Constructions for Perfect Maps and Pseudorandom Arrays

TUVI ETZION

Abstract—**A construction of perfect maps, i.e., periodic $r \times v$ binary arrays in which each $n \times m$ binary matrix appears exactly once, is given. A similar construction leads to arrays in which only the zero $n \times m$ matrix does not appear and to a construction in which only a few $n \times m$ binary matrices do not appear. A generalization to the nonbinary case is also given. The constructions involve an interesting problem in shift register theory. We give the solution for almost all the cases of this problem.**

I. Introduction

PERFECT MAPS and pseudorandom arrays are $r \times v$ binary two-dimensional periodic arrays in which all or most of the $n \times m$ binary matrices appear once as windows in one period of the array. These arrays can be used in two-dimensional range-finding, scrambling, various kinds of mask configurations, and other applications in communications and coding.

A *perfect map* is an $r \times v$ binary array, with $rv = 2^{nm}$, such that each binary $n \times m$ matrix appears exactly once as a window in the array. Reed and Stewart [1] gave an example of a 4×4 array with the 2×2 window property. Ma [2] and Fan *et al.* [3] gave constructions for perfect maps and proved that for each n and m there exist r and v such that $rv = 2^{nm}$ and there exists an $r \times v$ binary array with the $n \times m$ window property. They called this array an $(r, v; n, m)$-array.

Constructions for similar arrays of size $rv = 2^{nm} - 1$ such that each nonzero matrix of size $n \times m$ appears exactly once as a window in the array were given by Gordon [4] and Macwilliams and Sloane [5] who called them pseudorandom arrays. Other constructions for similar pseudorandom arrays were given by Nomura *et al.* [6], and Van Lint *et al.* [7].

In this paper we present a new construction of perfect maps and other pseudorandom arrays. The constructed arrays are different from all the arrays constructed in the aforementioned papers. Given appropriate sizes $r \times v$ and $n \times m$ the construction produces many arrays of size $r \times v$ with the $n \times m$ window property.

In Section II we give the background for the one-dimensional case, i.e., a binary sequence of length 2^n such that each n-tuple appears exactly once as a window in the sequence. Those sequences are called de Bruijn sequences [8]. We also present the nonbinary case of de Bruijn sequences.

In Section III we show that the two-dimensional case can be represented in a similar way to the t-ary de Bruijn graph (de Bruijn graph over an alphabet with t letters), and we give a method of constructing the two-dimensional arrays. Applying this method involves solving a problem in binary shift registers that is interesting in itself. We give a complete solution to this problem.

In Section IV we show that the method of Section III is generalized easily for the construction of $r \times v$ arrays in which only a few $n \times m$ binary matrices do not appear, and each of the other $n \times m$ matrices appears exactly once as a window. The case of $rv = 2^{nm} - 1$ in which only the zero matrix does not appear involves an interesting question in shift register theory; we give only a partial solution to it. A generalization to arrays with elements taken from an alphabet of t letters is given in Section V.

II. Shift Register Sequences

We now define the feedback shift registers and the de Bruijn graph; the definitions will be generalized in the next section to the two-dimensional case. We shall be using some of the ideas involved in the one-dimensional case to solve the problem in the two-dimensional case.

A *feedback shift register* of order n (FSR_n) has 2^n states corresponding to the set B^n of all binary n-tuples. The feedback function $f(X)$, $X = (x_0, x_1, \cdots, x_{n-1}) \in B^n$ of the FSR induces a mapping $\boldsymbol{F}$: $B^n \to B^n$ such that $X\boldsymbol{F} = Y$, where

$$y_i = x_{i+1}, \qquad i = 0, 1, \cdots, n-2, \text{ and } y_{n-1} = f(X).$$

The *companion* X' of a state $X = (x_0, \cdots, x_{n-2}, x_{n-1})$ is defined by

$$X' = (x_0, \cdots, x_{n-2}, \bar{x}_{n-1})$$

where $\bar{x}$ denotes the binary complement of x.

A *cycle* C of length q ($q = \textit{length}\ (C)$) of an FSR_n is a (cyclic) sequence of $q > 0$ distinct states $C = [X^{(1)}, X^{(2)}, \cdots, X^{(q)}]$, $X^{(i)} \in B^n$ such that $X^{(1)}\boldsymbol{F} = X^{(q)}$ and $X^{(i+1)}\boldsymbol{F} = X^{(i)}$, $i = 1, 2, \cdots, q-1$. We denote a cycle of length q by $C = [x_0^{(1)} x_0^{(2)} \cdots x_0^{(q)}]$, where each n consecutive bits correspond to a state. The state diagram of an FSR is called a *factor* if each state belongs to a cycle. Two

Manuscript received August 5, 1987; revised November 6, 1987. This work was supported in part by the Office of Naval Research under Contract N00014-84-K-0189.

The author was with the Department of Electrical Engineering-Systems, University of Southern California, Los Angeles, CA 90089-0272. He is now with the Computer Science Department, The Technion—Israel Institute of Technology, Haifa 32000, Israel.

IEEE Log Number 8824274.

0018-9448/88/0900-1308$01.00

cycles C_1 and C_2 are said to be *adjacent* if they are (state) disjoint and a state X exists on C_1 whose companion X' is on C_2. It is well-known [9] that C_1 and C_2 are joined into a single cycle when the predecessors of X and X' are interchanged. When all the cycles of a factor are joined into one cycle, this cycle has 2^n states, and it is called a full-length shift register cycle or a de Bruijn cycle.

The de Bruijn graph of order n, G_n [8], is a graph with 2^n vertices, each of which is represented by a different binary n-tuple. From vertex $X=(x_0, x_1, \cdots, x_{n-1})$ to vertex $Y=(y_0, y_1, \cdots, y_{n-1})$ there is a directed edge if and only if

$$y_i = x_{i+1}, \qquad i=0,1,\cdots,n-2, \text{ and } y_{n-1}\in B.$$

A factor in a directed graph is a set of vertex disjoint directed cycles which includes all the vertices of the graph. Clearly, there is a one-to-one mapping between the factors of G_n and the factors of the FSR_n. A de Bruijn cycle is a factor and a Hamiltonian cycle in G_n. Comprehensive work on shift registers can be found in [9], and a survey on de Bruijn cycles can be found in [10].

The de Bruijn graph may be generalized to an alphabet with t letters as follows. The de Bruijn graph [11] of order n over an alphabet with t letters, $G_{n,t}$, is a graph with t^n vertices, each of which is represented by a distinct t-ary n-tuple. From vertex $X=(x_0, x_1, \cdots, x_{n-1})$ to vertex $Y=(y_0, y_1, \cdots, y_{n-1})$ there is a directed edge if and only if (iff)

$$y_i = x_{i+1}, \qquad i=0,1,\cdots,n-2,$$

and

$$y_{n-1}\in\{0,1,\cdots,t-1\}.$$

A t-ary de Bruijn cycle is a Hamiltonian cycle in $G_{n,t}$. Constructions of t-ary de Bruijn sequences can be found in [12]–[14]. In our construction of perfect maps and pseudorandom arrays, we use some of the ideas from the construction of Etzion [14] for t-ary de Bruijn cycles.

