DEMONSTRATIO MATHEMATICA
Vol. XX No 3-4 1987

Marek Łatko

# ON A CONSTRUCTION OF ALL DE BRUIJN CYCLES DEFINED BY LEMPEL'S HOMOMORPHISM

## 1. Introduction

The de Bruijn graph $G_n$ is a directed graph which vertices are elements of the set $B^n = \{0,1\}^n$. Two vertices $\underline{x} = (x_1,x_2,\ldots,x_n)$ and $\underline{y} = (y_1,y_2,\ldots,y_n)$ are joined by an arc directed from $\underline{x}$ to $\underline{y}$ ($\underline{y}$ is a successor of $\underline{x}$) iff $y_i = x_{i+1}$, for $i=1,\ldots,n-1$. A factor of $G_n$ is each of its subgraphs formed by a set of disjoint cycles, containing all the vertices $G_n$. There is a one-to-one relation between each factor of $G_n$ and a certain boolean function $f:B^n \to B$ which determines connections among vertices in the cycles of the factor of $G_n$. A vertex $(x_1,x_2,\ldots,x_n)$ is connected with a vertex $(x_2,\ldots,x_n,f(x_1,\ldots,x_n))$ in a factor of $G_n$ determined by the function f.

There exist $2^{2^{n-1}-n}$ factors of $G_n$, each of which has a cycle enfolding all vertices of $G_n$ [1]. Such a cycle is called the de Bruijn cycle of span n. The problem of determination of de Bruijn cycles is a basic problem of the theory of de Bruijn graphs. Fredricksen [3] reviewed methods of determining such cycles. Most of these methods are based upon Yoeli's [8] theorem describing the ways of joining and disjoining of the cycles, e.g. if two conjugated vertices $\underline{x} = (x_1,x_2,\ldots,x_n)$ and $\hat{\underline{x}} = (x_1+1,x_2,\ldots,x_n)$ are in two disjoint cycles we can join these cycles by exchanging their successors. In the opposite situation, the cycles are disjoined. So, it is possible to construct the de Bruijn cycle of span n out of the factors with $r \geq 2$ cycles. In order to do that r-1 pairs of conjugated vertices should be determined. It is obvious that it is simplest when a factor has only two cycles (r=2).

Lempel [4] described the construction of a certain class of such factors basing on a homomorphism D from $G_n$ to $G_{n-1}$. The inverse $D^{-1}\underline{s}$ of any de Bruijn cycle $\underline{s}$ of span n-1 is a factor of $G_n$. Such a factor, called D-factor of $\underline{s}$, has exactly two cycles, each of which enfolds $2^{n-1}$ vertices. The only problem left is joining of its cycles. Lempel [4] showed two connections of this type for any D-factor; other were studied by [6,7].

Also Games [2] described a method of constructing some of two-cycle factors having the same connections as D-factor $D^{-1}\underline{s}$.

The present paper deals with the construction of all such **factors.** In addition the fact that there is no need to construct D-factor $D^{-1}\underline{s}$ as a cycle $\underline{s}$ itself determines the connections. It means a complete reccurence of this problem.

## 2. Preliminaria

We recall here notions and notations from [2].

A cycle $\underline{s} = (\underline{s}_0, \underline{s}_1, \dots, \underline{s}_{p-1})$ in the de Bruijn graph $G_n$ is a sequence of distinct vertices $\underline{s}_i$, $i=0,1,\dots,p-1$, with $\underline{s}_i$ adjacent to $\underline{s}_{i+1}$, $i=0,1,\dots,p-2$, and $\underline{s}_{p-1}$ adjacent to $\underline{s}_0$. The image of a cycle $\underline{s}$ is the set $\mathrm{Im}\underline{s} = \{\underline{s}_0, \underline{s}_1, \dots, \underline{s}_{p-1}\}$.

A convenient method of representing such a cycle $\underline{s}$ is by means a sequence of p binary digits $(s_0, s_1, \dots, s_{p-1})$, where vectors $\underline{s}_i = (s_i, s_{i+1}, \dots, s_{i+n-1})$ **(subscripts taken mod p)**, are elements of $\underline{s}$.

The D-morphism means mapping D from $G_n$ onto $G_{n-1}$ such that for each $\underline{x} = (x_1, \dots x_n) \in B^n$ we have

$$D\underline{x} = (x_1+x_2,\ x_2+x_3,\ \dots\ ,\ x_{n-1}+x_n).$$

D-morphism is a 2-to-1 map; it maps $\underline{x} = (x_1,x_2,\ldots,x_n)$ and the complement $\bar{\underline{x}} = (x_1+1,x_2+1,\ldots,x_n+1)$ of $\underline{x}$, to the same element. Conversely, if $\underline{y} = (y_1,y_2,\ldots,y_{n-1}) \in B^{n-1}$, then an element of $D^{-1}\underline{y}$ is determined by its first coordinate, and we define two maps $D_0^{-1}$ and $D_1^{-1}$ from $B^{n-1}$ to $B^n$, by

$$D_a^{-1}\underline{y} = \left(a,\ a+y_1,\ a+y_1+y_2,\ldots,a+\sum_{i=1}^{n-1} y_i\right)$$

for $a \in \{0,1\}$.

The D-morphism can be applied to a cycle $\underline{s}=(\underline{s}_0,\underline{s}_1,\ldots,\underline{s}_{p-1})$ in $G_n$ to yield a closed path $D\underline{s} = (D\underline{s}_0,\ldots,D\underline{s}_{p-1})$ in $G_{n-1}$. $D_{\underline{s}}$ is a cycle only in the situation when no complementary vertices occur in $Im\underline{s}$. If the cycle $\underline{s}$ is written in a binary sequence form $\underline{s} = (s_0,s_1,\ldots,s_{p-1})$, then $D\underline{s} = (s_0+s_1,\ldots,s_{p-1}+s_0)$.

