Canonical form of the universal circuits matrix of feedback functions

Jerzy Żurawiecki

Department of Applied Mathematics
Technical University of Lublin
Nadbystrzycka 38, 20-618 Lublin

This paper deals with a connection between the universal circuits matrix [10] and the crossing relation [1,5]. The value of the universal circuits matrix obtained for $\bar{\omega}$, where ω is an arbitrary feedback function that generates de Bruijn sequences, forms the binary matrix that represents the crossing relation of ω. This result simplifies the design and study of the feedback functions that generate the de Bruijn sequences and allows us to decipher many informations about the adjacency graphs of another feedback functions. For example, we apply these results to analyze the Hauge-Mykkeltveit classification of a family of de Bruijn sequences [4].

1. Introduction

One of useful tools for a design of stream ciphers are periodic binary sequences defined by *feedback functions.* Very important are the ones with maximal period, that is equal 2^k when the corresponding feedback function has k arguments. We call them *the de Bruijn sequences of order k* ([3]).

The difficulties with finding of a simple algorithm generating each of $2^{2^{k-1}-k}$ de Bruijn sequences are one of the guarantee of a relative safety of stream ciphers based on such sequences. If a feedback function does not define sequences with maximal period then it defines an undirected graph (called *the adjacency graph*) each of the spanning trees of which determines a de Bruijn sequence. Many known algorithms generate de Bruijn sequences after modification of a chosen feedback function according to one of the spanning trees of its adjacency graph. A useful tool to study the adjacency graphs is *universal circuit matrix* [10], that is, a mapping, the arguments of which are the feedback functions while the values – matrices, the rows of which, generate the vector space of the adjacency graphs. There is an effective way to obtain the values of the universal circuits matrix, and consequently the spanning trees of the adjacency graphs [7].

Generally, the spanning trees of the adjacency graph of one of the feedback functions do not suffice for obtaining all de Bruijn sequences. If one of the de Bruijn sequences of order k is known then the others can be obtained with help of a binary relation defined by the sequel of segments of length $k-1$. These relations, discovered by Cohn and Lempel [1], and studied by Latko [5], we call *the crossing relations.* An arbitrary crossing relation determines all feedback functions that generate the de Bruijn sequences of given order.

The main result of this paper establishes a simple connection between the universal circuits matrix and the family of crossing relations. For an arbitrary feedback function ω that generates a de Bruijn sequence, it is sufficient to transform the universal circuits matrix, using Gaussian operations only, to the form in which its value obtained for the feedback function $\bar{\omega}$ forms the characteristic matrix of the crossing relation of ω. This allows us to decipher many informations about the feedback functions. In particular, it has been shown that the fundamental circuits as well as the fundamental cut-sets of an adjacency graph a spanning tree of which determines ω are represented by families of rows of the binary representation of the crossing relation of ω. Thereby we can easily establish the other spanning trees of this adjacency graph and the corresponding de Bruijn sequences. We also present a few remarks about Hauge-Mykkeltveit classification of de Bruijn sequences [4].

2. The feedback functions

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

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

for each $(x_1, \ldots, x_k) \in \{0,1\}^k$, ($x_1 = x_1 + 1$ in $GF(2)$). Each function from $\mathcal{F}^k$ will be called a *feedback function.*

Each feedback function φ defines the family of 2^k infinite sequences $s_1, s_2, \ldots$ such that

$$(2.2) \quad (s_1, \ldots, s_k) \in \{0,1\}^k \quad \text{and} \quad s_{k+i} = \varphi(s_i, \ldots, s_{k+i-1}) \text{ for } i \geq 1.$$

It follows from (2.1) that each of the sequences is periodic, that is, there exists $p \in \{1, \ldots, 2^k\}$ such that $s_{i+p} = s_i$ for $i \geq 1$. Thereby we represent them as circuits of the directed graph B_k, called *the de Bruijn graph of order* k, that consists of the elements of $\{0,1\}^k$ as the vertices, where the vertex $(v_1, v_2, \ldots, v_k)$ is followed by the vertices $(v_2, \ldots, v_k, 0)$ and $(v_2, \ldots, v_k, 1)$. Each feedback function φ determines a maximal subgraph $B_k[\varphi]$ of B_k composed of disjoint directed circuits in which the vertex $v = (v_1, \ldots, v_k)$ is followed by $v' = (v_2, \ldots, v_k, \varphi(v))$. The graph $B_k[\varphi]$ is said to be *the factor of* B_k *corresponding to* φ.

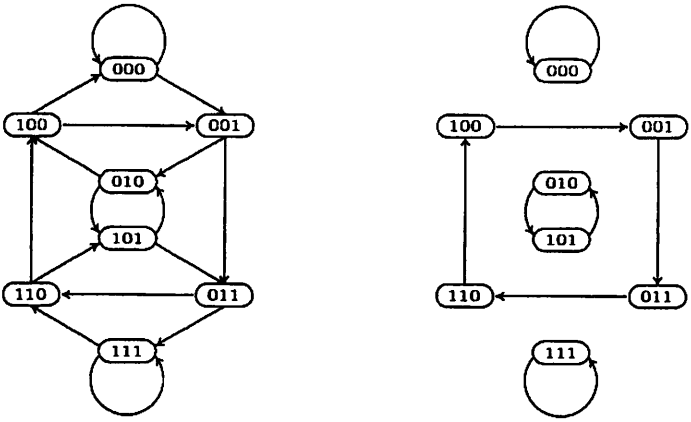


Figure 2.1. The de Bruijn graph B_3 and the factor $B_3[\alpha]$ with $\alpha(x_1, x_2, x_3) = x_1 + x_2 + x_3$

Note that $\varphi\colon \{0,1\}^k \to \{0,1\}$ is a feedback function if and only if

$$\varphi(x_1, x_2, \dots, x_k) = x_1 + \varphi(0, x_2, \dots, x_k), \tag{2.3}$$

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

$$\varphi_{\|X}(x_1, x_2, \dots, x_k) = \varphi(x_1, x_2, \dots, x_k) + \chi_X(x_2, \dots, x_k) \tag{2.4}$$

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

$$\mathcal{F}^k = \{\varphi_{\|X}\colon X \subseteq \{0,1\}^{k-1}\} \tag{2.5}$$

permitting to observe changes in a factor of the de Bruijn graph caused by the modifications of the values of the corresponding feedback function. The basis for applications of this property is the case when X consists of one element. To present this case assume that $(v, v)_\varphi$ is the sequence of consecutive vertices in the circuit of $B_k[\varphi]$, from the vertex followed v to the vertex v.

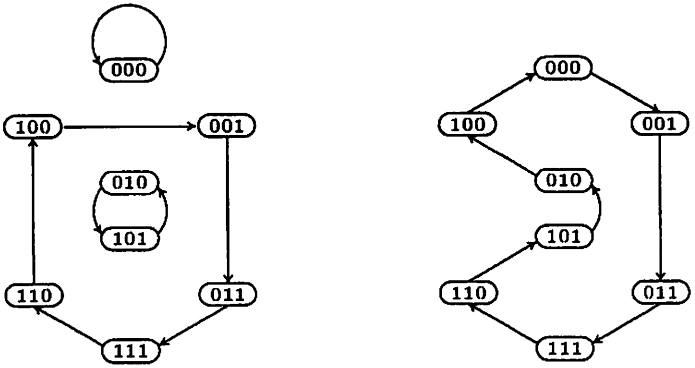


Figure 2.2. Factors $B_3[\alpha_{\|\{11\}}]$ and $B_3[\alpha_{\|\{00,10,11\}}]$

2.1. Theorem. [8] *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 $(v, v)_\varphi$ then for $u = (v_2, \ldots, v_k)$ we have:*

$$(v, v)_{\varphi_{\|\{u\}}} = (\hat{v}, \hat{v})_\varphi (v, v)_\varphi \text{ and } \hat{v} \text{ occurs in } (v, v)_{\varphi_{\|\{u\}}},$$

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

Theorem 2.1 establishes a natural order in $\mathcal{F}^k$. Let $\longrightarrow \subseteq \mathcal{F}^k \times \mathcal{F}^k$ be the binary relation such that for arbitrary feedback functions φ and ψ we have $\varphi \longrightarrow \psi$ if and only if there exists $u \in \{0,1\}^{k-1}$ such that:

(2.6) $\psi = \varphi_{\|\{u\}}$,

(2.7) *the vertices $v = (0, u_2, \ldots, u_k)$ and $\hat{v} = (1, u_2, \ldots, u_k)$ are in different circuits of $B_k[\varphi]$.*

Let $\overset{*}{\longrightarrow}$ be the reflexive and transitive closure of $\longrightarrow$. Then $\overset{*}{\longrightarrow}$ forms a partial order in $\mathcal{F}^k$. Some properties of this order have been presented in [6,11]. In particular, the maximal elements of $\mathcal{F}^k$ ordered by $\overset{*}{\longrightarrow}$ are the feedback functions, the factors of which forms Hamiltonian circuits in de Bruin graph, while the minimal ones are the feedback functions, the factors of which consist of circuits where none of them contains the $(x_1, x_2, \ldots, x_k)$ and $(\bar{x}_1, x_2, \ldots, x_k)$ in the same circuit [9].

