Acta Mathematica Academiae Paedagogicae Nyíregyháziensis
26 (2010), 1–15
www.emis.de/journals
ISSN 1786-0091

A BASIS OF THE CONJUNCTIVELY POLYNOMIAL-LIKE BOOLEAN FUNCTIONS

J. GONDA

Abstract. The spectra of the conjunctively polynomial-like Boolean functions belonging to their modified canonical normal forms induce a linear space over the field of two elements. A basis of this space was given in [7]. In this article we give another way to generate a matrix of the basis of the space.

In this article disjunction and logical sum, conjunction and logical product, exclusive or and modulo two sum, as well as complementation and negation are used in the same sense and they are denoted respectively by $+$, $\cdot$ (or simply without any operation sign), $\oplus$ and $\bar{\ }$. The elements of the field with two elements and the elements of the Boolean algebra with two elements are denoted by the same signs, namely by 0 and 1; $\mathbf{N}$ denotes the non-negative integers, and $\mathbf{N}^+$ the positive ones.

1. Introduction

Logical functions and especially the two-valued ones have important role in our everyday life, so it is easy to understand why they are widely investigated. A scope of the investigations is the representations of these functions and the transforms from one representation to another ([3, 4, 5, 8]). Another area of the examinations is the search of special classes of the set of the functions. Post determined the closed classes of the switching functions [10], but there are a lot of another classes of the Boolean functions invariant with respect to some property. Such properties can be for example linear transforms. In [6] and [7] it were introduced two classes of the Boolean functions invariant to some linear transforms. These functions are called polynomial-like and conjunctively polynomial-like.

2000 *Mathematics Subject Classification.* 06E30, 94C10, 15A18.

Key words and phrases. Boolean function, conjunctive normal form, Zhegalkin polynomial, conjunctively polynomial-like Boolean function.

This research was supported by the grant TÁMOP-4.2.1/B-09/1/KMR-2010-003.

1.1. **Representations of a Boolean function.** It is well-known that an arbitrary two-valued logical function of n variables can be written in the uniquely determined canonical disjunctive normal form, i.e. as a logical sum whose members are pairwise distinct logical products of n factors, where all of such logical products contain every logical variable exactly once, either negated or not negated exclusively. Clearly, there exist exactly 2^n such products. Supposing that the variables are indexed by the integers $0 \le j < n$ and the variable indexed by j is denoted by x_j, these products can be numbered by the numbers $0 \le i < 2^n$ in such a way that we consider the non-negative integer containing 0 in the j-th position of its binary expansion if the j-th variable of the given product is negated, and 1 in the other case. Of course, this is a one to one correspondence between the 2^n distinct products and the integers of the interval $[0..2^n-1]$, and if $i = \sum_{j=0}^{n-1} a_j^{(i)} 2^j$, where $a_j^{(i)}$ is either 0 or 1, then the product belonging to it is

$$m_i^{(n)} = \prod_{j=0}^{n-1} \left(\overline{a_j^{(i)}} \oplus x_j \right). \tag{1}$$

Such a product is called *minterm* (of n variables).

With the numbering given above we numbered the Boolean functions of n variables, too. A Boolean function is uniquely determined by the minterms contained in its canonical disjunctive normal form, so a Boolean function is uniquely determined by a 2^n long sequence of 0-s and 1-s, where a 0 in the j-th position (now $0 \le j < 2^n$) means that $m_j^{(n)}$ doesn't occur in that function, and 1 means that the canonical disjunctive normal form of the function contains the minterm of the index j (this sequence is the spectrum of the canonical disjunctive normal form of the function, and similarly will be defined the spectra with respect to other representations of the function), i.e. for $l = \sum_{i=0}^{2^n-1} \alpha_i^{(l)} 2^i$ with $\alpha_i^{(l)} \in \{0,1\}$

$$f_l^{(n)} = \sum_{i=0}^{2^n-1} \alpha_i^{(l)} m_i^{(n)}. \tag{2}$$

Now $f_l^{(n)}$ denotes the l-th Boolean function of n variables.

Instead of the 2^n-long sequence of 0-s and 1-s it is enough to give the indices of the 1-s:

$$f_l^{(n)} = \sum \left\{ i \in \mathbf{N} \,\middle|\, i < 2^n \wedge \alpha_i^{(l)} = 1 \right\} \tag{3}$$

or simply

$$f^{(n)} = \sum \left\{ i \in \mathbf{N} \,|\, i < 2^n \wedge \alpha_i = 1 \right\}. \tag{4}$$

If this notation is applied then it is easy to give a Boolean function not completely defined, that is, a Boolean function having so called don't care terms, briefly don't cares. In this case we give separately the indices of the minterms occuring in the function and the indices of the don't cares:

$$\begin{aligned} f^{(n)} &= \sum \{ i \in \mathbf{N} \,|\, i < 2^n \wedge \alpha_i = 1 \} \\ d^{(n)} &= \sum \{ i \in \mathbf{N} \,|\, i < 2^n \wedge m_i \text{ is a don't care term} \} . \end{aligned} \tag{5}$$

Another possibility for giving a Boolean function is the so-called Zhegalkin-polynomial. Let $S_i^{(n)} = \prod_{j=0}^{n-1} \left(\overline{a_j^{(i)}} + x_j \right)$, where $i = \sum_{j=0}^{n-1} a_j^{(i)} 2^j$ again. This product contains only non-negated variables, and the j-th variable is contained in it if and only if the j-th digit is 1 in the binary expansion of i. There exist exactly 2^n such products which are pairwise distinct. Now any Boolean function of n variables can be written as a modulo two sum of such terms, and the members occurring in the sum are uniquely determined by the function. That means that we can give the function by a 2^n-long 0 - 1 sequence, and if the i-th member of such a sequence is k_i then

$$f^{(n)} = \bigoplus_{i=0}^{2^n-1} k_i S_i^{(n)} . \tag{6}$$

Between the first and the second representation of the same Boolean function there is a very simple linear algebraic transform. Considering the coefficients of the canonical disjunctive normal form of a Boolean function of n variables and the coefficients of the Zhegalkin polynomial of a function of n variables, respectively, as the components of an element of a 2^n-dimensional linear space over the field of two elements, denoted by $\mathbf{F}_2$, the relation between the vectors belonging to the two representations of the same Boolean function of n variables can be given by $\underline{k} = \mathbf{A}^{(n)} \underline{\alpha}$. Here $\underline{k}$ is the vector containing the components of the Zhegalkin polynomial, $\underline{\alpha}$ is the vector, composed of the coefficients of the disjunctive representation of the given function, and $\mathbf{A}^{(n)}$ is the matrix of the transform in the natural basis.

