Annales Univ. Sci. Budapest., Sect. Comp. 32 (2010) 49-61

CONJUNCTIVELY POLYNOMIAL–LIKE BOOLEAN FUNCTIONS AND THE MAXIMAL CLOSED CLASSES

J. Gonda (Budapest, Hungary)

Abstract. In [7] it was introduced the notion of the conjunctively polynomial like Boolean functions. In this article it is investigated how these functions are related to the maximal closed classes of the Boolean functions and it is pointed out that there are bases of the Boolean functions containing only conjunctively polynomial-like Boolean functions.

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 roles in our everyday life, so it is easy to understand why they are widely investigated. A scope of 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 [9], but there are a lot of another classes of the Boolean functions invariant with respect to some

Mathematics Subject Classification: 06E30, 94C10, 15A18

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. In the following article we examine the relation between the latter type of Boolean functions and the maximal closed classes of the two-valued logical functions.

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 $0 \leq j < n$, 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 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 $0 \leq j < 2^n$) means that $m_j^{(n)}$ does not 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.

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

$$f^{(n)} = \bigoplus_{i=0}^{2^n-1} k_i S_i^{(n)}. \tag{3}$$

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 $\mathbf{F}_2$, 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

$$\mathbf{A}^{(n)} = \begin{cases} (1) & \text{if } n = 0, \\ \begin{pmatrix} \mathbf{A}^{(n-1)} & \mathbf{0}^{(n-1)} \\ \mathbf{A}^{(n-1)} & \mathbf{A}^{(n-1)} \end{pmatrix} & \text{if } n \in \mathbf{N}^+ \end{cases} \tag{4}$$

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

$$\mathbf{A}^{(n)^2} = \mathbf{I}^{(n)}, \tag{5}$$

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

$$\begin{pmatrix} \underline{u}_0 \\ \underline{u}_1 \end{pmatrix} = \begin{pmatrix} \mathbf{A}^{(n)} & \mathbf{0}^{(n)} \\ \mathbf{A}^{(n)} & \mathbf{A}^{(n)} \end{pmatrix} \begin{pmatrix} \underline{u}_0 \\ \underline{u}_1 \end{pmatrix} \tag{6}$$

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 $\underline{u}_0 = (\mathbf{A}^{(n)} + \mathbf{I}^{(n)})\underline{u}_1$, 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.

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

$$M_i^{(n)} = \sum_{j=0}^{n-1} \left(a_j^{(i)} \oplus x_j \right) \tag{7}$$

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

$$f^{(n)} = \prod_{i=0}^{2^n-1} \left(\alpha_i + M_i^{(n)} \right), \tag{8}$$

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

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

$$M_i^{(n)'} = \sum_{j=0}^{n-1}\left(\overline{a_j^{(i)}} \oplus x_j\right). \tag{9}$$

It is easy to see that $M_i^{(n)} = M_{2^n-1-i}^{(n)'}$. Now if $f^{(n)} = \prod_{i=0}^{2^n-1}\left(\beta_i + M_i^{(n)'}\right) = f_k^{(n)}$ 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 $\bar{u} \oplus v = u \oplus \bar{v}$, so $\overline{a_j^{(i)}} \oplus x_j = a_j^{(i)} \oplus \overline{x}_j$ and $M_i^{(n)'} = \sum_{j=0}^{n-1}\left(a_j^{(i)} \oplus \overline{x}_j\right)$. If $g^{(n)} = \prod_{i=0}^{2^n-1}\left(\beta_i + M_i^{(n)}\right)$, then

$$\begin{aligned} f^{(n)}(x_{n-1}, \ldots, x_0) &= \prod_{i=0}^{2^n-1}\left(\alpha_i + \sum_{j=0}^{n-1}\left(a_j^{(i)} \oplus x_j\right)\right) = \\ &= \prod_{i=0}^{2^n-1}\left(\alpha_i + M_i^{(n)}\right) = \prod_{i=0}^{2^n-1}\left(\beta_i + M_i^{(n)'}\right) = \\ &= \prod_{i=0}^{2^n-1}\left(\beta_i + \sum_{j=0}^{n-1}\left(a_j^{(i)} \oplus \overline{x}_j\right)\right) = \\ &= g^{(n)}(\overline{x}_{n-1}, \ldots, \overline{x}_0) = \overline{\overline{g^{(n)}}}(\overline{x}_{n-1}, \ldots, \overline{x}_0) = \\ &= \overline{g^{(n)D}}(x_{n-1}, \ldots, x_0), \end{aligned} \tag{10}$$

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 (10).