The inverse of D, when applied to a binary sequence, can take two forms [4]. If the number of nonzero entries in the vector $\underline{s}$ (the weight of $\underline{s}$) is even, then the inverse image is composed of two complementary sequences:

$$D_0^{-1}\underline{s} = \left(0,\ s_0,\ s_0+s_1,\ldots,\ \sum_{i=0}^{p-2} s_i\right),$$

$$D_1^{-1}\underline{s} = \left(1,\ 1+s_0,\ 1+s_0+s_1,\ldots,1+\sum_{i=0}^{p-2} s_i\right),$$

otherwise a single sequence of period 2p results

$$D^{-1}\underline{s} = \left\{\left(0,\ s_0,\ldots,\ \sum_{i=0}^{p-2} s_i,\ 1,\ 1+s_0,\ldots,1+\sum_{i=0}^{p-2} s_i\right)\right\}.$$

Now let us define a function $I_{\underline{s}}: T_{\underline{s}} \times T_{\underline{s}} \to \{0,1\}$, where $T_{\underline{s}} = \{\underline{x} \in B^n : \{\underline{x},\hat{\underline{x}}\} \in Im\underline{s}\}$ as follows

$$\mathcal{I}_{\underline{s}}(\underline{x},\underline{y}) = \begin{cases} 1 & \text{if there are positive integers } i,j,k,l \text{ such} \\ & \text{that } \underline{s}=(\underline{s}_0,\dots,\underline{s}_i,\dots,\underline{s}_j,\dots,\underline{s}_k,\dots,\underline{s}_l,\dots,\underline{s}_{p-1}) \\ & \text{and } \{\underline{x},\hat{\underline{x}}\} = \{\underline{s}_i,\underline{s}_k\} \text{ and } \{\underline{y},\hat{\underline{y}}\} = \{\underline{s}_j,\underline{s}_l\} \\ 0 & \text{otherwise.} \end{cases}$$

The range of $\mathcal{I}_{\underline{s}}$ will be presented in the form of a square binary matrix and denoted by $L_{\underline{s}}$. We assume that rows and columns of $L_{\underline{s}}$ are ordered according to lexicographical order of elements of the set $T_{\underline{s}}$.

For a nonempty subset $T$ of $T_{\underline{s}}$ we denote the submatrix of $L_{\underline{s}}$ restricted to $T\times T$ by means of $L_{\underline{s}|T}$. By $\underline{s}^T$ we denote the set of all cycles obtained by interchanging the successors of conjugated elements $\underline{x}$ and $\hat{\underline{x}}$, where $\underline{x}\in T$. If a set $\underline{s}^T$ contains exactly one cycle, such a cycle will be denoted also by means symbol $\underline{s}^T$.

Let $T^o_{\underline{s}} = \{\underline{x} = (x_1,\dots,x_n)\in T_{\underline{s}}:\ x_1=0\}$.

T h e o r e m 2.1. [5]. *For any cycle $\underline{s}$ in $G_n$ and nonempty $T\subset T^o_{\underline{s}}$ the set $\underline{s}^T$ contains a single cycle iff $L_{\underline{s}|T}$ is a nonsingular matrix over GF(2).*

*Moreover $\mathrm{Im}\underline{s} = \mathrm{Im}\underline{s}^T$.*

R e m a r k . It follows immediately from the definition of $T^o_{\underline{s}}$ that if $\underline{x},\underline{y}\in T^o_{\underline{s}}$ then we have

$$\mathcal{I}_{\underline{s}}(\underline{x},\underline{y}) = \mathcal{I}_{\underline{s}}(\hat{\underline{x}},\underline{y}) = \mathcal{I}_{\underline{s}}(\underline{x},\hat{\underline{y}}) = \mathcal{I}_{\underline{s}}(\hat{\underline{x}},\hat{\underline{y}}) = \mathcal{I}_{\underline{s}}(\underline{y},\underline{x}).$$

Thereby the matrix $L_{\underline{s}}$ has a form

$$L_{\underline{s}} = \left[\begin{array}{c|c} L_{\underline{s}}|_{T^o_{\underline{s}}} & L_{\underline{s}}|_{T^o_{\underline{s}}} \\ \hline L_{\underline{s}}|_{T^o_{\underline{s}}} & L_{\underline{s}}|_{T^o_{\underline{s}}} \end{array}\right]$$

For any two natural numbers $i$, $j$ $(i<j)$ the sequence of consecutive elements $(\underline{s}_i, \underline{s}_{i+1},\dots,\underline{s}_j)$ of the cycle $\underline{s}$ will be denoted as $\langle\underline{s}_i,\underline{s}_j\rangle_{\underline{s}}$, and the sum $s_i+s_{i+1}+\dots+s_j \pmod 2$ – as $|\langle\underline{s}_i,\underline{s}_j\rangle_{\underline{s}}|$.

