POWER SUMS OF MATRICES OVER A FINITE FIELD

J. V. BRAWLEY, L. CARLITZ, AND J. LEVINE

Let F denote the finite field of order q and let $F_{n \times n}$ denote the ring of $n \times n$ matrices over F. For $A \in F_{n \times n}$ let $\sigma_i(A) = \sigma_i$ denote the i-th elementary symmetric function of the roots of A. This paper is concerned with the evaluation of the sum

(1) $$\sum_{A \in C} \sigma_1^{\alpha_1} \sigma_2^{\alpha_2} \cdots \sigma_n^{\alpha_n} A^m$$

for various subsets C of $F_{n \times n}$ where $\alpha_1, \cdots, \alpha_n, m$ are nonnegative integers and where by definition $A^0 = I$, the identity matrix, for all $A \in F_{n \times n}$ and $\sigma^0 = 1$ for all $\sigma \in F$. A class of sets C for which results are obtained are the t-parameter linear sets and this class includes $F_{n \times n}$ itself, the symmetric and skew-symmetric matrices, the upper (lower) triangular matrices and the matrices with constant row (column) sums. For the case where $(n, q) = 1$ the sum (1) is evaluated for sets C which are the unions of similarity classes. Sets covered in this class include for example the nonsingular matrices, the rank r matrices, and the matrices satisfying a given scalar polynomial. Putting $\alpha_1 = \alpha_2 = \cdots = \alpha_n = 0$ in (1) yields $\sum A^m$.

1. Introduction. Let $F = GF(q)$ denote the finite field of q elements so that $q = p^\beta$ for some prime p and integer $\beta > 0$. A well-known result is that for a positive integer m

(1.1) $$\sum_{a \in F} a^m = \begin{cases} -1 & (q-1) \mid m \\ 0 & (q-1) \nmid m. \end{cases}$$

This elementary fact is useful in the theory of finite fields and has been employed for example to show that no reduced permutation polynomial on F except the linear polynomial $ax + b$, $a, b \in F$, $a \neq 0$, can have degree dividing $q - 1$ [5].

The present paper represents an outgrowth of an original desire to generalize (1.1) to obtain the sum $\sum A^m$ where A ranges over $F_{n \times n}$, the ring of $n \times n$ matrices over the finite field F. At the outset it was hoped that knowing this matric sum would be of help in determining conditions on a polynomial $f(x) \in F[x]$ in order that it represent via substitution a permutation of $F_{n \times n}$. It turned out (as we show in this paper) that the sum $\sum A^m$ was generally zero; consequently it was of little help on the matrix permutation problem, a problem which was subsequently solved by the authors in [1]. Still the material presented here is interesting for its own sake and might well prove useful to later problems.

Received September 26, 1973. The first author was supported in part by O. N. R. contract N00014-71-A-0339-0002. The second author was supported in part by N. S. F. grant GP-37924.