III. Construction of Perfect Maps

Now we present a procedure for generating an $r\times v$ doubly periodic array, where $rv=2^{nm}$ with the $n\times m$ window property, i.e., each $n\times m$ binary matrix appears exactly once in one period of the array. It is easy to verify that the number of rows of the array must be a power of 2, i.e., $r=2^k$. Since the zero $n\times m$ matrix appears exactly once, we also have $r>n$. Our construction will produce $(2^k, 2^{nm-k}; n, m)$-arrays whenever $n<2^k\le 2^n$, unless both $k=n$ and $m=2$. The construction involves a factor in G_n with 2^{n-k} cycles of length $r=2^k$. This factor will be called a *perfect factor* and will be denoted by $\mathrm{PF}(n)$. We will prove the existence of perfect factors for all possible values of r that are powers of 2 and satisfy $n<r\le 2^n$. When $m=1$, the array whose columns are the cycles of a perfect factor is clearly a $(2^k, 2^{n-k}; n, 1)$-array. Henceforth we will assume that $n>1$ and $m>1$.

A. The Zero Shift of a Cycle

Given a perfect factor, in each of the cycles of length 2^k we choose a unique state of size n to be the *zero state* in the cycle. All the other states will be numbered in ascending order. The representation of the cycle in which the zero state is at the beginning of the cycle will be called the *zero shift* of the cycle. All the other shifts will be numbered in ascending order from shift one to shift 2^k-1. We will choose the zero state as the minimal state in the cycles (we view the states as numbers in base 2 notation); note, however, that it can be chosen in other ways. We also order all the 2^{n-k} cycles in ascending order according to their zero state. Again, any other order could also serve for the construction and would produce a different perfect map. The *location* of the cycle c_i, $1\le i\le 2^{n-k}$, in this order will be denoted by $L(c_i)$, $0\le L(c_i)\le 2^{n-k}-1$.

Example 1: For $n=6$ and $r=8$ the following eight cycles are a perfect factor in G_6, presented in their zero shift and ordered in ascending order of their zero state:

0) [00000011]
1) [00001001]
2) [00010111]
3) [00011101]
4) [00101011]
5) [00110101]
6) [00111111]
7) [01101111].

For the cycle $c=$[00011101], $L(c)=3$, the zero state is (000111), and its shifts are as follows:

zero shift [00011101],
shift one [00111010],
shift two [01110100],
shift three [11101000],
shift four [11010001],
shift five [10100011],
shift six [01000111],
shift seven [10001110].

B. The Graph Representation

With each perfect factor $\mathrm{PF}(n)$ and each $m\ge 2$ we associate a graph $G_{\mathrm{PF}(n),m}$. The graph has 2^{nm-k} vertices, each one represented by a $2^k\times m$ vertically periodic matrix. Each matrix is an m-state $X=(x_0,(x_1,s_1),\cdots,(x_{m-1},s_{m-1}))$, where x_i is a cycle from $\mathrm{PF}(n)$, $s_i\in\{0,1,\cdots,2^k-1\}$ is the shift of x_i, and x_0 is always taken in its zero shift.

Lemma 1: Each $n\times m$ binary matrix appears exactly once as a window in one of the vertices.

Proof: By induction on m.

Basis: If $m=1$, then each $n\times 1$ binary matrix appears exactly once in one vertex since the vertices represent the cycles of the perfect factor $\mathrm{PF}(n)$ in G_n.

Induction: Assume the claim holds for the $n\times(m-1)$ windows in $G_{\mathrm{PF}(n),m-1}$. Let T_m be an $n\times m$ binary matrix. Let T_{m-1} be the matrix consisting of the first $m-1$ columns of T_m. By the induction hypothesis, T_{m-1} appears exactly once in one vertex of $G_{\mathrm{PF}(n),m-1}$. The vertices of $G_{\mathrm{PF}(n),m}$ can be generated by taking the $2^k\times(m-1)$ matrix of each vertex of $G_{\mathrm{PF}(n),m-1}$ and attaching to its end

all the cycles of PF(n) in all the 2^k possible shifts. Since each binary n-tuple appears as a window in PF(n), one of those shifts attaches the last column of T_m to T_{m-1}.

Q.E.D.

The graph $G_{\mathrm{PF}(n),m}$ has $2^{n(m+1)-k}$ directed edges. From the vertex $X=(x_0,(x_1,s_1),\cdots,(x_{m-1},s_{m-1}))$ there is a directed edge to the vertex $Y=(y_0,(y_1,t_1),\cdots,(y_{m-1},t_{m-1}))$ iff for each j, $1\le j\le m-2$, $(y_j,t_j)=(x_{j+1},s_{j+1}-s_1)$, where $s_{j+1}-s_1$ is taken modulo 2^k, $y_0=x_1$, $y_{m-1}\in \mathrm{PF}(n)$, and $t_{m-1}\in\{0,1,\cdots,2^k-1\}$. Thus for each vertex the out degree is 2^n, and that is also the in degree of the vertex.

The *set of companions* X' of an m-state $X=(x_0,(x_1,s_1),\cdots,(x_{m-2},s_{m-2}),(x_{m-1},s_{m-1}))$ is a set of m-states, where $Y=(y_0,(y_1,t_1),\cdots,(y_{m-2},t_{m-2}),(y_{m-1},t_{m-1}))\in X'$ iff $x_i=y_i$ and $s_i=t_i$ for $i=0,1,\cdots,m-2$, $y_{m-1}\in \mathrm{PF}(n)$, and one of the following holds: either $y_{m-1}\neq x_{m-1}$, and $t_{m-1}\in\{0,1,\cdots,2^k-1\}$, or $y_{m-1}=x_{m-1}$, $t_{m-1}\in\{0,1,\cdots,2^k-1\}$, and $t_{m-1}\neq s_{m-1}$. A cycle $C=[T^{(1)},T^{(2)},\cdots,T^{(q)}]$ in $G_{\mathrm{PF}(n),m}$, where $T^{(i)}$, $1\le i\le q$, are the consecutive vertices of the cycle also can be represented by the $2^k\times(q+m-1)$ matrix $R=[T_0^{(1)}T_0^{(2)}\cdots T_0^{(q)}T_1^{(q)}T_2^{(q)}\cdots T_{m-1}^{(q)}]$, where $T_i^{(j)}$ corresponds to the i column in $T^{(j)}$, and each of the consecutive m columns corresponds to a vertex in $G_{\mathrm{PF}(n),m}$. Note that we can erase the last $m-1$ columns if they are in the same shift as the first $m-1$ columns and consider the matrix R as a doubly periodic matrix. To avoid confusion, however, we will not erase those columns unless the matrix corresponds to a perfect map.

Theorem 1: A sufficient condition for the existence of a $(2^k,2^{nm-k};n,m)$-array, where $n<2^k\le 2^n$ and $m\neq 2$ if $k=n$, is the existence of a Hamiltonian cycle in $G_{\mathrm{PF}(n),m}$.

