Acta Mathematica Academiae Paedagogicae Nyíregyháziensis
23(2) (2007), 89–103
www.emis.de/journals
ISSN 1786-0091

CONJUNCTIVELY POLYNOMIAL-LIKE BOOLEAN FUNCTIONS

J. GONDA

Abstract. In this article we apply the notion of the modified conjunctive normal form of a Boolean function which is equal to the canonical conjunctive normal form of the complement of the dual of the same Boolean function. In the article a linear algebraic transform is given between the modified conjunctive normal form and the Zhegalkin polynomial of a Boolean function and then the notion of the conjunctively polynomial-like Boolean functions as the functions having the same series of the coefficients in their modified conjunctive normal forms and in their Zhegalkin polynomials is introduced.

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 $\overline{\ }$. 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; $\mathbf{N}_0$ denotes the non-negative integers, and $\mathbf{N}$ the positive ones.

1. Introduction

Logical functions and especially the two-valued ones have important roles in our everyday life, so it is easy to understand that 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, 7]). 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 [9], 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 the following article we examine such a class of the logical functions of two values.

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

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

This research was supported by the grants OTKA 5434.

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 $0 \le j < n$, 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 $[0 \ldots 2^n - 1]$, 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 series 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 series is the spectrum of the canonical disjunctive normal form of the function, and similarly will be defined the spectrum with respect to other representation of the function), i.e. for $k = \sum_{i=0}^{2^n-1} \alpha_i^{(k)} 2^i$ with $\alpha_i^{(k)} \in \{0, 1\}$

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

Now, $f_k^{(n)}$ denotes the k-th Boolean function of n variables.

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

$$M_i^{(n)} = \sum_{j=0}^{n-1} \left(a_j^{(i)} \oplus x_j \right) \tag{3}$$

for $2^n > i \in \mathbf{N}_0$. This function, the i-th *maxterm* of n variables is equal to 0 if and only if $x_j = a_j^{(i)}$ for every $0 \le j < n$. By these maxterms a Boolean function can be expressed as

$$f^{(n)} = \prod_{i=0}^{2^n-1} \left(\alpha_i + M_i^{(n)} \right) \tag{4}$$

where $\alpha_i = f^{(n)}\left(a_{n-1}^{(i)}, \dots, a_0^{(i)}\right)$. 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 $l = \sum_{i=0}^{2^n-1} \alpha_i 2^i$.

For our present investigations it will be more convenient to introduce the notion of the *modified maxterm* defined by

$$M_i^{(n)\prime} = \sum_{j=0}^{n-1}\left(\overline{a_j^{(i)}} \oplus x_j\right). \tag{5}$$

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 $\alpha_i = f^{(n)}\left(a_{n-1}^{(i)}, \dots, a_0^{(i)}\right) = \beta_{2^n-1-i}$. From now on we refer to this form of the function given by the modified maxterms as 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

$$\begin{aligned}
f^{(n)}\left(x_{n-1}, \dots, x_0\right) &= \prod_{i=0}^{2^n-1}\left(\alpha_i + \sum_{j=0}^{n-1}\left(a_j^{(i)} \oplus x_j\right)\right) \\
&= \prod_{i=0}^{2^n-1}\left(\alpha_i + M_i^{(n)}\right) = \prod_{i=0}^{2^n-1}\left(\beta_i + M_i^{(n)\prime}\right) \\
&= \prod_{i=0}^{2^n-1}\left(\beta_i + \sum_{j=0}^{n-1}\left(a_j^{(i)} \oplus \overline{x}_j\right)\right) \\
&= g^{(n)}\left(\overline{x}_{n-1}, \dots, \overline{x}_0\right) = \overline{\overline{g^{(n)}}}\left(\overline{x}_{n-1}, \dots, \overline{x}_0\right) \\
&= \overline{g^{(n)D}}\left(x_{n-1}, \dots, x_0\right)
\end{aligned} \tag{6}$$

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 (6).

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 series, and if the i-th member of such a series is k_i then

$$f^{(n)} = \bigoplus_{i=0}^{2^n-1} k_i S_i^{(n)}. \tag{7}$$

Between the first and the third representations 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 $\mathbf{F}_2$, 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

$$\mathbf{A}^{(n)} = \begin{cases} (1) & \text{if } n = 0 \\ \begin{pmatrix} \mathbf{A}^{(n-1)} & \mathbf{0}^{(n-1)} \\ \mathbf{A}^{(n-1)} & \mathbf{A}^{(n-1)} \end{pmatrix} & \text{if } n \in \mathbf{N} \end{cases} \tag{8}$$

(see for instance in [4]) and as a consequence that

$$\mathbf{A}^{(n)^2} = \mathbf{I}^{(n)}, \tag{9}$$

where $\mathbf{I}^{(n)}$ and $\mathbf{0}^{(n)}$ denote the 2^n-dimensional identity and zero matrix, respectively. From this follows that if $\underline{k} = \mathbf{A}^{(n)}\underline{\alpha}$, then $\underline{\alpha} = \mathbf{A}^{(n)}\underline{k}$. 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

$$\begin{pmatrix} \underline{u}_0 \\ \underline{u}_1 \end{pmatrix} = \begin{pmatrix} \mathbf{A}^{(n)} & \mathbf{0}^{(n)} \\ \mathbf{A}^{(n)} & \mathbf{A}^{(n)} \end{pmatrix} \begin{pmatrix} \underline{u}_0 \\ \underline{u}_1 \end{pmatrix} \tag{10}$$

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.

