DEMONSTRATIO MATHEMATICA
Vol. XXIX No 1 1996

Ewa Łazuka, Jerzy Żurawiecki

LOWER BOUNDS OF A FEEDBACK FUNCTION

1. Introduction

The feedback functions and the corresponding recurring sequences — having numerous applications, for instance in coding theory, in cryptography or in several branches of electrical engineering — have been studied with methods of linear algebra, ideal theory or formal power series [1,3,4]. In 1963 Yoeli [9] published two theorems dealing with sequences joining and a sequence splitting. This has led to a design of algorithms for finding the Hamiltonian circuits in a de Bruijn graph (*Cf.* [2,8,11]).

In more general case, the paper [9] yields a tool for studying connections between the feedback functions and allows us to describe them as the elements of a partially ordered set. For a study of this order it is convenient to investigate the families of upper bounds and lower bounds of a feedback function.

Here we present properties of the families of the lower bounds of feedback functions. Each of such family forms an upper semilattice. It is completely described by a binary relation, called *the independent splits relation,* closely related to *the interlacing relation* defined in [5]. We study the independent splits relations and isomorphisms of the semilattices mentioned above. For instance, an isomorphism of an independent splits relation determines an isomorphism of the corresponding semilattices, and conversely. We shall show several examples of such isomorphisms: in particular, upper semilattices are isomorphic if the corresponding independent splits relations are identical. We shall describe a transformation of a feedback function which preserves its independent splits relation.

2. An order in the family of feedback functions

Let $\mathcal{F}^k$ be the family of total functions $\varphi\colon \{0,1\}^k \to \{0,1\}$ such that

$$\varphi(x_1, x_2, \ldots, x_k) \neq \varphi(\bar{x}_1, x_2, \ldots, x_k), \tag{2.1}$$

for each $(x_1,\dots,x_k) \in \{0,1\}^k$, ($\bar{x}_1 = x_1 + 1$ in $GF(2)$). Each function from $\mathcal{F}^k$ will be called a *feedback function*. Note that $\varphi\colon \{0,1\}^k \to \{0,1\}$ is a feedback function iff

$$(2.2) \qquad \varphi(x_1,x_2,\dots,x_k) = x_1 + \varphi(0,x_2,\dots,x_k),$$

where $+$ is the addition in $GF(2)$. Then for $\varphi \in \mathcal{F}^k$ and $X \subseteq \{0,1\}^{k-1}$ the function $\varphi_{\|X}$, defined by

$$(2.3) \qquad \varphi_{\|X}(x_1,x_2,\dots,x_k) = \varphi(x_1,x_2,\dots,x_k) + \chi_X(x_2,\dots,x_k)$$

(χ_X is the characteristic function of X), is the feedback function too. This implies that for an arbitrary fixed $\theta \in \mathcal{F}^k$ we have

$$(2.4) \qquad \mathcal{F}^k = \{\theta_{\|X} : X \subseteq \{0,1\}^{k-1}\}.$$

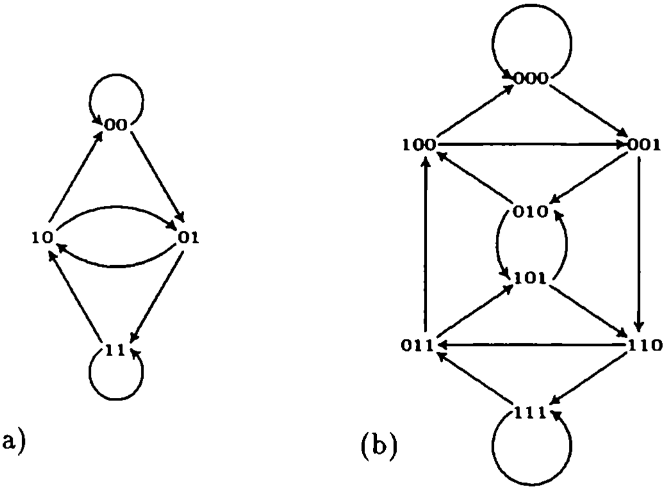

Figure 2.1. The de Bruijn graphs: (a) of order 2, (b) of order 3.

There exists an interesting connection between the feedback functions and subgraphs of the de Bruijn graph.

The de Bruijn graph of order k is a directed graph B_k that consists of the elements of $\{0,1\}^k$ as the vertices, where each edge $(v_1,v_2,\dots,v_k)$ is followed by two edges: $(v_2,\dots,v_k,0)$ and $(v_2,\dots,v_k,1)$. Each feedback function φ determines a maximal subgraph $B_k[\varphi]$ of B_k composed of disjoint directed circuits in which a vertex $v = (v_1,\dots,v_k)$ is followed by $v' = (v_2,\dots,v_k,\varphi(v))$. The graph $B_k[\varphi]$ is said to be *the factor of B_k corresponding to φ.*

Let v' and v'' be vertices of the same directed circuits of $B_k[\varphi]$ with $\varphi \in \mathcal{F}^k$. By $\langle v',v''\rangle_\varphi$ we denote the sequence of the consequtive vertices of the circuit from v' to v''. (If $v' = v''$ then $\langle v', v'\rangle_\varphi$ contains all vertices of the circuit and v' appears at the beginning and at the end of the sequence.) Moreover, $(v', v''\rangle_\varphi$ and $\langle v', v'')_\varphi$ denote the sequences which can be obtained from $\langle v', v''\rangle_\varphi$ by deleting v' and v'', respectively. In particular, each of the sequences $(v', v'\rangle_\varphi$ and $\langle v', v')_\varphi$ consists of all vertices of the circuit and each of them appears once.

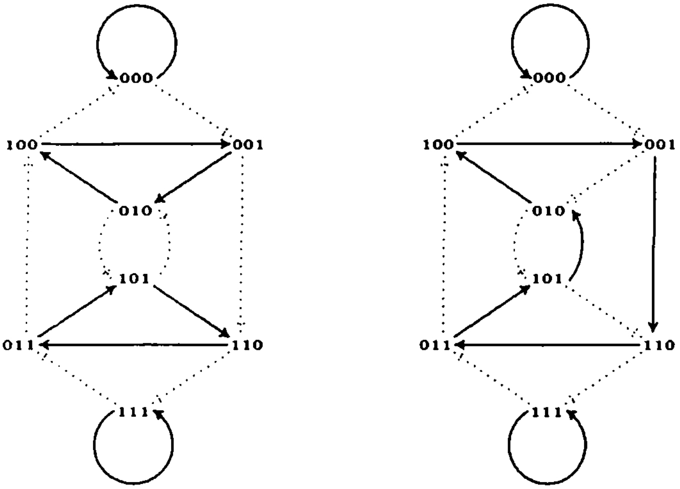

Figure 2.2. The factors $B_3[\vartheta]$ and $B_3[\vartheta_{\|\{01\}}]$ with $\vartheta(x_1, x_2, x_3) = x_1$.

