Atti Accademia Nazionale dei Lincei

Classe Scienze Fisiche Matematiche Naturali

Rendiconti

John H. Hodges

Ranked partitions of rectangular matrices over finite fields

Atti della Accademia Nazionale dei Lincei. Classe di Scienze Fisiche, Matematiche e Naturali. Rendiconti, Serie 8, Vol. **60** (1976), n.1, p. 6–12.

Accademia Nazionale dei Lincei

<http://www.bdim.eu/item?id=RLINA_1976_8_60_1_6_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/

Algebra. — *Ranked partitions of rectangular matrices over finite fields.* Nota di JOHN H. HODGES, presentata (*) dal Socio B. SEGRE.

RIASSUNTO. — Per certe matrici A_1, A_2, B, viene determinato in modo esplicito il numero delle soluzioni (U_1, U_2) dell'equazione matriciale (1·1) su di un campo finito, dove le U_1, U_2 abbiano ranghi assegnati.

1. INTRODUCTION

Let A_1 be an $m \times t$ matrix of rank ρ_1, A_2 be an $s \times n$ matrix of rank ρ_2 and B be an $s \times t$ matrix of rank r over a finite field F of q elements. In [3], the Author enumerated the pairs of $s \times m$ matrices U_1 and $n \times t$ matrices U_2 such that

$$U_1 A_1 + A_2 U_2 = B . \tag{1.1}$$

More recently, A. Duane Porter [7] and the Author [4] have determined for certain integers $a \geqq 1$, $b \geqq 1$, and matrices A_1, A_2, the number of solutions $W_a, \cdots, W_1, V_1, \cdots, V_b$ over F of the more general matrix equation

$$W_a \cdots W_1 A_1 + A_2 V_1 \cdots V_b = B . \tag{1.2}$$

In this paper we study the problem of determining the number of solutions U_1, U_2 of (1.1) of *given ranks* r_1, r_2, respectively, over F. If this problem could be solved for arbitrary A_1, A_2, then it would be possible to determine the number of solutions of (1.2) for arbitrary a, b, A_1, A_2 by using Porter's enumeration [6] of the solutions of the matrix equation $W_a \cdots W_1 = U_1$, which depends on the rank of U_1. Unfortunately, however, the enumeration given in the present paper is only complete for matrices A_1, A_2, and B satisfying certain special conditions that are implied by Porter's conditions in [7] on A_1 and A_2.

2. NOTATION AND PRELIMINARIES

Let F 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.

(*) Nella seduta del 10 gennaio 1976.

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 $\sigma(AB) = \sigma(BA)$.

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 [5] as

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

Following [2; (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 [2, 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

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

Since $H(B, z)$ as given by (2.6) depends only on s, t, ρ and z, we write $H(B, z) = H(s, t, \rho, z)$.

3. RANKED SOLUTIONS OF (1.1); GENERAL CASE

Let N denote the number of solutions $U_1 = U_1(s, m; r_1)$, $U_2 = U_2(n, t; r_2)$ over F of equation (1.1) for given $A_1 = A_1(m, t; \rho_1)$, $A_2 = A_2(s, n; \rho_2)$ and $B = B(s, t; r)$. Let P_1, Q_1, P_2, Q_2 be arbitrary, but fixed, nonsingular matrices of appropriate sizes over F such that $P_1 A_1 Q_1 = J_1 = I(m, t; \rho_1)$ and $P_2 A_2 Q_2 = J_2 = I(s, n; \rho_2)$. Then, letting $B_0 = B_0(s, t; r) = P_2 B Q_1$, it is easy to show that (1.1) is equivalent to

$$U_1 J_1 + J_2 U_2 = B_0 . \tag{3.1}$$

Therefore, in view of (2.3) and other properties of σ and e from section 2, N is given by

$$\begin{aligned} N &= q^{-st} \sum_{U_2, U_1} \sum_{C(t,s)} e\{\sigma((U_1 J_1 + J_2 U_2 - B_0) C)\} \\ &= q^{-st} \sum_{C(t,s)} e\{\sigma(B_0 C)\} \sum_{U_1} e\{-\sigma(U_1 J_1 C)\} \sum_{U_2} e\{-\sigma(J_2 U_2 C)\} , \end{aligned} \tag{3.2}$$

where the summations are over all $U_1 = U_1(s, m; r_1)$, $U_2 = U_2(n, t; r_2)$ and $C(t, s)$ over F.