Now, in the following parts of this article we deal with the relationship between the modified conjunctive normal form and the Zhegalkin polynomial of the function.

2. Development

Let $\underline{\beta}_{\leftarrow}$ denote the vector the i-th component of which is equal to the 2^n-1-i-th component of $\underline{\beta} \in \mathbf{F}_2^n$. If $\mathbf{P}^{(n)}$ is a $2^n \times 2^n$ matrix with the elements $P_{i,j} =$

$\delta_{2^n-1-i,j}$, that is with 1 in the side diagonal and with 0 at the other positions of the matrix, then $\underline{\alpha}=\underline{\beta}_{\leftarrow}=\mathbf{P}^{(n)}\underline{\beta}$. As $\underline{k}=\mathbf{A}^{(n)}\underline{\alpha}$, so $\underline{k}=\left(\mathbf{A}^{(n)}\mathbf{P}^{(n)}\right)\underline{\beta}$, that is, denoting $\mathbf{A}^{(n)}\mathbf{P}^{(n)}$ by $\mathbf{U}^{(n)}$,

$$\underline{k}=\mathbf{U}^{(n)}\underline{\beta}. \tag{11}$$

Let's investigate $\mathbf{U}^{(n)}$.

Theorem 1. $\mathbf{U}^{(0)}=(1)$ *and for* $n\in\mathbf{N}_0$

$$\mathbf{U}^{(n+1)}=\begin{pmatrix}\mathbf{0}^{(n)} & \mathbf{U}^{(n)}\\ \mathbf{U}^{(n)} & \mathbf{U}^{(n)}\end{pmatrix}. \tag{12}$$

Proof. $\mathbf{U}^{(0)}=\mathbf{A}^{(0)}\mathbf{P}^{(0)}=(1)\,(1)=(1)=\mathbf{I}^{(0)}$, and

$$\begin{aligned}\mathbf{U}^{(n+1)}&=\mathbf{A}^{(n+1)}\mathbf{P}^{(n+1)}\\ &=\begin{pmatrix}\mathbf{A}^{(n)} & \mathbf{0}^{(n)}\\ \mathbf{A}^{(n)} & \mathbf{A}^{(n)}\end{pmatrix}\begin{pmatrix}\mathbf{0}^{(n)} & \mathbf{P}^{(n)}\\ \mathbf{P}^{(n)} & \mathbf{0}^{(n)}\end{pmatrix}\\ &=\begin{pmatrix}\mathbf{0}^{(n)} & \mathbf{A}^{(n)}\mathbf{P}^{(n)}\\ \mathbf{A}^{(n)}\mathbf{P}^{(n)} & \mathbf{A}^{(n)}\mathbf{P}^{(n)}\end{pmatrix}\\ &=\begin{pmatrix}\mathbf{0}^{(n)} & \mathbf{U}^{(n)}\\ \mathbf{U}^{(n)} & \mathbf{U}^{(n)}\end{pmatrix}.\end{aligned} \tag{13}$$

□

Theorem 2. $\mathbf{U}^{(n)}$ *is regular for any* $n\in\mathbf{N}_0$. *The order of* $\mathbf{U}^{(n)}$ *is equal to* 1 *if* $n=0$ *and to* 3 *if* $n>0$.

Proof. ${\mathbf{U}^{(0)}}^3={\mathbf{I}^{(0)}}^3=\mathbf{I}^{(0)}$. Supposing that ${\mathbf{U}^{(n)}}^3=\mathbf{I}^{(n)}$ for an $n\in\mathbf{N}_0$,

$$\begin{aligned}{\mathbf{U}^{(n+1)}}^2&=\begin{pmatrix}\mathbf{0}^{(n)} & \mathbf{U}^{(n)}\\ \mathbf{U}^{(n)} & \mathbf{U}^{(n)}\end{pmatrix}\begin{pmatrix}\mathbf{0}^{(n)} & \mathbf{U}^{(n)}\\ \mathbf{U}^{(n)} & \mathbf{U}^{(n)}\end{pmatrix}\\ &=\begin{pmatrix}{\mathbf{U}^{(n)}}^2 & {\mathbf{U}^{(n)}}^2\\ {\mathbf{U}^{(n)}}^2 & \mathbf{0}^{(n)}\end{pmatrix}\end{aligned} \tag{14}$$

and

$$\begin{aligned}{\mathbf{U}^{(n+1)}}^3&=\begin{pmatrix}{\mathbf{U}^{(n)}}^2 & {\mathbf{U}^{(n)}}^2\\ {\mathbf{U}^{(n)}}^2 & \mathbf{0}^{(n)}\end{pmatrix}\begin{pmatrix}\mathbf{0}^{(n)} & \mathbf{U}^{(n)}\\ \mathbf{U}^{(n)} & \mathbf{U}^{(n)}\end{pmatrix}\\ &=\begin{pmatrix}{\mathbf{U}^{(n)}}^3 & \mathbf{0}^{(n)}\\ \mathbf{0}^{(n)} & {\mathbf{U}^{(n)}}^3\end{pmatrix}\\ &=\begin{pmatrix}\mathbf{I}^{(n)} & \mathbf{0}^{(n)}\\ \mathbf{0}^{(n)} & \mathbf{I}^{(n)}\end{pmatrix}=\mathbf{I}^{(n+1)}\end{aligned} \tag{15}$$

so for any non-negative integer n, ${\mathbf{U}^{(n)}}^3=\mathbf{I}^{(n)}$. (13) and (14) show that neither $\mathbf{U}^{(n+1)}$ nor ${\mathbf{U}^{(n+1)}}^2$ is equal to $\mathbf{I}^{(n+1)}$, so the order of $\mathbf{U}^{(n+1)}$ is equal to 3. Finally it is obvious that the order of (1) is equal to 1. □

Now, we determine the invariant factors of $\mathbf{U}^{(n)}$.

