J. Soc. Indust. Appl. Math.
Vol. 7, No. 1, March, 1959
Printed in U.S.A.

LINEAR RECURRING SEQUENCES[1]

NEAL ZIERLER[2]

1. Introduction. Sequences of maximum period generated by linear recurrences, m-sequences for short, constitute a small class of pseudo-random sequences with many remarkable and useful properties. This note is devoted to, first, some preliminaries on general linear recurring sequences of elements of a finite field; second, a determination of the periods of the members of the family of sequences satisfying a given linear recurrence; third, characterizations of m-sequences and a discussion of their properties with special reference to their autocorrelation functions.[3] The reader interested in the applications may consult, for example, [8, 11, 13, 15].

2. Preliminaries. Let p be a prime, let m be a positive integer and let K be a field with $q = p^m$ elements.[4] Let x be an indeterminate over K and let $K[x]$ and $K(x)$ denote, as usual, the ring of polynomials in x with coefficients in K and the corresponding field of quotients respectively. "Sequence" will always mean "sequence with values in K" and "polynomial" refers to a member of $K[x]$. The letters f, g and h are reserved for polynomials; (f, g) denotes the greatest common divisor of f and g, "$f \mid g$" stands for "f divides g" and $d(f)$ denotes the degree of f. If f is a nonzero element of $K \subset K[x]$, $d(f) = 0$; $d(0) = -1$.

Let $n \geqq 0$, let $c_0, \cdots, c_n$ be elements of K with $c_0 c_n \neq 0$ and let $G = G(c_0, \cdots, c_n)$ denote the set of all sequences $a = \{a_i\}_{i=0}^{\infty}$ satisfying

$$c_0 a_i + c_1 a_{i-1} + \cdots + c_n a_{i-n} = 0 \qquad (i = n, n+1, \cdots). \tag{1}$$

G contains q^n members, for $a_0, \cdots, a_{n-1}$ may be chosen arbitrarily in K and the remaining terms of a are then determined by the recurrence $a_i = -c_0^{-1}(c_1 a_{i-1} + \cdots + c_n a_{i-n})$. The elements of G are all the (linearly recurring) sequences *associated with* or *generated by* the $(n+1)$-tuple $c_0, \cdots, c_n$. A one-to-one correspondence between the set of all such $(n+1)$-tuples and the set of all polynomials f of degree n with $f(0) \neq 0$ is estab-

[1] Received by the editors December 19, 1957 and in revised form September 2, 1958.
[2] The research reported in this paper was supported jointly by the Army, Navy and Air Force under contract with the Massachusettes Institute of Technology.
[3] In recent years linear recurring sequences have been examined in detail by A. A. Albert, W. A. Blankinship, S. W. Golomb and the writer (and perhaps others) with considerable overlapping of methods and results. Much interesting material may be found in the earlier work of R. D. Carmichael [5], M. Hall [9] and M. Ward [17]; some specific indications appear below. Cf. also the note of J. L. Brenner [2].
[4] Basic algebraic ideas which appear here may be found, for example, in the book [1] of A. A. Albert.

lished by

$$f(x) = c_n x^n + \cdots + c_0 . \tag{2}$$

A polynomial f and $(n + 1)$-tuple which correspond in this way will often be identified; thus, we speak of sequences associated with or generated by polynomials; f is called the *characteristic polynomial* of the set $G(f)$. To avoid frequent repetition, a polynomial treated as being in the domain of G is automatically assumed to have nonzero constant term (with an exception to be noted below).

Let S be the set of all periodic sequences; i.e., $a \in S$ if and only if there exists $r > 0$ such that $a_0 = a_r$, $a_1 = a_{r+1}$, $\cdots$. The following three theorems will be established in this section.

THEOREM 1. *Let A be a finite nonempty subset of S. Then there exists a polynomial f, unique up to multiplication by nonzero elements of K, such that $A \subset G(g)$ if and only if $f \mid g$.*

The polynomial f of Theorem 1 is said to be the *minimum polynomial of the set A*; if A contains a single sequence a, f is also said to be the *minimum polynomial of the sequence a.*

If a and b are sequences and $d_0 \in K$, by $a + b$ we mean the sequence c such that $c_i = a_i + b_i$ for all i and by $d_0 a$, the sequence e such that $e_i = d_0 a_i$. Multiplication of sequences by elements of K is evidently distributive over their addition. If A and B are sets of sequences, let $A + B$ denote the set of all sequences of the form $a + b$ for $a \in A$ and $b \in B$. Clearly, the addition of sets of sequences is commutative and associative. The set A of sequences is called a *K-module* if it is closed under addition and multiplication by elements of K.

THEOREM 2. *Let $n > 0$ and let $f_1, \cdots, f_n$ be polynomials with least common multiple f. Then $G(f_1) + \cdots + G(f_n) = G(f)$.*

Let a be a sequence, $s \geqq 0$ and let b be the sequence satisfying $b_i = a_{i+s}$ for $i \geqq 0$. Then b is said to be the *translate of a by s.*

THEOREM 3. *Let A be a finite nonempty set of sequences. A necessary and sufficient condition for A to be the set of all sequences producible by a linear recurrence—i.e., for $A = G(f)$ for some f—is that A be a K-module contained in S and closed under translation.*

Let R be the set of all expressions $\sum_{k=-\infty}^{\infty} a_k x^k$ in which $a_k \in K$ for all k and for which there exists some integer n such that $a_k = 0$ for all $k < n$. For present purposes it would be sufficient to regard the elements of R as formal entities; indeed, it is not difficult to show directly that the eventually periodic elements of R—those for which there exist positive integers t and r such that $a_{k+r} = a_k$ for all $k > t$—form a field isomorphic to $K(x)$.[5]

[5] The operations in R are term by term addition and the following multiplication:

$$\sum a_i x^i \sum b_j x^j = \sum c_k x^k \quad \text{where} \quad c_k = \sum_{i=-\infty}^{\infty} a_{k-i} b_i .$$