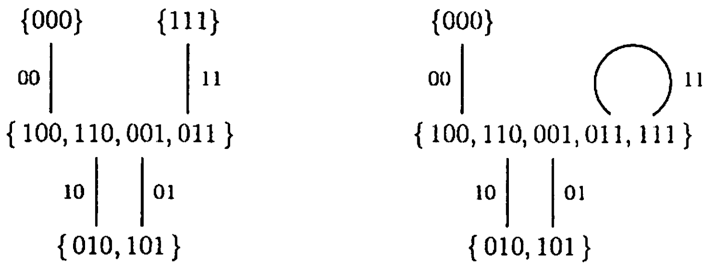


Figure 2.3. The adjacency graphs Q_α and $Q_{\alpha_{\|\{11\}}}$

For the complete characteristic of this order it is convenient to exploit the notion of the adjacency graph of a feedback function. For each $\varphi \in \mathcal{F}^k$ let $\{0,1\}^k/\varphi$ be the partition of $\{0,1\}^k$ composed of the sets each of which consists of the vertices of a circuit of $B_k[\varphi]$. The undirected graph Q_φ with $A \in \{0,1\}^k/\varphi$ as the vertices and with $e \in \{0,1\}^{k-1}$ as the edges: an edge $e = (e_1, \ldots, e_{k-1})$ is incident to A if and only if A contains $(0, e_1, \ldots, e_{k-1})$ or $(1, e_1, \ldots, e_{k-1})$, is called *the adjacency graph of* φ. Let $Q_\varphi[D]$ be the subgraph of Q_φ composed of the vertices of Q_φ and the edges from $D \subseteq \{0,1\}^{k-1}$. The following theorem establishes the fundamental connection between the relations $\varphi \overset{*}{\rightarrow} \varphi_{\|D}$ and the the subgraphs $Q_\varphi[D]$ of Q_φ.

2.2. Theorem. *Let $\varphi \in \mathcal{F}^k$. For each $D \subseteq \{0,1\}^{k-1}$ we have:*

$$\varphi \overset{*}{\rightarrow} \varphi_{\|D} \quad \textit{if and only if} \quad Q_\varphi[D] \quad \textit{is the graph without circuits.}$$

Proof. Necessity. Let us suppose that $\varphi \overset{*}{\rightarrow} \varphi_{\|D}$. Because of (2.6) and (2.7) we see that if $D = \{d\}$ then $\varphi \rightarrow \varphi_{\|\{d\}}$ if and only if $Q_\varphi[\{d\}]$ is not a loop, that is, it does not form a circuit. Thereby, it follows from the definition of $\overset{*}{\rightarrow}$ that for an arbitrary $D \subseteq \{0,1\}^{k-1}$ there exists an order $d_1, \ldots, d_m$ of the elements of D such that $\varphi \overset{*}{\rightarrow} \varphi_{\|\{d_1,\ldots,d_i\}}$ and $Q_\varphi[\{d_1, \ldots, d_i\}]$ does not contain any circuit, for each $i \in \{1, \ldots, m\}$. This completes the proof of necessity.

Sufficiency. If $Q_\varphi[D]$ has not any circuits then for each $e \in D$ we have $\varphi \overset{*}{\rightarrow} \varphi_{\|\{e\}}$ and $Q_{\varphi_{\|\{e\}}}[D \setminus \{e\}]$ has not any circuits too. This implies $\varphi \overset{*}{\rightarrow} \varphi_{\|D}$. ■

For the function α, the factor of which is presented in Figure 2.1, we have $\alpha \rightarrow \alpha_{\|\{11\}}$, and $\alpha \overset{*}{\rightarrow} \alpha_{\|\{00,10,11\}}$. (Compare with Fig. 2.2.)

3. The Hamiltonian functions and the crossing relation

Each feedback function $\varphi \in \mathcal{F}^k$ such that $B_k[\varphi]$ forms in B_k a Hamiltonian circuit we will call *a Hamiltonian function.* The set of all Hamiltonian functions will be denoted by $\mathcal{H}^k$. It is well known [3] that there exists $2^{2^{k-1}-k}$ Hamiltonian functions. Theorem 2.3 implies that the spanning trees of the adjacency graph of a feedback function establish a family of Hamiltonian functions. Generally, this family does not contain all Hamiltonian functions. But it appears that each Hamiltonian function contains the information about the others. In order to read this information it is sufficient to construct a binary relation in the set $\{0,1\}^{k-1}$. It is defined by the order of the vertices: $(0, x_2, \ldots, x_k)$, $(1, x_2, \ldots, x_k)$, $(0, y_2, \ldots, y_k)$, $(1, y_2, \ldots, y_k)$ of B_k in the corresponding Hamiltonian circuit. To this purpose let $\hat{x} = (\bar{x}_1, x_2, \ldots, x_k)$ for $x = (x_1, x_2, \ldots, x_k)$.

For $\omega \in \mathcal{H}^k$ let $\times_\omega$ be the binary relation in $\{0,1\}^{k-1}$ such that for arbitrary elements $u = (u_1, \ldots, u_{k-1})$ and $v = (v_1, \ldots, v_{k-1})$ of $\{0,1\}^{k-1}$, if $x = (0, u_1, \ldots, u_{k-1})$ and $y = (0, v_1, \ldots, v_{k-1})$ then $(u,v) \in \times_\omega$ if and only if either

$$(x,x\rangle_\omega = (x,y\rangle_\omega (y,\hat{x}\rangle_\omega (\hat{x},\hat{y}\rangle_\omega (\hat{y},x\rangle_\omega$$

or

$$(x,x\rangle_\omega = (x,\hat{y}\rangle_\omega (\hat{y},\hat{x}\rangle_\omega (\hat{x},y\rangle_\omega (y,x\rangle_\omega .$$

Of course $(u,v) \in \times_\omega$ if and only if $(v,u) \in \times_\omega$.