Theorem 3.

$$\mathbf{U}^{(n)}+\lambda\mathbf{I}^{(n)}\sim\begin{pmatrix}\mathbf{I}^{(r_n\times r_n)} & \mathbf{0}^{(r_n\times 1)} & \mathbf{0}^{(r_n\times s_n)}\\ \mathbf{0}^{(1\times r_n)} & 1+\lambda+\varepsilon_n\lambda^2 & \mathbf{0}^{(1\times s_n)}\\ \mathbf{0}^{(s_n\times r_n)} & \mathbf{0}^{(s_n\times 1)} & \left(1+\lambda^3\right)\mathbf{I}^{(s_n\times s_n)}\end{pmatrix},\tag{16}$$

where $\varepsilon_n=n \bmod 2$, $s_n=\left\lfloor\frac{2^n}{3}\right\rfloor$ *and* $r_n=2^n-1-s_n$.

Proof. If $n=0$ then $\varepsilon_0=s_0=r_0=0$ and $\mathbf{U}^{(0)}=\mathbf{I}^{(0)}$, so

$$\mathbf{U}^{(0)}+\lambda\mathbf{I}^{(0)}=(1+\lambda)\,.\tag{17}$$

In the case of $n=1$, $\varepsilon_1=1=r_1$, $s_1=0$ and

$$\begin{aligned}\mathbf{U}^{(1)}+\lambda\mathbf{I}^{(1)}&=\begin{pmatrix}\lambda & 1\\ 1 & 1+\lambda\end{pmatrix}\\ &\sim\begin{pmatrix}1 & 0\\ 0 & 1+\lambda+\lambda^2\end{pmatrix}\end{aligned}\tag{18}$$

and the two cases together give the following result for $n=0$ and $n=1$:

$$\mathbf{U}^{(n)}+\lambda\mathbf{I}^{(n)}=\begin{pmatrix}\mathbf{I}^{(r_n\times r_n)} & \mathbf{0}^{(r_n\times 1)} & \mathbf{0}^{(r_n\times s_n)}\\ \mathbf{0}^{(1\times r_n)} & 1+\lambda+\varepsilon_n\lambda^2 & \mathbf{0}^{(1\times s_n)}\\ \mathbf{0}^{(s_n\times r_n)} & \mathbf{0}^{(s_n\times 1)} & \left(1+\lambda^3\right)\mathbf{I}^{(s_n\times s_n)}\end{pmatrix}.\tag{19}$$

Now, let $n\in\mathbf{N}_0$. Then

$$\begin{aligned}\mathbf{U}^{(n+2)}+\lambda\mathbf{I}^{(n+2)}&=\begin{pmatrix}\lambda\mathbf{I}^{(n+1)} & \mathbf{U}^{(n+1)}\\ \mathbf{U}^{(n+1)} & \mathbf{U}^{(n+1)}+\lambda\mathbf{I}^{(n+1)}\end{pmatrix}\\ &\sim\begin{pmatrix}\mathbf{U}^{(n+1)} & \mathbf{U}^{(n+1)}+\lambda\mathbf{I}^{(n+1)}\\ \mathbf{0}^{(n+1)} & \mathbf{U}^{(n+1)}+\lambda\mathbf{I}^{(n+1)}+\lambda^2\mathbf{U}^{(n+1)^2}\end{pmatrix}\\ &\sim\begin{pmatrix}\mathbf{I}^{(n+1)} & \mathbf{0}^{(n+1)}\\ \mathbf{0}^{(n+1)} & \mathbf{U}^{(n+1)^2}+\lambda\mathbf{U}^{(n+1)}+\lambda^2\mathbf{I}^{(n+1)}\end{pmatrix}\end{aligned}\tag{20}$$

where in the second step we multiplied by $\begin{pmatrix}\mathbf{U}^{(n+1)^2} & \mathbf{U}^{(n+1)}+\lambda\mathbf{I}^{(n+1)}\\ \mathbf{0}^{(n+1)} & \mathbf{U}^{(n+1)}\end{pmatrix}$ from the right. Furthermore