For the matrix of the transform it is true that

$$\mathbf{A}^{(n+1)} = \begin{cases} (1) & \text{if } n = 0 \\ \begin{pmatrix} \mathbf{A}^{(n)} & \mathbf{0}^{(n)} \\ \mathbf{A}^{(n)} & \mathbf{A}^{(n)} \end{pmatrix} & \text{if } n \in \mathbf{N}^+ \end{cases} \tag{7}$$

(this form of the matrix shows that for every $n \in \mathbf{N}$, $\mathbf{A}^{(n)}$ is the n-th Kronecker-product power of the two-order $\begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}$ regular quadratic matrix). Really, let $\underline{u}$ be a 2^{n+1}-component vector, where n is a nonnegative integer, and let $\underline{u}^{(0)}$ and $\underline{u}^{(1)}$ denote the vectors containing the first and the last 2^n components of $\underline{u}$. In general, let $\left(\underline{x}, \underline{y}\right)$ denote the scalar product of $\underline{x}$ and $\underline{y}$. Then it is easy to see that

$$\left(\underline{u}, \underline{v}\right) = \left(\underline{u}^{(0)}, \underline{v}^{(0)}\right) \oplus \left(\underline{u}^{(1)}, \underline{v}^{(1)}\right) .$$

It is obvious that if $n = 0$ then $\underline{k} = \underline{\alpha}$, so if $\mathbf{A}^{(0)} = (1)$ then

$$\underline{k} = \mathbf{A}^{(0)} \underline{\alpha}.$$

Now let's suppose that for the n-variable Boolean functions $\underline{k} = \mathbf{A}^{(n)}\underline{\alpha}$ and $\underline{m}^{(n)}$ denotes the vector composed of the n-variable minterms and $\underline{S}^{(n)}$ denotes the vector composed of the n-variable Zhegalkin-monomials. Then

$$\begin{aligned}
\left(\underline{k}^{(0)}, \underline{S}^{(n+1)^{(0)}}\right) \oplus \left(\underline{k}^{(1)}, \underline{S}^{(n+1)^{(1)}}\right) &= \left(\underline{k}, \underline{S}^{(n+1)}\right) = \left(\mathbf{A}^{(n+1)}\underline{\alpha}, \underline{S}^{(n+1)}\right) \\
&= \left(\underline{\alpha}, \underline{m}^{(n+1)}\right) = \left(\underline{\alpha}^{(0)}, \underline{m}^{(n)}\overline{x}_n\right) \oplus \left(\underline{\alpha}^{(1)}, \underline{m}^{(n)}x_n\right) \\
&= \left(\underline{\alpha}^{(0)}, \underline{m}^{(n)}\left(1 \oplus x_n\right)\right) \oplus \left(\underline{\alpha}^{(1)}, \underline{m}^{(n)}x_n\right) \\
&= \left(\underline{\alpha}^{(0)}, \underline{m}^{(n)}\right) \oplus \left(\underline{\alpha}^{(0)} \oplus \underline{\alpha}^{(1)}, \underline{m}^{(n)}x_n\right) \\
&= \left(\underline{\alpha}^{(0)}, \underline{m}^{(n)}\right) \oplus x_n\left(\underline{\alpha}^{(0)} \oplus \underline{\alpha}^{(1)}, \underline{m}^{(n)}\right) \qquad (8) \\
&= \left(\mathbf{A}^{(n)}\underline{\alpha}^{(0)}, \underline{S}^{(n)}\right) \oplus x_n\left(\mathbf{A}^{(n)}\underline{\alpha}^{(0)} \oplus \mathbf{A}^{(n)}\underline{\alpha}^{(1)}, \underline{S}^{(n)}\right) \\
&= \left(\mathbf{A}^{(n)}\underline{\alpha}^{(0)}, \underline{S}^{(n)}\right) \oplus \left(\mathbf{A}^{(n)}\underline{\alpha}^{(0)} \oplus \mathbf{A}^{(n)}\underline{\alpha}^{(1)}, \underline{S}^{(n)}x_n\right) \\
&= \left(\mathbf{A}^{(n)}\underline{\alpha}^{(0)} \oplus \mathbf{0}^{(n)}\underline{\alpha}^{(1)}, \underline{S}^{(n+1)^{(0)}}\right) \\
&\oplus \left(\mathbf{A}^{(n)}\underline{\alpha}^{(0)} \oplus \mathbf{A}^{(n)}\underline{\alpha}^{(1)}, \underline{S}^{(n+1)^{(1)}}\right),
\end{aligned}$$

that is,

$$\mathbf{A}^{(n+1)} = \begin{pmatrix} \mathbf{A}^{(n)} & \mathbf{0}^{(n)} \\ \mathbf{A}^{(n)} & \mathbf{A}^{(n)} \end{pmatrix}. \qquad (9)$$

$\mathbf{0}^{(n)}$ stands for the n-order zero matrix. From the previous results immediately follows that

$$\begin{aligned}
\left(\mathbf{A}^{(n+1)}\right)^2 &= \begin{pmatrix} \mathbf{A}^{(n)} & \mathbf{0}^{(n)} \\ \mathbf{A}^{(n)} & \mathbf{A}^{(n)} \end{pmatrix}\begin{pmatrix} \mathbf{A}^{(n)} & \mathbf{0}^{(n)} \\ \mathbf{A}^{(n)} & \mathbf{A}^{(n)} \end{pmatrix} \\
&= \begin{pmatrix} \left(\mathbf{A}^{(n)}\right)^2 & \mathbf{0}^{(n)} \\ \mathbf{0}^{(n)} & \left(\mathbf{A}^{(n)}\right)^2 \end{pmatrix} \qquad (10)
\end{aligned}$$

and as $\left(\mathbf{A}^{(0)}\right)^2 = (1)$, so we get by induction that

$$\left(\mathbf{A}^{(n+1)}\right)^2 = \mathbf{I}^{(n+1)} \qquad (11)$$

where $\mathbf{I}^{(n)}$ denotes the n-order identity matrix.

A similar representation of a Boolean function is the canonical conjunctive normal form of the function. Let's consider

$$M_i^{(n)} = \sum_{j=0}^{n-1}\left(a_j^{(i)} \oplus x_j\right) \qquad (12)$$

for $2^n > i \in \mathbf{N}$. This function, the i-th *maxterm* of n variables is equal to 0 if and only if $x_j = a_j^{(i)}$ for every $0 \leq j < n$. By these maxterms a Boolean function can be expressed as

$$f^{(n)} = \prod_{i=0}^{2^n-1} \left(\alpha_i + M_i^{(n)}\right) \tag{13}$$

where $\alpha_i = f^{(n)}\left(a_{n-1}^{(i)}, \ldots, a_0^{(i)}\right)$. From this last property follows that

$$f^{(n)} = \prod_{i=0}^{2^n-1} \left(\alpha_i + M_i^{(n)}\right) = f_l^{(n)}$$

where $l = \sum_{i=0}^{2^n-1} \alpha_i 2^i$.