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 $\underline{\beta} = \underline{k} = \mathbf{A}^{(n)}\underline{\alpha} = (\mathbf{A}^{(n)}\mathbf{P}^{(n)})\underline{\beta} = \mathbf{U}^{(n)}\underline{\beta}$, 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 (4), we get that

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

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

$$\underline{\beta} = \begin{pmatrix} \mathbf{Q}^{(n)^{-1}}\mathbf{R}^{(n)} \\ \mathbf{I}^{(\mu_n \times \mu_n)} \end{pmatrix} \underline{u}. \tag{11}$$

Here $\mu_n = \frac{2^n+2(-1)^n}{3}$, $2^n - \mu_n$ is the rank of $\mathbf{U}^{(n)} + \mathbf{I}^{(n)} = \begin{pmatrix} \mathbf{Q}^{(n)} & \mathbf{R}^{(n)} \\ \mathbf{S}^{(n)} & \mathbf{T}^{(n)} \end{pmatrix}, \mathbf{Q}^{(n)}$ 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 2^{μ_n}-dimensional linear space over $\mathbf{F}_2$.

1.2. Maximal closed classes of the Boolean functions

An n-variable Boolean function f is

- zero preserving, if $f(0, \ldots, 0) = 0$;
- one preserving, if $f(1, \ldots, 1) = 1$;
- self-dual, if $\overline{f}(\overline{u}_0, \ldots, \overline{u}_{n-1}) = f(u_0, \ldots, u_{n-1})$ for every $\underline{u} \in \mathbf{F}_2^n$;
- monotone, if $f(\underline{u}) \leq f(\underline{v})$, supposing that $u_i \leq v_i$ for every $n > i \in \mathbf{N}$;
- affine, if $f(x_0, \ldots, x_{n-1}) = a + \sum_{i=0}^{n-1} a_i x_i$, where a and a_i are either 0 or 1 for every $n > i \in \mathbf{N}$, and f is linear, if it is affine and $a = 0$.

Let T_0 , T_1 , S , M and L denote the set of zero preserving, one preserving, self-dual, monotone and affine Boolean functions, respectively (sometimes we refer to an affine function as linear function independently of the value of the constant term of the function). These sets are the maximal closed classes of the set B of all of the Boolean functions, so the closure of a subset A of B is B, if and only if A contains a not 0 preserving, a not 1 preserving, a not self-dual, a nonmonotone and a nonlinear function (not unconditionally different from each other) (see for instance in [11]). A not 1 preserving function is either not

self-dual or not 0 preserving, so four functions are enough to generate each Boolean function. If A is minimal with respect to the property generating B, then A is a basis of B. It follows from the previous statements that a basis contains at most four Boolean functions. If a function itself is the basis of B, then it is a universal Boolean function. Universal Boolean functions are for instance the Sheffer function and the Pierce function, that is the NAND and the NOR functions.

2. New results

2.1. Zero and one preserving

Let us suppose that $\underline{u}$ is the spectrum of the modified conjunctive normal form of a conjunctively polynomial-like Boolean function of n variables where n is a nonnegative integer. Then

$$\underline{u} = \left(\mathbf{A}^{(n)}\mathbf{P}^{(n)}\right)\underline{u} = \mathbf{U}^{(n)}\underline{u} \tag{12}$$

and

$$u_0 = \left(\mathbf{U}^{(n)}\underline{u}\right)_0 = \sum_{j=0}^{2^n-1} U_{0,j}^{(n)} u_j = u_{2^n-1}. \tag{13}$$

This means that a conjunctively polynomial-like Boolean function is either zero preserving and not one preserving or one preserving and not zero preserving, exclusively. If $\mathbf{U}^{(n)} + \mathbf{I}^{(n)} = \begin{pmatrix} \mathbf{Q}^{(n)} & \mathbf{R}^{(n)} \\ \mathbf{S}^{(n)} & \mathbf{T}^{(n)} \end{pmatrix}$ then all of the conjunctively polynomial-like Boolean functions of n variables can be generated by

$$\underline{u} = \begin{pmatrix} {\mathbf{Q}^{(n)}}^{-1}\mathbf{R}^{(n)} \\ \mathbf{I}^{(\mu_n \times \mu_n)} \end{pmatrix} \underline{v}, \tag{14}$$

where $\underline{v}$ is an arbitrary element of the μ_n-dimensional Boolean space. If $n = 1$ then $\mu_n = \frac{2^n+2(-1)^n}{3} = 0$ and the only conjunctively polynomial-like Boolean function is $f_0^{(1)}$, that is the zero function of one variable. In every other case $\mu_n > 0$ and exactly half of the vectors of the μ_n-dimensional space is not

one preserving. But $u_{2^n-1} = v_{\mu_n-1}$ and that means that exactly half of the conjunctively polynomial-like Boolean functions is zero preserving.