2.1. Theorem. [9] *Let* $\varphi \in \mathcal{F}^k$ *and* $v = (v_1, v_2, \ldots, v_k) \in \{0,1\}^k$. *If* $\hat{v} = (\bar{v}_1, v_2, \ldots, v_k)$ *does not occur in* $(v, v\rangle_\varphi$ *then for* $u = (v_2, \ldots, v_k)$ *we have*

$$(v, v\rangle_{\varphi_{\|\{u\}}} = (\hat{v}, \hat{v}\rangle_\varphi (v, v\rangle_\varphi,$$

while $(v', v'\rangle_{\varphi_{\|\{u\}}} = (v', v'\rangle_\varphi$ *iff neither* v *nor* $\hat{v}$ *occurs in* $(v', v'\rangle_\varphi$, *for* $v' \in \{0,1\}^k \setminus \{v, \hat{v}\}$. ∎

2.2. Corollary. *Let* $\varphi \in \mathcal{F}^k$ *and* $v = (v_1, v_2, \ldots, v_k) \in \{0,1\}^k$. *If* $\hat{v} = (\bar{v}_1, v_2, \ldots, v_k)$ *occurs in* $(v, v\rangle_\varphi$ *then for* $u = (v_2, \ldots, v_k)$ *the sequences* $(v, v\rangle_{\varphi_{\|\{u\}}}$ *and* $(\hat{v}, \hat{v}\rangle_{\varphi_{\|\{u\}}}$ *do not have common elements and*

$$(v, v\rangle_\varphi = (v, v\rangle_{\varphi_{\|\{u\}}} (\hat{v}, \hat{v}\rangle_{\varphi_{\|\{u\}}}$$

while $(v', v'\rangle_{\varphi_{\|\{u\}}} = (v', v'\rangle_\varphi$ *iff neither* v *nor* $\hat{v}$ *occurs in* $(v', v'\rangle_\varphi$, *for* $v' \in \{0,1\}^k \setminus \{v, \hat{v}\}$. ∎

Let $\rightarrow \subseteq \mathcal{F}^k \times \mathcal{F}^k$ be the binary relation such that $\varphi \rightarrow \psi$ iff there exists $e = (e_1, \ldots, e_{k-1}) \in \{0,1\}^{k-1}$ for which $\psi = \varphi_{\|\{e\}}$ and the vertices $e_{(0)} = (0, e_1, \ldots, e_{k-1})$ and $e_{(1)} = (1, e_1, \ldots, e_{k-1})$ are in different circuits of $B_k[\varphi]$. Let $\overset{*}{\rightarrow}$ be the reflexive and transitive closure of $\rightarrow$. Then $\overset{*}{\rightarrow}$ is a partial order in $\mathcal{F}^k$.

The most interesting for applications is the family of feedback functions which form the maximal elements of $\overset{*}{\rightarrow}$. They correspond to the factors which form the Hamiltonian circuits in B_k ([2]), so they are said to be *the Hamiltonian functions* and the family of such functions is denoted by $\mathcal{H}^k$.

Beside $\mathcal{H}^k$, there exists another interesting family of feedback functions — the minimal elements of $\overset{*}{\rightarrow}$. They are called *locally reducible* feedback functions as forming a "bridge" between the families $\mathcal{F}^{k-1}$ and $\mathcal{F}^k$, because each circuit of the factor of a locally reducible feedback function may be reduced to a circuit of B_{k-1}, [10].'The family of all locally reducible feedback functions is denoted by $\mathcal{LR}^k$.

	φ_0	φ_1	φ_2	φ_3
00	0	0	1	1
01	0	1	0	1
10	1	1	0	0
11	1	0	1	0

Table 2.1. The feedback functions from $\mathcal{F}^2$

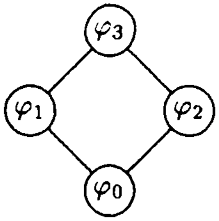

Figure 2.3. The diagram of $\overset{*}{\rightarrow}$ in $\mathcal{F}^2$

	φ_0	φ_1	φ_2	φ_3	φ_4	φ_5	φ_6	φ_7	φ_8	φ_9	φ_{10}	φ_{11}	φ_{12}	φ_{13}	φ_{14}	φ_{15}
000	0	0	0	0	0	0	0	0	1	1	1	1	1	1	1	1
001	0	0	0	0	1	1	1	1	0	0	0	0	1	1	1	1
010	0	0	1	1	0	0	1	1	0	0	1	1	0	0	1	1
011	0	1	0	1	0	1	0	1	0	1	0	1	0	1	0	1
100	1	1	1	1	1	1	1	1	0	0	0	0	0	0	0	0
101	1	1	1	1	0	0	0	0	1	1	1	1	0	0	0	0
110	1	1	0	0	1	1	0	0	1	1	0	0	1	1	0	0
111	1	0	1	0	1	0	1	0	1	0	1	0	1	0	1	0

Table 2.2. The feedback functions from $\mathcal{F}^3$.

For each feedback function $\varphi \in \mathcal{F}^k$ let us set $\mathcal{L}\langle\varphi\rangle = \{\psi : \psi \overset{*}{\rightarrow} \varphi\}$. We shall study the partially ordered set $(\mathcal{L}\langle\varphi\rangle, \overset{*}{\rightarrow})$.

