LINEAR RECURRING SEQUENCES OVER FINITE FIELDS

by

Robert James McEliece

In Partial Fulfillment of the Requirements

For the Degree of

Doctor of Philosophy

California Institute of Technology

Pasadena, California

1967

(Submitted March 27, 1967)

ACKNOWLEDGMENTS

It is a pleasure for me to take this opportunity to thank the people who have helped me in the preparation of this thesis. I am indebted to Professor Ernst Selmer, whose lectures on linear recurrences given at Cambridge University in 1965 stimulated my interest in the subject. Throughout my thesis research, I have received a constant supply of ideas and advice from Dr. Gustave Solomon, to whom I am especially grateful. Finally, I should like to thank my adviser, Professor Marshall Hall, Jr., not only for the help he has given me in the preparation of this thesis, but also for the active interest he has taken in my career ever since my undergraduate days. I owe him much more than I shall ever be able to repay.

I should also like to thank the National Science Foundation for their kind financial support of my graduate study.

ABSTRACT

This thesis deals with the problem of how the elements from a finite field F of characteristic p are distributed among the various linear recurrent sequences with a given fixed characteristic polynomial $f \in F[x]$. The first main result is a method of extending the so-called "classical method" for solving linear recurrences in terms of the roots of f. The main difficulty is that f might have a root θ which occurs with multiplicity exceeding $p-1$; this is overcome by replacing the solutions θ^t, $t\theta^t$, $t^2\theta^t$, ..., by the solutions θ^t, $\binom{t}{1}\theta^t$, $\binom{t}{2}\theta^t$, ... The other main result deals with the number N of times a given element $a \in F$ appears in a period of the sequence, and for $a \neq 0$, the result is of the form $N \equiv 0 \pmod{p^\epsilon}$, where ϵ is an integer which depends upon f, but not upon the particular sequence in question. Several applications of the main results are given.

TABLE OF CONTENTS

I. INTRODUCTION

This thesis is concerned with the problem of how the elements from a finite field F_q are distributed among the various sequences which satisfy a fixed linear recurrence relation with characteristic polynomial f(x). The space $\Omega(f)$ of all such sequences is viewed as a subspace of an e-dimensional vector space over F_q, where e is the exponent of f; this involves no loss since each sequence in $\Omega(f)$ is periodic of period e.

Chapter II presents the necessary preliminary material. Chapter III extends the so-called "classical method" for solving linear recurrences in fields of characteristic zero to the case of finite fields. Theorem 3.2 gives an explicit (if rather unwieldy) expression for the t^{th} element s_t of a sequence which satisfies the given recurrence in terms of the t^{th} powers of the roots of f in a splitting field. Previous attempts [10, 14] to extend the classical method have met with difficulty when a root of f occurred with a multiplicity which exceeded the characteristic of the field; theorem 3.2 overcomes the problem by replacing the powers t^i which occur in the classical solution by the binomial coefficients $\binom{t}{i}$ (which are suitably defined for the field F_q.) Also, theorem 3.2 makes heavy use of the fact that if θ is a root of f, then so is θ^q; this reduces the complexity of the solution considerably, since there are fewer "independent" roots of f than its degree. Chapter III concludes with two applications of the main theorem 3.2. If f is an irreducible polynomial in F_q, and m is an integer, let $p^{\mu-1} < m \leq p^{\mu}$. The polynomial $f^{(p^{\mu})}$ is obtained by raising each of the coefficients of f to the p^{μ} th power. Theorem 3.3 gives a precise description of the space $\Omega(f^m)$ in terms of the space $\Omega(f^{(p^{\mu})})$, and extends an earlier

result of Zierler [14], who proved the result in the special case $m = q^a$. Theorem 3.4 gives an upper bound on the number of distinct distributions of elements from F_q which may occur in $\Omega(f)$, when f is irreducible, in terms of the number of irreducible factors of a certain polynomial x^E-1.

Chapter IV, some of which appears in [11], is a digression and contains an explicit (though again somewhat unwieldy) expression for the so-called "monomial" symmetric functions in terms of the power-sum symmetric functions, in a field of characteristic zero. The method used to obtain the result, given in theorem 4.1, uses the method of Möbius inversion on a certain lattice of partitions, and may be of independent interest. A careful analysis shows that theorem 4.1 may be used to compute symmetric functions of roots of unity in a field of arbitrary characteristic; this fact, stated in theorem 4.2, is used heavily in the proof of theorem 5.2, the main result of chapter V.

Chapter V is an extension of some of the ideas in [11]; it presents a combinatorial-algebraic method which appears capable of completely solving the distribution problem in $\Omega(f)$, at least in the case that f has no repeated roots in a splitting field. Unfortunately, the difficulties encountered in pushing the method beyond a certain point are so great that theorem 5.2 is the best single result it has been possible to obtain. If N(s;a) represents the number of times a residue $a \in F_p$ occurs in a sequence $s \in \Omega(f)$, theorem 5.2 gives information of the type $N(s;a) \equiv 0 \pmod{p^\epsilon}$ for $a \neq 0$, and $N(s;0) \equiv e \pmod{p^\epsilon}$. Here ϵ is an integer which depends upon the fewest number of roots of f which can be multiplied together to give 1. Theorem 5.2 is a substantial generalization of the well-known result that if $p = 2$ and $(x - 1) \nmid f(x)$, then each sequence $s \in \Omega(f)$ contains an <u>even</u> number of ones; this result was previously thought to be peculiar to the binary

case; theorem 5.2 shows that it is not. Theorem 5.2 frequently gives enough information about the space $\Omega(f)$ so that it is possible to combine it with other information to obtain very precise information about the distributions which occur in $\Omega(f)$. This is illustrated by an example with $p = 3$, at the end of chapter V.

II. PRELIMINARIES

Throughout, if F is a field and x an indeterminant, then we denote by F[x] and F(x), respectively, the ring of polynomials with coefficients from F, and the field of rational fractions. We shall only be dealing with finite fields $F_q = GF[q]$ with $q = p^r$, p a prime, and in this case it is possible to identify the field $F_q(x)$ with the set of all ultimately periodic Laurent series; i.e., the set of all expressions of the form $a_n x^n + a_{n+1} x^{n+1} + \cdots$ in which n is an integer (positive, negative, or zero), $a_i \in F_q$, such that there exist integers r and t for which $a_i = a_{i+r}$ for all $i \geq t$. (Intuitively, in this representation one obtains the Laurent series corresponding to a fraction p(x)/ q(x) by actually performing the division.) For details about this isomorphism, see [14].

If a and b represent either integers or polynomials in F[x], we write $a \mid b$ to mean that a divides b, (a, b) for the greatest common divisor of a and b, and lcm(a, b) for the least common multiple of a and b.

Let $a_1, a_2, \ldots, a_n$, $a_n \neq 0$, be n arbitrary elements from F_q. We shall study sequences of elements $s = (s_0, s_1, s_2, \ldots)$ from F_q which satisfy the linear recurrence relation

$$s_t + a_1 s_{t-1} + \cdots + a_n s_{t-n} \quad \text{for all } t \geq n . \tag{2.1}$$

It is clear from (2.1) that the sequence s is completely determined by its initial values $s_0, s_1, \ldots, s_{n-1}$, and it follows that there are q^n distinct sequences s which satisfy (2.1). Also, if s and s' are two sequences which satisfy (2.1), and a and b are elements of F_q, the sequence $as + bs' = (as_0 + bs'_0, as_1 + bs'_1, \ldots)$ will also

satisfy (2. 1), so that the set of all such sequences may be viewed as a vector space of dimension n over F_q.

We associate the polynomial $f(x) = x^n + a_1 x^{n-1} + \cdots + a_n$ with the linear recurrence (2. 1), and call f(x) the characteristic polynomial of the recurrence. The vector space of all sequence satisfying (2. 1) is denoted by $\Omega(f)$.

For an arbitrary polynomial $p(x) \in F_q[x]$ such that $p(0) \neq 0$, let us define the exponent of f as the least integer e such that $f(x) \mid x^e - 1$. Then a basic fact [10] about the space $\Omega(f)$ is

Theorem 2. 1: All sequences which satisfy (2. 1) are periodic; i. e., for each $s \in \Omega(f)$, there is an integer ϵ such that $s_t = s_{t+\epsilon}$ for all t. Furthermore, if the characteristic polynomial f(x) has exponent e, then every sequence in $\Omega(f)$ has period e, and some have no shorter period.

In view of theorem 2. 1, it is natural to regard the sequences in $\Omega(f)$ as finite sequences of length e: $s = (s_0, s_1, \ldots, s_{e-1})$, and the space $\Omega(f)$ itself as an n-dimensional subspace of the space of all possible e-tuples from F_q. We shall call e the block length of $\Omega(f)$.

One of the results we shall require is the theory of the factorization of the polynomial $x^e - 1$ in $F_q[x]$. The results given below are implicit in the books by Albert [1] and Dickson [3], for example, but the point of view we wish to emphasize is sufficiently unusual to merit a somewhat detailed discussion. We will not, however, attempt to prove each statement made.

In factoring $x^e - 1$, we assume with no loss of generality that $(e, q) = 1$, for if $e = e_0 q^m$ with $(e_0, q) = 1$, then $x^e - 1 = (x^{e_0} - 1)^{q^m}$. The splitting field for $x^e - 1$ is $GF[q^n]$, where n is the least integer such that $q^n \equiv 1 \pmod{e}$.

Lemma 2.1: If $f \in F_q[x]$ has θ as a root in some splitting field, then θ^q is also a root.

In the field $GF[q^n]$, the roots of $x^e - 1$ will be powers of a primitive element θ of multiplicative order e; i.e., the roots are $1, \theta, \theta^2, \ldots, \theta^{e-1}$. If f(x) is an irreducible factor of $x^e - 1$, then f will have as one of its roots some power of θ; let us say $f(\theta^\alpha) = 0$. By lemma 2.2, f will also have as roots the powers θ^α, $\theta^{\alpha q}$, $\theta^{\alpha q^2}, \ldots, \theta^{\alpha q^{m-1}}$, where m is the least integer such that $\alpha q^m \equiv \alpha \pmod e$. Conversely, the elementary symmetric functions of the set $(\theta^\alpha, \theta^{\alpha q}, \ldots, \theta^{\alpha q^{m-1}})$ are fixed by the Galois group of $GF[q^n]$ over $GF[q]$, which is generated by the automorphism $x \to x^q$, so that the polynomial whose roots are $(\theta^\alpha, \theta^{\alpha q}, \ldots, \theta^{\alpha q^{m-1}})$ is in fact an element of $F_q[x]$. This polynomial is then an irreducible divisor of $x^e - 1$ of degree m. f turns out to be of exponent e if and only if $(\alpha, e) = 1$.

In this way we see that the question of the number of irreducible factors of any degree of $x^e - 1$ can be answered in an elementary fashion: given e and q, we permute the residues modulo e by the mapping $k \to kq \pmod e$. From the cycle structure of this permutation one reads off the number of irreducible factors of each degree. For example, let $q = 3$ and $e = 20$; the cycles are $(0)(1, 3, 9, 7)(2, 6, 18, 14)(4, 12, 16, 8)(5, 15)(10)(11, 13, 19, 17)$. Consequently $x^{20} - 1$ has 7 irreducible factors in F_3; two of degree one (these are naturally $x + 1$ and $x - 1$) one of degree two, and four of degree four. The cycles $(1, 3, 9, 7)$ and $(11, 13, 19, 17)$ exhaust the residues prime to 20, and correspond to the two irreducibles of degree four and exponent 20.

