Electronics Research Laboratory
University of California
Berkeley, California

THE CONSTRUCTION OF MAXIMAL LENGTH SHIFT-REGISTER SEQUENCES

by

A. Chang

Supported in part by the
Air Force Office of Scientific Research
of the Office of Aerospace Research;
Department of the Army, Army Research Office;
and Department of the Navy, Office of Naval Research
Grant No. AF-AFOSR-62-340

September 7, 1962

SUMMARY

The principal result of this report is a method of constructing all possible maximal length shift register sequences. The proposed construction is inductive in the sense that from a maximal length sequence of degree n-1, a family of maximal length sequences of degree n is constructed. This construction is a generalization of Golomb's and Welch's method.[2]

INTRODUCTION

Let S be a set consisting of m objects and let S^n be the set of all n-tuples of members of S. The elements of S will be denoted by Roman letters, $a, b, c, \ldots,$ and the members of S^n by Greek letters $\alpha, \beta, \ldots,$ or sometimes, more explicitly, by n-tuples such as $(a_1, a_2, \ldots, a_n)$. A function defined on S^n with values in S, $f:S^n \longrightarrow S$, and a member of S^n can be used to define a sequence in the following way: If $\alpha=(a_1, a_2, \ldots, a_n)$ is a member of S^n let the first n elements of the sequence be $a_1, a_2, \ldots, a_n$. If the first $n+k$ elements of the sequence have been defined, $k=0,1,2,\ldots,$ let $a_{n+k+1}=f(a_{k+1}, a_{k+2}, \ldots, a_{k+n})$ be the $n+k+1$ st element.

A sequence generated in this manner will be called a shift register sequence of degree n.[1] In keeping with this physically motivated terminology, the members of S and S^n will be called output symbols and states, respectively. The function f will be called a feedback function, and α is the initial state.

PART I

A feedback function f defines a function T on S^n into S^n by taking

$$T(a_1, a_2, \ldots, a_n) = (a_2, a_3, \ldots, a_{n-1}, f(a_1, a_2, \ldots, a_n)).$$

Conversely, a function $T:S^n \longrightarrow S^n$ with the property

$$T(a_1, a_2, \ldots, a_n) = (a_2, a_3, \ldots, a_n, a_{n+1})$$

defines a feedback function f by the relation $f(a_1, \ldots, a_n)=a_{n+1}$. T is called the state transition function. The reason for introducing T is that it simplifies the discussion of some aspects of shift register sequences.

Associated with each sequence generated by a feedback function f and initial state α is a sequence of states, namely, α, $T\alpha$, $T^2\alpha, \ldots$. Let $A_p = \{\beta \epsilon S^n | \beta = T^\ell \alpha, \; 0 \leq \ell \leq p-1\}$, $p = 0, 1, 2, \ldots$. Clearly the number of elements in A_p is at most p and $A_p \subset A_{p+1}$. Since S^n has exactly m^n elements, it follows that there exists an integer $N \leq m^n$ such that $A_N = A_{N+1}$. We have the following proposition:

<u>Proposition 1:</u> Let L be the least integer such that $A_L = A_{L+1}$. Then

(a). $T^L\alpha = T^j\alpha$ for some $j < L$ but

$T^i\alpha \neq T^j\alpha$ for $i < j < L$.

(b). $A_L = A_k$ for all $k \geq L$.

<u>Proof:</u> Statement (a) just expresses the fact that L is the least integer such that $A_L = A_{L+1}$. To prove (a), it suffices to prove $A_{L+2} \subset A_{L+1}$. This is equivalent to showing $T^{L+1}\alpha \epsilon A_{L+1}$. Since $T^L\alpha = T^j\alpha$ for some $j < L$, $T^{L+1}\alpha = T(T^L\alpha) = T(T^j\alpha) = T^{j+1}\alpha$. But $T^{j+1}\alpha \epsilon A_{L+1}$ since $j < L$, which proves (b).

Let j and L satisfy condition (a) of Proposition 1. Then if j equals zero, the sequence of states is periodic with period L. If j is greater than zero, the sequence obtained by deleting $\alpha, T\alpha, \ldots, T^{j-1}\alpha$ from the original sequence is periodic with period $L-j$. The states $\alpha, T\alpha, \ldots, T^{j-1}\alpha$ are called transient states; they appear only in the first part of the sequence.

