in Section 5 yields the number of rank r solutions to (1.3). These recurrences are of the same class of recurrence relations encountered by Buckhiester [**2**; **3**; **4**], Fulton [**10**], and Perkins [**14**] and solved by Carlitz [**6**].

2. Preliminaries. If $h(\, . \, , . \,)$ is a Hermitian scalar product of rank k on vector space $\mathscr{V}_n$ over $GF(q^2)$, it may be seen in the text by Jacobson [**12**, p. 153], for example, that there exists an ordered basis $(\nu_1, \ldots, \nu_k, \zeta_1, \ldots, \zeta_{n-k})$ of $\mathscr{V}_n$ such that the matrix of $h(\cdot, \cdot)$ relative to this ordered basis is the diagonal matrix $D = D[b_1, \ldots, b_k, 0, \ldots, 0]$, where $0 \neq b_i = h(\nu_i, \nu_i)$, $i = 1, \ldots, k$.

Since each b_i above is a Hermitian element of $GF(q^2)$ $(b_i \in GF(q))$, choose element $c_i \in GF(q)$ such that $c_i^2 = b_i$. Then $c_i\bar{c}_i = c_ic_i^q = c_i^2 = b_i$. Hence, there exists an ordered basis $(\omega_1, \ldots, \omega_k, \zeta_1, \ldots, \zeta_{n-k})$ such that the matrix of $h(\cdot, \cdot)$ relative to this basis is $\begin{bmatrix} I_k & 0 \\ 0 & 0 \end{bmatrix}$.

Carlitz and Hodges [**7**] use a theorem by Dickson [**8**, p. 46] to show that if q^2 is odd, there exists a basis $(\omega_1, \ldots, \omega_k, \zeta_1, \ldots, \zeta_{n-k})$ of $\mathscr{V}_n$ such that the matrix of $h(\cdot, \cdot)$ relative to this basis is $\begin{bmatrix} I_k & 0 \\ 0 & 0 \end{bmatrix}$, where I_k is the $k \times k$ identity matrix.

Let $M(r, k, n, s, m)$ be the number of $m \times n$ matrices X of rank r over $GF(q^2)$ which satisfy equation (1.3). Since A is $n \times n$ Hermitian of rank k, there exists an ordered basis $\mathscr{B}_1$ for $\mathscr{V}_n$ and, hence a matrix P of change of basis such that $PAP^* = \begin{bmatrix} I_k & 0 \\ 0 & 0 \end{bmatrix}$, where if $P = (p_{ij})$, $P^* = (p_{ij}^*)$ with $p_{ij}^* = \bar{p}_{ji}$. Similarly, since B is $m \times m$ Hermitian of rank s, there exists an ordered basis $\mathscr{B}_2$ for $\mathscr{V}_m$ and a matrix Q of change of basis such that $QBQ^* = \begin{bmatrix} I_s & 0 \\ 0 & 0 \end{bmatrix}$. Thus, the $m \times n$ matrix X of rank r over $GF(q^2)$ satisfies (1.3) if and only if

https://doi.org/10.4153/CJM-1977-017-5 Published online by Cambridge University Press

the $m \times n$ matrix $Z = QXP^{-1}$ of rank r satisfies

$$(2.1)\qquad Z\begin{bmatrix} I_k & 0 \\ 0 & 0 \end{bmatrix} Z^* = \begin{bmatrix} I_s & 0 \\ 0 & 0 \end{bmatrix}.$$

Hence, $M(r, k, n, s, m)$ is the number of rank r, $m \times n$ matrices Z over $GF(q^2)$ which are solutions to (2.1).

Partition Z as $Z = \begin{bmatrix} Z_1 & Z_2 \\ Z_3 & Z_4 \end{bmatrix}$, where Z_1 is $s \times k$, Z_2 is $s \times (n - k)$, Z_3 is $(m - s) \times k$, and Z_4 is $(m - s) \times (n - k)$. Then $Z = \begin{bmatrix} Z_1 & Z_2 \\ Z_3 & Z_4 \end{bmatrix}$ of rank r satisfies (2.1) if and only if

$$(2.2)\qquad \begin{bmatrix} Z_1 \\ Z_3 \end{bmatrix} [Z_1^*, Z_3^*] = \begin{bmatrix} I_s & 0 \\ 0 & 0 \end{bmatrix}.$$

