Atti Accademia Nazionale dei Lincei

Classe Scienze Fisiche Matematiche Naturali

Rendiconti

John H. Hodges

Note on a linear matrix equation over a finite field

Atti della Accademia Nazionale dei Lincei. Classe di Scienze Fisiche, Matematiche e Naturali. Rendiconti, Serie 8, Vol. **63** (1977), n.5, p. 304–309.

Accademia Nazionale dei Lincei

<http://www.bdim.eu/item?id=RLINA_1977_8_63_5_304_0>

Algebra. — *Note on a linear matrix equation over a finite field.* Nota di JOHN H. HODGES, presentata (*) dal Socio E. MARTINELLI a nome del compianto Socio B. SEGRE.

RIASSUNTO. — Si dà un metodo per determinare il numero N_n delle soluzioni $X_1, X_2, \cdots, X_n$ dell'equazione matriciale (1.1) su di un campo finito, con l'intervento di certe somme esponenziali, e lo si sviluppa completamente per $n = 2, 3$ e per speciali matrici A, C.

1. INTRODUCTION AND NOTATION

Let F denote the finite field of $q = p^d$ elements for an arbitrary prime p and integer $d \geqq 1$. Except as indicated, lower case Greek letters will denote elements of F and Roman capital letters will denote matrices over F. $A(s, m)$ denotes an $s \times m$ matrix and $A(s, m; \rho)$ a matrix of the same size having rank ρ. In this note we consider the problem of determining the number $N = N_n$ of solutions $X_1, \cdots, X_n$ over F of the matrix equation

$$A_1 X_1 C_1 + \cdots + A_n X_n C_n = B, \tag{1.1}$$

for given $B = B(s, t)$ and $A_i = A_i(s, m_i; \rho_i)$, $C_i = C_i(f_i, t; \nu_i)$ all $1 \leqq i \leqq n$ where $X_i = X_i(m_i, f_i)$ all $1 \leqq i \leqq n$. The problem was solved for the case $n = 1$ by the Author [1] a number of years ago, using exponential sums. The result in this case can also be easily obtained directly by appropriate partitioning of the matrices involved.

In the present Note, the numbers of solutions of (1.1) are found for $n = 2, 3$ for certain special matrices A_i and C_i. Although the direct method could be used in these cases, the results here are obtained by the use of exponential sums. For $n = 2$ we show that this approach leads in a natural way, for the A_i and C_i of arbitrary rank, to another as yet unsolved matrix problem which can be avoided by restricting the A_i and C_i as indicated in sections 3 and 4. The same techniques could be used to consider (1.1) for arbitrary $n > 1$, but it appears that the general results will be quite complicated and the author has not worked out the solution in case $n > 3$. If for all i, C_i is the identity matrix of order t so that $f_i = \nu_i = t$, then (1.1) and the results in this Note essentially reduce to an equation and its solution given previously by Porter [2].

(*) Nella seduta del 18 novembre 1977.

2. PRELIMINARIES

In addition to the notation introduced above, we let $I(s, m; \rho)$ denote the $s \times m$ matrix having the identity matrix of order ρ in its upper left-hand corner and zeros elsewhere and I_s denote the identity matrix of order s.

If $A = (\alpha_{ij})$ is square, then $\sigma(A) = \Sigma_i \alpha_{ii}$ is the *trace* of A and σ satisfies $\sigma(A + B) = \sigma(A) + \sigma(B)$ and $\sigma(AC) = \sigma(CA)$, when σ and the indicated operations are defined

For $\alpha \in F$, we define

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

from which it follows that $e(\alpha + \beta) = e(\alpha)\, e(\beta)$ and

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

where the sum is over all $\gamma \in F$. Then, using (2.2) we can prove that if $Y = Y(s, t)$,

$$\sum_{D} e\{\sigma(YD)\} = \begin{cases} q^{st} & (Y = O), \\ 0 & (Y \neq O), \end{cases} \tag{2.3}$$

where the summation is over all $D = D(t, s)$.

3. THE CASE $n = 2$

Let P_i, Q_i, R_i, T_i be nonsingular matrices of appropriate sizes such that for $i = 1, 2$,

$$P_i A_i Q_i = I(s, m_i; \rho_i) \quad \text{and} \quad R_i C_i T_i = I(f_i, t; \nu_i) . \tag{3.1}$$