Proof: By the definition of the matrix representation R of a cycle and Lemma 1, each $n\times m$ window appears in the matrix representation R of the Hamiltonian cycle in $G_{\mathrm{PF}(n),m}$. Hence we only have to prove that the last $m-1$ columns of R, which are the same as the first $m-1$ columns of R, are also in the same shift; this would imply that we can erase the last $m-1$ columns of R to obtain a $(2^k,2^{nm-k};n,m)$-array. For this we have to sum the shifts of the columns of R, where the shift of a column is relative to the shift of the previous column.

In R there are $2^{nm-k+m-1}$ columns. Each of the first 2^{nm-k} columns corresponds to a different vertex in $G_{\mathrm{PF}(n),m}$. There are 2^k possible shifts. Each shift appears $2^{nm-k}/2^k=2^{nm-2k}$ times. Hence the sum on all the shifts is

$$2^{nm-2k}\left(1+2+3+\cdots+(2^k-2)+(2^k-1)\right)$$
$$=(2^k-1)2^{nm-k-1}.$$

Since the vertical size of the array is 2^k, we take this sum modulo 2^k. To get the last $m-1$ columns in the same shift as the first $m-1$ columns, we must have $(2^k-1)2^{nm-k-1}\equiv 0(\mathrm{mod}\,2^k)$ or $nm-2k-1\ge 0$. Since $n>1$ and $m>1$, this implies that we will generate a $(2^k,2^{nm-k};n,m)$-array whenever $n<2^k\le 2^n$ unless both $k=n$ and $m=2$.

Q.E.D.

To generate a Hamiltonian cycle, we take a factor in $G_{\mathrm{PF}(n),m}$ and join the cycles into a single Hamiltonian cycle. This is done using the following theorem which can be easily verified.

Theorem 2: Two adjacent cycles C_1 and C_2, with an m-state X on C_1 and an m-state Y on C_2 such that $Y\in X'$, form a single cycle when the predecessors of X and Y are interchanged (the predecessor of X becomes the predecessor of Y, and the predecessor of Y becomes the predecessor of X).

Example 2: For $n=3$ and $r=4$ the following two cycles are a perfect factor PF(3) in G_3:

0) [0001]
1) [0111].

For $m=3$ we have 128 vertices in $G_{\mathrm{PF}(3),3}$. Consider the following two cycles in $G_{\mathrm{PF}(3),3}$

$$R_1=\begin{bmatrix}00100\\00100\\01001\\10110\end{bmatrix}\qquad R_2=\begin{bmatrix}00000\\00100\\01001\\10010\end{bmatrix}$$

by interchanging the predecessors of the m-states

$$\begin{pmatrix}001\\001\\010\\101\end{pmatrix}\quad\text{and}\quad\begin{pmatrix}000\\001\\010\\100\end{pmatrix}$$

we obtain the cycle

$$R_3=\begin{bmatrix}00000100\\00100100\\01001001\\10010110\end{bmatrix}.$$

Note that in all the cycles of Example 2 the last two columns are in the same shift as the first two columns. This is not always the situation. For example, if for the same perfect factor of Example 2 we look at the case $m=2$, we have 16 vertices. The vertex

$$\begin{pmatrix}00\\01\\00\\10\end{pmatrix}$$

has a self-loop edge. Hence the cycle

$$\begin{bmatrix}00\\01\\00\\10\end{bmatrix}$$

has only one vertex, and the last column is in a different shift from the first column.

C. General Construction of Hamiltonian Cycles

The *necklaces factor* (NF) is a factor of $G_{\mathrm{PF}(n),m}$ which is defined by the following property: $X=(x_0,(x_1,s_1),\cdots,$

$(x_{m-1}, s_{m-1}))$ and $Y = (y_0, (y_1, t_1), \cdots, (y_{m-1}, t_{m-1}))$ are on the same NF cycle iff X is a cyclic shift of Y, i.e., there exists an i such that $y_0 = x_i$ and for each j, $1 \le j \le m-1$, $(y_j, t_j) = (x_{i+j}, s_{i+j} - s_i)$ where subscripts are taken modulo m and $s_{i+j} - s_i$ is taken modulo 2^k. The NF factor in the one-dimensional case was used in the binary case [15], [16] and in the t-ary case [12]–[14] to produce de Bruijn cycles.

The σ-*weight* $W_\sigma(X)$ of an m-state $X = (x_0, (x_1, s_1), \cdots, (x_{m-1}, s_{m-1}))$, where for each x_i, $1 \le i \le m-1$, $L(x_i) \le \sigma$, is the number of x_i in X such that $L(x_i) = \sigma$. The σ-weight $W_\sigma(C)$ of a cycle C from NF is the σ-weight of each of its m-states.

Example 3: In Example 2 the cycle

$$\begin{bmatrix} 00100 \\ 00100 \\ 01001 \\ 10110 \end{bmatrix}$$

has three m-states (recall that the first column of an m-state should be in the zero shift and the other columns are shifted relative to the first column):

$$\begin{pmatrix} 001 \\ 001 \\ 010 \\ 101 \end{pmatrix} \quad \begin{pmatrix} 011 \\ 010 \\ 010 \\ 100 \end{pmatrix} \quad \begin{pmatrix} 001 \\ 110 \\ 100 \\ 100 \end{pmatrix}.$$

Each of these states has the cycle [0001], for which $L([0001]) = 0$, twice as a column, and the cycle [0111], for which $L([0111]) = 1$, once as a column. Hence the 1-weight of each m-state is one, and the 1-weight of their cycle R_1 is one. The cycle

$$\begin{bmatrix} 00000 \\ 00100 \\ 01001 \\ 10010 \end{bmatrix}$$

has 1-weight zero since all its m-states

$$\begin{pmatrix} 000 \\ 001 \\ 010 \\ 100 \end{pmatrix}, \begin{pmatrix} 001 \\ 000 \\ 010 \\ 100 \end{pmatrix}, \text{ and } \begin{pmatrix} 001 \\ 010 \\ 000 \\ 100 \end{pmatrix},$$

have only cycles with location less than one.

Lemma 2: Let C_1 be a cycle of σ-weight q, where $\sigma > 0$ and $q > 0$, from NF. Then an m-state X exists on C_1 with an m-state $Y \in X'$ such that Y is on a cycle C_2 whose σ-weight is $q-1$.

Proof: Since $W_\sigma(C_1) = q > 0$, an m-state exists of the form $X = (x_0, (x_1, s_1), \cdots, (x_{m-2}, s_{m-2}), (x_{m-1}, s_{m-1}))$, where $L(x_{m-1}) = \sigma$, on C_1. Hence each m-state of the form $Y = (x_0, (x_1, s_1), \cdots, (x_{m-2}, s_{m-2}), (y_{m-1}, t_{m-1}))$, where $L(y_{m-1}) < \sigma$, has σ-weight $q-1$. Therefore, $Y = (x_0, (x_1, s_1), \cdots, (x_{m-2}, s_{m-2}), (y_{m-1}, t_{m-1}))$ is an m-state on an NF-cycle C_2 with $W_\sigma(C_2) = q-1$ and $Y \in X'$. Q.E.D.

