ATTI ACCADEMIA NAZIONALE DEI LINCEI

CLASSE SCIENZE FISICHE MATEMATICHE NATURALI

RENDICONTI

JOHN H. HODGES

Note on some partitions of a rectangular matrix

Atti della Accademia Nazionale dei Lincei. Classe di Scienze Fisiche, Matematiche e Naturali. Rendiconti, Serie 8, Vol. **59** (1975), n.6, p. 662–666.

Accademia Nazionale dei Lincei

<http://www.bdim.eu/item?id=RLINA_1975_8_59_6_662_0>

Teorie combinatorie. — *Note on some partitions of a rectangular matrix.* Nota di John H. Hodges, presentata (*) dal Socio B. Segre.

Riassunto. — A complemento di risultati ottenuti da Porter in una precedente Nota lincea [5], si ottiene il numero delle soluzioni U,V per l'equazione matriciale $U_a \cdots U_1 A + BV_1 \cdots V_b = C$ su di un campo finito, dove A e B sono matrici arbitrarie e si suppone $a = 1$, $b > 1$, oppure $a > 1$, $b = 1$.

1. Introduction

Let A be an $m \times n$ matrix of rank r_1, B be an $s \times t$ matrix of rank r_2 and C be an $s \times n$ matrix over a finite field F of q elements. In this Note we study the problem of enumerating the solutions $U_a, \cdots, U_1, V_1, \cdots, V_b$ over F of the matrix equation

$$(1.1) \qquad U_a \cdots U_1 A + BV_1 \cdots V_b = C ,$$

where the matrices U_i, V_j for $1 \leqq i \leqq a$, $1 \leqq j \leqq b$ are of arbitrary but specified sizes such that the products, sum and equality in (1.1) are defined. In [2], the Author solved the problem in the case $a = b = 1$ with A and B arbitrary. More recently, A. Duane Porter [5] has given a solution for all a and b, whenever $r_1 = \text{rank } A = n$ and $r_2 = \text{rank } B = s$. In this Note, by use of the same methods as used in these two earlier papers, the Author solves the problem for arbitrary A and B in the cases $a = 1$, $b > 1$ and $a > 1$, $b = 1$. The results obtained reduce to those given by Porter [5; Theorems II, III] under the stated conditions on A and B. For arbitrary A and B and both $a > 1$ and $b > 1$, the methods used here lead to difficulties which are not resolved in this Note.

2. Notation and preliminaries

Let $F = GF(q)$ denote the finite field of $q = p^f$ elements, p a prime. Except as noted, Roman capitals A, B, $\cdots$ will denote matrices over F. $A(m, n)$ will denote a matrix of m rows and n columns and $A(m, n; r)$ a matrix of the same size with rank r. I_r will denote the identity matrix of order r and $I(m, n; r)$ will denote an $m \times n$ matrix with I_r in its upper left corner and zeros elsewhere.

If $A = (\alpha_{ij})$ is square, then $\sigma(A) = \Sigma \alpha_{ii}$ is the *trace* of A and whenever A+B or AB is square, then $\sigma(A + B) = \sigma(A) + \sigma(B)$ and $\sigma(AB) = \sigma(BA)$.

(*) Nella seduta del 13 dicembre 1975.

For $\alpha \in F$, we define

$$(2.1)\qquad e(\alpha) = \exp 2\pi i t(\alpha)/p \quad , \quad t(\alpha) = \alpha + \alpha^p + \cdots + \alpha^{p^{f-1}},$$

so that for all $\alpha, \beta \in F$, $e(\alpha) \in GF(p)$, $e(\alpha + \beta) = e(\alpha)\, e(\beta)$ and

$$(2.2)\qquad \sum_{\gamma \in F} e(\alpha\gamma) = \begin{cases} q, & \alpha = 0, \\ 0, & \alpha \neq 0, \end{cases}$$

where the sum is over all $\gamma \in F$. By use of (2.2) and properties of σ it is easily shown that for $A = A(m, n)$

$$(2.3)\qquad \sum_{B} e\{\sigma(AB)\} = \begin{cases} q^{mn}, & A = 0, \\ 0, & A \neq 0, \end{cases}$$

where the sum is over all matrices $B = B(n, m)$.

The number $g(u, v; y)$ of $u \times v$ matrices of rank y over F is given by Landsberg [3] as

$$(2.4)\qquad g(u, v; y) = \prod_{i=0}^{y-1} (q^u - q^i)(q^v - q^i)/(q^y - q^i).$$

Following [1; (8.4)], if $B = B(s, t; \rho)$ we define

$$(2.5)\qquad H(B, z) = \sum_{C} e\{-\sigma(BC)\},$$

where the sum is over all matrices $C = C(t, s; z)$. This sum is evaluated in [1, Theorem 7] to be

$$(2.6)\qquad H(B, z) = q^{\rho z} \sum_{j=0}^{z} (-1)^j q^{j(j-2\rho-1)/2} \begin{bmatrix} \rho \\ j \end{bmatrix} g(s-\rho, t-\rho; z-j),$$

where $\begin{bmatrix} \rho \\ j \end{bmatrix}$ denotes the q-binomial coefficient defined for nonnegative integers ρ and j by $\begin{bmatrix} \rho \\ 0 \end{bmatrix} = 1$, $\begin{bmatrix} \rho \\ j \end{bmatrix} = 0$ if $j > \rho$ and

$$\begin{bmatrix} \rho \\ j \end{bmatrix} = (1 - q^\rho) \cdots (1 - q^{\rho-j+1})/(1-q) \cdots (1-q^j), \qquad 0 < j \leq \rho.$$