2.3. THEOREM. *Let $\varphi \in \mathcal{F}^k$. The poset $(\mathcal{L}\langle\varphi\rangle, \overset{*}{\rightarrow})$ is an upper semilattice.*

Proof. For arbitrary functions φ_1 and φ_2 from $\mathcal{L}\langle\varphi\rangle$, if $\varphi_1 = \varphi_{\| X_1}$ and $\varphi_2 = \varphi_{\| X_2}$ then for each $U \subseteq X_1$ and for each $V \subseteq X_2$ we have

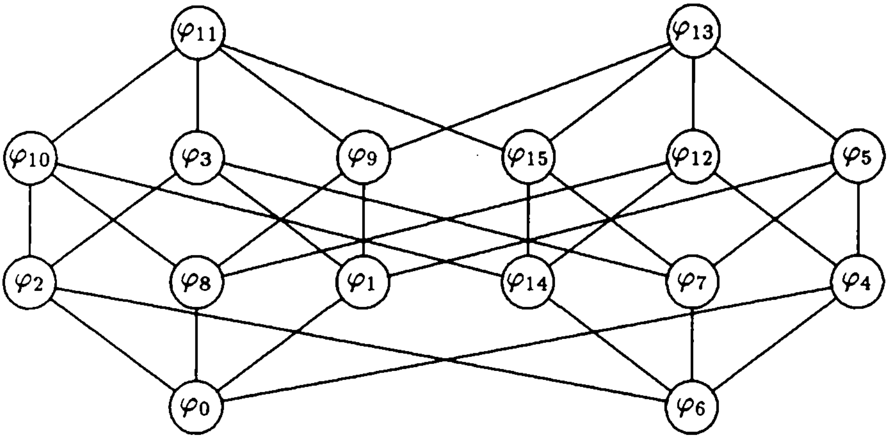

Figure 2.4. The diagram of $\overset{\bullet}{\rightarrow}$ in $\mathcal{F}^3$

$\varphi_{\|U} \in \mathcal{L}\langle\varphi\rangle$ and $\varphi_{\|V} \in \mathcal{L}\langle\varphi\rangle$. In particular $\varphi_{\|X_1\cap X_2} \in \mathcal{L}\langle\varphi\rangle$, therefore $\varphi_1 \vee \varphi_2 = \varphi_{\|X_1\cap X_2}$. ■

The semilattice $\left(\mathcal{L}\langle\varphi\rangle, \overset{\bullet}{\rightarrow}\right)$ may be extended to a lattice as follows. Let us set

$$\mathcal{L}^*\langle\varphi\rangle = \begin{cases} \mathcal{L}\langle\varphi\rangle, & \text{if } \left(\mathcal{L}\langle\varphi\rangle, \overset{\bullet}{\rightarrow}\right) \text{ is a lattice,} \\ \mathcal{L}\langle\varphi\rangle \cup \{\mathbf{0}\}, & \text{otherwise,} \end{cases}$$

where $\mathbf{0}$ denotes any object which is not a feedback function, and assume that $\mathbf{0} \overset{\bullet}{\rightarrow} \mathbf{0}$ and $\mathbf{0} \overset{\bullet}{\rightarrow} \psi$, if $\psi \in \mathcal{L}\langle\varphi\rangle$.

2.4. THEOREM. *The poset* $\left(\mathcal{L}^*\langle\varphi\rangle, \overset{\bullet}{\rightarrow}\right)$ *is a lattice.*

Proof. If there exists ψ such that $\psi \overset{\bullet}{\rightarrow} \varphi_1$ and $\psi \overset{\bullet}{\rightarrow} \varphi_2$, and if $\psi = \varphi_{\|X_1}$ and $\psi = \varphi_{\|X_2}$ then $\varphi_1 \wedge \varphi_2 = \psi_{\|X_1\cap X_2}$. Otherwise we set $\varphi_1 \wedge \varphi_2 = \mathbf{0}$. ■

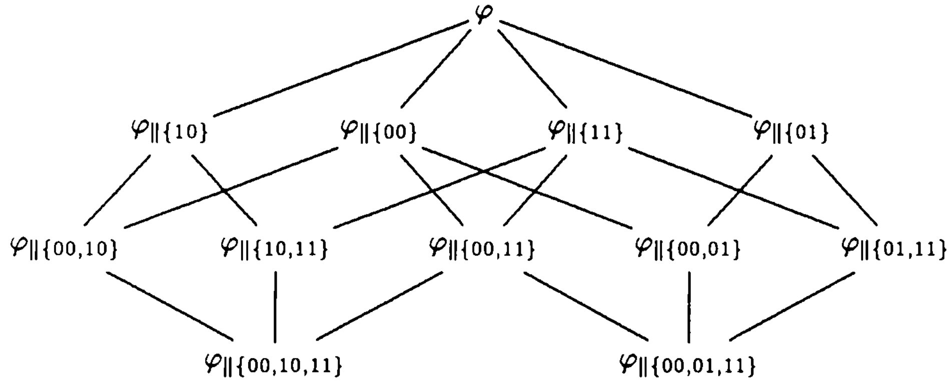

Figure 2.5. The poset $\left(\mathcal{L}\langle\varphi\rangle, \overset{\bullet}{\rightarrow}\right)$ for $\varphi = \varphi_{11}$.

3. The independent splits relation

It is convenient to analyse the relation $\dot{\rightarrow}$ with the help of a relation from $\{0,1\}^{k-1} \times \{0,1\}^{k-1}$. This relation deals with the vertices of the factor of a feedback function φ each of which may cause splitting one of the circuits of $B_k[\varphi]$. Elements u and v of $\{0,1\}^{k-1}$ will be in the relation iff the change of φ at $u_{(0)}$ and $u_{(1)}$ leaves the vertices $v_{(0)}$ and $v_{(1)}$ in the same circuit of $B_k[\varphi_{\|\{u\}}]$. It allows us to generalize Corollary 2.2 for more arguments.

The independent splits relation for $\varphi \in \mathcal{F}^k$ is a binary relation $\textcircled{)(}_\varphi \subseteq \{0,1\}^{k-1} \times \{0,1\}^{k-1}$ such that for arbitrary elements u and v of $\{0,1\}^{k-1}$ one of the following conditions holds:

(3.1) $(u,u) \in \textcircled{)(}_\varphi$ iff $(u_{(0)}, u_{(0)}\rangle_\varphi = (u_{(0)}, u_{(1)}\rangle_\varphi (u_{(1)}, u_{(0)}\rangle_\varphi$,