Thus,

$$(2.3)\qquad M(r, k, n, s, m) = \sum_{t=s}^{r} M(t, k, k, s, m) g(r - t, k, n, m),$$

where for each $m \times k$ matrix $\begin{bmatrix} Z_1 \\ Z_3 \end{bmatrix}$ of rank t which satisfies (2.2), $g(r - t, k, n, m)$ is the number of $m \times (n - k)$ matrices $\begin{bmatrix} Z_2 \\ Z_4 \end{bmatrix}$ over $GF(q^2)$ such that $Z = \begin{bmatrix} Z_1 & Z_2 \\ Z_3 & Z_4 \end{bmatrix}$ is $m \times n$ of rank $r \geqq s$. Brawley and Carlitz [**1**] have found $g(r - t, k, n, m)$ to be

$$(2.4)\qquad g(r - t, k, n, m) = \begin{bmatrix} n - k \\ r - t \end{bmatrix} q^{2t(n-k-r+t)} \prod_{j=0}^{r-t-1} (q^{2m} - q^{2(t+j)})$$

with

$$\begin{bmatrix} n - k \\ r - t \end{bmatrix} = \frac{\prod_{j=1}^{n-k} (q^j - 1)}{\prod_{i=1}^{r-t} (q^j - 1) \prod_{j=1}^{n-k-r+t} (q^j - 1)}$$

a *q-binomial coefficient.*

In Section 3, we determine $M(s, k, k, s, s)$, the number of rank s, $s \times k$ solutions Z_1 over $GF(q^2)$ to

$$(2.5)\qquad Z_1 Z_1^* = I_s.$$

In Section 4, we establish recurrence relations whose solution in Section 5 yields $M(t, k, k, s, m)$ and, thus, by (2.3), $M(r, k, n, s, m)$.

The remainder of this section contains needed results on exponential sums, on quadratic forms, and on the classical theory of Hermitian scalar products defined on $\mathscr{V}_c \times \mathscr{V}_c$.

Consider the mapping τ of $GF(q)$, $q = p^w$, p an arbitrary prime, onto $GF(p)$, defined by $\tau(a) = a + a^p + a^{p^2} + \ldots + a^{p^{w-1}}$. Define $e(a) = (-1)^{\tau(a)}$. Then it is widely known and an easy exercise that the exponential sum

$$(2.6)\qquad \sum_x e(ax) = \begin{cases} q & \text{if } a = 0, \\ 0 & \text{if } a \neq 0. \end{cases}$$

Dickson [**8**, pp. 197–199] has shown that every full rank quadratic form $f(\cdot)$ defined on $\mathscr{V}_n$ over $GF(q)$, $q = 2^w$, can, by appropriate choice of ordered basis for $\mathscr{V}_n$, be written in exactly one of the three forms

$$(2.7)\qquad f(\chi) = x_1x_{u+1} + x_2x_{u+2} + \ldots + x_ux_{2u} + x_{2u+1}^2, \quad n = 2u + 1,$$

$$(2.8)\qquad f(\chi) = x_1x_{u+1} + x_2x_{u+2} + \ldots + x_ux_{2u}, \quad n = 2u, \quad \text{or}$$

$$(2.9)\qquad f(\chi) = x_1x_{u+1} + \ldots + x_ux_{2u} + x_{2u+1}^2 + x_{2u+1}\,x_{2u+2} + bx_{2u+2},^2$$

where in (2.9), b is any element of $GF(q)$ such that the polynomial $x^2 + x + b$ is irreducible in $GF(q)[x]$. Full rank quadratic form $f(\cdot)$ in n variables is said to be of *type* $\phi = 0, 1$, or -1 according as $f(\cdot)$ is equivalent to (under change of basis in $\mathscr{V}_n$) (2.7), (2.8), (2.9), respectively. Carlitz [**5**] has examined the seemingly difficult task of determining from its coefficients the type of a quadratic form defined on vector space $\mathscr{V}_n$, n even over $GF(q)$, q even. In particular, if $f(\chi) = \sum_{1\leqq i \leqq j \leqq n} a_{ij}\, x_i\, x_j$ denotes a quadratic form of full rank n on $\mathscr{V}_n$, he defines the exponential sum

$$(2.10)\qquad S(f) = \sum_{\gamma \in \mathscr{V}_n} e(f(\gamma)),$$

and shows that

$$(2.11)\qquad S(f) = \begin{cases} 0, & n \text{ odd}, \\ \phi q^{n/2}, & n \text{ even}. \end{cases}$$

Hence, (2.10) and (2.11) can be used to determine the type of a full rank n quadratic form $f(\cdot)$ defined on $\mathscr{V}_n$ over $GF(q)$, q and n even.

