SIMILARITY AND ORTHOGONAL SIMILARITY IN A FINITE FIELD

By A. Duane Porter and John Adams

1. Introduction. A number of the well-known theorems concerning similarity and orthogonal similarity of real symmetric matrices do not hold in a finite field. For example, the usual proof that every real symmetric matrix is orthogonally similar to a diagonal matrix is not valid in a finite field. The proofs, valid for the real field, fail because (1) the sum of nonzero squares may equal zero and (2) for odd characteristic, exactly one half of the nonzero elements do not have square roots in the field.

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], [6], it would seem desirable to have suitable canonical forms available under similarity and orthogonal similarity. Hence the purpose of this paper is to obtain such canonical forms for certain symmetric matrices. In Definition 3.1, we define an R-Matrix and show in Theorems 3.4, 3.6, 4.2 that the properties of an R-Matrix are key properties for obtaining diagonal canonical forms under similarity and orthogonal similarity. Finally, Theorem 4.4 and Corollary 4.5 give fairly easy to apply sufficient conditions for orthogonal similarity to a diagonal matrix.

A number of the ideas for this paper were taken from a doctoral thesis written by the first-named author at the University of Colorado under the direction of Professor John H. Hodges.

2. Notation and preliminaries. Let $F = GF(q)$ be the finite field of $q = p^r$ elements, p odd. Elements of F will be denoted by the lower case Roman letters, a, b, a_i, b_i, v_i, w_i, and elements of any extension field of F will be denoted by c, d, f, c_i, d_i, f_i, h_i, where in each case i represents any subscript; r or r_i will denote eigenvalues of matrices; lower case Greek letters α, β, α_{ij}, β_{ij} $\cdots$, will denote vectors except for θ which has a special value defined below, and matrices will be denoted by Roman capitals A, B, C, D, P, Q, with I representing the identity matrix.

If $\theta \varepsilon GF(q^2)$, $\theta \not\varepsilon GF(q)$, $\theta^2 \varepsilon GF(q)$, then $a + b\theta \varepsilon GF(q^2)$ for all $a, b \varepsilon GF(q)$. By the *conjugate* of $f = a + b\theta$, we mean $\bar{f} = a - b\theta$, and by the conjugate of a matrix $A = (c_{ij})$ we mean the matrix $\bar{A} = (\bar{c}_{ij})$. We say a matrix $B = (b_{ij})$, $b_{ij} \varepsilon F$, is *symmetric* if $B = B'$, where the prime denotes transpose. A^* will denote $\bar{A}'$, i.e., the conjugate transpose of A. A square matrix P with elements from F such that $P'P = I =$ identity matrix will be called *orthogonal.* Two matrices A and B with elements from F will be said to be *orthogonally similar*

Received April 21, 1967; in revised form October 12, 1967.