AN HERMITIAN MATRIX EQUATION OVER A FINITE FIELD

BY JOHN H. HODGES

1. Introduction. Let $GF(q)$ denote the finite field of $q = p^n$ elements, p an odd prime. Let A and B be Hermitian matrices over $GF(q^2)$ of order e, rank m and order t, rank r, respectively. In this paper the number $N(A, B, k)$ of $e \times t$ matrices U of rank k over $GF(q^2)$ is determined which satisfy the equation

$$U^*AU = B, \tag{1.1}$$

where the asterisk denotes *conjugate* (with respect to $GF(q)$) *transpose*. First (Theorem 1), a formula is obtained which gives $N(A, B, k)$ as a sum involving the numbers $N(I_m, B_0, s)$, where I_m denotes the identity of order m, $B_0 = \text{diag}(B_1, 0)$ is Hermitely congruent to B so that B_1 is nonsingular of order r, and s runs from r to $\min(m, t, k)$. Then (Theorem 2), the number $N(I_m, B_0, s)$ is found in terms of certain exponential sums $H(t, r, z)$ whose explicit values have been found previously by L. Carlitz and the author [3]. Theorem 2 is proved by expressing the desired number as a certain finite trigonometric sum which is then evaluated. Together with the formulas for $H(t, r, z)$, Theorems 1 and 2 serve to give $N(A, B, k)$ explicitly.

This paper is motivated by the paper [3] by Carlitz and the author in which they determined the *total* number $N_t(A, B)$ of solutions U of (1.1) of arbitrary rank when $e = m$. For $e = m$, $N_t(A, B)$ is clearly the sum of $N(A, B, k)$ over all k such that $r \leq k \leq \min(m, t)$.

The skew analog of the problem treated here is already scheduled to appear [6] and the analogous symmetric and bilinear equations have been considered in separate papers [5] and [4], respectively. The symmetric equation is related to a paper [2] by L. Carlitz which is in part a generalization of some results of C. L. Siegel [8] on quadratic forms mod p.

2. Notation and preliminaries. Let $GF(q)$ denote the finite field of $q = p^n$ elements, p an odd prime. Let θ be an element of $GF(q^2)$ such that $\theta \notin GF(q)$ but $\theta^2 \in GF(q)$. Then if $\alpha \in GF(q^2)$, $\alpha = a + b\theta$ for $a, b \in GF(q)$. The element $\bar{\alpha} = a - b\theta$ of $GF(q^2)$ is called the *conjugate* of α.

Throughout this paper, except as indicated, Roman capitals will denote matrices over $GF(q^2)$. $X(m, t)$ will denote a matrix of m rows and t columns and $X(m, t; s)$ a matrix of the same size which has rank s. In particular, $I(m, t; s)$ will denote the $m \times t$ matrix which has I_s, the identity of order s, in its upper left-hand corner and zeros elsewhere. If $X = X(m, t; s)$, it is well known

Received November 3, 1964. The work on this paper has been supported by National Science Foundation Research Grant.