It follows from the periodicity of the sequence of states associated with a shift register sequence that the s. r. sequence itself is periodic and in fact, it has the same period as the former. The first $L+n-1$ terms of a shift register sequence will be called the <u>initial segment</u> of the sequence. When $j=0$ and $L=m^n$, the corresponding sequence is said to be of <u>maximal length.</u> Obviously, no shift register can have a longer period. Such a sequence, evidently, has the property that every member of S^n occurs as n consecutive symbols in the initial segment of the sequence.

Proposition 2 gives equivalent formulations of the condition $j=0$.

Proposition 2: Let L satisfy condition (a) of Proposition 1. Then the following four statements are equivalent:

(a). No transient states exist, i. e., $j=0$.

(b). Every state in A_L has a predecessor in A_L, i. e., if $\alpha \epsilon A_L$, then $\alpha = T\beta$ for some $\beta \epsilon A_L$.

(c). The restriction of T to A_L is a one-to-one function.

(d). $f(x, a_2, \ldots, a_n) \neq f(y, a_2, \ldots, a_n)$ if $x \neq y$ for all states in A_L.

Proof:

1. a $\Longrightarrow$ b: If $j=0$ then $\alpha = T^L \alpha = T(T^{L-1}\alpha)$. Since $A_L = \{\beta | \beta = T^{\ell} \alpha, 0 \leq \ell \leq L-1\}$, it follows that every member of A_L has a predecessor in A_L.

2. b $\Longrightarrow$ c: Let $T(A_L) = \{\alpha | \alpha = T\beta$ for some $\beta \epsilon A_L\}$. Assuming b, every member of A_L is a $T\beta$ for some $\beta \epsilon A_L$, so $T(A_L) \supset A_L$. But $T(A_L)$ cannot contain more members than A_L, since T is single valued. Hence, $A_k = T(A_k)$, which implies T is a one-to-one function on A_L onto A_L.

3. c $\Longrightarrow$ d: If T is one-to-one, then $f(x, a_2, \ldots, a_n) \neq f(y, a_2, \ldots, a_n)$ if $x \neq y$, for otherwise $(x, a_2, \ldots, a_n)$ and $(y, a_2, \ldots, a_n)$ would have the same image under T.

4. d $\Longrightarrow$ a: If $j \neq 0$, then $T^L \alpha = T^j \alpha$ for some $0<j<L$. By choice of L, $T^{L-1}\alpha \neq T^{j-1}\alpha$. Hence, $T^j \alpha$ has two distinct predecessors: $T^{L-1}\alpha$ and $T^{j-1}\alpha$. Let $(x, a_2, \ldots, a_n) = T^{L-1}\alpha$ and $(y, a_2, \ldots, a_n) = T^{j-1}\alpha$. Then $f(x, a_2, \ldots, a_n) = f(y, a_2, \ldots, a_n)$ but $x \neq y$. Hence, d $\Longrightarrow$ a.

Given a shift register sequence $\{a_i\}_{i=1}^{\infty}$, we can associate a sequence of n-tuples $\{\alpha_k\}_{k=1}^{\infty}$ by taking $\alpha_k = (a_k, a_{k+1}, \ldots, a_{k+n-1})$. A member of S^n is said to appear or occur in the s. r. sequence if it appears in the associated sequence of n-tuples. The s. r. sequence defines the set of all feedback functions which can generate it by restricting their values on those n-tuples which appear in the sequence. If the sequence has maximal length, it uniquely determines one feedback function as every n-tuple occurs in the sequence. Such sequences will be the principal object of interest in the sequel.

PART II

In this section a method for constructing all possible maximal length s.r. sequences will be developed. Because such sequences are periodic, it suffices to construct only the first m^n+n-1 terms of it (technically only the first m^n terms need be constructed but it is convenient to consider m^n+n-1 terms). The basic tool which will be used in the construction is called a preference function.[2]

Let S^{n-1} be the set of all (n-1)-tuples of elements of S and let Π be the set of all permutations of elements of S. A <u>preference function</u> is a mapping on S^{n-1} to Π. Equivalently, p is an m-tuple, $(p_1, p_2, \ldots, p_m)$ of functions p_i on S^{n-1} to S with the property that $p_i(a_1, a_2, \ldots, a_{n-1}) \neq p_j(a_1, \ldots, a_{n-1})$ for $i \neq j$ for any point in S^{n-1}. If n=1, S^{n-1} is empty. In this case, by convention, a preference function is taken as a permutation, i.e., a member of Π.