2.2. Self-duality

The Boolean function $f^{(n)}$ of n variables is self-dual if and only if

$$f^{(n)}(\overline{c_{n-1}}, \ldots, \overline{c_0}) = \overline{f^{(n)}}(c_{n-1}, \ldots, c_0) \tag{15}$$

for any value of the variables, and, as a special case, only if

$$\begin{aligned} f^{(n)}(1, \ldots, 1) &= f^{(n)}(\overline{0}, \ldots, \overline{0}) = \\ &= \overline{f^{(n)}}(0, \ldots, 0) = \overline{f^{(n)}(0, \ldots, 0)}. \end{aligned} \tag{16}$$

If $\underline{u}$ is the spectrum of the modified conjunctive normal form of the function and this condition is fulfilled then $\overline{u_0} = \overline{f^{(n)}(0, \ldots, 0)} = f^{(n)}(1, \ldots, 1) = u_{2^n-1}$ and this is impossible if $f^{(n)}$ is a conjunctively polynomial-like Boolean function (see 2.1), that is there is no self-dual conjunctively polynomial-like Boolean function.

2.3. Monotonicity

$f^{(n)}$ is monotone if

$$f^{(n)} = (a_{n-1}, \ldots, b_0) \leq f^{(n)}(b_{n-1}, \ldots, b_0) \tag{17}$$

in all cases when $a_i \leq b_i$ for every indices $n > i \in \mathbf{N}$. This is true if $f^{(n)}$ is the zero function or the one function, so the zero function of n variables for an arbitrary nonnegative integer n and the one function of zero variables are monotone conjunctively polynomial-like Boolean functions. If $f^{(n)}$ is not constant and $\underline{u}$ is the spectrum of the modified conjunctive normal form of the function then there exist such a $2^n > i = \sum_{k=0}^{n-1} a_k^{(i)} 2^k \in \mathbf{N}$ and a $2^n > j = \sum_{k=0}^{n-1} a_k^{(j)} 2^k \in \mathbf{N}$ that $u_i = 0$ and $u_j = 1$. Now let us suppose that $f^{(n)}$ is a conjunctively polynomial-like Boolean function, then either $u_0 = 0 = u_{2^n-1}$ or $u_0 = 1 = u_{2^n-1}$. In the first case

$$f^{(n)}\left(a_{n-1}^{(j)},\dots,a_0^{(j)}\right)=u_j=1\not\leqslant \not\leqslant 0=u_{2^n-1}=f^{(n)}(1,\dots,1) \tag{18}$$

and in the second case

$$f^{(n)}(0,\dots,0)=u_0=1\not\leqslant \not\leqslant 0=u_i=f^{(n)}\left(a_{n-1}^{(i)},\dots,a_0^{(i)}\right) \tag{19}$$

so a nonconstant conjunctively polynomial-like Boolean function is always nonmonotone.

$$\begin{pmatrix} 0 & \dots & 0 & 0 & 0 & \dots & 0 & 1\\ \vdots & & \vdots & \vdots & \vdots & & \vdots & \vdots\\ \vdots & & \vdots & \vdots & \vdots & & \vdots & \vdots\\ 0 & \dots & 0 & 1 & U_{2^n-1-r,r+1} & \dots & U_{2^n-1-r,2^n-2} & 1\\ \vdots & & \vdots & \vdots & \vdots & & \vdots & \vdots\\ 1 & \dots & 1 & 1 & 1 & \dots & 1 & 1 \end{pmatrix} \begin{pmatrix} u_0\\ \vdots\\ u_r\\ 0\\ \vdots\\ \vdots\\ 0 \end{pmatrix} \tag{20}$$