Now again the function can be given by the indices of the maxterms not included in the function and, if there is any, by the indices of the don't cares:

$$\begin{aligned} f^{(n)} &= \prod \{i \in \mathbf{N} \,|\, i < 2^n \wedge \alpha_i = 1\} \\ d^{(n)} &= \prod \{i \in \mathbf{N} \,|\, i < 2^n \wedge M_i \text{ is a don't care term}\}. \end{aligned} \tag{14}$$

In [7] it were defined the *modified maxterms* by

$$M_i^{(n)\prime} = \sum_{j=0}^{n-1} \left(\overline{a_j^{(i)} \oplus x_j}\right). \tag{15}$$

It is easy to see that $M_i^{(n)} = M_{2^n-1-i}^{(n)\prime}$. Now if $f^{(n)} = \prod_{i=0}^{2^n-1}\left(\beta_i + M_i^{(n)\prime}\right) = f_k^{(n)}$ then $\alpha_i = f^{(n)}\left(a_{n-1}^{(i)}, \ldots, a_0^{(i)}\right) = \beta_{2^n-1-i}$. This form of the function given by the modified maxterms is the *modified conjunctive normal form* of the function. For $\overline{u} \oplus v = u \oplus \overline{v}$, so $\overline{a_j^{(i)}} \oplus x_j = a_j^{(i)} \oplus \overline{x}_j$ and $M_i^{(n)\prime} = \sum_{j=0}^{n-1}\left(a_j^{(i)} \oplus \overline{x}_j\right)$. If $g^{(n)} = \prod_{i=0}^{2^n-1}\left(\beta_i + M_i^{(n)}\right)$, then

$$\begin{aligned} f^{(n)}(x_{n-1}, \ldots, x_0) &= \prod_{i=0}^{2^n-1}\left(\alpha_i + \sum_{j=0}^{n-1}\left(a_j^{(i)} \oplus x_j\right)\right) \\ &= \prod_{i=0}^{2^n-1}\left(\alpha_i + M_i^{(n)}\right) = \prod_{i=0}^{2^n-1}\left(\beta_i + M_i^{(n)\prime}\right) \\ &= \prod_{i=0}^{2^n-1}\left(\beta_i + \sum_{j=0}^{n-1}\left(a_j^{(i)} \oplus \overline{x}_j\right)\right) \\ &= g^{(n)}(\overline{x}_{n-1}, \ldots, \overline{x}_0) = \overline{\overline{g^{(n)}}}(\overline{x}_{n-1}, \ldots, \overline{x}_0) \\ &= \overline{g^{(n)D}}(x_{n-1}, \ldots, x_0) \end{aligned} \tag{16}$$

where ^{D} denotes the dual of the function. As if $f = \overline{g^D}$ then $g = \overline{f^D}$ so $g^{(n)}$ is the complement of the dual of $f^{(n)}$ in (16).

1.2. **Polynomial-like and conjunctively polynomial-like Boolean functions.** Let's consider again the transform between the canonical disjunctive normal form and the Zhegalkin polynomial of the same function. If $\underline{\alpha}$ is the spectrum of the canonical disjunctive normal form of the function, and $\underline{k}$ is the spectrum of the Zhegalkin polynomial of the function, then $\underline{k} = \mathbf{A}^{(n)}\underline{\alpha}$. In the special case when $\underline{\alpha} = \underline{k}$, the corresponding function is a *polynomial-like Boolean function* [6]. As $\mathbf{A}^{(0)} = (1)$, so each of the two zero variable Boolean functions is polynomial-like. Now let $\underline{u} = \underline{u}_0\underline{u}_1$ be the spectrum of the canonical disjunctive normal form of a Boolean function f of $n+1$ variables, where n is a nonnegative integer. Then

$$\begin{pmatrix} \underline{u}_0 \\ \underline{u}_1 \end{pmatrix} = \begin{pmatrix} \mathbf{A}^{(n)} & \mathbf{0}^{(n)} \\ \mathbf{A}^{(n)} & \mathbf{A}^{(n)} \end{pmatrix} \begin{pmatrix} \underline{u}_0 \\ \underline{u}_1 \end{pmatrix} \tag{17}$$

if and only if $\underline{u}_0 = \mathbf{A}^{(n)}\underline{u}_0$ and $\underline{u}_1 = \mathbf{A}^{(n)}\underline{u}_0 + \mathbf{A}^{(n)}\underline{u}_1 = \underline{u}_0 + \mathbf{A}^{(n)}\underline{u}_1$, that is f is polynomial-like if and only if $\underline{u}_0 = \left(\mathbf{A}^{(n)} + \mathbf{I}^{(n)}\right)\underline{u}_1$, where $\underline{u}_1$ is the spectrum of the canonical disjunctive normal form of an arbitrary Boolean function of n variables. As a consequence we get that the number of the $n+1$ variable polynomial-like Boolean functions is equal to 2^{2^n}. It is easy to see, too, that the spectra of the canonical disjunctive normal forms of the polynomial-like Boolean functions of $n+1$ variables make up a 2^n-dimensional subspace of the 2^{n+1}-dimensional linear space of the spectra of the canonical disjunctive normal forms of all of the $n+1$ variable Boolean functions. This space is spanned by the columns of the following matrix:

$$\begin{pmatrix} \mathbf{A}^{(n)} + \mathbf{I}^{(n)} \\ \mathbf{I}^{(n)} \end{pmatrix}. \tag{18}$$

The definition of the conjunctively polynomial-like Boolean functions is similar to the definition of the polynomial-like Boolean functions. An n-variable Boolean function f is *conjunctively polynomial-like* if the spectra of its Zhegalkin polynomial and its modified conjunctive normal form are equal, that is, if $\underline{\beta} = \underline{k} = \mathbf{A}^{(n)}\underline{\alpha} = \left(\mathbf{A}^{(n)}\mathbf{P}^{(n)}\right)\underline{\beta} = \mathbf{U}^{(n)}\underline{\beta}$ where $\mathbf{P}^{(n)}$ is a $2^n \times 2^n$ matrix with 1-s in the side diagonal, and with 0-s at the other positions, that is, $P_{i,j}^{(n)} = \delta_{i,2^n-1-j}$ for $2^n > i \in \mathbf{N}$ and $2^n > j \in \mathbf{N}$, and, consequently, $U_{i,j}^{(n)} = A_{i,2^n-1-j}^{(n)}$. Then, applying (7), we get that

$$\mathbf{U}^{(n)} = \begin{cases} (1) & \text{if } n = 0 \\ \begin{pmatrix} \mathbf{0}^{(n-1)} & \mathbf{U}^{(n-1)} \\ \mathbf{U}^{(n-1)} & \mathbf{U}^{(n-1)} \end{pmatrix} & \text{if } n \in \mathbf{N}^+. \end{cases} \tag{19}$$

The minimal polynomial of $\mathbf{U}^{(n)}$ is equal to $\lambda+1$, if $n=0$, to $\lambda^2+\lambda+1$, if $n=1$, and to λ^3+1 in every other case. It means that ${\mathbf{U}^{(n)}}^3 = \mathbf{I}^{(n)}$ for every nonnegative integer n, as $(\lambda+1)(\lambda^2+\lambda+1) = \lambda^3+1$.

The condition $\underline{\beta} = \mathbf{U}^{(n)}\underline{\beta}$ is fulfilled if and only if $\left(\mathbf{I}^{(n)} + \mathbf{U}^{(n)}\right)\underline{\beta} = \underline{0}$, where $\underline{0}$ is the 2^n-dimensional zero vector over $\mathbf{F}_2$, and the last equation is true if and only if $\underline{\beta}$ lies in the nullspace of $\mathbf{I}^{(n)} + \mathbf{U}^{(n)}$.

