Atti Accademia Nazionale dei Lincei

Classe Scienze Fisiche Matematiche Naturali

Rendiconti

Nick Mousouris, A.Duane Porter

The symmetric matric equation $X'_n \cdots X'_1 A X_1 \cdots X_n = B$.

Atti della Accademia Nazionale dei Lincei. Classe di Scienze Fisiche, Matematiche e Naturali. Rendiconti, Serie 8, Vol. **62** (1977), n.2, p. 126–130.

Accademia Nazionale dei Lincei

<http://www.bdim.eu/item?id=RLINA_1977_8_62_2_126_0>

Algebra. — *The symmetric matric equation* $X'_n \cdots X'_1 A X_1 \cdots X_n = B$. Nota di NICK MOUSOURIS e A. DUANE PORTER, presentata (*) dal Socio B. SEGRE.

RIASSUNTO. — Si determina il numero delle soluzioni $X_1, \cdots, X_n$ della suddetta equazione su di un campo di Galois, dove A e B designano due assegnate matrici simmetriche.

1. INTRODUCTION

Let $F = GF(q)$ denote the finite of $q = p^f$ elements, p odd. The transpose of a matrix X is denoted by X'.

L. Carlitz [2] and John H. Hodges [5] calculated the number of solutions X over F to the matric equation

$$X' AX = B. \tag{1.1}$$

Carlitz found the number $N_t(A, B)$ of $m \times t$ matrices X satisfying (1.1) for A and B symmetric, A nonsingular of order m and B of order t and rank r. We refer to this as the unranked case. Hodges gave an explicit formulation for the number $N(A, B; k)$ of $e \times t$ matrices X over F of rank k satisfying (1.1), where A and B are symmetric, A is of order e rank m and B is as above. $N(A, B; k)$ is the number of ranked solutions to (1.1).

In this paper we count the number of solutions $X_1, \cdots, X_n$ over F to the equation

$$X'_n \cdots X'_1 AX_1 \cdots X_n = B, \tag{1.2}$$

for A and B symmetric, where A is of order d_0, rank m and B is of order d_n and rank r in both the ranked and unranked cases. $N(\alpha, \beta, d_0, \cdots, d_n; m, r)$ represents the number of solutions $X_1, \cdots, X_n$, $n > 1$, where X_i is a $d_{i-1} \times d_i$ matrix, $i = 1, \cdots, n$ to (1.2), (the unranked case), and α, β represent the invariants of A and B respectively to be discussed in section 2. $N(\alpha, \beta, d_0, \cdots, d_n; m, r, k_1, \cdots, k_n)$, $n > 1$, denotes the number of solutions of (1.2) where $\alpha, \beta, d_0, \cdots, d_n, r$ and m have the same meaning as before and k_i is the rank of X_i, $i = 1, \cdots, n$, (the ranked case). The resulting formula for $N(\alpha, \beta, d_0, \cdots, d_n; m, r, k_1, \cdots, k_n)$ is the more general formula in the sense that by summing over all admissible ranks of X_i, $i = 1, \cdots, n$ it is possible to evaluate $N(\alpha, \beta, d_0, \cdots, d_n; m, r)$. For $n = 1$ (2.2) and (2.3) yield explicit formulations for the number of solutions to (1.1) in the unranked and ranked cases respectively.

(*) Nella seduta del 12 febbraio 1977.

2. NOTATION AND PRELIMINARIES

Let F be as in section 1. Matrices with elements from F are denoted by Roman capitals $A, B, \cdots$. $A(s, m)$ denotes a matrix of s rows and m columns and $A(s, m; r)$ denotes a matrix of the same dimensions having rank r. I_r denotes the identity matrix of order r and $I(s, m; r)$ denotes an $s \times m$ matrix having I_r in its upper left hand corner and zeros elsewhere.

If $A = A(e, e; m)$ is symmetric then A is congruent [3; 168] to a diagonal matrix $\operatorname{diag}(\alpha_1, \cdots, \alpha_m, 0, \cdots, 0)$. Let $\delta = \delta(A) = \alpha_1, \cdots, \alpha_m$ (clearly $\delta(A) \neq 0$ unless $m = 0$) and let ψ denote the generalized Legendre function defined by $\psi(\alpha) = 0, 1, -1$ according as $\alpha = 0$, a nonzero square or a nonsquare of F. Then as Hodges [5; 222] notes $\lambda(A)$ defined by $\lambda(A) = \psi(\delta(A))$ is an invariant under congruence and is called the invariant of A.

