ON THE VARIABLES OF THE CONJUNCTIVELY POLYNOMIAL-LIKE BOOLEAN FUNCTIONS

János Gonda (Budapest, Hungary)

Dedicated to the memory of Professor Antal Iványi

Communicated by Imre Kátai
(Received May 29, 2017; accepted July 29, 2017)

Abstract. Conjunctively polynomial-like Boolean functions form a class of the Boolean functions invariant with respect to a special transform of the linear space of the two-valued logical functions. In this article we prove that every variable of such functions – with the exception of the zero function of at least one variable – is essential.

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 $\vee$, $\wedge$, $\oplus$ 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 set of non-negative integers, and $\mathbf{N}^{+}$ denotes the set of 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.

Key words and phrases: Boolean function, conjunctive normal form, Zhegalkin polynomial, conjunctively polynomial-like Boolean function.
2010 Mathematics Subject Classification: 06E30, 94C10, 15A18.
https://doi.org/10.71352/ac.46.055

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 these 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 under some linear transforms. These functions are called polynomial-like and conjunctively polynomial-like.

1.1. Representations of a Boolean functions

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 each 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 $0 \leq j < n$ and the variable indexed by j is denoted by x_j, these products can be numbered by the numbers $0 \leq i < 2^n$ 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 corresponding with it is

$$m_i^{(n)} = \bigwedge_{j=0}^{2^n-1} x_j^{\left(a_j^{(i)}\right)}, \tag{1.1}$$

where $x^{(0)} = \overline{x} = \overline{0} \oplus x$ and $x^{(1)} = x = \overline{1} \oplus x$. 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 $0 \leq j < 2^n$) 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 $\alpha_i^{(l)} \in \{0,1\}$

$$f_l^{(n)} = \overset{2^n-1}{\underset{i=0}{\vee}} \left(\alpha_i^{(l)} \wedge m_i^{(n)}\right). \tag{1.2}$$

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

Another possibility for giving a Boolean function is the so-called Zhegalkin-polynomial. Let $S_i^{(n)} = \wedge_{j=0}^{n-1} x_j^{a_j^{(i)}}$, where $x^0 = 1 = \overline{0} \vee x$, $x^1 = x = \overline{1} \vee x$ and $i = \sum_{j=0}^{n-1} a_j^{(i)} 2^j$ 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

$$f^{(n)} = \overset{2^n-1}{\underset{i=0}{\oplus}} \left(k_i \wedge S_i^{(n)}\right). \tag{1.3}$$

But this polynomial can be considered as a polynomial over the field of two elements, and in this case we write the polynomial in the following form:

$$f^{(n)} = \sum_{i=0}^{2^n-1} k_i S_i^{(n)}. \tag{1.4}$$

where now $S_i^{(n)} = \prod_{j=0}^{n-1} x_j^{a_j^{(i)}}$, and the sum, the product and the exponentiation are the operations of the field.

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

$$\mathbf{A}^{(n)} = \begin{cases} (1) & \text{if } n = 0 \\ \begin{pmatrix} \mathbf{A}^{(n-1)} & \mathbf{0}^{(n-1)} \\ \mathbf{A}^{(n-1)} & \mathbf{A}^{(n-1)} \end{pmatrix} & \text{if } n \in \mathbf{N}^+ \end{cases} \tag{1.5}$$

(this form of the matrix shows that for every $n \in \mathbf{N}$, $\mathbf{A}^{(n)}$ is the n-th power of the two-order $\begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}$ regular quadratic matrix, if the operation is the Kronecker-product).

