SIAM Review
Vol. 10, No. 3, July, 1968

LINEAR RECURSIVE SEQUENCES*

JAY P. FILLMORE† AND MORRIS L. MARX‡

1. Introduction. It is with some trepidation that the authors write on a subject as thoroughly exploited as that of linear recursive sequences. However, because of recent work on shift registers and error correcting codes (see, for example, the references at the end of the paper), these sequences have taken on new interest.

Existing rigorous treatments of the subject require considerable familiarity with modern algebra. We here develop the theory rigorously using only the most rudimentary notions of modern algebra, and hence it should be accessible to the reader with a limited mathematical background.

The proofs presented here are constructive, so that these, together with W. A. Blankinship's version of the Euclidean algorithm [2], give an efficient method to study linear recursive sequences on a computer. Thus, this approach offers computational advantages over matrix oriented treatments of the sequences.

Although most of the results are well known in some form, the use of the sequences δ_h (defined in §3) to study the structure of sequences whose recursion is the power of an irreducible polynomial appears to be little exploited to date. They appear in unpublished writings of W. A. Blankinship and in T. L. Booth [3]. The proofs presented here for the structure theory using these sequences are new.

An *n-stage shift register* is a device which, by means of n two-state circuits, represents a vector $v = (v_1, \cdots, v_n)$, where v_i is 0 or 1, and which, when stepped once, yields a new vector $v' = (v_1', \cdots, v_n')$ which depends only on the vector v and fixed circuitry. Successively stepping the shift register gives a sequence of vectors $\{v(t)\}$, and it is this sequence that enjoys so many applications.

In general, properties of the sequence $\{v(t)\}$ are quite elusive (see, for example, [5]), but in the case where the sequence is linear recursive (defined in §2), a great deal can be said.

An n-stage shift register can be in at most 2^n possible states. Thus any $\{v(t)\}$ coming from a shift register will satisfy $v(t + e) = v(t)$ for some $e > 0$ and $t \geqq$ some t_0. If this $e > 0$ is minimal, e is called the *period* of $\{v(t)\}$. If one knows the period of a sequence generated by a shift register, a very accurate clock can be constructed from a shift register stepping at a constant rate. This is discussed further in [9, p. 14]. This leads to the problem of determining the periods of a sequence. The treatment of the linear case is not difficult. It is carried out in §4.

If we fix a single component of the vector $v(t)$, say the first component $v_1(t)$, we have a sequence $\{v_1(t)\}$ of 0's and 1's. We can ask how well does this sequence represent a random sequence (probability that $v_1(t + 1) = 0$ is $\frac{1}{2}$ independent of

* Received by the editors January 30, 1967, and in revised form November 7, 1967.

† Department of Mathematics, University of California at San Diego, La Jolla, California 92037.

‡ Vanderbilt University, Nashville, Tennessee 37203.

the values of $v_1(0), \cdots, v_1(t)$) of 0's and 1's. For example, one can request that the period of $\{v_1(t)\}$ be $e = 2^n$ or $2^n - 1$ and that for every $r = 1, 2, \cdots, n$, each of the 2^r possible stretches of r consecutive 0's and 1's occur exactly 2^{n-r} times, or all but one occur exactly 2^{n-r} times. Such a sequence can be generated as a linear recursive sequence whose recursion is a primitive polynomial. These are discussed in §4.

Finally, we indicate how a shift register is used to construct an *error correcting code*. Suppose a 4-stage shift register is stepped from (v_1, v_2, v_3, v_4) to (v_1', v_2', v_3', v_4') according to

$$\begin{aligned} v_1' &= v_2, \\ v_2' &= v_3, \\ v_3' &= v_4, \\ v_4' &= v_1 + v_3 + v_4. \end{aligned}$$

(This corresponds to the polynomial $x^4 + x^3 + x^2 + 1$ as will be seen later.) Inputting the 4-vector $(v_1(0), v_2(0), v_3(0), v_4(0))$, stepping the register six times and reading off the first components gives a 7-vector $(v_1(0), v_1(1), \cdots, v_1(6))$. Sending the 16 possible 4-vectors into the resulting 7-vectors gives an error correcting code in that any two of the 7-vectors differ in three or more places and one can tell from which 4-vector it comes, even if one of the entries in the 7-vector is in error. For example,

0	0	0	0	is sent to	0	0	0	0	0	0	0
0	0	0	1		0	0	0	1	1	0	1
0	0	1	0		0	0	1	0	1	1	1
0	0	1	1		0	0	1	1	0	1	0
etc.					etc.						

The reader should consult [6] for further details.

Thorough discussions on the uses and generation of shift register sequences are to be found in Golomb [5], [9].

2. Preliminaries. Let K^n denote the n-dimensional vector space over a field K. We are mainly interested in the case $K = F_2$, the field of two elements, but there is no loss of efficiency in considering the general case.