Then for $n = 2$, (1.1) is equivalent to the equation

$$\begin{aligned} H = I(s, m_1; \rho_1)\, Y_1\, I(f_1, t; \nu_1)\, T_0 + \\ + P_0\, I(s, m_2; \rho_2)\, Y_2\, I(f_2, t; \nu_2) = P_1 B T_2 , \end{aligned} \tag{3.2}$$

where $Y_i = Q_i^{-1} X_i R_i^{-1}$ for $i = 1, 2$, $T_0 = T_1^{-1} T_2$ and $P_0 = P_1 P_2^{-1}$. In view of (2.3) and other properties of σ, the number N_2 of solutions Y_1, Y_2 of (3.2) is given by

$$\begin{aligned} N_2 &= q^{-st} \sum_{Y_1, Y_2} \sum_{D} e\{\sigma((H - P_1 B T_2) D)\} \\ &= q^{-st} \sum_{D} e\{-\sigma(P_1 B T_2 D)\} \times S_1(D) \times S_2(D) , \end{aligned} \tag{3.3}$$

where the summations are independently over all $D = D(t, s)$, $Y_1 = Y_1(m_1, f_1)$ and $Y_2 = Y_2(m_2, f_2)$ and

$$S_1(D) = \sum_{V_1} e\{\sigma(I(f_1, t; \nu_1) T_0 DI(s, m_1; \rho_1) Y_1)\}$$

$$S_2(D) = \sum_{V_2} e\{\sigma(I(f_2, t; \nu_2) DP_0 I(s, m_2; \rho_2) Y_2)\}.$$

By (2.3), for a given D in (3.3), the product of the two inner sums $S_1(D)$ and $S_2(D)$ will be zero unless the coefficients of both Y_1 and Y_2 are zero. If we define $T_0 D = (\tau_{ij})$ and $DP_0 = (\pi_{ij})$ for $1 \leqq i \leqq t$, $1 \leqq j \leqq s$ and multiply out the coefficients of Y_1 and Y_2 in $S_1(D)$ and $S_2(D)$, respectively, we find that

$$(3.4) \quad S_1(D) S_2(D) = \begin{cases} q^{m_1 f_1 + m_2 f_2}, & \text{if (1) } \tau_{ij} = 0, \text{ all } 1 \leqq i \leqq \nu_1 \text{ and } 1 \leqq j \leqq \rho_1, \\ & \text{and (2) } \pi_{ij} = 0, \text{ all } 1 \leqq i \leqq \nu_2 \text{ and } 1 \leqq j \leqq \rho_2, \\ 0 & \text{, otherwise.} \end{cases}$$

If T_0, D and P_0 are partitioned into submatrices as $T_0 = (T_{uv})$, $D = (D_{uv})$, $P_0 = (P_{uv})$ for $u = 1, 2$ and $v = 1, 2$ with $T_{11} = T_{11}(\nu_1, \nu_2)$, $T_{12} = T_{12}(\nu_1, t - \nu_2)$, $T_{21} = T_{21}(t - \nu_1, \nu_2)$ $T_{22} = T_{22}(t - \nu_1, t - \nu_2)$ and $D_{11} = D_{11}(\nu_2, \rho_1)$, $D_{12} = D_{12}(\nu_2, s - \rho_1)$, $D_{21} = D_{21}(t - \nu_2, \rho_1)$, $D_{22} = D_{22}(t - \nu_2, s - \rho_1)$ and $P_{11} = P_{11}(\rho_1, \rho_2)$, $P_{12} = P_{12}(\rho_1, s - \rho_2)$, $P_{21} = P_{21}(s - \rho_1, \rho_2)$, $P_{22}(s - \rho_1, s - \rho_2)$, then the conditions (1) and (2) in (3.4) under which the product is nonzero can be written as

$$(3.5) \quad \begin{cases} (1) \quad T_{11} D_{11} + T_{12} D_{21} = 0 \\ (2) \quad D_{11} P_{11} + D_{12} P_{21} = 0. \end{cases}$$

If we also partition $B_0 = P_1 BT_2 = (\beta_{ij})$, $1 \leqq i \leqq s$, $1 \leqq j \leqq t$, as $B_0 = (B_{uv})$ for $u = 1, 2$ and $v = 1, 2$ with $B_{11} = B_{11}(\rho_1, \nu_2)$, $B_{12} = B_{12}(\rho_1, t - \nu_2)$, $B_{21} = B_{21}(s - \rho_1, \nu_2)$, $B_{22} = B_{22}(s - \rho_1, t - \nu_2)$, then for arbitrary D as partitioned above

$$(3.6) \quad e\{-\sigma(B_0 D)\} = e\{-\sigma(B_{11} D_{11})\} e\{-\sigma(B_{12} D_{21})\} \\ e\{-\sigma(B_{21} D_{12})\} e\{-\sigma(B_{22} D_{22})\}.$$

Therefore, in order to determine N_2 by evaluating the sums in (3.3) it would be necessary to sum the product on the right side of (3.6) over all D for which D_{22} is arbitrary, but D_{11}, D_{12} and D_{21} satisfy the equations (3.5). This implies that in order for $N_2 \neq 0$ it is necessary (but likely not sufficient) that $B_{22} = 0$, that is, $\beta_{ij} = 0$ for all $i > \rho_1$ and $j > \nu_2$.

