# On a Homomorphism of the de Bruijn Graph and Its Applications to the Design of Feedback Shift Registers

ABRAHAM LEMPEL, MEMBER, IEEE

**Abstract—A homomorphism of the de Bruijn graph that maps a graph of order $n$ onto one of order $n-1$ and its applications to the design of nonsingular feedback shift registers are discussed. The properties preserved under this mapping suggest a new design technique whose main advantage is due to the fact that the problem of designing a desired $n$-stage shift register may be reduced to a problem of order $n-1$ or less. Among the results obtained is a recursive formula for a feedback function that generates a cycle of maximum length.**

**Index Terms—de Bruijn graphs, design of binary nonsingular feedback shift registers, homomorphism.**

## I. Introduction

THIS paper discusses a homomorphism of the de Bruijn graph and its applications to the design of nonsingular, binary feedback shift registers (FSRs). The general form of a binary $n$-stage FSR is shown in Fig. 1. It consists of $n$ storage elements (stages) and a feedback logic producing a Boolean function $f(x_1, \cdots, x_n)$, where $x_i \in B = \{0, 1\}$ indicates the binary content of stage $i$. When a shift pulse is applied, the state $x=(x_1, \cdots, x_n)$ of the FSR is succeeded by the state $y=(y_1, \cdots, y_n)$, where

$$y_1 = x_{i+1}, i = 1, \cdots, n-1, \quad \text{and} \quad y_n = f(x). \qquad (1)$$

The feedback function $f$ induces a (next-state) mapping $F: B^n \to B^n$ determined by (1). An FSR and its feedback function $f$ are said to be *nonsingular* if the induced mapping $F$ is one-to-one, i.e., if $xF = yF$ implies $x = y$. Such a mapping $F$ is illustrated in Fig. 2, which shows the *state graph* representation of the mapping induced by $f(x_1, x_2, x_3) = x_1 \oplus x_2 \oplus x_3 \oplus 1$, where $\oplus$ indicates addition modulo 2. Evidently, an FSR is nonsingular if its state graph consists of branchless cycles.

The superposition of the state graphs for all possible $n$-stage FSRs is often referred to as the de Bruijn graph of order $n$, because of de Bruijn's early paper [1].

The problem of designing nonsingular FSRs with specified cycle lengths has received considerable attention in the literature [2]–[8] and most of the known theory is now available in the form of a book [8]. One of the well-known results is the existence of an $n$-stage FSR with a cycle of length $k$, for any $n \geq 1$ and any $1 \leq k \leq 2^n$. This result has recently been generalized [9] also for the nonbinary case. Of special interest is the problem of finding simple methods of designing maximum length ($k = 2^n$) cycles. Although very little is known about feedback functions which generate such cycles, fairly simple methods of constructing the corresponding binary sequences are available [8], [10]–[12].

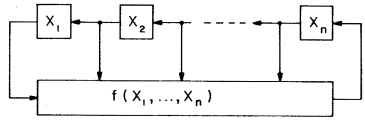


Fig. 1. General form of a binary, $n$-stage feedback shift register.

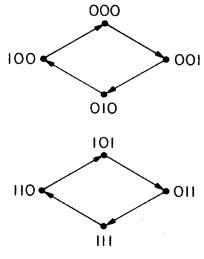


Fig. 2. State graph of the shift register with feedback function $f(x_1, x_2, x_3) = x_1 \oplus x_2 \oplus x_3 \oplus 1$.

This paper proposes a new approach to the design of nonsingular FSRs based on the results derived in Section III. This section, after some basic concepts and theorems are introduced in Section II, is concerned with a homomorphism of the de Bruijn graph that maps a graph of order $n$ onto one of order $n-1$. The properties preserved under this mapping give rise to a variety of applications, a few of which are discussed in Section IV. The main advantage of the proposed approach is due to the fact that, in many cases, the problem of designing a desired $n$-stage FSR may be reduced to a problem of order $n-1$, or less.

Among the results obtained in Section IV is a recursive formula for a feedback function which generates a maximum length cycle. To the best knowledge of the author, no such formula has yet been published. Some further results deal with cycles whose length is a power of 2, and an explicit formula for the function that generates the maximum possible number of equal length cycles for any given $n$ is presented. The same formula has also been derived earlier [13] by an entirely different approach.

Manuscript received May 8, 1969; revised May 16, 1970. This work was supported in part by the Army Research Office (Durham) under Contract DA-AROD-D-31-124G930.

The author was with the University of Southern California, Los Angeles, Calif. He is now with the Sperry Rand Research Center, Sudbury, Mass., on leave of absence from the Technion—Israel Institute of Technology, Haifa, Israel.

## II. Basic Concepts and Theorems

Consider the set of binary $n$-tuples $B^n$, formed by the $n$th Cartesian power of $B=\{0, 1\}$. In $B^n$ we define a relation $\rightarrow$ called the shift relation on $B^n$ by

$$x \rightarrow y \qquad \text{iff } (x_2, \cdots, x_n) = (y_1, \cdots, y_{n-1}). \tag{2}$$

The expression $x \rightarrow y$ should be read: "$x$ shifts into $y$," or "$y$ is a successor of $x$." For a given $x \in B^n$, there are exactly two successors of $x$, namely, $(x_2, x_3, \cdots, x_n, 0)$ and $(x_2, x_3, \cdots, x_n, 1)$. Similarly, there are exactly two predecessors of $x$ in $B^n$: $(0, x_1, \cdots, x_{n-1})$ and $(1, x_1, \cdots, x_{n-1})$.