DEFINITION 1. A sequence $v = \{v(t)\}, t = 0, 1, 2, \cdots$, of elements of K^n is called a *linear recursive sequence* (l.r.s.) over K^n if there exist $c_1, c_2, \cdots, c_m$ in K such that

$$v(t + m) = \sum_{i=1}^{m} c_i v(t + m - i) \quad \text{for each integer} \quad t \geqq 0.$$

The sequence v is said to *satisfy* the recursion associated with $f(x) = x^m - c_1 x^{m-1} - \cdots - c_{m-1}x - c_m$ (briefly, v satisfies the recursion $f(x)$). To say that v satisfies a polynomial with leading coefficient $c \neq 1$ means v satisfies $c^{-1}f(x)$.

Observe that if $v = \{v(t)\}$ satisfies a polynomial of degree m, then v is completely determined once $v(0), v(1), \cdots, v(m-1)$ are given.

The set of all sequences of elements of K^n forms a vector space over K if we define $(v + w)(t) = v(t) + w(t)$, $(av)(t) = a(v(t))$ for $a \in K$. The *shift operator* σ is defined on this vector space by $\sigma(v) = w$, where $w(t) = v(t+1)$ for $t \geqq 0$. Let σ^k denote σ composed with itself k times and put $(a\sigma^k + b\sigma^l)v = a(\sigma^k v) + b(\sigma^l v)$ for $a, b \in K$ and k, l nonnegative integers ($\sigma^0 v = v$).

An immediate consequence of the remark following the definition is that the set of all l.r.s.'s over K^n satisfying a given polynomial of degree m is a vector space of dimension mn.

PROPOSITION 1. (a) *The set of all operators of the form $f(\sigma)$, where $f(x) \in K[x]$, under addition and composition forms a ring isomorphic to $K[x]$.*

(b) *An l.r.s. v satisfies $f(x)$ if and only if $f(\sigma)v = 0$.*

(c) *If v satisfies $f(x)$ and $g(x)$, then v satisfies $f(x) + g(x)$ and $h(x)f(x)$ for any $h(x) \in K[x]$.*

(d) *If v satisfies $f(x)$ and w satisfies $g(x)$, then $v + w$ satisfies any common multiple of $f(x)$ and $g(x)$.*

(e) *If v is an l.r.s., there is a unique polynomial of least degree and leading coefficient 1 which v satisfies. This polynomial divides any other polynomial which v satisfies.*

Proof. (a)–(d) are easy. We prove (e). Let $f(x)$ be a polynomial of least degree and leading coefficient 1 such that $f(\sigma)v = 0$. If $g(x)$ satisfies the same conditions, then $f(x) - g(x)$ is a polynomial of degree $< \deg f(x) = \deg g(x)$ which v satisfies. Unless $f(x) - g(x) = 0$, we could make the lead coefficient 1 and obtain a contradiction. Let v satisfy $h(x)$. Write $h(x) = g(x)f(x) + r(x)$ where either $\deg r(x) < \deg f(x)$ or $r(x) = 0$. Since v satisfies $r(x)$, necessarily $r(x) = 0$ and $f(x)$ divides $g(x)$.

For reasons apparent later, we take the unique polynomial $f(x)$ of (e), factor out the largest power of x dividing $f(x)$, and call the resulting polynomial the *polynomial associated with the minimal recursion of v*, or the minimal recursion of v. The degree of this polynomial is called the *span* of v. By (e), the minimal recursion of v divides any recursion which v satisfies. The term "span" should not be confused with the notion of span in linear algebra.

A convenient way to generate an l.r.s. is the following: Select an $n \times n$ matrix A, an n-dimensional vector $v(0)$, and set $v(t) = A^t v(0)$. If $f(x)$ is a polynomial such that $f(A)v(0) = 0$, then

$$(f(\sigma)v)(t) = f(A)A^t v(0) = 0,$$

so v is an l.r.s. which satisfies $f(x)$. Such an $f(x)$ always exists, for example, the minimal polynomial of A. This also shows that the span of v is at most the degree of the minimal polynomial of A; however, it may be less, since $f(A)v(0)$ may be zero even though $f(A) \neq 0$. Since the span of an l.r.s. generated by an $n \times n$ matrix in this manner is $\leqq n$, the sequence is completely determined once $v(0), v(1), \cdots, v(n-1)$ are known. We remark in passing that given $v(t) = A^t v(0)$, it is not necessary to know A in order to find an $f(x)$ such that

$f(A)v(0) = 0$. Simply find a linear dependence $\sum_{i=0}^{n} a_i v(i) = 0$ among the first $n + 1$ vectors and set $f(x) = \sum_{i=0}^{n} a_i x^i$. Then $f(A)v(0) = 0$.

We mention two important special cases of this method of generating an l.r.s.