(3.2) if $u \neq v$ then $(u,v) \in \textcircled{)(}_\varphi$ iff $(u,u) \in \textcircled{)(}_\varphi$ and $(v,v) \in \textcircled{)(}_\varphi$ and either $v_{(0)}$ and $v_{(1)}$ do not occur in $(u_{(0)}, u_{(0)}\rangle_\varphi$ or the sequence $(u_{(0)}, u_{(0)}\rangle_\varphi$ has one of the form

$$(u_{(0)}, u_{(0)}\rangle_\varphi = (u_{(0)}, v_{(0)}\rangle_\varphi (v_{(0)}, v_{(1)}\rangle_\varphi (v_{(1)}, u_{(1)}\rangle_\varphi (u_{(1)}, u_{(0)}\rangle_\varphi$$
$$(u_{(0)}, u_{(0)}\rangle_\varphi = (u_{(0)}, v_{(1)}\rangle_\varphi (v_{(1)}, v_{(0)}\rangle_\varphi (v_{(0)}, u_{(1)}\rangle_\varphi (u_{(1)}, u_{(0)}\rangle_\varphi$$
$$(u_{(0)}, u_{(0)}\rangle_\varphi = (u_{(0)}, u_{(1)}\rangle_\varphi (u_{(1)}, v_{(0)}\rangle_\varphi (v_{(0)}, v_{(1)}\rangle_\varphi (v_{(1)}, u_{(0)}\rangle_\varphi$$
$$(u_{(0)}, u_{(0)}\rangle_\varphi = (u_{(0)}, u_{(1)}\rangle_\varphi (u_{(1)}, v_{(1)}\rangle_\varphi (v_{(1)}, v_{(0)}\rangle_\varphi (v_{(0)}, u_{(0)}\rangle_\varphi.$$

Note that if $(u,v) \in \textcircled{)(}_\varphi$ and the vertices $u_{(0)}, u_{(1)}, v_{(0)}, v_{(1)}$ are in the same circuit of $B_k[\varphi]$ then they have to keep the order as in Figure 3.1. The condition (3.1) and Theorem 2.1 imply

(3.3) $$\textcircled{)(}_\varphi = \emptyset \quad \text{iff} \quad \varphi \in \mathcal{LR}^k.$$

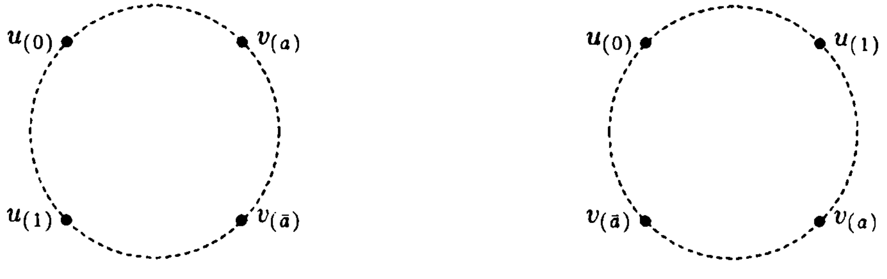

Figure 3.1.

The full characterization of the independent splits relations needs the confrontation them with the other relations, called *the interlacing relations,* defined and investigated in [5,6,7].

The interlacing relation of $\varphi \in \mathcal{F}^k$ is the relation $\otimes_\varphi \subseteq \{0,1\}^{k-1} \times \{0,1\}^{k-1}$ such that $(x,y) \in \otimes_\varphi$ iff the sequence $(x_{(0)}, x_{(0)}\rangle_\varphi$ has one of the form:

$$(x_{(0)},x_{(0)}\rangle_\varphi = (x_{(0)},y_{(0)}\rangle_\varphi(y_{(0)},x_{(1)}\rangle_\varphi(x_{(1)},y_{(1)}\rangle_\varphi(y_{(1)},x_{(0)}\rangle_\varphi$$

or

$$(x_{(0)},x_{(0)}\rangle_\varphi = (x_{(0)},y_{(1)}\rangle_\varphi(y_{(1)},x_{(1)}\rangle_\varphi(x_{(1)},y_{(0)}\rangle_\varphi(y_{(0)},x_{(0)}\rangle_\varphi.$$

Such a relation is *irreflexive* and *symmetric.* The connections between $\circledparallel_\varphi$ and $\otimes_\varphi$ are the best evident for the Hamiltonian functions: if $\omega \in \mathcal{H}^k$ then

$$\otimes_\omega \cup \circledparallel_\omega = \{0,1\}^{k-1} \times \{0,1\}^{k-1},$$

while $\otimes_\omega \cap \circledparallel_\omega = \emptyset$. In the general case we have

$$\otimes_\varphi \cup \circledparallel_\varphi = TR\{\varphi\} \times TR\{\varphi\},$$

with $TR\{\varphi\} = \{e \in \{0,1\}^{k-1} : (e,e) \in \circledparallel_\varphi\}$. (We have $TR\{\varrho\} = \emptyset$ for $\varrho \in \mathcal{LR}^k$ as well as $TR\{\omega\} = \{0,1\}^{k-1}$ for $\omega \in \mathcal{H}^k$.)

The difference between the relations $\otimes_\varphi$ and $\circledparallel_\varphi$ can be noticed if we observe the lines which join the vertices $x_{(0)}$ with $x_{(1)}$ as well as $y_{(0)}$ with $y_{(1)}$: if they are crossing then $(x,y) \in \otimes_\varphi$, otherwise $(x,y) \in \circledparallel_\varphi$. (If not all of the vertices $x_{(0)}, x_{(1)}, y_{(0)}, y_{(1)}$ are in the same circuit then $(x,y) \notin \otimes_\varphi$.)

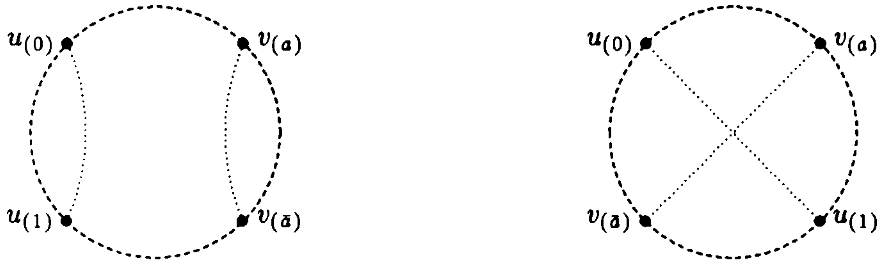

Figure 3.2.

3.1. THEOREM. *Let $\varphi \in \mathcal{F}^k$. For each $X \subseteq \{0,1\}^{k-1}$ we have*

$$\varphi_{\|X} \stackrel{\bullet}{\rightarrow} \varphi \quad \textit{iff} \quad X \times X \subseteq \circledparallel_\varphi.$$

Proof. For $X = \emptyset$ the proof is a direct consequence of the definition of the relation $\stackrel{\bullet}{\rightarrow}$. Let us assume that $X \neq \emptyset$ and let $\{X_1,\dots,X_m\}$ be a partition of X which corresponds with the family $\{C_1,\dots,C_m\}$ of the vertex disjoint circuits of $B_k[\varphi]$ such that for each $x \in X$ and for each $i \in \{1,\dots,m\}$

(*a*) $x \in X_i$ iff $x_{(0)}$ and $x_{(1)}$ are the vertices of C_i.