The *shift weight* $\mathrm{SW}(X)$ of an m-state $X = (x, (x, s_1), \cdots, (x, s_{m-1}))$, where $L(x) = 0$, is the number of values of i for which s_i is not zero. The shift weight $\mathrm{SW}(C)$ of a cycle C from NF, where $W_1(C) = 0$, is the minimum shift weight among its m-states.

Example 4: For the same parameters of Example 2 and

$$R_2 = \begin{bmatrix} 00000 \\ 00100 \\ 01001 \\ 10010 \end{bmatrix} \quad R_4 = \begin{bmatrix} 000 \\ 000 \\ 000 \\ 111 \end{bmatrix} \quad R_5 = \begin{bmatrix} 00000 \\ 00000 \\ 00100 \\ 11011 \end{bmatrix}$$

R_2 has three m-states, e.g.,

$$\begin{pmatrix} 000 \\ 001 \\ 010 \\ 100 \end{pmatrix},$$

each one with shift weight 2 since all the columns are shifts of [0001], for which $L([0001]) = 0$, and two columns are not in the zero shift, and hence $\mathrm{SW}(R_2) = 2$. R_4 has one m-state

$$\begin{pmatrix} 000 \\ 000 \\ 000 \\ 111 \end{pmatrix},$$

with shift weight 0 since all the columns are in the zero shift of [0001], and hence $\mathrm{SW}(R_4) = 0$. R_5 has two m-states with shift weight 1

$$\begin{pmatrix} 000 \\ 000 \\ 001 \\ 110 \end{pmatrix} \text{ and } \begin{pmatrix} 000 \\ 000 \\ 010 \\ 101 \end{pmatrix}$$

and one m-state with shift-weight 2,

$$\begin{pmatrix} 011 \\ 000 \\ 000 \\ 100 \end{pmatrix}$$

and hence $\mathrm{SW}(R_5) = 1$.

Lemma 3: Let C_1 be a cycle with shift weight $q > 0$ from NF. Then an m-state X exists on C_1 with an m-state $Y \in X'$ such that Y is on a cycle C_2 whose shift weight is $q-1$.

Proof: Since $\mathrm{SW}(C_1) = q > 0$, an m-state exists of the form $X = (x, (x, s_1), \cdots, (x, s_{m-2}), (x, s_{m-1}))$, where $L(x) = 0$, $s_{m-1} > 0$ {if $s_{m-1} = 0$ we can take $(x, (x, 0), (x, s_1), \cdots, (x, s_{m-2}))$}, and $\mathrm{SW}(X) = q$, on C_1. Hence the m-state $Y = (x, (x, s_1), \cdots, (x, s_{m-2}), (x, 0))$ has shift weight $q-1$. Therefore, $Y = (x, (x, s_1), \cdots, (x, s_{m-2}), (x, 0))$ is an m-state on an NF-cycle C_2 with $\mathrm{SW}(C_2) = q-1$ and $Y \in X'$. Q.E.D.

Construction A: Lemmas 2 and 3, along with Theorem 2, suggest a simple method of joining all the NF-cycles to construct a Hamiltonian cycle in $G_{\mathrm{PF}(n),m}$. At each step we have a main cycle obtained in the previous steps by joining a subset of the NF-cycles. Initially, the main cycle contains all the m-states of 1-weight zero. This cycle is constructed in $m+1$ initial steps. In initial step 0 the main cycle is the unique cycle of 1-weight zero and shift weight zero. Before initial step q, $1 \le q \le m$, the main cycle contains all the

m-states with 1-weight zero and shift weight less than or equal to $q-1$. In step q we extend the main cycle by joining to it all the NF-cycles of 1-weight zero and shift weight q (in arbitrary order). This is always possible because the current main cycle contains all of the states whose shift weight is less than q and since each NF-cycle of shift weight $q \geq 1$ has an m-state of the form $X = (x,(x,s_1),\cdots,(x,s_{m-2}),(x,s_{m-1}))$, where $L(x)=0$, $s_{m-1} > 0$, and SW $(X) = q$, it can be joined (see Theorem 2 and Lemma 3) to the current main cycle. After all the NF-cycles with 1-weight zero have been joined to the main cycle, the main cycle is extended by adjoining all the cycles of 1-weight one. In the general step $jm+i$, $(0 \leq j \leq 2^{n-k}-2$, $1 \leq i \leq m)$, we extend the main cycle by adjoining all the NF-cycles of $(j+1)$-weight i (in arbitrary order). This is always possible because the current main cycle contains all of the states whose $(j+1)$-weight is less than i and since each NF-cycle of $(j+1)$-weight $i \geq 1$ has an m-state of the form $X = (x_0,(x_1,s_1),\cdots,(x_{m-2},s_{m-2}),(x_{m-1},s_{m-1}))$, where $L(x_{m-1}) = j+1$, it can be joined (see Theorem 2 and Lemma 2) to the current main cycle. This procedure ends when all the NF-cycles have been joined together. An immediate consequence is the following theorem.

Theorem 3: Construction A produces a Hamiltonian cycle in $G_{\mathrm{PF}(n),m}$.

A specific procedure for generating the bits of the perfect maps can be given in a way that is similar to the procedure for generating t-ary de Bruijn cycles in [14]. Note that we can choose the zero states, order the cycles of PF(n), and choose the m-states through which we perform the join in many alternative ways, thereby forming many different perfect maps of the same size.

D. The Existence of Perfect Factors

To apply Construction A to generate $(r, v; n, m)$-arrays we must show the existence of perfect factors. This is an interesting question in shift register theory. We show that, for each k and n such that $k \leq n < 2^k$, a factor exists in G_n with 2^{n-k} cycles of length 2^k. For this we introduce the idea of linear complexity of a binary cycle.

Every binary sequence (cycle) $S = [s_0 s_1 \cdots s_{q-1}]$ satisfies a linear recursion

$$s_{i+d} + \sum_{j=1}^{d} a_j s_{i+d-j} = 0, \qquad i \geq 0$$

where d, the degree of the recursion, is less than or equal to *length*(S). In terms of the *shift operator* $\boldsymbol{E}$, defined by

$$\boldsymbol{E}[s_0, s_1, \cdots, s_{q-1}] = [s_1, s_2, \cdots, s_{q-1}, s_0],$$

the linear recursion takes the form

$$f(\boldsymbol{E})S = \left(\boldsymbol{E}^d + \sum_{j=1}^{d} a_j \boldsymbol{E}^{d-j}\right) S = 0^q$$

where a^q denotes a sequence of q a's.

The (linear) *complexity* $C(S)$ of S is defined as the least integer c for which there exists a polynomial $f(\boldsymbol{E})$ of degree c such that $f(\boldsymbol{E})S = 0^{\mathrm{length}}(S)$. For future reference purposes, we state the following known fact.

Fact 1[10], [17]: If S is a sequence whose length is a power of 2, then $C(S) = c$ if and only if $(\boldsymbol{E}+1)^{c-1}S = 1^{\mathrm{length}(S)}$.

