STOCHASTIC INVOLUTIONS OVER A FINITE FIELD

JOHN D. FULTON

Introduction. Throughout this paper for $q = p^t$, p a prime, F_q will denote the finite field with q elements and $\mathcal{V}_n$ will denote the n-dimensional vector space of n-tuples (column vectors) with scalars from F_q. An *involution* of $\mathcal{V}_n$ (or an involutory matrix) is an $n \times n$ matrix A over F_q such that $A = A^{-1}$. The $n \times n$ involutory matrix A will be said to have *signature* s [8] if A is similar to the diagonal matrix Diag $[I_{n-s}, -I_s]$ for some $s = 0, 1, 2, \cdots, n$ and for q odd, and if A is similar to the direct sum matrix Diag $[I_{n-2s}, E_1, E_2, \cdots, E_s]$, where for q even and for $s = 0, 1, \cdots, [n/2]$ each E_i is the matrix $\begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}$. I_k denotes the $k \times k$ identity matrix and $[k]$ is the greatest integer less than or equal to k.

A matrix A is said to be *row stochastic* (*column stochastic*) if each of its row sums (column sums) is a 1 and is said to be *doubly stochastic* if each of its row sums and each of its column sums is a 1.

Brawley and Levine [2] require an enumeration of the row stochastic involutions of signature s of $\mathcal{V}_n$ in their analysis of linear n-graphic cryptosystems with finite ring F_q. They enumerate the $n \times n$ row stochastic involutory matrices of signature s over F_q in the same paper.

It is the purpose of this paper to enumerate by signature the $n \times n$ row (column) stochastic (see §2) and the $n \times n$ doubly stochastic (see §3) involutory matrices over F_q. The enumeration in this paper of the row (column) stochastic involutions proceeds differently from that of Brawley and Levine. Also, in this paper an enumeration by signature of the $n \times n$ symmetric doubly stochastic involutions is presented (see §4). It should be remarked that Fisher and Alexander [5] have enumerated the $n \times n$ nonsingular matrices over F_q each with a prescribed row sum vector.

Levine and Nahikian [9] have shown that the $n \times n$ involutory matrix A over a field F has signature s if and only if it can be decomposed as $A = I_n + cQP$, where each of P and Q^t is $s \times n$ of rank s, where $c = -2$ and $PQ = I_s$ if the characteristic of F differs from 2, and where $c = 1$ and $PQ = 0$ if the characteristic of F is 2. Brawley [1] in his enumeration of $n \times n$ involutions of signature s over F_q (an enumeration first given by Hodges [8]) used the decomposition of Levine and Nahikian to partition the involutions into P-sets. Thus, involutions of signature s over F_q, $I_n + cQP$ and $I_n + cQ_1P_1$ have been said by Brawley

Received January 20, 1972. Revision received March 23, 1972. The author is indebted to his colleague Professor Joel V. Brawley, Jr. for suggesting the enumerations in this paper. The author also expresses his gratitude to the referee for his proof of Theorem 4.1 and for his other suggestions and comments.