A preference function and a member of S^{n-1} can be used to define a segment of a sequence by the following rules:

1. If $(a_1, a_2, \ldots, a_{n-1})$ is a member of S^{n-1}, let the first n-1 elements of the segment be $a_1, a_2, \ldots, a_{n-1}$.

2. If the first n+k-1 terms of the segment have been defined, determine the n+k-th term by the rule $a_{n+k} = p_i(a_{k+1}, a_{k+2}, \ldots, a_{k+n-1})$ where i is the smallest integer such that the word $(a_{k+1}, \ldots, a_{k+n})$ does not occur as n consecutive symbols twice in the first n+k terms of the segment.

3. If no such i exists, the segment is terminated. Let L denote the value of k such that this condition is fulfilled.

The following three lemmas, which in somewhat different form may be found in ref. 1, give the connection between the segments generated by preference functions and shift register sequences .

Lemma 1: Given a segment generated by a preference function, it is extendable to m distinct register sequences, i. e., the segment is the initial segment of m shift register sequences.

Proof: It suffices to exhibit m feedback functions which generate sequences having the given segment as an initial segment. Let $a_1, a_2, \ldots, a_{L+n-1}$ be the segment. By the way it is constructed, no state appears twice in it. Therefore, f can be defined (single valuedly) by the relation $f(a_p, a_{p+1}, \ldots, a_{p+n-1}) = a_{p+n}$ for $1 \leq p < L$. For $p=L$, define $f(a_{L+1}, \ldots, a_{L+n-1})$ arbitrarily (this gives m different functions). Note that because $(a_{L+1}, \ldots, a_{L+n-1})$ terminates the segment, it must have occurred $m+1$ times in the segment. Hence, $(a_{L+1}, \ldots, a_{L+n-1}, f(a_{L+1}, \ldots, a_{L+n-1}))$ must appear in the segment, so $k=L$ satisfies (a) of Proposition 1. It follows that the f so defined are the required functions.

Lemma 2: With the same notation of Lemma 1 if $f(a_{L+1}, \ldots, a_{L+n-1}) = a_n$, the period of the resulting s. r. sequence equals L.

Proof: It suffices to show $(a_1, a_2, \ldots, a_n) = (a_{L+1}, a_{L+2}, \ldots, a_{L+n-1}, a_n)$. Recall that $(a_{L+1}, \ldots, a_{L+n-1})$ appears $m+1$ times in the segment. If $(a_1, \ldots, a_n) \neq (a_{L+1}, \ldots, a_{L+n-1}, a_n)$ then $m+1$ states of the form $(x, a_{L+1}, \ldots, a_{L+n-1})$ of which at least two are the same appear in the segment, which is impossible.

Lemma 3: Every shift register sequence is the extension of a segment defined by a preference function. If the sequence is maximal, the corresponding preference function is unique.

Proof: Let $\{a_i\}_{i=1}^{\infty}$ be any shift register sequence and let L be the largest integer such that in the segment $a_1, a_2, \ldots, a_{L+n-1}$ any state occurs at most once. If $(x_1, x_2, \ldots, x_{n-1})$ are any $n-1$ consecutive symbols in the segment, define $p_i(x_1, x_2, \ldots, x_{n-1})$ to be the successor to the i-th occurrence of $(x_1, x_2, \ldots, x_{n-1})$ in $\{a_i\}_{i=1}^{\infty}$. If there are fewer than i occurrences, define the remaining components of p arbitrarily but subject to the restriction that the components are all distinct. The p so defined is the required function. When $\{a_i\}_{i=1}^{\infty}$ is maximal $L=m^n$ in which case every point in S^n appears once which implies every point of S^{n-1} occurs m times, each time with a successor. Hence, p is uniquely determined in this case.