For the proof of the existence of perfect factors we also need the ***D-morphism*** operator $\boldsymbol{D}$ for de Bruijn graphs and its inverse $\boldsymbol{D}^{-1}$ as defined by Lempel [18]. When applied to a sequence, $\boldsymbol{D}$ can be viewed as being equivalent to the operator $\boldsymbol{E}+1$ (see [17]). That is, for $S = [s_0, s_1, s_2, \cdots, s_{q-1}]$,

$$\begin{aligned}\boldsymbol{D}S &= (\boldsymbol{E}+1)S \\ &= [s_0+s_1, s_1+s_2, \cdots, s_{q-2}+s_{q-1}, s_{q-1}+s_0].\end{aligned}$$

When applied to individual states, $\boldsymbol{D}$ effects a two-to-one map from B^n (the set of all binary n-tuples) onto B^{n-1}. Thus $\boldsymbol{D}^{-1}$, when applied to a sequence $S = [s_0, s_1, s_2, \cdots, s_{q-1}]$ of even weight (the number of ones in S is even), yields a pair of complementary sequences:

$$\boldsymbol{D}^{-1}S = \left\{\left[0, s_0, s_0+s_1, \cdots, \sum_{i=0}^{q-2} s_i\right], \left[1, 1+s_0, 1+s_0+s_1, \cdots, 1+\sum_{i=0}^{q-2} s_i\right]\right\}$$

while when the weight of S is odd, the image of $\boldsymbol{D}^{-1}$ is a self-dual cycle:

$$\boldsymbol{D}^{-1}S = \left[0, s_0, s_0+s_1, \cdots, \sum_{i=0}^{q-2} s_i, 1, 1+s_0, 1+s_0+s_1, \cdots, 1+\sum_{i=0}^{q-2} s_i\right].$$

It also follows from the definition of $\boldsymbol{D}$ (see [17]) that if $f(\boldsymbol{E})S = 0$ and $\boldsymbol{E}+1$ is a factor of $f(\boldsymbol{E})$, then $C(\boldsymbol{D}S) = C(S)-1$. Hence by Fact 1 we obtain Fact 2.

Fact 2: Let *length*(S) be a power of 2. Then $C(\boldsymbol{D}^{-1}S) = C(S)+1$.

Another important fact was obtained in [17].

Fact 3: Let *length*$(S) = 2^n$. Then $C(S) = 2^n$ if and only if the weight of S is odd.

For a de Bruijn sequence S of length 2^n we have [17], $2^{n-1}+n \leq C(s) \leq 2^n-1$. Etzion and Lempel [19] proved that for all $n \geq 1$, the lower bound $2^{n-1}+n$ is attainable, i.e., there exists a de Bruijn sequence of order n and linear complexity $2^{n-1}+n$. They also gave a method of constructing such sequences. Another class of interesting sequences appears in the following lemma.

Lemma 4 [19], [20]: Let $M(n)$ denote a maximal set of sequences of length $2^{\lfloor \log n \rfloor + 1}$ and complexity $n+1$. Then each $S \in M(n)$ satisfies $(\boldsymbol{E}+1)^n S = 1^{\mathrm{length}(S)}$, the cardinality of $M(n)$ is $|M(n)| = 2^{n-\lfloor \log n \rfloor - 1}$, and each of the 2^n binary n-tuples appears exactly once in one of the members of $M(n)$.

Now we can state our main result on perfect factors in G_n.

Theorem 4: Let n and k be integers such that $k \leq n < 2^k$. Then a perfect factor exists in G_n with 2^{n-k} cycles of length 2^k.

Proof: We distinguish between two cases. In Case 1, $2^{k-1} < n < 2^k$. This case is covered by Lemma 4.

In Case 2, $k \leq n \leq 2^{k-1}$. Let S be a de Bruijn sequence of length 2^k and minimal complexity $2^{k-1}+k$. Apply $\boldsymbol{D}^{-(n-k)}$ on S to get sequences with complexity $2^{k-1}+n \leq 2^k$ (by Fact 2). By the definition of $\boldsymbol{D}$ and Fact 3 those sequences are a factor in $G_{k-n-k} = G_n$ and have length 2^k. Hence $\boldsymbol{D}^{-(n-k)}S$ is a factor in G_n which consists of 2^{n-k} sequences of length 2^k. Q.E.D.

Corollary 1: Let n and k be integers such that $n < 2^k \leq 2^n$. Then a perfect factor exists in G_n with 2^{n-k} cycles of length 2^k.

Corollary 1 shows the existence of perfect factors for all possible values of k and n, $n < 2^k \leq 2^n$. Thus Construction A can be applied for all those values.

Example 5: Assume we wish to construct a $(4,128;3,3)$-array. We take the factor in G_3 with the cycles [0001] and [0111]. $G_{\mathrm{PF}(3),3}$ has 128 vertices and the NF in $G_{\mathrm{PF}(3),3}$ contains 44 cycles of which 42 cycles have three vertices each and 2 cycles have one vertex each as follows.

Six cycles with 1-weight zero:

$$R_0 = \begin{bmatrix} 000 \\ 000 \\ 000 \\ 111 \end{bmatrix} \quad R_1 = \begin{bmatrix} 00000 \\ 00000 \\ 00100 \\ 11011 \end{bmatrix} \quad R_2 = \begin{bmatrix} 00000 \\ 00100 \\ 00000 \\ 11011 \end{bmatrix}$$

$$R_3 = \begin{bmatrix} 00100 \\ 00000 \\ 00000 \\ 11011 \end{bmatrix} \quad R_4 = \begin{bmatrix} 00000 \\ 00100 \\ 01001 \\ 10010 \end{bmatrix} \quad R_5 = \begin{bmatrix} 00000 \\ 01001 \\ 00100 \\ 10010 \end{bmatrix};$$

16 cycles with 1-weight one:

$$R_6 = \begin{bmatrix} 00000 \\ 00100 \\ 00100 \\ 11111 \end{bmatrix} \quad R_7 = \begin{bmatrix} 00100 \\ 00100 \\ 00100 \\ 11011 \end{bmatrix} \quad R_8 = \begin{bmatrix} 00100 \\ 00100 \\ 00000 \\ 11111 \end{bmatrix} \quad R_9 = \begin{bmatrix} 00100 \\ 00000 \\ 00100 \\ 11111 \end{bmatrix}$$

$$R_{10} = \begin{bmatrix} 00000 \\ 00100 \\ 01101 \\ 10110 \end{bmatrix} \quad R_{11} = \begin{bmatrix} 00100 \\ 00100 \\ 01101 \\ 10010 \end{bmatrix} \quad R_{12} = \begin{bmatrix} 00100 \\ 00100 \\ 01001 \\ 10110 \end{bmatrix} \quad R_{13} = \begin{bmatrix} 00100 \\ 00000 \\ 01101 \\ 10110 \end{bmatrix}$$

$$R_{14} = \begin{bmatrix} 00000 \\ 01101 \\ 00100 \\ 10110 \end{bmatrix} \quad R_{15} = \begin{bmatrix} 00100 \\ 01101 \\ 00100 \\ 10010 \end{bmatrix} \quad R_{16} = \begin{bmatrix} 00100 \\ 01101 \\ 00000 \\ 10110 \end{bmatrix} \quad R_{17} = \begin{bmatrix} 00100 \\ 01001 \\ 00100 \\ 10110 \end{bmatrix}$$

$$R_{18} = \begin{bmatrix} 01001 \\ 00100 \\ 00100 \\ 10110 \end{bmatrix} \quad R_{19} = \begin{bmatrix} 01101 \\ 00100 \\ 00100 \\ 10010 \end{bmatrix} \quad R_{20} = \begin{bmatrix} 01101 \\ 00100 \\ 00000 \\ 10110 \end{bmatrix} \quad R_{21} = \begin{bmatrix} 01101 \\ 00000 \\ 00100 \\ 10110 \end{bmatrix};$$