Case 1. Suppose v is an l.r.s. over K which satisfies $f(x) = x^n - c_1 x^{n-1} - \cdots - c_n$. Let A be the companion matrix of $f(x)$:

$$A = \begin{bmatrix} 0 & 1 & 0 & 0 & \cdots & 0 \\ 0 & 0 & 1 & 0 & \cdots & 0 \\ \vdots & & & & & \\ 0 & 0 & 0 & 0 & \cdots & 1 \\ c_n & c_{n-1} & \cdot & \cdots & & c_1 \end{bmatrix}.$$

Then $v(t)$ is the first component of the n-vector $A^t(v(0), \cdots, v(n-1))$ so $\{v(t)\}$ can be studied by studying $\{A^t v(0)\}$, which is in the matrix form discussed above.

Case 2. Let $f(x)$ be a polynomial of degree n over K. Then the sequence of vectors $v(t) = (a_0(t), a_1(t), \cdots, a_{n-1}(t))$, where

$$\sum_{i=0}^{n-1} a_i(t+1)x^i \equiv x \sum_{i=0}^{n-1} a_i(t)x^i \pmod{f(x)},$$

is an l.r.s. over K^n satisfying $f(x)$. We have $v(t+1) = Av(t)$, and consequently $v(t) = A^t v(0)$, where A is the transpose of the companion matrix of $f(x)$. The action of A in this example is the "shift and add" that gives shift registers their name.

Not every l.r.s. over K^n need be of the form $v(t) = A^t v(0)$. The reader can verify the following: If v is an l.r.s. over K^n of span $\leqq n$ and if $v(0), v(1), \cdots, v(n-1)$ are linearly independent, then there exists an $n \times n$ matrix A such that $v(t) = A^t v(0)$ for all $t \geqq 0$.

3. Decomposition of linear recursive sequences. The following two theorems reduce the study of an arbitrary l.r.s. to the study of l.r.s.'s satisfying irreducible polynomials.

THEOREM 1. *Suppose the polynomials $f_1(x), f_2(x), \cdots, f_k(x)$ are pairwise relatively prime. If v satisfies the recursion associated with $f_1(x) \cdot f_2(x) \cdot \cdots \cdot f_k(x)$, then there exist unique sequences $v_1, v_2, \cdots, v_k$ such that, for $1 \leqq i \leqq k$, v_i satisfies $f_i(x)$ and*

$$v = v_1 + v_2 + \cdots + v_k.$$

Proof. We prove the theorem for $k = 2$; an easy induction extends the result to the general case.

Since $f_1(x)$ and $f_2(x)$ are relatively prime, by the Euclidean algorithm there exist polynomials $g_1(x)$ and $g_2(x)$ such that $g_1(x)f_1(x) + g_2(x)f_2(x) = 1$. Hence,

$$v = g_1(\sigma)f_1(\sigma)v + g_2(\sigma)f_2(\sigma)v.$$

Let the first term on the right be v_2 and the second, v_1. By hypothesis, $f_1(\sigma)f_2(\sigma)v = 0$, and so $f_1(\sigma)v_1 = f_2(\sigma)v_2 = 0$.

If $f_1(x), \cdots, f_k(x)$ are taken to be powers of different irreducible polynomials, Theorem 1 tells us that we need only look at l.r.s.'s satisfying a polynomial of the form $f(x)^h$, where $f(x)$ is irreducible.

Define the sequence $\{\delta_h(t)\}$ for $h \geqq 0$ by

$$\delta_h(t) = \binom{t+h}{h} \text{ (mod characteristic } K) \quad \text{for} \quad t \geqq 0.$$

If v is any sequence over K^n and α is a sequence over K, we define αv by $(\alpha v)(t) = \alpha(t)v(t)$. Note that for $k \geqq 0$,

$$\sigma^k(\alpha v) = (\sigma^k\alpha)(\sigma^k v).$$

THEOREM 2. *Suppose $f(x)$ is irreducible. If $v_0, \cdots, v_{h-1}$ satisfy $f(x)$, then $\sum_{i=0}^{h-1} \delta_i v_i$ satisfies $f(x)^h$. Suppose, in addition, that $f(x)$ is separable. Then for any v that satisfies $f(x)^h$, there exist unique $v_0, v_1, \cdots, v_{h-1}$ satisfying $f(x)$ such that*

$$v = \sum_{i=0}^{h-1} \delta_i v_i .$$

We precede the proof of this theorem by two propositions.

It is true that (think of Pascal's triangle)

$$\delta_h(t+1) = \delta_h(t) + \delta_{h-1}(t+1), \qquad t \geqq 0,$$

or equivalently,

$$\sigma\delta_h = \delta_h + \sigma\delta_{h-1} .$$

PROPOSITION 2. *For $k \geqq 1$ and $h \geqq 0$,*

$$\sigma^k\delta_h = \sum_{i=0}^{h} \binom{h-i+k-1}{k-1} \delta_i .$$

Proof. The proof is by induction on k.

Using $\sigma\delta_h = \delta_h + \sigma\delta_{h-1}$ and induction on h gives

$$\delta_h = \sum_{l=0}^{h} \delta_l ,$$

which shows the truth of the proposition for $k = 1$.