It is clear that, conversely, given an exponent e, the degree n of an irreducible factor of $x^e - 1$ which is of exponent e is uniquely determined as the exponent to which q belongs modulo e, so that there are $\varphi(e)/n$ such factors.

Finally, we present three miscellaneous elementary number-theoretic results which will be needed in the proof of theorem 5.2, below.

Suppose p is a prime, n an integer ≥ 1. We write n in its unique p-ary expansion, $n = \sum_{k \geq 0} n_k p^k$, where $0 \leq n_k < p$, and of course only finitely many of the n_k are different from zero. Similarly $m = \sum_{k \geq 0} m_k p^k$.

Definitions: $W_p(n)$ = the "p-ary weight" of $n = \sum_{k \geq 0} n_k$. If r is any rational integer, write $r = p^t \cdot \frac{a}{b}$ where $(a, p) = (b, p) = 1$. Then $t = \mu_p(r)$.

Theorem 2.2: (Legendre; see Dickson [3 ; chapter IX].)

$$\mu_p(n!) = \frac{1}{p-1} \left(n - W_p(n)\right) .$$

Theorem 2.3: (Lucas; see Dickson [3 ; chapter IX].)

$$\binom{n}{m} \equiv \prod_{k \geq 0} \binom{n_k}{m_k} \pmod{p} .$$

Lemma 2.2: If R is a finite set of rationals, $\sum_{r \in R} r = S$, then $\mu_p(S) \geq \min \left\{ \mu_p(r) : r \in R \right\}$.

Proof: Obvious.

Throughout, if x is a finite set $|x|$ denotes the number of elements in x. If r is a real number, $[r]$ = the greatest integer $\leq r$; i.e., $[r]$ is the unique integer n which satisfies $r - 1 < n \leq r$.

III. THE "CLASSICAL METHOD"

Let $f(x) = x^n + a_1 x^{n-1} + \ldots + a_n$ be a polynomial in $F_q[x]$ of degree n and exponent e. Let $(f(x))$ be the principal ideal in $F_q[x]$ generated by $f(x)$, and denote the quotient ring $F_q[x]/(f(x))$ by R_f. Then $f(x)$ will have a "root" θ in R_f; i.e., an element of R_f with $\theta^e = 1$ and such that the powers $1, \theta, \theta^2, \ldots, \theta^{n-1}$ are linearly independent over F_q. With each element $x \in R_f$ we shall associate an ordered generalized coset of the multiplicative subgroup $T = \{1, \theta, \theta^2, \ldots, \theta^{e-1}\}$ as follows:

$$x \to \{x, x\theta, \ldots, x\theta^{e-1}\} = xT .$$

(These are not cosets in the ordinary sense since there can be fewer than e distinct elements in xT; indeed, unless $f(x)$ is irreducible, it will always be possible to find $x \neq 0$ with $|xT| < e$.)

Viewing R_f as an n-dimensional vector space over F_q, we choose a linear functional t of R_f over F_q. (That is, t is an F_q-linear mapping from R_f onto F_q.) With the aid of t, it is possible to a sequence of elements from F_q with each element $x \in R_f$:

$$x \to xT \to (t(x), t(x\theta), \ldots, t(x\theta^{e-1})) = s(x) . \qquad (3.1)$$

Theorem 3.1: The set of sequences (3.1) is identical with the solution space $\Omega(f)$.

Remark: Theorem 3.1 is a very minor generalization of the "secondary isomorphism" between R_f and $\Omega(f)$ given by Hall [5]. The only difference is that Hall proved theorem 3.1 for a particular linear functional t.

Proof of theorem 3.1: First let us show that for each $x \in R_f$, the sequence $s(x)$ given by (3.1) satisfies the appropriate linear recurrence. In R_f, $f(\theta) = 0$ and so

$$\theta^n + a_1\theta^{n-1} + \cdots + a_n = 0 .$$

Multiplying this expression by $\theta^k x$ and operating with t, we obtain

$$t(x\theta^{n+k}) + a_1 t(\theta^{n+k-1}) + \cdots + a_n t(x\theta^k) = 0 ,$$

which is the statement that $s(x)$ satisfies the recurrence with characteristic polynomial f.

Conversely, since $|R_f| = |\Omega(f)| = q^n$, if we show that the sequences $s(x)$ are all distinct we will have also shown that every sequence in $\Omega(f)$ must occur as $s(x)$ for some $x \in R_f$. We therefore assume by way of contradiction that $s(y) = s(z)$ for some $y \neq z$. If we let $x = y - z$, $s(x) = (0, 0, \ldots, 0)$ or equivalently $t(x\theta^i) = 0$, $i = 0, 1, \ldots, e - 1$. This means that the elements $y_i = x\theta^i$ are all in the nullspace of t, which has dimension $n - 1$, so that the elements $y_0, y_1, \ldots, y_{n-1}$ are linearly dependent; i.e., for certain $b_i \in F_q$ it is true that $\Sigma\, b_i y_i = 0$, so that $x\Sigma\, b_i\theta^i = 0$, which contradicts the fact that the set $\{1, \theta, \theta^2, \ldots, \theta^{n-1}\}$ is linearly independent. Hence $s(y) = s(z)$ implies $y = z$ and so the sequences $s(x)$ are all distinct. This completes the proof of theorem 3.1.

Corollary 3.1: If f is an irreducible polynomial, then R_f is isomorphic with the finite field $GF[q^n]$. In this case for each $s \in \Omega(f)$ it is possible to find an element $x \in GF[q^n]$ such that for all $t \geq 0$,

$$s_t = x\theta^t + x^q\theta^{qt} + \cdots + x^{q^{n-1}}\theta^{q^{n-1}t}. \qquad (3.2)$$

Proof: It is of course one of the fundamental facts about finite fields that $F_q[x]/(f(x)) \cong GF[q^n]$ when f is irreducible of degree n. The corollary follows from theorem 3.1 if we choose the linear functional t to be the trace of $GF[q^n]$ over $GF[q]$; i.e., for $x \in GF[q^n]$, $Tr(x) = x + x^q + \cdots + x^{q^{n-1}}$. (And in fact it is not difficult to prove that every linear functional t of $GF[q^n]$ over $GF[q]$ may be written as $t(x) = Tr(ax)$ for some $a \in GF[q^n]$; so that there is no loss in replacing t by Tr in this case.)

Since by lemma 2.1, the roots of f are $\theta, \theta^q, \ldots, \theta^{q^{n-1}}$, (3.2) is an expression for s_t in terms of the t^{th} powers of the roots of f; and in this way (3.2) resembles the classical method of representing s_t. It is therefore possible to view theorem 3.1 as a generalization of the classical method to the case of finite fields, in which the "roots" of f are thought of as lying in the ring R_f. In some sense, however, the most natural place to look for the roots of f is in the splitting field for f. In the pages to follow, a generalization of (3.2) will be given for arbitrary polynomials f, in which the basic algebraic structure is indeed the splitting field for f. The price we shall have to pay for this is a great deal of increased complexity of the solution. The following discussion follows the classical method as given in Hall [6], as closely as possible, under the circumstances.

With a sequence $s = (s_0, s_1, s_2, \ldots)$ which satisfies a linear recurrence with characteristic polynomial f, and which is considered to be infinite even though we know it is periodic, we associate a formal power series; i.e., an element of $F_q(x)$, as follows:

$$s \to s(x) = \sum_{k=0}^{\infty} s_k x^k \ . \tag{3.3}$$

s(x) is called the generating function for s. (No confusion should arise because the same symbol s(x) was used in theorem 3.1; the notation s(x) in (3.3) is only temporary and will be abandoned shortly.) We emphasize that the series s(x) is to be viewed as an element of $F_q(x)$, and that it is meaningless to ask questions about the "convergence" of (3.3). (3.3) gives a representation of s(x) as a Laurent series; our first step will be to express s(x) as a corresponding rational fraction.

Define $f^*(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + 1$, so that $f^*(x) = x^n f(\frac{1}{x})$. Now let us form the Cauchy product of s(x) and $f^*(x)$ in $F_q(x)$:

$$s(x)f^*(x) = \sum_{k=0}^{\infty} x^k \sum_{j=0}^{k} a_j s_{k-j}; \ a_0 = 1 \ . \tag{3.4}$$
$$a_k = 0, \ k \geq n.$$

For $k \geq n$, the coefficient of x^k in (3.4) vanishes because of the recurrence relation

$$s_t + a_1 s_{t-1} + \cdots + a_n s_{t-n} \ ,$$

so that

$$s(x)f^*(x) = c(x) \ , \tag{3.5}$$

with $c(x)$ a polynomial of degree $\leq n-1$ in $F_q[x]$. (3.5) is the required expression for $s(x)$ as a rational fraction. We suppose that $f(x)$ has the following factorization into irreducible factors in $F_q[x]$:

$$f(x) = \prod_{k=1}^{m} (f_k(x))^{m_k}, \tag{3.6}$$

where degree $(f_k) = d_k$ and so $n = \Sigma d_k m_k$. It follows from (3.6) and the definition of f^* that

$$f^*(x) = \prod_{k=1}^{m} (f_k^*(x))^{m_k}.$$

Then according to a generalized version of "partial fraction" decomposition [12, p. 88], we may use (3.5) to express $s(x)$ uniquely in the following way:

$$s(x) = \sum_{k=1}^{m} \frac{c_k(x)}{(f^*(x))^{m_k}}, \tag{3.7}$$

where each polynomial $c_k(x)$ is of degree $\leq d_k m_k$.

Let us examine more closely expressions of the form

$$\sigma(x) = \frac{c(x)}{(f^*(x))^m},$$

where $f(x)$ is irreducible over F_q and degree $(c(x)) \leq mn$, n = degree (f). If K is a splitting field for f, then $|K:F| = n$, and if θ is one root of f, then by lemma 2.1, the other roots are $\theta^q, \theta^{q^2}, \ldots, \theta^{q^{n-1}}$. We assume that f has exponent e, so that θ will have multiplicative order e. In the field $K(x)$, $f(x)$ factors completely as a product of linear factors, and so also does f^*, so that it is possible to further decompose $\sigma(x)$ into partial fractions in $K(x)$, as follows:

$$\sigma(x) = \sum_{k=0}^{n-1} \sum_{j=1}^{m} \frac{\alpha_{kj}}{(1 - \theta^{q^k} x)^j} , \tag{3.8}$$

where the α_{kj} are uniquely determined elements of K. The field $K(x)$ admits an automorphism A which is induced by the automorphism $A^*: y \to y^q$ of K itself; i.e., if an element $\rho(x) \in K(x)$ has the rational fraction representation

$$\rho(x) = \frac{\Sigma a_i x^i}{\Sigma b_j x^j} ,$$

then

$$A\rho(x) = \frac{\Sigma a_i^q x^i}{\Sigma b_j^q x^j} .$$

Clearly the fixed field of A is $F_q(x)$, and since $\sigma(x) \in F_q(x)$, it follows from (3.8) that

$$\sigma(x) = \sum_{k=0}^{n-1} \sum_{j=1}^{m} \alpha_{k,j}^{q} / (1 - \theta^{q^{k+1}} x)^{j} ,$$

and since the coefficients in (3.8) are unique, we see that $\alpha_{k+1,j} = \alpha_{k,j}^{q}$. (Subscripts reduced modulo n if necessary.) Therefore there are m elements from K, say $\alpha_1, \alpha_2, \ldots, \alpha_m$, such that $\alpha_{k,j} = \alpha_j^{q^k}$, so that

$$\sigma(x) = \sum_{k=0}^{n-1} \sum_{j=1}^{m} \alpha_j^{q^k} / (1 - \theta^{q^k} x)^{j} . \qquad (3.9)$$

We pause for a brief degression. Consider the fraction $(1 + ax)^{-m}$ as an element of $F_q(x)$, $a \in F_q$. We wish to find the Laurent series corresponding to $(1 + ax)^{-m}$, and of course the natural thing to do is use the binomial theorem $(1 + ax)^{-m} = \sum_{k \geq 0} \binom{-m}{k} a^k x^k$. This is in fact valid, but one has to exercise a certain amount of care in defining the "binomial coefficients" $\binom{n}{k}$. The most natural way of defining them from our point of view is by way of the recursion $\binom{n}{k} = \binom{n-1}{k} + \binom{n-1}{k-1}$, along with the boundary conditions $\binom{0}{0} = 1$, $\binom{n}{0} = \binom{n}{n} = 1$ for $n \neq 0$. (Of course these binomial coefficients are the usual ones reduced modulo p, the characteristic of F_q.) The recursive definition allows the usual proof of the binomial theorem to be applied - one uses induction on m, and in $F_q(x)$ there are no convergence problems to complicate the situation.

