Riv. Mat. Univ. Parma (2) 6 (1965), 79-81

JOHN H. HODGES (*)

The Matrix Equation $AXC = B$ over a Finite Field. (**)

1. - Introduction.

Let $GF(q)$ denote the finite field of $q = p^n$ elements. In this paper we consider the problem of determining the number of $m \times f$ matrices X over $GF(q)$ which satisfy the equation

$$AXC = B, \tag{1.1}$$

where A, C, B are matrices over $GF(q)$, A is $s \times m$ of rank ϱ, C is $f \times t$ of rank ν and B is $s \times t$. In § 3, it is shown that if the equation has any solutions, their number is q^z, where $z = mf - \varrho\nu$. A necessary and sufficient condition for existence of solutions is also obtained. The case where $C = I_t$, the identity of order t, was considered by the author in a paper [**1**] some years ago.

2. - Notation and preliminaries.

Except as indicated, lower case Greek letters will denote elements of $GF(q)$, $q = p^n$, p an arbitrary prime. Except as indicated, italic capitals will denote matrices over $GF(q)$. $A(s, m)$ denotes an $s \times m$ matrix and $A(s, m; \varrho)$ a matrix of the same size having rank ϱ. If $A = A(s, m; \varrho)$ it is well known [**2**, Theorem 3-7] that there exist (not uniquely) nonsingular $P(s, s)$ and $Q(m, m)$ such that $PAQ = I(s, m; \varrho)$, the $s \times m$ matrix having the identity matrix of order ϱ in its upper left-hand corner and zeros elsewhere.

(*) Indirizzo: Department of Mathematics, University of Colorado, Boulder, Colorado 80302, U. S. A..

(**) The work on this paper was supported by National Science Foundation Research Grant GP-2542. — Ricevuto: 31 - X - 1964.

If $A = (\alpha_{ij})$ is square, then $\sigma(A) = \sum_i \alpha_{ii}$ is the *trace* of A. It is easy to show that when the indicated operations are defined, then $\sigma(A+B) = \sigma(A) + \sigma(B)$ and $\sigma(AC) = \sigma(CA)$.

For $\alpha \in GF(q)$ we define

$$e(\alpha) = e^{2\pi i t(\alpha)/p}, \qquad t(\alpha) = \alpha + \alpha^p + \dots + \alpha^{p^{n-1}}, \tag{2.1}$$

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 $\gamma \in GF(q)$. Now, using (2.2) we can show that if $Y = Y(s,\ t)$ then

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

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

3. - The nnmber $N(A,C,B)$.

Let $N = N(A,\ C,\ B)$ denote the number of solutions $X(m,\ f)$ of the matrix equation (1.1). In view of (2.3) we have

$$\begin{aligned} N(A,\ C,\ B) &= q^{-st} \sum_{X} \sum_{D} e\{\sigma[(AXC - B)D]\} \\ &= q^{-st} \sum_{D} e\{-\sigma(BD)\} \sum_{X} e\{\sigma(AXCD)\}, \end{aligned} \tag{3.1}$$

where the summations are independently over all $D = D(t,\ s)$ and $X = X(m,\ f)$. Let $P,\ Q,\ R,\ T$ be any fixed nonsingular matrices of appropriate sizes such that

$$\begin{cases} PAQ = I(s,\ m;\ \varrho) & \text{so} \quad A = P^{-1} I(s,\ m;\ \varrho)\, Q^{-1} \\ RCT = I(f,\ t;\ \nu) & \text{so} \quad C = R^{-1} I(f,\ t;\ \nu)\, T^{-1}. \end{cases} \tag{3.2}$$

If we substitute into (3.1) the values of A and C given by (3.2), let $E = E(t,\ s) = T^{-1}DP^{-1}$ so that $D = TEP$, let $Y = Y(m,\ f) = Q^{-1}XR^{-1}$, and simplify the resulting expression by use of the property $\sigma(AB) = \sigma(BA)$, we get

$$N = q^{-st} \sum_{E(t,\ s)} e\{-\sigma(PBTE)\} \sum_{Y(m,\ f)} e\{\sigma[I(f,\ t;\ \nu)\, EI(s,\ m;\ \varrho) Y]\}. \tag{3.3}$$

