THE CONFIGURATIONS OF VECTORS INVARIANT UNDER TRANSFORMATION BY CLASSES OF INVOLUTORY MATRICES OVER A FINITE FIELD

By John D. Fulton

1. Introduction. A nonsingular matrix A over a Galois field $GF(m)$ of order m is said to be involutory if $A^2 = I$ over $GF(m)$. Involutory matrices have application in the area of algebraic cryptography [3], [4], [6], [7], [8]. Levine [8] has noticed that the invariant vectors over $GF(2)$ under transformation by classes of involutory matrices over $GF(2)$ form balanced incomplete block designs. Ryser [11] defines a balanced incomplete block design BIBD(b, v, r, k, λ) with parameters b, v, r, k, and λ (three independent) to be a pair (X, Y) consisting of a set X, with exactly v distinct elements called varieties, and a subset Y of the set of all subsets of X, containing exactly b distinct subsets of X, X_1 , X_2 , $\cdots$, X_b , such that the following requirements are satisfied:

(1.1) Each X_i is a subset of X of order k.
(1.2) Each subset of X of order 2 is a subset of exactly λ of the sets of Y.
(1.3) The integers v, k, and λ satisfy $0 < \lambda$ and $k \leq v - 1$.

It is the purpose of this paper (as seen in Theorem 3.2) to determine the BIBD(b, v, r, k, λ) induced by classes of involutory matrices over $GF(m)$, where $m = p^u$ for p a prime and u a positive integer. As a sidelight to this determination, the enumeration of involutory matrices over finite fields is related through Theorem 4.1 to the enumeration of certain subspaces of projective geometries which can be coordinatized by the elements of Galois fields. Table 5.1 and Table 5.2 contain BIBD(b, v, r, k, λ) induced by involutory matrices over $GF(m)$ for a case in which m is odd and for a case in which m is even, respectively.

2. Review of literature. Implicit in the enumeration by Hodges [5] of involutory matrices over a finite field is the concept of signature of an involutory matrix. Levine and Nahikian [9] gave the following definitions for the signature of an involutory matrix.

Definition 2.1. An $n \times n$ involutory matrix A over $GF(m)$, m odd, is involutory of signature s if and only if A is similar to one of the $n + 1$ matrices

$$J(s) = \text{Diag}\,(I_s\ , -I_{n-s}), \qquad s = 0, 1, \cdots, n,$$

where for $k = s$ or $k = n - s$, I_k is the k by k identity matrix over $GF(m)$.

Received April 1, 1966. Research sponsored by the U. S. Atomic Energy Commission under contract with the Union Carbide Corporation