Thus let us expand the term $(1 - \theta^{q^k} x)^{-j}$ which occurs in (3.9) by the binomial theorem:

$$(1 - \theta^{q^k} x)^{-j} = \sum_{t \geq 0} \binom{-j}{t} (-1)^t (\theta^{q^k} x)^t$$

$$\sum_{t \geq 0} \binom{j+t-1}{t} (\theta^{q^k} x)^t \quad . \tag{3.10}$$

Combining (3.9) and (3.10) we obtain the following Laurent series for $\sigma(x)$:

$$\sigma(x) = \sum_{t \geq 0} x^t \sum_{k=0}^{n-1} \sum_{j=1}^{m} \binom{j+t-1}{t} \alpha_j^{q^k} \theta^{q^k t} \quad . \tag{3.11}$$

The coefficient of x^t in (3.11) may be written as

$$\sum_{k=0}^{n-1} \sum_{j=1}^{m} \left\{ \binom{j+t-1}{t} \alpha_j \theta^t \right\}^{q^k}$$

$$= \sum_{j=1}^{m} \mathrm{Tr} \left\{ \binom{j+t-1}{t} \alpha_j \theta^t \right\} = \mathrm{Tr} \left\{ \theta^t \sum_{j=1}^{m} \binom{j+t-1}{t} \alpha_j \right\}, \tag{3.12}$$

where as before $\mathrm{Tr}(x) = x + x^q + \cdots + x^{q^{n-1}}$ in $GF[q^n]$.

It is possible to put (3.12) into slightly more palatable form as follows: the identity

$$\binom{j+t}{j} = \sum_{i} \binom{j}{i} \binom{t}{i}$$

means that

$$\sum_{j=0}^{m-1} \binom{t+j}{j} \alpha_j = \sum_{j=0}^{m-1} \alpha_j \sum_i \binom{j}{i} \binom{t}{i}$$

$$= \sum_i \binom{t}{i} \sum_{j=0}^{m-1} \alpha_j \binom{j}{i} = \sum_i \binom{t}{i} \gamma_i \ ,$$

where $\gamma_i = \Sigma\, \alpha_j \binom{j}{i}$. Consequently the coefficient of x^t in (3.11) may be written as

$$s_t = \mathrm{Tr}\left\{\theta^t \sum_{j=0}^{m-1} \binom{t}{j} \gamma_j\right\} . \tag{3.13}$$

(3.13) represents the general term of the sequence $s = (s_0, s_1, \ldots, s_t, \ldots)$ of $\Omega(f^m)$, where f is irreducible. In the classical case, the expression (3.13) would be replaced by

$$s_t = \sum_{k=1}^{n} \sum_{j=0}^{m-1} a_{kj} t^j \theta_k^t . \tag{3.14}$$

In 3.14, the elements θ_k are the distinct roots of f; the fact that the roots of f in the case under consideration are all powers of a single one is reflected in the fact that the outer sum in (3.14) is replaced by the trace in (3.13). The really crucial difference between

the two expressions, however, is that the powers t^j in (3.14) have been replaced by what we might call the "binomial functions" $\binom{t}{j}$ in (3.13). The essential reason why no expression of the form (3.14) can represent every $s \in \Omega(f)$ is that the set of functions $\{1, t, t^2, \ldots, t^{m-1}\}$ may fail to be independent in F_q, so that the dimension of the space of all sequences of the form (3.14) will be less than the dimension of the space $\Omega(f^m)$. (For example $t^p = t$ in $GF[q^n]$.) However, the binomial functions $\binom{t}{j}$ are independent over any field[1]; for let us take $\theta = 1$ in (3.13). Then $f(x) = x - 1$, and if there were a linear dependence among the binomial functions $\binom{t}{0}, \binom{t}{1}, \binom{t}{2}, \ldots, \binom{t}{m-1}$ with coefficients from F_p, then the space of all sequences of the form (3.13) would have dimension strictly less than m; but we have proved that every sequence in $\Omega(f^m)$ is of the form (3.13), so no linear dependence is possible. (Of course a linear dependence in a larger field implies a linear dependence in F_p.)

Let us extend (3.13) to the more general case where f(x) has the factorization given by (3.6). It is clear how to proceed, since at the earliest stage (3.7), s(x) was decomposed into partial fractions whose denominators were irreducible powers. We simply observe that in a splitting field for f(x), say $GF[q^d]$, d = l.c.m. $(d_1, d_2, \ldots, d_m)$, it is always possible to find a primitive element θ of multiplicative order e' = l.c.m. $(e_1, e_2, \ldots, e_m)$ where e_i is the exponent of f_i, and integers $b_1, b_2, \ldots, b_m$, such that

---

[1] Although the fact shall not concern us here, it is possible to extend the classical method to arbitrary (not necessarily finite) fields of characteristic p. Naturally we could in general lose the fact that the roots are powers of each other, but the binomial functions would enable us to handle multiple roots with no difficulty.

θ^{b_i} is a root of f_i in $GF[q^{d_i}]$. Combining these remarks with the expressions (3.7) and (3.13), we obtain

Theorem 3.2: Let $f \in F_q[x]$ have the factorization $f(x) = \prod_{k=1}^{m} (f_k(x))^{m_k}$, with each f_k irreducible of degree d_k. Then if $GF[q^d]$ is a splitting field for f, there is a primitive element $\theta \in GF[q^d]$ and integers $b_1, b_2, \ldots, b_m$ such that $f_k(\theta^{b_k}) = 0$. Furthermore, for any sequence $s \in \Omega(f)$ it is possible to find elements $\gamma_j^{(i)} \in GF[q^{d_i}]$ $i = 1, 2, \ldots, m$ $j = 0, 1, \ldots, m_i - 1$ such that for each $t \geq 0$,

$$s_t = \sum_{i=1}^{m} Tr^{(i)} \left\{ \theta^{b_i t} \sum_{j=0}^{m_i - 1} \binom{t}{j} \gamma_j^{(i)} \right\},$$

where $Tr^{(i)}$ is the trace on $GF[q^{d_i}]$ over F_q; i.e., $Tr^{(i)}(x) = x + x^q + \cdots + x^{q^{d_i - 1}}$.

We emphasize once more that theorem 3.2 is most valuable when f(x) has multiple roots; indeed, results essentially equivalent to theorem 3.2 are known when f is squarefree [8], or if f', the formal derivative of f, is squarefree [14].

As an application of some of these ideas, let us return to the case of a power of an irreducible polynomial f(x) of degree n, exponent e. Our goal is to give a relationship between the solution spaces $\Omega(f^m)$ and $\Omega(f)$. In view of (3.13), it will plainly be helpful to know the properties of the sequence (r_t) whose general term is $r_t = \binom{t}{r}$ for a fixed integer r. In this case the generating function for (r_t) is

$$p(x) = \sum_{t \geq 0} \binom{t}{r} x^t = x^r \sum_{t \geq 0} \binom{r+t}{r} x^t$$

$$= x^r \sum_{t \geq 0} (-1)^t \binom{-(r+1)}{t} x^t = \frac{x^r}{(1-x)^{r+1}} .$$

If the sequence (r_t) is to be periodic of period n, it must be true that $(1-x)^{r+1} \mid (1-x^n)$, since the Laurent series corresponding to $1/(1-x^n)$ is $1+x^n + x^{2n} + \cdots$. Suppose therefore that $n = n_0 p^f$ with $(n_0, p) = 1$. Then

$$1 - x^n = 1 - x^{n_0 p^f} = (1 - x^{p^f})(1 + x^{2p^f} + \cdots + x^{(n_0 - 1)p^f})$$

$$= (1 - x)^{p^e} Q(x) ,$$

where $Q(1) = n_0 \neq 0$, so that $(1 - x)^{r+1} \mid 1 - x^n$ if and only if $r + 1 \leq p^e$. Therefore the sequence (r_t) of binomial coefficients is periodic of period p^e, where e is the least integer such that $r + 1 \leq p^e$, and (r_t) is not periodic for any smaller value.

We wish to apply the preceding remarks to formula (3.13), which involves the binomial coefficients $\binom{t}{0}, \binom{t}{1}, \ldots, \binom{t}{m-1}$. Hence if μ is the unique integer which satisfies $p^{\mu-1} < m \leq p^\mu$, then each of the binomial coefficients will be constant on residue classes (mod p^μ).

Let $b = p^\mu$. We perform an operation, called decimation by b, on a sequence defined by (3.13), as follows: define b new

sequences $(s_t^{(i)})$ $i = 1, 2, \ldots, b$:

$$s_t^{(i)} = s_{bt+i} \ ,$$

i.e., the sequence $(s_t^{(i)})$ is formed from (s_t) by taking only those terms whose subscripts lie in the residue class containing i (mod b).