In a sequence $(x,x\rangle_\omega$ each element of $\{0,1\}^{k-1}$ appears twice. Write the elements of $(x,x\rangle_\omega$ on a circle and join the points with the same element of $\{0,1\}^{k-1}$ with line. Then $(u,v) \in \times_\omega$ if and only if the lines that join two points with u and two points with v crossed. Thereby u and v are said to be *ω-crossed.*

Let $\mathcal{X}_\omega$ be the characteristic function of $\times_\omega$, that is the function defined on $\{0,1\}^{k-1} \times \{0,1\}^{k-1}$ as follows

$$\mathcal{X}_\omega(u,v) = \begin{cases} 1, & \text{if } (u,v) \in \times_\omega, \\ 0, & \text{otherwise.} \end{cases}$$

We represent $\mathcal{X}_\omega$ as the binary matrix with the rows and columns ordered by an order of $\{0,1\}^{k-1}$, usually lexicographically. Then $\mathcal{X}_\omega$ is a symmetric matrix. Sometimes we will identify the set $\{0,1\}^{k-1}$ with the set $\{0,1,\ldots,2^{k-1}-1\}$ by the bijection $(x_1, \ldots, x_{k-1}) \rightarrow x_1 2^{k-2} + \cdots + x_{k-1} 2^0$.

x	$\omega_1(x)$	$\omega_2(x)$	$\omega_3(x)$	$\omega_4(x)$	$\omega_5(x)$	$\omega_6(x)$	$\omega_7(x)$	$\omega_8(x)$
0000	1	1	1	1	1	1	1	1
0001	1	0	1	0	0	1	1	0
0010	0	0	0	0	1	1	1	1
0011	1	1	0	0	1	1	0	0
0100	0	1	0	1	1	0	0	1
0101	1	1	1	1	0	0	0	0
0110	0	0	1	1	0	0	1	1
0111	1	1	1	1	1	1	1	1
1000	0	0	0	0	0	0	0	0
1001	0	1	0	1	1	0	0	1
1010	1	1	1	1	0	0	0	0
1011	0	0	1	1	0	0	1	1
1100	1	0	1	0	0	1	1	0
1101	0	0	0	0	1	1	1	1
1110	1	1	0	0	1	1	0	0
1111	0	0	0	0	0	0	0	0

x	$\omega_9(x)$	$\omega_{10}(x)$	$\omega_{11}(x)$	$\omega_{12}(x)$	$\omega_{13}(x)$	$\omega_{14}(x)$	$\omega_{15}(x)$	$\omega_{16}(x)$
0000	1	1	1	1	1	1	1	1
0001	0	0	1	0	1	1	0	1
0010	1	1	1	1	1	1	1	1
0011	1	0	0	0	0	1	1	1
0100	0	0	0	1	1	0	1	1
0101	1	1	1	1	1	1	1	1
0110	0	1	0	0	1	1	1	0
0111	1	1	1	1	1	1	1	1
1000	0	0	0	0	0	0	0	0
1001	1	1	0	1	0	0	1	0
1010	0	0	0	0	0	0	0	0
1011	0	1	1	1	1	0	0	0
1100	1	1	1	0	0	1	0	0
1101	0	0	0	0	0	0	0	0
1110	1	0	1	1	0	0	0	1
1111	0	0	0	0	0	0	0	0

Figure 3.1. The family $\mathcal{H}^4$

$$\begin{array}{c|cccccccc|} & 000 & 001 & 010 & 011 & 100 & 101 & 110 & 111 \\ \hline 000 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 001 & 0 & 0 & 1 & 0 & 1 & 0 & 0 & 0 \\ 010 & 0 & 1 & 0 & 1 & 1 & 1 & 1 & 0 \\ 011 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 \\ 100 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 \\ 101 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 110 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 \\ 111 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{array}$$

Figure 3.2. The matrix representation of $\times_{\omega_1}$ with ω_1 from Figure 3.1

A relation $\times_\omega$ is connected with theorem 2.1. Note that $(u, v) \in \times_\omega$ if and only if

$$\omega_{\|\{u\}} \to \omega \quad \text{and} \quad \omega_{\|\{u\}} \to \omega_{\|\{u,v\}}.$$

This implies that $\omega_{\|\{u,v\}}$ is also a Hamiltonian functions. Thereby $\times_\omega$ determines all Hamiltonian functions that differ in minimal number of arguments from ω. In order to establish the other Hamiltonian functions let us assume that for each $A \subseteq \{0,1\}^{k-1}$ by $\mathcal{X}_\omega[A]$ we denote the matrix obtained from $\mathcal{X}_\omega$ by deleting the rows and columns corresponding to $\{0,1\}^{k-1} \setminus A$.

3.1. Theorem. [1] *For each $\omega \in \mathcal{H}^k$ and for each $X \subseteq \{0,1\}^{k-1}$ we have $\omega_{\|X} \in \mathcal{H}^k$ if and only if $X = \emptyset$ or the matrix $\mathcal{X}_\omega[X]$ is nonsingular. In particular, $\omega_{\|\{i,j\}}$ is a Hamiltonian function if and only if the element x_{ij} of $\mathcal{X}_\omega$ is equal to* 1. ∎

It follows from the above theorem that if we determine for a Hamiltonian function all nonsingular submatrices $\mathcal{X}_\omega[X]$ of $\mathcal{X}_\omega$ then we determine all remaining Hamiltonian functions. In particular, the nonzero elements of $\mathcal{X}_\omega$ directly indicate some of the Hamiltonian function. It is easy to prove that apart from the rows corresponding to $(0\ldots0)$ and $(1\ldots1)$ each of the others contains at least one element equal to 1. Since the matrix is symmetric and its main diagonal consists of zeros, we can directly obtain at least $2^{k-1} - 3$ new Hamiltonian functions, however, not more than $1 + 2 + \cdots + 2^{k-1} - 3 = (2^{k-2} - 1) \cdot (2^{k-1} - 3)$. For each of them we can construct the new matrix of the crossing relation, and basing on it — new Hamiltonian functions.

3.2. Example. Note that $\mathcal{X}_{\omega_1}[X]$ with $X = \{0,1\}^{k-1} \setminus \{000, 111\}$ is nonsingular (Fig. 3.2). Thereby $\omega_{1\|X} \in \mathcal{H}^k$. One can observe that $\omega_{1\|X} = \omega_8$.

4. Universal circuits matrix of the adjacency graphs

The adjacency graphs of the feedback functions can be partially described by two vector spaces over $GF(2)$: the cut-set space $CUT\langle\varphi\rangle$, defined as the smallest vector space generated with the family of characteristic functions of the cut-sets of Q_φ, and the circuit space $CIR\langle\varphi\rangle$, defined as the smallest vector space generated with the family of characteristic functions of the circuits of Q_φ. (Cf. [2, Chapter 6].) For example, the Hauge-Mykkeltveit classification of de Bruijn sequences has been essentially based on some automorphisms of $CIR\langle\vartheta\rangle$, where $\vartheta(x_1, x_2, \ldots, x_k) = x_1$ [4, Lemma 4].

For each $\varphi \in \mathcal{F}^k$ the vector space $CUT\langle\varphi\rangle$ is generated by the family of functions h: $\{0,1\}^{k-1} \to \{0,1\}$ such that

$$h(e_1, \ldots, e_{k-1}) = \chi_A(0, e_1, \ldots, e_{k-1}) + \chi_A(1, e_1, \ldots, e_{k-1})$$

for $A \in \{0,1\}^k/\varphi$ and it follows from [2, Chapter 7] that $\dim CUT\langle\varphi\rangle = |\{0,1\}^k/\varphi| - 1$, since Q_φ is easily seen to be connected, and $\dim CIR\langle\varphi\rangle = 2^{k-1} + 1 - |\{0,1\}^k/\varphi|$, because the spaces $CIR\langle\varphi\rangle$ and $CUT\langle\varphi\rangle$ are orthogonal complements. Note that $\varphi \xrightarrow{*} \psi$ implies $CUT\langle\psi\rangle \subseteq CUT\langle\varphi\rangle$ and $CIR\langle\varphi\rangle \subseteq CIR\langle\psi\rangle$, but not conversely.

4.1. Example. For $\alpha(x_1, x_2, x_3) = x_1 + x_2 + x_3$ (See Fig. 2.1 and 2.3) we have $CIR\langle\alpha\rangle = \{g_0, g_1\}$ and $CUT\langle\alpha\rangle = \{h_0, h_1, h_2, h_3, h_4, h_5, h_6, h_7\}$, where

x	$g_0(x)$	$g_1(x)$
00	0	0
01	0	1
10	0	1
11	0	0

x	$h_0(x)$	$h_1(x)$	$h_2(x)$	$h_3(x)$	$h_4(x)$	$h_5(x)$	$h_6(x)$	$h_7(x)$
00	0	1	0	0	1	1	0	1
01	0	0	1	0	1	0	1	1
10	0	0	1	0	1	0	1	1
11	0	0	0	1	0	1	1	1

Note that $CIR\langle\alpha\rangle \subseteq CIR\langle\alpha_{\|\{11\}}\rangle$ and $CUT\langle\alpha_{\|\{11\}}\rangle \subseteq CUT\langle\alpha\rangle$.