In order to sum over all $C(t, s)$ in (3.2), we may group together all terms corresponding to C's of the same rank z with $0 \leqq z \leqq \min(t, s)$. For each such $z > 0$, we may let $C = PI(t, s; z) Q$, where P and Q are nonsingular of orders t and s, respectively. Then, to sum over all C of rank z in (3.2), we may sum independently over all such nonsingular P and Q and divide this sum by the number of different pairs P , Q which yield each different $C = C(t, s; z)$. This number is easily shown to be equal to $g_t g_s / g(t, s; z)$, where $g(t, s; z)$ is the number of such C over F as given by (2.4) and $g_k = g(k, k; k)$ is the number of nonsingular matrices of order k over F.

If all of the above is done in (3.2), we get

$$\begin{aligned} N = q^{-st} \Big[& g(s, m; r_1) g(n, t; r_2) + \\ & + \sum_{z=1}^{(t,s)} g(t, s; z) / g_t g_s \sum_{P,Q} e\{\sigma(B_0 PI(t, s; z) Q)\} \cdot S_1 \cdot S_2 \Big] , \end{aligned} \tag{3.3}$$

where (t, s) denotes the minimum of t and s, P and Q run independently through all nonsingular matrices of orders t and s, respectively, over F and for arbitrary but fixed z, P, and Q, the sums S_1 and S_2 are defined by

$$\left\{ \begin{aligned} S_1 &= \sum_{U_1(s,m;r_1)} e\{\sigma(U_1 J_1 PI(t, s; z))\} , \\ S_2 &= \sum_{U_2(n,t;r_2)} e\{\sigma(I(t, s; z) Q J_2 U_2)\} . \end{aligned} \right. \tag{3.4}$$

(Note that S_1 and S_2 have been simplified by replacing $-QU_1$ and $-U_2 P$ by U_1 and U_2, respectively).

If P and Q in (3.4) are partitioned into submatrices as $P = (P_{ij})$, $Q = (Q_{ij})$ for $i, j = 1, 2$, where $P_{11} = P_{11}(\rho_1, z; f_1)$ with $0 \leqq f_1 \leqq \min(\rho_1, z)$, $P_{12} = P_{12}(\rho_1, t - z)$, $P_{21} = P_{21}(t - \rho_1, z)$, $P_{22} = P_{22}(t - \rho_1, t - z)$ and $Q_{11} = Q_{11}(z, \rho_2; f_2)$ with $0 \leqq f_2 \leqq \min(z, \rho_2)$, $Q_{12} = Q_{12}(z, s - \rho_2)$, $Q_{21} = Q_{21}(s - z, \rho_2)$, $Q_{22} = Q_{22}(s - z, s - \rho_2)$, then it is easily shown that

$$\operatorname{rank} J_1 PI(t, s; z) = f_1 \quad \text{and} \quad \operatorname{rank} I(t, s; z) Q J_2 = f_2 .$$

Therefore, for any such P and Q, in view of the definition (2.5) and comment following (2.6), $S_1 = H(m, s, f_1, r_1)$ and $S_2 = H(t, n, f_2, r_2)$, where $H(s, t, \rho, z)$ is given by (2.6). Substituting these results into (3.3) and grouping terms for which P and Q have P_{11} and Q_{11} of ranks f_1 and f_2, respectively, we get

$$(3.5) \qquad N = q^{-st} \Bigg[g(s, m; r_1) g(n, t; r_2) + \sum_{z=1}^{(t,s)} g(t, s; z)/g_t g_s \sum_{f_1=0}^{(\rho_1, z)} \sum_{f_2=0}^{(z, \rho_2)} H(m, s, f_1, r_1) H(t, n, f_2, r_2) \cdot \sum_{P,Q} e\{\sigma(B_0 PI(t, s; z) Q)\} \Bigg],$$

where for each choice of z, f_1, and f_2, P and Q run independently through all nonsingular matrices of order t with rank $P_{11} = f_1$ and order s with rank $Q_{11} = f_2$, respectively. In order to proceed further, we must obtain a more explicit value for the inner sum in (3.5). This is done in section 4 for certain special B_0. The Author has been unable as yet to evaluate this sum for general B_0.

4. THE VALUE OF N FOR SPECIAL B_0

If certain assumptions are made concerning the form of B_0, then it is possible to obtain explicit values for N from the formula (3.5). For this purpose, let B_0 be partitioned as $B_0 = (B_{ij})$ for $i = 1, 2$, where B_{11} is $\rho_2 \times \rho_1$, B_{12} is $\rho_2 \times (t - \rho_1)$, B_{21} is $(s - \rho_2) \times \rho_1$, and B_{22} is $(s - \rho_2) \times (t - \rho_1)$.