In view of Lemmas 1-3, to construct all maximal length shift register sequences, it suffices to construct all preference functions which define segments of length m^n+n-1. Before proceeding further, it is necessary to introduce some notation. Let $b_1, b_2, \ldots, b_N$ be the initial segment of a shift register sequence of degree $n-1$ and let $x_2, x_3, \ldots, x_{n-1}$ be any $n-2$ consecutive symbols in it. If there are r occurrences of $(x_2, x_3, \ldots, x_{n-1})$ in the segment, the notation $(x_1^i, x_2, \ldots, x_{n-1})$, $1 \leq i \leq r$ will mean each $(x_1^i, x_2, \ldots, x_{n-1})$ occurs as $n-1$ consecutive symbols in the segment and $(x_1^i, x_2, \ldots, x_{n-1})$ appears "before" $(x_1^j, x_2, \ldots, x_{n-1})$ iff $i<j$.

If $b_1, b_2, \ldots, b_N$ is the initial segment of a maximal length sequence of degree $n-1$, then every member of S^{n-1} occurs as $n-1$ consecutive symbols in it. Thus the initial segment of a maximal sequence defines a partial ordering of S^{n-1} by the rule $(x_1^i, x_2, \ldots, x_{n-1})$ precedes $(x_1^j, x_2, \ldots, x_{n-1})$ iff $i < j$. With this notation, the following theorem shows how to construct a family of maximal length sequences of degree n from a maximal length sequence of degree $n-1$.

Theorem 1: Let $\{b_k\}_{k=1}^{\infty}$ be a maximal length sequence of degree n-1 and let S^{n-1} be partially ordered as defined above. Let x_n^i be the term which follows $(x_1^i, x_2, \ldots, x_{n-1})$ in $\{b_k\}_{k=1}^{\infty}$. Define a family P of preference functions $p=(p_1, p_2, \ldots, p_m)$ by the rule $p \in P$ iff:

(a) $p_1(b_1, b_2, \ldots, b_{n-1}) = b_n$

(b) $p_m(x_1^j, x_2, \ldots, x_{n-1}) \in \bigcup_{k=j}^{m} \{x_n^k\}$,

or equivalently,

$$p_m(x_1^j, x_2, \ldots, x_{n-1}) \notin \bigcup_{k=1}^{j-1} \{x_n^k\}$$

(c) p_j for $1 \leq j < m$ is arbitrary except for (a) and the requirement that p be a preference function.

Then, if $p \in P$, the segment defined by it and $(b_1, b_2, \ldots, b_{n-1})$ has length m^n+n-1.

Proof: Let $p \in P$ and let $\{a_i\}$ denote the initial segment defined by p and $(b_1, b_2, \ldots, b_{n-1})$. Then $\{a_i\}$ has length m^n+n-1 iff every member of S^n occurs in it, and this is so iff each member of S^{n-1} occurs m times, (as n-1 consecutive symbols) in $\{a_i\}$, each time with a successor. Since $\{b_k\}_{k=1}^{\infty}$ has degree n-1 and is maximal, every element of S^{n-1} occurs in the segment $b_1, b_2, \ldots, b_{m^{n-1}+n-1})$ and, moreover, $(b_1, b_2, \ldots, b_{n-1}) = (b_{m^{n-1}}, \ldots, b_{m^{n-1}+n-1})$. Hence, it suffices to show $(b_{N+1}, b_{N+2}, \ldots, b_{N+n-1})$ occurs m times in $\{a_i\}$, each time with a successor, for $1 \leq N \leq m^{n-1}$. The proof is by induction on N.

1. If $N = m^{n-1}$, from the proof of Lemma 2 $(b_1, b_2, \ldots, b_{n-1})$ occurs m+1 times in $\{a_i\}$, m of these times with a successor since $(b_1, b_2, \ldots, b_{n-1})=(b_{N+1}, \ldots, b_{N+n-1})$, the induction hypothesis is true for $N=m^{n-1}$.