Necessity. Suppose that $\varphi_{\|X} \overset{\cdot}{\rightarrow} \varphi$. Because of (a) each element x of X satisfies the condition

$$(x_{(0)}, x_{(0)}\rangle_\varphi = (x_{(0)}, x_{(1)}\rangle_\varphi (x_{(1)}, x_{(0)}\rangle_\varphi,$$

which means that $(x, x) \in \mathbb{O}_\varphi$. From this and the definition of $\{X_1, \ldots, X_m\}$ it follows that for every $\tilde{X} \in \{X_1, \ldots, X_m\}$ and $\tilde{x} \in \tilde{X}$ we have $(x, \tilde{x}) \in \mathbb{O}_\varphi$ if $x \in X \setminus \tilde{X}$. Let $\tilde{X} \in \{X_1, \ldots, X_m\}$. If $|\tilde{X}| > 1$ then for arbitrary elements x and $\tilde{x}$ of $\tilde{X}$ we have

$$(b) \qquad \varphi_{\|\tilde{X}} \overset{\cdot}{\rightarrow} \varphi_{\|\{x,\tilde{x}\}} \rightarrow \varphi_{\|\{x\}} \rightarrow \varphi.$$

The above condition means that the following circuits $(x_{(0)}, x_{(0)}\rangle_{\varphi_{\|\{x,\tilde{x}\}}}$ and $(x_{(1)}, x_{(1)}\rangle_{\varphi_{\|\{x,\tilde{x}\}}}$ of $B_k[\varphi_{\|\{x,\tilde{x}\}}]$ are vertex disjoint and either the vertex $\tilde{x}_{(0)}$ belongs to one of them and the vertex $\tilde{x}_{(1)}$ belongs to none of them or conversely. (Otherwise the relation $\varphi_{\|\tilde{X}} \overset{\cdot}{\rightarrow} \varphi$ would not hold.) On the other hand, there exists a circuit $\tilde{C} \in \{C_1, \ldots, C_m\}$ in $B_k[\varphi]$ containing each of the vertices: $x_{(0)}, x_{(1)}, \tilde{x}_{(0)}, \tilde{x}_{(1)}$. If $(x, \tilde{x}) \notin \mathbb{O}_\varphi$ then it would exist $a \in \{0, 1\}$ such that

$$(x_{(0)}, x_{(0)}\rangle_\varphi = (x_{(0)}, \tilde{x}_{(a)}\rangle_\varphi (\tilde{x}_{(a)}, x_{(1)}\rangle_\varphi (x_{(1)}, \tilde{x}_{(\bar{a})}\rangle_\varphi (\tilde{x}_{(\bar{a})}, x_{(0)}\rangle_\varphi.$$

Then

$$\begin{aligned} (x_{(0)}, x_{(0)}\rangle_{\varphi_{\|\{x\}}} &= (x_{(1)}, \tilde{x}_{(\bar{a})}\rangle_\varphi (\tilde{x}_{(\bar{a})}, x_{(0)}\rangle_\varphi \\ (x_{(1)}, x_{(1)}\rangle_{\varphi_{\|\{x\}}} &= (x_{(0)}, \tilde{x}_{(a)}\rangle_\varphi (\tilde{x}_{(a)}, x_{(1)}\rangle_\varphi \end{aligned}$$

and next

$$(x_{(0)}, x_{(0)}\rangle_{\varphi_{\|\{x,\tilde{x}\}}} = (x_{(1)}, \tilde{x}_{(\bar{a})}\rangle_\varphi (\tilde{x}_{(a)}, x_{(1)}\rangle_\varphi (x_{(0)}, \tilde{x}_{(a)}\rangle_\varphi (\tilde{x}_{(\bar{a})}, x_{(0)}\rangle_\varphi.$$

The last equality disagree with the disjointness of the circuits $(x_{(0)}, x_{(0)}\rangle_{\varphi_{\|\{x,\tilde{x}\}}}$ and $(x_{(1)}, x_{(1)}\rangle_{\varphi_{\|\{x,\tilde{x}\}}}$ of $B_k[\varphi_{\|\{x,\tilde{x}\}}]$. Thereby each pair of elements of $\tilde{X}$ is in $\mathbb{O}_\varphi$.

Sufficiency. Suppose that $X \times X \subseteq \mathbb{O}_\varphi$ and let $\tilde{X} \in \{X_1, \ldots, X_m\}$. For each $x \in \tilde{X}$ let us set $\tilde{X}(x) = \{\tilde{x} \in \tilde{X} : (x, \tilde{x}) \in \mathbb{O}_\varphi\}$. If $\tilde{X}(x) = \{x\}$ then $\varphi_{\|\tilde{X}(x)} \rightarrow \varphi$, because of Theorem 2.1. If $|\tilde{X}(x)| > 1$ then for $\tilde{x} \in \tilde{X}(x) \setminus \{x\}$ we have

$$(x_{(0)}, x_{(0)}\rangle_\varphi = (x_{(0)}, \tilde{x}_{(a)}\rangle_\varphi (\tilde{x}_{(a)}, \tilde{x}_{(\bar{a})}\rangle_\varphi (\tilde{x}_{(\bar{a})}, x_{(1)}\rangle_\varphi (x_{(1)}, x_{(0)}\rangle_\varphi$$

or

$$(x_{(0)}, x_{(0)}\rangle_\varphi = (x_{(0)}, x_{(1)}\rangle_\varphi (x_{(1)}, \tilde{x}_{(a)}\rangle_\varphi (\tilde{x}_{(a)}, \tilde{x}_{(\bar{a})}\rangle_\varphi (\tilde{x}_{(\bar{a})}, x_{(0)}\rangle_\varphi.$$