3. THE GENERAL CASE OF (1.1)

Let A, B, C be matrices as in (1.1) and $U_a = U_a(s, m_{a-1})$, $U_i = U_i(m_i, m_{i-1})$ for $1 < i < a$, $U_1 = U_1(m_1, m)$ and $V_1 = V_1(t, t_1)$, $V_j = V_j(t_{j-1}, t_j)$ for $1 < j < b$, $V_b = V_b(t_{b-1}, n)$. If N denotes the number of solutions of (1.1) over F, then in view of (2.3), N is given by

$$(3.1)\qquad N = q^{-sn} \Sigma_a \Sigma_b \sum_{D(n,s)} e\{\sigma((U_a \cdots U_1 A + BV_1 \cdots V_b - C)D)\},$$

where Σ_a and Σ_b denote sums over all $U_a, \cdots, U_1$ and $V_1, \cdots, V_b$, respectively. Applying various properties of σ and e from section 2 and interchanging the order of summation in (3.1) leads to

$$(3.2)\quad N = q^{-sn} \sum_{D} e\{-\sigma(CD)\} \Sigma_a e\{\sigma(U_a \cdots U_1 AD)\} \Sigma_b e\{\sigma(DBV_1 \cdots V_b)\}.$$

Let P_1, Q_1, P_2, Q_2 be arbitrary but fixed nonsingular matrices such that $A = P_1 I(m, n; r_1) Q_1$ and $B = P_2 I(s, t; r_2) Q_2$. If these values are substituted into (3.2), D is replaced by $Q_1^{-1} D P_2^{-1}$, U_1 is replaced by $U_1 P_1^{-1}$, U_a is replaced by $P_2^{-1} U_a$, V_1 is replaced by $Q_2^{-1} V_1$ and V_b is replaced by $V_b Q_1^{-1}$, then (3.2) becomes

$$(3.3)\quad N = q^{-sn} \sum_{D(n,s)} e\{\sigma(C_0 D)\} \Sigma_a e\{\sigma(U_a \cdots U_1 I(m, n; r_1) D\} \cdot$$
$$\cdot \Sigma_b e\{\sigma(DI(s, t; r_2) V_1 \cdots V_b)\},$$

where $C_0 = -P_2^{-1} C Q_1^{-1}$. If an arbitrary matrix $D = D(n, s)$ is partitioned as $D = (D_{uv})$ for $u, v = 1, 2$ where D_{11} is $r_1 \times r_2$, D_{12} is $r_1 \times (s - r_2)$, D_{21} is $(n - r_1) \times r_2$ and D_{22} is $(n - r_1) \times (s - r_2)$, then

$$I(m, n; r_1) D = A_0 = (A_{uv}) \quad \text{for} \quad u, v = 1, 2 \quad \text{where}$$
$$A_{11} = D_{11}, \quad A_{12} = D_{12}, \quad A_{21} = 0 \quad \text{and} \quad A_{22} = 0,$$

and

$$DI(s, t; r_2) = B_0 = (B_{uv}) \quad \text{for} \quad u, v = 1, 2 \quad \text{where}$$
$$B_{11} = D_{11}, \quad B_{21} = D_{21}, \quad B_{12} = 0 \quad \text{and} \quad B_{22} = 0.$$

Applying these results to the two inner sums in (3.3), it follows in view of (2.2) that these sums are given by

$$(3.4)\quad \Sigma_a e\{\sigma(U_a \cdots U_1 A_0)\} = \begin{cases} q^{sm}, & \text{if } D_{11} = 0 \text{ and } D_{12} = 0, \quad (a = 1), \\ 0, & \text{otherwise,} \end{cases}$$

$$= \begin{cases} q^{sm_{a-1}}, & \text{if } U_{a-1} \cdots U_1 A_0 = 0, \quad (a > 1), \\ 0, & \text{otherwise,} \end{cases}$$

$$(3.5)\quad \Sigma_b e\{\sigma(B_0 V_1 \cdots V_b)\} = \begin{cases} q^{nt}, & \text{if } D_{11} = 0 \text{ and } D_{21} = 0, \quad (b = 1), \\ 0, & \text{otherwise,} \end{cases}$$

$$= \begin{cases} q^{nt_{b-1}}, & \text{if } B_0 V_1 \cdots V_{b-1} = 0, \quad (b > 1), \\ 0, & \text{otherwise.} \end{cases}$$

