Atti Accademia Nazionale dei Lincei

Classe Scienze Fisiche Matematiche Naturali

Rendiconti

A. Duane Porter

The Matric Equation $AX_1 \cdots X_a = B$

Atti della Accademia Nazionale dei Lincei. Classe di Scienze Fisiche, Matematiche e Naturali. Rendiconti, Serie 8, Vol. **44** (1968), n.6, p. 727–732.

Accademia Nazionale dei Lincei

<http://www.bdim.eu/item?id=RLINA_1968_8_44_6_727_0>

Atti della Accademia Nazionale dei Lincei. Classe di Scienze Fisiche, Matematiche e Naturali. Rendiconti, Accademia Nazionale dei Lincei, 1968.

Algebra. — *The Matric Equation* $AX_1 \cdots X_a = B$. Nota di A. DUANE PORTER, presentata (*) dal Socio B. SEGRE.

RIASSUNTO. — Si determina il numero delle soluzioni dell'equazione matriciale $AX_1 \ldots X_a = B$ sopra un campo di Galois.

1. INTRODUCTION.—Let $F = GF(q)$ be the finite field of $q = p^f$ elements, p odd. Matrices with elements from F will be denoted by Roman capitals $A, B, \cdots$. $A(n, s)$ will denote a matrix of n rows and s columns, and $A(n, s; r)$ a matrix of the same dimensions with rank r. I_r will denote the identity matrix of order r, and $I(n, s; r)$ a matrix of n rows and s columns having I_r in its upper left hand corner and zeros elsewhere.

Let $A = A(n, s; r)$ and $B = B(n, t; u)$ with $r \geq u$. John H. Hodges [4] found the number of solutions $X = X(s, t)$ over F of the matrix equation $AX = B$. The problems of determining the number of solutions to various matric equations has also been considered in a number of other papers, e.g. [1], [2], [3], [5]. In this note we wish to generalize [4] and so consider the number of solutions $X_1, \cdots, X_a$ over F of the equation

$$AX_1 \cdots X_a = B, \tag{1.1}$$

with A, B defined as above; $a \geq 2$; $X_1 = X_1(s, s_1)$, $X_a = X_a(s_{a-1}, t)$, and for $1 < i < a$ we have $X_i = X_i(s_{i-1}, s_i)$ where s_i, $1 \leq i < a$ represents an arbitrary positive integer.

2. NOTATION AND PRELIMINARIES.—If $A = (\beta_{ij}) = A(n, n)$ then $\sigma(a) = \beta_{11} + \cdots + \beta_{nn}$ is the trace of A, and it is noted [5; § 2] that for AB square we have $\sigma(AB) = \sigma(BA)$. Also, it is clear that $\sigma(A + B) = \sigma(A) + \sigma(B)$. With F as previously defined and $\alpha \in F$, we define

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

from which it follows that

$$\begin{cases} e(\alpha + \beta) = e(\alpha)\, e(\beta) \quad \text{and} \\ \sum_{\beta \in F} e(\alpha\beta) = \begin{cases} q, \alpha = 0, \\ 0, \alpha \neq 0, \end{cases} \end{cases} \tag{2.2}$$

where the sum is over all $\beta \in F$. By use of (2.2), we may obtain for $A = A(m, n)$

$$\sum_{D(n,m)} e\{\sigma(AD)\} = \begin{cases} q^{mn}, A = 0, \\ 0 \quad , A \neq 0, \end{cases} \tag{2.3}$$

with the sum over all matrices $D = D(n, m)$.

(*) Nella seduta dell'8 giugno 1968.

If $B = B(s, t; u)$, then following [3; 8.4], we define

$$H(B, z) = \sum_{C(t,s;z)} e\{-\sigma(BC)\}, \tag{2.4}$$

with the sum over all $C = C(t, s; z)$. The value of this sum is given [3; Theorem 7] to be

$$H(B, z) = q^{uz} \sum_{j=0}^{z} (-1)^j q^{j(j-2u-1)/2} \begin{bmatrix} u \\ j \end{bmatrix} g(s-u, t-u; z-j), \tag{2.5}$$

where the bracket in (2.5) denotes the q–binomial coefficient defined for nonnegative integers by

$$\begin{bmatrix} u \\ 0 \end{bmatrix} = 1, \quad \begin{bmatrix} u \\ j \end{bmatrix} = \prod_{i=0}^{j-1} \frac{(1-q^{u-i})}{(1-q^{i+1})} \quad \text{if } 1 \leq i \leq u, \quad \begin{bmatrix} w \\ j \end{bmatrix} = 0 \quad \text{if } j > w,$$

and $g(m, k; y)$ represents the number of $m \times k$ matrices of rank y. By [6] we have

$$g(m, k; y) = q^{y(y-1)/2} \prod_{i=1}^{y} (q^{m-i+1}-1)(q^{k-i+1})/(q^i-1). \tag{2.6}$$

From (2.5) it is clear that $H(B, z)$ depends only upon the integers s, t, u, z, so we may write

$$H(B, z) = H(s, t, u; z). \tag{2.7}$$

Finally, as is noted in [3; p. 507], $H(s, t, 0; z) = g(s, t; z)$.