Then from (3.13),

$$s_t^{(i)} = \mathrm{Tr}\left\{\theta^i(\theta^b)^t \sum_{j=0}^{m-1} \binom{bt+i}{j}\gamma_j\right\}$$

$$= \mathrm{Tr}\left\{\theta^i(\theta^b)^t \sum \binom{i}{j}\gamma_j\right\} \ ,$$

since we have seen that $\binom{bt+i}{j} = \binom{i}{j}$ in F_p. (Of course the above calculations are performed in $GF[q^n]$, a splitting field for f(x).) Continuing,

$$s_t^{(i)} = \mathrm{Tr}\left\{\theta^i\beta_i(\theta^b)^t\right\}, \text{ with } \beta_i = \sum_{j=0}^{m-1} \binom{i}{j}\gamma_j \ . \qquad (3.15)$$

Formula (3.15) resembles the formula for a sequence from $\Omega(f)$, with one exception: the root θ is replaced by θ^b in (3.15). But this anomaly is easily understood: in $GF[q^n]$, the minimum polynomial for θ^b is $f^{(b)}$, the polynomial formed from f by raising each coefficient of f to the b^{th} power. (Recall $b = p^\mu$ so that $f^{(b)}(\theta^b) = (f(\theta))^b = 0$.) Hence (3.15) represents a sequence from

$\Omega(f^{(b)})$, rather than one from $\Omega(f)$ itself. (Of course if $q = p^r$ and $r \mid \mu$, $f = f^{(b)}$.) Thus according to the definition of the sequences $s_t^{(i)}$, the sequence $s^t \in \Omega(f^m)$ is formed by <u>interleaving</u> certain sequences from $\Omega(f^{(b)})$. But it does not follow that given any collection of b sequences from $\Omega(f^{(b)})$ it is possible to interleave them and obtain a sequence from $\Omega(f^m)$. Indeed, there are q^{nb} sequences which may be formed by interleaving sequences from $\Omega(f^{(b)})$, but only q^{nm} sequences in $\Omega(f^m)$. We shall now derive a relationship among the field elements β_i which appear in (3.15) which is both necessary and sufficient to ensure that the sequences $s_t^{(i)}$ may be interleaved to be obtained a sequence, viz,

$$\sum_{k=0}^{m} (-1)^k \binom{m}{k} \beta_{k+r} = 0 \qquad r \geq 0. \tag{3.16}$$

For proof we present the following calculations. For simplicity we omit limits of summation, it being understood that undefined summands are all zero:

$$\sum (-1)^k \binom{m}{k} \beta_k = \sum_{k,j} (-1)^k \binom{m}{k} \binom{k+r}{j} \gamma_j \quad \text{by (3.15)}$$

$$= \sum_{i,j,k} (-1)^k \binom{m}{k} \binom{k}{i} \binom{r}{j-i} \gamma_j = \sum_{i,j,k} (-1)^k \binom{m}{i} \binom{m-i}{k-i} \binom{r}{j-i} \gamma_j .$$

The sum on k is

$$\sum_k (-1)^k \binom{m-i}{k-i} = \sum_k (-1)^k \binom{m-i}{m-k} = \sum_k (-1)^{m-k} \binom{m-i}{k}$$

$$= (1 - 1)^{m-i} = 0 \quad \text{for } i < m .$$

Thus the β_i's themselves satisfy a linear recurrence relation (3.16) with characteristic polynomial $(x - 1)^m$. Conversely, given any set of β's which satisfy (3.16), it is possible to recover the γ's and obtain an element of $\Omega(f^m)$ by interlacing the corresponding $s_t^{(i)}$'s. This can be done by inverting the formula (3.15) for the β's, but an easier way is to observe that there are q^{nm} possible selections for the β's subject to (3.16), and this is precisely the number of elements in $\Omega(f^m)$. We summarize these results in a theorem:

Theorem 3.3: If $f(x)$ is irreducible of degree n, then every sequence in $\Omega(f^m)$ may be obtained by "interleaving" b sequences from $\Omega(f^{(b)})$. Here $b = p^\mu$ is the unique power of p such that $p^{\mu-1} < m \leq p^\mu$. Furthermore, a set of b sequences $s_t^{(i)}$ $i = 1, 2, \ldots, b$ which correspond to the elements $\theta^i \beta_i$ in $GF[q^n]$ (with $f(\theta) = 0$) in the isomorphism between $\Omega(f^{(b)})$ and $GF[q^n]$ may be interleaved to form a sequence from $\Omega(f^m)$ if and only if the sequence $(\beta_0, \beta_1, \ldots)$ satisfies the linear recurrence over $GF[q^n]$ whose characteristic polynomial is $(x - 1)^m$.

Theorem 3.3 is known in the special case that $m = q^c$ for some integer c [14, lemma 12]. Of course in this case $f^{(b)} = f$ and $b = m$, so that there is no relation imposed upon the β's.

We present another application of theorem 3.2 which involves the nation of decimation and is of interest. We assume for the following discussion that f(x) is an irreducible polynomial of degree n in $F_q[x]$, and that f belongs to exponent e, $eE = q^n - 1$.

It frequently happens that one is interested only in knowing the way in which the residue from F_q are distributed among the various sequences in $\Omega(f)$. From this point of view, a complete knowledge of $\Omega(f)$ will consist of a list of distributions which occur in $\Omega(f)$, along with their multiplicities; in such a case there will of course be no need to distinguish between a sequence $s = (s_0, s_1, \ldots, s_{e-1})$ and one of its translates, say $(s_k, s_{k+1}, \ldots, s_{e-1}, s_0, \ldots, s_{k-1})$. We therefore (ignoring the all-zero sequence) view $\Omega(f)$ not as a collection of q^n-1 sequences, but rather as a collection of $(q^n-1)/e = E$ cycles. (A cycle is nothing but a sequence whose starting point is considered irrelevant.) It is well known [10] that when f is irreducible, no sequence from $\Omega(f)$ except the all-zero sequence has a period which is shorter than e, so that for each sequence s, all of its e translates are distinct. In terms of the isomorphism provided by corollary 3.1, this point of view amounts to regarding two elements of $R_f \cong GF[q^n]$ as indistinguishable if they are in the same coset of the subgroup $T = \{1, \theta, \theta^2, \ldots, \theta^{e-1}\}$. The question about the distributions which occur in $\Omega(f)$ can be rephrased as follows:

> "How are the values of the trace distributed among the cosets of T?" (3.17)

We shall be able to simplify question (3.17) somewhat by exhibiting a trace-preserving automorphism of $GF[q^n]$ which permutes the cosets of T; viz, the automorphism $\alpha: x \to x^q$. To

show that this automorphism does in fact permute the cosets, suppose that $xy^{-1} = \theta^r$ for some r; i.e., that x and y are in the same coset of T. Then $x^q y^{-q} = (xy^{-1})^q = \theta^{rq} \in T$. Therefore the set X of cosets of T admits a cyclic permutation group $A = \{1, \alpha, \ldots, \alpha^{n-1}\}$. Clearly two cosets in the same orbit of X under A will have the same distribution of trace values, since $Tr(x) = Tr(x^q)$.

Theorem 3.4: The number of orbits of X under the action of A is the same as the number of irreducible factors of $X^E - 1$ in $F_q[x]$.

Proof: Choose ψ as a primitive root for $GF[q^n]$ such that $\theta = \psi^E$, so that $T = \{1, \psi^E, \psi^{2E}, \ldots, \psi^{(e-1)E}\}$. It is clear that the coset of T to which an element ψ^s belongs is determined by the value of s modulo E. Thus if $x = \psi^s$ is taken as a coset representative of Tx, the successive images of Tx under α are $T\psi^s$, $T\psi^{sq}$, ..., so that the number of cosets in the orbit of Tx is the least integer m such that $sq^m \equiv s \pmod{E}$. But the process of mapping the residues modulo E into themselves by $x \to x^q$ is exactly the process described in chapter 1 for determining the number of irreducible factors of $x^E - 1$. This proves theorem 3.4.

Corollary 3.2: The number of distinct distributions which occur in $\Omega(f)$ is less than or equal to the number of irreducible factors of $x^E - 1$.

Corollary 3.2 is sometimes very accurate in giving the number of distributions in $\Omega(f)$, but usually not. It is possible, however, to formulate an amusing converse to corollary 3.2 which

will provide us with a large number of polynomials for which the bound is quite good.

Theorem 3.5: For any integer E such that $(E, q) = 1$, there are infinitely many irreducible polynomials f_t with degrees n_t and exponents e_t, such that $e_t E = q^{n_t} - 1$.

Proof: Suppose φ is the exponent to which q belongs modulo E. For each $t \geq 1$, let $e_t = \frac{1}{E}(q^{\varphi t} - 1)$. As pointed out in chapter II, for each exponent e prime to q, there is at least one polynomial f of exponent e, and the degree of f is the exponent to which q belongs modulo e. For each t, we let f_t be one such polynomial (i.e., with exponent e_t), and we shall show that with the possible exception of $t = 1$, each f_t has degree $n_t = \varphi t$. Since $q^{\varphi t} \equiv 1 \pmod{E}$, it follows that $n_t \mid \varphi t$. But since

$$(q^{n_t} - 1)/\frac{q^{\varphi t} - 1}{E} = E \cdot \frac{q^{n_t} - 1}{q^{\varphi t} - 1},$$

it follows that $(q^{\varphi t} - 1)/(q^{n_t} - 1)$ must be a divisor of E and therefore $\leq E$. But for $t \geq 2$, and $n_t < \varphi t$,

$$\frac{q^{\varphi t} - 1}{q^{n_t} - 1} > q^{\varphi t - n_t} \geq q^{\varphi \frac{t}{2}} \geq q^{\varphi} > E,$$

a contradiction. (For $t = 1$, there may or may not be an exception. This is illustrated by $q = 2$, $E = 5$ in which case $t = 1$ is exceptional,

and $E = 11$ for which $t = 1$ is not exceptional.) This completes the proof of theorem 3.5.

Corollary 3.2 gives most information when E is such that $x^E - 1$ has few factors; an especially interesting case is when $x^E - 1$ has only the two irreducible factors $x - 1$ and $x^{E-1} + x^{E-2} + \cdots + x + 1$; it follows from the remarks in chapter 1 that this will be the case if and only if E is a prime for which q is a primitive root; so that with the aid of theorem 3.5 and a list of the primes for which q is a primitive root it is possible to find a very large number of irreducible polynomials f such that $\Omega(f)$ contains only two (non-zero) distinct distributions. In these cases it is usually possible to determine the distributions exactly; for an example see the end of chapter IV.

IV. A THEOREM ON SYMMETRIC FUNCTIONS

This chapter does not deal directly with linear recurrence relations but presents certain results which will be needed in chapter V. Some of these results appear in [11].

Consider the algebra of all symmetric "polynomials" in a countably infinite set of variables $x_1, x_2, \ldots$, with coefficients in a field F. Of course by "polynomial" we mean merely that the functions in question are formal sums of monomials $x_{i_1}^{a_1} x_{i_2}^{a_2} \cdots x_{i_r}^{a_r}$; such functions, being symmetric, must all have infinitely many terms. We shall frequently make statements such as "the symmetric function of $(y_1, y_2, \ldots, y_n)$". This should be interpreted to mean "the symmetric function of $(x_1, x_2, \ldots)$ with the substitution $x_1 = y_1, \ldots, x_n = y_n, x_{n+1} = x_{n+2} = \cdots = 0$".

If A_n is the space of all symmetric polynomials which are homogeneous of degree n, then it is known that a basis for A_n will be formed by the monomial symmetric functions k_λ defined by

$$k_\lambda = [\lambda_1, \lambda_2, \ldots, \lambda_r] = \sum_{\text{sym}} x_1^{\lambda_1} x_2^{\lambda_2} \cdots x_r^{\lambda_r}, \qquad (4.1)$$

where $\lambda = (\lambda_1, \lambda_2, \ldots, \lambda_r)$ is any partition of the integer n (i.e., the λ_i's are positive integers and $\lambda_1 + \cdots + \lambda_r = n$), and by the usual convention, the sum on the right-hand side of (4.1) is taken over all distinct monomials which can be obtained from the one actually written by permutations of the variables $(x_1, x_2, \ldots)$. When no confusion will arise, the abbreviation "sym" on symmetric

sums of the form (4.1) will be omitted. As an example, let $n = 6$ and $\lambda = (4, 2, 2)$. The symmetric function k_λ of the variables x_1, x_2, x_3, x_4 is given by

$$\begin{aligned} k_\lambda = [4, 2, 2] = {} & x_1^4 x_2^2 x_3^2 + x_1^4 x_2^2 x_4^2 + x_1^4 x_3^2 x_4^2 \\ & + x_2^4 x_1^2 x_3^2 + x_2^4 x_1^2 x_4^2 + x_2^4 x_3^2 x_4^2 \\ & + x_3^4 x_1^2 x_2^2 + x_3^4 x_1^2 x_4^2 + x_3^4 x_2^2 x_4^2 \\ & + x_4^4 x_1^2 x_2^2 + x_4^4 x_1^2 x_3^2 + x_4^4 x_2^2 x_3^2 . \end{aligned}$$

If repetitions occur among the integers $\lambda_1, \lambda_2, \ldots$, it is customary to write

$$\lambda = (1^{m_1} 2^{m_2} 3^{m_3} \cdots) \tag{4.2}$$

which means that the partition λ involves m_1 ones, m_2 twos, etc. Thus we write $(2^2 4)$ in place of $(4, 2, 2)$.

