Atti Accademia Nazionale dei Lincei

Classe Scienze Fisiche Matematiche Naturali

Rendiconti

A. Allan Riveland, A. Duane Porter

The skew 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. **60** (1976), n.6, p. 751–755.

Accademia Nazionale dei Lincei

<http://www.bdim.eu/item?id=RLINA_1976_8_60_6_751_0>

L'utilizzo e la stampa di questo documento digitale è consentito liberamente per motivi di ricerca e studio. Non è consentito l'utilizzo dello stesso per motivi commerciali. Tutte le copie di questo documento devono riportare questo avvertimento.

Articolo digitalizzato nel quadro del programma bdim (Biblioteca Digitale Italiana di Matematica) SIMAI & UMI

http://www.bdim.eu/

Atti della Accademia Nazionale dei Lincei. Classe di Scienze Fisiche, Matematiche e Naturali. Rendiconti, Accademia Nazionale dei Lincei, 1976.

Teorie combinatorie. — *The skew matric equation* $X'_n \cdots X'_1 A X_1 \cdots X_n = B$. Nota di A. ALLAN RIVELAND e A. DUANE PORTER, presentata (*) dal Socio B. SEGRE.

RIASSUNTO. — La suddetta equazione matriciale viene studiata su di un campo finito, ottenendo risultati che estendono ed in parte correggono proprietà precedentemente date in argomento da altri Autori.

1. INTRODUCTION

All matrices under consideration will have entries in the Galois field $GF(q)$, $q = p^f$, p an odd prime. X' will denote the matric transpose of the matrix X. In [2] Leonard Carlitz determined the number of $2m \times t$ matrices X for which

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

where A and B are fixed skew matrices $(A' = -A, B' = -B)$, A nonsingular of order $2m$, B of order t and rank $2r$, $r \leq m$. Related counting problems have been investigated in [1], [3], [4], and [6]. In this note we wish to generalize the results in [2] by counting the number of solutions $X_1, X_2, \cdots, X_n$ to the matric equation

$$X'_n \cdots X'_1 A X_1 \cdots X_n = B \tag{1.2}$$

where A and B are skew matrices and the dimension of all matrices are such that matric multiplication is defined. Similar generalizations of [4] and [6] have been performed by Porter in [7] and [8] respectively.

We also correct a minor error in one of Carlitz's formulas in [2] and correct the main theorem in [5] which was dependent upon the faulty formula in [2].

2. NOTATION AND PRELIMINARIES

It is well known that if A is a skew matrix of rank $2r$ then there exists a nonsingular matrix P over $GF(q)$ for which

$$P'AP = \operatorname{diag}(E_1, \cdots, E_r, 0, \cdots, 0) \quad , \quad E_i = \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix}, \quad i = 1, \cdots, r.$$

We will reserve the notation $C(t, 2r)$ to denote the above described canonical form for a $t \times t$ skew matrix of rank $2r$.

(*) Nella seduta del 10 giugno 1976.

It is easy to show that the number of solutions to the matric equation (1.2) remains invariant if the matrices A and B are replaced by their respective canonical forms. Hence the problem posed in the previous section may be solved by finding the number of solutions to the matric equation

$$X'_n \cdots X'_1 C(d_0, 2m) X_1 \cdots X_n = C(d_n, 2r) \tag{2.1}$$

where each X_i is of dimension $d_{i-1} \times d_i$, $i = 1, \cdots, n$. We denote this number by $N(d_0, \cdots, d_n; 2m, 2r)$. With this notation $N(2m, t; 2m, 2r)$ will represent the number of solutions to (1.1) which was determined by Carlitz [2; Theorem 5, denoted $Z_t(A, B)$].

It is clear that $N(d_0, \cdots, d_n; 2m, 2r) = 0$ if $\min(d_1, \cdots, d_n, 2m) < 2r$. Hence without loss of generality we can require that

$$2r \leq \min(d_1, \cdots, d_n, 2m). \tag{2.2}$$

Although it is not needed here, it is easy to show that (2.2) is also a sufficient condition for the existence of a solution to (2.1).