Let $E(t,\ s)$ be partitioned as $E = (E_{ij})$ for $i,\ j = 1,\ 2$, where $E_{11} = E_{11}(\nu,\ \varrho)$, $E_{12} = E_{12}(\nu,\ s - \varrho)$, $E_{21} = E_{21}(t - \nu,\ \varrho)$ and $E_{22} = E_{22}(t - \nu,\ s - \varrho)$. For fixed E in (3.3), by (2.3), the inner sum over Y is equal to q^{mf} if the coefficient $I(f, t; \nu)\, EI(s, m; \varrho)$ of Y is equal to zero. Otherwise the sum itself is equal to zero. By appropriately partitioning $I(f, t; \nu)$ and $I(s, m; \varrho)$ and computing the product by use of multiplication of submatrices, it is easy to show that

$$I(f, t; \nu)\, EI(s, m; \varrho) = 0, \quad \text{if and only if } E_{11} = 0\,. \tag{3.4}$$

Using this fact in (3.3) we have

$$N = q^{mf-st} \sum_{E(t,\, s)}{}' e\{-\sigma(PBTE)\}, \tag{3.5}$$

where the prime indicates that the sum is restricted to those $E(t, s)$ for which, in the partitioning described above, $E_{11} = 0$.

If we partition $B_0 = B_0(s, t) = PBT$ as $B_0 = (B_{ij})$ for $i, j = 1, 2$, where $B_{11} = B_{11}(\varrho, \nu)$, $B_{12} = B_{12}(\varrho, t-\nu)$, $B_{21} = B_{21}(s-\varrho, \nu)$ and $B_{22} = B_{22}(s-\varrho, t-\nu)$, compute the product B_0E by use of multiplication of submatrices, and finally use properties of σ and $e(\alpha)$ given in § 2, we find that for E as in (3.5),

$$e\{-\sigma(B_0\, E)\} = e\{-\sigma(B_{12}\, E_{21})\}\, e\{-\sigma(B_{21}\, E_{12})\}\, e\{-\sigma(B_{22}\, E_{22})\}. \tag{3.6}$$

If we substitute (3.6) into (3.5) and sum independently over all E_{21}, E_{12}, E_{22} it follows from (2.3) that the sum over the restricted E is equal to q^w, where $w = \varrho(t-\nu) + \nu(s-\varrho) + (t-\nu)(s-\varrho)$, if all of $B_{12} = 0$, $B_{21} = 0$, $B_{22} = 0$, Otherwise the sum is equal to zero. Finally, if we use this information in (3.5) and simplify the exponent of q we obtain the

Theorem. *If $N(A, C, B)$ denotes the number of solutions of the matrix equation* (1.1) *over $GF(q)$ and P, Q, R, T are any fixed nonsingular matrices of appropriate sizes such that $PAQ = I(s, m; \varrho)$, $RCT = I(f, t; \nu)$, then*

$$N(A, C, B) = q^{mf-\varrho\nu}\, h(B_0), \tag{3.7}$$

where $B_0 = B_0(s, t) = PBT = (\beta_{ij})$ and $h(B_0) = 1$ if all $\beta_{ij} = 0$ for $i > \varrho$ or $j > \nu$, and otherwise $h(B_0) = 0$.

We note that this theorem contains a necessary and sufficient condition, in terms of B_0, for existence of solutions of equation (1.1). It can be shown directly that the property of B_0 in question does not depend upon the particular choice of the transforming matrices P, Q, R, T. For $C = I_t$, the identity of order t, (3.7) reduces to the result obtained previously [1, Theorem 1].

References.

[1] J. H. Hodges, *The matric equation $AX = B$ in a finite field,* Amer. Math. Monthly **53** (1956), 243-244.

[2] S. Perlis, *Theory of matrices,* Cambridge, Mass. 1952.

* * *