Suppose the proposition is true for $k-1$. Then

$$\begin{aligned} \sigma^k\delta_h &= \sigma^{k-1}\left(\sum_{l=0}^{h} \delta_l\right) \\ &= \sum_{l=0}^{h} \sum_{i=0}^{l} \binom{l-i+k-2}{k-2} \delta_i \\ &= \sum_{i=0}^{h} \sum_{l=i}^{h} \binom{l-i+k-2}{k-2} \delta_i . \end{aligned}$$

But

$$\sum_{l=i}^{h}\binom{l-i+k-2}{k-2}=\sum_{l=0}^{h-i}\binom{l+k-2}{k-2}=\sum_{l=0}^{h-i}\binom{l+k-2}{l}$$
$$=\sum_{l=0}^{h-i}\delta_l(k-2)=(\sigma\delta_{h-1})(k-2)$$
$$=\binom{h-i+k-1}{h-i}=\binom{h-i+k-1}{k-1},$$

and so the statement holds for k.

PROPOSITION 3. *Let $v \neq 0$ be an l.r.s. satisfying an irreducible polynomial $f(x)=\sum_{k=0}^{m}a_kx^k$, $m \geqq 1$, and let $h \geqq 1$. Then there exist l.r.s.'s $v_0, v_1, \cdots, v_{h-1}$ such that*

$$f(\sigma)(\delta_h v)=\sum_{i=0}^{h-1}\delta_i v_i$$

and v_i satisfies $f(x)$ for $0 \leqq i \leqq h-1$. If $f(x)$ is separable, then $v_{h-1} \neq 0$.

Proof.

$$f(\sigma)(\delta_h v)=\sum_{k=0}^{m}a_k\,\sigma^k(\delta_h v)=\sum_{k=0}^{m}a_k(\sigma^k\delta_h)(\sigma^k v)$$
$$=a_0\,\delta_h v+\sum_{k=1}^{m}a_k\left[\sum_{i=0}^{h}\binom{h-i+k-1}{k-1}\delta_i\right](\sigma^k v)$$
$$=\delta_h\sum_{k=0}^{m}a_k\,\sigma^k v+\delta_{h-1}\sum_{k=1}^{m}ka_k\,\sigma^k v$$
$$+\sum_{k=1}^{m}\sum_{i=0}^{h-2}a_k\binom{h-i+k-1}{k-1}\delta_i(\sigma^k v)$$
$$=0+\delta_{h-1}\sum_{k=1}^{m}ka_k\,\sigma^k v+\sum_{i=0}^{h-2}\delta_i\sum_{k=1}^{m}a_k\binom{h-i+k-1}{k-1}\sigma^k v.$$

The zero above appears by virtue of the fact that v satisfies $f(x)$.

Set $v_i=\sum_{k=1}^{m}a_k\binom{h-i+k-1}{k-1}\sigma^k v$, $0 \leqq i \leqq h-1$, and note that $v_{h-1}=\sum_{k=1}^{m}ka_k\sigma^k v=\sigma f'(\sigma)v$, where $f'(x)$ is the formal derivative of $f(x)$. It follows that the v_i satisfy $f(x)$, $0 \leqq i \leqq h-1$, and the v_i are defined so that

$$f(\sigma)\delta_h v=\sum_{i=0}^{h-1}\delta_i v_i.$$

Suppose now that $f(x)$ is separable; then $f'(x) \neq 0$. If v_{h-1} were zero, since $f(x)$ is the minimal recursion of v, we could have $f(x) \mid xf'(x)$. This implies that $f(x) \mid x$ or $f(x) \mid f'(x)$, neither of which is possible.

Proof of Theorem 2. Suppose first that $v=\sum_{i=0}^{h-1}\delta_i v_i$. We wish to show $f(\sigma)^h v=0$. By Proposition 3 there exist v_{ij} satisfying $f(x)$ such that

$f(\sigma)(\delta_i v_i) = \sum_{j=0}^{i-1} \delta_j v_{ij}$. Then we have

$$f(\sigma)^h v = f(\sigma)^{h-1} f(\sigma) v = f(\sigma)^{h-1} \sum_{i=0}^{h-1} f(\sigma)(\delta_i v_i)$$

$$= f(\sigma)^{h-1} \sum_{i=0}^{h-1} \sum_{j=0}^{i-1} \delta_j v_{ij}.$$

An induction on h shows this expression vanishes as desired.

Now let $V = \{v \mid f(\sigma)^h v = 0\}$; V is a vector space of dimension mnh. Suppose $W = \{\sum_{i=0}^{h-1} \delta_i v_i \mid f(\sigma) v_i = 0,\ 0 \leqq i \leqq h-1\}$. By the first part of the proof, $W \subset V$ and, in fact, is a subspace of V. Choose l.r.s.'s $u_1, u_2, \cdots, u_{mn}$ such that $f(\sigma) u_i = 0$, $1 \leqq i \leqq mn$, and the $\{u_i\}$ are linearly independent. If we show that $\{\delta_i u_j \mid 0 \leqq i \leqq h-1,\ 1 \leqq j \leqq mn\}$ is a basis for W, the proof we be complete; for then the dimensions of W and V will be equal and we have $W = V$.