From the previous results immediately follows that

$$\begin{aligned} \left(\mathbf{A}^{(n+1)}\right)^2 &= \begin{pmatrix} \mathbf{A}^{(n)} & \mathbf{0}^{(n)} \\ \mathbf{A}^{(n)} & \mathbf{A}^{(n)} \end{pmatrix} \begin{pmatrix} \mathbf{A}^{(n)} & \mathbf{0}^{(n)} \\ \mathbf{A}^{(n)} & \mathbf{A}^{(n)} \end{pmatrix} = \\ &= \begin{pmatrix} \left(\mathbf{A}^{(n)}\right)^2 & \mathbf{0}^{(n)} \\ \mathbf{0}^{(n)} & \left(\mathbf{A}^{(n)}\right)^2 \end{pmatrix} \end{aligned} \tag{1.6}$$

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

$$\left(\mathbf{A}^{(n+1)}\right)^2 = \mathbf{I}^{(n+1)} \tag{1.7}$$

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

$$M_i^{(n)} = \bigvee_{j=0}^{2^n-1} x_j^{\left(\overline{a_j^{(i)}}\right)} = \bigvee_{j=0}^{2^n-1} \left(a_j^{(i)} \oplus x_j\right) \tag{1.8}$$

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

$$f^{(n)} = \bigwedge_{i=0}^{2^n-1} \left(\alpha_i \vee M_i^{(n)}\right) \tag{1.9}$$

where $\alpha_i = f^{(n)}\left(a_0^{(i)}, \ldots, a_{n-1}^{(i)}\right)$. From this last property follows that $f^{(n)} = = \wedge_{i=0}^{2^n-1}\left(\alpha_i \vee M_i^{(n)}\right) = f_l^{(n)}$ where $l = \sum_{i=0}^{2^n-1} \alpha_i 2^i$.

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

$$M_i^{(n)\prime} = \bigvee_{i=0}^{2^n-1} x_j^{\left(a_j^{(i)}\right)} = \bigvee_{i=0}^{2^n-1} \left(\overline{a_j^{(i)}} \oplus x_j\right). \tag{1.10}$$

It is easy to see that $M_i^{(n)} = M_{2^n-1-i}^{(n)\prime}$. Now if $f^{(n)} = \wedge_{i=0}^{2^n-1}\left(\beta_i \vee M_i^{(n)\prime}\right) = = f_k^{(n)}$ 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 $M_i^{(n)\prime} = \vee_{j=0}^{n-1}\left(a_j^{(i)}\oplus\overline{x}_j\right)$. If $g^{(n)} = \prod_{i=0}^{2^n-1}\left(\beta_i + M_i^{(n)}\right)$, then

$$
\begin{aligned}
f^{(n)}\left(x_0,\ldots,x_{n-1}\right) &= \bigwedge_{i=0}^{2^n-1}\left(\alpha_i \vee \bigvee_{j=0}^{n-1}\left(a_j^{(i)}\oplus x_j\right)\right) = \\
&= \bigwedge_{i=0}^{2^n-1}\left(\alpha_i \vee M_i^{(n)}\right) = \bigwedge_{i=0}^{2^n-1}\left(\beta_i \vee M_i^{(n)\prime}\right) = \\
&= \bigwedge_{i=0}^{2^n-1}\left(\beta_i \vee \bigvee_{j=0}^{n-1}\left(a_j^{(i)}\oplus \overline{x}_j\right)\right) = \qquad (1.11)\\
&= g^{(n)}\left(\overline{x}_0,\ldots,\overline{x}_{n-1}\right) = \overline{\overline{g^{(n)}}}\left(\overline{x}_0,\ldots,\overline{x}_{n-1}\right) = \\
&= \overline{g^{(n)D}}\left(x_0,\ldots,x_{n-1}\right)
\end{aligned}
$$

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 (1.11).

1.2. Polynomial-like and conjunctively polynomial-like Boolean functions

Let us 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

$$
\begin{pmatrix} \underline{u}_0 \\ \underline{u}_1 \end{pmatrix} = \begin{pmatrix} \mathbf{A}^{(n)} & \mathbf{0}^{(n)} \\ \mathbf{A}^{(n)} & \mathbf{A}^{(n)} \end{pmatrix}\begin{pmatrix} \underline{u}_0 \\ \underline{u}_1 \end{pmatrix} \qquad (1.12)
$$

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:

$$\left(\begin{array}{c} \mathbf{A}^{(n)}+\mathbf{I}^{(n)} \\ \mathbf{I}^{(n)} \end{array}\right). \tag{1.13}$$