3. THE CASE $a = 2$.—We first prove

THEOREM I.—*Let n, s, s_1, t represent arbitrary positive integers; r, u arbitrary integers with $r \geq u \geq 0$; $A = A(n, s; r)$, $B = B(n, t; u)$, $X_1 = X_1(s, s_1)$, $X_2 = X_2(s_1, t)$. Then the number $N_2 = N_2(s, s_1, t, r, u)$ of solutions X_1, X_2 of the matric equation*

$$AX_1X_2 = B, \tag{3.1}$$

if any exist, is given by

$$N_2 = q^{t(s_1-r)+ss_1} \sum_{z_1=0}^{(t,r)} H(r, t, u; z_1) q^{-s_1 z_1},$$

where (t, r) = minimum of t and r; $H(r, t, u; z_1)$ is given by (2.5) and (2.7) with $H(0, t, 0; 0) = 1$.

During the proof of Theorem I, we will also obtain a solvability criterion for (3.1). We state this result now, for continuity of presentation.

THEOREM II.—*If P, Q, R, T are nonsingular matrices over F such that $PAQ = I(n, s; r)$ and $RBT = I(n, t; u)$, and if $D = PR^{-1} = (\delta_{ij})$, then (3.1) will have solutions if and only if $\delta_{ij} = 0$ for $r < i \leq n$, $1 \leq j \leq u$.*

It is of interest to note that Theorem II corresponds exactly to the solvability criterion obtained by Hodges for the equation $AX = B$ [4; Th. 2].

Proofs. (of Theorem I and Theorem II).—If P , Q , R , T , D are as defined in Theorem II, then (3.1) may be transformed into an equivalent matrix equation

$$I(n, s; r)\, Y_1 Y_2 = DI(n, t; u), \tag{3.2}$$

with $Y_1 = Q^{-1} X_1 = Y_1(s, s_1)$ and $Y_2 = X_2 T = Y_2(s_1, t)$, $D = D(n, n)$. By (2.3) the number of solutions of (3.2) is given by

$$N_2 = q^{-nt} \sum_{C} \sum_{Y_1, Y_2} e\{\sigma([I(n, s; r)\, Y_1 Y_2 - DI(n, t; u)]\, C)\},$$

where the sum over C is over all $C = C(t, n)$ and which, in view of (2.2), may be written as

$$N_2 = q^{-nt} \sum_{C} e\{-\sigma(DI(n, t; u)\, C)\} \sum_{Y_1, Y_2} e\{\sigma(I(n, s; r)\, Y_1 Y_2 C)\}. \tag{3.3}$$

Since $\sigma(I(n, s; r)\, Y_1 Y_2 C) = \sigma(CI(n, s; r)\, Y_1 Y_2)$, the inner sum in (3.3) may be evaluated by (2.3) as

$$\sum_{Y_1, Y_2} e\{\sigma(CI(n, s; r)\, Y_1 Y_2)\} = \begin{cases} q^{ts_1}, & CI(n, s; r)\, Y_1 = 0, \\ 0, & \text{otherwise.} \end{cases} \tag{3.4}$$

We now seek the number of solutions $Y_1(s_1, t)$ of

$$CI(n, s; r)\, Y_1 = 0(t, s_1). \tag{3.5}$$

We may write (3.5) as

$$[C_1 C_2] \begin{bmatrix} I_r & 0 \\ 0 & 0 \end{bmatrix} \begin{bmatrix} Y_{11} \\ Y_{12} \end{bmatrix} = [C_1 Y_{11}] = 0,$$

with $C_1 = C_1(t, r)$, $C_2 = C_2(t, n - r)$, $Y_{11} = Y_{11}(r, s_1)$, $Y_{12} = Y_{12}(s - r, s_1)$. The choice of elements of Y_1 corresponding to the block Y_{12} is clearly arbitrary, so their number is $q^{s_1(s-r)}$, and if C_1 is of rank z_1, $0 \leq z_1 \leq (t, r)$, the number of solutions of $C_1 X_{11} = 0$ is given [4; Theorem I] to be $q^{s_1(r-z_1)}$. Hence, the number of solutions of (3.5) is $q^{s_1(s-z_1)}$, so that the value of the sum in (3.4), subject to the condition rank $C_1 = z_1$, is