Suppose $\sum_{j=1}^{mn} \sum_{i=0}^{h-1} a_{ij} \delta_i u_j = 0$ with $a_{ij} \in K$. We must show that all $a_{ij} = 0$. Let

$$w_i = \sum_{j=1}^{mn} a_{ij} u_j \quad \text{for} \quad 0 \leqq i \leqq h-1.$$

Then $\sum_{i=0}^{h-1} \delta_i w_i = 0$. If every $w_i = 0$, then all $a_{ij} = 0$ by the independence of the $\{u_j\}$. Suppose some $w_i \neq 0$. Let r be the largest subscript for which this occurs. We may assume $1 \leqq r \leqq h-1$. We have $-\delta_r w_r = \sum_{i=0}^{r-1} \delta_i w_i$ and so by the first part of the proof $f(\sigma)^r \delta_r w_r = 0$. We shall have completed the proof if we show this implies $w_r = 0$.

To this end we prove: if $w \neq 0$ satisfies the separable and irreducible polynomial $f(x)$, then $f(\sigma)^r \delta_r w \neq 0$.

We proceed by induction on r. The statement is trivial for $r = 0$. Assume it is true for $r-1$. Using Proposition 3 we have

$$f(\sigma)^r \delta_r w = f(\sigma)^{r-1} \left(\sum_{i=0}^{r-1} \delta_i v_i \right) = f(\sigma)^{r-1} \delta_{r-1} v_{r-1}$$

with $v_{r-1} \neq 0$. By the induction hypothesis, $f(\sigma)^{r-1} \delta_{r-1} v_{r-1} \neq 0$ which proves the statement.

Example. Let $K = F_2(s)$, where s is transcendental over F_2. Then $f(x) = x^2 + s$ is irreducible but not separable. Let V be the vector space of all sequences satisfying $f(x)$. The sequences

$$w = 1, 0, s, 0, s^2, 0, s^3, 0, \cdots$$

and

$$u = 0, 1, 0, s, 0, s^2, 0, s^3, \cdots$$

are a basis for V. Note that $\delta_1 w = w$ and $\delta_1 u = 0$. For any $v \in V$, $v = aw + bu$, where $a, b \in K$. Hence, $\delta_1 v = a\delta_1 w + b\delta_1 u = aw \in V$, so anything of the form $\delta_1 v_1 + \delta_0 v_0$, where $v_0, v_1 \in V$, is in V. However, the sequence

$$0, 0, 0, 1, 0, 0, 0, s^2, 0, 0, 0, s^4, \cdots$$

satisfies $f(x)^2$ but is not in V and so not of the form $\delta_1 v_1 + \delta_0 v_0$. Thus the second part of the theorem does not hold in this case.

COROLLARY. *δ_h has minimal recursion $(x-1)^{h+1}$.*

Proof. Let $v(t) = 1$ for all $t \geqq 0$. Then v satisfies the irreducible and separable $f(x) = x - 1$. By the theorem $\delta_h = \delta_h v$ satisfies $(x-1)^{h+1}$, and by the last part of the proof of the theorem, δ_h does not satisfy $(x-1)^h$.

4. Period structure of linear recursive sequences. As an application of the decomposition theorems of the last paragraph, we determine now the complete cycle structure of an l.r.s.

Suppose v is an l.r.s. over K^n where K is finite and suppose that v satisfies $f(x)$ of degree m. Since K is finite, there are t_1 and t_2, $t_1 \neq t_2$, such that $v(t_1 + t) = v(t_2 + t)$ for $t = 0, 1, 2, \cdots, m-1$. Since $\{v(t_1 + t)\}$ and $\{v(t_2 + t)\}$ are l.r.s.'s satisfying $f(x)$ and agree for m consecutive values of t, we have $v(t_1 + t) = v(t_2 + t)$ for all $t \geqq 0$. Letting $e = |t_1 - t_2|$ and denoting by t_0 the lesser of t_1 and t_2, we obtain

$$v(t + e) = v(t) \quad \text{for all} \quad t \geqq t_0.$$

Of course, an l.r.s. v can satisfy such an equation when K is infinite.

DEFINITION 2. An l.r.s. v over K^n (K possibly infinite) is called *periodic* if there is a t_0 and an $e > 0$ such that

$$v(t + e) = v(t) \quad \text{for all} \quad t \geqq t_0.$$

If t_0 is the least integer such that an e exists satisfying this equation, then $v(0), v(1), \cdots, v(t_0 - 1)$ is called the *tail* of v and t_0 is the *length of the tail.* The least e for which this equation holds is called the *period* or *cycle length* of v.