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 (1.5), we get that

$$\mathbf{U}^{(n)}=\begin{cases} (1) & \text{if } n=0 \\ \left(\begin{array}{cc} \mathbf{0}^{(n-1)} & \mathbf{U}^{(n-1)} \\ \mathbf{U}^{(n-1)} & \mathbf{U}^{(n-1)} \end{array}\right) & \text{if } n\in\mathbf{N}^+. \end{cases} \tag{1.14}$$

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

$$\underline{\beta}=\left(\begin{array}{c} \mathbf{Q}^{(n)^{-1}}\mathbf{R}^{(n)} \\ \mathbf{I}^{(\mu_n\times\mu_n)} \end{array}\right)\underline{u}. \tag{1.15}$$

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

$$\mathbf{U}^{(n)}+\mathbf{I}^{(n)}=\left(\begin{array}{cc} \mathbf{Q}^{(n)} & \mathbf{R}^{(n)} \\ \mathbf{S}^{(n)} & \mathbf{T}^{(n)} \end{array}\right), \tag{1.16}$$

$\mathbf{Q}^{(n)}$ 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.

2. New results

In the previous section a linear transform was given which makes a correspondence between the coefficient-systems of the canonical disjunctive normal form and the Zhegalkin polynomial of a given n-variable Boolean function, that is, between of the spectra belonging to the before mentioned two forms of the function. At the same time, a Boolean function of n variables can be considered as a function over the field of two elements, such a function that maps the n-th power of the field containing two elements into the same field, so $f : \mathbb{F}_2^n \to \mathbb{F}_2$.

In a more general way, let $P_q^{(n;k)}$ be the set of the polynomials in n indeterminates with degrees less than k in every indeterminate over the field of q elements, formally let $P_q^{(n;k)} = \{p \in \mathbb{F}_q\left[x_0, , x_{n-1}\right] | \forall (n > i \in \mathbb{N}) : deg_i\left(p\right) < k\}$, and let $F_q^{(n)} = \{f : \mathbb{F}_q^n \to \mathbb{F}_q\}$. If f is an n-variable function mapping the field of q elements into itself, then there exists one and only one polynomial p in $P_q^{(n;q)}$ that $f\left(u_0, \ldots, u_{n-1}\right) = \hat{p}\left(u_0, \ldots, u_{n-1}\right)$ for every $\mathbf{u} = u_0 \ldots u_{n-1} \in \mathbb{F}_q^n$, where $\hat{p}$ denotes the polynomial function belonging to p. It is easy to give this polynomial:

$$p = \sum_{v_0 \ldots v_{n-1} \in \mathbb{F}_q^n} f\left(v_0, \ldots, v_{n-1}\right) \prod_{j=0}^{n-1} \left(e - \left(x_j - v_j\right)^{q-1}\right) \tag{2.1}$$

(e denotes the unity of the field). The cardinalities of the two sets, $P_q^{(n;q)}$ and $F_q^{(n)}$ are the same, namely q^{q^n}, and if $p \in P_q^{(n;q)}$, then the polynomial corresponding to $\hat{p} \in F_q^{(n)}$ is obviously p. It means that the given mapping of $F_q^{(n)}$ into $P_q^{(n;q)}$ is surjective, consequently injective, too, hence the given correspondence is bijective.

In the case when the field is $\mathbb{F}_2$, then $q - 1 = 1$, $a - b = a + b$ and $e + a = \overline{a}$, so then

$$p = \sum_{v_0 \ldots v_{n-1} \in \mathbb{F}_2^n} f\left(v_0, \ldots, v_{n-1}\right) \prod_{j=0}^{n-1} \left(\overline{v}_j + x_j\right). \tag{2.2}$$

Now $\overline{v}$ is the opposite of v, and $\overline{v}=1-v=1+v$ (the identity of the field of two elements is denoted by 1).