There exists a simple tool for description of the adjacency graphs of the feedback functions and the corresponding vector spaces. Let us consider a total function $f : \{0,1\}^k \to \{0,1\}$ such that

$$f(x_1,\dots,x_k) = f(x_2,\dots,x_k,\varphi(x_1,\dots,x_k)). \tag{4.1}$$

If we set $f(x_1,\dots,x_k) = f_0(x_1,\dots,x_{k-1}) + f_1(x_1,\dots,x_{k-1}) \cdot x_k$ in $GF(2)$ then the above equality has the form:

$$\begin{aligned} &f_0(x_1,\dots,x_{k-1}) + f_0(x_2,\dots,x_k) + \\ &f_1(x_1,\dots,x_{k-1}) \cdot x_k + f_1(x_2,\dots,x_k) \cdot \varphi(x_1,x_2,\dots,x_k) = 0, \end{aligned} \tag{4.2}$$

which may be considered as a system of 2^k linear equations with the unknowns $f_0(u)$ and $f_1(u)$ for $u \in \{0,1\}^{k-1}$. By linear transformations of (4.2) we obtain the following system of linear equations dealing only with the unknowns $f_1(u)$:

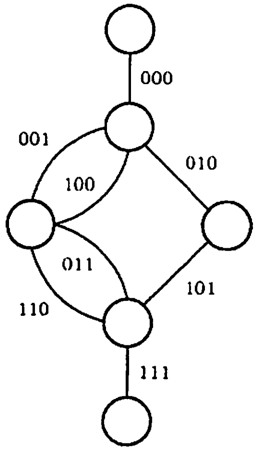
$$\begin{cases} f_1(0,x_1,\dots,x_{k-2}) + f_1(x_1,\dots,x_{k-2},0) + \\ f_1(1,x_1,\dots,x_{k-2}) + f_1(x_1,\dots,x_{k-2},1) = 0, \\ \quad \text{for } (x_1,\dots,x_{k-2}) \in \{0,1\}^{k-2} \setminus \{(1,\dots,1)\}; \\ \varphi(0,0,\dots,0) \cdot f_1(0,\dots,0) = 0; \\ f_1(x_1,\dots,x_{k-2},0) + f_1(x_1,\dots,x_1,x_1) + S_\varphi^1(0,\dots,0) + \\ S_\varphi^0(x_1,\dots,x_{k-2},0) + S_\varphi^1(x_1,\dots,x_{k-2},0) = 0, \\ \quad \text{for } (x_1,\dots,x_{k-2}) \in \{0,1\}^{k-2} \setminus \{(0,\dots,0)\}; \\ \varphi(0,1,\dots,1) \cdot f_1(1,\dots,1) = 0; \end{cases} \tag{4.3}$$

where

$$S_\varphi^t(u_1,\dots,u_{k-1}) =$$
$$\sum_{i=0}^{k-3} f_1(t,\dots,t,u_1,\dots,u_{k-i-2}) \left[\varphi(t,t,\dots,t,u_1,\dots,u_{k-i-2}) + u_{k-i-1}\right],$$

for $t \in \{0,1\}$ and $(u_1,\dots,u_{k-1}) \in \{0,1\}^{k-1}$.

4.2. Theorem. [10] *For each $\varphi \in \mathcal{F}^k$ the rows of the coefficient matrix of (4.3) generate the vector space $CIR(\varphi)$.* ■



$$U_{[4]}(\vartheta) = \begin{pmatrix} 0 & 1 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 1 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 1 & 1 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 1 & 1 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix}$$

Figure 4.1. An illustration of Theorem 4.2: the graph Q_ϑ and the matrix $U_{[4]}(\vartheta)$ for $\vartheta(x_1, x_2, x_3, x_4) = x_1$.

The coefficient matrix of (4.3) depends on the values $\varphi(0, 0, \ldots, 0)$, $\varphi(0, 0, \ldots, 1), \ldots, \varphi(0, 1, \ldots, 1)$ of φ. Thereby, Theorem 4.2 establishes the mapping that assigns each of $\varphi \in \mathcal{F}^k$ a circuits matrix of Q_φ. This mapping will be called *the universal circuit matrix of order k* and denoted by $U_{[k]}$. We assume that the i-th column of $U_{[k]}$ corresponds to the edge $(x_2, \ldots, x_k)$ where $x_2 \cdots x_k$ forms the binary representation of i. Because this column depends only on the values of $\varphi(0, x_2, \ldots, x_k)$ it is convenient to replace each $\varphi(0, x_2, \ldots, x_k)$ by the term τ_i and each $1 + \varphi(0, x_2, \ldots, x_k)$ by $\bar{\tau}_i$.

4.3. Example. For $k = 4$ we have

$$U_{[4]} = \begin{pmatrix} 0 & 1 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 1 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 1 & 1 & 1 & 0 \\ \tau_0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ \tau_0 & \tau_1 & 1 & 0 & \bar{\tau}_4 & \bar{\tau}_5 & 1 & 0 \\ \tau_0 & \tau_1 & \tau_2 & 0 & \tau_4 & 0 & 0 & 0 \\ \tau_0 & \bar{\tau}_1 & 0 & \tau_3 & \bar{\tau}_4 & 0 & \tau_6 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & \tau_7 \end{pmatrix},$$

where $\tau_0 = \varphi(0000), \tau_1 = \varphi(0001), \ldots, \tau_7 = \varphi(0111)$ and $\bar{\tau}_i = \tau_i + 1$ for $i \in \{0, 1, \ldots, 7\}$. A value of $U_{[4]}$ is presented in Figure 4.1.

If $\omega \in \mathcal{H}^k$ then $U_{[k]}(\omega)$ is a nonsingular matrix. Thereby, applying to its rows the Gaussian transformations, we can obtain the identity matrix. Let U_ω be the matrix which we obtain as the result the simultaneous transformations on $U_{[k]}(\omega)$ and $U_{[k]}$, when the i-th column of $U_{[k]}$, for $i \in \{0, 1, \ldots, 2^{k-1} - 1\}$, is assumed to be a matrix over $GF(4)$ with the elements $0, 1, \tau_i, \bar{\tau}_i$. The matrix U_ω is said to be *the canonical form of the universal circuits matrix with respect to* ω. One can observe that for each $\omega \in \mathcal{H}^k$ and for each $\varphi \in \mathcal{F}^k$ the rows of $U_\omega(\varphi)$ generate the vector space $CIR\langle\varphi\rangle$. Thereby, the matrix U_ω forms another mapping of $\mathcal{F}^k$ onto family of circuits matrices of the adjacency graphs of the feedback functions.

4.4. Example. For $k = 4$ and ω_1 defined in Figure 3.1 we have

$$U_{[4]}(\omega_1) = \begin{pmatrix} 0 & 1 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 1 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 1 & 1 & 1 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 1 & 1 & 0 & 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 1 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix}$$

and after transformations $U_{[4]}(\omega_1)$ and $U_{[4]}$ we obtain

$$U_{\omega_1} = \begin{pmatrix} \tau_0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & \tau_1 & \tau_2 & 0 & \tau_4 & 0 & 0 & 0 \\ 0 & \bar{\tau}_1 & \bar{\tau}_2 & \bar{\tau}_3 & \tau_4 & \bar{\tau}_5 & \tau_6 & 0 \\ 0 & 0 & \tau_2 & \tau_3 & 0 & 0 & \tau_6 & 0 \\ 0 & \bar{\tau}_1 & \tau_2 & 0 & \bar{\tau}_4 & 0 & 0 & 0 \\ 0 & 0 & \tau_2 & 0 & 0 & \tau_5 & 0 & 0 \\ 0 & 0 & \tau_2 & \tau_3 & 0 & 0 & \tau_6 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & \tau_7 \end{pmatrix}.$$

The matrix U_{ω_1} forms the canonical form of $U_{[4]}$ with respect to ω_1. Note that any of the elements of the main diagonal of U_{ω_1} is neither zero nor one. Moreover, the main diagonal corresponds to truth table of ω_1, that is to the binary vector $(\omega_1(0,0,0,0), \omega_1(0,0,0,1), \ldots, \omega_1(0,1,1,1))$. If we have $\omega_1(0, x_2, x_3, x_4) = 1$ then the corresponding term in the main diagonal has the form τ, otherwise, it is equal to $\bar{\tau}$.