An l.r.s. v has tail length t_0 and period e if and only if $(\sigma^e - 1)\sigma^{t_0} v = 0$, where t_0 and e are minimal as described in the definition.

If $v_1, \cdots, v_k$ are l.r.s.'s satisfying recursions which are pairwise relatively prime, then $\sum_{i=1}^{k} v_i$ is periodic if and only if each v_i is periodic.

Let v be a periodic l.r.s. Let $f(x)$ be the minimal recursion of v and let $x^l f(x)$ be the polynomial of least degree which v satisfies. Using Theorem 1 write $v = v' + v''$, where $f(\sigma)v' = 0$ and $\sigma^l v'' = 0$. Then v' and v'' are periodic, v' has tail length 0 and the same period as v, and v'' has tail length l and period 1.

Thus the tail length of a periodic l.r.s. v is equal to the largest power of x which divides the unique polynomial of least degree and leading coefficient 1 which v satisfies. Furthermore, we can write v as a sum of a "periodic part" v' and a "trivial" sequence v'' which is the tail of v. Consequently, we can restrict ourselves to l.r.s.'s without tails when computing periods.

PROPOSITION 4. *Suppose $v_1, v_2, \cdots, v_k$ are nonzero l.r.s.'s with periods $e_1, e_2, \cdots, e_k$, respectively, and without tails. If the polynomials of the minimal recursions of the v_i are relatively prime, then $v = v_1 + v_2 + \cdots + v_k$ has period equal to the least common multiple of $e_1, e_2, \cdots, e_k$.*

Proof. We prove the theorem for $k = 2$. Suppose e is the period of v. It is immediate that e divides the least common multiple of e_1 and e_2. Hence, we need only show that $e_1 \mid e$ and $e_2 \mid e$. Now,

$$v_1(t + e) + v_2(t + e) = v(t + e) = v(t) = v_1(t) + v_2(t).$$

This implies that $\{v_1(t+e) - v_1(t)\}$ satisfies the minimal recursion associated with v_2. If $v_1(t+e) - v_1(t) \not\equiv 0$ for some t, the polynomial of the minimal recursion of v_1 and that of v_2 could not be relatively prime. Thus, $v_1(t+e) = v_1(t)$ for all t and so $e_1 \mid e$. Similarly, $e_2 \mid e$.

This proposition shows that we need only be able to compute the periods of l.r.s.'s which satisfy a power of an irreducible polynomial in order to compute the period of an arbitrary l.r.s.

PROPOSITION 5. *Let $v \not\equiv 0$ be an l.r.s. satisfying the irreducible polynomial $f(x)$. Then v is periodic if and only if there is an integer $e > 0$ such that $x^e \equiv 1 \pmod{f(x)}$. The least e for which this holds is the period of v.*

The proof is immediate. This proposition of course holds when "$f(x)$ irreducibe" is replaced by "$f(x)$ is the minimal recursion of v."

The least $e > 0$, when it exists, such that $x^e \equiv 1 \pmod{f(x)}$ for an irreducible polynomial $f(x)$ is called the *period* of $f(x)$, or $f(x)$ is said to *belong to the exponent e*. We then say $f(x)$ is *periodic*. If ω is a root of $f(x)$ in an extension field E of K, then the period of $f(x)$ is the order of ω as an element of the multiplicative group of E.

COROLLARY. *If K is the finite field of q elements and $v \not\equiv 0$ is an l.r.s. satisfying the irreducible polynomial $f(x)$ of degree m, then v is periodic and its period divides $q^m - 1$.*

Proof. Since $f(x)$ is irreducible, $x^{q^m-1} \equiv 1 \pmod{f(x)}$.

We may also give an elementary proof with the material at hand. We have already remarked that if K is finite, then v is periodic. Also, since x does not divide $f(x)$, v has no tail. It only remains to show that the period e divides $q^m - 1$. Let V be the vector space of all l.r.s.'s over K which satisfy $f(x)$; then V is of dimension $m = \text{degree } f(x)$. Call two nonzero sequences v_1 and v_2 in V equivalent if there is an integer k such that $v_2 = \sigma^k v_1$ (i.e., v_1 and v_2 lie on the same "cycle"). This is an equivalence relation. By Proposition 5 every equivalence class contains the same number, e, of elements. Since $V - \{0\}$ has $q^m - 1$ elements, necessarily $e \mid q^m - 1$ is asserted.

An irreducible polynomial $f(x)$ of degree m over the finite field K of q elements is called *primitive* in the case when its period is $e = q^m - 1$. The cycle length of an l.r.s. satisfying a primitive polynomial is maximal and of importance where long cycles are required, as for example, when an l.r.s. is used to generate random numbers.