Then

$$\begin{aligned}(x_{(0)}, x_{(0)})_{\varphi_{\|\{x\}}} &= (x_{(1)}, x_{(0)})_{\varphi}\\ (x_{(1)}, x_{(1)})_{\varphi_{\|\{x\}}} &= (x_{(0)}, \tilde{x}_{(a)})_{\varphi}(\tilde{x}_{(a)}, \tilde{x}_{(\bar{a})})_{\varphi}(\tilde{x}_{(\bar{a})}, x_{(1)})_{\varphi}\end{aligned}$$

or

$$\begin{aligned}(x_{(0)}, x_{(0)})_{\varphi_{\|\{x\}}} &= (x_{(1)}, \tilde{x}_{(a)})_{\varphi}(\tilde{x}_{(a)}, \tilde{x}_{(\bar{a})})_{\varphi}(\tilde{x}_{(\bar{a})}, x_{(0)})_{\varphi}\\ (x_{(1)}, x_{(1)})_{\varphi_{\|\{x\}}} &= (x_{(0)}, x_{(1)})_{\varphi},\end{aligned}$$

respectively. This means that $\varphi_{\|\{x\}} \rightarrow \varphi$ and $\mathbb{O}_{\varphi_{\|\{x\}}} = \mathbb{O}_{\varphi} \setminus \big(\{(x,\tilde{x}) : \tilde{x} \in \tilde{X}(x)\} \cup \{(\tilde{x},x) : \tilde{x} \in \tilde{X}(x)\}\big)$. It follows from the definition of $\overset{\bullet}{\rightarrow}$ that $\varphi_{\|X} \overset{\bullet}{\rightarrow} \varphi$. ■

3.2. Corollary. *Let $\varphi \in \mathcal{F}^k$. If $X \subseteq \{0,1\}^{k-1}$ then $\varphi_{\|X} \in \mathcal{LR}^k$ iff X is a maximal set such that $X \times X \subseteq \mathbb{O}_{\varphi}$.* ■

3.3. Corollary. *Let $\varphi \in \mathcal{F}^k$ and $X \subseteq \{0,1\}^{k-1}$. If $\varphi_{\|X} \overset{\bullet}{\rightarrow} \varphi$ then $\mathbb{O}_{\varphi_{\|X}} \subseteq \mathbb{O}_{\varphi}$.* ■

Theorem 3.1 gives an effective method to estabish all elements of the family $\mathcal{L}\langle\varphi\rangle$ and it describes its structure determined by $\overset{\bullet}{\rightarrow}$.

3.4. Example. For the feedback function $\varphi = \varphi_{11}$, where φ_{11} is defined in Table 2.2, we obtain

$$(000, 000)_{\varphi} = 001, 010, 101, 011, 111, 110, 100, 000.$$

Then the matrix which represents the characteristic function of $\mathbb{O}_{\varphi}$ has the form

$$\begin{array}{c c} & \begin{array}{cccc} 00 & 01 & 10 & 11 \end{array} \\ \begin{array}{c} 00\\ 01\\ 10\\ 11 \end{array} & \begin{pmatrix} 1 & 1 & 1 & 1\\ 1 & 1 & 0 & 1\\ 1 & 0 & 1 & 1\\ 1 & 1 & 1 & 1 \end{pmatrix}. \end{array}$$

So, there exist two different maximal sets mentioned in Corollary 3.2, namely $\{00, 10, 11\}$ and $\{00, 01, 11\}$. Then $\varphi_{\|\{00,10,11\}} = \varphi_0$ but $\varphi_{\|\{00,01,11\}} = \varphi_6$. (Note that the relations $\mathbb{O}_{\varphi_0}$ and $\mathbb{O}_{\varphi_6}$ are empty.) The poset $\big(\mathcal{L}\langle\varphi\rangle, \overset{\bullet}{\rightarrow}\,\big)$, the subset of $\big(\mathcal{F}^k, \overset{\bullet}{\rightarrow}\,\big)$ is presented in Figure 2.5.

3.5. Corollary. *Let $\varphi \in \mathcal{F}^k$. The poset $\big(\mathcal{L}\langle\varphi\rangle, \overset{\bullet}{\rightarrow}\,\big)$ is a lattice iff $\mathbb{O}_{\varphi}$ is an equivalence relation.* ■

4. An isomorphism of the posets $(\mathcal{L}\langle\varphi\rangle, \dot{\rightarrow}\ )$

Let $\varphi \in \mathcal{F}^k$. We shall state all functions $\tilde{\varphi} \in \mathcal{F}^k$ for which the posets $(\mathcal{L}\langle\varphi\rangle, \dot{\rightarrow}\ )$ and $(\mathcal{L}\langle\tilde{\varphi}\rangle, \dot{\rightarrow}\ )$ are isomorphic.

4.1. THEOREM. *Let $\varphi \in \mathcal{F}^k$. For every function $\tau \in \mathcal{F}^k$ the posets $(\mathcal{L}\langle\varphi\rangle, \dot{\rightarrow}\ )$ and $(\mathcal{L}\langle\tau\rangle, \dot{\rightarrow}\ )$ are isomorphic iff the relations $\circledcirc_\varphi$ and $\circledcirc_\tau$ are isomorphic.*

Proof. If $\mathcal{L}\langle\varphi\rangle = \{\varphi\}$ then the posets $(\mathcal{L}\langle\varphi\rangle, \dot{\rightarrow}\ )$ and $(\mathcal{L}\langle\tau\rangle, \dot{\rightarrow}\ )$ are isomorphic iff one of the equivalent conditions holds:

(a) $\mathcal{L}\langle\tau\rangle = \{\tau\}$,

(b) $\tau \in \mathcal{LR}^k$,

(c) $\circledcirc_\varphi = \emptyset = \circledcirc_\tau$.

The condition (c) means that the relations $\circledcirc_\varphi$ and $\circledcirc_\tau$ are isomorphic.

If $\mathcal{L}\langle\varphi\rangle$ contains the functions different from φ then, according to Theorem 3.1, each element of the family $\mathcal{L}\langle\varphi\rangle$ has the form $\varphi_{\|X}$, where X is a subset of $\{0,1\}^{k-1}$ such that the relation $\circledcirc_\varphi$ restricted to X is an equivalence relation.