$$\begin{aligned}\mathbf{U}^{(n+1)^2}+\lambda\mathbf{U}^{(n+1)}+\lambda^2\mathbf{I}^{(n+1)}&=\begin{pmatrix}\mathbf{U}^{(n)^2}+\lambda^2\mathbf{I}^{(n)} & \mathbf{U}^{(n)^2}+\lambda\mathbf{U}^{(n)}\\ \mathbf{U}^{(n)^2}+\lambda\mathbf{U}^{(n)} & \lambda\mathbf{U}^{(n)}+\lambda^2\mathbf{I}^{(n)}\end{pmatrix}\\ &\sim\begin{pmatrix}\mathbf{U}^{(n)}+\lambda\mathbf{I}^{(n)} & \lambda\mathbf{I}^{(n)}+\lambda^2\mathbf{U}^{(n)^2}\\ \mathbf{U}^{(n)^2}+\lambda^2\mathbf{I}^{(n)} & \mathbf{U}^{(n)^2}+\lambda\mathbf{U}^{(n)}\end{pmatrix}\\ &\sim\begin{pmatrix}\mathbf{U}^{(n)}+\lambda\mathbf{I}^{(n)} & \lambda\mathbf{I}^{(n)}+\lambda^2\mathbf{U}^{(n)^2}\\ \mathbf{0}^{(n)} & \mathbf{U}^{(n)^2}+\lambda^3\mathbf{U}^{(n)^2}\end{pmatrix}\\ &\sim\begin{pmatrix}\mathbf{U}^{(n)}+\lambda\mathbf{I}^{(n)} & \mathbf{0}^{(n)}\\ \mathbf{0}^{(n)} & \left(1+\lambda^3\right)\mathbf{I}^{(n)}\end{pmatrix}.\end{aligned}\tag{21}$$

Putting this result into the matrix we got previously in (20)

$$\begin{aligned}\mathbf{U}^{(n+2)} + \lambda \mathbf{I}^{(n+2)} &\sim \begin{pmatrix} \mathbf{I}^{(n+1)} & \mathbf{0}^{(n+1)} \\ \mathbf{0}^{(n+1)} & \mathbf{U}^{(n+1)^2} + \lambda \mathbf{U}^{(n+1)} + \lambda^2 \mathbf{I}^{(n+1)} \end{pmatrix} \\ &\sim \begin{pmatrix} \mathbf{I}^{(n+1)} & \mathbf{0}^{(2^{n+1}\times 2^n)} & \mathbf{0}^{(2^{n+1}\times 2^n)} \\ \mathbf{0}^{(2^n\times 2^{n+1})} & \mathbf{U}^{(n)} + \lambda \mathbf{I}^{(n)} & \mathbf{0}^{(n)} \\ \mathbf{0}^{(2^n\times 2^{n+1})} & \mathbf{0}^{(n)} & \left(1+\lambda^3\right) \mathbf{I}^{(n)} \end{pmatrix}.\end{aligned} \tag{22}$$

Let's suppose that

$$\mathbf{U}^{(n)} + \lambda \mathbf{I}^{(n)} \sim \begin{pmatrix} \mathbf{I}^{(r_n\times r_n)} & \mathbf{0}^{(r_n\times 1)} & \mathbf{0}^{(r_n\times s_n)} \\ \mathbf{0}^{(1\times r_n)} & 1+\lambda+\varepsilon_n\lambda^2 & \mathbf{0}^{(1\times s_n)} \\ \mathbf{0}^{(s_n\times r_n)} & \mathbf{0}^{(s_n\times 1)} & \left(1+\lambda^3\right) \mathbf{I}^{(s_n\times s_n)} \end{pmatrix} \tag{23}$$

and let's take into consideration that

$$2^n + s_n = 2^n + \left\lfloor \frac{2^n}{3} \right\rfloor = \left\lfloor \frac{2^{n+2}}{3} \right\rfloor = s_{n+2} \tag{24}$$

and

$$\begin{aligned} 2^{n+1} + r_n &= 2^{n+1} + 2^n - 1 - s_n \\ &= 2^{n+2} - 1 - \left(2^n + s_n\right) \\ &= 2^{n+2} - 1 - s_{n+2} = r_{n+2}. \end{aligned} \tag{25}$$

Then substituting $\mathbf{U}^{(n)} + \lambda \mathbf{I}^{(n)}$ in (22) by the right hand side of (23), after repartitioning the matrix we get that

$$\begin{aligned}&\mathbf{U}^{(n+2)} + \lambda \mathbf{I}^{(n+2)} \sim \\ &\sim \begin{pmatrix} \mathbf{I}^{(r_{n+2}\times r_{n+2})} & \mathbf{0}^{(r_{n+2}\times 1)} & \mathbf{0}^{(r_{n+2}\times s_{n+2})} \\ \mathbf{0}^{(1\times r_{n+2})} & 1+\lambda+\varepsilon_{n+2}\lambda^2 & \mathbf{0}^{(1\times s_{n+2})} \\ \mathbf{0}^{(s_{n+2}\times r_{n+2})} & \mathbf{0}^{(s_{n+2}\times 1)} & \left(1+\lambda^3\right) \mathbf{I}^{(s_{n+2}\times s_{n+2})} \end{pmatrix}.\end{aligned} \tag{26}$$

□

With these results we know the minimal and the characteristic polynomial of the transform belonging to $\mathbf{U}^{(n)}$, too, namely

Corollary 1. *Let $n \in \mathbf{N}_0$. The minimal polynomial of $\mathbf{U}^{(n)}$ is*

$$m^{(n)}(\lambda) = \begin{cases} \lambda + 1 & n = 0 \\ \lambda^2 + \lambda + 1 & n = 1 \\ \lambda^3 + 1 & n \geq 2 \end{cases} \tag{27}$$

and the characteristic polynomial of the transform given by $\mathbf{U}^{(n)}$ in the natural basis of the 2^n-dimensional Boolean space is

$$\begin{aligned} c^{(n)}(\lambda) &= \left(\lambda^3+1\right)^{s_n} (\lambda+1)^{1-\varepsilon_n} \left(\lambda^2+\lambda+1\right)^{\varepsilon_n} \\ &= (\lambda+1)^{s_n+(1-\varepsilon_n)} \left(\lambda^2+\lambda+1\right)^{s_n+\varepsilon_n}. \end{aligned} \tag{28}$$

