An Algorithm for Generating Stable Feedback Shift Registers of Order *n*

FREDERIC J. MOWLE

Purdue University, Lafayette, Indiana

ABSTRACT. It is shown in this paper that the stable feedback shift registers, when classified according to Hamming weight (the number of fundamental product terms in expanded sum of products form), are binomially distributed, i.e., there are $\binom{2^n - n - 1}{w}$ stable feedback shift registers of order n with Hamming weight equal to w. Using this relationship, a recursive algorithm is established which will generate all stable feedback shift registers of order n. Formulas are also given for determining the number of stable feedback shift registers which have $j + 1$ starting states and $j + 1$ branch states, $0 \leq j \leq 2^{n-1} - 1$.

Introduction

In a previous paper [1] the author has shown that the number of stable feedback shift registers of order n is exactly $2^{2^n - n - 1}$. In the same paper, the author also showed that the number of stable feedback shift registers of order n is the same as the number of stable maximum transient feedback shift registers of order $n + 1$. In this paper it is shown that the feedback shift registers of order n are distributed binomially according to Hamming weight. From this relationship a recursive algorithm is established for generating all stable feedback shift registers of order n.

Basic Definitions and Properties

The general form of the autonomous binary feedback shift register, denoted by FSR, is shown in Figure 1.

The *order n* of an FSR is equal to the number of unit delay stages. The n-tuple $\mathbf{s} = (s_{n-1}, s_{n-2}, \cdots, s_1, s_0)$ is the *state* of the FSR, where each s_j is the output of one of the unit delay stages. The *feedback function* $f(\mathbf{s})$ can be any of the 2^{2^n} distinct Boolean functions of the binary variables s_j, $j = 0, \cdots, n - 1$. If $\mathbf{s}$ is the present state of an FSR, then the next state is denoted by $\theta\mathbf{s} = (f(\mathbf{s}), s_{n-1}, \cdots, s_2, s_1)$. θ is called the next state operator. The state after j shifts is denoted by $\theta^j\mathbf{s}$.

For notational convenience, if

$$\mathbf{s} = (s_{n-1}, s_{n-2}, \cdots, s_1, s_0),$$

then

$$\begin{aligned} \mathbf{s}^{\{0\}} &= (s_{n-1}, s_{n-2}, \cdots, s_1, s_0 \oplus 1), \\ \mathbf{s}^{\{1\}} &= (s_{n-1}, s_{n-2}, \cdots, s_1 \oplus 1, s_0), \\ \mathbf{s}^{\{i\}} &= (s_{n-1}, s_{n-2}, \cdots, s_i \oplus 1, s_{i+1}, \cdots, s_0), \\ \mathbf{s}^{\{n-1\}} &= (s_{n-1} \oplus 1, s_{n-2}, \cdots, s_0), \end{aligned}$$

The work reported here is part of the author's Ph.D. dissertation, submitted to the University of Notre Dame, Notre Dame, Indiana, January 1966. This work was supported by the National Science Foundation under Grant No. GP-2547.

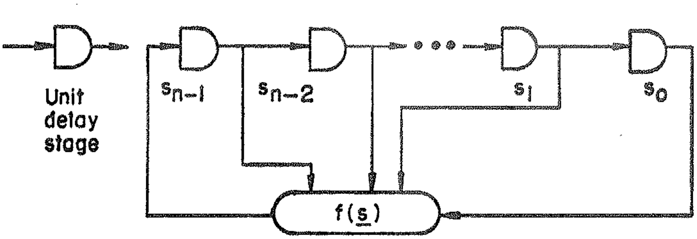

Fig. 1. Autonomous binary feedback shift register

where $\oplus$ denotes module 2 addition, i.e., $\mathbf{s}^{(i)}$ is the state whose components agree with the components of state s in all positions except the ith.

The *state diagram* of an FSR of order n is a directed linear graph consisting of 2^n nodes, one for each state on the FSR, and 2^n directed branches, one leaving each node (state), such that the branch leaving node α terminates on node β if and only if $\theta \mathbf{s}_\alpha = \mathbf{s}_\beta$.

The node on a state diagram corresponding to a state $\mathbf{s} = (s_{n-1}, s_{n-2}, \cdots, s_1, s_0)$ may be denoted by either the binary integer $s_{n-1}s_{n-2} \cdots s_1s_0$ or the decimal integer $S = \sum_{k=0}^{n-1} s_k 2^k$. Since the correspondence between S and s is unique, in this report a state referred by S is understood to be the state s which corresponds to the binary representation of the decimal integer S.

A state s such that $\theta \mathbf{s} = \mathbf{s}$ will be called a persistent state [2] or an *equilibrium state* [3]. The states $\mathbf{0} = (0, 0, \cdots, 0)$ and $\mathbf{1} = (1, 1, \cdots, 1)$ are the only possible equilibrium states on an FSR. A sequence of T distinct states $(T > 1)\mathbf{s}_1, \mathbf{s}_2, \cdots, \mathbf{s}_T$ such that $\theta \mathbf{s}_T = \mathbf{s}_1$ and $\theta \mathbf{s}_j = \mathbf{s}_{j+1}$, $j = 1, \cdots, T - 1$, will be called a *closed cycle of period* T [4]. In this report the term *cycle* is used only when the discussion pertains to both closed cycles and equilibrium states.

A sequence of L distinct states $\mathbf{s}^*, \theta\mathbf{s}^*, \cdots, \theta^{L-1}\mathbf{s}^*$ none of which lie on a cycle will be called a transient of length L if and only if $\theta^L\mathbf{s}^*$ lies on a cycle. The state $\mathbf{s}^*$ will be called the starting state for the transient.

Although every state on an FSR has a unique successor state, a state may have no predecessor, a single predecessor state or at most two distinct predecessor states. The two possible predecessors of a state $\mathbf{s} = (s_{n-1}, s_{n-2}, \cdots, s_1, s_0)$ are the states $(s_{n-2}, \cdots, s_1, s_0, 1)$ and $(s_{n-2}, \cdots, s_1, s_0, 0)$. A state s which has two predecessors will be called a *branch state*, and a state s which has no predecessors will be called a *starting state.*

The *Hamming weight of a binary n-tuple* [3] is equal to the number of its nonzero components. The Hamming weight of a state s is denoted by $W(\mathbf{s})$.