The $n$th order de Bruijn graph $G_n$ is a directed graph with $2^n$ vertices, labeled by the elements of $B^n$. The vertices $x$ and $y$ of $G_n$, $x, y \in B^n$, are joined by an arc $\langle x, y\rangle$, directed from $x$ to $y$, iff $x \rightarrow y$. de Bruijn graphs of order 1, 2, 3, and 4 are shown in Fig. 3.

Now let $x=(x_1, x_2, \cdots, x_n) \in B^n$. We define $\hat{x}$, the *conjugate* of $x$, and $\bar{x}$, the *dual* of $x$, by

$$\hat{x} = (\bar{x}_1, x_2, \cdots, x_n)$$

and

$$\bar{x} = (\bar{x}_1, \bar{x}_2, \cdots, \bar{x}_n)$$

where $\bar{x}_i$ denotes the Boolean complement of $x_i$.

Obviously,

$$\hat{\bar{x}} = \bar{\hat{x}} \tag{3}$$

and

$$x \rightarrow y \qquad \text{iff } \hat{x} \rightarrow y. \tag{4}$$

It has been observed elsewhere [5], that the one-to-one correspondence $x \leftrightarrow \bar{x}$ is the only nontrivial automorphism of the de Bruijn graph, that is,

$$x \rightarrow y \qquad \text{iff } \bar{x} \rightarrow \bar{y}. \tag{5}$$

A *cycle* of length $k$ ($k$-cycle) in $G_n$ is a closed sequence (ring sequence) of $k$ distinct vertices $[x^{(1)}, x^{(2)}, \cdots, x^{(k)}]$ such that $x^{(k)} \rightarrow x^{(1)}$ and $x^{(i)} \rightarrow x^{(i+1)}$, $i=1, \cdots, k-1$. A convenient method of representing such a $k$-cycle is by means of a ring sequence of $k$ binary digits $[c_1, c_2, \cdots, c_k]$, where $c_i = x_1^{(i)}$ is the first component of the $n$-tuple $x^{(i)}$, $i=1, \cdots, k$. By the shift relation between consecutive vertices in a cycle, it is clear that vertex $x^{(i)}$ is represented in the binary ring sequence by the $n$ consecutive digits that begin with $c_i$. For instance, the eight-cycle [(000), (001), (010), (101), (011), (111), (110), (100)] in $G_3$, which is a maximum length cycle for a three-stage FSR, may simply be represented by the ring sequence [00010111].

Let $C=[c_1, c_2, \cdots, c_k]$ be a $k$-cycle in $G_n$ and let $x^{(i)}$, $i=1, \cdots, k$, be the vertices of $C$. It follows from (5) that $\bar{C}=[\bar{c}_1, \bar{c}_2, \cdots, \bar{c}_k]$ is also a $k$-cycle in $G_n$, with vertices $\bar{x}^{(i)}$, $i=1, \cdots, k$. The cycles $C$ and $\bar{C}$ are said to be *dual to each other*. A cycle $C$ is said to be *self-dual* if the ring sequence $[\bar{c}_1, \cdots, \bar{c}_k]$ is a cyclic shift of $[c_1, \cdots, c_k]$, i.e., if $C$ and $\bar{C}$ represent the same cycle. A cycle $C$ will be referred to as *primitive* if it is (vertex) disjoint from its dual $\bar{C}$. For example, the two four-cycles [0001] [1110] (see Fig. 2) are a pair of primitive cycles, dual to each other, while [0011] is a self-dual four-cycle in $G_n$ for all $n \geq 2$. A cycle $C$ in $G_n$ is called *reducible* if there exists a cycle $C'$ in $G_n$ such that the vertices contained in $C'$ form a proper subset of those contained in $C$. It may easily be verified that a cycle $C$ is reducible iff it contains at least one pair of conjugate vertices $x$ and $\hat{x}$.

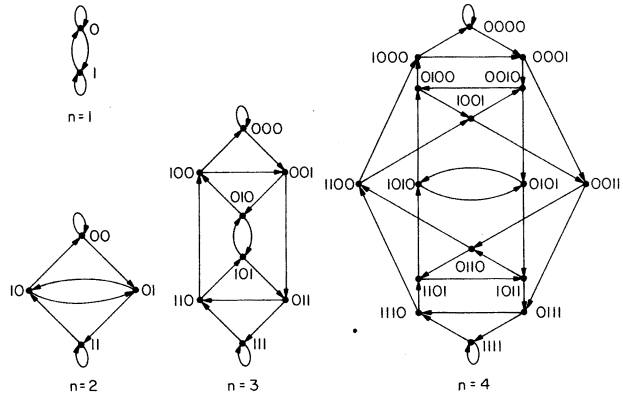

Fig. 3. The de Bruijn graphs of order $n=1, 2, 3$, and 4.