In [7] it was stated that both of the 0-variable Boolean functions are conjunctively polynomial-like, and the conjunctively polynomial-like Boolean functions of n variables can be given by

$$\underline{\beta} = \begin{pmatrix} {\mathbf{Q}^{(n)}}^{-1}\mathbf{R}^{(n)} \\ \mathbf{I}^{(\mu_n \times \mu_n)} \end{pmatrix} \underline{u}. \tag{20}$$

Here $\mu_n = \frac{2^n + 2(-1)^n}{3}$, $2^n - \mu_n$ is the rank of

$$\mathbf{U}^{(n)} + \mathbf{I}^{(n)} = \begin{pmatrix} \mathbf{Q}^{(n)} & \mathbf{R}^{(n)} \\ \mathbf{S}^{(n)} & \mathbf{T}^{(n)} \end{pmatrix}, \tag{21}$$

$\mathbf{Q}^{(n)}$ is a $2^n - \mu_n$-order quadratic regular submatrix of $\mathbf{U}^{(n)} + \mathbf{I}^{(n)}$, and $\underline{u}$ is an arbitrary element of the μ_n-dimensional linear space over $\mathbf{F}_2$. If we denote $\begin{pmatrix} {\mathbf{Q}^{(n)}}^{-1}\mathbf{R}^{(n)} \\ \mathbf{I}^{(\mu_n \times \mu_n)} \end{pmatrix}$ by $\mathbf{Y}^{(n)}$ then $\mathbf{Y}^{(n)}$ is a $2^n \times \mu_n$ matrix and the rank of this matrix is equal to μ_n as the matrix has a μ_n-order identity matrix as a submatrix. This result can be achieved as follows.

It is almost obvious that both of the 0-variable Boolean functions are conjunctively polynomial-like. Now let $\mu_n = \frac{2^n + 2(-1)^n}{3}$ and

$$\mathbf{U}^{(n)} + \mathbf{I}^{(n)} = \begin{pmatrix} \mathbf{Q}^{(n)} & \mathbf{R}^{(n)} \\ \mathbf{S}^{(n)} & \mathbf{T}^{(n)} \end{pmatrix}$$

where $\mathbf{Q}^{(n)}$ is a $2^n - \mu_n$-order quadratic submatrix of $\mathbf{U}^{(n)} + \mathbf{I}^{(n)}$. In [7] it was proved that $\mathbf{Q}^{(n)}$ is regular, and

$$\begin{aligned} &\begin{pmatrix} {\mathbf{Q}^{(n)}}^{-1} & \mathbf{0}^{((2^n-\mu_n)\times\mu_n)} \\ \mathbf{S}^{(n)}{\mathbf{Q}^{(n)}}^{-1} & \mathbf{I}^{(\mu_n\times\mu_n)} \end{pmatrix} \begin{pmatrix} \mathbf{Q}^{(n)} & \mathbf{R}^{(n)} \\ \mathbf{S}^{(n)} & \mathbf{T}^{(n)} \end{pmatrix} \\ &= \begin{pmatrix} \mathbf{I}^{((2^n-\mu_n)\times(2^n-\mu_n))} & {\mathbf{Q}^{(n)}}^{-1}\mathbf{R}^{(n)} \\ \mathbf{0}^{(\mu_n\times(2^n-\mu_n))} & \mathbf{0}^{(\mu_n\times\mu_n)} \end{pmatrix}. \end{aligned} \tag{22}$$

If $\mathbf{Z}^{(n)} = \begin{pmatrix} {\mathbf{Q}^{(n)}}^{-1} & \mathbf{0}^{((2^n-\mu_n)\times\mu_n)} \\ \mathbf{S}^{(n)}{\mathbf{Q}^{(n)}}^{-1} & \mathbf{I}^{(\mu_n\times\mu_n)} \end{pmatrix}$, then

$$\begin{aligned} &\begin{pmatrix} \mathbf{Q}^{(n)} & \mathbf{0}^{((2^n-\mu_n)\times\mu_n)} \\ \mathbf{S}^{(n)} & \mathbf{I}^{(\mu_n\times\mu_n)} \end{pmatrix} \mathbf{Z}^{(n)} \\ &= \begin{pmatrix} \mathbf{I}^{((2^n-\mu_n)\times(2^n-\mu_n))} & \mathbf{0}^{((2^n-\mu_n)\times\mu_n)} \\ \mathbf{0}^{(\mu_n\times(2^n-\mu_n))} & \mathbf{I}^{(\mu_n\times\mu_n)} \end{pmatrix} = \mathbf{I}^{(n)}, \end{aligned} \tag{23}$$

that is, $\mathbf{Z}^{(n)}$ is a regular matrix, so $\left(\mathbf{U}^{(n)} + \mathbf{I}^{(n)}\right)\underline{\beta} = \underline{0}$ if and only if

$$\mathbf{Z}^{(n)}\left(\mathbf{U}^{(n)} + \mathbf{I}^{(n)}\right)\underline{\beta} = \underline{0}.$$

By (22) this last equation is equivalent to

$$\left(\mathbf{I}^{((2^n-\mu_n)\times(2^n-\mu_n))}\ \mathbf{Q}^{(n)^{-1}}\mathbf{R}^{(n)}\right)\begin{pmatrix}\underline{\beta}^{(1)}\\ \underline{\beta}^{(2)}\end{pmatrix}=\underline{0}^{(2^n-\mu_n)} \tag{24}$$

where $\underline{\beta}^{(1)}\in\mathbf{F}_2^{2^n-\mu_n}$ and $\underline{\beta}^{(2)}\in\mathbf{F}_2^{\mu_n}$. It means that $\underline{\beta}$ is an eigenvector of the transform represented by $\mathbf{U}^{(n)}$ if and only if $\underline{\beta}^{(1)}=\mathbf{Q}^{(n)^{-1}}\mathbf{R}^{(n)}\underline{\beta}^{(2)}$, that is, if and only if

$$\underline{\beta}=\begin{pmatrix}\mathbf{Q}^{(n)^{-1}}\mathbf{R}^{(n)}\\ \mathbf{I}^{(\mu_n\times\mu_n)}\end{pmatrix}\underline{u} \tag{25}$$

with an arbitrary $\underline{u}\in\mathbf{F}_2^{\mu_n}$.

