ORTHOGONAL SIMILARITY OF NORMAL MATRICES IN $GF(q)$

BY A. DUANE PORTER AND LESLIE ANN HANSON

1. Introduction. It is well known [6; Theorem 9–27] that over the real field every $n \times n$ normal matrix A is orthogonally similar to a matrix of the form diag $[D_1, \cdots, D_m, R]$, where

$$D_j = \begin{bmatrix} a_j & -b_j \\ b_j & a_j \end{bmatrix}, \qquad 1 \leq j \leq m,$$

$R = \text{diag}\ (r_{2m+1}, \cdots, r_n)$ with $a_j \pm b_j i$, $1 \leq j \leq m$, complex characteristic roots of A and r_t, $2m < t \leq n$, real characteristic roots. The proof of this theorem, as well as the proofs of other theorems concerning real normal matrices, fails over a finite field because (1) the sum of non-zero squares may equal zero, (2) for odd characteristic, exactly one-half of the nonzero elements do not have square roots in the field and (3) the characteristic roots of a matrix may lie in an extension field of degree greater than 2 over the field of elements of the matrix.

In view of the use of canonical forms for finding the number of solutions of matric equations over a finite field (for examples see [1], [2], [3], [4], [5]), it would seem desirable to have suitable canonical forms available under orthogonal similarity. Thus the purpose of this paper is to obtain such canonical forms for certain normal matrices. In [9] Porter and Adams obtained such canonical forms for certain symmetric matrices over a finite field. Also in [7] and [8] Porter obtained canonical forms under orthogonal similarity for other symmetric matrices and certain skew matrices. It is hoped this present paper will serve as a supplement to these three papers.

In Definitions 1.1 and 1.2 we define a characteristic K-vector and a K-normal matrix. Then in Theorems 1 and 2 we prove some preliminary properties about K-normal matrices. Theorem 3 states the main theorem on orthogonal similarity of normal matrices, and Theorems 4 and 5 give some interesting sidelights of the proof of Theorem 3.

2. Notation and definitions. Let $F = GF(q)$ be the finite field of $q = p^r$ elements, p odd. Elements of F will be denoted by lower case Roman letters a, b, a_i, b_i, f_i, h_i, u, and elements of any extension field of F will be denoted by c, d, c_i, c_{ij}, d_i, where in each case i, j represent any subscripts; r or r_i will denote eigenvalues of matrices; lower case Greek letters α, β, α_i, β_i, $\cdots$ will denote vectors except for θ which has a special value defined below; matrices will be denoted by Roman capitals A, B, D, D_i, P, Q except for P_i which is

Received February 12, 1970. Revision received January 8, 1971.