LEMMA. *Let K be of characteristic $p > 0$. If $f(x)$ is irreducible and belongs to the exponent e, then $p \nmid e$.*

Proof. Suppose $p \mid e$, say, $e = e'p$. Then $x^e - 1 \equiv (x^{e'} - 1)^p \equiv 0 (\text{mod } f(x))$. Since $f(x)$ is irreducible, $x^{e'} - 1 \equiv 0 (\text{mod } f(x))$ which contradicts the minimality of e.

The following corollary assures us that the hypothesis of separability in Theorem 2 is not too restrictive.

COROLLARY. *Let $f(x)$ be an irreducible polynomial over the field K. In order that $f(x)$ be separable, it suffices that any one of the following hold:*

(i) *K is of characteristic* 0,

(ii) *K is finite, or*

(iii) *$f(x)$ is periodic.*

Proof. (i) and (ii) are well known. We prove (iii). By (i) we may assume that the characteristic p of K is >0. By the lemma, p does not divide the period e of $f(x)$. Hence $x^e - 1$ has distinct roots. Since $f(x)$ divides $x^e - 1$, $f(x)$ also has distinct roots.

PROPOSITION 6. *Suppose K has characteristic $p > 0$. Let $w \neq 0$ be an l.r.s. having $f(x)^{h+1}$ as its minimal recursion, where $f(x)$ is irreducible and of period e. Then v has period ep^α, where $p^{\alpha-1} \leqq h < p^\alpha$.*

Proof. Observe first that δ_h has period p^α. For by the corollary to Theorem 2, δ_h satisfies $(x-1)^{p^\alpha} = x^{p^\alpha} - 1$, and hence its period divides p^α and is p^β for some $\beta \leqq \alpha$. But this implies δ_h satisfies $x^{p^\beta} - 1 = (x-1)^{p^\beta}$. By the same corollary, δ_h does not satisfy $(x-1)^j$ for $j \leqq h$. Thus $\beta = \alpha$ and δ_h has period p^α.

By Theorem 2, write $v = \sum_{i=0}^{h} \delta_i v_i$, where v_i satisfies $f(x)$ and has period e if it is not equal to 0. Since $\sum_{i=0}^{h-1} \delta_i v_i$ satisfies $f(x)^h$, necessarily $v_h \neq 0$. The period e' of v divides the l.c.m. of the periods of the $\delta_i v_i$. If $p^{\alpha_i - 1} \leqq i < p^{\alpha_i}$ defines α_i, then δ_i has period p^{α_i} by the observation above, so $\delta_i v_i$ has period dividing ep^{α_i} and e' divides l.c.m. $(ep^{\alpha_i}) = ep^\alpha$. Hence $e' = e''p^\beta$ for some $e'' \mid e$ and $\beta \leqq \alpha$.

Now

$$\begin{aligned} v = \sigma^{e'}v &= \sum_{i=0}^{h} (\sigma^{e'}\delta_i)(\sigma^{e'}v_i) \\ &= \sum_{i=0}^{h} \sum_{j=0}^{i} \binom{h-j+e'-1}{e'-1} \delta_j \sigma^{e'} v_i \\ &= \sum_{j=0}^{h} \delta_j \left(\sum_{i=j}^{h} \binom{h-j+e'-1}{e'-1} \sigma^{e'} v_i \right). \end{aligned}$$

The term in the parentheses satisfies $f(x)$ for each j, so by the uniqueness part of Theorem 2, it equals v_j. For $j = h$ this gives $\sigma^{e'}v_h = v_h$, so $e \mid e'$. Since $(p, e) = 1$, $e \mid e''$ and $e' = ep^\beta$.

Since ep^β is the period of v, jep^β is a period of v for all $j \geqq 0$. Since $(e, p^\alpha) = 1$, there is a j with $je \equiv 1 \pmod{p^\alpha}$. For this j we have

$$v = \sigma^{jep^\beta}v = \sum_{i=0}^{h} (\sigma^{jep^\beta}\delta_i)(\sigma^{jep^\beta}v_i) = \sum_{i=0}^{h} (\sigma^{p^\beta}\delta_i)v_i,$$

since δ_i has period dividing p^α.

Choose any t_0 such that $v_h(t_0) \neq 0$. For each $t \geqq 0$, there exists a such that $ap^\alpha \equiv (t_0 - t) \bmod p$. Thus

$$\sum_{i=0}^{h} \delta_i(t + ap^\alpha)v_i(t + ap^\alpha) = \sum_{i=0}^{h} \delta_i(t + ap^\alpha + p^\beta)v_i(t + ap^\alpha)$$

and

$$\sum_{i=0}^{h} \delta_i(t)v_i(t_0) = \sum_{i=0}^{h} \delta_i(t + p^\beta)v_i(t_0).$$

Hence the sequence $u = \sum_{i=0}^{h} v_i(t_0)\delta_i$ satisfies $(x-1)^{p^\beta}$.