Let $n\in\mathbb{N}$, f a Boolean function of n variables, $\phi(f)$ the Zhegalkin-polynomial of f, $f_{\leftarrow}=\overline{f^*}$ ($\overline{f}$ is the complement of the function and f^* is the dual of f, that is $f^*(x_0,\dots,x_{n-1})=\overline{f}(\overline{x}_0,\dots,\overline{x}_{n-1})$), π is a permutation of the set $\mathbb{N}_n=\{k\in\mathbb{N}|k<n\}$, and $f^{(\pi)}(x_0,\dots,x_{n-1})=f\left(x_{\pi(0)},\dots,x_{\pi(n-1)}\right)$. As $f_{\leftarrow}$ is the complement of the dual of f, so $f_{\leftarrow}(x_0,\dots,x_{n-1})=$ $=f(\overline{x}_0,\dots,\overline{x}_{n-1})$, and it can be seen that $(f_{\leftarrow})_{\leftarrow}=f$. Furthermore $\left(f^{(\pi)}\right)^{\left(\pi^{-1}\right)}=f$ is true, too. First of all, we will prove that the two operations, $f\to f_{\leftarrow}$ and $f\to f^{(\pi)}$, are interchangeable.

Theorem 2.1. *Let $n\in\mathbb{N}$, f a Boolean function of n variables, $f_{\leftarrow}=\overline{f^*}$, π is a permutation of $\mathbb{N}_n$, and let $f^{(\pi)}(x_0,\dots,x_{n-1})=f\left(x_{\pi(0)},\dots,x_{\pi(n-1)}\right)$. Then $(f_{\leftarrow})^{(\pi)}=\left(f^{(\pi)}\right)_{\leftarrow}$.*

Proof. Let $\overline{x}$ be denoted by y. Then

$$\begin{aligned}(f_{\leftarrow})^{(\pi)}&=(f(\overline{x}_0,\dots,\overline{x}_{n-1}))^{(\pi)}=(f(y_0,\dots,y_{n-1}))^{(\pi)}=\\&=f\left(y_{\pi(0)},\dots,y_{\pi(n-1)}\right)=f\left(\overline{x}_{\pi(0)},\dots,\overline{x}_{\pi(n-1)}\right)=\\&=\left(f\left(x_{\pi(0)},\dots,x_{\pi(n-1)}\right)\right)_{\leftarrow}=\left(f^{(\pi)}\right)_{\leftarrow}.\end{aligned}\tag{2.3}$$ ■

From the above result follows that the composed operation can be denoted simply by $f_{\leftarrow}^{(\pi)}$, and $\left(f_{\leftarrow}^{(\pi)}\right)_{\leftarrow}^{\left(\pi^{-1}\right)}=f$. This result can be achieved easily, as

$$\begin{aligned}\left(f_{\leftarrow}^{(\pi)}\right)_{\leftarrow}^{\left(\pi^{-1}\right)}&=\left(\left((f_{\leftarrow})^{(\pi)}\right)_{\leftarrow}\right)^{\left(\pi^{-1}\right)}=\\&=\left(\left((f_{\leftarrow})^{(\pi)}\right)^{\left(\pi^{-1}\right)}\right)_{\leftarrow}=(f_{\leftarrow})_{\leftarrow}=f.\end{aligned}\tag{2.4}$$

Let us determine the polynomial $\phi\left(f_{\leftarrow}^{(\pi)}\right)$ belonging to $f_{\leftarrow}^{(\pi)}$.

Theorem 2.2. *Permuting the order of the variables of a Boolean function, the indeterminates of its Zhegalkin polynomial are rearranged in the same way.*

Formally the statement of the theorem is $\phi\left(f_{\leftarrow}^{(\pi)}\right)=(\phi(f_{\leftarrow}))^{(\pi)}$.