16 cycles with 1-weight two:

$$R_{22} = \begin{bmatrix} 00000 \\ 11011 \\ 11011 \\ 11111 \end{bmatrix} \quad R_{23} = \begin{bmatrix} 00000 \\ 11011 \\ 11111 \\ 11011 \end{bmatrix} \quad R_{24} = \begin{bmatrix} 00000 \\ 11111 \\ 11011 \\ 11011 \end{bmatrix}$$

$$R_{25} = \begin{bmatrix} 00100 \\ 11011 \\ 11011 \\ 11011 \end{bmatrix} \quad R_{26} = \begin{bmatrix} 01001 \\ 11011 \\ 11011 \\ 10110 \end{bmatrix} \quad R_{27} = \begin{bmatrix} 01001 \\ 11011 \\ 11111 \\ 10010 \end{bmatrix}$$

$$R_{28} = \begin{bmatrix} 01001 \\ 11111 \\ 11011 \\ 10010 \end{bmatrix} \quad R_{29} = \begin{bmatrix} 01101 \\ 11011 \\ 11011 \\ 10010 \end{bmatrix} \quad R_{30} = \begin{bmatrix} 01001 \\ 11011 \\ 10010 \\ 11111 \end{bmatrix}$$

$$R_{31} = \begin{bmatrix} 01001 \\ 11011 \\ 10110 \\ 11011 \end{bmatrix} \quad R_{32} = \begin{bmatrix} 01001 \\ 11111 \\ 10010 \\ 11011 \end{bmatrix} \quad R_{33} = \begin{bmatrix} 01101 \\ 11011 \\ 10010 \\ 11011 \end{bmatrix}$$

$$R_{34} = \begin{bmatrix} 01001 \\ 10010 \\ 11011 \\ 11111 \end{bmatrix} \quad R_{35} = \begin{bmatrix} 01001 \\ 10010 \\ 11111 \\ 11011 \end{bmatrix} \quad R_{36} = \begin{bmatrix} 01001 \\ 10110 \\ 11011 \\ 11011 \end{bmatrix}$$

$$R_{37} = \begin{bmatrix} 01101 \\ 10010 \\ 11011 \\ 11011 \end{bmatrix};$$

six cycles with 1-weight three:

$$R_{38} = \begin{bmatrix} 000 \\ 111 \\ 111 \\ 111 \end{bmatrix} \quad R_{39} = \begin{bmatrix} 00100 \\ 11111 \\ 11111 \\ 11011 \end{bmatrix} \quad R_{40} = \begin{bmatrix} 00100 \\ 11111 \\ 11011 \\ 11111 \end{bmatrix}$$

$$R_{41} = \begin{bmatrix} 00100 \\ 11011 \\ 11111 \\ 11111 \end{bmatrix} \quad R_{42} = \begin{bmatrix} 01101 \\ 11111 \\ 11011 \\ 10110 \end{bmatrix} \quad R_{43} = \begin{bmatrix} 01101 \\ 11011 \\ 11111 \\ 10110 \end{bmatrix}.$$

By applying Construction A to join the cycles with 1-weight zero we can obtain the following cycle:

$$\begin{bmatrix} 000000000000000100 \\ 000010000100100000 \\ 000100100010000000 \\ 111001011001011011 \end{bmatrix}.$$

Applying Construction A to the remaining NF-cycles, we obtain the following (4,128; 3,3)-array which is divided into two parts consisting of its first and last 64 columns, respectively. Note that the last two columns of the cycle representation were erased along with the outside braces:

```
0000001001001000010010010000000100100100001001001000010010010000|
0011011011010010010010000000111111111011011011010010010000010|
0011011010011010010000010001111111011111111111011111011010011010|
1111110111111111110111111111101110111111110100110110110011011001|

|0000000010010010000100100100000001001011011011011000101101101
|0001111111111110110110110100100100011011111011011010010110010000
|1000110110100110100100000100100000110110111110100110100100000100
|0110110100110110110010110110010110110101101100110110110010110110
```

Choosing different m-states through which the joining of the NF-cycles is performed, or joining some of the NF-cycles in different order, will result in different perfect maps.

IV. Pseudorandom Arrays

Let $2^n-1=d_1d_2$. If a factor of G_n exists with the cycle [0] and d_1 cycles of length d_2, where $d_2>n$, then a pseudorandom array exists of size $d_2\times d_1(2^{n(m-1)}+2^{n(m-2)}+\cdots+2^n+1)$ with the $n\times m$ window property. In this array all the nonzero $n\times m$ binary matrices appear as windows. A factor with the cycle [0] and d_1 cycles of length d_2 will be called a zero factor with *exponent* d_2 and will be denoted by ZF(n). The theory of linear feedback shift registers gives many examples of zero factors. Each feedback shift register $f(x_0,x_1,\cdots,x_{n-1})=\sum_{i=0}^{n-1}a_ix_i$ has a *characteristic polynomial* $f(x)=1+\sum_{i=0}^{n-1}a_ix_i$.

Theorem 5 [9]: If the characteristic polynomial $f(x)$ of a shift register is irreducible, then the shift register produces a zero factor with exponent d, where d is the smallest integer such that $f(x)$ divides $1-x^d$.

Theorem 6 [9]: Every factor e of 2^n-1 which is not a factor of any number 2^d-1 with $d<n$ occurs as the exponent of a zero cycle which corresponds to an irreducible polynomial of degree n. There are $\phi(e)/n$ irreducible polynomials which correspond to zero factors with exponent e, where ϕ is the Euler function.

Another result which follows directly from the theory of linear shift registers [9] is the following theorem.

Theorem 7: Let $f_i(x)$, $1\le i\le q$, be q different irreducible polynomials of degree n, and let their corresponding shift registers have zero factors with exponent e. Then the feedback shift register which has the characteristic polynomial $\prod_{i=1}^{k}f_i(x)$ produces a zero factor with exponent e.

Tables of irreducible polynomials are readily available in the literature [21]–[23]. The first value which is not covered by Theorems 5–7 is a zero factor with exponent 15 in G_{12}, and the next value is a zero factor with exponent 21 in G_{18}. A problem of considerable interest arises here: if $2^n-1=d_1d_2$, where $d_2>n$, does there exist a factor of G_n which contains the cycle [0] and d_1 cycles of length d_2?