If p^β were $< p^\alpha$, by Theorem 2 there would exist constants $c_0, c_1, \cdots, c_{p^\beta-1}$ such that $u = \sum_{i=0}^{p^\beta-1} c_i\delta_i$. Since $p^\beta - 1 < h$, we would obtain

$$\sum_{i=0}^{p^\beta-1} (v_i(t_0) - c_i)\delta_i + \sum_{i=p^\beta}^{h} v_i(t_0)\delta_i = 0.$$

Since $v_h(t_0) \neq 0$, this would contradict the uniqueness part of Theorem 2. Thus $\beta = \alpha$ and the proof is complete.

COROLLARY. *Suppose K has characteristic $p > 0$. Let $w \neq 0$ be an l.r.s. satisfying an irreducible polynomial. If v is periodic with period e, then $\delta_h v$ has period ep^α, where $p^{\alpha-1} \leqq h < p^\alpha$.*

Given a polynomial $f(x)$, we can now describe the possible periods an l.r.s. v satisfying $f(x)$ can have. Factor $f(x)$ as

$$f(x) = x^l f_1(x)^{h_1} f_2(x)^{h_2} \cdots f_r(x)^{h_r},$$

where the $f_i(x)$ are distinct, irreducible and not equal to x. Then v will have a tail of length at most l, and its period will be of the form l.c.m. $(e_i)p^\alpha$, where e_i is either the period of $f_i(x)$ or $e_i = 1$, and $p^{\alpha-1} \leqq \max(h_i - 1)$. If $f(x)$ is the polynomial of least degree and leading coefficient 1 which v satisfies, then v has tail length equal to l, and its period is l.c.m. $(e_i)p^\alpha$, where e_i is the period of $f_i(x)$ and p^α is determined by $p^{\alpha-1} \leqq \max(h_i - 1) < p^\alpha$.

5. Application: The order of a nonsingular matrix. A nonsingular matrix A has *finite order* if there is an integer $e > 0$ such that A^e is the identity matrix. The least e for which this happens is called the *order* of A.

THEOREM 3. *Let A be a nonsingular $n \times n$ matrix over the field K. Suppose that A has finite order. Let $f(x) = f_1(x)^{h_1} \cdots f_r(x)^{h_r}$ be the minimal polynomial of A, where the $f_i(x)$ are irreducible and pairwise relatively prime. Let e_i be the period of $f_i(x)$, $e =$ l.c.m. (e_i), and $h = \max(h_i)$.*

(i) *If K has characteristic 0, then $h = 1$ and e is the order of A.*

(ii) *If K has characteristic $p > 0$, then A has order ep^α, where $p^{\alpha-1} < h \leqq p^\alpha$.*

Proof. Let $u_1, \cdots, u_n$ be a basis of K^n. Consider the l.r.s. over the n^2-dimensional vector space consisting of n-tuples of vectors from K^n defined by

$$v(t) = \begin{bmatrix} A & & & 0 \\ & A & & \\ & & \ddots & \\ & & & \ddots \\ 0 & & & A \end{bmatrix}^t \begin{bmatrix} u_1 \\ u_2 \\ \cdot \\ \cdot \\ \cdot \\ u_n \end{bmatrix}.$$

Clearly $g(A) = 0$ if and only if $g(\sigma)v = 0$ where $g(x) \in K[x]$. Hence, the minimal recursion of v is $f(x)$ and the period of v is the order of A. The theorem now follows from the discussion in §4.

Of course, this theorem can be proved by putting A into Jordan canonical form, but then, the whole subject of l.r.s.'s can be developed along such lines.

REFERENCES

[1] T. G. BIRDSALL AND M. P. RISTENBATT, *Introduction to linear shift-register generated sequences*, Tech. Rep. 90, Electronic Defense Group, Department of Electrical Engineering, University of Michigan, Ann Arbor, 1958.

[2] W. A. BLANKINSHIP, *A new version of the Euclidean algorithm*, Amer. Math. Monthly, 70 (1963), pp. 742–745.

[3] T. L. BOOTH, *An analytical representation of signals in sequential networks*, Proc. Symposium on Mathematical Theory of Automata, New York, 1962, Polytechnic Press of the Polytechnic Institute of Brooklyn, Brooklyn, New York, 1963, pp. 301–340.

[4] B. ELSPAS, *The theory of autonomous linear sequential networks*, IRE Trans. Circuit Theory, CT-6 (1959), pp. 45–60.

[5] S. W. GOLOMB, *Shift Register Sequences*, Holden-Day, San Francisco, 1967.

[6] W. W. PETERSON, *Error-Correcting Codes*, John Wiley, New York, 1961.

[7] E. S. SELMER, *Linear recurrence relations over finite fields*, Department of Mathematics, University of Bergen, Norway, 1966.

[8] N. ZIERLER, *Linear recurring sequences*, J. Soc. Indust. Appl. Math., 7 (1959), pp. 31–48.

[9] S. W. GOLOMB, ed., *Digital Communications, with Space Applications*, Prentice-Hall, Englewood Cliffs, New Jersey, 1964.