A *factor* of $G_n$ is a partial graph of $G_n$ formed by a set of disjoint cycles that, together, include all the vertices of $G_n$. Evidently, the state graph of every nonsingular $n$-stage FSR is a factor of $G_n$ and every factor of $G_n$ is the state graph of some nonsingular FSR. We shall use the notation $(B^n, F)$ for the factor of $G_n$ that is generated by the nonsingular function $f$.

The following are some well-known theorems that we shall need in the sequel.

*Theorem 1* [5], [8]: An FSR is nonsingular iff its feedback function $f(x)$ is of the form

$$f(x_1, x_2, \cdots, x_n) = x_1 \oplus f_0(x_2, \cdots, x_n) \tag{6}$$

where $f_0(x_2, \cdots, x_n) = f(0, x_2, \cdots, x_n)$ is an arbitrary Boolean function in the $n-1$ variables $x_2, \cdots, x_n$.

By (6), the nonsingularity of $f$ also implies the nonsingularity of its complement $\bar{f}$.

Two cycles $C_1$ and $C_2$ are said to be *adjacent* if they are disjoint and there exists a vertex $x$ in $C_1$ such that its conjugate $\hat{x}$ belongs to $C_2$.

*Theorem 2* [7], [8]: A reducible cycle $C$ is split into two adjacent cycles when the successors of a conjugate pair $x$ and $\hat{x}$ in $C$ are interchanged. Two adjacent cycles $C_1$ and $C_2$, with $x$ in $C_1$ and $\hat{x}$ in $C_2$, are joined into a single cycle when the successors of $x$ and $\hat{x}$ are interchanged.

To illustrate Theorem 2, consider the two four-cycles of Fig. 2. These cycles are adjacent, with (001) and (010) in one of them being conjugate to (101) and (110), respectively, in the other one. By interchanging the successors of, say, the pair (010) and (110) we obtain the eight-cycle [(000), (001), (010), (101), (011), (111), (110), (100)]. The pair (001) and (101) belong now to the same cycle and, interchanging their successors, results in the two-cycle [(010), (101)] and the six-cycle [(000), (001), (011), (111), (110), (100)].

We conclude this section by stating the change in the feedback function that corresponds to a split of a reducible cycle or to a join of two adjacent cycles. Let $f(x_1, \cdots, x_n)$ be the feedback function of a nonsingular FSR and let

$$h(x_1, \cdots, x_n) = f(x_1, \cdots, x_n) \oplus x_2^{a_2} \cdot x_3^{a_3} \cdots x_n^{a_n} \quad (7)$$

where $(a_2, a_3, \cdots, a_n) \in B^{n-1}$ and $x_i^1$ and $x_i^0$ denote $x_i$ and $\bar{x}_i$, respectively. The function $h$ differs from $f$ only for the conjugate $n$-tuples $a=(a_1, a_2, \cdots, a_n)$ and $\hat{a}=(\bar{a}_1, a_2, \cdots, a_n)$ and, hence the following theorem.

*Theorem 3* [5], [8]: The factors $(B^n, F)$ and $(B^n, H)$, corresponding to the functions $f$ and $h$ of (7), respectively, may be obtained from each other by interchanging the respective successors of the vertices $a$ and $\hat{a}$.

## III. The $D$-Morphism of the de Bruijn Graph

Consider the set of binary $n$-tuples $B^n$. We define a mapping $D: B^n \to B^{n-1}$, $n \geq 2$, as follows. For $a=(a_1, \cdots, a_n) \in B^n$ and $\alpha=(\alpha_1, \cdots, \alpha_{n-1}) \in B^{n-1}$, $aD=\alpha$ iff

$$\alpha_i = a_i \oplus a_{i+1} \qquad i = 1, \cdots, n-1. \quad (8)$$

Given $\alpha \in B^{n-1}$ and $a_1 \in B$, the unique solution of (8) for the remaining $n-1$ $a_i$'s is

$$a_i = a_1 \oplus s_i \qquad i = 2, \cdots, n \quad (9)$$

where

$$s_i = \alpha_1 \oplus \alpha_2 \oplus \cdots \oplus \alpha_{i-1} \qquad i = 2, \cdots, n \quad (10)$$

Hence, we deduce the following lemma.

*Lemma 1:* The mapping $D$ is *onto*, i.e., every element in $B^{n-1}$ is an image under $D$ of some element in $B^n$.

*Lemma 2:* For $x, y \in B^n$, $xD=yD$ iff $x=y$ or $x=\bar{y}$. Thus, $D$ is a mapping of $B^n$ onto $B^{n-1}$ under which every element in $B^{n-1}$ is the image of a pair of dual elements in $B^n$. Furthermore, $D$ preserves the shift relation, because, if $a, b \in B^n$ and $a \to b$ then $b_i=a_{i+1}$, $i=1, \cdots, n-1$, $\beta_i=b_i \oplus b_{i+1}=a_{i+1} \oplus a_{i+2}=\alpha_{i+1}$, $i=1, \cdots, n-2$, and $\alpha=aD \to bD=\beta$.