Example 6: To obtain a zero factor with nine cycles of length 7 in G_6 we take two irreducible polynomials of degree 3 which correspond to two shift registers with a zero factor of exponent 7 and multiply them to obtain the desired factor. Hence the characteristic polynomial $f(x)=(x^3+x^2+1)(x^3+x+1)=x^6+x^5+x^4+x^3+x^2+x+1$, and its corresponding shift register with the function $f(x_0,x_1,\cdots,x_5)=x_0\oplus x_1\oplus\cdots\oplus x_5$ has a zero factor with exponent 7. The zero factor in G_6 contains the cycle [0] and the following nine cycles of length 7:

1) [0000011]
2) [0000101]
3) [0001001]
4) [0001111]
5) [0010111]
6) [0011011]
7) [0011101]
8) [0101011]
9) [0111111].

The construction of the pseudorandom arrays is similar to Construction A. We generate a graph $G_{\mathrm{ZF}(n),m}$ from the zero factor ZF(n). In this graph only the zero matrix does not appear as a window in some vertex, and the zero cycle of ZF(n) is taken in its only shift, the zero shift.

Theorem 8: Let ZF(n) be a zero factor in G_n. If Construction A is applied on $G_{\mathrm{ZF}(n),m}$, the result is a pseudorandom array for all the values of m.

Proof: This is a similar claim to the one in Theorem 1, but we do not have to sum the shifts. Since the array has $m-1$ consecutive columns of zeros, we can arrange the array (from the general Hamiltonian cycle) in such a way that the first $m-1$ columns are the same as the last $m-1$ columns. Q.E.D.

Example 7: From the sequence [000111101100101] of length 15 in G_4 we can generate the following 15×17

pseudorandom array with the 4×2 window property:

00111101010111100
00000100100100000
00010000100001000
11001111111110010
11100110101100110
11101011011010110
11110010101001110
00110100100101100
11010010001001010
11111111011111110
00101001110010100
00011001010011000
11011011111011010
00100100000100100
11001111011110010.

Note that each of the 16 zero factors with exponent 15 in G_4 will work equally well.

If we have a factor of G_n with d_1 cycles of length d_2 and d_1d_2 is close to 2^n, we can generate a pseudorandom array in which only a few $n\times m$ binary matrices do not appear. This construction is illustrated in the following example.

Example 8: In G_4 we have a factor $F(4)$ with three cycles of length 4, one of length 2, and two of length 1:

0) [0001]
1) [0011]
2) [0111]
3) [01]
4) [0]
5) [1].

We can construct a 4×60 array with the 4×2 window property in which only 16 4×2 matrices do not appear. $G_{F(4),2}$ has 60 vertices and the NF in $G_{F(4),2}$ contains 33 cycles as follows.

Three cycles with 1-weight zero:

$$R_0=\begin{bmatrix}00\\00\\00\\11\end{bmatrix}\quad R_1=\begin{bmatrix}000\\000\\010\\101\end{bmatrix}\quad R_2=\begin{bmatrix}00\\01\\00\\10\end{bmatrix};$$

four cycles with 1-weight one:

$$R_3=\begin{bmatrix}000\\000\\101\\111\end{bmatrix}\quad R_4=\begin{bmatrix}000\\000\\111\\101\end{bmatrix}\quad R_5=\begin{bmatrix}000\\010\\101\\101\end{bmatrix}$$

$$R_6=\begin{bmatrix}010\\000\\101\\101\end{bmatrix};$$

three cycles with 1-weight two:

$$R_7=\begin{bmatrix}00\\00\\11\\11\end{bmatrix}\quad R_8=\begin{bmatrix}000\\010\\111\\101\end{bmatrix}\quad R_9=\begin{bmatrix}01\\01\\10\\10\end{bmatrix};$$

eight cycles with 2-weight one:

$$R_{10}=\begin{bmatrix}000\\101\\101\\111\end{bmatrix}\quad R_{11}=\begin{bmatrix}000\\101\\111\\101\end{bmatrix}\quad R_{12}\begin{bmatrix}000\\111\\101\\101\end{bmatrix}$$

$$R_{13}=\begin{bmatrix}010\\101\\101\\101\end{bmatrix}\quad R_{14}=\begin{bmatrix}000\\101\\111\\111\end{bmatrix}\quad R_{15}=\begin{bmatrix}000\\111\\111\\101\end{bmatrix}$$

$$R_{16}=\begin{bmatrix}010\\111\\101\\101\end{bmatrix}\quad R_{17}=\begin{bmatrix}010\\101\\101\\111\end{bmatrix};$$

three cycles with 2-weight two:

$$R_{18}=\begin{bmatrix}00\\11\\11\\11\end{bmatrix}\quad R_{19}=\begin{bmatrix}010\\111\\111\\101\end{bmatrix}\quad R_{20}=\begin{bmatrix}01\\11\\10\\11\end{bmatrix};$$

six cycles with 3-weight one:

$$R_{21}=\begin{bmatrix}000\\101\\000\\111\end{bmatrix}\quad R_{22}=\begin{bmatrix}000\\101\\010\\101\end{bmatrix}\quad R_{23}=\begin{bmatrix}000\\101\\010\\111\end{bmatrix}$$

$$R_{24}=\begin{bmatrix}000\\111\\010\\101\end{bmatrix}\quad R_{25}=\begin{bmatrix}000\\111\\010\\111\end{bmatrix}\quad R_{26}=\begin{bmatrix}010\\111\\010\\101\end{bmatrix};$$

three cycles with 4-weight one:

$$R_{27}=\begin{bmatrix}000\\000\\000\\010\end{bmatrix}\quad R_{28}=\begin{bmatrix}000\\000\\010\\010\end{bmatrix}\quad R_{29}=\begin{bmatrix}000\\010\\010\\010\end{bmatrix};$$

three cycles with 5-weight one:

$$R_{30}=\begin{bmatrix}101\\101\\101\\111\end{bmatrix}\quad R_{31}=\begin{bmatrix}101\\101\\111\\111\end{bmatrix}\quad R_{32}=\begin{bmatrix}101\\111\\111\\111\end{bmatrix}.$$

Applying Construction A to these 33 NF-cycles we obtain the following 4×60 array:

000001010101000000101000000010001010101001011110010001000100
000100010100011101110100000010100010100011111111111101010110
000001010001010101111101010111011111011111100000101010010100
101110101111111101110110110111110101111110111000000010101101.