Proof. We apply the earlier mentioned connection that

$$p=\sum_{v_0\dots v_{n-1}\in\mathbb{F}_2^n}f(v_0,\dots,v_{n-1})\prod_{j=0}^{n-1}(\overline{v}_j+x_j).$$

$$\begin{aligned}
\phi\left(f_{\leftarrow}^{(\pi)}\right) &= \sum_{v_0 \ldots v_{n-1} \in \mathbb{F}_2^n} f_{\leftarrow}^{(\pi)}\left(v_0, \ldots, v_{n-1}\right) \prod_{j=0}^{n-1}\left(\overline{v}_j + x_j\right) = \\
&= \sum_{v_0 \ldots v_{n-1} \in \mathbb{F}_2^n} f^{(\pi)}\left(\overline{v}_0, \ldots, \overline{v}_{n-1}\right) \prod_{j=0}^{n-1}\left(\overline{v}_j + x_j\right) = \\
&= \sum_{v_0 \ldots v_{n-1} \in \mathbb{F}_2^n} f\left(\overline{v}_{\pi(0)}, \ldots, \overline{v}_{\pi(n-1)}\right) \prod_{j=0}^{n-1}\left(\overline{v}_j + x_j\right) = \\
&= \sum_{v_0 \ldots v_{n-1} \in \mathbb{F}_2^n} f\left(\overline{v}_0, \ldots, \overline{v}_{n-1}\right) \prod_{j=0}^{n-1}\left(\overline{v}_{\pi^{-1}(j)} + x_j\right) = \tag{2.5} \\
&= \sum_{v_0 \ldots v_{n-1} \in \mathbb{F}_2^n} f\left(\overline{v}_0, \ldots, \overline{v}_{n-1}\right) \prod_{j=0}^{n-1}\left(\overline{v}_j + x_{\pi(j)}\right) = \\
&= \sum_{v_0 \ldots v_{n-1} \in \mathbb{F}_2^n} f_{\leftarrow}\left(v_0, \ldots, v_{n-1}\right) \prod_{j=0}^{n-1}\left(\overline{v}_j + x_{\pi(j)}\right) = \\
&= \phi\left(f_{\leftarrow}\right) \circ \left(x_{\pi(0)}, \ldots, x_{\pi(n-1)}\right) = \phi\left(f_{\leftarrow}\right)^{(\pi)}.
\end{aligned}$$

■

The canonical disjunctive normal form of an n-variable Boolean function is $f = \vee_{i=0}^{2^n-1}(u_i \wedge m_i)$, where $u_i \in \{0,1\}$ and $m_i = \wedge_{j=0}^{n-1} x_j^{\left(a_j^{(i)}\right)}$ so that $i = \sum_{j=0}^{n-1} a_j^{(i)} 2^i$, and $x^{(0)} = \overline{x}$, $x^{(1)} = x$. Similarly, if p is the Zhegalkin polynomial of the Boolean function f, then $p = \sum_{i=0}^{2^n-1} v_i S_i$, $v_i \in \{0,1\}$ and $S_i = \prod_{j=0}^{n-1} x_j^{a_j^{(i)}}$. Both $\mathbf{u}$ composed of the sequence of the u_i-s and $\mathbf{v}$ composed of the sequence of the v_i-s are the spectrum of the function, spectrum belonging to the appropriate form of the function. It is obvious that changing the order of the variables rearranges the spectra, too. Let us see now the alteration of the spectra.

$$\wedge_{j=0}^{n-1} x_{\pi(j)}^{\left(a_j^{(i)}\right)} = \wedge_{j=0}^{n-1} x_j^{\left(a_{\pi^{-1}(j)}^{(i)}\right)} = m_l \text{ and } \prod_{j=0}^{n-1} x_{\pi(j)}^{a_j^{(i)}} = \prod_{j=0}^{n-1} x_j^{a_{\pi^{-1}(j)}^{(i)}} = S_l,$$

where $l = \sum_{j=0}^{n-1} a_{\pi^{-1}(j)}^{(i)} 2^j$. If $i_1 \neq i_2$, then $a_j^{(i_1)} \neq a_j^{(i_2)}$ for at least one j. Then for such an index j $a_{\pi^{-1}(j)}^{(i_1)}$ and $a_{\pi^{-1}(j)}^{(i_2)}$, consequently l_1 and l_2 differ from each other, too. As both values are in $\mathbb{N}_n$, so permuting the indices results in the rearrangement of the spectra, and by the former results the orders of the elements of the two spectra change equivalently. Let Π denote the rearrangement of the spectrum induced by π, that is, if $\mathbf{w}$ is a spectrum then let $\Pi\mathbf{w}$ be the rearranged spectrum.