Proof. The minimal polynomial of a transform is its last invariant factor and it is equal to that indicated in (17), (18) and (23), that is in (27). Similarly, the characteristic polynomial is the product of all of the invariant factors of the transform. In (23) we can see that λ^3+1 is an invariant factor with a multiplicity of s_n, additionally if n is an even integer then $\lambda+1$, and in the other case $\lambda^2+\lambda+1$ is a simple invariant factor, and there is no other invariant factor. As $\lambda^3+1=(\lambda+1)\left(\lambda^2+\lambda+1\right)$ and the second operand of the product is irreducible over $\mathbf{F}_2$, we get also the second form of the characteristic polynomial. □

Another consequence of Theorem 3 is the following corollary.

Corollary 2. *The eigenvalue of the transform is 1 and the multiplicity of this only eigenvalue is* $\mu_n=\frac{2^n+2(-1)^n}{3}$.

By Corollary 2 the subspace of the 2^n-dimensional Boolean space belonging to the only eigenvalue of the transform determined by the matrix $\mathbf{U}^{(n)}=\mathbf{A}^{(n)}\mathbf{P}^{(n)}$ in the natural basis of the space is $\frac{2^n+2(-1)^n}{3}$-dimensional.

Proof. As the multiplicity of $\lambda+1$ in $c^{(n)}(\lambda)$ is equal to $s_n+1-\varepsilon_n$, and $\lambda^2+\lambda+1$ is irreducible over $\mathbf{F}_2$, so the only eigenvalue of the transform is 1 with the multiplicity of $\mu_n=s_n+1-\varepsilon_n$ and

$$\begin{aligned}\mu_n=s_n+1-\varepsilon_n&=\left\lfloor\frac{2^n}{3}\right\rfloor+1-(n \bmod 2)\\&=\frac{2^n-2^{\varepsilon_n}}{3}+1-(n \bmod 2)\\&=\frac{2^n-1-(n \bmod 2)}{3}+1-(n \bmod 2)\\&=\frac{2^n+2-4\,(n \bmod 2)}{3}=\frac{2^n+2\,(-1)^n}{3}.\end{aligned}\tag{29}$$

□

Remark 1. Another way to gain μ_n is the recursion: $\mu_0=1$ and

$$\begin{aligned}\mu_{n+1}&=\frac{2^{n+1}+2\,(-1)^{n+1}}{3}=\frac{2\cdot 2^n-2\,(-1)^n}{3}\\&=2\frac{2^n+2\,(-1)^n}{3}-2\,(-1)^n=2\mu_n-2\,(-1)^n\,.\end{aligned}\tag{30}$$

We have to find a basis of this subspace.

Theorem 4. *Let* $\mathbf{U}^{(n)}+\mathbf{I}^{(n)}=\begin{pmatrix}\mathbf{Q}^{(n)} & \mathbf{R}^{(n)}\\ \mathbf{S}^{(n)} & \mathbf{T}^{(n)}\end{pmatrix}$ *where* $\mathbf{Q}^{(n)}$ *is a* $2^n-\mu_n$*-order and* $\mathbf{T}^{(n)}$ *is a* μ_n*-order quadratic matrix. Then* $\mathbf{Q}^{(n)}$ *is regular, and the subspace of the eigenvectors of the transform is*

$$\begin{pmatrix}{\mathbf{Q}^{(n)}}^{-1}\mathbf{R}^{(n)}\\ \mathbf{I}^{(\mu_n\times\mu_n)}\end{pmatrix}\underline{u}\tag{31}$$

where $\underline{u}$ is an arbitrary element of the μ_n-dimensional Boolean space.

Proof. If $\lambda = 1$ then $\mathbf{U}^{(n)} + \lambda\mathbf{I}^{(n)} = \mathbf{U}^{(n)} + \mathbf{I}^{(n)}$. $\mathbf{U}^{(0)} + \mathbf{I}^{(0)} = (0)$, so if $n = 0$, then every element of the Boolean space, that is all of the Boolean functions of 0 variables are conjunctively polynomial-like. We get the same result by our theorem, as now $\mu_0 = 1$ and so

$$\begin{pmatrix} \mathbf{Q}^{(0)^{-1}}\mathbf{R}^{(0)} \\ \mathbf{I}^{(\mu_0\times\mu_0)} \end{pmatrix} = \mathbf{I}^{(0)}. \tag{32}$$

If $n = 1$ then

$$\begin{aligned} \mathbf{U}^{(1)} + \mathbf{I}^{(1)} &= \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix} + \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix} \\ &\sim \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \sim \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}. \end{aligned} \tag{33}$$

This matrix is regular, so its nullspace contains only the nullvector, the transform has no eigenvector, the only conjunctively polynomial-like Boolean function of one variable is the zero function of 1 variable. It is equal to we get by the theorem: $\mu_1 = 2\mu_0 - 2\,(-1)^0 = 0$ and $2^1 - \mu_1 = 2$, so $\mathbf{U}^{(1)} = \mathbf{Q}^{(1)}$ and

$$\begin{pmatrix} \mathbf{Q}^{(1)^{-1}}\mathbf{R}^{(1)} \\ \mathbf{I}^{(\mu_1\times\mu_1)} \end{pmatrix} = () \tag{34}$$

where $()$ is a 2×0-matrix which spans the 0-dimensional subspace of the 2-dimensional Boolean space.