Let $h(\cdot\,,\cdot)$ denote a Hermitian scalar product defined on an n-dimensional (finite) vector space over a field F such that the equation $x + \bar{x} = b$ has a solution x in F for every Hermitian element b of F. If $\mathscr{S}$ is a subspace of $\mathscr{V}$, then $\mathscr{S}^\perp$ will denote the subspace $\mathscr{S}^\perp = \{\nu \in \mathscr{V} : h(\nu, \sigma) = 0 \text{ for all } \sigma \in \mathscr{S}\}$. The *radical* of a subspace $\mathscr{S}$ is the subspace Rad $(\mathscr{S}) = \mathscr{S} \cap \mathscr{S}^\perp$. A subspace $\mathscr{S}$ of $\mathscr{V}$ is said to be *nonisotropic*, *isotropic*, or *totally isotropic* according as Rad $(\mathscr{S})$ is $\{0\}$, is not $\{0\}$, or is $\mathscr{S}$, respectively. The Hermitian scalar product $h(\cdot\,,\cdot)$ is said to be *nondegenerate* (full rank) or *degenerate* according as Rad $\mathscr{V}$ is or is not $\{0\}$, respectively. Subspaces $\mathscr{S}_1$ and $\mathscr{S}_2$ of $\mathscr{V}$ are said to be *h-equivalent* if and only if there exists a linear isomorphism U of $\mathscr{S}_1$ onto $\mathscr{S}_2$ such that $h(\chi, \eta) = h(\chi U, \eta U)$ for all $\chi, \eta \in \mathscr{S}_1$. Also, if U defines an h-equivalence of $\mathscr{V}$ with itself, then U is said to be an *h-unitary transformation on* $\mathscr{V}$.

https://doi.org/10.4153/CJM-1977-017-5 Published online by Cambridge University Press

Witt's Theorem applies in our setting [**12**, p. 162]. We restate it here as Theorem 2.1.

THEOREM 2.1. *If $\mathcal{S}_1$ and $\mathcal{S}_2$ are nonisotropic and h-equivalent subspaces of vector space $\mathcal{V}$, where $h(\cdot, \cdot)$ is a nondegenerate, Hermitian scalar product on $\mathcal{V}$, then $\mathcal{S}_1^{\perp}$ and $\mathcal{S}_2^{\perp}$ are h-equivalent.*

Jacobson [**12**, p. 167] uses Theorem 2.1 to prove another version of Witt's Theorem for $h(\cdot, \cdot)$ a nondegenerate Hermitian scalar product on n-dimensional vector space $\mathcal{V}$. We restate the theorem as Theorem 2.2 for later reference.

THEOREM 2.2. *If $\mathcal{S}$ is a sbuspace of $\mathcal{V}$, then* $\dim(\mathcal{S}^{\perp}) = n - \dim(\mathcal{S})$. *Moreover, if $\mathcal{S}$ with basis $(\eta_1, \ldots, \eta_m)$ is isotropic with basis $(\eta_1, \ldots, \eta_v)$ for* Rad $(\mathcal{S})$, *then there exist linearly independent vectors $\beta_1, \ldots, \beta_v$ in $\mathcal{V}$ such that*

$$h(\eta_i, \beta_j) = \begin{cases} 1, i = j \\ 0, i \neq j \end{cases}, \quad i = 1, \ldots, m, j = 1, \ldots, v$$

and such that subspace $\mathcal{B} = [\beta_1, \ldots, \beta_v]$ is totally isotropic. Moreover $\mathcal{S} \cap \mathcal{B} = \{0\}$ and $\mathcal{S} \oplus \mathcal{B}$ is nonisotropic. Thus, every h-equivalence of a subspace $\mathcal{S}$ of $\mathcal{V}$ can be extended to an h-unitary transformation on $\mathcal{V}$.