Besides the k_λ's, there are several other important bases for A_n; we present here only the two which will concern us in the applications:

(1). The elementary symmetric functions a_m are the functions $[1^m]$; i.e., $a_m = \Sigma\, x_1 x_2 \cdots x_m$. For a partition $\lambda = (\lambda_1, \lambda_2, \ldots)$ of n write $a_\lambda = a_{\lambda_1} a_{\lambda_2} \cdots$. The fact that the a_λ form a basis for A_n is called the Fundamental Theorem on Symmetric Functions. [12, p. 78].

(2). The power sum symmetric functions s_m are the functions $[m]$; i.e., $s_m = \Sigma\, x_1^m$. For a partition $\lambda = (\lambda_1, \lambda_2, \ldots, \lambda_r)$ of n write $s_\lambda = s_{\lambda_1} s_{\lambda_2} \ldots s_{\lambda_r}$. The functions s_λ form a basis for A_n whenever F has characteristic zero.

The important difference between the bases $\{a_\lambda\}$ and $\{s_\lambda\}$ of A_n when F has characteristic zero is that the $\{a_\lambda\}$ form an integral basis for A_n relative to the basis $\{k_\lambda\}$, while the $\{s_\lambda\}$ do not. Thus a symmetric function which has integral coefficients when expressed in terms of the k_λ's will also have integral coefficients when expressed in terms of the a_λ's, but this will not necessarily be the case when the function is expressed in terms of the s_λ's. It is for this reason that the s_λ's cannot form a basis for A_n when F has characteristic $p > 0$; indeed $s_1^p = s_p$ in such a field, so that the set $\{s_\lambda\}$ is not linearly independent.[1]

The aim of this chapter is to express the functions k_λ in terms of the functions s_λ, in the case that F has characteristic zero. Surprisingly, it will be possible to apply this result under certain special circumstances to fields of prime characteristic.

Let us fix λ and n for the rest of the chapter, with $\lambda = (\lambda_1, \lambda_2, \ldots, \lambda_r)$ and with multiplicities m_i as given in (4.2). We define a new function h_λ of the variables $(x_1, x_2, \ldots)$ as follows:

---

[1] What is not difficult to show is that when the field F has characteristic p, the dimension of the subspace of A_n spanned by $\{s_\lambda\}$ is exactly the number of partitions of n in which each summand is $\leq p - 1$.

$$h_\lambda = (\prod_i m_i\,!)k_\lambda = \sum_{\mathrm{sym}(*)} x_1^{\lambda_1} x_2^{\lambda_2} \cdots x_r^{\lambda_r}, \qquad (4.3)$$

where the summation "sym(*)" is extended over all r! monomials obtainable from the one actually written by permutations of the variables (1, 2, ..., r). Of course (4.3) follows since each distinct monomial appearing in the sum k_λ occurs $\prod m_i!$ times in the sum h_λ. Another way to look at (4.3) is to regard the integers $(\lambda_1, \lambda_2, \ldots, \lambda_r)$ to be formally distinct; perhaps one could "label" two identical integers with subscripts. For example $(2^2 4)$ becomes $(2_1, 2_2, 4)$. From this point of view the function h_λ is no different from k_λ, since now every monomial $x_{i_1}^{\lambda_1} x_{i_2}^{\lambda_2} \cdots x_{i_r}^{\lambda_r}$ is distinguishable from every other.

Now consider the set P_λ of all partitions of the set $\lambda = \{\lambda_1, \lambda_2, \ldots, \lambda_r\}$, regarding the λ_i as a set of formally distinct symbols. (It will always be clear whether we are viewing λ as a collection of integers or as a set of symbols, so that we need not formally distinguish these logical differences.) A partition π of the set P_λ is a way to write P_λ as a disjoint union of subsets B_k, called blocks:

$$\pi: \lambda = \bigcup_{k=1}^{\ell} B_k, \qquad (4.4)$$

with $B_i \cap B_j = \Phi$ if $i \neq j$ and $B_k \neq \Phi$ for all k. ℓ is called the length of the partition π.

It is possible to introduce a partial order "$\geq$" on P_λ in such a way that P_λ becomes a lattice: if π and π' are both partitions of λ, write $\pi \geq \pi'$ if and only if every block of π is a subset of some block of π'; i.e., $\pi \geq \pi'$ if π is a refinement of π'. It is easy to show [9] that under this partial ordering, P_λ becomes a lattice with top element (maximal with respect to $\geq$) t, where t is the partition $\{\lambda_1\}\{\lambda_2\}\cdots\{\lambda_r\}$.

With each element $\pi \in P_\lambda$, given by (4.4), we recall that the elements of λ are really integers and define, for each $k = 1, 2, \ldots, \ell$

$$\beta_k = \sum_{\lambda_j \in B_k} \lambda_j \,. \tag{4.5}$$

We now associate with π two symmetric polynomials in $(x_1, x_2, \ldots)$; they are $f(\pi) = h_{\beta_1} h_{\beta_2} \cdots h_{\beta_\ell}$, and $g(\pi) = h_\beta$, where $\beta = (\beta_1, \beta_2, \ldots, \beta_\ell)$ is the partition of n given by (4.5), and the functions h are given by (4.3). For example, if $\lambda = \{\lambda_1, \lambda_2, \lambda_3, \lambda_4, \lambda_5\}$ and π is $\{\lambda_1, \lambda_3, \lambda_4\}\{\lambda_2, \lambda_6\}\{\lambda_5\}$, then

$$f(\pi) = h_{\lambda_1 + \lambda_3 + \lambda_4} h_{\lambda_2 + \lambda_6} h_{\lambda_5}, \text{ and}$$

$$g(\pi) = h_{\lambda_1 + \lambda_3 + \lambda_4, \lambda_2 + \lambda_6, \lambda_5} \,.$$

The following lemma is the crux of the matter:

Lemma 4.1: $f(\pi) = \sum_{\pi' \leq \pi} g(\pi')$

Proof: By definition,

$$f(\pi) = (\sum x_1^{\beta_1})(\sum x_1^{\beta_2}) \cdots (\sum x_1^{\beta_\ell}) ,$$

where the sums are symmetric by the convention (4.1). We expand this as

$$f(\pi) = \sum x_{i_1}^{\beta_1} x_{i_2}^{\beta_2} \cdots x_{i_\ell}^{\beta_\ell} , \tag{4.6}$$

and this sum is extended over all possible monomials obtainable by selection of ℓ of the variables $x_1, x_2, \ldots$. We do not require that the subscripts $i_1, i_2, \ldots, i_\ell$ be distinct.

Let $B = \{B_1, B_2, \ldots, B_\ell\}$, and to each monomial which occurs in the summation (4.6) we assign a partition of B as follows: B_s and B_t are to be in the same block of the partition if and only if $i_s = i_t$. We call two such monomials equivalent if they induce the same partition of B. Now to each equivalence class of monomials there corresponds in a natural way a partition $\pi' \in P_\lambda$ with $\pi' \leq \pi$; i.e., to a partition of B such as $\{B_{i_1}, B_{i_2}, \ldots\}\{B_{j_1}, B_{j_2}, \ldots\}\ldots$ we associate the following partition of λ: $\{B_{i_1} \cup B_{i_2} \cup \cdots\}$ $\{B_{j_1} \cup B_{j_2} \cup \cdots\} \cdots$. It is clear that the sum of the monomials of (4.6) which belong to a fixed equivalence class is a $g(\pi')$ for some

$\pi' \leq \pi$, and conversely, given any $\pi' \leq \pi$ there is an equivalence class corresponding to π' which contributes $g(\pi')$ to (4.6). This completes the proof of lemma 4.1.

In view of lemma 4.1, it is now possible to apply Möbius inversion on the lattice P_λ in order to calculate the functions $g(\pi)$:

$$g(\pi) = \sum_{\pi' \leq \pi} \mu(\pi')f(\pi') \quad , \tag{4.7}$$

where $\mu(\pi')$ is the Möbius function associated with P_λ. (For details about Möbius inversion on a lattice, see [9].) In particular, we apply (4.7) with $\pi = t$, the top element of P_λ, and obtain

$$h_\lambda = g(t) = \sum_{\pi \in P_\lambda} \mu(\pi)f(\pi) \, . \tag{4.8}$$

(4.8) is almost an explicit expression for h_λ in terms of the power-sum functions $f(\pi)$; all that lacks is the function $\mu(\pi)$ for the lattice. Fortunately this function has already been calculated [9]; if the partition π is given by (4.4), and if $|B_k| = b_k > 0$, then

$$\mu(\pi) = (-1)^{r-\ell} \prod_{k=1}^{\ell} (b_k - 1)! \tag{4.9}$$

We combine these results in a theorem:

Theorem 4.1: If $\lambda = (1^{m_1} 2^{m_2} \cdots)$ is a partition of n, then in a field F of characteristic zero,

$$k_\lambda = \frac{1}{\pi m_i!} \sum_{\pi \in P_\lambda} \mu(\pi) f(\pi)$$

with the Möbius function μ given by (4.9).

The cases $r = 1$ and $r = 2$ of theorem 4.1 appear in MacMahon [7, p. 7], where, however, he dismisses the results with the remark "In actual practice there are easier ways of calculating the many-part [monomial symmetric] functions and the general formula is of little importance."

With the aid of theorem 4.1 it is possible to compute the functions k_λ in the special case that the x_i ($i = 1, 2, \ldots, m$) are the e^{th} roots of unity in F, and $x_{e+1} = x_{e+2} = \cdots = 0$, remembering always that F is of characteristic zero. In this case we know that the functions s_m are all zero, unless $m \equiv 0 \pmod{e}$, in which case $s_m = e$. When applying theorem 4.1, therefore we need only include those partitions $\pi \in P_\lambda$ whose associated numbers β_k given by (4.5) are all multiples of e. We denote that subset of P_λ by P_λ^e, and so for the e^{th} roots of unity theorem 4.1 becomes

$$k_\lambda = \frac{1}{\pi m_i!} \sum_{\pi \in P_\lambda^e} \mu(\pi) e^{\ell(\pi)}, \tag{4.10}$$

where $\ell(\pi)$ is the length of the partition π. In particular we see that $k_\lambda = 0$ unless $e \mid (\lambda_1 + \lambda_2 + \cdots + \lambda_r)$, but it is not difficult to show this directly.

Finally we discuss the possibility of relaxing the assumption that F has characteristic zero, at least for the application (4.10).