First of all, it was shown by the author [3, Theorem 7] that with A_1, A_2 and B_0 as defined earlier, a necessary condition that (1.1) has solutions U_1, U_2 of any ranks is that $B_{22} = 0$. In this case, it is easy to show that for P and Q defined and partitioned as in section 3, the summand in the inner sum in (3.5) becomes

$$(4.1) \qquad e\{\sigma(B_0 PI(t, s; z) Q)\} = e\{\sigma(B_{11} P_{11} Q_{11})\} e\{\sigma(B_{12} P_{21} Q_{11})\} e\{\sigma(B_{21} P_{11} Q_{12})\}.$$

The difficulty in obtaining a more explicit value for the inner sum in (3.5) occurs because in (4.1) the matrices P_{11} and Q_{11} are each involved in two different factors. If we assume that not only $B_{22} = 0$, but also $B_{12} = 0$ and $B_{21} = 0$, so that B_{11} has rank $r \leqq \min(\rho_1, \rho_2)$, then we can prove

THEOREM. *Let* $A_1 = A_1(m, t; \rho_1)$, $A_2 = A_2(s, n; \rho_2)$ *and* $B = B(s, t; r)$, *with* $r \leqq \min(\rho_1, \rho_2)$. *Let* P_1, Q_1, P_2, Q_2 *be arbitrary nonsingular matrices over* F *such that* $P_1 A_1 Q_1 = I(m, t; \rho_1)$ *and* $P_2 A_2 Q_2 = I(s, n; \rho_2)$ *and let* $B_0 = P_2 B Q_1$ *be partitioned as above, with* $B_{11} = B_{11}(\rho_2, \rho_1; r)$, $B_{12} = 0$, $B_{21} = 0$ *and* $B_{22} = 0$. *Then the number* N *of solutions* $U_1 = U_1(s, m; r_1)$,

$U_2 = U_2(n, t; r_2)$ *of equation* (1.1) *over* F *is given by*

$$(4.2) \qquad N = q^{-st}\Bigg[g(s, m; r_1)\, g(n, t; r_2) + \sum_{z=1}^{(t,s)} g(t, s; z)/g_t g_s \sum_{f_1=0}^{(\rho_1,z)} \sum_{f_2=0}^{(z,\rho_2)} H(m, s, f_1, r_1)\, H(t, n, f_2, r_2) \cdot$$

$$\cdot\, \varphi(f_1, t-\rho_1, z, z)\, \varphi(z, t-z, t, t)\, \varphi(f_2, s-\rho_2, z, z)\, \varphi(z, s-z, s, s) \cdot$$

$$\cdot \sum_{y=0}^{(r,f_1)} g(r, z; y)\, \varphi(y, \rho_1 - r, z, f_1)\, H(\rho_2, z, y, f_2)\Bigg],$$

where $g(u, v; y)$ *is the number of* $u \times v$ *matrices of rank* y *over* F *as given by* (2.4) *and* $g_k = g(k, k; k)$ *is the number of nonsingular matrices of order* k *over* F, (a, b) *denotes the minimum of integers* a *and* b, *the value of the function* $H(s, t, \rho, z)$ *is given by* (2.6) *and* $\varphi(r, n, t, r+v)$, *as given by* (4.5) *below is the number of* $(n+m)\times t$ *matrices of rank* $r+v$ *over* F *whose last* m *rows are those of a given* $m \times t$ *matrix of rank* r.

Proof. Suppose that the hypotheses of the theorem are true. Then in view of (4.1), we see that the inner sum in (3.5) becomes

$$(4.3) \qquad S = \sum_{P,Q} e\{\sigma(B_{11} P_{11} Q_{11})\},$$

where for fixed z, f_1, and f_2, P and Q run independently through all nonsingular matrices of order t with $P_{11} = P_{11}(\rho_1, z; f_1)$ and order s with $Q_{11} = Q_{11}(z, \rho_2; f_2)$, respectively. For each fixed such pair of matrices P_{11}, Q_{11}, the number of distinct corresponding pairs of nonsingular matrices P, Q is easily seen to be

$$(4.4) \qquad \varphi(f_1, t-\rho_1, z, z)\, \varphi(z, t-z, t, t)\, \varphi(f_2, s-\rho_2, z, z)\, \varphi(z, s-z, s, s),$$

where $\varphi(r, n, t, r+v)$ is the number of $(n+m)\times t$ matrices of rank $r+v$ over F whose last m rows are those of a given $m \times t$ matrix of rank r. This number has been determined by Brawley and Carlitz [1; Lemma, p. 167] as

$$(4.5) \qquad \varphi(r, n, t, r+v) = \begin{bmatrix} n \\ v \end{bmatrix} q^{r(n-v)} \prod_{i=0}^{v-1} (q^t - q^{r+i}),$$

where $\begin{bmatrix} n \\ v \end{bmatrix}$ denotes the q-binomial coefficient defined for non-negative integers n and v in section 2. Thus, sum S defined by (4.3) is equal to the expression (4.4) times the sum

$$(4.6) \qquad S' = \sum_{P_{11},Q_{11}} e\{\sigma(B_{11} P_{11} Q_{11})\} = \sum_{P_{11},Q_{11}} e\{\sigma(I(\rho_2, \rho_1; r)\, P_{11} Q_{11})\}.$$