Definition 1. All states s on an nth order FSR such that $f(\mathbf{s}) = 0$ will be called *zero feedback* states (ZFS), and all states s such that $f(\mathbf{s}) = 1$ will be called unit feedback states (UFS).

Since every state on an nth order FSR is either a zero feedback state or a unit feedback state, the following definition is appropriate.

Using integer notation, for each state S, $F(S) \equiv f(\mathbf{s})$ if S is the decimal integer which corresponds to the binary representation of the state s.

Definition 2. The 2^n-tuple $\mathbf{F} = (F(0), F(1), F(2), \cdots, F(2^n - 1))$ will be called the *canonic representation* of the FSR.

Definition 3. The *Hamming weight of an FSR* of order n is equal to the number of the nonzero components in its canonic representation and will be denoted by $W(\mathbf{F})$.

Property 1. The number of branch states on an FSR of order n is always equal to the number of starting states.

Property 2. (This is due to Magleby [5].) If state $\mathbf{s}_\beta$ is a possible successor of state $\mathbf{s}_\alpha$ on an nth order FSR, then state $\mathbf{s}_\beta$ is also a possible successor of state $\mathbf{s}_\alpha^{\{0\}}$ and state $\mathbf{s}_\beta^{\{n-1\}}$ is the other possible successor for states $\mathbf{s}_\alpha$ and $\mathbf{s}_\alpha^{\{0\}}$.

Definition 4. (This is due to Massey and Liu [3].) An FSR is *stable* if and only if there exists an integer N such that for all states $\mathbf{s}$, $\theta^N\mathbf{s} = \mathbf{0}$; i.e., $\mathbf{0}$ is the only equilibrium state and there are no closed cycles.

Property 3. On every stable FSR of order n, $\theta\mathbf{1} = \mathbf{1}^{\{n-1\}}$ and $\theta\mathbf{0}^{\{0\}} = \mathbf{0}$; i.e., $f(\mathbf{1}) = 0$ and $f(\mathbf{0}^{\{0\}}) = 0$.

The FSR of order 3, defined by $f(\mathbf{s}) = s_0(s_1 \oplus s_2 \oplus s_1s_2)$, is unstable. An example of a stable FSR of order 3 is $f(\mathbf{s}) = s_2(s_1 \oplus 1)$.

Definition 5. An FSR of order n will be called a *stable maximum transient FSR*, if it is stable and has a single starting state.

Property 4. The state $\mathbf{s} = \mathbf{0}^{\{n-1\}} = (1, 0, \cdots, 0)$ is the only starting state for all stable maximum transient FSR's of order n and is a starting state on every stable FSR.

Distribution of Stable FSR's by Hamming Weight

In [1, 6] it is shown that there are exactly 2^{2^n-n-1} distinct stable feedback shift registers of order n. The canonic representation of the single stable FSR of order 1 is $\mathbf{F} = (0, 0)$. The Hamming weight of this FSR is $W(\mathbf{F}) = 0$. The canonic representations of the two stable FSR's of order 2 are $\mathbf{F} = (0, 0, 0, 0)$ and $\mathbf{F} = (0, 0, 1, 0)$, with Hamming weights 0 and 1, respectively. The canonic representations of the 16 stable FSR's of order 3 are given in Table 1 along with their respective Hamming weights.

TABLE 1. CANONIC REPRESENTATIONS OF STABLE FSR'S OF ORDER 3

$\mathbf{F}$	$W(\mathbf{F})$	$\mathbf{F}$	$W(\mathbf{F})$
(0, 0, 0, 0, 0, 0, 0, 0)	0	(0, 0, 0, 0, 1, 1, 0, 0)	2
(0, 0, 0, 1, 0, 0, 0, 0)	1	(0, 0, 0, 0, 1, 0, 1, 0)	2
(0, 0, 0, 0, 1, 0, 0, 0)	1	(0, 0, 0, 0, 0, 1, 1, 0)	2
(0, 0, 0, 0, 0, 1, 0, 0)	1	(0, 0, 1, 0, 1, 1, 0, 0)	3
(0, 0, 0, 0, 0, 0, 1, 0)	1	(0, 0, 1, 0, 0, 1, 1, 0)	3
(0, 0, 1, 0, 0, 1, 0, 0)	2	(0, 0, 0, 1, 1, 0, 1, 0)	3
(0, 0, 0, 1, 0, 0, 1, 0)	2	(0, 0, 0, 0, 1, 1, 1, 0)	3
(0, 0, 0, 1, 1, 0, 0, 0)	2	(0, 0, 1, 0, 1, 1, 1, 0)	4

An inspection of Table 1 reveals that the Hamming weights of the stable FSR's of order 3 are distributed binomially; i.e., the number of stable FSR's of order 3 with Hamming weight $W(\mathbf{F}) = w$ is given by $\binom{4}{w}$. The Hamming weight distribu-

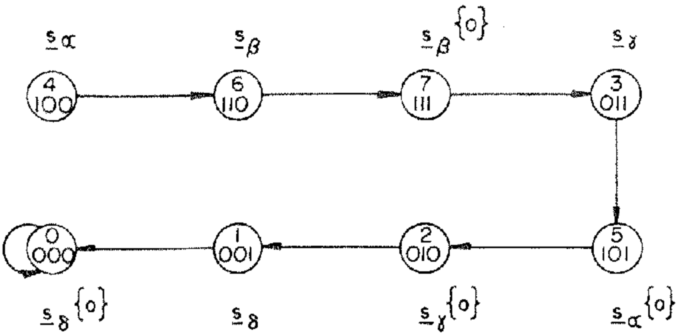

FIG. 2. State diagram of a stable maximum transient FSR of order 3

tion for the stable FSR's of orders 1 and 2 are clearly $\binom{0}{w}$ and $\binom{1}{w}$. Using a UNIVAC 1107 digital computer,[1] it was determined that the Hamming weights of the stable FSR's of order 4 are also distributed binomially according to $\binom{11}{w}$.