4.5. Proposition. *In each column of U_ω we have:*

(a) *the term that appears in the main diagonal (the main term of the column) is neither zero nor one;*

(b) *each of the other terms of the column is either zero or the complement of the main term.*

Proof. Because $U_\omega(\omega)$ is the identity matrix, each of the elements that appears in the main diagonal is equal to one, thereby the corresponding terms of U_ω are non zero. On the other hand, for each feedback function φ the matrix $U_\omega(\varphi)$ is a circuits matrix of Q_φ. The matrix $U_\omega(\omega)$ is the identity one because each edge of Q_ω forms a loop. If we take $\varphi = \omega_{\|\{e\}}$, for an arbitrary $e \in \{0,1\}^{k-1}$, then we obtain the matrix $U_\omega(\omega_{\|\{e\}})$ that differs with the identity matrix only in the column corresponding to e. Then each row of $U_\omega(\omega_{\|\{e\}})$ differs with the corresponding rows of identity matrix at most in the element that appears in the e-th column. In particular, because e is not a loop in $Q_{\omega_{\|\{e\}}}$ the row of $U_\omega(\omega_{\|\{e\}})$ corresponding to e must be zero. It shows that in each of the columns of U_ω the main term is neither zero nor one, which proves (a). The statement (b) immediately follows from (a) and the assumption that $U_\omega(\omega)$ is the identity matrix. ■

4.6. Theorem. *For each $\omega \in \mathcal{H}^k$ we have $U_\omega(\bar{\omega}) = \mathcal{X}_\omega$.*

Proof. The matrix $U_\omega(\omega)$ is the identity one. This means that in s-th column of U_ω the main term has the form τ_s, if $\omega(s) = 1$, or $\bar{\tau}_s$, if $\omega(s) = 0$. Each of the other terms in this column is either zero or the complement of the main term. Thereby the matrix $U_\omega(\bar{\omega})$ has ones only beyond the main diagonal in each place where the matrix U_ω has nonzero terms. Because of Theorem 3.1, we must prove that the element u_{ij} of $U_\omega(\bar{\omega})$ is equal to 1 if and only if $\omega_{\|\{i,j\}} \in \mathcal{H}^k$. To this purpose, note that the columns of $U_\omega(\omega_{\|\{i,j\}})$ are identical with the corresponding columns of the identity matrix $U_\omega(\omega)$, except the i-th and j-th columns that are identical with the corresponding columns of $U_\omega(\bar{\omega})$. Thereby $U_\omega(\omega_{\|\{i,j\}})$, as a circuits matrix of $\omega_{\|\{i,j\}}$, is nonsingular if and only if $\omega_{\|\{i,j\}} \in \mathcal{H}^k$, that is if and only if $u_{ij} = 1$ and $u_{ji} = 1$, which completes the proof. ■

4.7. Corollary. *Let $\omega \in \mathcal{H}^k$ and let $U_\omega = (u_{ij})$. We have*

$$\omega_{\|\{i,j\}} \in \mathcal{H}^k \quad \textit{if and only if} \quad u_{ij} \in \{\tau_j, \bar{\tau}_j\},$$

for different i and j from $\{0,1,\ldots,2^{k-1}-1\}$. ■

Because of Theorem 4.6 and Proposition 4.5 we can show a simple transformation each of $\mathcal{X}_\omega$ on U_ω. An algorithm can be based on the following observation.

4.8. Corollary. *Let $\omega \in \mathcal{H}^k$ and let (t_{ij}) with $i \in \{0,\dots,2^{k-1}-1\}$ and $j \in \{0,\dots,2^{k-1}-1\}$ be the matrix such that the elements of the j-th column of which are defined as follows: if $\omega(0,x_2,\dots,x_k)=1$, where $x_2\cdots x_k$ is the binary representation of j, then*

$$t_{ij} = \begin{cases} \tau_j, & \textit{if } i = j, \\ \tau_j, & \textit{if } i \neq j \textit{ and } \mathcal{X}_\omega(i,j) = 1, \\ 0, & \textit{if } i \neq j \textit{ and } \mathcal{X}_\omega(i,j) = 0, \end{cases}$$

else

$$t_{ij} = \begin{cases} \bar{\tau}_j, & \textit{if } i = j, \\ \tau_j, & \textit{if } i \neq j \textit{ and } \mathcal{X}_\omega(i,j) = 1, \\ 0, & \textit{if } i \neq j \textit{ and } \mathcal{X}_\omega(i,j) = 0, \end{cases}$$

Then $U_\omega = (t_{ij})$. ■

4.9. Example. We shall illustrate Corollary 4.8 with the construction of U_{ω_6}, where ω_6 has been defined in Figure 3.1, beginning from

$$\mathcal{X}_{\omega_6} = \begin{pmatrix} 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 1 & 1 & 1 & 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix}.$$

Let

$$\begin{aligned}(d_0, d_1, \dots, d_7) &= (\omega_6(0,0,0,0), \omega_6(0,0,0,1), \dots, \omega_6(0,1,1,1)) \\ &= (1,1,1,1,0,0,0,1).\end{aligned}$$

We make the construction in two steps.

- *We replace the elements of the main diagonal of $\mathcal{X}_{\omega_6}$, consisting of zeros, with the elements of the vector $(d_0 + \bar{\tau}_0, d_1 + \bar{\tau}_1, \ldots, d_7 + \bar{\tau}_7)$, respectively.*

Putting $0 + \bar{\tau}_i = \bar{\tau}_i$ and $1 + \bar{\tau}_i = \tau_i$ for $i \in \{0, 1, \ldots, 7\}$ we obtain

$$\begin{pmatrix}
\tau_0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & \tau_1 & 0 & 0 & 1 & 1 & 0 & 0 \\
0 & 0 & \tau_2 & 0 & 0 & 1 & 0 & 0 \\
0 & 0 & 0 & \tau_3 & 0 & 1 & 1 & 0 \\
0 & 1 & 0 & 0 & \bar{\tau}_4 & 1 & 0 & 0 \\
0 & 1 & 1 & 1 & 1 & \bar{\tau}_5 & 1 & 0 \\
0 & 0 & 0 & 1 & 0 & 1 & \bar{\tau}_6 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & \tau_7
\end{pmatrix}.$$

- *In each of the columns we replace each of the ones with the term complementary to the main term of the column.*

Now we obtain the final matrix

$$U_{\omega_6} = \begin{pmatrix}
\tau_0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & \tau_1 & 0 & 0 & \tau_4 & \tau_5 & 0 & 0 \\
0 & 0 & \tau_2 & 0 & 0 & \tau_5 & 0 & 0 \\
0 & 0 & 0 & \tau_3 & 0 & \tau_5 & \tau_6 & 0 \\
0 & \bar{\tau}_1 & 0 & 0 & \bar{\tau}_4 & \tau_5 & 0 & 0 \\
0 & \bar{\tau}_1 & \bar{\tau}_2 & \bar{\tau}_3 & \tau_4 & \bar{\tau}_5 & \tau_6 & 0 \\
0 & 0 & 0 & \bar{\tau}_3 & 0 & \tau_5 & \bar{\tau}_6 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & \tau_7
\end{pmatrix}.$$

This matrix can be easily transformed on U_ω for each of $\omega \in \mathcal{H}^4$.

The mapping $U_{|k|}$ has been directly defined by (4.3) which does not bring to light too much informations about the circuits of the adjacency graphs of feedback functions. Theorem 4.6 establishes a basic connection between the universal circuits matrix and the family of the crossing relations of the Hamiltonian functions. This discloses a kind of an information bounded up with a canonical form of $U_{|k|}$, which is discussed in the next two sections.

5. The matrix U_ω and the problem $\varphi \overset{*}{\rightarrow} \omega$

For a Hamiltonian function ω and a feedback function φ such that $\varphi \overset{*}{\rightarrow} \omega$, if $Q_\varphi[D]$ forms the spanning tree of Q_φ such that $\omega = \varphi_{\|D}$ then we will write $\varphi \overset{D}{\rightarrow} \omega$.