2. New results

Let $\mathbf{U}^{(n)}$ denote the matrix of the transform of the modified canonical disjunctive normal form of a Boolean function to its Zhegalkin polynomial. As 1 is the (only) eigenvalue of the transform, the space of the eigenvectors of the transform is equal to the nullspace of the transform determined by $\mathbf{U}^{(n)}+\mathbf{I}^{(n)}$, so, if we want to generate the conjunctively polynomial-like Boolean functions, we have to determine a basis of this nullspace. From now on we denote the matrix the columns of which are linearly independent, and which span the nullspace of $\mathbf{U}^{(n)}+\mathbf{I}^{(n)}$ by $\mathbf{V}^{(n)}$. This matrix is a $2^n\times\mu_n$-order matrix where $\mu_n=\frac{2^n+2(-1)^n}{3}$. As we saw, such a matrix is for instance $\begin{pmatrix}\mathbf{Q}^{(n)^{-1}}\mathbf{R}^{(n)}\\ \mathbf{I}^{(\mu_n\times\mu_n)}\end{pmatrix}$ where $\mathbf{Q}^{(n)}$ is the $2^n-\mu_n$-order left upper submatrix of $\mathbf{U}^{(n)}+\mathbf{I}^{(n)}$, and $\mathbf{R}^{(n)}$ is the $(2^n-\mu_n)\times\mu_n$-size right upper submatrix of the same matrix. If $n>1$ then $\mu_n>1$, and then $\mathbf{V}^{(n)}$ is not uniquely determined, as every column of $\mathbf{V}^{(n)}$ contains at least one nonzero element, and then adding for instance the first column to the second one, this matrix differs from $\mathbf{V}^{(n)}$, the columns of the new matrix are linearly independent, and also they span the nullspace of $\mathbf{U}^{(n)}+\mathbf{I}^{(n)}$. If the last μ_n rows of $\mathbf{V}^{(n)}$ establish a μ_n-order identity matrix, and we want to emphasize this property of the matrix, then this matrix will be denoted by $\mathbf{V}_0^{(n)}$ (earlier such a matrix was denoted by $\mathbf{Y}^{(n)}$). In the case of $n=1$, $\mu_n=0$, so $\mathbf{V}^{(n)}$ is uniquely determined, and the last μ_n rows of this matrix form an identity matrix. If $n=0$, then $\mu_n=1$, $\mathbf{U}^{(n)}+\mathbf{I}^{(n)}=(0)$, and (1) is the only $\mathbf{V}^{(n)}$, so in this case again $\mathbf{V}^{(n)}$ is uniquely determined, and the last μ_n rows of $\mathbf{V}^{(n)}$ form an identity matrix. Now we have that if $n<2$ then necessarily

$$\mathbf{V}^{(n)}=\mathbf{V}_0^{(n)}. \tag{26}$$

In general, $\mathbf{V}_0^{(n)}$ is uniquely determined as if $\mathbf{V}$ is a matrix with similar properties, then $\mathbf{V}=\mathbf{V}_0^{(n)}\mathbf{K}$ with a regular μ_n-order quadratic matrix, and then it is true for the last μ_n rows of the matrices, too, that is $\mathbf{I}^{(\mu_n\times\mu_n)}=\mathbf{I}^{(\mu_n\times\mu_n)}\mathbf{K}$, so $\mathbf{K}=\mathbf{I}^{(\mu_n\times\mu_n)}$ and $\mathbf{V}=\mathbf{V}_0^{(n)}$.

Theorem 1. *If* $\mu_n = \frac{2^n+2(-1)^n}{3}$ *for* $n \in \mathbf{N}$ *then* $\mu_{n+2} = 2^n + \mu_n$.

Proof.

$$\begin{aligned} \mu_{n+2} &= \frac{2^{n+2} + 2\,(-1)^{n+2}}{3} = \frac{4 \cdot 2^n + 2\,(-1)^n}{3} \\ &= 2^n + \frac{2^n + 2\,(-1)^n}{3} = 2^n + \mu_n. \end{aligned} \tag{27}$$

□

From the previous theorem follows that $\mathbf{V}^{(n+2)}$ is a $2^{n+2} \times \mu_{n+2} = 2^{n+2} \times (2^n + \mu_n)$-size matrix. Then it can be partitioned to a 1×2 hypermatrix so that the first element of this matrix is a μ_n-column matrix, and the second element is a matrix with 2^n columns.

By recursion we can express $\mathbf{U}^{(n+2)} + \mathbf{I}^{(n+2)}$ in the following form:

$$\mathbf{U}^{(n+2)} + \mathbf{I}^{(n+2)} = \begin{pmatrix} \mathbf{I}^{(n)} & \mathbf{0}^{(n)} & \mathbf{0}^{(n)} & \mathbf{U}^{(n)} \\ \mathbf{0}^{(n)} & \mathbf{I}^{(n)} & \mathbf{U}^{(n)} & \mathbf{U}^{(n)} \\ \mathbf{0}^{(n)} & \mathbf{U}^{(n)} & \mathbf{I}^{(n)} & \mathbf{U}^{(n)} \\ \mathbf{U}^{(n)} & \mathbf{U}^{(n)} & \mathbf{U}^{(n)} & \mathbf{U}^{(n)} + \mathbf{I}^{(n)} \end{pmatrix}. \tag{28}$$

We will use this form in the further parts of the paper.

Theorem 2. *The columns of*

$$\mathbf{W}^{(n+2)} = \begin{pmatrix} \mathbf{0}^{(2^n \times \mu_n)} \\ \mathbf{V}^{(n)} \\ \mathbf{V}^{(n)} \\ \mathbf{0}^{(2^n \times \mu_n)} \end{pmatrix} \tag{29}$$

are eigenvectors of the transform determined by $\mathbf{U}^{(n+2)}$.

Proof. As the columns of $\mathbf{V}^{(n)}$ establish a basis of the subspace of the eigenvectors of the transform of $\mathbf{U}^{(n)}$, and the eigenvalue of the transform is equal to 1, so

$$\left(\mathbf{U}^{(n)} + \mathbf{I}^{(n)}\right) \mathbf{V}^{(n)} = \mathbf{0}^{(2^n \times \mu_n)}. \tag{30}$$

Then

$$\begin{aligned} \left(\mathbf{U}^{(n+2)} + \mathbf{I}^{(n+2)}\right) \mathbf{W}^{(n+2)} &= \begin{pmatrix} \mathbf{I}^{(n)} & \mathbf{0}^{(n)} & \mathbf{0}^{(n)} & \mathbf{U}^{(n)} \\ \mathbf{0}^{(n)} & \mathbf{I}^{(n)} & \mathbf{U}^{(n)} & \mathbf{U}^{(n)} \\ \mathbf{0}^{(n)} & \mathbf{U}^{(n)} & \mathbf{I}^{(n)} & \mathbf{U}^{(n)} \\ \mathbf{U}^{(n)} & \mathbf{U}^{(n)} & \mathbf{U}^{(n)} & \mathbf{U}^{(n)} + \mathbf{I}^{(n)} \end{pmatrix} \begin{pmatrix} \mathbf{0}^{(2^n \times \mu_n)} \\ \mathbf{V}^{(n)} \\ \mathbf{V}^{(n)} \\ \mathbf{0}^{(2^n \times \mu_n)} \end{pmatrix} \\ &= \begin{pmatrix} \mathbf{0}^{(2^n \times \mu_n)} \\ \mathbf{0}^{(2^n \times \mu_n)} \\ \mathbf{0}^{(2^n \times \mu_n)} \\ \mathbf{0}^{(2^n \times \mu_n)} \end{pmatrix}. \end{aligned}$$

□

From the theorem above it follows that we can search $\mathbf{V}^{(n+2)}$ in the following form:

$$\mathbf{V}^{(n+2)} = \begin{pmatrix} \mathbf{W}^{(n+2)} & \mathbf{M}^{(n+2)} \end{pmatrix} \tag{31}$$

where $\mathbf{M}^{(n+2)}$ is a $2^{n+2}\times 2^n = 4\cdot 2^n \times 2^n$-size matrix. The columns of $\mathbf{V}^{(n+2)}$ form a basis of the μ_{n+2}-dimensional subspace of the $n+2$-variable conjunctively polynomial-like Boolean functions, and then the columns of $\mathbf{V}^{(n+2)}$ are linearly independent. In this case $\mathbf{V}^{(n+2)}$ can contain a μ_{n+2}-order identity matrix as a submatrix. The 2^n last rows of $\mathbf{W}^{(n+2)}$ contain only 0-s, so if the last 2^n rows of $\mathbf{M}^{(n+2)}$ give a 2^n-order identity matrix, then with this choice the columns of $\begin{pmatrix} \mathbf{W}^{(n+2)} & \mathbf{M}^{(n+2)} \end{pmatrix}$ are surely linearly independent. We shall see that really there is a basis of the space of the $n+2$-variable conjunctively polynomial-like Boolean functions with this property.

