THE ELEMENTARY SYMMETRIC FUNCTIONS IN A FINITE FIELD OF PRIME ORDER

BY

OLIVER ABERTH

1. Introduction

For a finite field F of prime order and a given positive integer n let $\mathcal{P}_n(F)$ be the set of all functions in n variables $x_1, x_2, \cdots, x_n$ where both the function and the variables assume values in F. Let $F[X_1, X_2, \cdots, X_n]$ be the ring of polynomials with coefficients in F in the n indeterminates $X_1, X_2, \cdots, X_n$. If $g \in \mathcal{P}_n(F)$, the finite range of the variables allows the construction by interpolation techniques of an element $G \in F[X_1, \cdots, X_n]$ such that g is obtained from G by the obvious substitution mapping. However, the element G is not uniquely determined unless we impose some further requirement, e.g. that its degree in each variable separately be less than the number of elements in F (see [3]).

We shall be interested in the subring $\mathcal{S}_n(F)$ of $\mathcal{P}_n(F)$ consisting of those functions g which are symmetric in the variables $x_1, x_2, \cdots, x_n$. For such a function g the polynomial G can be taken as a symmetric polynomial. For example, the above requirement on the degrees will produce a symmetric polynomial. Now any symmetric polynomial can be obtained from the elementary symmetric polynomials by means of a finite number of additions, subtractions, and multiplications. Thus, by making the obvious homomorphism from $F[X_1, \cdots, X_n]$ onto $\mathcal{P}_n(F)$, we see that $\mathcal{S}_n(F)$ is the subring of $\mathcal{P}_n(F)$ generated by the elementary symmetric functions

$$U_k(x_1, \cdots, x_n) = \sum_{i_1<i_2<\cdots<i_k} x_{i_1}x_{i_2} \cdots x_{i_k} \qquad (k = 1, 2, \cdots, n).$$

We shall show that actually $\mathcal{S}_n(F)$ is generated by a subset of the functions $U_1, U_2, \cdots, U_n$.

In the final section we study the asymptotic distribution of the U_k as the number of variables tends to infinity.

2. Elementary symmetric function relations

We will require the following lemma, the statement and proof of which is a slight variation of one proved by Fine [1, Lemma 5].

LEMMA. *For any set $C_1, C_2, \cdots, C_{p-1}$ of members of a finite field F of prime order p, there is a unique set of integers $\alpha_1, \alpha_2, \cdots, \alpha_{p-1}$ with $0 \leqq \alpha_i < p$, such that in $F[X]$*

$$(1) \quad \prod_{i=1}^{p-1} (1 + iX)^{\alpha_i} = 1 + C_1 X + C_2 X^2 + \cdots + C_{p-1} X^{p-1} + \cdots .$$

Received May 10, 1962; received in revised form October 6, 1962.