Let now i,j,k,l be natural numbers such that $0<i<j<k<l<p-1$ and $\{\underline{a},\hat{\underline{a}}\} = \{\underline{s}_i,\underline{s}_k\}$, $\{\underline{b},\hat{\underline{b}}\} = \{\underline{s}_j,\underline{s}_l\}$. The cycle $\underline{s}$ can be described as follows

$$\underline{s} = \langle \underline{s}_0,\underline{s}_i\rangle_{\underline{s}} \langle \underline{s}_{i+1},\underline{s}_j\rangle_{\underline{s}} \langle \underline{s}_{j+1},\underline{s}_k\rangle_{\underline{s}} \langle \underline{s}_{k+1},\underline{s}_l\rangle_{\underline{s}} \langle \underline{s}_{l+1},\underline{s}_{p-1}\rangle_{\underline{s}}.$$

As $I_{\underline{s}}(\underline{a},\underline{b}) = 1$, then it follows from Theorem 2.1 that

$$\underline{s}\{\underline{a},\underline{b}\} = \langle \underline{s}_0,\underline{s}_i\rangle_{\underline{s}} \langle \underline{s}_{k+1},\underline{s}_l\rangle_{\underline{s}} \langle \underline{s}_{j+1},\underline{s}_k\rangle_{\underline{s}} \langle \underline{s}_{i+1},\underline{s}_j\rangle_{\underline{s}} \langle \underline{s}_{l+1},\underline{s}_{p-1}\rangle_{\underline{s}}.$$

Obviously, $Im\underline{s} = Im\underline{s}\{\underline{a},\underline{b}\}$.

E x a m p l e 2.1. The cycle $\underline{s}$ = (0000,0001,0011,0111, 1111,1110,1101,1010,0101,1011,0110,1100,1001,0010,0100,1000) is a de Bruijn cycle of span 4. Then

$$T^0_{\underline{s}} = \{0000,0001,0010,0011,0100,0101,0110,0111\}$$

and

$$L_{\underline{s}|T^0_{\underline{s}}} = \begin{bmatrix} 0&0&0&0&0&0&0&0\\ 0&0&1&0&1&0&0&0\\ 0&1&0&1&1&1&1&0\\ 0&0&1&0&0&0&1&0\\ 0&1&1&0&0&0&0&0\\ 0&0&1&0&0&0&0&0\\ 0&0&1&1&0&0&0&0\\ 0&0&0&0&0&0&0&0 \end{bmatrix}$$

For T = {0001,0011,0100,0110} we obtain a nonsingular matrix

$$L_{\underline{s}|T} = \begin{bmatrix} 0&0&1&0\\ 0&0&0&1\\ 1&0&0&0\\ 0&1&0&0 \end{bmatrix}$$

and $\underline{s}^T$ = (0000,0001,0010,0100,1001,0011,0110,1101,1010,0101, 1011,0111,1111,1110,1100,1000).

There exist 15 different nonsingular submatrices of $L_{\underline{s}|T^{o}_{\underline{s}}}$ each of which determines one de Bruijn sequence of span 4.

### 3. Joining of cycles of D-factor

Here a relation between sets of joints of cycles of two different D-factors of $G_{n+1}$ will be shown.

Let $\underline{s} = (\underline{s}_0, \underline{s}_1, \ldots, \underline{s}_{2^n-1})$ be a de Bruijn cycle of span n. Since the weight of the sequence $\underline{s}$ is even, we have $D^{-1}\underline{s} = \{\underline{s}_{(0)}, \underline{s}_{(1)}\}$, where

$$\underline{s}_{(0)} = D_0^{-1}\underline{s} \quad \text{and} \quad \underline{s}_{(1)} = D_1^{-1}\underline{s}.$$

Cycles $\{\underline{s}_{(0)}, \underline{s}_{(1)}\}$ form D-factor of $G_{n+1}$ [4]. Our aim here is to join the cycles $\underline{s}_{(0)}$ and $\underline{s}_{(1)}$ into one cycle $\underline{u}$ which is a de Bruijn cycle of span n+1. It is possible if and only if there exists $\underline{x} \in B^{n+1}$ such that

$$\underline{u}^{\{\underline{x}\}} = \{\underline{s}_{(0)}, \underline{s}_{(1)}\} .$$

Let $A_{\underline{s}}$ denote the set of all such joints, e.g.

$$\{\underline{x} \in B^{n+1} : \underline{x} \in \operatorname{Im}\underline{s}_{(0)} \text{ and } \hat{\underline{x}} \in \operatorname{Im}\underline{s}_{(1)} \text{ or } \hat{\underline{x}} \in \operatorname{Im}\underline{s}_{(0)} \text{ and } \underline{x} \in \operatorname{Im}\underline{s}_{(1)}\}.$$

Lempel [4] showed that for any de Bruijn cycle $\underline{s}$ of span n the set $A_{\underline{s}}$ is nonempty.

Let us consider the mapping $\lambda_{\underline{s}} : B^n \to \{0,1\}$ such that

$$\lambda_{\underline{s}}(\underline{x}) = \begin{cases} 0 & \text{for } \underline{x} \in D(A_{\underline{s}}) \\ 1 & \text{for } \underline{x} \in D(B^{n+1} - A_{\underline{s}}) \end{cases}$$

where $D(A_{\underline{s}})$ is an image of the set $A_{\underline{s}}$ under D. It is worth to note that $\lambda_{\underline{s}}(\underline{x}) = \lambda_{\underline{s}}(\hat{\underline{x}})$.

Determination of the mapping $\lambda_{\underline{s}}$ means exactly the same as determination of all joints of the cycles of D-factor $\{\underline{s}_{(0)}, \underline{s}_{(1)}\}$.

So, if $\lambda_{\underline{s}}(\underline{x}) = 0$, then

(3.1) $D_0^{-1}\underline{x}$, $D_1^{-1}\underline{x}$, $D_0^{-1}\hat{\underline{x}}$, $D_1^{-1}\hat{\underline{x}}$ are elements of the set $A_{\underline{s}}$;

(3.2) $D_0^{-1}\underline{x}$, $D_1^{-1}\hat{\underline{x}}$ and $D_0^{-1}\hat{\underline{x}}$, $D_1^{-1}\underline{x}$ are conjugates in $B^{n+1}$, respectively.