Now, let $C_0 = C_0(s, n)$ in (3.3) be partitioned as $C_0 = (C_{uv})$, for $u, v = 1, 2$, where C_{11} is $r_2 \times r_1$, C_{12} is $r_2 \times (n - r_1)$, C_{21} is $(s - r_2) \times r_1$ and C_{22} is $(s - r_2) \times (n - r_1)$. In case $a = b = 1$, in view of (3.4) and (3.5) the only terms in (3.3) which are possibly nonzero correspond to matrices D for which $D_{11} = 0$, $D_{12} = 0$, $D_{21} = 0$ and D_{22} is arbitrary and for all such D, $\sigma(C_0 D) = \sigma(C_{22} D_{22})$. Therefore, summing in (3.3) over only such D and applying (2.3) again leads to the result

$$N = q^{s(m-r_1)+n(t-r_2)+r_1 r_2} h(C_{22}), \tag{3.6}$$

where $h(C_{22}) = 1$ if $C_{22} = 0$ and $h(C_{22}) = 0$ otherwise. This is the result given previously in [2, Theorem 7].

In case $b > 1$, the value of the sum (3.5) is just $q^{nt_{b-1}}$ times the number of solutions $V_1, \cdots, V_{b-1}$ over F of the equation $B_0 V_1 \cdots V_{b-1} = 0$. This number $N_{b-1}(z)$, which depends on the sizes of the matrices involved and on the rank z of B_0, has been determined explicitly by Porter [4, Theorem II]. His formula, which involves sums of the function $g(u, v; y)$ given by (2.4), will not be repeated here. A similar comment applies to (3.4) and rank w of A_0 in case $a > 1$.

4. THE CASE $a = 1, b > 1$

In this case, we can prove

THEOREM 1. *For $a = 1$, $b > 1$ and matrices* A, B, C *as in* (1.1), *the number of solutions of* (1.1) *over* F *is*

$$N = q^e h(C_{22}) \sum_{z=0}^{(n-r_1, r_2)} N_{b-1}(z) H(C_{12}, z), \tag{4.1}$$

where $e = s(m - r_1) + n(t_{b-1} - r_2) + r_1 r_2$, $h(C_{22}) = 1$ or 0 according to whether $C_{22} = 0$ or $\neq 0$, $N_{b-1}(z)$, the number of solutions $V_1, \cdots, V_{b-1}$ over F *of the equation $B_0 V_1 \cdots V_{b-1} = 0$ depends on the sizes of the V_j and the size and rank of B_0, C_{22} and C_{12} are submatrices of C_0 as defined above, $(n - r_1, r_2)$ denotes the minimum of $n - r_1$ and r_2, and $H(C_{12}, z)$ is given explicitly by* (2.6) *with* B *replaced by* C_{12}.

(An analogous result holds for the case $a > 1$, $b = 1$ with C_{12} replaced by C_{21}).

Proof. Assume that $a = 1$, $b > 1$ in (3.3) and so in (3.4) and (3.5). By (3.4), the inner sum in (3.3) over U_1 is nonzero if and only if $D_{11} = 0$ and $D_{12} = 0$, in which case the sum is equal to q^{sm}. Thus, restricting $D(n, s)$ in (3.3) to those matrices that satisfy this condition, it follows that rank $B_0 = \text{rank } D_{21} = z$, where $0 \leqq z \leqq \min(n - r_1, r_2)$. For each D_{21} of a given rank z, the number $N_{b-1}(z)$ of solutions of the equation $B_0 V_1 \cdots V_{b-1} = 0$ depends only on the sizes of the matrices involved and on z.

Also, for all such restricted $D = D(n, s)$ it follows that $e\{\sigma(C_0 D)\} = e\{\sigma(C_{12} D_{21})\} e\{\sigma(C_{22} D_{22})\}$, where D_{22} is not involved in the two inner sums in (3.3) and so is arbitrary. Therefore, to sum (3.3) over all restricted D, one may sum independently over all D_{22} and all D_{21} of rank z for all $0 \leqq z \leqq \min(n - r_1, r_2)$. If this is done in (3.3), in view of (2.3), (3.5) and the definition (2.5), after some simplification we obtain (4.1) with the explanations given in the statement of the theorem.

5. The case $a > 1$ and $b > 1$

If A and B are arbitrary and both $a > 1$ and $b > 1$, then the involvement of D in the two inner sums in (3.3) is more complicated and interrelated and the simplification that led to Theorem 1 does not occur. At this time, the author is unable to resolve the difficulties presented in obtaining a more explicit form for N from (3.3) in this general case. For rank $A = n$ and rank $B = s$ in (1.1), (3.3) leads to Porter's results [5].

References

[1] John H. Hodges (1956) – *Representations by bilinear forms in a finite field*, « Duke Math J. », *22*, 497–510.

[2] John H. Hodges (1957) – *Some matrix equations over a finite field*, « Annali di Mat. », *14*, 245–250.

[3] Georg Landsberg (1893) – *Über eine Anzahlbestimmung und eine damit zusammenhängende Reihe*, « Journal f.d. Reine u. Ang. Math. », *3*, 87–88.

[4] A. Duane Porter (1970) – *Generalized bilinear forms in a finite field*, « Duke Math. J. », *37*, 55–60.

[5] A. Duane Porter (1974) – *Some partitions of a rectangular matrix*, « Rend. Acc. Naz. dei Lincei », *56*, 667–671.