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.

If (1) is to hold, then the coefficients C_i are equal to $U_i(x_1, \cdots, x_N)$, where $N = \alpha_1 + \alpha_2 + \cdots + \alpha_{p-1}$, and α_1 of the variables x_j are equal to 1, α_2 are equal to 2, $\cdots$, α_{p-1} are equal to $p - 1$. Using Newton's identities, which hold in F, we have

$$\begin{aligned} S_1 &= \sum_{j=1}^{N} x_j = \sum_{i=1}^{p-1} \alpha_i i = C_1, \\ S_2 &= \sum_{j=1}^{N} x_j^2 = \sum_{i=1}^{p-1} \alpha_i i^2 = C_1 S_1 - 2C_2, \\ &\vdots \\ S_{p-1} &= \sum_{j=1}^{N} x_j^{p-1} = \sum_{i=1}^{p-1} \alpha_i i^{p-1} = C_1 S_{p-2} - C_2 S_{p-3} + \cdots \\ &\qquad + (-1)^{p-1} C_{p-2} S_1 + (-1)^p (p-1) C_{p-1}. \end{aligned}$$

Eliminating S_1 from the right side of the second equation, S_1 and S_2 from the right side of the third equation, etc., yields the set of equations

$$\begin{aligned} \sum_{i=1}^{p-1} \alpha_i i &= C_1 = Q_1, \\ \sum_{i=1}^{p-1} \alpha_i i^2 &= C_1^2 - 2C_2 = Q_2, \\ &\vdots \\ \sum_{i=1}^{p-1} \alpha_i i^{p-1} &= \cdots = Q_{p-1}, \end{aligned} \tag{2}$$

where the Q_i are certain functions of $C_1, C_2, \cdots, C_{p-1}$. If the α_i were members of F instead of integers, (2) would be $p - 1$ linear equations in F in $p - 1$ unknowns. The determinant of the coefficients of the unknowns is the Vandermonde $| c_{ij} |$, $c_{ij} = j^i$, which is never equal to zero. Thus for any choice of $C_1, \cdots, C_{p-1}$ there is a unique set of elements in F such that the equations (2) hold. Since any element in F may be written uniquely as $n \cdot 1$ where $1 \in F$ and n is an integer satisfying $0 \leqq n < p$, we also obtain unique integers α_i ($0 \leqq \alpha_i < p$) satisfying (2), and the lemma is proved.

On the right side of (1) let the coefficients of powers of X higher than $p - 1$ be $C_p, C_{p+1}, \cdots, C_{(p-1)^2}$. For each choice of $C_1, \cdots, C_{p-1}$, these other coefficients are determined, since the α_i are unique. Thus for $i \geqq p$ each C_i is a function of $C_1, \cdots, C_{p-1}$:

$$C_i = R_i(C_1, C_2, \cdots, C_{p-1}), \qquad i = p, p+1, \cdots, (p-1)^2. \tag{3}$$

Actually, if we again view the α_i in (2) as members of F, we can solve for α_i as functions of $C_1, C_2, \cdots, C_{p-1}$; then if the C_i for $i \geqq p$ are expressed in terms of the α_i by expanding the left side of (1) and equating like powers of X, substitution for α_i would lead directly to the desired expressions (3).

For the convenient statement of the theorems, we introduce the following notation: if p is a positive prime, let L_p denote the set of integers of the form tp^s, where s is a positive integer or zero, and t is any integer from 1 to $p - 1$ inclusive.

THEOREM 1. *For a finite field of prime order p, each elementary symmetric function U_k can be expressed as a function in the U_λ, $\lambda \in L_p$ and $\lambda \leqq k$, the expression holding independently of the number of variables $x_1, x_2, \cdots, x_n$ of U_k.*

As an immediate consequence we have the

COROLLARY. *In a finite field of prime order p, every symmetric function in n variables can be expressed as a function in the U_λ, $\lambda \in L_p$ and $\lambda \leqq n$.*