5.1. Theorem. *Let $\omega \in \mathcal{H}^k$. If $\varphi \overset{D}{\rightarrow} \omega$ then the nonzero rows of $U_\omega(\varphi)$ represent the fundamental circuits of Q_φ with respect to $Q_\varphi[D]$ or loops.*

Proof. Because of Theorem 4.2 the nonzero rows of $U_\omega(\varphi)$ represents circuits of Q_φ and we must only prove that they form the set of fundamental circuits with respect to $Q_\omega[D]$. To this purpose note that the matrix $U_\omega(\varphi)$ differs with the identity matrix $U_\omega(\omega)$ only on the columns corresponding to the branches of $Q_\omega[D]$. Thereby, in each of the nonzero rows of Q_φ the nonzero elements are in the columns corresponding to the branches of $Q_\omega[D]$ or in the main diagonal. Let R_e be the row of $U_\omega(\varphi)$ corresponding to an edge e of Q_φ.

If $e \in D$ then the common element of R_e and the main diagonal is equal to zero, because in $U_\omega(\omega)$ it is equal to one. Thereby, each of the other elements of R_e is equal to zero, otherwise R_e represents the circuit of Q_φ composed of branches of a spanning tree, which is impossible.

If $e \notin D$ then the common element of R_e and the main diagonal is equal to one and represents a chord of $Q_\varphi[D]$ while the other nonzero elements represent branches of $Q_\varphi[D]$. In this case R_e represents a fundamental circuit of Q_φ, or a loop, if e is the unique edge in this circuit. ■

5.2. Corollary. *Let ω be a Hamiltonian function. For each feedback function φ the relation $\varphi \overset{D}{\rightarrow} \omega$ holds if and only if the rows of $U_\omega(\varphi)$ corresponding to the elements of D are zero vectors.* ■

5.3. Theorem. *If $\varphi \overset{D}{\rightarrow} \omega$ then the matrix which consists of the rows of $U_\omega(\bar{\varphi})$ that correspond to the elements of the set D is the fundamental cut-set matrix of Q_φ with respect to $Q_\varphi[D]$.*

Proof. Let us set $U_\omega = (u_{ij}^{\tau})$, $U_\omega(\varphi) = (u_{ij}^{\varphi})$ and $U_\omega(\bar{\varphi}) = (u_{ij}^{\bar{\varphi}})$. For each branch d of $Q_\varphi[D]$ let $\{d, c_1, \ldots, c_m\}$ be the cut-set of Q_φ that contains d. Then $c_1, \ldots, c_m$ are the chords Q_φ each of which establishes one of the fundamental circuits containing d. It follows from Theorem 5.1 that

$$u_{id}^{\varphi} = \begin{cases} 1, & \text{for } i \in \{c_1, \ldots, c_m\}, \\ 0, & \text{otherwise}, \end{cases}$$

and $u^{\varphi}_{dj} = 0$ for all j. On the other hand, we have

$$u^{\tau}_{id} = \begin{cases} t, & \text{for } i \in \{c_1, \dots, c_m\}, \\ \bar{t}, & \text{for } i = d, \\ 0, & \text{otherwise,} \end{cases}$$

where $t \in \{\tau_d, \bar{\tau}_d\}$ is a nonzero term, and Theorem 4.6 implies that $u^{\tau}_{id} \neq 0$ if and only if $u^{\tau}_{di} \neq 0$. Thereby we have

$$u^{\bar{\varphi}}_{dj} = \begin{cases} 1, & \text{for } j \in \{d, c_1, \dots, c_m\}, \\ 0, & \text{otherwise.} \end{cases}$$

This means that $(u^{\bar{\varphi}}_{d1}, \dots, u^{\bar{\varphi}}_{d2^{k-1}})$ is a cut-set vector of Q_{φ}. ■

5.4. Corollary. *For each $\varphi \in \mathcal{F}^k$ we have $CUT(\varphi) \subseteq CIR(\bar{\varphi})$.* ■

Let us set $\mathcal{X}^*_{\omega} = I + \mathcal{X}_{\omega}$. The matrix $\mathcal{X}^*_{\omega}$ contains full information about all feedback functions φ such that $\varphi \xrightarrow{*} \omega$.

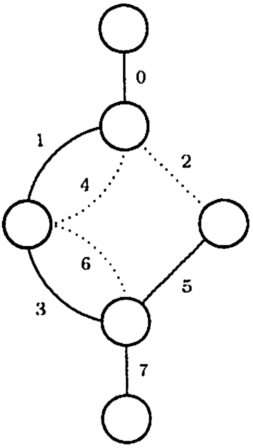
5.5. Corollary. *Let $\omega \in \mathcal{H}^k$. Each row of $\mathcal{X}^*_{\omega}$ is the cut-set vector of the adjacency graph each of the feedback functions φ such that $\varphi \xrightarrow{*} \omega$. In particular, the row corresponding to d is the fundamental cut-set vector of the adjacency graph each of the feedback functions φ such that $\varphi \xrightarrow{D} \omega$, where $d \in D$. Then the matrix that consists the rows of $\mathcal{X}^*_{\omega}$ corresponding to the elements of D is the fundamental cut-set matrix of Q_{φ} with respect to $Q_{\varphi}[D]$.* ■

5.6. Corollary. *Let $\omega \in \mathcal{H}^k$. For each $D \subseteq \{0,1\}^{k-1}$ we have $\omega_{\|D} \xrightarrow{*} \omega$ if and only if $\mathcal{X}^*_{\omega}[D]$ is the identity matrix of rank $|D|$.* ■

5.7. Corollary. *Let $\omega \in \mathcal{H}^k$. If $\varphi \xrightarrow{D} \omega$ and $\mathcal{X}^D_{\omega} = (x^D_{ij})$ is the matrix defined as follows*

$$x^D_{ij} = \begin{cases} 0, & \text{if } i \neq j,\ i \in \{0,1\}^{k-1} \setminus D,\ j \in \{0,1\}^{k-1} \setminus D, \\ x^*_{ij}, & \text{otherwise,} \end{cases}$$

then the rows of $\mathcal{X}^D_{\omega}$ that correspond to D are the fundamental cut-set vectors and the others – the fundamental circuit vectors of Q_{φ} with respect to $Q_{\varphi}[D]$. ■



$$\mathcal{X}^*_{\omega_1} = \begin{array}{c|cccccccc} & 0 & 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ \hline 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 1 & 1 & 0 & 1 & 0 & 0 & 0 \\ 2 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 0 \\ 3 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 0 \\ 4 & 0 & 1 & 1 & 0 & 1 & 0 & 0 & 0 \\ 5 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 \\ 6 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 0 \\ 7 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{array}$$

$$\tilde{\mathcal{X}}^*_{\omega_1} = \begin{array}{c|cccccccc} & 0 & 1 & 3 & 5 & 7 & 2 & 4 & 6 \\ \hline 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 1 & 0 & 0 & 0 & 1 & 1 & 0 \\ 3 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 1 \\ 5 & 0 & 0 & 0 & 1 & 0 & 1 & 0 & 0 \\ 7 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 2 & 0 & 1 & 1 & 1 & 0 & 1 & 1 & 1 \\ 4 & 0 & 1 & 0 & 0 & 0 & 1 & 1 & 0 \\ 6 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 1 \end{array}$$

$$\tilde{\mathcal{X}}^D_{\omega_1} = \begin{array}{c|cccccccc} & 0 & 1 & 3 & 5 & 7 & 2 & 4 & 6 \\ \hline 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 1 & 0 & 0 & 0 & 1 & 1 & 0 \\ 3 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 1 \\ 5 & 0 & 0 & 0 & 1 & 0 & 1 & 0 & 0 \\ 7 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 2 & 0 & 1 & 1 & 1 & 0 & 1 & 0 & 0 \\ 4 & 0 & 1 & 0 & 0 & 0 & 0 & 1 & 0 \\ 6 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 1 \end{array}$$

Figure 5.1. An illustration of Corollary 5.7 with $\omega_1 = \vartheta_{||D}$ where $\vartheta(x_1, x_2, x_3, x_4) = x_1$ and $D = \{000, 001, 011, 101, 111\}$. The matrices $\tilde{\mathcal{X}}^*_{\omega_1}$ and $\tilde{\mathcal{X}}^D_{\omega_1}$ differs with $\mathcal{X}^*_{\omega_1}$ and $\mathcal{X}^D_{\omega_1}$ in the order of the rows and columns.