In [7] the following theorem determining the values of mapping $\lambda_{\underline{s}}$ was proved.

T h e o r e m 3.1. For a de Bruijn cycle $\underline{s} = (\underline{s}_0,\dots,\underline{s}_{2^n-1})$ of span n and any $\underline{x} \in B^n$, if i and k $(i<k)$ are natural numbers such that $\{\underline{x},\hat{\underline{x}}\} = \{\underline{s}_i,\underline{s}_k\}$, then

$$(3.3) \qquad \lambda_{\underline{s}}(\underline{x}) = s_i + s_{i+1} + \dots + s_{k-1} (\mathrm{mod}\ 2).$$

Let us consider two elements $\underline{a}$ and $\underline{b}$ from the cycle $\underline{s}$ such that $\mathcal{I}_{\underline{s}}(\underline{a},\underline{b}) = 1$. Let $\underline{r}$ denote a de Bruijn cycle of span n being the only element of the set $\underline{s}^{\{\underline{a},\underline{b}\}}$. Our aim here is to show the relation between sets $A_{\underline{s}}$ and $A_{\underline{r}}$ containing, respectively, joints of the cycles of the D-factors $\{\underline{s}_{(0)},\underline{s}_{(1)}\}$ and $\{\underline{r}_{(0)},\underline{r}_{(1)}\}$. This relation can be expressed as a relation between functions $\lambda_{\underline{s}}$ and $\lambda_{\underline{r}}$.

T h e o r e m 3.2. For any elements $\underline{a}$ and $\underline{b}$ from the set $B^n$ and a de Bruijn cycle $\underline{s}$ of span n, if $\mathcal{I}_{\underline{s}}(\underline{a},\underline{b}) = 1$, then for the de Bruijn cycle $\underline{r} = \underline{s}^{\{\underline{a},\underline{b}\}}$ of span n the function $\lambda_{\underline{r}}$ is determined as follows

$$(3.4) \qquad \lambda_{\underline{r}}(\underline{x}) = \begin{cases} \lambda_{\underline{s}}(\underline{b}) & \text{for } \underline{x}=\underline{a} \\ \lambda_{\underline{s}}(\underline{a}) & \text{for } \underline{x}=\underline{b} \\ \lambda_{\underline{s}}(\underline{x}) + \mathcal{I}_{\underline{s}}(\underline{a},\underline{x})(\lambda_{\underline{s}}(\underline{b}) + 1) + & \text{for } \underline{x}\neq\underline{a},\underline{b} \\ \quad + \mathcal{I}_{\underline{s}}(\underline{b},\underline{x})(\lambda_{\underline{s}}(\underline{a}) + 1) & \end{cases}$$

P r o o f . Let i,j,k,l be the natural numbers such that $0 \leqslant i < j < k < l \leqslant 2^n-1$ and $\{\underline{a},\hat{\underline{a}}\} = \{\underline{s}_i,\underline{s}_k\}$ , $\{\underline{b},\hat{\underline{b}}\} = \{\underline{s}_j,\underline{s}_l\}$. Moreover let

$$\underline{s} = \langle \underline{s}_0, \underline{s}_i\rangle_{\underline{s}} \langle \underline{s}_{i+1}, \underline{s}_j\rangle_{\underline{s}} \langle \underline{s}_{j+1}, \underline{s}_k\rangle_{\underline{s}} \langle \underline{s}_{k+1}, \underline{s}_l\rangle_{\underline{s}} \langle \underline{s}_{l+1}, \underline{s}_{2^n-1}\rangle_{\underline{s}}.$$

The proof will be made for consecutive cases:

A. Let $\underline{x} \in \{\underline{a},\underline{b}\}$. Since

$$\underline{r} = \underline{s}^{\{\underline{a},\underline{b}\}} = \langle \underline{s}_0, \underline{s}_i\rangle_{\underline{s}} \langle \underline{s}_{k+1}, \underline{s}_l\rangle_{\underline{s}} \langle \underline{s}_{j+1}, \underline{s}_k\rangle_{\underline{s}} \langle \underline{s}_{i+1}, \underline{s}_j\rangle_{\underline{s}} \langle \underline{s}_{l+1}, \underline{s}_{2^n-1}\rangle_{\underline{s}}$$

then

$$(3.5)\quad \lambda_{\underline{r}}(\underline{a}) = \left|\langle \underline{s}_i, \underline{s}_{k-1}\rangle_{\underline{r}}\right| = s_i + \left|\langle \underline{s}_{k+1}, \underline{s}_l\rangle_{\underline{s}}\right| + \left|\langle \underline{s}_{j+1}, \underline{s}_{k-1}\rangle_{\underline{s}}\right| = s_j + \left|\langle \underline{s}_{j+1}, \underline{s}_{k-1}\rangle_{\underline{s}}\right| + s_k + \left|\langle \underline{s}_{k+1}, \underline{s}_{l-1}\rangle_{\underline{s}}\right| + s_i + s_j + s_k + s_l = \left|\langle \underline{s}_j, \underline{s}_{l-1}\rangle_{\underline{s}}\right| = \lambda_{\underline{s}}(\underline{b}).$$

In a similar way we arrive at the equality

$$(3.6)\qquad \lambda_{\underline{r}}(\underline{b}) = \lambda_{\underline{s}}(\underline{a}).$$

B. Let $\underline{x} \notin \{\underline{a},\underline{b}\}$ and p,q $(p<q)$ be the natural numbers such that $\{\underline{x},\hat{\underline{x}}\} = \{\underline{s}_p, \underline{s}_q\}$.