Necessity. If the posets $(\mathcal{L}\langle\varphi\rangle, \dot{\rightarrow}\ )$ and $(\mathcal{L}\langle\tau\rangle, \dot{\rightarrow}\ )$ are isomorphic and the transformation $I\colon \mathcal{L}\langle\varphi\rangle \rightarrow \mathcal{L}\langle\tau\rangle$ is an isomorphism then for each $X \subseteq \{0,1\}^{k-1}$ such that $\varphi_{\|X} \in \mathcal{L}\langle\varphi\rangle$ and $\varphi_{\|X} \dot{\rightarrow} \varphi$ there exists $\tilde{X} \subseteq \{0,1\}^{k-1}$ satisfying the following conditions:

$$\tau_{\|\tilde{X}} = I(\varphi_{\|X}) \quad \text{and} \quad \tau_{\|\tilde{X}} \dot{\rightarrow} \tau,$$

and for every $x \in X$ it is true that

$$\varphi_{\|X} \rightarrow \varphi_{\|X\setminus\{x\}}$$

and there exists $\tilde{x} \in \tilde{X}$ satisfying the conditions

$$\tau_{\|\tilde{X}\setminus\{\tilde{x}\}} = I(\varphi_{\|X\setminus\{x\}}) \quad \text{and} \quad \tau_{\|\tilde{X}} \rightarrow \tau_{\|\tilde{X}\setminus\{\tilde{x}\}}.$$

Then every transformation $i\colon \{0,1\}^{k-1} \rightarrow \{0,1\}^{k-1}$ such that $i(x) = \tilde{x}$ is an isomorphism of the relations $\circledcirc_\varphi$ and $\circledcirc_\tau$.

Sufficiency. If $i\colon \{0,1\}^{k-1} \rightarrow \{0,1\}^{k-1}$ is an isomorphism of the relations $\circledcirc_\varphi$ and $\circledcirc_\tau$ then for every $X \subseteq \{0,1\}^{k-1}$ such that $\varphi_{\|X} \in \mathcal{L}\langle\varphi\rangle$ the relation $\circledcirc_\varphi$ restricted to $\tilde{X} = \{i(x) : x \in X\}$ is an equivalence relation. Therefore $\tau_{\|\tilde{X}} \in \mathcal{L}\langle\tau\rangle$ and $\tau_{\|\tilde{X}} \dot{\rightarrow} \tau$ and it is sufficient to set

$$I(\varphi_{\|X}) = \tau_{\|\tilde{X}}.$$

Then I is an isomorphism of the sets $\left(\mathcal{L}\langle\varphi\rangle, \overset{\bullet}{\to}\right)$ and $\left(\mathcal{L}\langle\tau\rangle, \overset{\bullet}{\to}\right)$. ∎

4.2. Corollary. *Let $\varphi \in \mathcal{F}^k$ and $X \subseteq \{0,1\}^{k-1}$. If $\varphi_{\|X} \overset{\bullet}{\to} \varphi$ then for every function $\tau \in \mathcal{F}^k$, for which there exists an isomorphism $i\colon \{0,1\}^{k-1} \to \{0,1\}^{k-1}$ of the relations $\circledcirc_\varphi$ and $\circledcirc_\tau$, the following conditions hold:*

(*a*) $\tau_{\|i(X)} \overset{\bullet}{\to} \tau$,

(*b*) *the relations $\circledcirc_{\varphi_{\|X}}$ and $\circledcirc_{\tau_{\|i(X)}}$ are isomorphic,*

(*c*) *the posets $\left(\mathcal{L}\langle\varphi_{\|X}\rangle, \overset{\bullet}{\to}\right)$ and $\left(\mathcal{L}\langle\tau_{\|i(X)}\rangle, \overset{\bullet}{\to}\right)$ are isomorphic.* ∎

4.3. Example. For arbitrary function $\varphi \in \mathcal{F}^k$ the transformation $i\colon \{0,1\}^{k-1} \to \{0,1\}^{k-1}$ defined by the equality

$$i(x_1, \dots, x_{k-1}) = (\bar{x}_1, \dots, \bar{x}_{k-1})$$

is an isomorphism of the relations $\circledcirc_\varphi$ and $\circledcirc_{\tilde{\varphi}}$, where

$$\tilde{\varphi}(x_1, x_2, \dots, x_k) = \varphi(x_1, \bar{x}_2, \dots, \bar{x}_k).$$

So, it transforms an arbitrary sequence $(c_1, c_2, \dots, c_k, c_{k+1}) \in \{0,1\}^{k+1}$ into the sequence $(\bar{c}_1, \bar{c}_2, \dots, \bar{c}_k, \bar{c}_{k+1})$. If $c_{k+1} = \tilde{\varphi}(c_1, c_2, \dots, c_k)$ then

$$\bar{c}_{k+1} = 1 + \tilde{\varphi}(c_1, c_2, \dots, c_k) = \tilde{\varphi}(\bar{c}_1, c_2, \dots, c_k) = \varphi(\bar{c}_1, \bar{c}_2, \dots, \bar{c}_k).$$

It means that the graphs $B_k[\varphi]$ and $B_k[\tilde{\varphi}]$ are isomorphic, so the relations $\circledcirc_\varphi$ and $\circledcirc_{\tilde{\varphi}}$ are isomorphic too.

4.4. Example. For arbitrary function $\varphi \in \mathcal{F}^k$ let us consider a function $\tilde{\varphi}$ such that

$$\tilde{\varphi}(x_1, x_2, \dots, x_k) = \varphi(x_1, x_k, \dots, x_2).$$

If $(x_1, x_2, \dots, x_k, x_{k+1}) \in \{0,1\}^{k+1}$ and $x_{k+1} = \varphi(x_1, x_2, \dots, x_k)$ then in comparison with the condition (2.2) we have $x_{k+1} = x_1 + \varphi(0, x_2, \dots, x_k)$, from where

(*a*) $x_1 = \varphi(0, x_2, \dots, x_k) + x_{k+1}$.

We shall prove that the graphs $B_k[\varphi]$ and $B_k[\tilde{\varphi}]$ are isomorphic. To this purpose let us notice that each circuit of the graph $B_k[\varphi]$ represented by the sequence of the vertices $\langle v, v\rangle_\varphi$ determines the finite binary sequence $c_1, \dots, c_p$ such that

(*b*) $v = (c_1, \dots, c_k)$,

(*c*) $c_{i+k} = \varphi(c_i, \dots, c_{i+k-1})$, for $i \in \{1, \dots, p-k\}$,

where p is a number of the elements of the sequence $\langle v, v\rangle_\varphi$. Now, let us consider the sequence $c_p, \dots, c_1$ and notice that it corresponds with the sequence $\langle u, u\rangle_\varphi$ of the vertices of a certain circuit of $B_k[\tilde{\varphi}]$. According to the conditions (a) and (b) we have

$(d)\quad c_i = \tilde{\varphi}(c_{i+k}, c_{i+k-1}, \ldots, c_{i+1}).$

Hence, the transformation $i^*\colon \{0,1\}^k \to \{0,1\}^k$ satisfying the condition

$$i^*(c_1, \ldots, c_k) = (c_p, \ldots, c_{p-k+1})$$

states an isomorphism of the graphs $B_k[\varphi]$ and $B_k[\tilde{\varphi}]$. It follows that the transformation $i\colon \{0,1\}^{k-1} \to \{0,1\}^{k-1}$ defined by the equality

$$i(x_1, \ldots, x_{k-1}) = (x_{k-1}, \ldots, x_1)$$

states an isomorphism of the relations $\textcircled{)(}_\varphi$ and $\textcircled{)(}_{\tilde{\varphi}}$.