Because of the difficulty in carrying out the summation in the general case (it is not clear just how one would proceed to do this), we examine the simpler problem obtained by assuming that in (3.1) $P_1 = P_2 = I_s$, so

that $P_0 = I_s$, and $T_1 = T_2 = I_t$, so that $T_0 = I_t$. Then $D = (\delta_{ij}) = DP_0 = T_0 D$ so that conditions (1), (2) in (3.4) become conditions on the elements $\delta_{ij} = \tau_{ij} = \pi_{ij}$ of D itself. Without loss of generality, we may assume that $\nu_1 \leqq \nu_2$. Then there are two mutually exclusive cases to be considered:

Case 1. $\rho_1 \leqq \rho_2$. In this case condition (2) on D in (3.4) implies condition (1). If we take (possibly) different partitions of $D = (D_{uv})$ and $B_0 = B = (B_{uv})$ from those above with $D_{11} = D_{11}(\nu_2, \rho_2)$, $D_{12} = D_{12}(\nu_2, s-\rho_2)$, $D_{21} = D_{21}(t-\nu_2, \rho_2)$, $D_{22} = D_{22}(t-{}_2\nu, s-\rho_2)$ and $B_{11} = B_{11}(\rho_2, \nu_2)$, $B_{12} = B_{12}(\rho_2, t-\nu_2)$, $B_{21} = B_{21}(s-\rho_2, \nu_2)$, $B_{22} = B_{22}(s-\rho_2, t-\nu_2)$, then (3.6) still is valid and condition (2) on D is equivalent to $D_{11} = O$. Substituting (3.4) into (3.3) gives, since all terms vanish for which $D_{11} \neq O$,

$$(3.7)\quad N_2 = q^{-st+m_1f_1+m_2f_2} \sum_{D_{21}, D_{12}, D_{22}} e\{-\sigma(B_{12}D_{21})\}\, e\{-\sigma(B_{21}D_{12})\}\, e\{-\sigma(B_{22}D_{22})\},$$

where the sum is over all D_{21}, D_{12}, D_{22} independently. In view of (2.3) this sum is equal to zero unless $B_{12} = O$, $B_{21} = O$ and $B_{22} = O$, when its value is q^w, where $w = \rho_2(t-\nu_2) + \nu_2(s-\rho_2) + (s-\rho_2)(t-\nu_2)$. Substituting this result into (3.7) and simplifying gives.

THEOREM 1. *If* $n = 2$ *in* (1.1) *with* $\nu_1 \leqq \nu_2$ *and* $\rho_1 \leqq \rho_2$ *and there exist nonsingular matrices* Q_i *and* R_i *such that* $A_i Q_i = I(s, m_1; \rho_i)$ *and* $R_i C_i = I(f_i, t; \nu_i)$ *for* $i = 1, 2$, *then the number of solutions of the matrix equation over* F *is*

$$(3.8)\qquad N_2 = q^{m_1f_1+m_2f_2-\rho_2\nu_2}\, h(B),$$

where if $B = (\beta_{ij})$ *for* $1 \leqq i \leqq s$, $1 \leqq j \leqq t$, *then* $h(B) = 1$ *if* $\beta_{ij} = 0$ *for all* i, j *such that* $i > \rho_2$ *or* $j > \nu_2$, *and* $h(B) = 0$ *otherwise.*

Case 2. $\rho_1 > \rho_2$. Let D and B be partitioned as indicated preceding (3.6) and B_{11} and D_{11} be further partitioned as $B_{11} = (E_{uv})$ and $D_{11} = (G_{uv})$ for $u = 1, 2$ and $v = 1, 2$ with $E_{11} = E_{11}(\rho_2, \nu_1)$, $E_{12} = E_{12}(\rho_2, \nu_2 - \nu_1)$, $E_{21} = E_{21}(\rho_1 - \rho_2, \nu_1)$, $E_{22} = E_{22}(\rho_1 - \rho_2, \nu_2 - \nu_1)$ and $G_{11} = G_{11}(\nu_1, \rho_2)$, $G_{12} = G_{12}(\nu_1, \rho_1 - \rho_2)$, $G_{21} = G_{21}(\nu_2 - \nu_1, \rho_2)$, $G_{22} = G_{22}(\nu_2 - \nu_1, \rho_1 - \rho_2)$. Then it is easily seen that conditions (1), (2) on D in (3.4) are equivalent to $G_{11} = O$, $G_{12} = O$ and $G_{21} = O$ and for D satisfying these conditions, $e\{-\sigma(B_{11}D_{11})\} = e\{-\sigma(E_{22}G_{22})\}$. Therefore, using (3.4) in (3.3) gives in this case

$$(3.9)\qquad N_2 = q^{-st+m_1f_1+m_2f_2} \sum_{E_{22}} e\{-\sigma(E_{22}G_{22})\} \times \Sigma,$$

where Σ is a sum of the form of the sum in (3.7), but for (possibly) different partitions of B and D. Applying the same arguments as in the proof of Theorem 1 leads to