Although we have chosen to expand k_λ in terms of the functions s_λ it is nevertheless also possible to expand it in terms of the functions a_λ, at least in theory. Since the functions a_λ form an integral basis for the space A_n, such an expansion will have the form

$$k_\lambda = \sum_\mu c_\mu a_\mu, \tag{4.11}$$

where the summation is extended over all partitions of the integer n, and each c_μ is an integer (possibly negative or zero.) Furthermore (4.11) is a polynomial identity, and so it is valid over any field, although naturally in a field of characteristic $p > 0$ one would reduce the coefficients c_μ modulo p. If the variables x_i are the e^{th} roots of unity, the statement "the elementary symmetric functions a_m are all zero except that $a_e = (-1)^{e+1}$," is true in any field, so that in order to calculate the functions k_λ of the e^{th} roots of unity we need only insert the values of the appropriate a_λ (which do not depend on the field) into (4.11) and reduce the resulting expression modulo the characteristic of the field. <u>But it is equally possible to find the value of (4.11) by using (4.10).</u> Therefore it is possible to compute the k_λ in <u>any</u> field by using (4.10):

<u>Theorem 4.2</u>: Let F be a field of characteristic $p > 0$. In order to compute the symmetric function k_λ of the e^{th} roots of unity in F, it is sufficient to compute the same function in the rational field and reduce the resulting expression modulo p.

A careful application of (4.10), which is permissible because of theorem 4.2, will allow us to prove the main theorem of chapter V.

V. A COMBINATORIAL APPROACH

Throughout this chapter $F = F_p$ will be a finite prime field. Let $V = V_e(F)$ be on e-dimensional vector space over F whose elements are the e-tuples $v = (v_0, v_1, \ldots, v_{e-1})$ with entries from F. For each $a \in F$, we define a function $N(v;a)$: $N(v;a)$ is the number of times the element a occurs as a component for v. The function $N(v;a)$ is not easily studied; let us instead write it in its formal p-ary expansion:

$$N(v;a) = \sum_{k \geq 0} N_k(v;a) p^k . \tag{5.1}$$

Thus $N_k(v;a)$ represents the k^{th} digit in the p-ary expansion of the number of a's which appear as coordinates for v. The advantage of expanding $N(v;a)$ as in (5.1) is that it is possible to view the functions $N_k(v;a)$ as mappings from V into F by regarding an integer between 0 and p - 1 as an element in the field F. Furthermore, since F is finite each function $N_k(v;a)$ is in fact a polynomial in the coordinates $(v_0, v_1, \ldots, v_{e-1})$. (To prove this one could use an interpolation argument.) Also the function N_k is clearly invariant under permutations of the coordinates of v, so that it is in fact a symmetric polynomial. We need not appeal to these abstract considerations, however, because of

Theorem 5.1: $N_k(v;a) = a_{p^k}(1-(v_0-a)^{p-1}, 1-(v_1-a)^{p-1}, \ldots, 1-(v_{e-1}-1)^{p-1})$.

Proof: The abbreviation on the right-hand side of the equation is to represent the symmetric function a_{p^k} of the variables $y_i = 1-(v_i-a)^{p-1}$, $i = 0, 1, \ldots, e-1$. Notice that the y_i have the property that $y_i = 1$ if $v_i = a$, and $y_i = 0$ otherwise. Theorem 5.1 is a consequence of Lucas' theorem 2.3: in theorem 2.3 take $m = p^k$. We obtain that $n_k \equiv \binom{n}{p^k} \pmod p$. Hence $N_k(v;a) \equiv \binom{N(v;a)}{p^k} \pmod p$, so that if we apply a_{p^k} to the variables $y_0, y_1, \ldots, y_{e-1}$, we get a contribution of 1 for each subset of order p^k from $(y_0, y_1, \ldots, y_{e-1})$ which has the form $(1, 1, \ldots, 1)$. This completes the proof of theorem 5.1.

Theorem 5.1 shows not only that N_k is a symmetric polynomial, but also that it has degree $p^k(p-1)$. Hence according to the fundamental theorem on symmetric functions it is possible to express $N_k(v;a)$ as a polynomial with integral coefficients in the symmetric functions a_λ:

$$N_k(v;a) = \sum_\lambda c_\lambda a_\lambda , \tag{5.2}$$

where the summation is extended over all partitions of all integers $\leq p^k(p-1)$, and the c_λ are integers.

The object of this chapter is to apply theorem 3.2, together with (5.2), in order to obtain information about the functions N_k. We shall depend heavily on the results of chapter IV.

Let $f(x)$ be a polynomial $F_p[x]$ which has no repeated roots in a splitting field; $f(x) = f_1(x)f_2(x) \cdots f_m(x)$ with the f_i distinct and irreducible. If θ is a root of $f(x)$ in a splitting field

F^*, and if f_i has degree n_i and exponent e_i, we may assume that $F^* = GF[p^n]$ where $n = \text{l. c. m. } (n_1, n_2, \ldots, n_m)$, and that θ is a primitive e^{th} root of unity with $e = \text{l. c. m. } (e_1, e_2, \ldots, e_m)$. If $g_i = e/e_i$, then it may also be assumed that θ^{g_i} is a primitive e_i^{th} root of unity in $GF[p^{n_i}]$ and $f_i(\theta^{g_i}) = 0$.

We apply theorem 3.2 to the polynomial f; it tells us that for any sequence $(s_t) \in \Omega(f)$, it is possible to write the general term as

$$s_t = \sum_{i=1}^{m} \mathrm{Tr}^{(i)} (x_i \theta^{g_i t}) , \tag{5.3}$$

where $\mathrm{Tr}^{(i)}$ is the trace of $GF[p^{n_i}]$ over $GF[p]$ and the x_i are suitably chosen elements of the corresponding fields $GF[p^{n_i}]$. Let us expand (5.3) by using the algebraic form for the trace: $\mathrm{Tr}^{(i)}(x) = x + x^p + \cdots + x^{p^{n_i-1}}$:

$$s_t = \sum_{i=1}^{m} \sum_{j=0}^{n_i-1} (x_i (\theta^t)^{g_i})^{p^j} . \tag{5.4}$$

We regard the expression (5.4) as a polynomial in θ^t, say $s_t = P(\theta^t)$, where

$$P(\varphi) = \sum_{i=1}^{m} \sum_{j=0}^{n_i-1} (x_i \varphi^{g_i})^{p^j} = \sum_{k \in K} c_k \varphi^k . \tag{5.5}$$

In (5.5), the set K is the set of integers k which the coefficient of x^k in $P(\varphi)$ is formally different from zero. It is clear from (5.5) that the set K is precisely the set $\{g_i p^j : i = 1, 2, \ldots, m;\ j = 0, 1, \ldots, n_i - 1\}$. The integers $g_i p^j$ are all distinct since f is assumed to have no repeated roots, and so the coefficient of $\varphi^{g_i p^j}$ in (5.5) is $x_i^{p^j}$.

(There is nothing new about regarding (5.4) as a polynomial in φ^t in the case that f is squarefree; the idea is due to Mattson and Solomon [8]. The point to be emphasized is that the only case when theorem 3.2 yields such a polynomial is when f is squarefree, on account of the presence of the nonconstant binomial coefficients $\binom{t}{j}$ when f has a repeated factor.)

Using the polynomial P of (5.5) it is possible to express an element $(s_t) \in \Omega(f)$ in the following form:

$$s = (P(\theta^0),\ P(\theta^1),\ \ldots,\ P(\theta^{e-1})).$$

We wish to compute the functions $N_k(v;a)$ for each $v \in \Omega(f)$, with $\Omega(f)$ regarded as a subspace $V_e(F)$. To do this, we must apply theorem 5.1 along with expression (5.2), and compute the various functions $a_r(P(\theta^0),\ P(\theta^1),\ \ldots,\ P(\theta^{e-1}))$. This function is

$$a_r = \sum_{\text{sym}} P(\theta^0)P(\theta^1)\cdots P(\theta^r) = \sum_{\text{sym}} \prod_{j=1}^{r} \sum_{k \in K} c_k(\theta^j)^k. \qquad (5.6)$$

We shift our emphasis and regard (5.6) not as a polynomial in the single variable θ, but rather as a polynomial in the c_k's.

From this point of view (5.6) is a linear combination of monomials $c_{k_1} c_{k_2} \cdots c_{k_r}$. To simplify the notation we replace θ^j by θ_j; then the coefficient of $c_{k_1} c_{k_2} \cdots c_{k_r}$ in (5.6) is clearly

$\sum_{\text{sym}} \theta_0^{k_1} \theta_2^{k_2} \cdots \theta_{r-1}^{k_r}$, so that

$$a_r = \sum_{(\lambda)} k_\lambda c_\lambda \ , \tag{5.7}$$

where the summation (λ) is extended over all unordered collections $\lambda = (k_1, k_2, \ldots, k_r)$ of integers from K, c_λ is short for $c_{k_1} c_{k_2} \cdots c_{k_r}$, and k_λ is the monomial symmetric function of the variables $\theta_0, \theta_1, \ldots, \theta_{e-1}$. (5.7) is why the results of chapter IV will be needed; for the k_λ in (5.7) are the symmetric functions of the θ_j, which are the e^{th} roots of unity in $GF[p^n]$, so that theorem 4.2 will apply.

As we remarked after (4.10), the functions k_λ are all zero unless $k_1 + k_2 + \cdots + k_r \equiv 0 \pmod{e}$. This leads us to the concept of the K-weight of an integer:

Definitions: If K is a set of positive integers, and if $a \geq 0$ is an integer, we define the K-weight of a, written $W_K(a)$, as the smallest integer s for which it is possible to write $a = k_1 + k_2 + \cdots + k_s$ with each $k_i \in K$. (For example if $K = \{1, p, p^2, \ldots\}$ it is clear that $W_K(a) = \mathbf{W}_p(a)$ as defined in chapter II.)

Also define $\omega_K(a) = \min_{n \geq 1} W_K(na)$; i.e., $\omega_K(a)$ is the least integer s for which it is possible to write $k_1 + k_2 + \cdots + k_s \equiv 0 \pmod{a}$.

It is now possible to state the main theorem of this chapter.

Theorem 5.2: Let $f(x) = f_1(x)f_2(x) \cdots f_m(x)$ be a squarefree polynomial in $F_p[x]$, and let the set K be as defined by (5.5). If $\omega = \omega_K(e)$, with e the exponent of f, and $\epsilon = [\frac{\omega-1}{p-1}]$. Then for all $s \in \Omega(f)$,

$$N(s;a) \equiv 0 \pmod{p^\epsilon} \quad \text{for } a \neq 0, \text{ and}$$

$$N(s;0) \equiv e \pmod{p^\epsilon}.$$

Proof: Since the proof is rather lengthy, perhaps a brief sketch is in order. The idea is to apply (4.10) to evaluate the functions k_λ which appear in (5.7), and to show that each k_λ is zero whenever r is "sufficiently small" relative to ω. This is the difficult part of the proof and is labelled lemma 5.2. The vanishing of the k_λ will in turn imply the vanishing of enough of the a_λ which appear in (5.2) to force each of the polynomials $N_k(v;a)$ to be zero for $1 \leq k \leq \epsilon$, and $a \neq 0$. The statement about $N(s;0)$ follows automatically since $\sum_a N(v;a) = e$.

Lemma 5.1: If K is the set given by (5.5), and if $m_1k_1 + m_2k_2 + \cdots \equiv 0 \pmod{e}$, for integers m_i and elements $k_i \in K$, then $\sum_i W_p(m_i) \geq \omega_K(e)$.

