A BILINEAR MATRIX EQUATION OVER A FINITE FIELD

By John H. Hodges

1. Introduction. Let $GF(q)$ denote the finite field of $q = p^n$ elements. Let A be an $e \times f$ matrix and B be an $s \times t$ matrix of rank w over $GF(q)$. This paper is concerned with the problem of determining the number $N(A, B, k_1, k_2)$ of pairs U, V of matrices over $GF(q)$ such that

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

where U is $s \times e$ of rank k_1 and V is $f \times t$ of rank k_2. First (Theorem 1), a formula is proved which gives $N(A, B, k_1, k_2)$ as a sum involving the numbers $N(I_m, B_0, r_1, r_2)$, where $m = \text{rank } A$ and I_m is the identity matrix of order m, B_0 is a canonical form for B under equivalence of matrices and r_1, r_2 run from w to $\min(m, k_1)$ and $\min(m, k_2)$, respectively. Then (Theorem 2) the number $N(I_m, B_0, r_1, r_2)$ is found in terms of certain exponential sums $H(s, t, w; z)$ whose explicit values are known [1; §8]. Theorem 2 is proved by expressing the desired number as a double finite trigonometric sum which is then evaluated. Together with the formula for $H(s, t, w; z)$, Theorems 1 and 2 serve to give $N(A, B, k_1, k_2)$ explicitly.

The total number $N_t^s(A, B)$ of solutions U, V of (1.1) of arbitrary rank has been determined previously by the writer [1; Theorem 3]. This number is clearly the sum of $N(A, B, k_1, k_2)$ over all k_1 and k_2 such that $w \leq k_1 \leq \min(s, e)$ and $w \leq k_2 \leq \min(f, t)$.

2. Notation and preliminaries. Throughout this paper Roman capitals A, B, $\cdots$ will denote matrices over $GF(q)$, $q = p^n$, except as indicated. $A(e, f)$ will denote a matrix of e rows and f columns and $A(e, f; m)$ a matrix of the same size which has rank m. In particular, $I(e, f; m)$ will denote the matrix of e rows and f columns which has I_m, the identity of order m, in its upper left-hand corner and zeros elsewhere. If $A = A(e; f; m)$, then there exist non-singular matrices $P(e, e)$ and $Q(f, f)$ such that $PAQ = I(e, f; m)$.

If $A = (\alpha_{ij})$ is square, then $\sigma(A) = \sum_i \alpha_{ii}$ is the *trace* of A. It is easily shown that $\sigma(A + B) = \sigma(A) + \sigma(B)$ and for AC square, $\sigma(AC) = \sigma(CA)$.

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

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

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

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

Received September 16, 1963. The work on this paper has been supported by National Science Foundation Research Grant G19894.