Carlitz's formula [2; Theorem 5] for $N_t(A, B)$, the number of solutions $X(m, t)$ to (1.1), requires A to be nonsingular. If in (1.1) A is taken to be symmetric, $A = A(e, e; m)$ and B is symmetric $B = B(t, t; r)$ then by Hodges argument [5; 224] (1.1) can be reduced to the equivalent matrix equation

$$X' \operatorname{diag}(A_1, 0) X = B_1 = \operatorname{diag}(B_2, 0), \tag{2.1}$$

where A_1 is symmetric and nonsingular of order m with $\lambda(A_1) = \lambda(A)$ and B_2 is symmetric and nonsingular of order r with $\lambda(B) = \lambda(B_1) = \lambda(B_2)$. The number of solutions $X(m, t)$ of (1.1) for A and B symmetric, $A = A(e, e; m)$ and $B = B(t, t; r)$ can now be calculated from

$$N(\lambda(A), \lambda(B), e, t; m, r) = q^{(e-m)t} N_t(A_1, B_1). \tag{2.2}$$

Hodges' formula for the number of solutions $X(m, t; k)$ to (1.1) for A and B symmetric, $A = A(e, e; m)$ and $B = B(t, t; r)$, as corrected by Porter and Riveland [7; 3.9] is given by

$$N(\lambda(A), \lambda(B), e, t; m, r, k) = \tag{2.3}$$

$$\sum_{s=h}^{\min(k,m)} q^{s(e-m)} g(e-m, t-s, k-s) N(A_1, B_1, s),$$

where A_1 and B_1 are as above, $h = \max(k, k-e+m)$, $N(A_1, B_1, s)$ is given explicitly in [4] and [5] and $g(m, t, s)$ is the well known formula due to Landsberg [6] for the numbers of $m \times t$ matrices of rank s given by

$$g(m, t, s) = q^{s(s-1)/2} \prod_{i=1}^{s} (q^{m-i+1} - 1)(q^{t-i+1} - 1)/(q^i - 1).$$

We use g_m to denote $g(m, m, m)$.

Finally Carlitz's formula [2; Theorem 3] for the number of symmetric matrices $C = C(m, m; r)$, $\lambda(C) = \mu$ is given by

$$S(m, r, \mu) = g_m [q^{r(m-r)} g_{m-r} E(r, \mu)]^{-1}, \tag{2.4}$$

where $E(r, \mu)$ denotes the number of automorphs of C given by

$$E(r, \mu) = \begin{cases} 2q^{r(r-1)/2} \{1 - \mu [\psi(-1) q^{-1}]^{r/2}\} \prod\limits_{i=1}^{(r-2)/2} (1 - q^{2i-r}), & r \text{ even}, \\ 2q^{r(r-1)/2} \prod\limits_{i=1}^{(r-1)/2} (1 - q^{2i-r-1}), & r \text{ odd}. \end{cases}$$

3. The number $N(\alpha, \beta, d_0, \cdots, d_n; m, r)$

Lemma 1. *For $n > 1$, $r \le \min(d_0, \cdots, d_n, m)$, the number of solutions $X_i(d_{i-1}, d_i)$, $i = 1, \cdots, n$ to (1.2), where A is symmetric, $A = w(d_0, d_0, m)$, $\lambda(A) = \alpha$, B is symmetric, $B = B(d_n, d_n; r)$, $\lambda(B) = \beta$ is given by the reduction formula*

$$N(\alpha, \beta, d_0, \cdots, d_n; m, r) = \sum_{r_{n-1}=r}^{u} \sum_{\beta_{n-1}=-1,0,1} N(\alpha, \beta_{n-1}, d_0, \cdots \tag{3.1}$$

$$\cdots, d_{n-1}; m, r_{n-1}) \cdot N(\beta_{n-1}, \beta, d_{n-1}, d_n; r_{n-1}, r) S(d_{n-1}, r_{n-1}, \beta_{n-1}),$$

where $u = \min(m, d_0, \cdots, d_{n-1})$ and $N(\alpha, \beta_{n-1}, d_0, \cdots, d_{n-1}; m, r_{n-1})$ is of the same form as $N(\alpha, \beta, d_0, \cdots, d_n; m, r)$ for $n > 2$. If $n - 1 = 1$ then $N(\alpha, \beta_1, d_0, d_1, m, r_1)$ is given by (2.2), $N(\beta_{n-1}, \beta, d_{n-1}, d_n; r_{n-1}, r)$ is given by (2.2) adn $S(d_{n-1}, r_{n-1}, \beta_{n-1})$ is given by (2.4).