In this paper it is shown generally that the Hamming weights of the stable FSR's of order n are distributed binomially according to $\binom{2^n - n - 1}{w}$. A recursive algorithm is also given which generates the canonic representations of all stable feedback shift registers.

In order to establish the Hamming weight enumeration formula, the following preliminary algorithms and lemmas are necessary.

Associated FSR's.

Definition 6. Let $f_m(\mathbf{s})$ be the defining function of an nth order stable maximum transient FSR. Let A be an arbitrary set of states on the FSR. Then the *A determined FSR* is the FSR whose feedback function $\mathrm{f}(\mathbf{s})$ is given by the following construction:

$$f(\mathbf{s}_\alpha) = f_m(\mathbf{s}_\alpha), \qquad \mathbf{s}_\alpha \notin A,$$

$$f(\mathbf{s}_\alpha) = f_m(\mathbf{s}_\alpha) \oplus 1, \qquad \mathbf{s}_\alpha \in A.$$

On any particular stable maximum transient FSR, each pair of states $\mathbf{s}_\alpha$ and $\mathbf{s}_\alpha^{\{0\}}$ can be ordered as successors of the single starting state $\mathbf{0}^{\{n-1\}}$ such that $\mathbf{s}_\alpha = \theta^i\mathbf{0}^{\{n-1\}}$ and $\mathbf{s}_\alpha^{\{0\}} = \theta^j\mathbf{0}^{\{n-1\}}$, $0 \leq i < j \leq 2^n - 1$. Thus the states labeled $\mathbf{s}_\alpha$ and $\mathbf{s}_\alpha^{\{0\}}$ will be the ith and jth successors of the starting state. (See Figure 2.)

LEMMA 1. *Let* $\mathbf{s}_\alpha = \theta^i\mathbf{0}^{\{n-1\}}$ *and* $\mathbf{s}_\alpha^{\{0\}} = \theta^j\mathbf{0}^{\{n-1\}}$, $0 \leq i < j \leq 2^n - 1$, *be the i-th and j-th successors of the starting state* $\mathbf{0}^{\{n-1\}}$ *on a particular stable maximum transient FSR. Let* $\mathbf{s}_\beta = \theta^{i+1}\mathbf{0}^{\{n-1\}}$ *be the successor of* $\mathbf{s}_\alpha$ *and* $\mathbf{s}_\beta^{\{n-1\}} = \theta^{j+1}\mathbf{0}^{\{n-1\}}$ *be the successor of* $\mathbf{s}_\alpha^{\{0\}}$. *Let the set A consist of the single arbitrary state* $\mathbf{s}^*$.

1. *If* $\mathbf{s}^* = \mathbf{0}^{\{0\}}$ *or is some state* $\mathbf{s}_\alpha^{\{0\}}$ *then the resulting* $2^{n-1} + 1$ *possible distinct A determined FSR's are unstable.*

[1] All digital computer computation was performed on the UNIVAC 1107 at the University of Notre Dame Computing Center.

2. *If* $\mathbf{s}^* \neq \mathbf{0}$ *or is some state* $\mathbf{s}_\alpha$, *then the resulting* $2^{n-1} - 1$ *possible distinct* A *determined FSR's are stable.*

PROOF. *Case* 1. Let $A = \{\mathbf{0}^{\{0\}}\}$, by Property 3 $f_m(\mathbf{0}^{\{0\}}) = 0$. Thus $f(\mathbf{0}^{\{0\}}) = f_m(\mathbf{0}^{\{0\}}) \oplus 1 = 1$ on the A determined FSR. Hence $\theta\mathbf{0} = \mathbf{0}^{\{n-1\}}$ and the A determined FSR is unstable.

Case 2. Let $A = \{\mathbf{0}\}$. Then $\mathbf{0}$ is some state $\mathbf{s}_\alpha^{\{0\}}$ and $f_m(\mathbf{0}) = 0$. Thus $f(\mathbf{0}) = f_m(0) \oplus 1 = 1$ on the A determined FSR. Hence $\theta\mathbf{0} = \mathbf{0}^{\{n-1\}}$ and the A determined FSR is unstable.

Case 3. Let A consist of the single state $\mathbf{s}_\alpha^{\{0\}} = \theta\mathbf{0}^j\mathbf{0}^{\{n-1\}}$ for $0 \leq i < j \leq 2^n - 3$ where $\mathbf{s}_\alpha = \theta^i\mathbf{0}^{\{n-1\}}$. On the stable maximum transient FSR of order n, disjoint sequences Q_1 and Q_2 exist where

$$Q_1 = \{\mathbf{0}^{\{n-1\}}, \theta\mathbf{0}^{\{n-1\}}, \cdots, \theta^{i-1}\mathbf{0}^{\{n-1\}}, \mathbf{s}_\alpha, \mathbf{s}_\beta, \cdots, \theta^{j-1}\mathbf{0}^{\{n-1\}}, \mathbf{s}_\alpha^{\{0\}}\}$$

and

$$Q_2 = \{\mathbf{s}_\beta^{\{n-1\}}, \theta\mathbf{s}_\beta^{\{n-1\}}, \cdots, \theta^{2^n-j-3}\mathbf{s}_\beta^{\{n-1\}}, \mathbf{0}^{\{0\}}, \mathbf{0}\}.$$

Both of these sequences will also exist on the A determined FSR. Since $\theta\mathbf{s}_\alpha^{\{0\}} = \mathbf{s}_\beta$ on the A determined FSR, the sequence Q_3 of distinct states

$$\{\mathbf{s}_\beta, \theta\mathbf{s}_\beta, \cdots, \theta^{j-i-2}\mathbf{s}_\beta, \mathbf{s}_\alpha^{\{0\}}\}$$

will form a closed cycle of period $T = j - i$ if $T > 1$ or if $T = 1$, the sequence Q^3 will degenerate to the equilibrium state $\mathbf{1}$. There are $2^{n-1} - 1$ distinct states $\mathbf{s}_\alpha^{\{0\}}$ which satisfy the conditions of this case all of which yield unstable A determined FSR's.