If $\mathfrak{X}_{\underline{s}}(\underline{a},\underline{x}) = \mathfrak{X}_{\underline{s}}(\underline{b},\underline{x}) = 0$, then from the definition of $\underline{r}$ follows the equality

$$(3.7)\qquad \lambda_{\underline{r}}(\underline{x}) = \lambda_{\underline{s}}(\underline{x}).$$

If $\mathfrak{X}_{\underline{s}}(\underline{a},\underline{x}) = 1$ and $\mathfrak{X}_{\underline{s}}(\underline{b},\underline{x}) = 0$, then

$$\underline{s} = \langle \underline{s}_0, \underline{s}_p\rangle_{\underline{s}} \langle \underline{s}_{p+1}, \underline{s}_i\rangle_{\underline{s}} \langle \underline{s}_{i+1}, \underline{s}_q\rangle_{\underline{s}} \langle \underline{s}_{q+1}, \underline{s}_j\rangle_{\underline{s}} \langle \underline{s}_{j+1}, \underline{s}_k\rangle_{\underline{s}} \langle \underline{s}_{k+1}, \underline{s}_l\rangle_{\underline{s}} \langle \underline{s}_{l+1}, \underline{s}_{2^n-1}\rangle_{\underline{s}}$$

and

$$\underline{r} = \underline{s}^{\{\underline{a},\underline{b}\}} = \langle \underline{s}_0, \underline{s}_p\rangle_{\underline{s}} \langle \underline{s}_{p+1}, \underline{s}_i\rangle_{\underline{s}} \langle \underline{s}_{k+1}, \underline{s}_l\rangle_{\underline{s}} \langle \underline{s}_{j+1}, \underline{s}_k\rangle_{\underline{s}} \langle \underline{s}_{i+1}, \underline{s}_q\rangle_{\underline{s}} \langle \underline{s}_{q+1}, \underline{s}_j\rangle_{\underline{s}} \langle \underline{s}_{l+1}, \underline{s}_{2^n-1}\rangle_{\underline{s}}.$$

Hence

(3.8) $$\lambda_{\underline{r}}(\underline{x}) = |\langle \underline{s}_p,\underline{s}_{q-1}\rangle_{\underline{r}}| = s_p + |\langle \underline{s}_{p+1},\underline{s}_i\rangle_{\underline{s}}| + |\langle \underline{s}_{k+1},\underline{s}_l\rangle_{\underline{s}}| + |\langle \underline{s}_{j+1},\underline{s}_k\rangle_{\underline{s}}| + |\langle \underline{s}_{i+1},\underline{s}_{q-1}\rangle_{\underline{s}}| = s_p + |\langle \underline{s}_{p+1},\underline{s}_i\rangle_{\underline{s}}| + |\langle \underline{s}_{i+1},\underline{s}_{q-1}\rangle_{\underline{s}}| + s_j + |\langle \underline{s}_{j+1},\underline{s}_k\rangle_{\underline{s}}| + |\langle \underline{s}_{k+1},\underline{s}_{l-1}\rangle_{\underline{s}}| + s_l + s_j = |\langle \underline{s}_p,\underline{s}_{q-1}\rangle_{\underline{s}}| + |\langle \underline{s}_j,\underline{s}_{l-1}\rangle_{\underline{s}}| + 1 = \lambda_{\underline{s}}(\underline{x}) + \lambda_{\underline{s}}(\underline{b}) + 1.$$

Similarly, if $I_{\underline{s}}(\underline{a},\underline{x}) = 0$ and $I_{\underline{s}}(\underline{b},\underline{x}) = 1$, then

(3.9) $$\lambda_{\underline{r}}(\underline{x}) = \lambda_{\underline{s}}(\underline{x}) + \lambda_{\underline{s}}(\underline{a}) + 1.$$

If $I_{\underline{s}}(\underline{a},\underline{x}) = I_{\underline{s}}(\underline{b},\underline{x}) = 1$, then

$$\underline{s} = \langle \underline{s}_0,\underline{s}_i\rangle_{\underline{s}}\langle \underline{s}_{i+1},\underline{s}_p\rangle_{\underline{s}}\langle \underline{s}_{p+1},\underline{s}_j\rangle_{\underline{s}}\langle \underline{s}_{j+1},\underline{s}_k\rangle_{\underline{s}}\langle \underline{s}_{k+1},\underline{s}_q\rangle_{\underline{s}}\langle \underline{s}_{q+1},\underline{s}_l\rangle_{\underline{s}}\langle \underline{s}_{l+1},\underline{s}_{2^n-1}\rangle_{\underline{s}}$$

and

$$\underline{r} = \underline{s}^{\{\underline{a},\underline{b}\}} = \langle \underline{s}_0,\underline{s}_i\rangle_{\underline{s}}\langle \underline{s}_{k+1},\underline{s}_q\rangle_{\underline{s}}\langle \underline{s}_{q+1},\underline{s}_l\rangle_{\underline{s}}\langle \underline{s}_{j+1},\underline{s}_k\rangle_{\underline{s}}\langle \underline{s}_{i+1},\underline{s}_p\rangle_{\underline{s}}\langle \underline{s}_{p+1},\underline{s}_j\rangle_{\underline{s}}\langle \underline{s}_{l+1},\underline{s}_{2^n-1}\rangle_{\underline{s}}.$$