Proof. To count the number of solutions to (1.2) we first count the number of solutions to each of the following matric equations

$$X'_{n-1} \cdots X'_1 A X_1 \cdots X_{n-1} = D, \tag{3.2}$$

$$X'_n D X_n = B. \tag{3.3}$$

Since A is symmetric, equation (3.2) forces D to be symmetric of order d_{n-1}. Fix D and let its rank be r_{n-1} and $\lambda(D) = \beta_{n-1}$. The number of solutions to (3.2) can be represented by $N(\alpha, \beta_{n-1}, d_0, \cdots, d_{n-1}; m, r_{n-1})$. The number of solutions to (3.3) is given by $N(\beta_{n-1}, \beta, d_{n-1}, d_n, r_{n-1}, r)$. In order that there be solutions to (3.2) and (3.3) it is necessary that $r \le r_{n-1} \le \min(m, d_0, \cdots, d_{n-1})$.

The product $N(\alpha, \beta_{n-1}, d_0, \cdots, d_{n-1}; m, r_{n-1}) \cdot N(\beta_{n-1}, \beta, d_{n-1}, d_n; r_{n-1}, r)$ represents the number of solutions $X_1, \cdots, X_n$ to the system of equations (3.2) and (3.3) for D described above. Multiplying this product by the number

$S(d_{n-1}, r_{n-1}, \beta_{n-1})$ of symmetric matrices D with order d_{n-1}, rank r_{n-1} and invariant β_{n-1} and summing over all possible values for r_{n-1} and β_{n-1} we obtain the desired result (3.1).

Theorem 1 now follows from the lemma and mathematical induction.

THEOREM 1. *The number* $N = N(\alpha, \beta, d_0, \cdots, d_n; m, r)$, *of solutions* $X_1(d_0, d_1), \cdots, X_n(d_{n-1}, d_n)$ *to the matric equation* (1.2) *is given by*

$$N = \sum_{r_i=r}^{s_i} \sum_{\beta_k=0,1,-1} N(\alpha, \beta, d_0, d_1; m, r_1) \cdot \tag{3.4}$$

$$\cdot \prod_{j=1}^{n-1} N(\beta_j, \beta_{j+1}, d_j, d_{j+1}; r_j, r_{j+1}) S(d_j, r_j, \beta_j),$$

where $s_i = \min(m, d_0, \cdots, d_i)$, $\beta_n = \beta$, $r_n = r$, $1 \leq i, k \leq n-1$, $n > 1$ *and* $r \leq \min(d_0, \cdots, d_n, m)$.

The above formulation together with the formulae for evaluating (2.2) and (2.4) give N as an explicit function of the variables $\alpha, \beta, d_0, \cdots, d_n, m$ and r. We will not take the space here to list this combined formula. For $n = 1$, the number of solutions to (1.2) is given by (2.2) Hence the number of solutions $X_i(d_{i-1}, d_i)$, $i = 1, \cdots, n$ to (1.2) can now be calculated in all cases where solutions exist for $n \geq 1$.

4. THE NUMBER $N(\alpha, \beta, d_0, \cdots, d_n; k_1, \cdots, k_n, m, r)$

In this section we obtain a formula for the number of solutions to (1.2) in the ranked case, that is where $X_i = X_i(d_{i-1}, d_i, k_i)$, $1 \leq i \leq n$. The proofs of Lemma 2, which gives a reduction formula, and for Theorem 2, which gives the desired result, are analogous to the proofs of Lemma 1 and Theorem 1 and will not be included.