We conclude this section with the cardinality $|\mathcal{U}_n(q^2)|$ of the unitary subgroup $\mathcal{U}_n(q^2)$ of the full linear group of $n \times n$ nonsingular matrices over $GF(q^2)$. This cardinality may be found in [**15**, p. 33], for example:

$$(2.12) \quad |\mathcal{U}_n(q^2)| = q^{(n^2-n)/2} \prod_{i=1}^{n} (q^i - (-1)^i).$$

3. Determination of $M(s, k, k, s, s)$. The $m \times k$ matrix $\begin{bmatrix} Z_1 \\ Z_3 \end{bmatrix}$ of rank t over $GF(q^2)$ satisfies (2.2) if and only if Z_1, $s \times k$ of rank s, satisfies (2.5), and Z_3, $(m - s) \times k$ such that $Z = \begin{bmatrix} Z_1 \\ Z_3 \end{bmatrix}$ has rank t, satisfies $RS(Z_3) \subseteq (RS(Z))^{\perp}$, where $RS(Z_i)$ is the row space of matrix Z_i. We determine $M(s, k, k, s, s)$, the number $s \times k$, rank s solutions to (2.5). Let ϵ_i denote the ith unit vector of $\mathcal{V}_k$ over $GF(q^2)$. Then $\mathcal{S}_1 = [\epsilon_1, \ldots, \epsilon_s]$ is a nonisotropic subspace of $\mathcal{V}_k$. Moreover, the identity linear transformation I defines an h-equivalence of $\mathcal{S}_1$ with itself. By Theorem 2.1, relative to the basis of elementary unit vectors for $\mathcal{V}_k$, there exists $P \in \mathcal{U}_k(q^2)$ extending I. Let $\mathcal{I}$ be the subgroup of unitary matrices $P \in \mathcal{U}_k(q^2)$ such that P extends I. Clearly, $\mathcal{I}$ is isomorphic to $\mathcal{U}_{k-s}(q^2)$.

Let $Z_1 = \begin{bmatrix} \zeta_1 \\ \cdot \\ \cdot \\ \cdot \\ \zeta_s \end{bmatrix}$ satisfy (2.5) and let $\mathcal{S}_2 = RS(Z_1)$, nonisotropic. Then $T : \mathcal{S}_1 \rightarrow \mathcal{S}_2$ such that $(\epsilon_i)T = \zeta_i$, $i = 1, \ldots, s$, defines an h-equivalence of

https://doi.org/10.4153/CJM-1977-017-5 Published online by Cambridge University Press

$\mathscr{S}_1$ onto $\mathscr{S}_2$. By Theorem 2.1, there exists $P_1 \in \mathscr{U}_k(q^2)$ such that P_1 extends T. Moreover, the coset $\mathscr{I}P_1$ of $\mathscr{I}$ in $\mathscr{U}_k(q^2)$ is precisely $\{U \in \mathscr{U}_k(q^2)\colon U \text{ extends } T\}$. Hence, the number solutions Z_1 to (2.5) is the index of $\mathscr{I}$ in $\mathscr{U}_k(q^2)$. That is,

$$(3.1) \qquad M(s, k, k, s, s) = |\mathscr{U}_k(q^2)|/|\mathscr{U}_{k-s}(q^2)|,$$

where the cardinalities of $\mathscr{U}_k(q^2)$ and $\mathscr{U}_{k-s}(q^2)$ are given by (2.12).

4. Recurrences for $M(t, k, k, s, m)$. Suppose Z_1 is any of the $M(s, k, k, s, m)$ solutions to (2.5), where $M(s, k, k, s, m)$ is given by (3.1). Let $t = s + u$. For each such Z_1, let $N(u, k, s, m)$ be the number of $m \times k$ matrices $Z = \begin{bmatrix} Z_1 \\ Z_3 \end{bmatrix}$ of rank t such that Z satisfies (2.2). Then

$$(4.1) \qquad M(t, k, k, s, m) = M(s, k, k, s, s)N(u, k, s, m).$$

Hence, to complete the problem posed in this paper we need only determine $N(u, k, s, m)$, the number of $(m - s) \times k$ matrices Z_3, for given Z_1, $s \times k$ of rank t satisfying (2.5), such that

$$(4.2) \qquad Z = \begin{bmatrix} Z_1 \\ Z_3 \end{bmatrix} \text{ has rank } t, \quad \text{and}$$

$$(4.3) \qquad RS(Z_3) \subseteq (RS(Z))^{\perp}.$$

Let $\mathscr{T} = \{\chi \in \mathscr{V}_k\colon h(\chi, \chi) = 0\}$, $h(\cdot, \cdot)$ nondegenerate. Thus, we identify the following recurrence for $N(u, k, s, m)$:

$$(4.4) \qquad N(u, k, s, m) = K(u, k, s)N(u, k, s, m - 1) + L(u, k, s)N(u - 1, k, s, m - 1),$$

where for given $(m - 1) \times k$ matrix $Z = \begin{bmatrix} Z_1 \\ Z_3 \end{bmatrix}$ of rank $t = s + u$ satisfying (2.2), $K(u, k, s)$ is the number of vectors $\zeta \in \mathscr{V}_k$ such that

$$(4.5) \qquad \zeta \in \text{Rad } (RS(Z)) \cap \mathscr{T} = \text{Rad } (RS(Z))$$

and where for given $(m - 1) \times k$ matrix $Z = \begin{bmatrix} Z_1 \\ Z_3 \end{bmatrix}$ of rank $t - 1 = s + u - 1$ satisfying (2.2), $L(u, k, s)$ is the number of $\zeta \in \mathscr{V}_k$ such that

$$(4.6) \qquad (\zeta \in [(RS(Z))^{\perp} - RS(Z)] \cap \mathscr{T}.$$

We proceed to determine $K(u, k, s)$. Suppose for given $Z = \begin{bmatrix} Z_1 \\ Z_3 \end{bmatrix}$, $(m - 1) \times k$ of rank $t = s + u$ satisfying (2.2), $\zeta \in \mathscr{V}_k$ and satisfies (4.5). Let $Z_1 = \begin{bmatrix} \chi_1 \\ \cdot \\ \cdot \\ \cdot \\ \chi_s \end{bmatrix}$ and let $\xi_1, \ldots, \xi_u$ be rows of Z_3 such that $RS(Z) = [\chi_1, \ldots, \chi_s, \xi_1, \ldots, \xi_u]$.

Now $\operatorname{Rad}(RS(Z)) \subseteq RS(Z)$. Thus, $\zeta = \sum_{i=1}^{s} a_i\chi_i + \sum_{i=1}^{u} b_i\xi_i$. Since each $\xi_i \in RS(Z_3) \subseteq RS(Z_1)^{\perp}$, $i = 1, \ldots, u$, and since $\zeta \in \operatorname{Rad}(RS(Z)) \subseteq (RS(Z_1))^{\perp}$, $a_j = h(\zeta, \chi_j) = 0, j = 1, \ldots, s$. Hence, $\zeta \in [\xi_1, \ldots, \xi_u]$. Conversely, if $\zeta \in [\xi_1, \ldots, \xi_u]$, ζ satisfies (4.5). Hence, $\operatorname{Rad}(RS(Z)) = [\xi_1, \ldots, \xi_u]$, and, therefore,

(4.7) $K(u, k, s) = q^u$.

An expression for $L(u, k, s)$ is not so readily determined. Suppose for given $Z = \begin{bmatrix} Z_1 \\ Z_3 \end{bmatrix}$, $(m-1) \times k$ of rank $t - 1 = s + u - 1$ satisfying (2.2), $\zeta \in \mathscr{V}_k$ and satisfies (4.6). Let $Z_1 = \begin{bmatrix} \chi_1 \\ \cdot \\ \cdot \\ \cdot \\ \chi_s \end{bmatrix}$. Let $\xi_1, \ldots, \xi_{u-1}$ be linearly independent row vectors of Z_3 such that $RS(Z) = [\chi_1, \ldots, \chi_s, \xi_1, \ldots, \xi_{u-1}]$. We saw in the determination of an expression for $K(u, k, s)$ that $\operatorname{Rad}(RS(Z)) = [\xi_1, \ldots, \xi_u]$. For the present consideration $\operatorname{Rad}(RS(Z)) = [\xi_1, \ldots, \xi_{u-1}]$. By Theorem 2.2, there exist vectors $\beta_1, \ldots, \beta_{u-1}$ in $\mathscr{V}_k$ such that

$$h(\xi_i, \beta_j) = \begin{cases} 1, i = j \\ 0, i \neq j \end{cases},$$

$i, j = 1, \ldots, u - 1$, such that $h(\chi_i, \beta_j) = 0, i = 1, \ldots, s, j = 1, \ldots, u - 1$, and such that the subspace $\mathscr{B} = [\beta_1, \ldots, \beta_{u-1}]$ is totally isotropic. Moreover, $\mathscr{V}_k = RS(Z) \oplus \mathscr{B} \oplus (RS(Z) \oplus \mathscr{B})^{\perp}$. Let $\mathscr{X} = (RS(Z) \oplus \mathscr{B})^{\perp} = [\gamma_1, \gamma_2, \ldots, \gamma_d]$, where $d = \dim \mathscr{X} = k - s - 2(u-1)$. Hence, $\dim(RS(Z))^{\perp} = k - \dim RS(Z) = (u-1) + d$. Now