Therefore, we have the following theorem.

*Theorem 4:* The mapping $D$ is a homomorphism of $G_n$ onto $G_{n-1}$.

If $H$ is a subgraph of $G_n$ and $H^*$ is its homomorphic image, under $D$ in $G_{n-1}$, we shall refer to $H^*$ as the *D-morphic* image of $H$ and use the notation $H^*=HD$. For the remaining part of this section we shall mostly be concerned with cycles and factors of $G_n$ such that their $D$-morphic images in $G_{n-1}$ are also cycles and factors, respectively.

Noting that a primitive cycle contains no pair of dual vertices we have Lemma 3.

*Lemma 3:* The $D$-morphic image of a primitive $k$-cycle is also a $k$-cycle. Using the binary ring sequence representation of a cycle, the following lemma holds.

*Lemma 4:* If $C=[c_1, \cdots, c_k]$ is a primitive $k$-cycle in $G_n$ then the $k$-cycle $CD=\Gamma=[\gamma_1, \cdots, \gamma_k]$ in $G_{n-1}$ is given by

$$\gamma_i = c_i \oplus c_{i+1} \qquad i = 1, \cdots, k-1 \quad (11)$$

and

$$\gamma_k = c_k \oplus c_1. \quad (12)$$

The *weight* $W(C)$ of a $k$-cycle $C=[c_1, \cdots, c_k]$ is defined to be the number of nonzero digits among the $k$ $c_i$'s, i.e.,

$$W(C) = \sum_{i=1}^{k} c_i.$$

*Theorem 5:* A $k$-cycle $\Gamma$ in $G_{n-1}$ is the $D$-morphic image of a primitive $k$-cycle $C$ in $G_n$ iff $W(\Gamma)$ is even.

*Proof:* If $C$ is primitive and $\Gamma=CD$ then, by Lemma 4, we have

$$\begin{aligned}\gamma_1 \oplus \gamma_2 \oplus \cdots \oplus \gamma_{k-1} \oplus \gamma_k &= (c_1 \oplus c_2) \oplus (c_2 \oplus c_3) \oplus \cdots \oplus (c_{k-1} \oplus c_k) \oplus (c_k \oplus c_1) \\ &= c_1 \oplus c_2 \oplus c_2 \oplus c_3 \oplus \cdots \oplus c_{k-1} \oplus c_k \oplus c_k \oplus c_1 = 0.\end{aligned}$$

Thus, the modulo 2 sum of the $\gamma_i$'s is zero and, hence, $W(\Gamma)$ is even. Now, let $\Gamma=[\gamma_1, \cdots, \gamma_k]$ be a $k$-cycle of even weight in $G_{n-1}$ and let

$$c_i = c_1 \oplus \gamma_1 \oplus \gamma_2 \oplus \cdots \oplus \gamma_{i-1} \qquad i = 2, \cdots, k \quad (13)$$

where $c_1$ is either 0 or 1. We claim that the dual binary ring sequences $C=[c_1, c_2, \cdots, c_k]$ and $\bar{C}=[\bar{c}_1, \bar{c}_2, \cdots, \bar{c}_k]$, with $c_1 \in B$ and the $c_i$'s, $i=2, \cdots, k$, determined by (13), represent the pair of primitive and dual $k$-cycles in $G_n$ whose $D$-morphic image is $\Gamma$. To show this, we first observe that (13) is the solution of (11) for the $c_i$'s. Furthermore, since $W(\Gamma)$ is even, $\gamma_k=\gamma_1 \oplus \gamma_2 \oplus \cdots \oplus \gamma_{k-1}$ and (13) is also consistent with (12). Secondly, since $\Gamma$ is a $k$-cycle in $G_{n-1}$, the $k$ $(n-1)$-tuples formed by consecutive $\gamma_i$ digits are all distinct, which, in view of (11) and (12), implies that the $k$ $n$-tuples formed by consecutive $c_i$'s are not only distinct, but, also that no two of these $n$-tuples are dual to each other.

The following is also an immediate consequence of the proof of Theorem 5.

*Corollary 1:* There exists a one-to-one correspondence between the $k$-cycles $\Gamma$ of even weight in $G_{n-1}$ and the primitive pairs of dual $k$-cycles $C$ and $\bar{C}$ in $G_n$ under which $\Gamma=CD=\bar{C}D$.

As an example consider the graphs $G_2$ and $G_3$ (Fig. 3). The only even weight cycles in $G_2$ are $\Gamma_1=[0]$, $\Gamma_3=[011]$, and $\Gamma_4=[0011]$. The corresponding cycle pairs in $G_3$ are $C_1=[0]$ and $\bar{C}_1=[1]$, $C_3=[001]$ and $\bar{C}_3=[110]$, and the pair $C_4=[0001]$ and $\bar{C}_4=[1110]$. These are all and the only primitive cycles in $G_3$.

We proceed now to derive an analogous correspondence in which cycles of odd weight are involved.