Case 4. Let A consist of the single state $\mathbf{s}_\alpha = \theta^i\mathbf{0}^{\{n-1\}}0 \leq i < j \leq 2^n - 3$ where $\mathbf{s}_\alpha^{\{0\}} = \theta^j\mathbf{0}^{\{n-1\}}$. (Note $\mathbf{s}_\alpha$ cannot be equal to $\mathbf{0}^{\{0\}}$.) On the stable maximum transient FSR of order n, disjoint sequence Q_4 and Q_5 exist where

$$Q_4 = \{\mathbf{0}^{\{n-1\}}, \theta\mathbf{0}^{\{n-1\}}, \cdots, \theta^{i-1}\mathbf{0}^{\{n-1\}}, \mathbf{s}_\alpha\}$$

and

$$Q_5 = \{\mathbf{s}_\beta, \theta\mathbf{s}_\beta, \cdots, \theta^{j-i-2}\mathbf{s}_\beta, \mathbf{s}_\alpha^{\{0\}}, \mathbf{s}_\beta^{\{n-1\}}, \cdots, \theta^{2^n-i-3}\mathbf{s}_\beta^{\{n-1\}}, \mathbf{0}^{\{0\}}, \mathbf{0}\}.$$

Both of these sequences will exist on the A determined FSR. Since $\theta\mathbf{s}_\alpha = \mathbf{s}_\beta^{\{n-1\}}$ on the A determined FSR, the sequence

$$Q_6 = \{\mathbf{0}^{\{n-1\}}, \theta\mathbf{0}^{\{n-1\}}, \cdots, \mathbf{s}_\alpha, \mathbf{s}_\beta^{\{n-1\}}, \cdots, \theta^{2^n-i-3}\mathbf{s}_\beta, \mathbf{0}^{\{0\}}, \mathbf{0}\}$$

will also exist. Therefore, there exists an integer N such that $\theta^N\mathbf{s} = \mathbf{0}$ for all states on the A determined FSR and hence it is stable. There are $2^{n-1} - 1$ distinct states $\mathbf{s}_\alpha$ which satisfy the conditions of this case, all of which yield stable A determined FSR's.

Part 1 of this lemma follows from Cases 1, 2, and 3. Part 2 follows directly from Case 4. Q.E.D.

Potentially Stable and Unstable States

The set of $2^{n-1} - 1$ distinct states on a particular stable maximum transient FSR which yield stable A determined FSR's in Lemma 1 will be called the *set of potentially* *stable states* for that particular stable maximum transient FSR, and will be denoted by Z.

The set of $2^{n-1} + 1$ distinct states on a particular stable maximum transient FSR which yield unstable A determined FSR's in Lemma 1 will be called the *set of potentially unstable states* for that particular stable maximum transient FSR, and will be denoted by U.

For every FSR of order n, a deBruijn [7] or Good [8] diagram can be constructed. A *deBruijn diagram* differs from the ordinary state diagram in that there are two branches leaving each state (node), one for each of the two possible values of the feedback function $f(\mathbf{s})$ and two branches terminating on each node, since each state is a possible successor of two distinct states. The 2^n nodes may be numbered with the binary n-tuple corresponding to the 2^n states or with the decimal integers corresponding to these states. The two branches leaving node i terminate on nodes j and k respectively, if the first $n-1$ binary digits of the n-tuple denoting node i correspond to the last $n - 1$ binary digits in the n-tuples denoting nodes j and k.[2]

The directed branches are numbered with the binary $(n + 1)$-tuple whose first binary digit is equal to the first binary digit in the binary n-tuple at the head of the directed branch and whose last n binary digits correspond to the binary n-tuple at the tail of the directed branch.

On a deBruijn diagram of order n, if one stars the 2^n branches, one leaving each node, which *are not* on the state diagram of the stable FSR, leaving the 2^n branches, one leaving each node, which *are* on the state diagram of the stable FSR unstarred, the resulting diagram will be called an *associated deBruijn diagram*. The following algorithm generates a stable maximum transient FSR of order $n + 1$ by making a *complete circuit* of the associated deBruijn diagram of a stable FSR of order n. The validity of the algorithm has been established in previous papers [1, 7, 9].

Algorithm 1

```
1. Set $i = 1$.
2. Let $\alpha$ be node 0.
3. If the starred branch leaving node $\alpha$ has not been used, leave node $\alpha$ by the starred branch.
   Otherwise leave by the unstarred branch.
4. Set $\mathbf{s}_i$ equal to the $(n + 1)$-tuple corresponding to the branch traversed.
5. Let $\alpha$ be the node reached in step 3. If both branches leaving node $\alpha$ have been used, go
   to step 6. Otherwise set $i = i + 1$ and go to step 3.
6. Construct a stable maximum transient FSR of order $n + 1$ such that $\theta\mathbf{s}_i = \mathbf{s}_{i+1}$, $i = 1,$
   $\ldots, 2^{n+1} - 1$ and $\theta\mathbf{s}_{2^{n+1}} = \mathbf{s}_{2^{n+1}}$.
```

Figures 3, 4, and 6 (see pages 536, 537) show the state diagram of a stable third order FSR, the associated deBruijn diagram for this FSR, and the resulting stable maximum transient FSR of order 4, respectively.

It is also possible to determine which states in the sets U and Z are unit feedback states and which states are zero feedback states from the associated deBruijn diagram. Consider the following algorithm for accomplishing this objective.

[2] Using decimal notation, the two branches leaving node I terminate on nodes J and K if $J = \left\lfloor \frac{I}{2} \right\rfloor$ and $K = \left\lfloor \frac{I}{2} \right\rfloor + 2^{n-1}$. The directed branch connecting node I to node J is denoted by I if $I > J$ and by $I + 2^n$ if $I < J$.