(4.8) $((RS(Z))^{\perp} - RS(Z) \cap \mathscr{T} = (RS(Z))^{\perp} \cap \mathscr{T} - \operatorname{Rad} RS(Z)$.

Clearly, $(RS(Z))^{\perp} = [\xi_1, \ldots, \xi_{u-1}, \gamma_1, \gamma_2, \ldots, \gamma_d]$, while $\operatorname{Rad} RS(Z) = [\xi_1, \ldots, \xi_{u-1}]$. Since by Theorem 2.2, $RS(Z) \oplus \mathscr{B}$ is nonisotropic, so is $\mathscr{X}$ nonisotropic. Thus, we can assume that the basis $\gamma_1, \gamma_2, \ldots, \gamma_d$ for $\mathscr{X}$ has been chosen such that $h(\gamma_i, \gamma_j) = \delta_{ij}$, the Kronecker delta. If $\zeta \in \mathscr{V}_k$ such that ζ satisfies (4.6), then $\zeta = \sum_i^{u-1} a_i\xi_i + \sum_i^d c_i\gamma_i$, where $\zeta \notin \operatorname{Rad} RS(Z)$ and where

(4.9) $$0 = h(\zeta, \zeta) = \sum_{i=1}^{d} c_i\bar{c}_i.$$

Therefore, in order to determine $L(u, k, s)$, we must find the number of solutions $(c_1, \ldots, c_d) \in \mathscr{V}_d$ over $GF(q^2)$ to (4.9). Now each c_i in $GF(q^2)$ can be written as $c_i = x_i + lx_{d+i}$, where, for q^2 even, l is a primitive element of $GF(q^2)$ over $GF(q)$ and where each $x_i \in GF(q)$. Thus, (4.9) can be used to define a quadratic form in $2d$ variables on $\mathscr{V}_{2d}$ over $GF(q)$,

(4.10) $$f(x_1, \ldots, x_{2d}) = \sum_i^d c_i\bar{c}_i = \sum_i^d (x_i^2 + (l^q + l)x_ix_{d+1} + l^{q+1}x_{d+i}^2),$$

for which we seek the number of solutions to $f(x_1, \ldots, x_{2d}) = 0$. Relative to the ordered basis of elementary unit vectors for $\mathscr{V}_{2d}$, the matrix of f is (in partitioned form)

$$(4.11)\quad \begin{bmatrix} I_d & (l^q + l)I_d \\ 0 & l^{q+1}I_d \end{bmatrix}.$$

Hence, the matrix of the symmetric, alternating bilinear form associated with f is

$$(4.12)\quad G + G^T = (l^q + l)\begin{bmatrix} 0 & I_d \\ I_d & 0 \end{bmatrix}.$$

Since from (4.11) and (4.12), $G + G^T$ has full rank $2d$, f is a quadratic form of full rank $2d$ on $\mathscr{V}_d$.

Using (2.10) and (2.11), we seek to determine the type ϕ of f. Now from (2.10),

$$(4.13)\quad \begin{aligned} S(f) &= \sum_{(z_1, \ldots, z_{2d}) \in \mathscr{V}_{2d}} e(f(z_1, \ldots, z_{2d})), \\ &= \prod_i^d \sum_{z_i} \sum_{z_{d+i}} e(z_i^2 + (l^q + l)z_i z_{d+i} + l^{q+1} z_{d+i}^2). \end{aligned}$$