We will prove the theorem by showing how the function may be constructed for U_k when $k \notin L_p$. If we set a_i equal to the number of the variables $x_1, x_2, \cdots, x_n$ equal to i for $i = 1, 2, \cdots, p-1$, then from the expression

$$\prod_{j=1}^{n} (1 + x_j \cdot X) = 1 + \sum_{k=1}^{n} U_k X^k$$

we obtain

$$\Phi(X) = \prod_{i=1}^{p-1} (1 + iX)^{a_i} = 1 + \sum_{k=1}^{n} U_k X^k.$$

Writing the integers a_i in the p-ary number system,

$$a_i = \alpha_i^{(0)} + \alpha_i^{(1)} p + \cdots + \alpha_i^{(r)} p^r, \qquad 0 \leqq \alpha_i^{(j)} < p,$$

we have

$$\Phi(X) = \prod_{i=1}^{p-1} (1 + iX)^{\alpha_i(0)} \cdot \prod_{i=1}^{p-1} (1 + iX^p)^{\alpha_i(1)} \cdot \prod_{i=1}^{p-1} (1 + iX^{p^2})^{\alpha_i(2)} \cdots.$$

If we set

$$(4) \qquad \prod_{i=1}^{p-1} (1 + iX^{p^j})^{\alpha_i(j)} = 1 + C_1^{(j)} X^{p^j} + C_2^{(j)} X^{2p^j} + \cdots,$$

then if $p^s \leqq k < p^{s+1}$ for some nonnegative integer s,

$$(5) \qquad U_k = \sum C_{\beta_0}^{(0)} C_{\beta_1}^{(1)} \cdots C_{\beta_s}^{(s)},$$

where the sum extends over all $(s+1)$-tuples $\beta_0, \beta_1, \cdots, \beta_s$ with $\beta_0 + p\beta_1 + \cdots + p^s\beta_s = k$ (we define $C_0^{(j)}$ equal to 1).

If $k = tp^s$ for some integer $t < p$, then the $(s+1)$-tuple $0, 0, \cdots, 0, t$ gives rise in (5) to the term $C_t^{(s)}$, and we may rewrite (5) in this case as

$$(6) \qquad C_t^{(s)} = U_{tp^s} - \sum C_{\beta_0}^{(0)} C_{\beta_1}^{(1)} \cdots C_{\beta_s}^{(s)},$$

where the sum extends over all $(s+1)$-tuples $\beta_0, \beta_1, \cdots, \beta_s$ with $\beta_0 + p\beta_1 + \cdots + p^s\beta_s = tp^s$ and $\beta_s < t$.

Since (4) is the same type of equation as (1), we may apply the result (3) obtained in the discussion following the lemma and write

$$(7) \qquad C_i^{(j)} = R_i(C_1^{(j)}, C_2^{(j)}, \cdots, C_{p-1}^{(j)}), \qquad i = p, p+1, \cdots, (p-1)^2.$$

Equations (5), (6), and (7) may be used to construct the desired functions. For any integer k satisfying $tp^s < k < (t+1)p^s$, we start with (5) and use (6) to eliminate in succession the variables $C_t^{(s)}, C_{t-1}^{(s)}, \cdots, C_1^{(s)}$. Then U_k is expressed as a function of $U_{tp^s}, U_{(t-1)p^s}, \cdots, U_{p^s}$, and $C_i^{(j)}$, $j \leqq s-1$. Using (7), we can eliminate the variables $C_i^{(s-1)}$ for $i \geqq p$. Then we can use

(6) again to eliminate in succession the variables $C_{p-1}^{(s-1)}, C_{p-2}^{(s-1)}, \cdots, C_1^{(s-1)}$. We then have U_k expressed as a function of $U_{tp^s}, \cdots, U_{p^s}$; $U_{(p-1)p^{s-1}}, \cdots, U_{p^{s-1}}$; and the variables $C_i^{(j)}$, $j \leqq s-2$. Continuing this process to its conclusion leads to the desired expression for U_k. This completes the proof of Theorem 1.

We show the uniqueness of the constructed functional expression for U_k in our second theorem.

THEOREM 2. *There is one and only one function for U_k in terms of the U_λ, $\lambda \in L_p$, which holds for any number n of the variables x_i.*

In particular this theorem shows that it is not possible to reduce the number of basic elementary symmetric functions U_λ, $\lambda \in L_p$, by expressing one of them in terms of the others.