Proof: We replace each integer m_i by its p-ary expansion as a sum of $W_p(m_i)$ powers of p and for each summand m_ik_i obtain an expression of the form

$$p^{a_1} k_i + p^{a_2} k_i + \cdots \quad . \tag{5.8}$$

We recall that each $k \in K$ is of the form $g_i p^j$, and since $g_i p^{n_i} \equiv g_i \pmod{e}$ by definition, we may replace each term in (5.8) by a bona fide element of K without destroying the fact that the sum is $\equiv 0 \pmod{e}$. Hence starting with the expression $\Sigma\, m_i k_i \equiv 0 \pmod{e}$ we obtain a sum of $\Sigma\, W_p(m_i)$ elements of K with the same property. But we have defined $\omega_K(e)$ as the smallest possible number of elements with this property. Thus $\Sigma\, W_p(m_i) \geq \omega_K(e)$, as asserted.

Lemma 5.2: If $\omega_K(e) > 1 + (p-1)\log_p(r)$, then any monomial symmetric function

$$k_\lambda = \sum \theta_0^{k_1} \theta_1^{k_2} \cdots \theta_{r-1}^{k_r}$$

must vanish, provided that the $\theta_i = \theta^i$ are the e^{th} roots of unity over F_p and the k_i are chosen from the set K.

Proof: The plan is to show that under the given conditions, the rational integer given by (4.10) is divisible by p. It is however not the case that each summand σ of (4.10) has $\mu_p(\sigma) \geq 1$, which would be sufficient for our purposes in view of lemma 2.2. It will be necessary first to combine certain of the terms of (4.10) to obtain the result. Let us first observe that since f is squarefree, $(e, p) = 1$, so that the terms $e^{\ell(\pi)}$ in (4.10) may be disregarded in a discussion of divisibility by p.

A typical partition $\pi \in P_\lambda^e$ which appears in the sum (4.10) with $\ell = \ell(\pi)$ blocks $B_1, B_2, \ldots, B_\ell$ is characterized by the integers m_{ij}, where m_{ij} = the multiplicity of the integer i in B_j. Then clearly $\sum_j m_{ij} = m_i$ and $\sum_i m_{ij} = b_j = |B_j|$. (Recall that m_i is the multiplicity of the integer i in λ as a whole.) We are of course interested only in partitions π such that the numbers β_k given by (4.5) are all divisible by e; this is the definition of P_λ^e.

Let us recall that a given partition $\pi \in P_\lambda^e$ was only formally distinguishable from certain other partitions π' whose blocks contained the same integers with the same multiplicities; we assigned "labels" to the integers which occurred in λ more than once. Our task now is to recombine those terms in the sum (4.10) which are distinguishable only because of the artificial labels attached. The problem may be formulated as follows: given a collection $\lambda = (1^{m_1} 2^{m_2} 3^{m_3} \ldots)$ of integers, in how many ways is it possible to partition λ into blocks $B_1, B_2, \ldots, B_\ell$ with given multiplicities m_{ij}, assuming the integers in λ are all somehow distinguishable? Stated this way the problem is a familiar combinatorial one: there are $m_1!/m_{11}!m_{12}! \cdots m_{1\ell}!$ ordered ways of placing the 1's, $m_2!/m_{21}!m_{22}! \cdots m_{2\ell}!$ ordered ways of placing the 2's, etc. To obtain the total number of ways we must however account for the fact that the block lengths b_i need not all be different; thus if the block lengths $(b_1, b_2, \ldots, b_\ell)$ occur with multiplicities $(1^{d_1} 2^{d_2} \ldots)$, we must divide the product of multinomial coefficients by $\prod_i d_i!$ The total contribution of all partitions π with the given multiplicities m_{ij} to the sum (4.10) is the formidable expression

$$C = (-1)^{r-\ell} \frac{(\prod_i \frac{m_i!}{m_{i1}!m_{i2}!\cdots m_{i\ell}!})(\prod_i (b_i-1)!)}{(\prod d_i!)(\prod m_i!)} e^{\ell}$$

$$= (-1)^{r-\ell} \frac{\prod (b_i-1)!}{(\prod d_i!)(\prod m_{ij}!)} e^{\ell} = (-1)^{r-\ell} \frac{B}{D \cdot M} e^{\ell} , \qquad (5.9)$$

where $B = \pi(b_i-1)!$, $D = \pi d_i!$, $M = \pi m_{ij}!$ It is the object of the next few pages to show that $\mu_p(C) \geq 1$, so that by lemma 2.2 we obtain $k_\lambda = 0$ in F_p. We have already observed that the term e^{ℓ} cannot contribute to (5.9), so that

$$\mu_p(C) = \mu_p(B) - \mu_p(D) - \mu_p(M) \ . \qquad (5.10)$$

We may evaluate the terms on the right-hand side of (5.10) by means of Legendre's theorem 2.2:

$$\mu_p(B) = \frac{1}{p-1} \sum_i (b_i - 1 - W_p(b_i-1)) = \frac{1}{p-1} (r-\ell - \sum_i W_p(b_i - 1)) \qquad (5.11)$$

$$\mu_p(D) = \frac{1}{p-1} \sum (d_i - W_p(d_i)) = \frac{1}{p-1} (\ell - \sum W_p(d_i)) \qquad (5.12)$$

$$\mu_p(M) = \frac{1}{p-1} \sum_{i,j} (m_{ij} - W_p(m_{ij})) = \frac{1}{p-1} (r - \sum_{i,j} W_p(m_{ij})) \qquad (5.13)$$

combining these last three relations with (5.10), we obtain

$$\mu_p(C) = \frac{1}{p-1}\left(\sum_{i,j} W_p(m_{ij}) + \sum_i W_p(d_i) - 2\ell - \sum_i W_p(b_i-1)\right). \qquad (5.14)$$

Since $\mu_p(C)$ is an integer, if we only wish to show that $\mu_p(C) \geq 1$, it will be sufficient to drop the factor $\frac{1}{p-1}$ from (5.14) and prove that the remaining expression is positive. This will be done by bounding certain of the terms in (5.14). We need one more lemma.

Lemma 5.3: Suppose $\sum_{k=1}^{n} s_k = S$ for integers $s_k > 0$. Then $\sum W_p(s_k) \leq n(p-1)\log_p(1 + S/n)$.

Proof: We begin by showing that for any integer $s \geq 0$ it is true that

$$W_p(s) \leq (p-1)\log_p(s+1) . \qquad (5.15)$$

For a fixed $W > 0$, let us find the least integer s such that $W_p(s) = W$. This can most easily be done by writing $W = k(p-1) + m$ with $0 \leq m < p-1$, and observing that the smallest such s must use $p-1$ 1's, $p-1$ p's, ..., $(p-1)$ p^{k-1}'s and finally m p^k's. Hence $s = p^k - 1 + mp^k = (m+1)p^k - 1$. For this value of s, (5.15) reduces to

$$m \leq (p-1)\log_p(m+1) . \qquad (5.16)$$

But (5.16) is true for $m = 0$, $m = p-1$, and the function $x/\log_p(x+1)$ is monotonic increasing for $x \geq 1$. Since the right-hand side of (5.15) is itself a monotonic function of s, (5.15) must be generally true.

Because of (5.15) we may write

$$\sum_{k=1}^{n} W_p(s_k) \leq (p-1) \sum \log_p(s_k+1) = (p-1)\log_p(\pi(s_k+1)).$$

But since $\Sigma(s_k+1) = S + n$, the maximum value of the product $\pi(s_k+1)$ is attained when $s_k+1 = 1/n\ (S + n) = S/n + 1$. Hence

$$\sum W_p(s_k) \leq (p-1)\log_p\ (1 + \frac{S}{n})^n = n(p-1)\log_p(1 + \frac{S}{n}),$$

as asserted.

Note: Although the bound given by lemma 5.3 is usually very crude, the example $s_k = p^r-1$, $k = 1, 2, \ldots, n$, shows that it is sometimes sharp.

We apply lemma 5.3 to the term $\Sigma W_p(b_i-1)$ of (5.14), and obtain

$$\sum_{i=1}^{\ell} W_p(b_i-1) \leq \ell(p-1)\log_p\ (\frac{r}{\ell})\ . \tag{5.17}$$

We apply lemma 5.1 to the sum $\Sigma\ W_p(m_{ij})$, and obtain that for each j, $\sum_i W_p(m_{ij}) \geq \omega$, so that

$$\sum_{i,j} W_p(m_{ij}) \geq \omega\ell \quad . \tag{5.18}$$

Combining (5.17) and (5.18) with (5.14), we conclude that

$$\mu_p(C) \geq \frac{1}{p-1}(\omega\ell + \sum W_p(d_i) - 2\ell - \ell(p-1)\log_p(\frac{r}{\ell})).$$

Hence in order to prove that $\mu_p(C) > 0$, we need

$$\omega + \frac{1}{\ell}\sum W_p(d_i) + (p-1)\log_p(\ell) > 2 + (p-1)\log_p(r) \; . \tag{5.19}$$

But by hypothesis $\omega > 1 + (p-1)\log_p(r)$, so it remains to show that

$$\frac{1}{\ell}\sum W_p(d_i) + (p-1)\log_p(\ell) \geq 1 \; .$$

But if $(p-1)\log_p(\ell) < 1$, we have $\ell^{p-1} < p$, so that $\ell = 1$, in which case $\frac{1}{\ell}\Sigma W_p(d_i) > 1$. This proves (5.19) and also that $\mu_p(C) \geq 1$, so that by lemma 2.2, $k_\lambda = 0$ in F_p. This completes the proof of lemma 5.2.

Lemma 5.2 allows us to complete the proof of theorem 5.2 without much difficulty. According to (5.2), N_k involves only the symmetric functions a_r with $r \leq p^k(p-1)$. Furthermore, if $a \neq 0$, $N(0;a) = 0$, and so also $N_0(0;a) = N_1(0;a) = \cdots = 0$; i.e., no constant terms are involved in the polynomials $N_k(v;a)$ with $a \neq 0$. Therefore if each a_r, $1 \leq r \leq p^k(p-1)$ is zero, we have $N_0 = N_1 = \cdots = N_k = 0$, and so $N(v;a) \equiv 0 \pmod{p^{k+1}}$. But as we have seen,

when v is restricted to the subspace $\Omega(f)$, each a_r is a polynomial in the functions k_λ, with λ a partition of r involving only elements of K; this was equation (5.7). By lemma 5.2, each k_λ will vanish if $\omega > 1 + (p-1)\log_p(r)$. Therefore in order that $N(v;a) \equiv 0 \pmod{p^\epsilon}$, it is sufficient that each $a_r = 0$ with $r \leq p^{\epsilon-1}(p-1)$; i.e., $\omega > 1 + (p-1)\log_p(p^{\epsilon-1}(p-1)) = 1 + (p-1)(t-1) + (p-1)\log_p(p-1)$; this is equivalent to

$$\frac{\omega-1}{p-1} > \epsilon - 1 + \log_p(p-1) .$$

And since $\log_p(p-1) < 1$ this follows from the hypothesis $\frac{\omega-1}{p-1} \geq \epsilon$. Hence theorem 5.2 is proved for $a \neq 0$, and as we remarked earlier, the statement for $a = 0$ follows immediately since $\sum_a N(r;a) = e$ for each $v \in \Omega(f)$.