Carlitz [**5**] shows that

$$(4.14)\quad \sum_{a,b \in GF(q)} e(a^2 + ab + kb^2) = -q$$

if $k \in GF(q)$ such that the polynomial $x^2 + x + k$ is irreducible in $GF(q)[x]$. A change of variable transforms (4.13) into a product of d exponential sums of the form (4.14), where the polynomial $x^2 + x + l^{q+1}(l^q + l)^{-2}$ is irreducible in $GF(q)[x]$. (It is reducible in $GF(q^2)[x]$). Hence,

$$(4.15)\quad S(f) = (-q)^d = (-1)^d q^d,$$

and f has type $\phi = -1$ if d is odd and type $\phi = 1$ if d is even. It is seen in [**9**] that the number of solutions to $f(x_1, \ldots, x_{2d}) = 0$, where f is a full rank quadratic form of type ϕ on vector space $\mathscr{V}_{2d}$ over $GF(q)$, q even, is given by

$$(4.16)\quad Q(d) = q^{2d-1} + \phi\, q^{d-1}(q - 1) = q^{2d-1} + (-1)^d q^{d-1}(q - 1),$$

where ϕ, the type of f, is 1 if f is equivalent to (2.8) and is -1 if is equivalent to (2.9).

Now $|\text{Rad } RS(Z)| = q^{u-1}$. Hence, for q^2 even,

$$(4.17)\quad L(u, k, s) = q^{u-1}Q(d) - q^{u-1} = q^{u-1}(Q(d) - 1).$$

If q^2 were odd, then $\sum_i^d c_i \bar{c}_i = \sum_i^d (x_i^2 - vx_{d+i}^2)$, where $v = l^2 = g^{q+1}$, g a generator for the multiplicative group of $GF(q^2)$. Dickson [**8**, p. 47] shows that the number of solutions to $\sum_i^d c_i \bar{c}_i = \sum_i^d (x_i^2 - vx_{d+i}^2) = 0$, for q odd, is given by (4.16) and thus $L(u, k, s)$ is given by (4.17) for q even and q odd. In view of the comments by Kaplansky [**13**, p. 36] concerning the values in $GF(q)$ of $|c| = c\bar{c}$ for c in $GF(q^2)$, this should not be surprising.

Thus, we have developed an explicit recurrence expression for $N(u, k, s, m)$. Recalling that $d = k - s - 2(u - 1)$ and applying (4.7), (4.16), and (4.17) to (4.4), we obtain

$$(4.18)\quad N(u, k, s, m) = q^u N(u, k, s, m - 1) + q^{u-1}(Q(k - s - 2(u - 1)) - 1)N(u - 1, k, s, m - 1)$$

with initial conditions

$$(4.19)\quad N(u, k, s, s) = \begin{cases} 1, & u = 0 \\ 0, & u > 0 \end{cases}.$$

5. Solution to the recurrence for $N(u, k, s, m)$. Carlitz [**6**], after examining a recurrence arising in a paper by Perkins [**14**], gave solutions for a class of recurrences, or finite difference equations of the form

$$(5.1)\quad V(u, k, s, m) = q^u V(u, k, s, m - 1) + A(u, k, s)V(u - 1, k, s, m - 1),$$

where $A(u, k, s)$ is known. Carlitz applied the change of variable $V(u, k, s, m) = q^{um}\bar{V}(u, k, s, m)$ to transform (5.1) to the equation

$$(5.2)\quad \bar{V}(u, k, s, m) = \bar{V}(u, k, s, m - 1) + q^{1-m-u}A(u, k, s)\bar{V}(u - 1, k, s, m - 1).$$

Then, he applied the operator E, where $E(f(u)) = f(u + 1)$, $E^0(f(u)) = f(u)$, and $E^{-1}(f(u)) = f(u - 1)$, to write (5.2) in the simple recurrence form

$$(5.3)\quad \bar{V}(u, k, s, m) = (1 + q^{1-m-u}A(u, k, s)E^{-1})\bar{V}(u, k, s, m - 1)$$

and applied the initial conditions and the relationship

$$(5.4)\quad \prod_{i=1}^{m} [1 + q^{-i}g(u)E^{-1}] = \sum_{i=0}^{m} \begin{bmatrix} m \\ i \end{bmatrix} q^{-im+1/2i(i-1)} g(u)g(u - 1) \dots g(u - i + 1)E^{-i}$$

to solve (5.2) and, hence, (5.1). Using Carlitz' methods, we have as solution to the finite difference equation (4.18) with initial conditions given by (4.19),

$$(5.5)\quad N(u, k, s, m) = \begin{bmatrix} m - s \\ u \end{bmatrix} \prod_{i=1}^{u} L(i, k, s),$$

where $L(i, k, s)$ is given by (4.17) and (4.16) and where $\begin{bmatrix} m - s \\ u \end{bmatrix}$ is a q-binomial coefficient. To summarize, we conclude with the following theorem.