$$q^{s_1(s+t-z_1)}. \tag{3.6}$$

We note that $\sigma(DI(n, t; u)\, C) = \sigma(CDI(n, t; u))$ and write $CDI(n, t; u)$ as

$$[C_1, C_2] \begin{bmatrix} D_{11} & D_{12} \\ D_{21} & D_{22} \end{bmatrix} \begin{bmatrix} I_u & 0 \\ 0 & 0 \end{bmatrix} = [C_1, C_2] \begin{bmatrix} D_1 \\ D_2 \end{bmatrix} = [C_1 D_1 + C_2 D_2],$$

where $D_{11} = D_{11}(r, u)$, $D_{12} = D_{12}(r, n - u)$, $D_{21} = D_{21}(n - r, u)$, $D_{22} = D_{22}(n - r, n - u)$, $D_1 = [D_{11}, 0] = D_1(r, t; u)$, $D_2 = [D_{21}, 0] = D_2(n - r, t)$. Hence, by (2.2) and the properties of the trace

$$e\{-\sigma(CDI(n, t; u))\} = e\{-\sigma(C_1 D_1)\}\, e\{-\sigma(C_2 D_2)\};$$

hence the summation over C in (3.3) is equivalent to the summation over C_1 and C_2 independently, so that

$$(3.7) \qquad \sum_{C} e\{-\sigma(CDI(n,t;u))\} = \sum_{C_1} e\{-\sigma(D_1 C_1)\} \sum_{C_2} e\{-\sigma(D_2 C_2)\}.$$

In order for (3.6) to represent the value of the inner sum of (3.3), we must have C_1 of a fixed rank. Hence, we divide the sum over C_1 into successive sums over all $C_1 = C_1(t, r; z_1)$, $0 \leq z_1 \leq (t, r)$, and by (2.4) have

$$(3.8) \qquad \sum_{C_1} e\{-\sigma(D_1 C_1)\} = \sum_{z_1=0}^{(t,r)} H(D_1, z_1) = \sum_{z_1=0}^{(t,r)} H(r, t, u; z_1).$$

The value in (3.6) is independent of rank C_2 so we have

$$(3.9) \qquad \sum_{C_2} e\{-\sigma(D_2 C_2)\} = \begin{cases} q^{t(n-r)}, & D_2 = 0, \\ 0, & D_2 \neq 0. \end{cases}$$

Theorem II follows from (3.9), since the value of (3.7) and thus the value of (3.3) is not zero if and only if $D_2 = 0$, and $D_2 = 0$ if and only if $\delta_{ij} = 0$, $r < i \leq n$, $1 \leq j \leq u$, where $D = (\delta_{ij})$.

If we now substitute (3.6) and the value of the left sum in (3.7) which is given by (3.8) and (3.9) into (3.3) Theorem I is established.

4. THE GENERAL THEOREM.—We may now prove

THEOREM III.—*Let a be an integer > 1; $n, s, t, s_1, \cdots, s_{a-1}$ represent arbitrary positive integers; r, u represent arbitrary integers with $r \geq u \geq 0$; $A = A(n, s; r)$, $B = B(n, t; u)$, $X_1 = X_1(s, s_1)$, $X_i = X_i(s_{i-1}, s_i)$ for $1 < i < a$, $X_a = X_a(s_{a-1}, t)$. Then the number $N = N(a, s, t, s_i, r, u)$ of solutions in F of (1.1), if any exist, is given by*

$$N = q^{t(s_{a-1}-r)+ss_1+s_1s_2+\cdots+s_{a-2}s_{a-1}} \sum_{z_{a-1}=0}^{(r,t)} H(r, t, u; z_{a-1}) q^{-z_{a-1}s_{a-1}} \times$$

$$\times \prod_{i=2}^{a-1} \sum_{z_{a-i}=0}^{(z_{a-i+1}, s_{a-i+1})} g(z_{a-i+1}, s_{a-i+1}; z_{a-i}) q^{-z_{a-i}s_{a-i}},$$

with $(x, y) =$ minimum of x and y, $H(r, t, u; z_{a-1})$ defined by (2.5); $g(m, k; y)$ defined by (2.6); and we define $H(0, t, 0; 0) = g(0, k; 0) = 1$; the product over i is defined to be 1 for $a = 2$; $s_{a-2} = 0$ for $a = 2$.