*Lemma 5:* A cycle $C=[c_1, \cdots, c_k]$ in $G_n$ is self-dual iff it is of even length $k=2p$ and

$$c_{i+p} = \bar{c}_i \qquad i = 1, \cdots, p. \quad (14)$$

*Proof:* The "if" part of this lemma is obvious. For the "only if" part, we first observe that if $C$ is a self-dual $k$-cycle and $x$ is a vertex of $C$ then also $\bar{x}$ belongs to $C$ and $k$ must be even. Secondly, since the ring sequence $\bar{C}=[\bar{c}_1, \cdots, \bar{c}_k]$ is a cyclic shift of the ring sequence $C=[c_1, \cdots, c_k]$, it follows that if $y$ is the successor of $x$ on $C$ then $\bar{y}$ is the successor of $\bar{x}$. This is possible only if the distance between a pair of dual vertices on $C$ is the same for all such pairs. If $k=2p$, this distance must be $p$ and, hence, condition (14) of the lemma.

*Lemma 6:* The $D$-morphic image of a self-dual $2p$-cycle is a $p$-cycle. If $C=[c_1, \cdots, c_{2p}]$ is a self-dual $2p$-cycle in $G_n$, then the $p$-cycle $CD=\Gamma=(\gamma_1, \cdots, \gamma_p)$ in $G_{n-1}$ is given by

$$\gamma_i = c_i \oplus c_{i+1} \qquad i = 1, \cdots, p. \tag{15}$$

This lemma is a straightforward result of Lemma 5 and needs no further evidence.

The analogue of Theorem 5 may now be stated as follows.

*Theorem 6:* A $p$-cycle $\Gamma$ in $G_{n-1}$ is the $D$-morphic image of a self-dual $2p$-cycle $C$ in $G_n$ iff $W(\Gamma)$ is odd.

*Proof:* From (15), we have $\gamma_1 \oplus \gamma_2 \oplus \cdots \oplus \gamma_p = c_1 \oplus c_{p+1}$, which, with $i=1$ in (14) reduces to $\gamma_1 \oplus \gamma_2 \oplus \cdots \oplus \gamma_p = 1$. This proves the necessity part of the theorem. As for the other part, let $\Gamma=[\gamma_1, \cdots, \gamma_p]$ be a $p$-cycle of odd weight in $G_{n-1}$ and let

$$c_i = \gamma_1 \oplus \gamma_2 \oplus \cdots \oplus \gamma_{i-1} \qquad i = 2, \cdots, p. \tag{16}$$

It may readily be verified, by using arguments similar to those used in the proof of Theorem 5, that the binary ring sequence $C=[0, c_2, \cdots, c_p, 1, \bar{c}_2, \cdots, \bar{c}_p]$, with the $c_i$'s, $i=2, \cdots, p$, determined by (16), represents the self-dual $2p$-cycle in $G_n$ whose $D$-morphic image is the $p$-cycle $\Gamma$.

To complete the analogy, we have the following corollary.

*Corollary 2:* There exists a one-to-one correspondence between the $k$-cycles $\Gamma$ of odd weight in $G_{n-1}$ and the self-dual $2k$-cycles $C$ in $G_n$ under which $\Gamma=CD$.

Continuing with the previous example, the only odd weight cycles in $G_2$ are $\Gamma_1=[1]$, $\Gamma_2=[01]$, and $\Gamma_3=[001]$. The corresponding self-dual cycles in $G_3$ are $C_1=[01]$, $C_2=[0011]$, and $C_3=[000111]$. These are all and the only self-dual cycles in $G_3$.

Table I lists all the cycles of $G_3$ and their corresponding primitive and self-dual cycles in $G_4$.

The correspondences established in Table I for individual cycles may easily be extended to a correspondence between factors. It is clear that if a set of cycles form a factor of $G_n$ then the set of their duals is also a factor of $G_n$. Two factors consisting of dual cycle sets are called dual factors and a factor is said to be self-dual if, along with every cycle $C$ in this factor, $\bar{C}$ also belongs to this factor. Obviously, a factor is self-dual iff it consists of self-dual cycles and/or primitive pairs of dual cycles. From the preceding results it is also perfectly clear that the following theorem holds.

*Theorem 7:* There exists a one-to-one correspondence between the factors $(B^{n-1}, \Phi)$ of $G_{n-1}$ and the self-dual factors $(B^n, F)$ of $G_n$ under which

$$(B^{n-1}, \Phi) = (B^n, F)D. \tag{17}$$

More explicitly, (17) means that $B^{n-1}=B^nD$ and that for every $x \in B^n$, $(xF)D=(xD)\Phi$. Now, if the mappings $F$ and $\Phi$ are induced by the functions $f$ and $\phi$, respectively, and $(\zeta_1, \cdots, \zeta_{n-1})=(x_1, \cdots, x_n)D$, then

$$(xF)D = (x_2, \cdots, x_n, f(x))D = (\zeta_2, \cdots, \zeta_{n-1}, x_n \oplus f(x)) \tag{18}$$

$$(xD)\Phi = (\zeta_1, \cdots, \zeta_{n-1})\Phi = (\zeta_2, \cdots, \zeta_{n-1}, \phi(\zeta)). \tag{19}$$