Now let $n \geq 0$. Then

$$\begin{aligned} \mathbf{U}^{(n+2)} + \mathbf{I}^{(n+2)} &= \begin{pmatrix} \mathbf{I}^{(n+1)} & \mathbf{U}^{(n+1)} \\ \mathbf{U}^{(n+1)} & \mathbf{U}^{(n+1)} + \mathbf{I}^{(n+1)} \end{pmatrix} \\ &\sim \begin{pmatrix} \mathbf{I}^{(n+1)} & \mathbf{U}^{(n+1)} \\ \mathbf{0}^{(n+1)} & \mathbf{U}^{(n+1)^2} + \mathbf{U}^{(n+1)} + \mathbf{I}^{(n+1)} \end{pmatrix} \end{aligned} \tag{35}$$

$$\begin{aligned} \mathbf{U}^{(n+1)^2} + \mathbf{U}^{(n+1)} + \mathbf{I}^{(n+1)} &= \begin{pmatrix} \mathbf{U}^{(n)^2} + \mathbf{I}^{(n)} & \mathbf{U}^{(n)^2} + \mathbf{U}^{(n)} \\ \mathbf{U}^{(n)^2} + \mathbf{U}^{(n)} & \mathbf{U}^{(n)} + \mathbf{I}^{(n)} \end{pmatrix} \\ &\sim \begin{pmatrix} \mathbf{U}^{(n)} + \mathbf{I}^{(n)} & \mathbf{U}^{(n)^2} + \mathbf{I}^{(n)} \\ \mathbf{0}^{(n)} & \mathbf{0}^{(n)} \end{pmatrix} \end{aligned} \tag{36}$$

and so

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

From here it is easy to see by induction that the left upper $(2^n - \mu_n)\times(2^n - \mu_n)$ submatrix of $\mathbf{U}^{(n)} + \mathbf{I}^{(n)}$ is regular (as we manipulated only the rows of the matrix, and we added a multiple of a row to another row always downwards), and this regular submatrix can't be extended regularly due to the rank of the matrix. If

$$\mathbf{U}^{(n)} + \mathbf{I}^{(n)} = \begin{pmatrix} \mathbf{Q}^{(n)} & \mathbf{R}^{(n)} \\ \mathbf{S}^{(n)} & \mathbf{T}^{(n)} \end{pmatrix} \tag{38}$$

where $\mathbf{Q}^{(n)}$ is the above mentioned regular submatrix, then $\left(\mathbf{U}^{(n)} + \mathbf{I}^{(n)}\right)\underline{u} = \underline{0}$ if and only if

$$\begin{aligned} \underline{0}^{(2^n)} &= \begin{pmatrix} \mathbf{Q}^{(n)^{-1}} & \mathbf{0}^{((2^n-\mu_n)\times\mu_n)} \\ \mathbf{S}^{(n)}\mathbf{Q}^{(n)^{-1}} & \mathbf{I}^{(\mu_n\times\mu_n)} \end{pmatrix} \left(\mathbf{U}^{(n)} + \mathbf{I}^{(n)}\right)\underline{u} \\ &= \begin{pmatrix} \mathbf{Q}^{(n)^{-1}} & \mathbf{0}^{((2^n-\mu_n)\times\mu_n)} \\ \mathbf{S}^{(n)}\mathbf{Q}^{(n)^{-1}} & \mathbf{I}^{(\mu_n\times\mu_n)} \end{pmatrix} \begin{pmatrix} \mathbf{Q}^{(n)} & \mathbf{R}^{(n)} \\ \mathbf{S}^{(n)} & \mathbf{T}^{(n)} \end{pmatrix} \begin{pmatrix} \underline{u}^{(0)} \\ \underline{u}^{(1)} \end{pmatrix} \\ &= \begin{pmatrix} \mathbf{I}^{((2^n-\mu_n)\times(2^n-\mu_n))} & \mathbf{Q}^{(n)^{-1}}\mathbf{R}^{(n)} \\ \mathbf{0}^{(\mu_n\times(2^n-\mu_n))} & \mathbf{0}^{(\mu_n\times\mu_n)} \end{pmatrix} \begin{pmatrix} \underline{u}^{(0)} \\ \underline{u}^{(1)} \end{pmatrix} \end{aligned} \tag{39}$$

that is if and only if

$$\begin{pmatrix} \mathbf{I}^{((2^n-\mu_n)\times(2^n-\mu_n))} & \mathbf{Q}^{(n)^{-1}}\mathbf{R}^{(n)} \end{pmatrix} \begin{pmatrix} \underline{u}^{(0)} \\ \underline{u}^{(1)} \end{pmatrix} = \underline{0}^{(2^n-\mu_n)}. \tag{40}$$