During the proof of Theorem III, we will find that the solvability criterion for the general equation is exactly the same as for the case $a = 2$. Hence, we state

THEOREM IV.—*A necessary and sufficient condition for the solvability of (1.1) is obtained by replacing (3.1) by (1.1) in Theorem II.*

Proof.—We prove theorem III by induction for all $a > 1$. The case for $a = 2$ is proven in Theorem I, so we suppose Theorem III is valid for $a = k - 1$, and consider $a = k \geq 3$. By proceeding as in Theorem I, we

obtain an equation corresponding to (3.3) which represents N_k = number of solutions of (1.1) for $a = k$ as

$$N_k = q^{-nt} \sum_{C} e\{-\sigma(DI(n, t; u)C\} \sum_{Y_1, \cdots, Y_k} e\{\sigma(I(n, s; r)Y_1 \cdots Y_k C\}, \tag{4.1}$$

with $C = C(t, n)$. If we write $C = [C_1, C_2]$, with $C_1 = C_1(t, r; z_{k-1})$, $C_2 = C_2(t, n-r)$, then it is clear the value of the sum over C in (4.1) is given by (3.8) and (3.9) to be

$$\sum_{C} e\{-\sigma(DI(n, t; u)C\} = q^{t(n-r)} \sum_{z_{k-1}=0}^{(t,r)} H(r, t, u; z_{k-1})\, \psi(D_2) \tag{4.2}$$

with $\psi(D_2) = 1$ or 0 depending on $D_2 = 0$ or $D_2 \neq 0$ where D_2 is as defined below (3.6). Hence, the solvability criterion for the general case is exactly as stated in Theorem IV.

By noting (2.3) and the properties of trace, we may evaluate the inner sum in (4.1) as

$$\sum_{Y_1, \cdots, Y_k} e\{\sigma(CI(n, s; r)Y_1 \cdots Y_k\} = \begin{cases} q^{ts_{k-1}}, & CI(n, s; r)Y_1 \cdots Y_{k-1} = 0, \\ 0, & CI(n, s; r)Y_1 \cdots Y_{k-1} \neq 0. \end{cases} \tag{4.3}$$

We now need the number of solutions of the equation $CI(n, s; r)Y_1 \cdots \cdots Y_{k-1} = 0$. If C is as defined above and $Y_1 = \mathrm{col}(Y_{11}, Y_{12})$ with $Y_{11} = Y_{11}(r, s_1)$, $Y_{12} = Y_{12}(s-r, s_1)$, this number is given by

$$q^{(s-r)s_1} \bar{N}, \tag{4.4}$$

where $\bar{N}$ = number of solutions of $C_1 Y_{11} \cdots Y_{k-1} = 0$. Since the constant in this equation is zero, the solvability condition is satisfied, so that $\bar{N}$ is given our induction hypothesis to be

$$\left.\begin{aligned} \bar{N} &= q^{s_{k-1}(s_{k-2}-z_{k-1})+rs_1+\cdots+s_{k-3}s_{k-2}} \times \\ &\times \sum_{z_{k-2}=0}^{(z_{k-1}, s_{k-1})} H(z_{k-1}, s_{k-1}, 0; z_{k-2})\, q^{-z_{k-2}s_{k-2}} \times \\ &\times \prod_{i=2}^{k-2} \sum_{z_{k-i-1}=0}^{(z_{k-i}, s_{k-i})} g(z_{k-i}, s_{k-i}; z_{k-i-1})\, q^{-z_{k-i-1}s_{k-i-1}}, \end{aligned}\right\} \tag{4.5}$$

where $s_{k-3} = 0$ if $k = 3$. If we recall that $H(z_{k-1}, s_{k-1}, 0; z_{k-2}) = g(z_{k-1}, s_{k-1}, z_{k-2})$, and combine the results of (4.1) through (4.5), we have

$$N_k = q^{t(s_{k-1}-r)+ss_1+\cdots+s_{k-2}s_{k-1}} \sum_{z_{k-1}=0}^{(r,t)} H(r, t, u; z_{k-1})\, q^{z_{k-1}s_{k-1}} \times$$

$$\times \prod_{i=2}^{k-2} \sum_{z_{k-i}=0}^{(z_{k-i+1}, s_{k-i+1})} g(z_{k-i+1}, s_{k-i+1}; z_{k-i})\, q^{-z_{k-i}s_{k-i}}.$$

But this is exactly Theorem III for $a = k$ so that the theorem is proven for all $a \geq 2$.

REFERENCES.

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

[2] L. CARLITZ, *Simultaneous representations in quadratic and linear forms over* $GF[q, x]$, « Duche Mathematical Journal », *30*, 259–270 (1963).

[3] J. H. HODGES, *Representations by bilinear forms in a finite field*, « Duke Mathematical Journal », *22*, 497–510 (1955).

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

[5] J. H. HODGES, *A bilinear matrix equation over a finite field*, « Duke Mathematical Journal », *31*, 661–666 (1964).

[6] G. LANDSBERG, *Ueber eine Anzahlbestimmung und eine damit zusammenhängende Reihe.*