Let's partition $\mathbf{M}^{(n+2)}$ into the column-matrix of four 2^n-order quadratic matrices, the fourth of which is the identity matrix:

$$\mathbf{M}^{(n+2)} = \begin{pmatrix} \mathbf{B}^{(n)} \\ \mathbf{C}^{(n)} \\ \mathbf{D}^{(n)} \\ \mathbf{I}^{(n)} \end{pmatrix}. \tag{32}$$

As

$$\mathbf{U}^{(n+1)} = \begin{pmatrix} \mathbf{0}^{(n)} & \mathbf{U}^{(n)} \\ \mathbf{U}^{(n)} & \mathbf{U}^{(n)} \end{pmatrix} \tag{33}$$

and then

$$\begin{aligned} \mathbf{U}^{(n+2)} &= \begin{pmatrix} \mathbf{0}^{(n+1)} & \mathbf{U}^{(n+1)} \\ \mathbf{U}^{(n+1)} & \mathbf{U}^{(n+1)} \end{pmatrix} \\ &= \begin{pmatrix} \mathbf{0}^{(n)} & \mathbf{0}^{(n)} & \mathbf{0}^{(n)} & \mathbf{U}^{(n)} \\ \mathbf{0}^{(n)} & \mathbf{0}^{(n)} & \mathbf{U}^{(n)} & \mathbf{U}^{(n)} \\ \mathbf{0}^{(n)} & \mathbf{U}^{(n)} & \mathbf{0}^{(n)} & \mathbf{U}^{(n)} \\ \mathbf{U}^{(n)} & \mathbf{U}^{(n)} & \mathbf{U}^{(n)} & \mathbf{U}^{(n)} \end{pmatrix}, \end{aligned} \tag{34}$$

from the criterion of $\left(\mathbf{U}^{(n+2)} + \mathbf{I}^{(n+2)}\right)\mathbf{M}^{(n+2)} = \mathbf{0}^{\left(2^{n+2}\times 2^n\right)}$ we get the following equations:

$$\begin{aligned} \mathbf{B}^{(n)} + \mathbf{U}^{(n)} &= \mathbf{0}^{(n)} \\ \mathbf{C}^{(n)} + \mathbf{U}^{(n)}\left(\mathbf{D}^{(n)} + \mathbf{I}^{(n)}\right) &= \mathbf{0}^{(n)} \\ \mathbf{D}^{(n)} + \mathbf{U}^{(n)}\left(\mathbf{C}^{(n)} + \mathbf{I}^{(n)}\right) &= \mathbf{0}^{(n)} \\ \mathbf{U}^{(n)}\left(\mathbf{B}^{(n)} + \mathbf{C}^{(n)} + \mathbf{D}^{(n)}\right) + \left(\mathbf{U}^{(n)} + \mathbf{I}^{(n)}\right) &= \mathbf{0}^{(n)} \end{aligned} \tag{35}$$

or, in another form

$$
\begin{array}{rcccccl}
\mathbf{B}^{(n)} & & & & & = & \mathbf{U}^{(n)} \\
& & \mathbf{C}^{(n)} & + & \mathbf{U}^{(n)}\mathbf{D}^{(n)} & = & \mathbf{U}^{(n)} \\
& & \mathbf{U}^{(n)}\mathbf{C}^{(n)} & + & \mathbf{D}^{(n)} & = & \mathbf{U}^{(n)} \\
\mathbf{U}^{(n)}\mathbf{B}^{(n)} & + & \mathbf{U}^{(n)}\mathbf{C}^{(n)} & + & \mathbf{U}^{(n)}\mathbf{D}^{(n)} & = & \mathbf{U}^{(n)} + \mathbf{I}^{(n)}.
\end{array} \tag{36}
$$

Considering that $\left(\mathbf{U}^{(n)}\right)^3 = \mathbf{I}^{(n)}$, the last equation is a consequence of the previous three equations, as

$$
\begin{pmatrix}
\mathbf{I}^{(n)} & \mathbf{0}^{(n)} & \mathbf{0}^{(n)} & \mathbf{0}^{(n)} \\
\mathbf{0}^{(n)} & \mathbf{I}^{(n)} & \mathbf{0}^{(n)} & \mathbf{0}^{(n)} \\
\mathbf{0}^{(n)} & \mathbf{U}^{(n)2} & \mathbf{U}^{(n)} & \mathbf{0}^{(n)} \\
\mathbf{U}^{(n)} & \mathbf{U}^{(n)} + \mathbf{I}^{(n)} & \mathbf{U}^{(n)2} & \mathbf{I}^{(n)}
\end{pmatrix}
\begin{pmatrix}
\mathbf{I}^{(n)} & \mathbf{0}^{(n)} & \mathbf{0}^{(n)} & \mathbf{U}^{(n)} \\
\mathbf{0}^{(n)} & \mathbf{I}^{(n)} & \mathbf{U}^{(n)} & \mathbf{U}^{(n)} \\
\mathbf{0}^{(n)} & \mathbf{U}^{(n)} & \mathbf{I}^{(n)} & \mathbf{U}^{(n)} \\
\mathbf{U}^{(n)} & \mathbf{U}^{(n)} & \mathbf{U}^{(n)} & \mathbf{U}^{(n)} + \mathbf{I}^{(n)}
\end{pmatrix} =
$$

$$
= \begin{pmatrix}
\mathbf{I}^{(n)} & \mathbf{0}^{(n)} & \mathbf{0}^{(n)} & \mathbf{U}^{(n)} \\
\mathbf{0}^{(n)} & \mathbf{I}^{(n)} & \mathbf{U}^{(n)} & \mathbf{U}^{(n)} \\
\mathbf{0}^{(n)} & \mathbf{0}^{(n)} & \mathbf{U}^{(n)} + \mathbf{I}^{(n)} & \mathbf{U}^{(n)2} + \mathbf{I}^{(n)} \\
\mathbf{0}^{(n)} & \mathbf{0}^{(n)} & \mathbf{0}^{(n)} & \mathbf{0}^{(n)}
\end{pmatrix} \tag{37}
$$

(and

$$
\begin{pmatrix}
\mathbf{I}^{(n)} & \mathbf{0}^{(n)} & \mathbf{0}^{(n)} & \mathbf{0}^{(n)} \\
\mathbf{0}^{(n)} & \mathbf{I}^{(n)} & \mathbf{0}^{(n)} & \mathbf{0}^{(n)} \\
\mathbf{0}^{(n)} & \mathbf{U}^{(n)2} & \mathbf{U}^{(n)} & \mathbf{0}^{(n)} \\
\mathbf{U}^{(n)} & \mathbf{U}^{(n)} + \mathbf{I}^{(n)} & \mathbf{U}^{(n)2} & \mathbf{I}^{(n)}
\end{pmatrix} \tag{38}
$$

is a regular matrix as it is a lower triangle matrix – as a hypermatrix! – with regular matrices in its main diagonal).