Only the following 16 4×2 binary matrices do not appear as windows in this 4×60 array:

$$w_1=\begin{Bmatrix}00\\00\\00\\00\end{Bmatrix}\quad w_2=\begin{Bmatrix}00\\01\\00\\01\end{Bmatrix}\quad w_3=\begin{Bmatrix}01\\00\\01\\00\end{Bmatrix}\quad w_4=\begin{Bmatrix}00\\10\\00\\10\end{Bmatrix}$$

$$w_5=\begin{Bmatrix}10\\00\\10\\00\end{Bmatrix}\quad w_6=\begin{Bmatrix}01\\01\\01\\01\end{Bmatrix}\quad w_7=\begin{Bmatrix}10\\10\\10\\10\end{Bmatrix}\quad w_8=\begin{Bmatrix}00\\11\\00\\11\end{Bmatrix}$$

$$w_9=\begin{Bmatrix}11\\00\\11\\00\end{Bmatrix}\quad w_{10}=\begin{Bmatrix}01\\10\\01\\10\end{Bmatrix}\quad w_{11}=\begin{Bmatrix}10\\01\\10\\01\end{Bmatrix}\quad w_{12}=\begin{Bmatrix}01\\11\\01\\11\end{Bmatrix}$$

$$w_{13}=\begin{Bmatrix}11\\01\\11\\01\end{Bmatrix}\quad w_{14}=\begin{Bmatrix}10\\11\\10\\11\end{Bmatrix}\quad w_{15}=\begin{Bmatrix}11\\10\\11\\10\end{Bmatrix}\quad w_{16}=\begin{Bmatrix}11\\11\\11\\11\end{Bmatrix}.$$

V. Nonbinary Perfect Maps and Pseudorandom Arrays

The same constructions can be used to obtain perfect maps and pseudorandom arrays with entries which, instead of being 0's, and 1's are taken from an alphabet of t symbols. Sometimes, however, we can get perfect maps with values which are not obtained in Theorem 1. As an example, for odd t and $m=2$ we can take a t-ary de Bruijn sequence of order n and form a t-ary $(t^n, t^n; n, 2)$-array. In column number one we put the de Bruijn sequence in some shift. In column i, $2\le i\le t^n$, we put the sequence shifted in $i-1$ positions relative to the sequence in column $i-1$. The only missing shift is the zero shift. This one will occur if the last column is the same as the first column. As in the proof of Theorem 1 we have to sum all the shifts

$$1+2+3+\cdots+(t^n-2)+(t^n-1)=(t^n-1)\frac{t^n}{2},$$

and it is easy to verify that $(t^n-1)t^n/2\equiv 0(\mathrm{mod}\, t^n)$, and hence the last column is the same as the first one and the array is a t-ary $(t^n, t^n; n, 2)$-array.

Example 9: For $t=3$ the sequence [001122021] is a 3-ary de Bruijn sequence of order two, and the following array is a 3-ary $(9, 9; 2, 2)$-array:

010111010
002202200
101202101
110010011
210212012
221121122
021020120
202000202
122121221.

Again, in general, applying a construction similar to Construction A for generating perfect maps involves the existence of a perfect factor in $G_{n,t}$, i.e., a factor with d_1 cycles of length d_2, where $t^n=d_1d_2$. The existence of pseudorandom arrays in which only the zero matrix does not appear involves the existence of a zero factor in $G_{n,t}$, i.e., a factor with the cycle [0] and d_1 cycles of length d_2, where $t^n-1=d_1d_2$. The solution to those two questions is of considerable interest.

Acknowledgment

The author wishes to thank Prof. Solomon W. Golomb, Prof. Herbert Taylor, and Prof. Harold M. Fredricksen for many valuable discussions. Prof. Taylor's help in editing the paper is also gratefully acknowledged.

References

[1] I. S. Reed and R. M. Stewart, "Note on the existence of perfect maps," *IRE Trans. Inform. Theory*, vol. IT-8, pp. 10–12, Jan. 1962.
[2] S. L. Ma, "A note on binary arrays with a certain window property," *IEEE Trans. Inform. Theory*, vol. IT-30, pp. 774–775, Sept. 1984.
[3] C. T. Fan, S. M. Fan, S. L. Ma, and M. K. Siu, "On de Bruijn arrays," *Ars Combinatoria*, vol. 19A, pp. 205–213, May 1985.
[4] B. Gordon, "On the existence of perfect maps," *IEEE Trans. Inform. Theory*, vol. IT-12, pp. 486–487, Oct. 1966.
[5] F. J. MacWilliams and N. J. A. Sloane, "Pseudo-random sequences and arrays," *Proc. IEEE*, vol. 64, pp. 1715–1729, Dec. 1976.
[6] T. Nomura, H. Miyakawa, H. Imai, and A. Fukuda, "A theory of two-dimensional linear recurring arrays," *IEEE Trans. Inform. Theory*, vol. IT-18, pp. 775–785, Nov. 1972.
[7] J. H. van Lint, F. J. MacWilliams, and N. J. A. Sloane, "On pseudo-random arrays," *SIAM J. Appl. Math.*, vol. 36, pp. 62–72, Feb. 1979.
[8] N. G. de Bruijn, "A combinatorial problem," *Nederl. Akad. Wetensch. Proc.*, vol. 49, pp. 758–764, 1946.
[9] S. W. Golomb, *Shift Register Sequences*. Laguna Hills, CA: Aegean Park Press, 1982.
[10] H. M. Fredricksen, "A survey of full length nonlinear shift register cycle algorithms," *SIAM Rev.*, vol. 24, pp. 195–221, Apr. 1982.
[11] T. van Aardenne-Ehrenfest and N. G. de Bruijn, "Circuits and trees in ordered linear graphs," *Simon Steven*, vol. 28, pp. 203–217, 1951.
[12] H. M. Fredricksen and J. Maiorana, "Necklaces of beads in k colors and k-ary de Bruijn sequences," *Discrete Math.*, vol. 23, pp. 207–210, Sept. 1978.
[13] A. Ralston, "A new memoryless algorithm for de Bruijn sequences," *J. Algorithms*, vol. 2, pp. 50–62, Mar. 1981.
[14] T. Etzion, "An algorithm for constructing m-ary de Bruijn sequences," *J. Algorithms*, vol. 7, pp. 331–340, Sept. 1986.
[15] H. Fredricksen, "A class of non-linear de Bruijn cycles," *J. Combin. Theory*, Ser. A, vol. 19, pp. 191–199, Sept. 1975.
[16] T. Etzion and A. Lempel, "Algorithms for the generation of full-length shift-register sequences," *IEEE Trans. Inform. Theory*, vol. IT-30, pp. 480–484, May 1984.
[17] A. H. Chan, R. A. Games, and E. L. Key, "On the complexities of de Bruijn sequences," *J. Combin. Theory*, Ser. A, vol. 33, pp. 233–246, Nov. 1982.
[18] A. Lempel, "On a homomorphism of the de Bruijn graph and its applications to the design of feedback shift registers," *IEEE Trans. Comput.*, vol. C-19, pp. 1204–1209, Dec. 1970.
[19] T. Etzion and A. Lempel, "Construction of de Bruijn sequences of minimal complexity," *IEEE Trans. Inform. Theory*, vol. IT-30, pp. 705–709, Sept. 1984.
[20] B. Elspas, "Theory of autonomous linear sequential networks," *IRE Trans. Circuit Theory*, vol. CT-6, pp. 45–60, Mar. 1959.
[21] R. W. Marsh, "Tables of irreducible polynomials over GF(2) through degree 19," United States Dept. of Commerce, Washington, DC, 1957.
[22] J. D. Alanen and D. E. Knuth, "Tables of finite fields," *Sankhya*, Ser. A, vol. 26, pp. 305–328, Dec. 1964.
[23] S. Mossige, "Tables of irreducible polynomials over GF[2] of degree 10 through 20," *Math. Comput.*, vol. 26, pp. 1007–1009, Oct. 1972.