THEEOEM 5.1. *The number $M(r, k, n, s, m)$ of $m \times n$ matrices X of rank r*

https://doi.org/10.4153/CJM-1977-017-5 Published online by Cambridge University Press

over $GF(q^2)$, q^2 even, such that $XAX^* = B$ for specified Hermitian A of rank k and specified Hermitian B of rank s, $0 \leqq s \leqq r \leqq k \leqq n$ and $0 \leqq 2(r-s) \leqq k-s$, is given by

$$M(r, k, n, s, m) = \sum_{t=s}^{r} M(t, k, k, s, m) g(r-t, k, n, m),$$

where

$$g(r-t, k, n, m) = \begin{bmatrix} n-k \\ r-t \end{bmatrix} q^{2t(n-k-r+t)} \prod_{j=0}^{r-t-1} (q^{2m} - q^{2(t+j)}),$$

and where

$$M(t, k, k, s, m) = M(s, k, k, s, s) N(u, k, s, m)$$

with

$$M(s, k, k, s, s) = |\mathcal{U}_k(q^2)|/|\mathcal{U}_{k-s}(q^2)|$$

and

$$N(u, k, s, m) = \begin{bmatrix} m-s \\ u \end{bmatrix} \prod_{i=1}^{u} L(i, k, s).$$

$L(i, k, s)$ is given by (4.16) *and* (4.17).

Proof. We need only point out that the inequality $0 \leqq 2(r-s) \leqq k-s$ follows from Theorem 2.2.

References

1. J. Brawley and L. Carlitz, *Enumeration of matrices with prescribed row and column sums*, Lin. Alg. and its Applications *6* (1973), 165–174.
2. P. Buckhiester, *Rank r solutions to the matrix equation $XAX^T = C$, A nonalternate, C alternate, over $GF(2^y)$*, Can. J. Math. *26* (1974), 78–90.
3. ——— *Rank r solutions to the matrix equation $XAX^T = C$, A alternate, over $GF(2^y)$*, Trans. Amer. Math. Soc. *189* (1974), 201–209.
4. ——— *Rank r solutions to the matrix equation $XAX^T = C$, A and C nonalternate, over $GF(2^y)$*, Math. Nachr. *63* (1974), 413–422.
5. L. Carlitz, *Gauss sums over finite fields of order 2^n*, Acta Arith. *15* (1969), 247–265.
6. ——— *The number of solutions of certain matrix equations over a finite field*, Math. Nachr. *56* (1973), 105–109.
7. L. Carlitz and J. Hodges, *Representations by Hermitian forms in a finite field*, Duke Math. J. *22* (1965), 393–406.
8. L. Dickson, *Linear groups with an exposition of the Galois theory* (Leipzig, reprinted by Dover, 1958).
9. J. Fulton, *Gauss sums and solutions to simultaneous equations over $GF(2^y)$*, to appear, Acta Arith.
10. ——— *Representations by quadratic forms of arbitrary rank in a finite field of characteristic two*, Linear And Multilinear Algebra *4* (1976), 89–101.
11. J. Hodges, *An Hermitian matrix equation over a finite field*, Duke Math. J. *33* (1966), 123–130.
12. N. Jacobson, *Lectures in abstract algebra, Volume II* (New York, 1953).
13. I. Kaplansky, *Linear algebra and geometry* (Boston, 1969).
14. J. Perkins, *Rank r solutions to the matrix equation $XX^T = 0$ over a field of characteristic two*, Math. Nachr. *48* (1971), 69–76.

https://doi.org/10.4153/CJM-1977-017-5 Published online by Cambridge University Press

15. G. Wall, *On the conjugacy classes in the unitary, symplectic and orthogonal groups*, J. Australian Math. Soc. *3* (1963), 1–62.

16. Z. Wan and B. Yang, *Studies in finite geometries and the construction of incomplete block designs, III: some "anzahl" theorems in unitary geometry over finite fields and their applications*, Acta. Math. Sinica *15* (1965), 533–544 (Chinese Math. Acta *7* (1965), 252–264).

Clemson University,
Clemson, South Carolina

https://doi.org/10.4153/CJM-1977-017-5 Published online by Cambridge University Press