From the second equation in (35)

$$
\mathbf{C}^{(n)} = \mathbf{U}^{(n)}\left(\mathbf{D}^{(n)} + \mathbf{I}^{(n)}\right), \tag{39}
$$

and with this result we get from the third equation that

$$
\left(\mathbf{U}^{(n)2} + \mathbf{I}^{(n)}\right)\mathbf{D}^{(n)} = \mathbf{U}^{(n)2} + \mathbf{U}^{(n)}. \tag{40}
$$

Multiplying from the left by $\mathbf{U}^{(n)}$

$$
\left(\mathbf{U}^{(n)} + \mathbf{I}^{(n)}\right)\mathbf{D}^{(n)} = \mathbf{U}^{(n)2} + \mathbf{I}^{(n)} = \left(\mathbf{U}^{(n)} + \mathbf{I}^{(n)}\right)^2. \tag{41}
$$

This last equation has several solutions, as $\mathbf{U}^{(n)}+\mathbf{I}^{(n)}$ is not regular. Apparently one of the solutions is the following:

$$
\mathbf{D}^{(n)} = \mathbf{U}^{(n)} + \mathbf{I}^{(n)}. \tag{42}
$$

Then

$$
\mathbf{C}^{(n)} = \mathbf{U}^{(n)}\left(\mathbf{D}^{(n)} + \mathbf{I}^{(n)}\right) = \mathbf{U}^{(n)2} \tag{43}
$$

and from the first equation in (36)

$$
\mathbf{B}^{(n)} = \mathbf{U}^{(n)}. \tag{44}
$$

With all of these results we get that we can choose $\mathbf{M}^{(n+2)}$ as follows:

$$\mathbf{M}^{(n+2)} = \begin{pmatrix} \mathbf{U}^{(n)} \\ \mathbf{U}^{(n)^2} \\ \mathbf{U}^{(n)} + \mathbf{I}^{(n)} \\ \mathbf{I}^{(n)} \end{pmatrix} \tag{45}$$

and then the columns of

$$\mathbf{O} = \begin{pmatrix} \mathbf{0}^{(2^n \times \mu_n)} & \mathbf{U}^{(n)} \\ \mathbf{V}^{(n)} & \mathbf{U}^{(n)^2} \\ \mathbf{V}^{(n)} & \mathbf{U}^{(n)} + \mathbf{I}^{(n)} \\ \mathbf{0}^{(2^n \times \mu_n)} & \mathbf{I}^{(n)} \end{pmatrix} \tag{46}$$

set up a basis of the linear space of the conjunctively polynomial-like Boolean functions of $n+2$ variables. This means that $\mathbf{O} = \mathbf{V}^{(n+2)}$.

If $n > 1$ then $\mu_n > 1$, and the last μ_n rows of $\mathbf{U}^{(n)} + \mathbf{I}^{(n)}$ contain nonzero elements, so the submatrix of the last μ_{n+2} rows of $\mathbf{O}$ is not equal to the μ_{n+2}-order identity matrix. From this follows that $\mathbf{V}^{(n+2)}$ given above is not equal to $\mathbf{V}_0^{(n+2)}$. But if $\mathbf{V}^{(n)}$ in $\mathbf{O}$ is equal to $\mathbf{V}_0^{(n)}$, then

$$\mathbf{V}^{(n)} = \mathbf{V}_0^{(n)} = \begin{pmatrix} \mathbf{H}^{(n)} \\ \mathbf{I}^{(\mu_n \times \mu_n)} \end{pmatrix} \tag{47}$$

where $\mathbf{H}^{(n)}$ is a $(2^n - \mu_n) \times \mu_n$-size matrix. Let

$$\mathbf{U}^{(n)} + \mathbf{I}^{(n)} = \begin{pmatrix} \mathbf{F}^{(n)} \\ \mathbf{G}^{(n)} \end{pmatrix} \tag{48}$$

with a $\mu_n \times 2^n$-size $\mathbf{G}^{(n)}$. Then

$$\begin{aligned} \left(\mathbf{U}^{(n)} + \mathbf{I}^{(n)}\right) + \mathbf{V}_0^{(n)}\mathbf{G}^{(n)} &= \begin{pmatrix} \mathbf{F}^{(n)} \\ \mathbf{G}^{(n)} \end{pmatrix} + \begin{pmatrix} \mathbf{H}^{(n)} \\ \mathbf{I}^{(\mu_n \times \mu_n)} \end{pmatrix} \mathbf{G}^{(n)} \\ &= \begin{pmatrix} \mathbf{F}^{(n)} + \mathbf{H}^{(n)}\mathbf{G}^{(n)} \\ \mathbf{0}^{(\mu_n \times 2^n)} \end{pmatrix} \end{aligned} \tag{49}$$

and consequently

$$\begin{aligned} \mathbf{O} \cdot \begin{pmatrix} \mathbf{I}^{(\mu_n \times \mu_n)} & \mathbf{G}^{(n)} \\ \mathbf{0}^{(2^n \times \mu_n)} & \mathbf{I}^{(n)} \end{pmatrix} &= \begin{pmatrix} \mathbf{0}^{(2^n \times \mu_n)} & \mathbf{U}^{(n)} \\ \mathbf{V}_0^{(n)} & \mathbf{U}^{(n)^2} \\ \mathbf{V}_0^{(n)} & \mathbf{U}^{(n)} + \mathbf{I}^{(n)} \\ \mathbf{0}^{(2^n \times \mu_n)} & \mathbf{I}^{(n)} \end{pmatrix} \cdot \begin{pmatrix} \mathbf{I}^{(\mu_n \times \mu_n)} & \mathbf{G}^{(n)} \\ \mathbf{0}^{(2^n \times \mu_n)} & \mathbf{I}^{(n)} \end{pmatrix} \\ &= \begin{pmatrix} \mathbf{0}^{(2^n \times \mu_n)} & \mathbf{U}^{(n)} \\ \mathbf{V}_0^{(n)} & \mathbf{U}^{(n)^2} + \mathbf{V}_0^{(n)}\mathbf{G}^{(n)} \\ \mathbf{V}_0^{(n)} & \left(\mathbf{U}^{(n)} + \mathbf{I}^{(n)}\right) + \mathbf{V}_0^{(n)}\mathbf{G}^{(n)} \\ \mathbf{0}^{(2^n \times \mu_n)} & \mathbf{I}^{(n)} \end{pmatrix} \end{aligned}$$

$$= \begin{pmatrix} \mathbf{0}^{(2^n\times\mu_n)} & \mathbf{U}^{(n)} \\ \mathbf{V}_0^{(n)} & \mathbf{U}^{(n)^2} + \mathbf{V}_0^{(n)}\mathbf{G}^{(n)} \\ \mathbf{H}^{(n)} & \mathbf{F}^{(n)}+\mathbf{H}^{(n)}\mathbf{G}^{(n)} \\ \mathbf{I}^{(\mu_n\times\mu_n)} & \mathbf{0}^{(\mu_n\times 2^n)} \\ \mathbf{0}^{(2^n\times\mu_n)} & \mathbf{I}^{(n)} \end{pmatrix} \tag{50}$$

$$= \begin{pmatrix} \mathbf{H}^{(n+2)} \\ \mathbf{I}^{(\mu_{n+2}\times\mu_{n+2})} \end{pmatrix} = \mathbf{V}_0^{(n+2)}.$$

