DISTRIBUTION OF CYCLIC MATRICES IN A FINITE FIELD

By E. R. Berlekamp

In this paper, we obtain a generating function which enumerates by rank the cyclic $n \times n$ matrices over any finite field. This result complements similar enumerations of all matrices [6 (Landsberg, 1893)], bordered symmetric, skew, and hermitian matrices [3 (Carlitz and Hodges, 1956a)], and persymmetric matrices [4 (Daykin, 1960)]. (Persymmetric matrices are matrices with constant minor diagonals: $a_{i,j} = a_{k,m}$ whenever $i + j = k + m$.)

An $n \times n$ matric is said to be cyclic iff $a_{i,j} = a_{k,m}$ whenever $i + j \equiv k + m$ mod n. Cyclic matrices are a subclass of persymmetric matrices. A cyclic matrix is completely determined by specifying the entries in its first row. Thus there are q^n $n \times n$ cyclic matrices over the finite field of q elements, $GF(q)$.

Cyclic matrices arise in the study of cyclic codes used for detection and correction of errors in digital communication systems. Following Peterson (1960), we observe that the rows of a cyclic matrix can be represented as polynomials modulus $X^n - 1$. For example, the first row is represented as $a_{1,1}X^{n-1} + a_{1,2}X^{n-2} + \cdots + a_{1,n-1}X + a_{1,n}$. The $(i + 1)$st row of the matrix is then X times the i-th row, because polynomial multiplication by X module $X^n - 1$ is equivalent to a cyclic shift.

The first row of the matrix is considered the generator polynomial and is denoted by $g(X)$. A linear combination of rows can then be written as the product of $g(X)$ and some other polynomial $f(X)$ in $GF[q, X]$, the ring of polynomials in X over the finite field $GF(q)$. For example, the sum of the second and fourth rows is $g(X)(X^3 + X)$ mod $X^n - 1$. The set of all rows which can be formed by taking linear combinations of the rows of the cyclic matrix is just the set of all polynomials which are multiples of $g(X)$ mod $X^n - 1$. This set of polynomials is called the ideal generated by $g(X)$.

There are q^n different residue classes mod $X^n - 1$ and hence q^n possible generators corresponding to the q^n possible cyclic matrices. If all q^n distinct residue classes lie in the ideal generated by $g(X)$, then all possible rows are linear combinations of some rows of the cyclic matrix and the matrix has rank n. If, however, only q^r distinct residue classes lie in the ideal generated by $g(X)$, then the matrix has degree r. We call r the dimension of the ideal generated by $g(X)$ mod $X^n - 1$. Let deg (F) denote the degree of the polynomial $F(X)$. It is a theorem of algebra (See [1; 48]), that the ideal generated by $g(X)$ contains $q^{\deg(f)-\deg(d)}$ distinct residue classes mod $f(X)$, where $d(X)$ is the com-

Received August 23, 1964. Most of the work reported here was done at Bell Telephone Laboratories, Murray Hill, New Jersey, during the summer of 1963. The author is indebted to L. Carlitz, J. H. Hodges, J. Riordan, D. Slepian, J. B. Kruskal, R. L. Graham, R. I. Jewett and A. D. Wyner for helpful advice and critical comments.