Carlitz [2; Theorem 3] determined the number $S(t, 2r)$ of $t \times t$ skew matrices over GF (q) of rank $2r$. He obtained

$$S(t, 2r) = q^{r(r-1)} \prod_{i=0}^{2r-1} (q^{t-i} - 1) \Big/ \prod_{i=1}^{r} (q^{2i} - 1), \qquad r > 0. \tag{2.3}$$

3. THE MAIN THEOREM

Before stating main result we need the following:

LEMMA 1. *For* $n > 1$

$$N(d_0, \cdots, d_n; 2m, 2r) =$$
$$= \sum_{k \in M} N(d_0, \cdots, d_{n-1}; 2m, k) S(d_{n-1}, k) N(d_{n-1}, d_n; k, 2r)$$

where M *is the set of even integers* k *for which* $2r \leq k \leq \min(d_1, \cdots, d_{n-1}, 2m)$ *and* S *is given by* (2.3).

Proof. To count solutions to (2.1) under condition (2.2) we may count solutions to the matric equation

$$X'_{n-1} \cdots X'_1 C(d_0, 2m) X_1 \cdots X_{n-1} = D, \tag{2.4}$$

then count solutions to the matric equation

$$X'_n D X_n = C(d_n, 2r), \tag{2.5}$$

then multiply these numbers, and sum as D ranges over all possible $d_{n-1} \times d_{n-1}$ matrices. But equations (2.4) and (2.5) both have solutions only if D is skew and has even rank k where $2r \leq k \leq \min(d_1, \cdots, d_{n-1}, 2m)$. In other words we sum as D ranges over M where M is as described in Lemma 1.

For each $k \in \mathrm{M}$ there will be exactly $\mathrm{S}(d_{n-1}, k)$ skew $d_{n-1} \times d_{n-1}$ matrices of rank k. Each of these matrices has canonical form $\mathrm{C}(d_{n-1}, k)$ and gives rise to

$$\mathrm{N}(d_0, \cdots, d_{n-1}; 2m, k)\, \mathrm{N}(d_{n-1}, d_n; k, 2r)$$

solutions of (2.1). This product is obtained by replacing D in (2.4) and (2.5) by its canonical form, counting solutions to the resulting equations and multiplying. Therefore, each $k \in \mathrm{M}$ gives rise to

$$\mathrm{S}(d_{n-1}, k)\, \mathrm{N}(d_0, \cdots, d_{n-1}; 2m, k)\, \mathrm{N}(d_{n-1}, d_n; k, 2r)$$

solutions. Summing as k ranges over M will produce the desired conclusion.

The main theorem follows directly from the preceding lemma and mathematical induction. The proof is omitted.

THEOREM 1. *The number* $\mathrm{N} = \mathrm{N}(d_0, \cdots, d_n; 2m, 2r), n > 1$, *of solutions* $\mathrm{X}_1, \cdots, \mathrm{X}_n$ *of the matric equation* (2.1) *under condition* (2.2) *is given by*

$$\mathrm{N} = \sum_{i_j \in \mathrm{M}_j} \mathrm{N}(d_0, d_1; 2m, i_1) \prod_{k=1}^{n-1} \mathrm{S}(d_k, i_k)\, \mathrm{N}(d_k, d_{k+1}; i_k, i_{k+1}), \qquad j = 1, \cdots, n-1$$

where S *is given in* (2.3) *and* M_j *is the set of even integers* i_j *for which* $2r \leq i_j \leq \min(2m, d_1, \cdots, d_j)$, $j = 1, \cdots, n-1$, $i_n = 2r$.

Using [2; Theorem 5] (subject to the correction indicated in Theorem 2 of this paper) it would now be possible to express N in terms of the variables $d_0, \cdots, d_1, r$, and m but we will not take the space to do so.

It should be noted that Carlitz's formula for $\mathrm{N}(2m, t; 2m, 2r)$ which counts solutions to (1.1) required that the matrix A be nonsingular. However as Carlitz observes, this requirement causes no loss of generality. Indeed, it is easy to show that

$$\mathrm{N}(p, t; 2m, 2r) = q^{t(p-2m)}\, \mathrm{N}(2m, t; 2m, 2r)$$

so if the central matrix A in (1.1) is not already nonsingular the problem is easily reduced to one in which this is the case.