Algorithm 2

1. Construct the associated deBruijn diagram of order n corresponding to a given stable FSR of order n.
2. For a given stable FSR, place a check mark next to each node on the associated deBruijn diagram which corresponds to a unit feedback state.
3. Construct a node entry table for the associated deBruijn diagram of the following form:

Node	0	1	2	•••	2^n-2	2^n-1
1st time entered by branch						
2nd time entered by branch						

   a. Place a check mark next to each node which corresponds to a unit feedback state.
   b. Using Algorithm 1, make a complete circuit of the associated deBruijn diagram noting which branches were used to enter each node the first time and which branches were used to enter each node the second time.
4. Determine from the node entry table the states in the sets U and Z as follows:
   a. The states on the stable maximum transient FSR of order $n+1$ which correspond to the branches which enter each checked node (unchecked node) for the second time on the associated deBruijn diagram of order n are elements of the set U of potentially unstable states and are unit feedback (zero feedback) states.
   b. The state on the stable maximum transient FSR of order $n+1$ which corresponds to the branch which enters node 0 for the first time on the associated deBruijn diagram of order n is a zero feedback state and an element of the set U of potential unstable states.
   c. The states on the stable maximum transient FSR of order $n+1$ which correspond to the branches which enter each check node (unchecked node) except node 0 for the first time on the associated deBruijn diagram, are the elements of the set Z of potentially stable states and are zero feedback (unit feedback) states.

Proof. It is clear that changing the successor of a state on a stable maximum transient FSR of order $n + 1$ corresponds to changing the successor of a branch on a complete circuit of its associated deBruijn diagram of order n. In this sense, Algorithm 2 is just a restatement of Lemma 1.

Example 1. Apply Algorithm 2 to the stable FSR of order 3 defined by $f(\mathbf{s}) = s_2(s_1 \oplus 1)$. The state diagram for the stable FSR is shown in Figure 3 and the associated deBruijn diagram for this FSR is shown in Figure 4.

Since states 4 and 5 are unit feedback states on the stable third order FSR, nodes 4 and 5 are check marked on the associated deBruijn diagram in Figure 4. The node entry table for the associated deBruijn diagram is shown in Figure 5.

Applying step 4 of Algorithm 2, the set U of potentially unstable states consists of the states $\{0, 1, 3, 5, 6, 9, 11, 13, 15\}$. The set Z of potentially stable states consists of the states $\{2, 4, 7, 8, 10, 12, 14\}$. States 9 and 11 are the only unit feedback states in the set U. States 8 and 10 are the only zero feedback states in Z.

The associated stable maximum transient FSR of order 4 for the stable FSR of order 3 defined by $f(\mathbf{s}) = s_2(s_1 \oplus 1)$ is shown in Figure 6.

From Lemma 1, it is clear that changing the successor of a single state $\mathbf{s}_\alpha$ on a stable maximum transient FSR of order n will yield a stable FSR of order n, if and

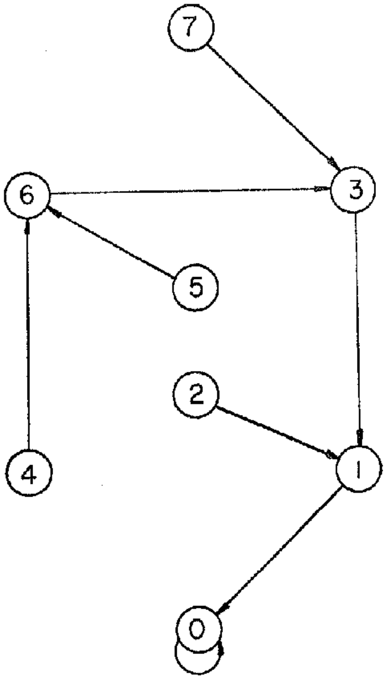

Fig. 3. State diagram for the FSR of order 3 with $f(\mathbf{s}) = s_2(s_1 \oplus 1)$

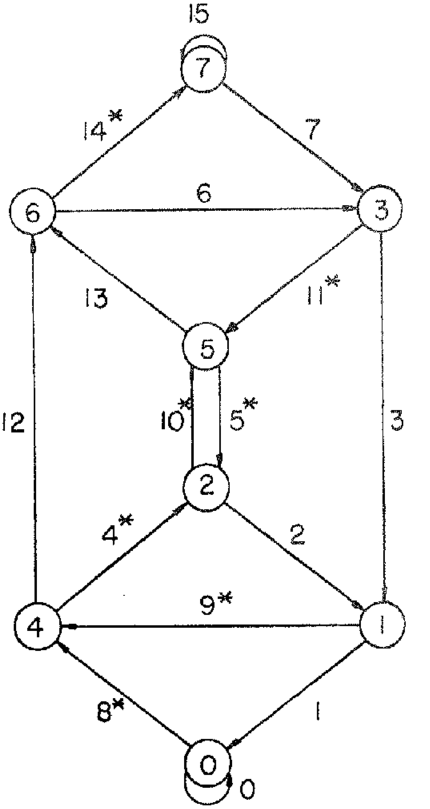

Fig. 4. Associated deBruijn diagram o order 3 for the FSR with $f(\mathbf{s}) = s_2(s_1 \oplus 1$

only if $\mathbf{s}_\alpha$ is an element of the set Z of potentially stable states. Let us now consider changing the successors of an arbitrary number of states from Z.

Definition 7.[3] Let $f_m(\mathbf{s})$ be the defining function of an nth order stable maximum transient FSR. Let Z^* be some subset of the set Z of potentially stable states for this stable maximum transient FSR. Then the Z^* *determined FSR* is the FSR whose feedback function $f(\mathbf{s})$ is given by the following construction:

$$f(\mathbf{s}_\alpha) = f_m(\mathbf{s}_\alpha), \qquad \mathbf{s}_\alpha \notin Z^*,$$
$$f(\mathbf{s}) = f_m(\mathbf{s}) \oplus 1, \qquad \mathbf{s}_\alpha \in Z^*.$$

Lemma 2. *Let N be the smallest integer such that $\theta^N \mathbf{s}^* = \mathbf{0}$ where $\mathbf{s}^*$ is some state on a stable maximum transient FSR of order n. On the Z^* determined FSR, if $\mathbf{s}^* \in Z^*$, then there exists an integer $K < N$ such that $\theta^K \mathbf{s}^* = \mathbf{0}$.*

Proof. Let $\mathbf{s}_i = \theta^i \mathbf{0}^{(n-1)}$ denote the ith successor of $\mathbf{0}^{(n-1)}$ on a stable maximum transient FSR of order n, $0 \le i \le 2^n - 1$; then $N_i = 2^n - i - 1$ is the smallest integer such that $\theta^{N_i} \mathbf{s}_i = \mathbf{0}$, $0 \le i \le 2^n - 1$.