If now any arbitrary, but fixed, P_{11} in (4.6) is partitioned as $P_{11} = \mathrm{col}(P_{111}, P_{112})$, where P_{111} is $r \times z$ of rank y, $0 \leqq y \leqq \min(r, f_1)$, then

$I(\rho_2, \rho_1; r) P_{11} = \text{col}(P_{111}, 0)$ is $\rho_2 \times z$ of rank y so that in view of definition (2.5),

$$(4.7) \qquad \sum_{Q_{11}(z,\rho_2:f_2)} e\{\sigma(I(\rho_2, \rho_1; r) P_{11} Q_{11}\} = H(\rho_2, z, y, f_2),$$

where $H(s, t, \rho, z)$ is given by (2.6). For each y, the number of such matrices P_{111} over F is $g(r, z; y)$ and for each such fixed matrix P_{111}, the number of matrices $P_{11}(\rho_1, z; f_1)$ is just $\varphi(y, \rho_1 - r, z, f_1)$ as given by (4.5). Therefore, it follows from (4.6) and (4.7) that sum S defined by (4.3) is equal to the expression (4.4) times the sum

$$(4.8) \qquad \sum_{y=0}^{(r,f_1)} g(r, z; y)\, \varphi(y, \rho_1 - r, z, f_1)\, H(\rho_2, z, y, f_2).$$

If the value of S so obtained is substituted for the inner sum in (3.5), we get formula (4.2) so that the theorem is proved.

5. AN ILLUSTRATION OF THE THEOREM

We close with an example of matrices A_1, A_2 and B in (1.1) for which the hypotheses of the theorem, concerning B_0, apply. Consider (1.1) for matrices A_1 and A_2 such that $\rho_1 = \text{rank } A_1 = t$ and $\rho_2 = \text{rank } A_2 = s$ and $B = B(s, t; r)$. If P and Q are arbitrary but fixed nonsingular matrices such that $PBQ = I(s, t; r)$, then (1.1) is easily shown to be equivalent to

$$(5.1) \qquad V_1(A_1 Q) + (PA_2) V_2 = I(s, t; r),$$

where $A_1 Q$ is $m \times t$ of rank t and PA_2 is $s \times n$ of rank s. If we take $A_1 Q$ and PA_2 in place of A_1 and A_2, respectively, in the theorem, it follows by virtue of the special ranks of these matrices that we may take both Q_1 and P_2 to be identity matrices and so $B_0 = I(s, t; r)$ satisfies the hypotheses of the theorem concerning its submatrices. Thus, the number N of solutions $V_1 = V_1(s, m; r_1)$, $V_2 = V_2(n, t; r_2)$ of (5.1), which is equal to the number of solutions $U_1 = U_1(s, m; r_1)$, $U_2 = U_2(n, t; r_2)$ of (1.1), is given by (4.2).

We note that these conditions on A_1 and A_2 are exactly those assumed by Porter [7] in connection with equation (1.2) for arbitrary a and b.

REFERENCES

[1] J. V. BRAWLEY and L. CARLTIZ (1973) – *Enumeration of matrices with prescribed row and column sums*, « Linear Algebra and its Applications », 6, 165–174.
[2] JOHN H. HODGES (1956) – *Representations by bilinear forms in a finite field*, « Duke Math. J. », 22, 497–510.
[3] JOHN H. HODGES (1957) – *Some matrix equations over a finite field*, « Annali di Mat. », 44, 245–250.

[4] JOHN H. HODGES (1975) – *Note on some partitions of a rectangular matrix*, « Rend. Acc. Naz. dei Lincei ».
[5] GEORG LANDSBERG (1893) – *Über eine Anzahlbestimmung und eine damit zusammenhängende Reihe*, « J. f.d. Reine und Ang. Math. », 87–88.
[6] A. DUANE PORTER (1968) – *The matrix equation* $AX_1 \cdots X_a = B$, « Rend. Acc. Naz. dei Lincei », *44*, 727–732.
[7] A. DUANE PORTER (1974) – *Some partitions of a rectangular matrix*, « Rend. Acc. Naz. dei Lincei », *56*, 667–671.