LEMMA 2. *For* $n > 1$, $r \leq \min(m, k_1, \cdots, k_n)$, *the number of solutions* $X_i(d_{i-1}, d_i; k_i)$, $i = 1, \cdots, n$ *of* (1.2) *where* A *is symmetric*, $A = A(d_0, d_0, m)$, $\lambda(A) = \alpha$, B *is symmetric*, $B = B(d_n, d_n; r)$, $\lambda(B) = \beta$ *is given by*

$$N(\alpha, \beta, d_0, \cdots, d_n; k_1, \cdots, k_n, m, r) =$$

$$= \sum_{r_{n-1}=r}^{u} \sum_{\beta_{n-1}=-1,0,1} N(\alpha, \beta_{n-1}, d_0, \cdots, d_{n-1}; k_1, \cdots, k_{n-1}, m, r_{n-1}) \cdot$$

$$\cdot N(\beta_{n-1}, \beta, d_{n-1}, d_n; k_n, r_{n-1}, r) \cdot S(d_{n-1}, r_{n-1}, \beta_{n-1}),$$

where $u = \min(m, k_1, \cdots, k_n)$ *and* $N(\alpha, \beta_{n-1}, d_0, \cdots, d_{n-1}; k_1, \cdots, k_{n-1}, m, r_{n-1})$ *is of the same form as* $N(\alpha, \beta, d_0, \cdots, d_n; k_1, \cdots, k_n, m, r)$ *for* $n > 2$. *If* $n - 1 = 1$, *then* $N(\alpha, \beta, d_0, d_1; k_1, m, r)$ *is given by* (2.3). $N(\beta_{n-1}, \beta, d_{n-1}, d_n; k_n, r_{n-1}, r)$ *is given by* (2.3) *and* $S(d_{n-1}, r_{n-1}, \beta_{n-1})$ *is given by* (2.4).

THEOREM 2. *The number* $M = N(\alpha, \beta, d_0, \cdots, d_n; k_1, \cdots, k_n, m, r)$ *of solutions* $X_1(d_0, d_1; k_1), \cdots, X_n(d_{n-1}, d_n; k_n)$ *of the matric equation* (1.2) *is given by*

$$M = \sum_{r_i=r}^{t_i} \sum_{\beta_j=-1,0,1} N(\alpha, \beta_1, d_0, d_1; m, r_1, k_1) \cdot \tag{4.1}$$

$$\cdot \prod_{h=1}^{n-1} N(\beta_h, \beta_{h+1}, d_h, d_{h+1}; r_h, r_{h+1}, k_{h+1}) \cdot S(d_h, r_h, \beta_h)$$

where $\beta_n = \beta$, $r_n = r$ *and* $t_i = \min(m, k_1, \cdots, k_i)$, $1 \leq i, j \leq n-1$, $n > 1$ *and* $r \leq \min(m, k_1, \cdots, k_n)$.

As in Theorem 1 all of the forms appearing on the right in (4.1) can be calculated explicitly in terms of $\alpha, \beta, d_0, \cdots, d_n, k_1, \cdots, k_n, m$ and r. The process begins by referring to (2.3) and (2.5). We will not take the space here to put the various formulae together to write a single explicit formula.

REFERENCES

[1] W. N. BAILEY (1935) – *Generalized Hypergeometric Series*, Cambridge.

[2] L. CARLITZ – *Representations by Quadratic Forms in a Finite Field*, «Duke Math. J.», *21*, 123–138.

[3] L. E. DICKSON (1901) – *Linear Groups*, Leipzig.

[4] JOHN H. HODGES (1956) – *Exponential Sums for Symmetric Matrices in a Finite Field*, «Mathematische Nachrichten», *15*, 331–339.

[5] JOHN H. HODGES (1965) – *A Symmetric Matrix Equation Over a Finite Field*, «Mathematische Nachrichten», *30*, 221–228.

[6] GEORGE LANDSBERG (1893) – *Über eine Anzahlbestimmung und eine Damit Zusammenhägende Reihe*, «Journal für die Reine und Angewandte Mathematik», *111*, 87–88.

[7] A. DUANE PORTER and A. ALLAN RIVELAND (1975) – *A Generalized Skew Equation Over a Finite Field*, «Mathematische Nachrichten», *69*, 291–296.

[8] A. ALLAN RIVELAND and A. DUANE PORTER – *The Skew Matric Equation* $X'_n \cdots X'_1 AX_1 \cdots X_n = B$, «Rend. Accademia Nazionale dei Lincei» (to appear).