TABLE I

THE CYCLES OF $G_3$ AND THEIR CORRESPONDING CYCLES IN $G_4$

| | Cycles of $G_3$ | Corresponding Cycles in $G_4$ | |
|---|---|---|---|
| Even Weight Cycles | [0] | [0] ; [1] | Primitive Cycles |
| | [011] | [001] ; [110] | |
| | [0011] | [0001] ; [1110] | |
| | [00011] | [00001] ; [11110] | |
| | [0010111] | [0001101] ; [1110010] | |
| | [0011101] | [0001011] ; [1110100] | |
| | [00010111] | [00001101] ; [11110010] | |
| | [00011101] | [00001011] ; [11110100] | |
| Odd Weight Cycles | [1] | [01] | Self-Dual Cycles |
| | [01] | [0011] | |
| | [001] | [000111] | |
| | [0001] | [00001111] | |
| | [0111] | [00101101] | |
| | [00111] | [0001011101] | |
| | [000111] | [000010111101] | |
| | [001011] | [000110111001] | |
| | [001101] | [000100111011] | |
| | [0001011] | [000011011111001] | |
| | [0001101] | [000010011111011] | |

Thus, $(B^{n-1}, \Phi)$ is the $D$-morphic image of $(B^n, F)$ iff $\phi(\zeta)=x_n \oplus f(x)$, or, since $\zeta_i=x_i \oplus x_{i+1}$, $i=1, \cdots, n-1$,

$$f(x_1, x_2, \cdots, x_n) = x_n \oplus \phi[(x_1 \oplus x_2), (x_2 \oplus x_3), \cdots, (x_{n-1} \oplus x_n)]. \tag{20}$$

It should be noted that this expression for $f$ in terms of $\phi$ holds not only in the nonsingular case, but also for any pair of mappings $F: B^n \to B^n$ and $\Phi: B^{n-1} \to B^{n-1}$ such that $FD=D\Phi$. In this paper, however, we are interested only in the nonsingular case and no attempt to reach beyond this case will be made.

## IV. SOME APPLICATIONS

The results derived in the previous section provide a basis for a new approach to the design of various types of nonsingular FSRs. A few of the possible applications are presented below.

### A. Cycles of Maximum Length

Suppose $\Gamma=[\gamma_1, \cdots, \gamma_m]$ is an $m$-cycle, $m=2^{n-1}$, in $G_{n-1}$. It is well known that for $s \geq 2$, all the $2^s$-cycles of $G_s$ are of even weight and, therefore, by Theorem 5, $\Gamma$ is the $D$-morphic image of a dual pair of primitive $m$-cycles $C$ and $\bar{C}$ in $G_n$, $n>2$.

Given $\Gamma$, this pair of cycles may readily be obtained from (13) by putting $c_1=0$ and using the recursive relation

$$c_{i+1} = c_i \oplus \gamma_i \qquad i = 1, \cdots, m-1. \tag{21}$$

The cycles $C$ and $\bar{C}$ are, of course, adjacent and if $x$ and $\hat{x}$ are a pair of conjugate vertices such that $x$ is on $C$ and $\hat{x}$ is on $\bar{C}$ then, according to Theorem 3, interchanging the successors of $x$ and $\hat{x}$ will result in a $2^n$-cycle in $G_n$. Thus, to obtain a maximum length cycle in $G_n$, $n>2$, we have to find one $\Gamma=[\gamma_1, \cdots, \gamma_m]$ in $G_{n-1}$, transform it according to (21) into $C$ and $\bar{C}$, and interchange the successors of a pair of conjugate vertices shared by $C$ and $\bar{C}$. This simple

procedure may, of course, be started at any $k<n$ for which a $2^k$-cycle in $G_k$ is known and iterated $n-k$ times to obtain a maximum length cycle in $G_n$.

The described transition from a $2^{n-1}$-cycle in $G_{n-1}$ to a $2^n$-cycle in $G_n$ may also be expressed in terms of a recursive formula for a feedback function that will generate a maximum length cycle of an $n$-stage FSR. Obviously, the $m$-cycle $\Gamma$ and the corresponding pair of cycles $C$ and $\bar{C}$ form a pair of corresponding factors under Theorem 7. Let $(B^{n-1}, \Phi)$ and $(B^n, F)$ be the factor notation for $\Gamma$ and the pair $C$ and $\bar{C}$, respectively. Thus, if $\phi$ is the feedback function generating $\Gamma$, the function $f$ that generates the two cycles of $(B^n, F)$ is given by (20). To obtain the function that will join these two cycles into one maximal cycle, we need to know explicitly a pair of conjugate vertices, shared by $C$ and $\bar{C}$. Consider the vertex $e=(e_1, \cdots, e_n)$, $e_1=0$ and $e_{i+1}=\bar{e}_i$, $i=1, \cdots, n-1$. Evidently, if $e$ belongs to $C$ then $\bar{e}$ belongs to $\bar{C}$ and vice versa. Since $e$ and $\bar{e}$ are on different cycles and $e \to \bar{e}$, it follows that $\bar{e}=\hat{e}F$, where $\hat{e}$ is the conjugate of $e$. Thus, $e$ and $\hat{e}$ is an explicit conjugate pair that we need and, by (7), the function $h$ which will generate a maximum length cycle of an $n$-stage FSR is given by

$$h(x_1, \cdots, x_n) = x_n \oplus \phi[(x_1 \oplus x_2), (x_2 \oplus x_3), \cdots, (x_{n-1} \oplus x_n)] \oplus x_2^{e_2} \cdot x_3^{e_3} \cdot \cdots \cdot x_n^{e_n} \quad (22)$$

where $e_2=1$ and $e_{i+1}=\bar{e}_i$, $i=2, \cdots, n-1$.