In order to be able to make use of theorem 5.2, it is necessary to have an effective means of calculating the value of $\omega = \omega_K(e) = \min\{W_K(me): m = 1, 2, \ldots\}$, and as given the definition appears to involve an infinite amount of calculation. But it is easy to see that this is not the case, as follows:

Suppose that a minimum value for $W_K(me)$ is attained by an equation of the form

$$k_1 + k_2 + \cdots + k_t \equiv 0 \pmod{e} . \tag{5.20}$$

Now each k_i in (5.20) is an element of K and so has the form $g_i p^j$. But $g_i p^{n_i} \equiv g_i \pmod{e}$, so that we may as well assume that a term of the form $g_i p^j$ which occurs in (5.20) has $j < n_i$. Also if a term $g_i p^j$ occurs more than p-1 times in (5.19) we could replace it by fewer

terms of the same form; for example $p \cdot g_i p^j$ would be replaced by $g_i p^{j+1}$; but since (5.20) is assumed to involve the minimum possible number of elements of K, this cannot happen. Thus the left-hand side of (5.20) is bounded by

$$(p-1) \sum_{i=1}^{m} \sum_{j=1}^{n_i-1} g_i p^j = \sum_i g_i (p^{n_i}-1) = Me,$$

for suitable M. We have proved

Theorem 5.3: $\omega_K(e) = \min \left\{ W_K(me): \ m = 1, 2, \ldots, M \right\}$.

Remark: In the case that f is an irreducible polynomial of degree n, the set K is $K = \left\{1, p, p^2, \ldots, p^{n-1}\right\}$. In this case $M = E = \frac{1}{e}(p^n-1)$, so that $\omega_K(e) = \omega_p(e)$ may be found by computing the values $W_p(e), W_p(2e), \ldots, W_p(Ee)$.

Let us observe that the value ω may be interpreted as the least integer t for which it is possible to write 1 as a product of t of the roots of f. Using this interpretation it is possible to state theorem 5.2 in a slightly different form, which does not add anything essentially new to the theory, but which is possibly more suggestive: let us define a sequence of polynomials $f = f_1, f_2, \ldots,$ where $f_k(x)$ is the polynomial of $F_p[x]$ whose roots are all possible products of k roots from among those of f, so that $f_k(x)$ has degree n^m.

Theorem 5.2': Let f be a squarefree element of $F_p[x]$. If ω is the smallest integer such that $(x-1) \mid f_\omega(x)$, and if $e = [\frac{\omega-1}{p-1}]$, then

$$N(s;a) \equiv 0 \pmod{p^{\epsilon}} \qquad a \neq 0, \text{ and}$$

$$N(s;0) \equiv e \pmod{p^{\epsilon}}$$

for all $s \in \Omega(f)$.

Corollary 5.1: If $\omega \geq p-1$, then $N(s;a)$ is divisible by p for each $a \neq 0$, and each $s \in \Omega(f)$.

Corollary 5.1 is well-known for the case $p=2$, where the hypothesis reduces merely to $(x-1) \nmid f(x)$. But the result had been thought to be peculiar to the binary case previously. (Selmer [10, p. 157]).

Let us illustrate how the theorems in this thesis can be applied to a particular example: consider the linear recurrence

$$s_{k+6} + s_{k+3} + s_{k+2} - s_{k+1} - s_k = 0$$

over GF[3]. The associated polynomial is $f(x) = x^6 + x^3 + x^2 - x - 1$, and according to Church's table [2], $f(x)$ is irreducible and belongs to exponent $e = 104$. Using only this one borrowed piece of information, it is possible to describe completely the distribution of the elements from GF[3] (which we take to be 0, +1, and -1) in the space $\Omega(f)$. Here $eE = p^n - 1$ becomes $104 \cdot 7 = 3^6 - 1$.

Let us first apply corollary 3.2; i.e., we regard $\Omega(f)$ not as a vector space but as a set of $E = 7$ nonzero cycles of elements from GF[3], which correspond to the cosets of the cyclic subgroup T of order 104 in $GF[3^6]$. Since $q = 3$ is a primitive root of $E = 7$, $x^7 - 1$ has only two irreducible factors and so only two distinct distributions of trace values occur among the cycles of $\Omega(f)$; i.e.,

the subgroup T has one distribution and all other cosets Tx have the other distribution. Hence we denote by S_0, S_1, S_{-1} and C_0, C_1, and C_{-1} the number of zeros, ones, and minus ones occurring in the subgroup, and the cosets, respectively. Since the trace assumes every value in GF[3] $3^5 = 243$ times, we obtain

$$S_0 + 6C_0 = 243 - 1 = 242 \tag{5.21a}$$

$$S_1 + 6C_1 = 243 \tag{5.21b}$$

$$S_{-1} + 6C_{-1} = 243, \tag{5.21c}$$

as well as the obvious relations

$$S_0 + S_1 + S_{-1} = 104 \tag{5.22a}$$

$$C_0 + C_1 + C_{-1} = 104 \ . \tag{5.22b}$$

We now wish to apply theorem 5.2, and to do so it is necessary by theorem 5.3 to compute the values $W_3(104k)$ for $k = 1, 2, 3, 4, 5, 6, 7$. The ternary expansions are

$$104 = 3^4 + 2\cdot 3^2 + 3 + 2\cdot 1 \ ; \quad W_3(104) = 6$$

$$208 = 2\cdot 3^4 + 3^3 + 2\cdot 3^2 + 1 \ ; \quad W_3(208) = 6$$

$$312 = 3^5 + 2\cdot 3^3 + 3^2 + 2\cdot 3 \ ; \quad W_3(312) = 6$$

$$416 = 3^5 + 2\cdot 3^4 + 3^2 + 2\cdot 1 \ ; \quad W_3(416) = 6$$

$$520 = 2\cdot 3^5 + 3^3 + 2\cdot 3 + 1 \ ; \quad W_3(520) = 6$$

$$624 = 2\cdot 3^5 + 3^4 + 2\cdot 3^3 + 3 \qquad ; \ W_3(624) = 6$$

$$728 = 2\cdot 3^5 + 2\cdot 3^4 + 2\cdot 3^3 + 2\cdot 3^2 + 2\cdot 3 + 2 \ ; \ W_3(728) = 12 .$$

Consequently $\omega_3(104) = 6$, since $[\ \frac{6-1}{3-1}\ ] = 2$, theorem 4.2 shows that

$$S_1 \equiv C_1 \equiv S_{-1} \equiv C_{-1} \equiv 0 \pmod 9$$

$$S_0 \equiv C_0 \equiv 104 \equiv S \pmod 9 . \tag{5.23}$$

From (5.20a) and (5.23) we obtain $(242 - S_0)/6 = C_0 \equiv 5 \pmod 9$, from which it follows that $S_0 \equiv 212 \equiv 50 \pmod{54}$ so that $S_0 = 50$. (The possibility $S_0 = 104$ corresponds to the all-zero solution in $\Omega(f)$ which has explicitly been excluded from consideration.) Similarly from (5.20b) and (5.23) we obtain $S_1 \equiv 243 \equiv 27 \pmod{54}$ and finally $S_{-1} \equiv 27 \pmod{54}$. Hence S_1 and S_{-1} are either 27 or 81, but the possibility 81 is excluded by (5.22a). Hence $S_1 = S_{-1} = 27$. Hence also, $C_0 = 32$, $C_1 = 36$, $C_{-1} = 36$. This completely solves the distribution problem for $\Omega(f)$.

It would be interesting to know whether or not theorem 5.2 is the best possible of its kind; i.e., as there exist polynomials f for which either

$$N(s;a) \equiv 0 \pmod{p^{\varepsilon+1}} \qquad a \neq 0, \quad \text{or} \tag{5.24}$$

$$N(s;0) \equiv c \pmod{p^{\varepsilon+1}}, \tag{5.25}$$

for all $s \in \Omega(f)$? It is the feeling of the author that this happens only rarely:

Conjecture: (5.24) is never true for all $s \in \Omega(f)$, and (5.25) can occur only for $p > 2$.

One reason that $a = 0$ seems to play a special role in the conjecture is that the proof of theorem 5.2 for $a = 0$ only made use of the fact that $\sum N(s;a) = e$. It is possible that each $N(s;a) \not\equiv 0 \pmod{p^{\epsilon+1}}$, while $\sum_{a\neq 0} N(s;a) \equiv 0 \pmod{p^{\epsilon+1}}$ for $p > 2$. And in fact this sort of thing happens for $p = 3$ and $f(x) = x^5 - x - 1$ which has exponent 121. The values of $N(s;1)$ and $N(s;-1)$ are 45 and 36 for certain cycles $s \in \Omega(f)$, and 36 and 45 for the others. But $36 + 45 = 81 = 3^4$, whereas theorem 5.2 gives only $\epsilon = 2$.

Let us observe finally that if we apply theorem 5.2 to the case where $f(x)$ is a primitive polynomial of degree n in $F_p[x]$; i.e., when f has exponent $e = p^n - 1$. Here $\omega_p(e) = W_p(e) = n(p-1)$, so that $\epsilon = n-1$. And in this case theorem 5.2 is exact since it is obvious that $N(s;a) = p^{n-1}$ for $a \neq 0$ and $N(s;0) = p^{n-1} - 1$, for in this case the subgroup T of theorem 3.1 is the complete multiplicative subgroup of $GF[p^n]$, so that the trace assumes every nonzero value p^{n-1} times on T, and zero $p^{n-1} - 1$ times. Thus theorem 5.2 can be exact for both large and small values of ϵ, and so it is unlikely that there is a general theorem which is stronger than theorem 5.2.

REFERENCES

[1] Albert, A. A.: Fundamental Concepts of Higher Algebra; University of Chicago Press, 1956.

[2] Church, R.: "Tables of Irreducible Polynomials for the First Four Prime Moduli;" Ann. Math. 36(1935) pp. 198-209.

[3] Dickson, L. E.: Linear Groups; Springer, Berlin, 1900; Dover Pub. 1958.

[4] Dickson, L. E.: History of the Theory of Numbers, vol. 1; Carnegie Publication No. 256, reprinted, Chelsea 1952.

[5] Hall, Marshall, Jr.: "An Isomorphism between Linear Recurring Sequences and Algebraic Rings;" Trans. Am. Math. Soc. 44(1938), pp. 196-218.

[6] Hall, Marshall, Jr.: Combinatorial Theory, Blaisdell, 1967.

[7] MacMahon, P. A.: Combinatory Analysis, vol. 1; University Press, Cambridge, England, 1915; reprinted, Chelsea 1960.

[8] Mattson, H. F., and Solomon, G.: "A New Treatment of Bose-Chaudhuri Codes;" J. Soc. Ind. Appl. Math. 9(1961), pp. 654-669.

[9] Rota, G.-C.: "On the Foundations of Combinatorial Theory. I. Theory of Möbius Functions;" Zeit. Wahrshein. 2(1964), pp. 340-368.

[10] Selmer, E. S.: Linear Recurrence Relations over Finite Fields; mimeographed lecture notes available for $5.00 from Dept. Math., University of Bergen, Norway.

[11] Solomon, G. and McEliece, R. J.: "Weights of Cyclic Codes;" J. Comb. Theory, to appear.

[12] van der Warden, B. L.: Modern Algebra, vol. 1; Ungar, New York, 1953.

[13] Ward, M.: "The Arithmetical Theory of Linear Recurring Sequences," Trans. Am. Math. Soc. 35(1933), pp. 600-628.

[14] Zierler, N.: "Linear Recurring Sequences;" J. Soc. Ind. Appl. Math. 7(1959), pp. 31-48.