[3] It should be noted here that Definition 7 is just a restatement of Definition 6 with the set A of Definition 6 restricted to a subset of the set Z of potentially stable states. However, since this restriction applies in the remainder of this paper, it is convenient to designate this restriction with a separate definition.

					✓	✓		
Node	0	1	2	3	4	5	6	7
1st time entered by branch	1	2	4	7	8	10	12	14
2nd time entered by branch	0	3	5	6	9	11	13	15

FIG. 5. Node entry table for the associated deBruijn diagram of Figure 4

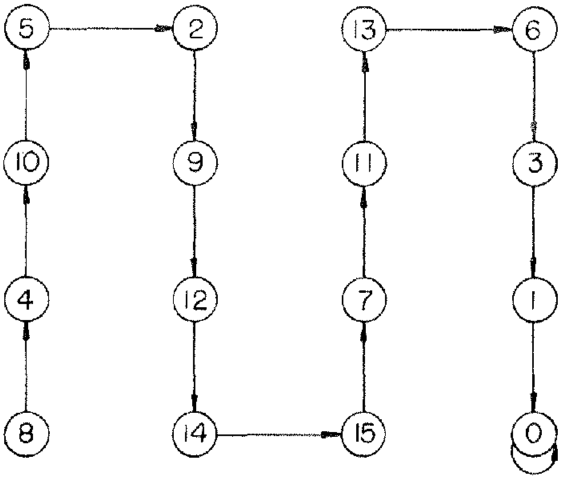

FIG. 6. State diagram of the stable maximum transient FSR of order 4 associated with the third order stable FSR with $f(\mathbf{s}) = s_2(s_1 \oplus 1)$

If the set Z^* is the empty set, there is nothing to prove. If the set Z^* contains only a single state, then the lemma follows directly from Lemma 1. Let Z^* be an arbitrary set of $m - 1$ states from Z, $2 \leq m \leq 2^{n-1} - 2$, and assume that the lemma is true for this case. The lemma is now shown to be true for m states in Z^*.

Let $\mathbf{s}_\alpha = \theta^\alpha \mathbf{0}^{(n-1)}$ be a state in Z which is not in Z^*. Let $\mathbf{s}_\beta$ be the successor of $\mathbf{s}_\alpha$ on the stable maximum transient FSR. $N_\alpha = 2^n - \alpha - 1$ is the smallest integer such that $\mathbf{s}_\alpha^{N_\alpha} = \mathbf{0}$ on the stable maximum transient FSR. Therefore the sequence $\{\mathbf{s}_\alpha, \mathbf{s}_\beta, \cdots, \mathbf{s}_\alpha^{(0)}, \mathbf{s}_\beta^{(n-1)}, \cdots, \theta^{2^n-\alpha-2}\mathbf{s}_\alpha, \mathbf{0}\}$ will exist on the stable maximum transient FSR. Changing the successor of $\mathbf{s}_\alpha$ from $\mathbf{s}_\beta$ to $\mathbf{s}_\beta^{(n-1)}$ on the Z^* determined FSR clearly eliminates the states $\mathbf{s}_\beta, \cdots, \mathbf{s}_\alpha^{(0)}$ from this sequence. To assume otherwise contradicts the assumption that $\mathbf{s}_\alpha$ is a state in Z. There are two cases to be considered.

Case 1. No state in the sequence $\{\mathbf{s}_\beta^{(n-1)}, \theta\mathbf{s}_\beta^{(n-1)}, \cdots, \mathbf{0}\}$ is an element of Z^*. Clearly for this case there exists an integer $K_\alpha < N_\alpha$ such that $\theta^{K_\alpha}\mathbf{s}_\alpha = \mathbf{0}$ on the Z^* determined FSR.

Case 2. At least one state in the sequence $\{\mathbf{s}_\beta^{(n-1)}, \theta\mathbf{s}_\beta^{(n-1)}, \cdots, \mathbf{0}\}$ is an element of Z. Let k be the smallest integer such that $\mathbf{s}_\gamma = \theta^k\mathbf{s}_\beta^{(n-1)}$ is such a state. On the stable maximum transient FSR $\theta^{N_\gamma}\mathbf{s}_\gamma = \mathbf{0}$ and $\theta^{(N_\alpha - N_\gamma)}\mathbf{s}_\alpha = s_\gamma$. By the induction hypothesis there exists an integer $K_\gamma < N_\alpha$ such that $\theta^\gamma\mathbf{s}_\gamma = \mathbf{0}$ on the associated FSR. The sequence $\{\mathbf{s}_\alpha, \mathbf{s}_\beta^{(n-1)}, \theta\mathbf{s}_\beta^{(n-1)}, \cdots, \theta^{k-1}\mathbf{s}_\beta^{(n-1)}, \mathbf{s}_\gamma\}$ exists on the Z^* determined FSR since $\mathbf{s}_\gamma$ is the first state after $\mathbf{s}_\beta^{\{n-1\}}$ which is an element of Z^*. Thus there exist integers $N^* < N_\alpha - N_\gamma$ and $K_\alpha = N^* + K_\gamma$ such that $\theta^{N^*}\mathbf{s}_\alpha = \mathbf{s}_\gamma$ and $\theta^{K_\alpha}\mathbf{s}_\alpha = \mathbf{0}$ on the Z^* determined FSR. Since $K_\gamma < N_\gamma$, $K_\alpha < N_\alpha - N_\gamma + N_\gamma < N_\alpha$ and thus the lemma is true for m states in Z^*, $0 \le m \le 2^{n-1} - 1$, and since m was arbitrary it is true in general. Q.E.D.

Lemma 3. *All Z^* determined FSR's are stable.*

Proof. Follows directly from Lemma 2.