Let $\mathcal{H}^k\langle\varphi\rangle = \{\omega \in \mathcal{H}^k : \varphi \xrightarrow{*} \omega\}$. According to Theorem 2.2 the family $\mathcal{H}^k\langle\varphi\rangle$ may be identified with the family of the spanning trees of Q_φ. On the other hand, Theorem 3.1 allows us to describe the family $\mathcal{H}^k\langle\varphi\rangle$ based on an arbitrary feedback function from $\mathcal{H}^k\langle\varphi\rangle$. We shall show how the results of this section simplify this description. To this purpose, let us assume that if X and Y are nonempty subsets of $\{0,1\}^{k-1}$ then $\mathcal{X}_\omega[X,Y]$ denotes the submatrix of $\mathcal{X}_\omega$ arising by deleting the rows corresponding to the edges from $\{0,1\}^{k-1} \setminus X$ and the columns corresponding to the edges from $\{0,1\}^{k-1} \setminus Y$. In the case $X = Y$ we have $\mathcal{X}_\omega[X,Y] = \mathcal{X}_\omega[X]$.

5.8. Theorem. *Let $\varphi \in \mathcal{F}^k$ and $\varphi \xrightarrow{D} \omega$. For each nonempty set $X \subseteq \{0,1\}^{k-1}$ we have $\omega_{\|X} \in \mathcal{H}^k\langle\varphi\rangle$ if and only if $|X \cap D| = |X \setminus D|$ and the matrix $\mathcal{X}_\omega[X \cap D, X \setminus D]$ is nonsingular.*

Proof. Note that $\omega \in \mathcal{H}^k\langle\varphi\rangle$. According to Theorem 2.2 we have $\omega_{\|X} \in \mathcal{H}^k\langle\varphi\rangle$ if and only if there exists $D_X \subseteq \{0,1\}^{k-1}$ such that $Q_\varphi[D_X]$ forms a spanning tree of Q_φ. It is known that for the spanning trees $Q_\varphi[D]$ and $Q_\varphi[D_X]$ of Q_φ there exists the one-to-one transformation from D on D_X such that $f(d) = d$ for $d \in D \cap D_X$ and $f(d)$ is one of the chords from the fundamental cut-set of Q_φ with respect to $Q_\varphi[D]$ which contains d for $d \in D \setminus D_X$. Thereby, the equality $|X \cap D| = |X \setminus D|$ is necessary for the relation $\omega_{\|X} \in \mathcal{H}^k\langle\varphi\rangle$. Let us consider the matrix $\mathcal{X}_\omega[X]$ and assume that its rows and columns are ordered as follows: the first are rows (and columns) that correspond to the elements of $X \cap D$ and next to the elements of $X \setminus D$. Then it has the form

$$\begin{array}{cc} & \begin{array}{cc} X\cap D & X\setminus D \end{array} \\ \begin{array}{c} X\cap D \\ X\setminus D \end{array} & \left(\begin{array}{cc} 0 & A \\ A^T & B \end{array}\right), \end{array}$$

where $A = \mathcal{X}_\omega[X \cap D, X \setminus D]$. According to Theorem 3.1 we have $\omega_{\|X} \in \mathcal{H}^k\langle\varphi\rangle$ if and only if the matrix $\mathcal{X}_\omega[X]$ is nonsingular. Since $\mathcal{X}_\omega[X \cap D]$ is zero matrix we see that $\mathcal{X}_\omega[X]$ is nonsingular if and only if $\mathcal{X}_\omega[X \cap D, X \setminus D]$ is nonsingular. This completes the proof. ∎

5.9. Example. Let $k = 4$. For $\omega = \omega_1$ and $\varphi = \vartheta$ (Figure 5.1) we have $D = \{000, 001, 011, 101, 111\}$. Then $X = \{001, 011, 101\} \cup \{010, 100, 110\}$ is the greatest subset of $\{0,1\}^3$ established by Theorem 5.8, that is the matrix $\mathcal{X}_{\omega_1}[\{001, 011, 101\}, \{010, 100, 110\}]$ is nonsingular. One can check that $Q_\vartheta[\{000, 010, 100, 110, 111\}]$ forms a spanning tree of Q_ϑ, thereby $\omega_{1\|X} \in \mathcal{H}^4\langle\vartheta\rangle$.

6. Connections to the Hauge-Mykkeltveit classification

In [4] the classification of the de Bruijn sequences based on groups of permutations of the set $\{0,1\}^{k-1}$ has been considered. Each permutation $\wp\colon \{0,1\}^{k-1} \to \{0,1\}^{k-1}$ establishes the mapping from $\mathcal{F}^k$ into $\mathcal{F}^k$ defined as follows. For $\varphi \in \mathcal{F}^k$ we set

$$\varphi_\wp(x_1, x_2, \ldots, x_k) = \varphi(x_1, y_2, \ldots, y_k),$$

where $(y_2, \ldots, y_k) = \wp^{-1}(x_2, \ldots, x_k)$ for $(x_1, x_2, \ldots, x_k) \in \{0,1\}^k$. Some of these transformations lead from Hamiltonian functions to Hamiltonian ones. For example, each of the well known permutations of $\{0,1\}^{k-1}$: $\wp_c(u_1, \ldots, u_{k-1}) = (\bar{u}_1, \ldots, \bar{u}_{k-1})$ and $\wp_r(u_1, \ldots, u_{k-1}) = (u_{k-1}, \ldots, u_1)$ transforms the family $\mathcal{H}^k$ onto itself. In this section we study the idea of Hauge and Mykkeltveit with respect of the relation $\times_\omega$, represented by $\mathcal{X}^*_\omega$.

Let $\Pi_k\langle\varphi\rangle$ be the family of the permutations $\wp\colon \{0,1\}^{k-1} \to \{0,1\}^{k-1}$ that transforms each spanning tree of Q_φ onto a spanning tree of $Q_{\varphi_\wp}$. For each $\omega \in \mathcal{H}^k$ we have

$$\Pi_k\langle\omega\rangle = \{\wp\colon \omega_\wp \in \mathcal{H}^k\},$$

because, if $\wp \in \Pi_k\langle\varphi\rangle$ then $|\{0,1\}^k/\varphi| = |\{0,1\}^k/\varphi_\wp|$ and Q_ω does not contain any nonempty spanning tree. The families $\Pi_k\langle\omega\rangle$ establish a partition of $\mathcal{H}^k$. This is stated with the following observation. For each $\wp \in \Pi_k\langle\varphi\rangle$ we have

$$\mathcal{H}^k\langle\varphi_\wp\rangle = \{\omega_\wp\colon \omega \in \mathcal{H}^k\langle\varphi\rangle\}. \tag{6.1}$$

We shall characterize the families $\mathcal{H}^k\langle\varphi_\wp\rangle$ by a connection among the matrix $\mathcal{X}^*_\omega$ and the matrices $\mathcal{X}^*_{\omega_\wp}$. To this purpose for each permutation $\wp$ of $\{0,1\}^{k-1}$ and for arbitrary $2^{k-1} \times 2^{k-1}$ binary matrices M_1 and M_2 we set $M_1 \overset{\wp}{=} M_2$ if and only if M_1 and M_2 differ only with the permutations of rows and columns according to $\wp$. Moreover, for each $X \subseteq \{0,1\}^{k-1}$ we set $X_\wp = \{\wp(x) : x \in X\}$.