2. Assume the hypothesis for all $N \geq r_o+1 > 2$. We have to show $(b_{r_o+1}, \dots, b_{r_o+n-1})$ occurs m times in $\{a_i\}$. Consider the m words $(x_1^i, x_2, \dots, x_{n-1}, x_n^i)$ in S^n with $(x_2, x_3, \dots, x_{n-1}) = (b_{r_o+2}, \dots, b_{r_o+n-1})$, and suppose $x_1^j = b_{r_o+1}$. Consider the identities,

$$(x_1^j, x_2, \dots, x_{n-1}, x_n^j) = (b_{r_o+1}, b_{r_o+2}, \dots, b_{r_o+n-1}, b_{r_o+n})$$

$$(x_1^{j+1}, x_2, \dots, x_{n-1}, x_n^{j+1}) = (b_{r_1+1}, b_{r_1+2}, \dots, b_{r_1+n-1}, b_{r_1+n})$$

$$\vdots \qquad\qquad\qquad \vdots$$

$$(x_1^m, x_2, \dots, x_{n-1}, x_n^m) = (b_{r_{m-j}+1}, b_{r_{m-j}+2}, \dots, b_{r_{m-j}+n-1}, b_{r_{m-j}+n})$$

Clearly $r_{m-j} > r_{m-j-1} > \dots > r_o$. By hypothesis, the $(b_{r_k+2}, \dots, b_{r_k+n-1}, b_{r_k+n})$, $0 \leq k \leq m-j$, appear m times from which it follows that $(x_1^j, x_2, \dots, x_{n-1}, x_n^k)$ occurs in $\{a_i\}$ for k=j, j+1, ..., m, for otherwise the m occurrence of some $(b_{r_k+2}, \dots, b_{r_k+n-1}, b_{r_k+n})$ would be succeeded by at most m-1 different symbols and hence at least two identical states would appear in $\{a_i\}$ which is impossible.

For any $p \in P$, $p_m(x_1^j, x_2, \dots, x_{n-1}) \in \bigcup_{k=j}^{m} \{x_n^k\}$. To be specific, suppose $p_m(x_1^j, x_2, \dots, x_{n-1}) = x_n^j$. As a consequence $p_k(x_1^j, x_2, \dots, x_{n-1}) \neq x_n^j$ for $1 \leq k < m$. Then this last remark together with the fact that $(x_1^j, x_2, \dots, x_{n-1}, x_n^j)$ occurs in $\{a_i\}$ imply that $(x_1^j, x_2, \dots, x_{n-1}) = (b_{r_o+1}, b_{r_o+2}, \dots, b_{r_o+n-1})$ occurs m times in $\{a_i\}$, each time with a successor.For $p_m(x_1^j, x_2, \dots, x_{n-1})$ chosen otherwise the argument is analogous. This completes the proof of Theorem 1.

The preceding theorem indicates how to construct a family of maximal length sequences of degree n given a maximal length sequence of degree n-1. If instead of using a single sequence of degree n-1 in this construction, we use the set of all maximal length sequences of degree n-1, we can obtain a collection of families of maximal length sequences. The following theorem implies that this collection is, in fact, the set of all maximal length sequences.

Theorem 2: Let $\{a_i\}_{L=1}^{\infty}$ be a maximal length s. r. sequence of degree n. Then, there exists at least one maximal length s. r. sequence of degree n-1, $\{b_k\}_{k=1}^{\infty}$, such that $\{a_i\}_{L=1}^{\infty}$ can be constructed from $\{b_k\}_{k=1}^{\infty}$ via the method of Theorem 1.

Proof: We have to show there exists a $\{b_k\}_{k=1}^{\infty}$ which is maximal and such that the preference function associated with $\{a_i\}_{i=1}^{\infty}$ (see Lemma 3) belongs to the family of functions generated by $\{b_k\}_{k=1}^{\infty}$ and the method of Theorem 1. It suffices to consider only the initial segments of the sequences.

Let p_m be the m-th component of the preference function associated with $\{a_i\}_{i=1}^{\infty}$. Using the notation described in the paragraphs preceding Theorem 1, we construct the initial segment of $\{b_k\}_{k=1}^{\infty}$ according to the following rules:

1. $a_i = b_i$ for $1 \leq i \leq n$.