Examples of maximal-cycle functions $h_n$ for $n=3, 4, 5$ obtained, recursively, according to (22) from the function $h_2(x_1, x_2)=\bar{x}_1$, which generates a four-cycle in $G_2$, are the following.

$$h_3(x_1, x_2, x_3) = x_3 \oplus \overline{(x_1 \oplus x_2)} \oplus x_2\bar{x}_3 = \bar{x}_1 \oplus \bar{x}_2 x_3$$

$$\begin{aligned} h_4(x_1, x_2, x_3, x_4) &= x_4 \oplus (\bar{x}_1 \oplus x_2) \\ &\quad \oplus (\bar{x}_2 \oplus x_3)(x_3 \oplus x_4) \oplus x_2\bar{x}_3 x_4 \\ &= \bar{x}_1 \oplus x_2 \oplus x_3 \oplus \bar{x}_2 x_3 \bar{x}_4 \end{aligned}$$

$$\begin{aligned} h_5(x_1, x_2, x_3, x_4, x_5) &= x_5 \oplus (\bar{x}_1 \oplus x_2) \oplus (x_2 \oplus x_3) \oplus (x_3 \oplus x_4) \\ &\quad \oplus (\bar{x}_2 \oplus x_3)(x_3 \oplus x_4)(\bar{x}_4 \oplus x_5) \\ &\quad \oplus x_2\bar{x}_3 x_4 \bar{x}_5 \\ &= \bar{x}_1 \oplus x_2 x_3 \oplus x_4 x_5 \oplus \bar{x}_2 x_4 \oplus \bar{x}_3 x_5 \\ &\quad \oplus \bar{x}_2 x_3 \bar{x}_4 x_5. \end{aligned}$$

### B. Factors with Cycles Whose Length is a Power of 2

In certain cases it is possible to solve the recursion formula (20) and to obtain an explicit expression for $f(x_1, \cdots, x_n)$. An especially interesting case is the one in which the initial function is set to be $f_1=x_1$ for $n=1$. It can be shown that the sequence of functions $\{f_n\}$, obtained from $f_1=x_1$, according to

$$\begin{aligned} &f_n(x_1, \cdots, x_n) \\ &\quad = x_n \oplus f_{n-1}[(x_1 \oplus x_2), (x_2 \oplus x_3), \cdots, (x_{n-1} \oplus x_n)] \end{aligned} \quad (23)$$

are of the form

$$f_n(x_1, \cdots, x_n) = x_1 \oplus c_2 x_2 \oplus \cdots \oplus c_n x_n \quad (24)$$

where the binary coefficients $c_i$, $i=2, \cdots, n$, are obtained from the expansion

$$(z \oplus 1)^n = z^n \oplus c_2 z^{n-1} \oplus c_3 z^{n-2} \oplus \cdots \oplus c_n z \oplus 1. \quad (25)$$

Let $(B^n, F_n)$ be the factor of $G_n$ whose cycles are generated by $f_n$, $n \geq 2$, and let $p \geq 0$ be an integer so that $2^p < n \leq 2^{p+1}$.

The following is a summary of results, partially known [2], [8] and partially derived in a forthcoming paper [14].

1) Every cycle in $(B^n, F_n)$ is of length $k=2^i$, with $0 \leq i \leq p+1$.
2) There are two cycles of length $k=1$; for each $i$, $1 \leq i \leq p$, there are
$$N_i = 2^{-i}(2^{2^i} - 2^{2^{i-1}}) \quad (26)$$
cycles of length $k=2^i$, and the number of cycles of length $k=2^{p+1}$ is
$$N_{p+1} - 2^{-(p+1)}(2^n - 2^{2^p}). \quad (27)$$
3) The total number of cycles in $(B^n, F_n)$ is
$$N = 2^{-(p+1)}\left[2^n + \sum_{i=0}^{p} 2^{i+2^{p-i}}\right] \quad (28)$$
and this is the maximum possible number of cycles in a factor of $G_n$ such that the length of every cycle in the factor is a power of 2.

The sequence of functions $\{\bar{f}_n\}$, where $\bar{f}_n=f_n \oplus 1$, also satisfies the recursion (23) and for the corresponding factors $(B^n, \bar{F}_n)$ of $G_n$, we have the following.

4) All the cycles in $(B^n, \bar{F}_n)$ are of the same length $k=2^{r+1}$, where $r \geq 0$ is an integer such that $2^r \leq n < 2^{r+1}$. (Note the difference in the definitions of integers $r$ and $p$.)

This result has also been obtained recently elsewhere [13], through a different approach.

The following is true.