THEOREM 2. *If* $n = 2$ *in* (1.1) *with* $\nu_1 \leqq \nu_2$ *and* $\rho_1 > \rho_2$ *and there exist nonsingular matrices* Q_i *and* R_i *such that* $AQ_i = I(s, m_i; \rho_i)$ *and* $R_i C_i = I(f_i, t; \nu_i)$ *for* $i = 1, 2$, *then the number of solutions of the matrix equation over* F *is*

$$N_2 = q^{m_1 f_1 + m_2 f_2 - \rho_2 \nu_2 - \rho_1 \nu_1 + \rho_2 \nu_1} h(B), \tag{3.10}$$

where if $B = (\beta_{ij})$ *for* $1 \leqq i \leqq s$, $1 \leqq j \leqq t$, *then* $h(B) = 1$, *if* $\beta_{ij} = 0$ *for all* i, j *such that* $i > \rho_1$ *or* $j > \nu_2$ *or* $\rho_2 < i \leqq \rho_1$ *and* $\nu_1 < j \leqq \nu_2$, *and* $h(B) = 0$ *otherwise.*

4. THE CASE $n = 3$

For the sake of brevity, the results in this case will be simply stated without proofs. The proofs are quite similar to those given for Theorems 1 and 2 but somewhat more complicated.

THEOREM 3. *If* $n = 3$ *in* (1.1) *and there exist nonsingular matrices* Q_i *and* R_i *such that* $A_i Q_i = I(s, m_i; \rho_i)$ *and* $R_i C_i = I(f_i, t; \nu)$ *for* $i = 1, 2, 3$, *then the number of solutions of the matrix equation over* F *is* $q^e h(B)$, *where, if* $B = (\beta_{ij})$ *for* $1 \leqq i \leqq s$, $1 \leqq j \leqq t$, *then* e *and* $h(B)$ *are defined as follows*:

Let $M = \max(\rho_1, \rho_2, \rho_3)$ *and* $K = \max(\nu_1, \nu_2, \nu_3)$.

Case 1. For some r, $M = \rho_r$ and $K = \nu_r$. Then

$$e = m_1 f_1 + m_2 f_2 + m_3 f_3 - MK,$$

$$h(B) = \begin{cases} 1, & \text{if } \beta_{ij} = 0 \quad \text{for all } i, j \text{ such that } i > M \text{ or } j > K, \\ 0, & \text{otherwise.} \end{cases}$$

Case 2. For all r, if $\rho_r = M$, then $\nu_r < K$.

Let $k = \max\{\nu_r \mid \rho_r = M\}$ and $m = \max\{\rho_r \mid \nu_r = K\}$.

(*a*) For some r, $m < \rho_r < M$ and $k < \nu_r < K$. Then

$$e = m_1 f_1 + m_2 f_2 + m_3 f_3 - \rho_r \nu_r - k(M - \rho_r) - m(K - \nu_r),$$

$$h(B) = \begin{cases} 1, & \text{if } \beta_{ij} = 0 \quad \text{for all } i, j \text{ such that } i > M \text{ or } j > K \\ & \qquad \text{or } \rho_r < i \leqq M \text{ and } k < j \leqq \nu_r \\ & \qquad \text{or } m < i \leqq \rho_r \text{ and } \nu_r < j \leqq K \\ & \qquad \text{or } \rho_r < i \leqq M \text{ and } \nu_r < j \leqq K, \\ 0, & \text{otherwise.} \end{cases}$$

(*b*) No r exists as in (*a*). Then

$$e = m_1 f_1 + m_2 f_2 + m_3 f_3 + mk - m\mathrm{K} - k\mathrm{M}$$

$$h(\mathrm{B}) = \begin{cases} 1, \text{ if } \beta_{ij} = 0 \text{ for all } i, j \text{ such that } i > \mathrm{M} \text{ or } j > \mathrm{K} \\ \qquad\qquad \text{or } m < i \leqq \mathrm{M} \text{ and } k < j \leqq \mathrm{K}, \\ 0, \text{ otherwise.} \end{cases}$$

REFERENCES

[1] JOHN H. HODGES (1965) – *The matrix equation* AXC = B *over a finite field*, « Riv. Mat. Univ. Parma », (2) *6*, 79–81.

[2] A. DUANE PORTER (1973) – *The matrix equation* $A_1 X_1 + \cdots + A_m X_m = B$ *in* GF(q), « J. Natur. Sci. and Math. », *13* (1), 115–124.