2. Suppose $b_1, b_2, \ldots, b_{k+n-1}$, $k > 0$, have been defined. Let $(x_2, x_3, \ldots, x_{n-1}) = (b_{k+2}, \ldots, b_{k+n-1})$ and suppose $(x_2, x_3, \ldots, x_{n-1})$ has occurred j times in $b_1, b_2, \ldots, b_{+n-1}$. Denote by x_1^i and x_n^i, respectively, the successor and predecessor of the i-th occurrence of $(x_2, x_3, \ldots, x_{n-1})$. Then let the choice of b_{k+n} satisfy the rule:

$$b_{k+n} = x_n^j \notin \bigcup_{x_1 \notin \bigcup_{i=1}^{j} x_1^i} \{p_m(x_1, x_2, \ldots, x_{n-1})\} \cup \bigcup_{i=1}^{j-1} \{x_n^i\}$$

3. If no such b_{k+n} exists, the segment is terminated.

Condition 2 on b_{k+n} allows p_m to satisfy condition (b) of Theorem 1. To see this note that

$$x_n^j \notin \bigcup_{x_1 \notin \bigcup_{i=1}^{j} x_1^i} \{p_m(x_1, x_2, \ldots, x_{n-1})\} \; \forall j \Longrightarrow p_m(x_1^j, x_2, \ldots, x_{n-1}) \neq x_n^i \; \forall i < j$$

$$\Longrightarrow p_m(x_1^j, x_2, \ldots, x_{n-1}) \notin \bigcup_{i=1}^{j-1} \{x_n^i\} \Longrightarrow \text{condition (b) of Theorem 1}$$

Condition (a) of Theorem 1 is satisfied because $a_n = p_1(a_1, a_2, \ldots, a_{n-1}) = b_n$, and condition (c) is trivially satisfied.

Thus, it remains to show that the segment so defined is the initial segment of a maximal length s. r. sequence. The condition, $x_n^j \notin \bigcup_{i=1}^{j-1} \{x_n^i\}$, guarantees that no n-1 symbol word occurs twice; hence the desired result will follow if we can show every n-1 symbol word occurs in the segment. Suppose, on the contrary, that some n-1 symbol word does not occur. Consider $a_1, a_2, \ldots, a_{m^n+n-1}$, the initial segment of $\{a_i\}_{i=1}^{\infty}$. Then there exists a greatest integer $N \leq m^n - 1$ such that $(a_{N+2}, a_{N+3}, \ldots, a_{N+n})$ occurs in the segment but $\alpha = (a_{N+1}, a_{N+2}, \ldots, a_{N+n-1})$ does not. (The existence of such an N follows from the occurrence of $(a_2, a_3, \ldots, a_n) = (a_{N+2}, a_{N+3}, \ldots, a_{N+n})$ for $N = m^n - 1$.) It is clear from the definition of N that $(a_{N+1}, \ldots, a_{N+n-1})$ is the m-th (i, e., last) occurrence of α in the initial segment of $\{a_i\}_{i=1}^{\infty}$

Hence $p_m(a_{N+1}, \ldots, a_{N+n-1}) = a_{N+n}$. To conform with the notation of condition 2, let $(x_2, x_3, \ldots, x_{n-1}) = (a_{N+2}, \ldots, a_{N+n-1})$ and assume $a_{N+n} = x_n^j$ for some j. Since α does not occur in the segment, $a_{N+1} \notin \bigcup_{i=1}^{j} \{x_1^i\}$ for any j. Hence, $a_{N+n} = x_n^j \neq p_m(a_{N+1}, a_{N+2}, \ldots, a_{N+n-1}) = a_{N+n}$ which is a contradiction. This completes the proof of Theorem 2.

Theorems 1 and 2 indicate how, in principle, one can construct every maximal length shift register sequence for arbitrary degree, n, and number of output symbols, m. J. van Ardenne-Ehrenfest and N. G. de Bruijn[3] have shown by a combinatorial argument that the number of such sequences is $m^{-n}(m!)^{m^{n-1}}$. For even modest values of m and n this number becomes astronomically large. It is also possible to arrive at this number, at least for small values of m, by making use of Theorems 1 and 2 and some simple computations.

REFERENCES

1. Elpsas, B., "The Theory of Autonomous Linear Sequential Networks," IRE Trans. on Circuit Theory, Vol. CT-6 (March 1959), p. 45.

2. Golomb, S. W. and Welch, L. R., "Nonlinear Shift-Register Sequences," Jet Propulsion Laboratory Memorandum No. 20-149, Calif. Inst. of Technology, Pasadena, Calif., October 1957.

3. van Ardenne-Ehrenfest, J. and de Bruijn, N. G., "Circuits and Trees in Oriented Linear Graphs," Simon Stevin, Vol. 26 (1950-1951), pp. 203-217.