From this equation we get that

$$\begin{pmatrix} \underline{u}^{(0)} \\ \underline{u}^{(1)} \end{pmatrix} = \begin{pmatrix} \mathbf{Q}^{(n)^{-1}}\mathbf{R}^{(n)} \\ \mathbf{I}^{(\mu_n\times\mu_n)} \end{pmatrix} \underline{u}^{(1)} \tag{41}$$

is the solution of the equation

$$\begin{pmatrix} \mathbf{Q}^{(n)} & \mathbf{R}^{(n)} \\ \mathbf{S}^{(n)} & \mathbf{T}^{(n)} \end{pmatrix} \begin{pmatrix} \underline{u}^{(0)} \\ \underline{u}^{(1)} \end{pmatrix} = \begin{pmatrix} \underline{0}^{(2^n-\mu_n)} \\ \underline{0}^{(\mu_n)} \end{pmatrix} \tag{42}$$

with an arbitrary $\underline{u}^{(1)}$ vector of the μ_n-dimensional Boolean space. □

Finally, we define the class of the Boolean functions having the properties we dealt with in this article.

Definition 1. Let f be a Boolean function of n variables, and let $\underline{\beta}$ and $\underline{k}$ be the spectra of the modified conjunctive normal form and the Zhegalkin polynomial of f, respectively. Then f is a conjunctively polynomial-like Boolean function, if $\underline{\beta} = \underline{k}$.

Example 1. Let $n = 2$.

$$\begin{aligned} \mathbf{U}^{(2)} + \mathbf{I}^{(2)} &= \begin{pmatrix} 1 & 0 & 0 & 1 \\ 0 & 1 & 1 & 1 \\ 0 & 1 & 1 & 1 \\ 1 & 1 & 1 & 0 \end{pmatrix} \sim \begin{pmatrix} 1 & 0 & 0 & 1 \\ 0 & 1 & 1 & 1 \\ 0 & 1 & 1 & 1 \\ 0 & 1 & 1 & 1 \end{pmatrix} \\ &\sim \begin{pmatrix} 1 & 0 & 0 & 1 \\ 0 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix} = \begin{pmatrix} \mathbf{I}^{(1)} & \mathbf{Q}^{(2)^{-1}}\mathbf{R}^{(2)} \\ \mathbf{0}^{(1)} & \mathbf{0}^{(1)} \end{pmatrix}. \end{aligned} \tag{43}$$

Then

$$\begin{pmatrix} \mathbf{Q}^{(2)^{-1}}\mathbf{R}^{(2)} \\ \mathbf{I}^{(2\times 2)} \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 1 & 1 \\ 1 & 0 \\ 0 & 1 \end{pmatrix} \tag{44}$$

and the two-variable conjunctively polynomial-like Boolean functions are as follows:

(45)

	$f_0^{(2)}$	$f_6^{(2)}$	$f_{13}^{(2)}$	$f_{11}^{(2)}$
$M_0^{(2)\prime}$	0	0	1	1
$M_1^{(2)\prime}$	0	1	1	0
$M_2^{(2)\prime}$	0	1	0	1
$M_3^{(2)\prime}$	0	0	1	1

Really,

$$\begin{aligned} &\left(0+M_0^{(2)\prime}\right)\left(0+M_1^{(2)\prime}\right)\left(0+M_2^{(2)\prime}\right)\left(0+M_3^{(2)\prime}\right) \\ &= M_0^{(2)\prime}M_1^{(2)\prime}M_2^{(2)\prime}M_3^{(2)\prime} \\ &= \left(\overline{x}_1+\overline{x}_0\right)\left(\overline{x}_1+x_0\right)\left(x_1+\overline{x}_0\right)\left(x_1+x_0\right) \\ &= 0 = 0\cdot S_0 + 0\cdot S_1 + 0\cdot S_2 + 0\cdot S_3 \end{aligned} \tag{46}$$

$$\begin{aligned} &\left(0+M_0^{(2)\prime}\right)\left(1+M_1^{(2)\prime}\right)\left(1+M_2^{(2)\prime}\right)\left(0+M_3^{(2)\prime}\right) \\ &= M_0^{(2)\prime}M_3^{(2)\prime} = \left(\overline{x}_1+\overline{x}_0\right)\left(x_1+x_0\right) \\ &= \overline{x}_1x_0 + x_1\overline{x}_0 = x_1 \oplus x_0 \\ &= 0\cdot S_0 + 1\cdot S_1 + 1\cdot S_2 + 0\cdot S_3 \end{aligned} \tag{47}$$

$$\begin{aligned} &\left(1+M_0^{(2)\prime}\right)\left(1+M_1^{(2)\prime}\right)\left(0+M_2^{(2)\prime}\right)\left(1+M_3^{(2)\prime}\right) \\ &= M_2^{(2)\prime} = \left(x_1+\overline{x}_0\right) \\ &= 1\oplus x_0 \oplus x_1x_0 \\ &= 1\cdot S_0 + 1\cdot S_1 + 0\cdot S_2 + 1\cdot S_3 \end{aligned} \tag{48}$$

and finally

$$\begin{aligned} &\left(1+M_0^{(2)\prime}\right)\left(0+M_1^{(2)\prime}\right)\left(1+M_2^{(2)\prime}\right)\left(1+M_3^{(2)\prime}\right) \\ &= M_1^{(2)\prime} = \left(\overline{x}_1+x_0\right) \\ &= 1\oplus x_1 \oplus x_1x_0 \\ &= 1\cdot S_0 + 0\cdot S_1 + 1\cdot S_2 + 1\cdot S_3. \end{aligned} \tag{49}$$