4.5. Example. *For $k = 5$ and the functions φ and $\tilde{\varphi}$ defined as follows:*

$$\varphi(x_1, \ldots, x_5) = x_1 + x_2x_3x_4x_5 + \bar{x}_2\bar{x}_3\bar{x}_4x_5$$
$$\tilde{\varphi}(x_1, \ldots, x_5) = \varphi(x_1, \ldots, x_5) + \bar{x}_2x_3x_4 + \bar{x}_3x_4x_5,$$

we have

$$\textcircled{)(}_\varphi = \textcircled{)(}_{\tilde{\varphi}} = \left\{\begin{array}{l} (0001, 0001), \\ (0001, 1111), \\ (1111, 1111), \\ (1111, 0001), \\ (1111, 1000), \\ (1000, 1111), \\ (1000, 1000) \end{array}\right\}.$$

It means that the sets $(\mathcal{L}\langle\varphi\rangle, \overset{\bullet}{\rightarrow})$ and $(\mathcal{L}\langle\tilde{\varphi}\rangle, \overset{\bullet}{\rightarrow})$ are isomorphic.

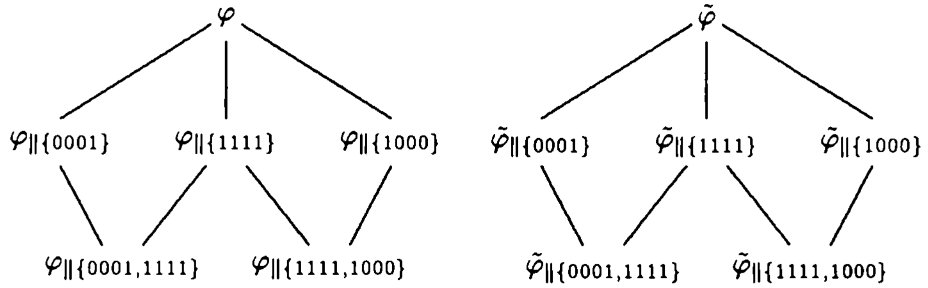
φ
$\varphi\|\{0001\}$
$\varphi\|\{1111\}$
$\varphi\|\{1000\}$
$\varphi\|\{0001,1111\}$
$\varphi\|\{1111,1000\}$
$\tilde{\varphi}$
$\tilde{\varphi}\|\{0001\}$
$\tilde{\varphi}\|\{1111\}$
$\tilde{\varphi}\|\{1000\}$
$\tilde{\varphi}\|\{0001,1111\}$
$\tilde{\varphi}\|\{1111,1000\}$

Figure 4.1. The sets $(\mathcal{L}\langle\varphi\rangle, \overset{\bullet}{\rightarrow})$ and $(\mathcal{L}\langle\tilde{\varphi}\rangle, \overset{\bullet}{\rightarrow})$ from Example 4.5.

The above example shows that may exist feedback functions with the same independent splits relation. We can state a transformation of a feedback function which preserves its independent splits relation.

4.6. THEOREM. *For each* $X \subseteq \{0,1\}^{k-1} \setminus TR\{\varphi\}$ *we have*

$$\mathbb{O}_{\varphi_{\|X}} = \mathbb{O}_{\varphi} \quad \text{iff} \quad TR\{\varphi_{\|X}\} = TR\{\varphi\}.$$

Proof. The proof of the necessity is obvious. Let us suppose that $TR\{\varphi_{\|X}\} = TR\{\varphi\}$. If X is nonempty then there exists a nonempty subset U of X such that $\varphi \dot{\rightarrow} \varphi_{\|U}$. By Corollary 3.3 we obtain $\mathbb{O}_{\varphi} \subsetneq \mathbb{O}_{\varphi_{\|U}}$. On the other hand we have $\varphi_{\|X} \dot{\rightarrow} \varphi_{\|U}$, thereby $\mathbb{O}_{\varphi_{\|X}} \subsetneq \mathbb{O}_{\varphi_{\|U}}$. This implies, because of $TR\{\varphi_{\|X}\} = TR\{\varphi\}$, the equality $\mathbb{O}_{\varphi} = \mathbb{O}_{\varphi_{\|X}}$. ∎

References

[1] G. Birkhoff, T.C. Bartee, *Modern Applied Algebra*, McGraw-Hill Company, 1970.

[2] H. Fredricksen, *A survey of full length nonlinear shift register cycle algorithms*, SIAM Rev. 24(1982), 195-221.

[3] S.W. Golomb, *Shift register sequences*, Holden-Day, San Francisco 1967.

[4] R. Lidl, H. Niederreiter, *Introduction to finite fields and their applications*, Cambridge University Press, Cambridge 1986.

[5] M. Łatko, *The similitude of shift registers*, Demonstratio Math. 19(1986), 469- 485.

[6] M. Łatko, *On a construction of all de Bruijn cycles defined by Lempel's homomorphism*, Demonstratio Math. 21(1988), 441-455.

[7] M. Łatko, *Design of the maximal factors in the de Bruijn graphs*, (in Polish), Ph. D. thesis, Lublin 1987.

[8] P. Wlaź, J. Żurawiecki, *An algorithm for generating M-sequences using universal circuit matrix*, Ars Combinatoria, 41 (1995), 203–216.

[9] M. Yoeli, *Counting with nonlinear feedback shift registers*, IEEE Trans. Comput. 124(1963), 357-361.

[10] J. Żurawiecki, *Locally reducible iterative systems*, Demonstratio Math. 23(1990), 961–983.

[11] J. Żurawiecki, *The strong similitude of Hamiltonian circuits of a de Bruijn graph*, Journal of Inf. Process. Cybern. EIK 28(1992)6, 385-399.

INSTITUTE OF APPLIED MATHEMATICS
TECHNICAL UNIVERSITY IN LUBLIN
Bernardyńska 13
20-950 LUBLIN, POLAND

Received May 26, 1994.