5) The number $2^{n-(r+1)}$ of cycles in $(B^n, \bar{F}_n)$ is the maximum possible number of cycles in a factor of $G_n$ with equal length cycles.

### C. Joining and Splitting of Cycles

The results of Section III may also be applied to simplify, in certain cases, the method of designing nonsingular FSRs proposed by Yoeli [7].

It is easily observed that if $a$ and $\hat{a}$ are a pair of conjugate vertices in $G_n$, then $aD$ and $\hat{a}D$ are conjugate in $G_{n-1}$. Also, if $\alpha=aD$ and $\beta=bD$ are conjugates in $G_{n-1}$, then either the pairs $(a, b)$ and $(\bar{a}, \bar{b})$ or the pairs $(a, \bar{b})$ and $(\bar{a}, b)$ are conjugate pairs in $G_n$. This observation has the following implications on the adjacency relationships between a pair of cycles $\Gamma_1$ and $\Gamma_2$ in $G_{n-1}$ and the corresponding cycles $C_1$, $C_2$, $\bar{C}_1$ and $\bar{C}_2$ in $G_n$.

*Case 1:* The weight of both $\Gamma_1$ and $\Gamma_2$ is odd. In this case $C_i$ and $\bar{C}_i$ represent the same self-dual cycle in $G_n$ and the

cycles $\Gamma_1$ and $\Gamma_2$ are adjacent iff $C_1$ and $C_2$ are adjacent.

*Case 2:* The weight of $\Gamma_1$ is odd and that of $\Gamma_2$ is even. In this case $C_1$ is self-dual, $C_2$ and $\bar{C}_2$ are primitive and $\Gamma_1$ and $\Gamma_2$ are adjacent iff $C_1$ is adjacent to both $C_2$ and $\bar{C}_2$.

*Case 3:* The weight of both $\Gamma_1$ and $\Gamma_2$ is even. This time all four cycle $C_1$, $\bar{C}_1$, $C_2$ and $\bar{C}_2$ are primitive and $\Gamma_1$ and $\Gamma_2$ are adjacent iff either $(C_1, C_2)$ and $(\bar{C}_1, \bar{C}_2)$ or, $(C_1, \bar{C}_2)$ and $(\bar{C}_1, C_2)$ are pairs of adjacent cycles.

A similar correspondence may also be established between reducible cycles in $G_{n-1}$ and $G_n$.

The previous discussion suggests that the technique of joining and splitting known cycles to obtain new cycles of specified length in $G_n$ may, in many cases, be performed on a "cycle transition graph" [7] of order $n-1$, rather than $n$.

## ACKNOWLEDGMENT

The author wishes to thank Prof. S. W. Golomb and Prof. L. R. Welch of the Department of Electrical Engineering, University of Southern California, Los Angeles, Calif., for many helpful discussions.

## REFERENCES

[1] N. G. de Bruijn, "A combinatorial problem," *Proc. Kon. Ned. Akad. Wetensch.*, vol. 49, pp. 758–764, 1946.

[2] B. Elspas, "Theory of autonomous linear sequential networks," *IRE Trans. Circuit Theory*, vol. CT-6, pp. 45–60, March 1959.

[3] S. W. Golomb, L. R. Welch, and R. M. Goldstein, "Cycles from nonlinear shift registers," Jet Propulsion Lab., California Institute of Technology, Pasadena, Calif., Prog. Rept. 20-389, August 1959.

[4] W. W. Peterson, *Error-Correcting Codes.* Cambridge, Mass.: M.I.T. Press, 1961.

[5] M. Yoeli, "Nonlinear feedback shift registers," IBM Development Lab., Poughkeepsie, N. Y., Tech. Rept. TR00.809, September 1961.

[6] P. R. Bryant, F. G. Heath, and R. D. Killick, "Counting with feedback shift registers by means of a jump technique," *IRE Trans. Electronic Computers* (Correspondence), vol. EC-11, pp. 285–286, April 1962.

[7] M. Yoeli, "Counting with nonlinear binary feedback shift registers," *IEEE Trans. Electronic Computers*, vol. EC-12, pp. 357–361, August 1963.

[8] S. W. Golomb, *Shift Register Sequences.* San Francisco, Calif.: Holden-Day, 1967.

[9] A. Lempel, "*m*-ary closed sequences," *J. Combinatorial Theory*, to be published March 1971.

[10] L. R. Ford, Jr., "A cyclic arrangements of *m*-tuples," RAND Corporation, Santa Monica, Calif., Rept. P-1071, April 1957.

[11] C. Eldert, H. J. Gray, Jr., H. M. Gurk, and M. Rubinoff, "Shifting counters," *AIEE Trans.* (*Commun. Electron.*), vol. 77, pp. 70–74, March 1958.

[12] E. B. Leach, "Regular sequences and frequency distributions," *Proc. Amer. Math. Soc.*, vol. 11, August 1960.

[13] M. Perlman, "Decomposition of the states of a linear feedback shift register into cycles of equal length," *JPL Space Programs Summary 37-52*, vol. 3, pp. 149–154, August 1968.

[14] A. Lempel, "On extremal factors of the de Bruijn graph," *J. Combinatorial Theory*, to be published.