In [7] it was stated that the columns of $\begin{pmatrix} \mathbf{Q}^{(n)^{-1}}\mathbf{R}^{(n)} \\ \mathbf{I}^{(\mu_n\times\mu_n)} \end{pmatrix}$ form a basis of the nullspace of $\mathbf{U}^{(n)} + \mathbf{I}^{(n)}$, where

$$\mathbf{U}^{(n)} + \mathbf{I}^{(n)} = \begin{pmatrix} \mathbf{Q}^{(n)} & \mathbf{R}^{(n)} \\ \mathbf{S}^{(n)} & \mathbf{T}^{(n)} \end{pmatrix} \tag{51}$$

with the $2^n - \mu_n$-order regular matrix of $\mathbf{Q}^{(n)}$. As $\mathbf{V}_0^{(n)}$ is uniquely determined, so we get that

$$\mathbf{Q}^{(n+2)^{-1}}\mathbf{R}^{(n+2)} = \mathbf{H}^{(n+2)} = \begin{pmatrix} \mathbf{0}^{(2^n\times\mu_n)} & \mathbf{U}^{(n)} \\ \mathbf{V}_0^{(n)} & \mathbf{U}^{(n)2} + \mathbf{V}_0^{(n)}\mathbf{G}^{(n)} \\ \mathbf{H}^{(n)} & \mathbf{F}^{(n)}+\mathbf{H}^{(n)}\mathbf{G}^{(n)} \end{pmatrix}. \tag{52}$$

3. Conclusion

In an earlier paper [7] a matrix was given, the columns of which linearly independent are and generate the space of the conjunctively polynomial-like Boolean functions. If

$$\mathbf{U}^{(n)} + \mathbf{I}^{(n)} = \begin{pmatrix} \mathbf{Q}^{(n)} & \mathbf{R}^{(n)} \\ \mathbf{S}^{(n)} & \mathbf{T}^{(n)} \end{pmatrix} \tag{53}$$

where $\mathbf{U}^{(n)}$ denotes the matrix of the transform from the space of the modified canonical conjunctive form of the Boolean functions to the space of the Zhegalkin polynomial of the switching functions and $\mathbf{Q}^{(n)}$ is a $2^n - \mu_n$-order quadratic matrix then this generator matrix is

$$\begin{pmatrix} \mathbf{Q}^{(n)^{-1}}\mathbf{R}^{(n)} \\ \mathbf{I}^{(\mu_n\times\mu_n)} \end{pmatrix}. \tag{54}$$

To determine this matrix one have to invert a rather big matrix which is a time-consuming procedure. In the present paper it was pointed out that this matrix can be generated recursively, too. If we don't hold to a matrix containing an identity matrix as a submatrix as large as the number of the columns of the matrix, then our matrix can be generated rather quickly by the following recursion:

$$\mathbf{V}^{(0)} = (1) \tag{55}$$

$$\mathbf{V}^{(1)} = () \tag{56}$$

and for $n \in \mathbf{N}$

$$\mathbf{V}^{(n+2)} = \begin{pmatrix} \mathbf{0}^{(2^n \times \mu_n)} & \mathbf{U}^{(n)} \\ \mathbf{V}^{(n)} & \mathbf{U}^{(n)^2} \\ \mathbf{V}^{(n)} & \mathbf{U}^{(n)} + \mathbf{I}^{(n)} \\ \mathbf{0}^{(2^n \times \mu_n)} & \mathbf{I}^{(n)} \end{pmatrix}. \tag{57}$$

Also $\mathbf{U}^{(n)}$ and $\left(\mathbf{U}^{(n)}\right)^2$ can be generated by very simple recursions: $\mathbf{U}^{(0)} = (1)$, and the recursion for $\mathbf{U}^{(n)}$ is as follows

$$\mathbf{U}^{(n+1)} = \begin{pmatrix} \mathbf{0}^{(n)} & \mathbf{U}^{(n)} \\ \mathbf{U}^{(n)} & \mathbf{U}^{(n)} \end{pmatrix}; \tag{58}$$

finally for every $n \in \mathbf{N}$, $2^n > i \in \mathbf{N}$ and $2^n > j \in \mathbf{N}$

$$\left(\left(\mathbf{U}^{(n)}\right)^2\right)_{i,j} = \mathbf{U}^{(n)}_{2^n-1-i,2^n-1-j}. \tag{59}$$

By recursion it means that $\left(\mathbf{U}^{(0)}\right)^2 = (1)$ and

$$\left(\mathbf{U}^{(n+1)}\right)^2 = \begin{pmatrix} \left(\mathbf{U}^{(n)}\right)^2 & \left(\mathbf{U}^{(n)}\right)^2 \\ \left(\mathbf{U}^{(n)}\right)^2 & \mathbf{0}^{(n)} \end{pmatrix}. \tag{60}$$

References

[1] S. B. J. Akers. On a theory of Boolean functions. *J. Soc. Ind. Appl. Math.*, 7:487–498, 1959.

[2] R. Beigel. The polynomial method in circuit complexity. In *Proceedings of the Eighth Annual Structure in Complexity Theory Conference (San Diego, CA, 1993)*, pages 82–95, Los Alamitos, CA, 1993. IEEE Comput. Soc. Press.

[3] P. Calingaert. Switching function canonical forms based on commutative and associative binary operations. In *FOCS '61: Proceedings of the 2nd Annual Symposium on Switching Circuit Theory and Logical Design (SWCT 1961)*, pages 217–224, Washington, DC, USA, 1961. IEEE Computer Society.

[4] M. Davio, J.-P. Deschamps, and A. Thayse. *Discrete and switching functions.* Georgi Publishing Co., St., 1978. With a foreword by Raymond T. Yeh.

[5] J. Gonda. Transformation of the canonical disjunctive normal form of a Boolean function to its Zhegalkin-polynomial and back. *Ann. Univ. Sci. Budapest. Sect. Comput.*, 20:147–156, 2001.

[6] J. Gonda. Polynomial-like Boolean functions. *Ann. Univ. Sci. Budapest. Sect. Comput.*, 25:13–23, 2005.

[7] J. Gonda. Conjunctively polynomial-like Boolean functions. *Acta Math. Acad. Paedagog. Nyházi. (N.S.)*, 23(2):89–103, 2007.

[8] R. J. Lechner. Harmonic analysis of switching functions. In *Recent Developments in Switching Theory*, pages 121–228. Academic Press, New York, 1971.

[9] E. L. Post. Introduction to a general theory of elementary propositions. *Am. J. Math.*, 43:163–185, 1921.

[10] E. L. Post. *The two-valued iterative systems of mathematical logic.* (Annals of Mathematics Studies. 5) Princeton, N.J.: Princeton University Press, VIII, 122 p. , 1941.

Received September 18, 2008. Revised March 30, 2010.

Department of Computer Algebra,
Faculty of Informatics,
Eötvös Loránd Universitiy,
H1117 Budapest, Pázmány Péter sétány 1/c
E-mail address: andog@compalg.inf.elte.hu