Theorem 2.3. *If f is a conjunctively polynomial-like Boolean function, then $f^{(\pi)}$ is conjunctively polynomial-like, too.*

Proof. If the spectrum of the conjunctively polynomial-like Boolean function f is $\mathbf{w} \in \mathbb{F}_2^{2^n}$, then $\mathbf{w} = \mathbf{APw}$, and by the previous result $\mathbf{AP\Pi w} = \mathbf{\Pi APw}$, where Π is the rearrangement of the spectrum induced by π. From these two results, we get that $\mathbf{AP}\left(\mathbf{\Pi w}\right) = \mathbf{AP\Pi w} = \mathbf{\Pi APw} = \mathbf{\Pi}\left(\mathbf{APw}\right) = \mathbf{\Pi w}$. ■

The next statement follows easily from the previous results.

Theorem 2.4. *Each variable of a conjunctively polynomial-like Boolean function of at least one variable different from the zero function is essential.*

Proof. It is enough to prove that the variable belonging to the greatest index is essential, otherwise $\underline{u}_0 = \underline{u}_1$ in $\underline{u} = \underline{u}_0\underline{u}_1$. But in that case we get from the equation

$$\begin{pmatrix} \underline{u}_0 \\ \underline{u}_1 \end{pmatrix} = \begin{pmatrix} \mathbf{0}^{(n)} & \mathbf{U}^{(n)} \\ \mathbf{U}^{(n)} & \mathbf{U}^{(n)} \end{pmatrix} \begin{pmatrix} \underline{u}_0 \\ \underline{u}_1 \end{pmatrix} \tag{2.6}$$

that $\underline{u}_0 = \mathbf{U}^{(n)}\underline{u}_0 + \mathbf{U}^{(n)}\underline{u}_0 = \underline{0}$, that is $\underline{u} = \underline{0}$. ■

3. Conclusion

In earlier papers we proved that there are bases of the space of the Boolean functions containing only polynomial-like Boolean functions or only conjunctively polynomial-like Boolean functions, so these classes of the Boolean functions have nice properties. It was also proved that polynomial-like Boolean functions of at least one variable different from the zero-function have no fictive variables. Now, in this paper was proved that the conjunctively polynomial-like Boolean functions have the same property, that is, every variable of a non-constant conjunctively polynomial-like Boolean function is essential, the function essentially depends on all of its variables.

In the article there is another result, too. As permuting the order of the variables, we get from a conjunctively polynomial-like Boolean function again a conjunctively polynomial-like function, knowing such a function we can know other conjunctively polynomial-like Boolean functions only rearranging the variables of the function (it is only a possibility as there are conjunctively polynomial-like Boolean functions that are invariant with respect to these rearrangements, for instance all of the three-variable conjunctively polynomial-like Boolean functions).

References

[1] **Akers, S. H.,** On a Theory of Boolean functions, *J. SIAM*, **7** (1959), 487–498.

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

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

[4] **Davio, M., J.-P. Deschamps and A. Thayse,** *Discrete and Switching Functions*, McGraw-Hill International Book Co, New York, 1966.

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

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

[7] **Gonda, J.,** Conjunctively polynomial-like Boolean functions, *Acta Mathematica Academiae Paedagogicae Nyíregyháziensis*, **23(2)** (2007), 89–103.

[8] **Lechner, R. J.,** Harmonic analysis of switching functions, in: *Recent Developments in Switching Theory* (Oberwolfach, 1983), International Series of Numerical Mathematics **71**, Academic Press, New York, 1971, 121–228.

[9] **Post, E. L.,** Introduction to a general theory of elementary propositions, *Amer. J. Math.*, **43(3)** (1921), 163–185.

[10] **Post, E. L.,** *Two-Valued Iterative Systems of Mathematical Logic*, *Annals of Mathematics Studies, no. 5* Princeton University Press, Princeton, New York, 1941.

J. Gonda
Department of Computer Algebra
Eötvös Loránd Universitiy
Faculty of Informatics
H-1117 Budapest
Pázmány Péter sétány 1/C
Hungary
andog@inf.elte.hu