Example 2. Let $n = 3$. Now,

$$\mathbf{A}^{(3)} = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 \\ 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \end{pmatrix} \tag{50}$$

$$\mathbf{U}^{(3)} + \mathbf{I}^{(3)} = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 & 0 & 0 & 1 \\ 0 & 0 & 1 & 1 & 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 1 & 0 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 & 1 & 1 & 1 & 0 \end{pmatrix} \tag{51}$$

and $\mu_3 = 2\mu_2 - 2\left(-1\right)^2 = 2$, $2^3 - \mu_3 = 6$, so

$$\mathbf{Q}^{(3)} = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 1 & 0 & 1 \end{pmatrix} \tag{52}$$

and

$$\mathbf{R}^{(3)} = \begin{pmatrix} 0 & 1 \\ 1 & 1 \\ 0 & 1 \\ 1 & 1 \\ 0 & 1 \\ 1 & 1 \end{pmatrix}. \tag{53}$$

Then,

$$\mathbf{Q}^{(3)^{-1}} = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 & 0 \end{pmatrix} \tag{54}$$

and

$$\begin{pmatrix} \mathbf{Q}^{(3)^{-1}}\mathbf{R}^{(3)} \\ \mathbf{I}^{(2\times 2)} \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 1 & 1 \\ 1 & 1 \\ 1 & 0 \\ 1 & 1 \\ 1 & 0 \\ 1 & 0 \\ 0 & 1 \end{pmatrix}. \tag{55}$$

Really,

$$\begin{aligned} \mathbf{U}^{(3)} \begin{pmatrix} \mathbf{Q}^{(3)^{-1}}\mathbf{R}^{(3)} \\ \mathbf{I}^{(1)} \end{pmatrix} &= \begin{pmatrix} 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 \\ 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & 1 \\ 1 & 1 \\ 1 & 0 \\ 1 & 1 \\ 1 & 0 \\ 1 & 0 \\ 0 & 1 \end{pmatrix} \\ &= \begin{pmatrix} 0 & 1 \\ 1 & 1 \\ 1 & 1 \\ 1 & 0 \\ 1 & 1 \\ 1 & 0 \\ 1 & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} \mathbf{Q}^{(3)^{-1}}\mathbf{R}^{(3)} \\ \mathbf{I}^{(1)} \end{pmatrix} \end{aligned} \tag{56}$$

that shows that the columns of

$$\begin{pmatrix} \mathbf{Q}^{(3)^{-1}}\mathbf{R}^{(3)} \\ \mathbf{I}^{(2\times 2)} \end{pmatrix}$$

are eigenvectors of the transform. From here we get the four conjunctively polynomial-like Boolean functions of three variables as the four linear combinations of the two columns of the matrix of the right hand side of the equation

(55). Namely,

(57)

	$f_0^{(3)}$	$f_{126}^{(3)}$	$f_{233}^{(3)}$	$f_{151}^{(3)}$
$M_0^{(3)\prime}$	0	0	1	1
$M_1^{(3)\prime}$	0	1	1	0
$M_2^{(3)\prime}$	0	1	1	0
$M_3^{(3)\prime}$	0	1	0	1
$M_4^{(3)\prime}$	0	1	1	0
$M_5^{(3)\prime}$	0	1	0	1
$M_6^{(3)\prime}$	0	1	0	1
$M_7^{(3)\prime}$	0	0	1	1

3. Conclusion

In the article above we dealt with a special transform of the Boolean functions given between the spectrum of the Zhegalkin polynomial of a Boolean function and the vector containing the elements of the spectrum of the canonical disjunctive normal form of the same function in reversed order. It was stated that the order of the transform is equal to three (with the exception of the case of $n = 0$). The set of the functions of n variables invariant with respect to this transform is a linear subspace of the linear space of all of the n-variable Boolean functions and the dimension of this subspace is equal to $\mu_n = \frac{2^n+2(-1)^n}{3}$. In the article we gave a basis of this subspace, too. If $\mathbf{U}^{(n)}$ denotes the matrix of the transform then the rank of $\mathbf{U}^{(n)} + \mathbf{I}^{(n)}$ is equal to $2^n - \mu_n$ 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 regular quadratic matrix. Then the columns of $\begin{pmatrix} {\mathbf{Q}^{(n)}}^{-1}\mathbf{R}^{(n)} \\ \mathbf{I}^{(\mu_n \times \mu_n)} \end{pmatrix}$ make up a basis of the transform.

References

[1] S. H. Akers. On the theoiry of Boolean functions. *J. SIAM.*, 7:487–498, 1959.

[2] R. Beigel. The polynomila method in circuit complexity. In *36th Annual Symposium on Foundations of Computer Science, IEEE Conference Proceedings*, pages 82–95, 1995.

[3] P. Calingaert. Switching functions: canonical forms based on commutative and associative binary operations. *Trans. AIEE*, 1961.

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

[8] E. L. Post. Introduction to a General Theory of Elementary Propositions. *Amer. J. Math.*, 43(3):163–185, 1921.

[9] E. L. Post. *The Two-Valued Iterative Systems of Mathematical Logic*. Annals of Mathematics Studies, no. 5. Princeton University Press, Princeton, N. J., 1941.

Received July 28, 2005; 31 January, 2007 in revised form.

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