We will prove the theorem as soon as we show that any possible set of values for a finite number of the U_λ, $\lambda \in L_p$, is actually assumed for some $x_1, x_2, \cdots, x_n$ if n is large enough. Accordingly, let r be given, and suppose it is desired to fix arbitrarily all the U_λ, $\lambda < p^r$ and $\lambda \in L_p$. We must show how to choose the $\alpha_j^{(j)}$, $j < r$ so that the polynomial

$$\Phi(X) = \prod_{i=1}^{p-1} (1 + iX)^{\alpha_i^{(0)}} \cdot \prod_{i=1}^{p-1} (1 + iX^p)^{\alpha_i^{(1)}} \cdots \prod_{i=1}^{p-1} (1 + iX^{p^{r-1}})^{\alpha_i^{(r-1)}}$$

has the coefficient of each X^λ, $\lambda \in L_p$, the corresponding desired value of U_λ. By the lemma we may first choose the $\alpha_i^{(0)}$ so that the coefficients of $X, X^2, \cdots, X^{p-1}$ of $\prod_{i=1}^{p-1} (1 + iX)^{\alpha_i^{(0)}}$ are the desired values for $U_1, U_2, \cdots, U_{p-1}$, respectively.

Similarly it will be possible to choose $\alpha_i^{(1)}$ so that the coefficients of $X^p, X^{2p}, \cdots, X^{(p-1)p}$ in $\prod_{i=1}^{p-1} (1 + iX^p)^{\alpha_i^{(1)}}$ are any values we wish. In particular we may choose them so that $\prod_{i=1}^{p-1} (1 + iX)^{\alpha_i^{(0)}} \cdot \prod_{i=1}^{p-1} (1 + iX^p)^{\alpha_i^{(1)}}$ has the coefficients of $X^p, X^{2p}, \cdots, X^{(p-1)}$ equal to the desired values for $U_p, U_{2p}, \cdots, U_{(p-1)p}$, respectively. The coefficients of $X, X^2, \cdots, X^{p-1}$ in this expression are identical to the corresponding coefficients of $\prod_{i=1}^{p-1} (1 + iX)^{\alpha_i^{(0)}}$. Continuing the process we see that by fixing each set of $\alpha_i^{(j)}$ for $j = 0, 1, 2, \cdots, (r-1)$ in sequence, we may obtain the desired coefficients for X^λ, $\lambda < p^r$ and $\lambda \in L_p$, and the theorem is proved. Note that there is a one-to-one mapping between the sets of $\alpha_i^{(j)}$, $j < r$, and the sets of U_λ, $\lambda < p^r$ and $\lambda \in L_p$, since the number of possible sets is the same for each.

3. Examples: The cases $p = 2$ and $p = 3$

For the field of two elements, L_2 is the set of integers of the form 2^s, $s \geqq 0$. The product $\prod_{i=1}^{p-1} (1 + X^{p^j})^{\alpha_i^{(j)}}$ becomes simply $(1 + X^{2^j})^{\alpha_1^{(j)}}$ which equals $1 + \alpha_1^{(j)} X^{2^j}$ since $\alpha_1^{(j)}$ is either 0 or 1. Thus there are no $C_i^{(j)}$ with $i \geqq p = 2$, and equation (7) is unnecessary. For $k = k_0 + k_1 2 + \cdots + k_s 2^s$,

$k_i = 0$ or 1, equations (5) and (6) become

$$U_k = C_{k_0}^{(0)} C_{k_1}^{(1)} \cdots C_{k_s}^{(s)} \quad \text{and} \quad C_1^{(j)} = U_{2^j},$$

so that $U_k = \prod U_{2^j}$ for all j with $kj \neq 0$.

For the field of three elements, the relationships for U_k are more complicated, and we are unable to obtain a general formula for U_k. Equation (4) becomes

$$(1 + X^{3^j})^{\alpha_1(j)}(1 + 2X^{3^j})^{\alpha_2(j)}$$
$$= 1 + C_1^{(j)}X^{3^j} + C_2^{(j)}X^{2\cdot 3^j} + C_3^{(j)}X^{3\cdot 3^j} + C_4^{(j)}X^{4\cdot 3^j},$$

and the functions in (7) must be determined for $C_3^{(j)}$ and $C_4^{(j)}$. They are

$$C_3^{(j)} = C_1^{(j)}C_2^{(j)}(C_1^{(j)} + 2C_2^{(j)}),$$
$$C_4^{(j)} = C_1^{(j)}C_2^{(j)}(C_1^{(j)} - 1)(C_2^{(j)} - 1).$$