Thereby

(3.10) $$\lambda_{\underline{r}}(\underline{x}) = |\langle \underline{s}_p,\underline{s}_{q-1}\rangle_{\underline{r}}| = |\langle \underline{s}_q,\underline{s}_{p-1}\rangle_{\underline{r}}| = s_q + |\langle \underline{s}_{q+1},\underline{s}_l\rangle_{\underline{s}}| + |\langle \underline{s}_{j+1},\underline{s}_k\rangle_{\underline{s}}| + |\langle \underline{s}_{i+1},\underline{s}_{p-1}\rangle_{\underline{s}}| = (s_p + |\langle \underline{s}_{p+1},\underline{s}_j\rangle_{\underline{s}}| + |\langle \underline{s}_{j+1},\underline{s}_k\rangle_{\underline{s}}| + |\langle \underline{s}_{k+1},\underline{s}_{q-1}\rangle_{\underline{s}}|) + (s_i + |\langle \underline{s}_{i+1},\underline{s}_{p-1}\rangle_{\underline{s}}| + s_p + |\langle \underline{s}_{p+1},\underline{s}_j\rangle_{\underline{s}}| + |\langle \underline{s}_{j+1},\underline{s}_{k-1}\rangle_{\underline{s}}|) + (s_j + |\langle \underline{s}_{j+1},\underline{s}_{k-1}\rangle_{\underline{s}}| + s_k + |\langle \underline{s}_{k+1},\underline{s}_{q-1}\rangle_{\underline{s}}| + |\langle \underline{s}_q,\underline{s}_{l-1}\rangle_{\underline{s}}|) + (s_i + s_j + s_k + s_l) = \lambda_{\underline{s}}(\underline{x}) + \lambda_{\underline{s}}(\underline{a}) + \lambda_{\underline{s}}(\underline{b}).$$

From (3.7)-(3.10) we arrive the following equality

$$\lambda_{\underline{r}}(\underline{x}) = \lambda_{\underline{s}}(\underline{x}) + \lambda_{\underline{s}}(\underline{a})\mathcal{I}_{\underline{s}}(\underline{b},\underline{x}) + \lambda_{\underline{s}}(\underline{b})\mathcal{I}_{\underline{s}}(\underline{a},\underline{x}) + \mathcal{I}_{\underline{s}}(\underline{a},\underline{x}) + $$
$$+ \mathcal{I}_{\underline{s}}(\underline{b},\underline{x}) = \lambda_{\underline{s}}(\underline{x}) + \mathcal{I}_{\underline{s}}(\underline{a},\underline{x})(1 + \lambda_{\underline{s}}(\underline{b})) +$$
$$+ \mathcal{I}_{\underline{s}}(\underline{b},\underline{x})(1 + \lambda_{\underline{s}}(\underline{a})).$$

E x a m p l e 3.1. Let us consider a de Bruijn cycle $\underline{s}$ of span 4 presented in Example 2.1. There exist seven different pairs $(\underline{a}_i,\underline{b}_i) \in T^0_{\underline{s}} \times T^0_{\underline{s}}$, $i=1,\ldots,7$:

$$(\underline{a}_1,\underline{b}_1) = (0001,0010),$$
$$(\underline{a}_2,\underline{b}_2) = (0001,0100),$$
$$(\underline{a}_3,\underline{b}_3) = (0010,0011),$$
$$(\underline{a}_4,\underline{b}_4) = (0010,0100),$$
$$(\underline{a}_5,\underline{b}_5) = (0010,0101),$$
$$(\underline{a}_6,\underline{b}_6) = (0010,0110),$$
$$(\underline{a}_7,\underline{b}_7) = (0011,0110),$$

such that $\mathcal{I}_{\underline{s}}(\underline{a}_i,\underline{b}_i) = 1$.

Since each of the matrices $L_{\underline{s}} \big|\{\underline{a}_i,\underline{b}_i\}$ is nonsingular over GF(2), each of the corresponding cycles $\underline{s}^{\{\underline{a}_i,\underline{b}_i\}}$, $i=1,\ldots,7$, is a de Bruijn cycle of span 4.

The function $\lambda_{\underline{s}}$ is determined in the following way

$$\lambda_{\underline{s}}(\underline{x}) = \begin{cases} 1 & \text{for } \underline{x} \in \{0000,1000\} \\ 0 & \text{for } \underline{x} \in B^4 - \{0000,1000\}. \end{cases}$$

The sets of values of the functions $\lambda_i = \lambda_{\underline{s}^i}$ determined for the cycles $\underline{s}^i = \underline{s}^{\{\underline{a}_i,\underline{b}_i\}}$ is shown in Table I.

| | | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | 0 | 1 | 0 | 1 | 0 | 1 | 0 | 1 | 0 | 1 | 0 | 1 | 0 | 1 | 0 | 1 |
| $\underline{x}$ | 0 | 0 | 1 | 1 | 0 | 0 | 1 | 1 | 0 | 0 | 1 | 1 | 0 | 0 | 1 | 1 |
| | 0 | 0 | 0 | 0 | 1 | 1 | 1 | 1 | 0 | 0 | 0 | 0 | 1 | 1 | 1 | 1 |
| | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 |
| $\lambda_s(\underline{x})$ | 1 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 1 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| $\lambda_1(\underline{x})$ | 1 | 0 | 0 | 1 | 0 | 1 | 1 | 0 | 1 | 0 | 0 | 1 | 0 | 1 | 1 | 0 |
| $\lambda_2(\underline{x})$ | 1 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 1 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| $\lambda_3(\underline{x})$ | 1 | 1 | 0 | 0 | 1 | 1 | 1 | 0 | 1 | 1 | 0 | 0 | 1 | 1 | 1 | 0 |
| $\lambda_4(\underline{x})$ | 1 | 0 | 0 | 1 | 0 | 1 | 1 | 0 | 1 | 0 | 0 | 1 | 0 | 1 | 1 | 0 |
| $\lambda_5(\underline{x})$ | 1 | 1 | 0 | 1 | 1 | 0 | 1 | 0 | 1 | 1 | 0 | 1 | 1 | 0 | 1 | 0 |
| $\lambda_6(\underline{x})$ | 1 | 1 | 0 | 0 | 1 | 1 | 0 | 0 | 1 | 1 | 0 | 0 | 1 | 1 | 0 | 0 |
| $\lambda_7(\underline{x})$ | 1 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 1 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |

Table I

The condition (3.4) can be applied to a cycle $\underline{s}^T$, if the cardinality of the set T is greater than 2. In [5] it is proved that if $T = \{\underline{a}_1,\dots,\underline{a}_p,\underline{b}_1,\dots,\underline{b}_p\}$ then there exists a partition $\{\underline{a}_{i_1},\underline{b}_{i_1}\},\dots,\{\underline{a}_{i_p},\underline{b}_{i_p}\}$ of T determining the following sequence of de Bruijn cycles:

$$(3.11)\qquad \begin{cases} {}^{0}\underline{u} = \underline{s}; \\ {}^{j}\underline{u} = {}^{j-1}\underline{u}^{\{\underline{a}_{ij},\underline{b}_{ij}\}}, \quad \text{for } j=1,\dots,p; \\ {}^{p}\underline{u} = \underline{s}^T; \end{cases}$$

where $T_{i_{\underline{u}}}(\underline{a}_{ij},\underline{b}_{ij}) = 1$.

Applying (3.4) to consecutive cycles ${}^{i}\underline{u}$, for $i=1,\dots,p$, we get a sequence of functions $\lambda_{1_{\underline{u}}},\dots,\lambda_{p_{\underline{u}}}$.

## 4. A class of factors connected with D-factor

Let us consider a de Bruijn cycle $\underline{s}$ of span n and its corresponding D-factor $\{\underline{s}_{(0)},\underline{s}_{(1)}\}$. For a cycle $\underline{s}$ the class $\mathcal{F}^*_{\underline{s}}$ of the Bruijn cycles of span n is defined in the following way [2]:

$$\mathcal{F}^*_{\underline{s}} = \{\underline{r}:\ Im\underline{r}_{(0)} = Im\underline{s}_{(0)} \ \text{ and } \ Im\underline{r}_{(1)} = Im\underline{s}_{(1)}\}.$$

Some elements of $\mathcal{F}^*_{\underline{s}}$ have been found by Games [2].

T h e o r e m 4.1. [2]. Let $\underline{s}$ be a de Bruijn cycle of span n. If $\{\underline{a},\underline{b}\} \subset Im\underline{s}_{(0)}$ and $I_{\underline{s}_{(0)}}(\underline{a},\underline{b}) = 1$, then

$$(4.1) \qquad \underline{r} = D(\underline{s}^{\{\underline{a},\underline{b}\}}_{(0)}) \ \text{ is an element of } \ \mathcal{F}^*_{\underline{s}}.$$

Condition (4.1) allows for determination of some subset of the class $\mathcal{F}^*_{\underline{s}}$. It can be illustrated by the following example.

E x a m p l e 4.1. Let us consider two de Bruijn cycles of span 4

$\underline{s}$ = (0000,0001,0011,0111,1111,1110,1101,1011,0110,1100,1001, 0010,0101,1010,0100,1000) and

$\underline{r}$ = (0000,0001,0010,0101,1010,0100,1001,0011,0110,1101,1011, 0111,1111,1110,1100,1000).

Since for the cycles $\underline{s}$ and $\underline{r}$ the equalities

$$Im\underline{s}_{(0)} = Im\underline{r}_{(0)} \ \text{ and } \ Im\underline{s}_{(1)} = Im\underline{r}_{(1)}$$

hold, the cycle $\underline{r}$ belongs to the class $\mathcal{F}^*_{\underline{s}}$.

On the other hand

$$\underline{r} = D(\underline{s}^{\{00001,00010,00100,01000\}}_{(0)})$$

So, the cycle $\underline{r}$ does not fulfill the condition (4.1). For each $n \geqslant 4$ it is possible to find de Bruijn cycles with the above mentioned characteristics.

Let us formulate a necessary and sufficient condition for the cycle $\underline{r}$ to belong to the class $\mathcal{F}^*_{\underline{s}}$. The condition utilizes only some features of the cycle $\underline{s}$.

T h e o r e m 4.2. Let $\underline{s}$ be an arbitrary de Bruijn cycle of span n. For any de Bruijn cycle $\underline{r}$ of span n

$$\underline{r} \in \mathcal{F}^*_{\underline{s}} \quad \text{iff} \quad \underline{r} = \underline{s}^T,$$

where T is a subset of $T^o_{\underline{s}}$ fulfilling conditions

(4.2) $L_{\underline{s}|T}$ is nonsingular matrix over GF(2);

(4.3) $\lambda_{\underline{s}}(\underline{x}) = 1$, for each $\underline{x} \in T$.