4. CORRECTIONS

In [2; p. 25, line 12] the exponent $2t - r$ of q is incorrect. This exponent should be $2t - 2r$. We employ the notation of this paper and state as corrected the formula [2; p. 25, line 14] which was being developed when the error occurred.

THEOREM 2.

$$\mathrm{N}(2m, t; 2m, 0) = q^{-1/2t(t-1)} \sum_{0 \leq 2r \leq t} q^{m(2t-2r)}\, \mathrm{S}(t, 2r).$$

In [5] John Hodges developed a formula for certain exponential sums involving skew matrices. His development from the outset depended upon the results we corrected in Theorem 2. Using the methods outlined by Hodges we have redone the development of the main theorem [5; Theorem 1] and restate it here as corrected.

THEOREM 3. *If* B *is a skew matrix of order* t *and rank* $2j$ *then*

$$W(B, r) = q^{2jr} \sum_{k=0}^{r} (-1)^k q^{k(k-1-2j)} \begin{bmatrix} j \\ k \end{bmatrix}' S(t-2j, 2r-2k)$$

where W *is described in* [5; (3.1)], S *is given by* (2.3) *and the prime indicates that* q *is to be replaced by* q^2 *in the* q*-binomial coefficients.*

Hodges' results on hypergeometric sums [5; Theorem 2] and the conclusion drawn [5; p. 119, lines 1–3] will also be altered by the correction.

5. EXAMPLES

As a partial check on our results we investigate a few simple examples. We first calculate directly the number of solutions over GF (q) to the matric equation

$$\begin{bmatrix} x & y \\ z & w \end{bmatrix}' \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix} \begin{bmatrix} x & y \\ z & w \end{bmatrix} = \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}$$

the problem reduces to counting solutions over GF (q) to be equation $xw - zy = 0$. There are $q^3 + q^2 - q$ such solutions. This quantity equals the value of N $(2, 2; 2, 0)$ determined by Theorem 2.

In a similar manner we can determine the number of solutions to the matric equation

$$\begin{bmatrix} x & y \\ z & w \end{bmatrix}' \begin{bmatrix} a & b \\ c & d \end{bmatrix}' \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix} \begin{bmatrix} a & b \\ c & d \end{bmatrix} \begin{bmatrix} x & y \\ z & w \end{bmatrix} = \begin{bmatrix} 0 & 1 \\ -1 & 1 \end{bmatrix}$$

by counting solutions over GF (q) to the equation $(ad - bd)(xw - zy) = 1$. There are $q^7 - q^6 - 2q^5 + 2q^4 + q^3 - q^2$ such solutions. This quantity equals the value N $(2, 2; 2, 0)$ which we obtain from Theorem 1.

Although we do not go through the details, it is easy to show by direct calculation that $W(B, r) = q - 1$ where B is the 2×2 zero matrix and $r = 1$. This also agrees with results obtained by appropriate substitutions in Theorem 3.

REFERENCES

[1] L. CARLITZ (1954) – *Representations by quadratic forms in a finite field*, « Duke Mathematical Journal », *21*, 123–137.

[2] L. CARLITZ (1954) – *Representations by skew forms in a finite field*, « Archiv der Mathematik », *5*, 19–31.

[3] L. CARLITZ and JOHN HODGES (1955) – *Representations by Hermitian forms in a finite field*, « Duke Mathematical Journal », *22*, 393–405.

[4] JOHN H. HODGES (1955) – *Representations by bilinear forms in a finite field*, « Duke Mathematical Journal », *22*, 487–510.

[5] JOHN H. HODGES (1956) – *Exponential sums for skew matrices in a finite field*, « Archiv der Mathematik », *7*, 116–121.

[6] JOHN H. HODGES (1956) – *The matric equation* $AX = B$ *in a finite field*, « American Mathematical Monthly », *63*, 243–244.

[7] A. DUANE PORTER (1968) – *The matric equation* $AX_1 \cdots X_a = B$, « Rendic. Accad. Naz. Lincei », *44*, 727–732.

[8] A. DUANE PORTER (1970) – *Generalized bilinear forms in a finite field*, « Duke Mathematical Journal », *37*, 55–60.