Theorem 1. *There are exactly $2^{2^{n-1}-1}$ distinct Z^* determined stable FSR's associated with each stable maximum transient FSR of order n.*

Proof. From Lemma 3 all Z^* determined FSR's are stable. From Lemma 1 there are $2^{n-1} - 1$ distinct states in Z. Hence there are $\binom{2^{n-1} - 1}{j}$ distinct ways of having j states from Z in Z^*. Summing over j yields the required number.

$$\sum_{j=0}^{2^{n-1}-1} \binom{2^{n-1}-1}{j} = 2^{2^{n-1}-1}.$$

Q.E.D.

Lemma 4. *Given any two distinct stable maximum transient FSR's of order n; there is at least one state $\mathbf{s}_\alpha$ common to the sets U of potential unstable states such that $f(\mathbf{s}_\alpha) = 0$ on one and $f(\mathbf{s}_\alpha) = 1$ on the other.*

Proof. Given any two distinct stable FSR's of order $n - 1$, $n > 2$ there will be at least one state $\mathbf{s}_\alpha$ which is a unit feedback state on one, $f(\mathbf{s}_\alpha) = 1$, and a zero feedback state on the other, $f(\mathbf{s}_\alpha) = 0$. To assume otherwise would imply that the two canonic representations are the same, contradicting the assumption that the FSR's were distinct.

Without loss of generality, if there is more than one such state, let $\mathbf{s}_\alpha$ be the first such state encountered on a complete circuit where the value of the feedback functions differ; if branch $\mathbf{b}_k$ is the first branch to enter this node on one associated deBruijn diagram, it will also be the first branch to enter the corresponding node on the other associated deBruijn diagram. By Algorithm 2, the state on the stable maximum transient FSR's associated with branch $\mathbf{b}_k^{\{0\}}$ will be common to both sets U of potentially unstable states, and this state will be a zero feedback state on one and a unit feedback state on the other. Q.E.D.

Lemma 5. *Given any two distinct stable maximum transient FSR's of order n, the sets of $2^{2^{n-1}-1}$ distinct Z^* determined stable FSR's corresponding to each stable maximum transient FSR of order n are disjoint.*

Proof. Follows directly from Lemma 4.

Lemma 6. *Given a stable maximum transient FSR of order n which has j unit feedback states in its set U of potentially unstable states; $\binom{2^{n-1} - 1}{k}$ distinct Z^* determined stable FSR's with Hamming weight $W(\mathbf{F}) = j + k$, $0 \le k \le 2^{n-1} - 1$ can be obtained.*

Proof. Since the successor of the states in U are not changed, the Hamming weight of the Z^* determined FSR's will at least be j. Without loss of generality, let there be i unit feedback states in the set Z. Let Z_1 denote the subset of Z containing these i unit feedback states and let Z_2 denote the subset of Z containing the

$2^{n-1} - 1 - i$ zero feedback states. A stable FSR of order n with Hamming weight $W(\mathbf{F}) = j + k$ can be obtained by deleting k_1 states from Z_1, $0 \le k_1 \le i$ and adding k_2 states from Z_2 to Z, $0 \le k_2 \le 2^{n-1} - 1 - i$ where $k_1 + k_2 = k$, $0 \le k \le 2^{n-1} - 1$. The total number of ways of obtaining a stable FSR with Hamming weight $W(\mathbf{F}) = j + k$ is given by

$$\sum_{k_1=0}^{k} \binom{i}{k_1} \binom{2^{n-1} - 1 - i}{k - k_1} = \binom{2^{n-1} - 1}{k}.$$

Q.E.D.

With the aid of the above lemmas it is now possible to prove the result stated at the beginning of this paper.

Enumeration of Stable FSR's by Hamming Weight

THEOREM 2. *There are exactly* $\binom{2^n - n - 1}{w}$ *distinct stable FSR's of order* n *which have Hamming weight* $W(\mathbf{F}) = w$, $0 \le w \le 2^n - n - 1$.

PROOF. The theorem was shown to be true for $n = 1$, 2, and 3 at the beginning of this paper. Assume the theorem is true for $n = m$. We now show it to be true for $n = m + 1$.

It follows directly from Algorithm 2 that corresponding to each stable FSR of order m with Hamming weight $W(\mathbf{F}) = j$, $0 \le j \le 2^m - m - 1$, there is a stable maximum transient FSR of order $m + 1$ which has j unit feedback states in its set U of potentially unstable states.

Lemma 6 states that $\binom{2^m - 1}{k}$ distinct Z^* determined stable FSR's with Hamming weight $W(\mathbf{F}) = j + k$ can be associated with each stable maximum transient FSR.

Lemma 5 states that the sets of 2^{2^m-1} distinct Z^* determined stable FSR's obtained from different stable maximum transient FSR's are disjoint. The number of stable FSR's of order $m + 1$ with $W(\mathbf{F}) = 0$ is thus given by

$$\binom{2^m - m - 1}{0} \cdot \binom{2^m - 1}{0} = 1.$$

The number of stable FSR's of order $m + 1$ with $W(\mathbf{F}) = 1$ is given by

$$\binom{2^m - m - 1}{0} \binom{2^m - 1}{1} + \binom{2^m - m - 1}{1} \binom{2^m - 1}{0} = 2^{m+1} - m - 2,$$

and in general the number of FSR's of order $m + 1$ with $W(\mathbf{F}) = w$ is given by

$$\sum_{j=0}^{w} \binom{2^m - m - 1}{j} \cdot \binom{2^m - 1}{w - j} = \binom{2^{m+1} - m - 2}{w}.$$

Thus the theorem is true for $m + 1$ and since m is arbitrary, it is true in general. Q.E.D.

Algorithm for Generating All Stable FSR's of Order n

Having established the Hamming weight enumeration formula, it is now possible to give a set of rules for generating all stable FSR's of any order. Consider the following recursive algorithm.

Algorithm 3. Rules for generating all stable FSR's of order n, $n > 1$ are as follows:

1. Start with the single FSR of order 1 with $F(S) = (0, 0)$.
2. Set $k = 1$.
3. Apply Algorithms 1 and 2 to each stable FSR of order k obtaining the 2^{2^k-k-1} distinct stable maximum transient FSR's of order $k+1$ along with their respective sets Z and U of potentially stable and unstable states.
4. For each stable maximum transient FSR of order $k+1$ find all the possible Z^* determined stable FSR's, thus obtaining the $2^{2^{k+1}-k-2}$ distinct stable FSR's of order $k+1$.
5. If $k = n-1$, stop. Otherwise increase k by one and go to step 3.