P r o o f . Necessity. Let us assume that $\underline{r} \in \mathcal{F}^*_{\underline{s}}$. This means that $Im\underline{r}_{(0)} = Im\underline{s}_{(0)}$ and $Im\underline{r}_{(1)} = Im\underline{s}_{(1)}$. The existence of the set $\tilde{T} \subset T^o_{\underline{s}_{(0)}}$ such that $L_{\underline{s}_{(0)}|\tilde{T}}$ is a nonsingular matrix over GF(2) and $\underline{r}_{(0)} = \underline{s}^{\tilde{T}}_{(0)}$ follows from the theorem 2.1. According to the definition of D we have the equality

$$I_{\underline{s}_{(0)}}(\underline{a},\underline{b}) = I_{\underline{s}}(D\underline{a},D\underline{b}), \quad \text{for each} \quad \underline{a},\underline{b} \in T_{\underline{s}_{(0)}}.$$

A nonsingular matrix $L_{\underline{s}_{(0)}|\tilde{T}}$ corresponds to a nonsingular matrix $L_{\underline{s}|T}$, where $T = D(\tilde{T})$, which implies the equality $\underline{r} = \underline{s}^T$. Moreover, from the definition of $\lambda_{\underline{s}}$ follows that $\lambda_{\underline{s}}(\underline{x}) = 1$, for each $\underline{x} \in T$.

Sufficiency. Let $\underline{r} = \underline{s}^T$, $L_{\underline{s}|T}$ is a nonsingular matrix over GF(2) and $\lambda_{\underline{s}}(\underline{x}) = 1$, for each $\underline{x} \in T$.

It follows from Theorem 3.2 that if $I_{\underline{s}}(\underline{a},\underline{b}) = 1$ and $\lambda_{\underline{s}}(\underline{a}) = \lambda_{\underline{s}}(\underline{b}) = 1$, then $\lambda_{\underline{s}}(\underline{x}) = \lambda_{\underline{s}}\{\underline{a},\underline{b}\}(\underline{x})$, for each $\underline{x} \in B^n$.

On the basis of the considerations from the preceding paragraph and (3.11) we can conclude that

$$\lambda_{\underline{s}}(\underline{x}) = \lambda_{\underline{r}}(\underline{x}) \quad \text{for each} \quad \underline{x} \in B^n.$$

The cycle $\underline{r}$ belongs to the class $\mathcal{F}^*_{\underline{s}}$.

Let us consider now a class $\mathcal{F}_{\underline{s}}$ of pairs of cycles $\{\underline{u},\underline{v}\}$ such that

$$Im\underline{u} = Im\underline{s}_{(0)} \quad \text{and} \quad Im\underline{v} = Im\underline{s}_{(1)},$$

for the de Bruijn cycle $\underline{s}$ of span n.

Each element of the class $\mathcal{F}_{\underline{s}}$ is a factor of $G_{n+1}$. The cycles of factors of $\mathcal{F}_{\underline{s}}$ have identical joints as cycles of D-factor $\{\underline{s}_{(0)},\underline{s}_{(1)}\}$; what is more, these are the only two-cycle factors of $G_{n+1}$ with this characteristics.

Elements of $\mathcal{F}_{\underline{s}}$ can be obtained directly from $\mathcal{F}^*_{\underline{s}}$ in the following way

$$\mathcal{F}_{\underline{s}} = \bigcup_{\underline{r}\in\mathcal{F}^*_{\underline{s}}} \Big( \bigcup_{\underline{z}\in\mathcal{F}^*_{\underline{s}}} \{D_0^{-1}\underline{r},\ D_1^{-1}\underline{z}\} \Big).$$

So, if two cycles of a factor $\{\underline{u},\underline{v}\} \in \mathcal{F}_{\underline{s}}$ are joined on elements $\{\underline{x},\hat{\underline{x}}\}$ from the set $A_{\underline{s}}$, we obtain a de Bruijn cycle of span n+1.

E x a m p l e 4.2. Let us consider the de Bruijn cycle of span 5 represented by a binary sequence

$$\underline{s} = (00000110110011111010010101110001).$$

The class $\mathcal{F}^*_{\underline{s}}$ contains 56 de Bruijn cycles of span 5 and the class $\mathcal{F}_{\underline{s}}$ includes 3136 two-cycle factors of $G_6$. The cycles of each of these factors can be joined on 14 conjugated pairs $\{\underline{x},\hat{\underline{x}}\}$ belonging to the set $A_{\underline{s}}$. It allows for the construction of 43904 de Bruijn cycles of span 6.

## REFERENCES

[1] N.G. D e B r u i j n : A combinatorial problem, Proc. Kon. Ned. Akad. Wetensch., 49 (1946) 758-764.

[2] R.A. G a m e s : A generalized recursive construction for de Bruijn sequences, IEEE Trans. Inform. Theory, IT-29, (1983) 843-850.

[3] H. F r e d r i c k s e n : A survey of full length nonlinear shift register cycle algorithms, SIAM rev., 24 (1982) 195-221.

[4] A. Lempel: On a homomorphism of the de Bruijn graph and its applications to the design of feedback shift registers, IEEE Trans. Computers, C-19 (1970) 1204-1209.
[5] M. Łatko: The similitude of shift registers, Demonstratio Math. 19 (1986) 469-485.
[6] J. Mykkeltveit, M.K. Siu, P. Tong: On the cycle structure of some nonlinear shift register sequences, Information and Control, 43 (1979) 202-215.
[7] M.K. Siu, P. Tong: Generation of some de Bruijn sequences, Discrete Math., (1980) 97-100.
[8] M. Yoeli: Counting with nonlinear binary feedback shift registers, IEEE Trans. Comput., EC-12 (1963) 357-361.

INSTITUTE OF MATHEMATICS, TECHNICAL UNIVERSITY OF LUBLIN,
20-618 LUBLIN, POLAND
Received November 5, 1985.