L_3 is the set of integers of the form 3^s or $2\cdot 3^s$, so that 4 and 5 are the two smallest integers not in L_3. Following the procedure outlined in Theorem 1, we obtain for U_4 and U_5

$$U_4 = U_3 U_1 + 2U_2^2 U_1^2 + 2U_2^2 U_1 + 2U_2 U_1^2,$$
$$U_5 = U_3 U_2 + 2U_2^2 U_1^2 + U_2 U_1.$$

4. Asymptotic distribution for U_k

The elementary symmetric function $U_k(x_1, \cdots, x_n)$ has p^n different sets of values for its variables if the field F has order p. Of these let q be the number for which $U_k = a$. Then, following Fine [1], we set $P_n(k, a) = q/p^n$, the fraction of times $U_k = a$. Fine investigated the behavior of $P_n(k, a)$ as the number of variables n goes to infinity. He proved that $\lim_{n\to\infty} P_n(k, a)$ always exists, and designated this limit by $P_k(a)$. Furthermore, he showed that the $P_k(a)$ can be evaluated in the following manner:

Choose r so that $p^r > k$, and count the number of times, q, that the coefficient of X^k in

$$(8) \quad \prod_{i=1}^{p-1}(1 + iX)^{\alpha_i(0)} \cdot \prod_{i=1}^{p-1}(1 + iX^p)^{\alpha_i(1)} \cdots \prod_{i=1}^{p-1}(1 + iX^{p^{r-1}})^{\alpha_i(r-1)}$$

is equal to a for all possible choices of $\alpha_i^{(j)}$ satisfying $0 \leqq \alpha_i^{(j)} < p$. Then $P_k(a) = q/N$ where $N = p^{r(p-1)}$ is the number of possible choices for the $\alpha_i^{(j)}$. Actually as the $\alpha_i^{(j)}$ run through their values, the coefficients of the X^k for $k < p^r$ not only display the limiting distribution $U_k = a$, but also any desired limiting multiple distribution, as for example $U_k = a$, $U_1 = b$. Using this fact and remembering that there is a one-to-one mapping between the $\alpha_i^{(j)}$ and all the sets of values for U_λ, $\lambda \in L_p$ and $\lambda < p^r$, we obtain an alternate method for calculating $P_k(a)$, which we state in a generalized form:

THEOREM 3. *In the field F of prime order p, let V, a symmetric function in variables $x_1, x_2, \cdots, x_n$, where n may be any number, be expressed as a function*

R in the U_λ, $\lambda \in L_p$. Then the asymptotic distribution $P(a)$ (defined for V in similar fashion as for U_k) equals q/N where q is the number of times $R = a$ as the variables U_λ in R range over their possible sets of values, and N is the total number of such sets.

Fine calculated $P_k(a)$ explicitly for the case $p = 2$, and obtained $P_k(a)$ for $p = 3$ as a set of recurrence formulas. For both $p = 2$ and $p = 3$, the asymptotic distribution $P_k(a)$ exhibited the properties:

1a. $P_k(0) \geqq 1/p$,
1b. $P_k(0) = 1/p$ only if $k \in L_p$,
2. $P_k(a) = 1/p$ if $k \in L_p$,
3. $P_{kp}(a) = P_k(a)$,
4. $P_k(0) \geqq P_k(a)$, $a \neq 0$, with equality only for $k \in L_p$.
5. $\operatorname{Lim\,Sup}_{k\to\infty} P_k(0) = 1$.

1 is implied by 4, but we list it separately for convenience in discussion. Fine proved 2 true for all p (also implied by Theorem 3), and proposed as problems the proof or disproof of the other properties for general p.

For $p = 5$, calculation yields the following results: $P_6(0) = \frac{1}{5}$, which disproves 1b; $P_6(2) = 26/125 > \frac{1}{5} = P_6(0)$, and this furnishes a counterexample to 4; finally $P_{30}(0) = 78745/625^2 > \frac{1}{5} = P_6(0)$, and thus 3 also fails.

On the other hand, the corollary to the next theorem will show that 5 is valid for all p, and this leaves only 1a unresolved.

THEOREM 4. *Let the order of F be the prime p. Express the integer k in the p-ary number system, $k = k_0 + k_1 p + k_2 p^2 + \cdots + k_s p^s$ where $0 \leqq k_i < p$, and let h be the number of nonzero coefficients k_i. Then*

$$\left(1 - \frac{1}{p}\right)^h \leqq 1 - P_k(0) \leqq \left(1 - \frac{1}{p^{2(p-1)}}\right)^{[(h+1)/2]},$$

where square brackets denote the greatest integer function.