Enumeration Formulas for Stable FSR's by Starting and Branch States

Having established the enumeration formula for the stable FSR's by Hamming weight, we do not establish an enumeration formula for the stable FSR's by starting states and by branch states.

LEMMA 7. *The number of starting states on a Z^* determined stable FSR is equal to the cardinality of the set Z^* plus one.*

PROOF. Follows from property 1 and the fact that the successor of each state in Z^* on the stable maximum transient FSR is a starting state on the Z^* determined FSR.

COROLLARY 1. *The number of branch states on a Z^* determined stable FSR of order n is equal to the cardinality of the set Z^* plus* 1.

PROOF. Follows immediately from Lemma 7 and Property 1. Q.E.D.

THEOREM 3. *There are exactly $2^{2^{n-1}-n}\binom{2^{n-1}-1}{j}$ stable FSR's of order n which have $j+1$ starting states and $j+1$ branch states.*

PROOF. There are $2^{2^{n-1}-n}$ distinct stable maximum transient FSR's of order n [1]. For each stable maximum transient FSR of order n, there are $\binom{2^{n-1}-1}{j}$ different ways of having j elements in Z^*. Thus it follows from Lemma 7 and Corollary 1 that the number of stable FSR's of order n with $j+1$ starting states and $j+1$ branch states is equal to

$$2^{2^{n-1}-n}\binom{2^{n-1}-1}{j}.$$

Q.E.D.

COROLLARY 2. *There are exactly $\binom{2^{n-1}-1}{k}\cdot\binom{2^{n-1}-n}{w-k}$ stable FSR's of order n which have Hamming weight $W(\mathbf{F}) = w$, $0 \le w \le 2^n - n - 1$ and $k+1$ starting states and $k+1$ branch states where $0 \le k \le 2^{n-1}-1$, $k \le w$.*

PROOF. From Lemma 6, $\binom{2^{n-1}-1}{k}$ distinct stable FSR's with Hamming weight $W(\mathbf{F}) = j + k$ can be associated with each stable maximum transient FSR of order n which has j unit feedback states in its set U of potentially unstable states. From Algorithm 2 and Theorem 1, it follows that there are $\binom{2^{n-1}-n}{j}$ stable maximum transient FSR's with j unit feedback states in their sets U of potentially unstable states. Thus there are $\binom{2^{n-1} - n}{w - k} \cdot \binom{2^{n-1} - 1}{k}$ distinct stable FSR's of order n with Hamming weight $W(\mathbf{F}) = w$ and $k + 1$ starting states and $k + 1$ branch states. Q.E.D.

Table 2 gives the breakdown of the stable FSR's of order 3 with Hamming weight $W(\mathbf{F}) = w$ and $j + 1$ starting states and $j + 1$ branch states.

It should be noted that summing across the rows of Table 2 yields the number of stable FSR's with Hamming w, and summing down the columns of Table 2 yields the number of stable FSR's with $j + 1$ starting states and $j + 1$ branch states.

TABLE 2. Number of Stable FSR's of Order 3 With Hamming Weight $W(F) = w$ and $j+1$ Starting States and $j+1$ Branch States

w	$J = 0$	1	2	3	Row Sum
0	1	0	0	0	1
1	1	3	0	0	4
2	0	3	3	0	6
3	0	0	3	1	4
4	0	0	0	1	1
Column sum. . .	2	6	6	2	

Results and Conclusions

In this paper it is shown that there are $\binom{2^n - n - 1}{w}$ distinct stable FSR's of order n which have Hamming weight $W(\mathbf{F}) = w$. Using this result, an algorithm for obtaining all stable FSR's of order n is established. It is also shown that the number of stable FSR's of order n with $j + 1$ starting states and $j + 1$ branch states is equal to $2^{2^{n-1}-n}\binom{2^{n-1} - 1}{j}$. Finally, it is shown that the number of stable FSR's of order n which have Hamming weight $W(\mathbf{F}) = w$ and also have $j + 1$ starting states and $j + 1$ branch states is equal to $\binom{2^{n-1} - n}{w - j}\binom{2^{n-1} - 1}{j}$.

ACKNOWLEDGMENT. The author wishes to acknowledge the helpful comments and suggestions of Professor J. L. Massey of the University of Notre Dame in the preparation of this paper.

REFERENCES

1. Mowle, F. J. Relations between P_n cycles and stable feedback shift registers. *IEEE Trans. EC-15*, 3 (June 1966), 375–378.
2. Gill, A. *Introduction to the Theory of Finite State Machines.* McGraw-Hill, New York, 1962.
3. Massey, J., and Liu, R. Application of Lyapunov's direct method to the error-propagation effect in convolutional codes. *IEEE Trans. IT-10*, 3 (July 1964), 248–250.
4. —— and ——. Monotone feedback shift registers. Proc. Second Annual Allerton Conf. on Circuit and System Theory, U. of Illinois, Urbana, Ill., Sept. 1964, pp. 860–874.
5. Magleby, K. B. The Synthesis of Nonlinear Feedback Shift Registers. Stanford Electronics Laboratory, Rep. 6207-1, Stanford, Cal., Oct. 1963.

6. Mowle, F. J. Enumeration and Classification of Stable Feedback Shift Registers. Ph.D. dissertation submitted to Dep. of Elec. Eng., U. of Notre Dame, Notre Dame, Ind., Jan. 1966; also U. of Notre Dame Elec. Eng. Dep. Tech. Rep. No. 661, Notre Dame, Ind., Jan. 12, 1966.

7. deBruijn, N. G. A combinatorial problem. *Proc. Koninkl. Ned. Akad. Wetenschap. 49*, Pt. 2 (1946), 758–764.

8. Good, I. G. Normal recurring decimals. *J. London Math. Soc. 21*, Pt. 3 (1946), 167–169.

9. Golomb, S. W. *Shift Register Sequences.* Holden Day, San Francisco, 1965.

received June, 1966; revised february, 1967