6.1. Theorem. *Let $\varphi \in \mathcal{F}^k$. For each $\omega \in \mathcal{H}^k\langle\varphi\rangle$ and $\wp \in \Pi_k\langle\varphi\rangle$ we have*

$$\text{if } \varphi \xrightarrow{D} \omega \text{ then } \varphi_\wp \xrightarrow{D_\wp} \omega_\wp \text{ and } \mathcal{X}^D_\omega \overset{\wp}{=} \mathcal{X}^{D_\wp}_{\omega_\wp}.$$

Proof. If $\wp \in \Pi_k\langle\varphi\rangle$ then the spanning tree $Q_\varphi[D]$ is transformed onto the spanning tree $Q_{\varphi_\wp}[D_\wp]$. We shall show that $\wp$ maps the set of fundamental circuits of Q_φ with respect to $Q_\varphi[D]$ onto the set of fundamental circuits of $Q_{\varphi_\wp}$ with respect to $Q_{\varphi_\wp}[D_\wp]$ (compare with [4, Lemma 4]) as well as the set of the fundamental cut-sets of Q_φ with respect to $Q_{\varphi_\wp}[D_\wp]$ onto the fundamental cut-sets of Q_φ with respect to $Q_{\varphi_\wp}[D_\wp]$.

For each fundamental circuit $C = \{b_1, \ldots, b_m, c\}$ of Q_φ that consists of the branches $b_1, \ldots, b_m$ and the chord c there exist the spanning trees $T_1, \ldots, T_m$ of Q_φ each of which differs with $Q_\varphi[D]$ only on the edges b_i and c for $i \in \{1, \ldots, m\}$. Because the images $T_1^\wp, \ldots, T_m^\wp$ of $T_1, \ldots, T_m$ form spanning trees of $Q_{\varphi_\wp}$ each of which differs with $Q_{\varphi_\wp}[D_\wp]$ only on the edges $\wp(b_i)$ and $\wp(c)$ for $i \in \{1, \ldots, m\}$ the image $C_\wp$ of C forms the fundamental circuit of $Q_{\varphi_\wp}$ with respect to $Q_{\varphi_\wp}[D_\wp]$ as well as each of the spanning trees $T_1^\wp, \ldots, T_m^\wp$.

Note now that the construction each of the spanning trees $T_1, \ldots, T_m$ does not change the fundamental circuit that contains the edges b_i and c. This proves that $\wp$ maps the the set of the fundamental cut-sets of Q_φ with respect to Q_φ onto the set of the fundamental cut-sets of $Q_{\varphi_\wp}$ with respect to $Q_{\varphi_\wp}[D_\wp]$.

Because of the partition of $\mathcal{X}_\omega^D$ stated by Corollary 5.7 the proof is completed. ■

6.2. Theorem. *Let $\omega \in \mathcal{H}^k$. For each $\wp \in \Pi_k\langle\omega\rangle$, if $\mathcal{X}_\omega^* \overset{\wp}{=} \mathcal{X}_{\omega_\wp}^*$ then $\wp \in \bigcap_{\omega \in \mathcal{H}^k} \Pi_k\langle\omega\rangle$.*

Proof. Let us consider an arbitrary $\tilde{\omega} \in \mathcal{H}^k$ and let $\tilde{\omega} = \omega_{\|X}$. The assumption $\mathcal{X}_\omega^* \overset{\wp}{=} \mathcal{X}_{\omega_\wp}^*$ implies that the matrix $\mathcal{X}_\omega[X]$ is nonsingular if and only if $\mathcal{X}_{\omega_\wp}[X_\wp]$ is nonsingular. Because $\tilde{\omega}_\wp = \omega_{\wp\|X_\wp}$ we have $\tilde{\omega}_\wp \in \mathcal{H}^k$ which implies that $\wp \in \Pi_k\langle\tilde{\omega}\rangle$ for an arbitrary $\tilde{\omega} \in \mathcal{H}^k$. Thereby, $\wp \in \bigcap_{\omega \in \mathcal{H}^k} \Pi_k\langle\omega\rangle$. ■

6.3. Theorem. *For each positive k we have*

$$\bigcap_{\omega \in \mathcal{H}^k} \Pi_k\langle\omega\rangle = \{\wp : \mathcal{X}_\omega^* \overset{\wp}{=} \mathcal{X}_{\omega_\wp}^* \quad \text{for each } \omega \in \mathcal{H}^k\}.$$

Proof. If $\wp \in \bigcap_{\omega \in \mathcal{H}^k} \Pi_k\langle\omega\rangle$ then for each $\omega \in \mathcal{H}^k$ we have $\omega_\wp \in \mathcal{H}^k$. Let $\mathcal{X}_\omega^*(u, v) = 1$. Then $\omega_{\|\{u,v\}} \in \mathcal{H}^k$ and $(\omega_{\|\{u,v\}})_\wp \in \mathcal{H}^k$. Thereby

$$\omega_{\wp\|\{\wp(u),\wp(v)\}} = (\omega_{\|\{u,v\}})_\wp \in \mathcal{H}^k.$$

This implies that $\mathcal{X}_{\omega_\wp}^*(\wp(u), \wp(v)) = 1$ which leads to the conclusion that $\mathcal{X}_\omega^* \overset{\wp}{=} \mathcal{X}_{\omega_\wp}^*$. Then we have

$$\bigcap_{\omega \in \mathcal{H}^k} \Pi_k\langle\omega\rangle \subseteq \{\wp : \mathcal{X}_\omega^* \overset{\wp}{=} \mathcal{X}_{\omega_\wp}^* \quad \text{for each } \omega \in \mathcal{H}^k\}.$$

The inverse inclusion immediately follows from Theorem 6.2. ■

6.4. Example. We shall show that

$$\bigcap_{\omega \in \mathcal{H}^4} \Pi_4\langle\omega\rangle = \Pi_4\langle\vartheta\rangle,$$

where $\vartheta(x_1, x_2, x_3, x_4) = x_1$. To this purpose note that for each $\omega \in \mathcal{H}^4$ either $\vartheta \xrightarrow{*} \omega$ or $\bar{\vartheta} \xrightarrow{*} \omega$. Thereby, because of Corollary 5.5 and Theorem 6.3, if $\wp \in \bigcap_{\omega \in \mathcal{H}^4} \Pi_4\langle\omega\rangle$ then $\wp \in \Pi_4\langle\vartheta\rangle \cap \Pi_4\langle\bar{\vartheta}\rangle$. On the other hand, if $\varphi \xrightarrow{*} \omega$ then $\Pi_4\langle\varphi\rangle \subseteq \Pi_4\langle\omega\rangle$. This implies that

$$\Pi_4\langle\vartheta\rangle \cap \Pi_4\langle\bar{\vartheta}\rangle = \bigcap_{\omega \in \mathcal{H}^4} \Pi_4\langle\omega\rangle.$$

It has been proved in [4] that $\Pi_4\langle\vartheta\rangle \subseteq \Pi_4\langle\bar{\vartheta}\rangle$. This implies the equality $\bigcap_{\omega \in \mathcal{H}^4} \Pi_4\langle\omega\rangle = \Pi_4\langle\vartheta\rangle$. The family $\Pi_4\langle\vartheta\rangle$ has been established in [4].

Acknowledgement. The author is greatly indebted to the referee for pointing out mistakes in the paper.

7. References

[1] M. Cohn, A. Lempel, *Cycle decomposition by disjoint transpositions,* J. of Combinatorial Theory(A) 13(1972), 83-89.

[2] N. Deo, *Graph theory with applications to engineering and computer science,* Prentice-Hall, Inc., Englewood Cliffs. 1974

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

[4] E. R. Hauge, J. Mykkeltveit, *On the classification of de Bruijn sequences,* Discrete Math. 148(1996), 65-83.

[5] M. Latko, *The similitude of shift registers,* Demonstratio Math., Vol. 19, 2(1986), 469- 485.

[6] E. Lazuka, J. Żurawiecki, *The lower bounds of a feedback function,* Demonstratio Math. Vol. 29, 1(1996), 191-203.

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

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

[9] J. Żurawiecki, *Locally reducible iterative systems,* Demonstratio Math., Vol. 23, 4(1990), 961-983.

[10] J. Żurawiecki, *Universal circuits matrix for adjacency graphs of feedback functions,* Discrete Math., 126(1994), 441-445.

[11] J. Żurawiecki, *The upper bounds of a feedback function,* Demonstratio Math. Vol. 32, 3(1999), 457-468.