The left-hand part of the inequality is Theorem 11 in [1]. To derive the right-hand part, we will estimate the number of times the coefficient of X^k is 0 in the expression (8) as the integers $\alpha_i^{(j)}$ run through all possible sets of values with $0 \leqq \alpha_i^{(j)} < \text{p}$. We may assume $r > s$. Expanding each product $\prod_{i=1}^{p-1} (1 + iX^{p^j})^{\alpha_i^{(j)}}$ as in (4), the coefficient of X^k will be given by the sum (5). Suppose that the coefficient k_q in the p-ary expansion of k is $\neq 0$, where $q \geqq 1$. Then if $\alpha_i^{(q)}$ and $\alpha_i^{(q-1)}$ are all zero for $i = 1, 2, \cdots, p - 1$, the sum (5) must also be zero. For we have that $C_i^{(q-1)} = C_i^{(q)} = 0$ for $i \neq 0$, and every term in the sum (5) will be zero except those that are of the form $C_{\beta_0}^{(0)} \cdots C_0^{(q-1)} C_0^{(q)} \cdots C_{\beta_s}^{(s)}$. However, there actually are no terms of this type, since from $\beta_0 + p\beta_1 + \cdots + p^s\beta_s = k = k_0 + k_1 p + \cdots + k_s p^s$ and $k_q \neq 0$, it is required that

$$\beta_0 + p\beta_1 + \cdots + p^{q-2}\beta_{q-2} \geqq k_q p^q \geqq p^q.$$

But since $\beta_i \leqq (p-1)^2$, we must have

$$\beta_0 + p\beta_1 + \cdots + p^{q-2}\beta_{q-2} \leqq (p-1)(p^{q-1}-1) < p^q.$$

Thus all terms in (5) are zero, and the coefficient of X^k is zero when $\alpha_i^{(q-1)} = \alpha_i^{(q)} = 0$, for $k_q \neq 0$. In the case $k_0 \neq 0$, it is easy to see that if $\alpha_i^{(0)} = 0$ for all i, the coefficient of X^k is also zero.

Let θ be the number of terms $k_q \neq 0$ for q an odd integer. Then the coefficient of X^k is zero whenever $\alpha_i^{(q)} = \alpha_i^{(q-1)} = 0$, where q is one of these odd integers. If N is the total number of sets $\alpha_i^{(j)}$, then the number of ways in which this can happen is

$$N - N\left(\frac{p^{2(p-1)} - 1}{p^{2(p-1)}}\right)^\theta.$$

Thus $P_k(0) \geqq 1 - (1 - 1/p^{2(p-1)})^\theta$. Similarly if ε is the number of terms $k_q \neq 0$ for q an even integer, we obtain

$$P_k(0) \geqq 1 - (1 - 1/p^{2(p-1)})^\varepsilon,$$

with a trivial modification in the argument in the case $k_0 \neq 0$. Since the larger of the two numbers θ, ε is at least $[(h+1)/2]$, the right-hand side of the inequality stated in the theorem is obtained.

COROLLARY. $\text{Lim Sup}_{k\to\infty} P_k(0) = 1$.

Letting k run through the integers of the form $p^m - 1$, we see by the preceding theorem that $P_k(0)$ can be made as close to 1 as desired by taking m large enough.

Acknowledgement. I wish to thank Professor N. J. Fine for his very helpful suggestions and discussions. Thanks are also due Professor P. T. Bateman for his generous assistance in writing the introductory section.

BIBLIOGRAPHY

1. N. J. FINE, *On the asymptotic distribution of the elementary symmetric functions (mod p)*, Trans. Amer. Math. Soc., vol. 69 (1950), pp. 109–129.
2. RALPH HULL, *The number of solutions of congruences involving only k^{th} powers*, Trans. Amer. Math. Soc., vol. 34 (1932), pp. 908–937.
3. H. DAVENPORT, *The higher arithmetic, an introduction to the theory of numbers*, London, Hutchinson's University Library, 1952, p. 56.

SWARTHMORE COLLEGE
SWARTHMORE, PENNSYLVANIA
UNIVERSITY OF ILLINOIS
URBANA, ILLINOIS