2.4. Linearity

The zero function and the one function of zero variables are conjunctively polynomial-like and affine functions, even more the former one is linear. From now on let the functions we deal with be of n variables where n is equal to at least 1. If $u_i=0$ for every $2^n>i\in\mathbf{N}$ greater than a given $2^n>r\in\mathbf{N}$, then all of the components of $\mathbf{U}^{(n)}\underline{u}$ belonging to the indices less than 2^n-1-r are equal to 0 and $(\mathbf{U}^{(n)}\underline{u})_{2^n-1-r}=u_r$ (see (20)). In the Zhegalkin polynomial of an affine Boolean function all of the coefficients are equal to 0 with the exceptions of maybe some of those belonging to the index 0 or to the indices equal to a power of 2 with nonnegative exponents less than n and if there exists such an index then it is less than or equal to 2^{n-1}. Let $\underline{u}$ be the spectrum of the modified conjunctive normal form of a conjunctively polynomial-like Boolean function. Then $\underline{u}$ is the spectrum of the Zhegalkin polynomial of the function, too, and then every component of $\underline{u}$ with an index greater than 2^{n-1} is equal to 0. From this follows by the previous results that all of the components of $\underline{u}$ belonging to the indices less than $2^n-1-2^{n-1}=2^{n-1}-1$ are equal to zero

and $u_{2^{n-1}-1} = (\mathbf{U}^{(n)}\underline{u})_{2^{n-1}-1} = u_{2^{n-1}}$. If $u_{2^{n-1}} = 0$ then $u_{2^{n-1}-1} = 0$ and the components belonging to the indices less than $2^{n-1}-1$ or greater than 2^{n-1} are equal to zero, too, so $\underline{u} = \underline{0}$, that is $\underline{u}$ is the spectrum of the zero function. Let now $u_{2^{n-1}} = 1$. Then $u_{2^{n-1}-1} = 1$ and all of the other components of $\underline{u}$ are equal to zero. As the function is affine so either $2^{n-1}-1 = 2^t$ with a nonnegative integer less than $n-1$ or $2^{n-1}-1 = 0$. In the latter case $n = 1$ and $\underline{u}^T = 11$, but this function is not a conjunctively polynomial-like Boolean function as

$$\mathbf{U}^{(1)}\underline{u} = \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}\begin{pmatrix} 1 \\ 1 \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \end{pmatrix} \neq \begin{pmatrix} 1 \\ 1 \end{pmatrix} = \underline{u}. \tag{21}$$

In the other case $2^{n-1} = 2^t + 1 \geq 2$, so $n \geq 2$ and then 2^{n-1} is an even number. From this follows that $2^t = 2^{n-1} - 1$ is an odd integer. But the only 2-power which is an odd integer 1, so $2^t = 1$ and $2^{n-1} = 2^t + 1 = 1 + 1 = 2$, that implies that $n = 2$. Then $u_1 = u_{2^{n-1}-1} = 1 = u_{2^{n-1}} = u_2$ and $u_0 = 0 = u_3$, that is, $\underline{u}^T = 0110$ and this is the spectrum of the modified conjunctive normal form of a conjunctively polynomial-like Boolean function of two variables, indeed, as

$$\mathbf{U}^{(2)}\underline{u} = \begin{pmatrix} 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 \\ 1 & 1 & 1 & 1 \end{pmatrix}\begin{pmatrix} 0 \\ 1 \\ 1 \\ 0 \end{pmatrix} = \begin{pmatrix} 0 \\ 1 \\ 1 \\ 0 \end{pmatrix} = \underline{u}. \tag{22}$$

2.5. Conjunctively polynomial-like bases of the space of the Boolean functions

With the previous results the closure of the set of the conjunctively polynomial-like Boolean functions is the whole set of the Boolean functions. Really, all of the zero preserving conjunctively polynomial-like Boolean functions different from the zero function and the exclusive or function of two variables are not one preserving, not self-dual, nonmonotone and nonlinear, so every set of the one function of zero variables and of any zero preserving conjunctively polynomial like Boolean function not equal to the zero function and to the exclusive or function of two variables is a basis of the space of the Boolean functions.

The only conjunctively polynomial-like Boolean function of one variable is the zero function. There are altogether four conjunctively polynomial-like Boolean functions of two variables and among them there are exactly two which

are zero preserving, namely the zero function and the exclusive or function of two variables, so with these functions we do not get a basis. The first conjunctively polynomial-like Boolean function of three variables not equal to the zero function is $f_{126}^{(3)}$ as $126_{10} = 01111110_2$ and

$$\begin{pmatrix} 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 \\ 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \end{pmatrix} \begin{pmatrix} 0 \\ 1 \\ 1 \\ 1 \\ 1 \\ 1 \\ 1 \\ 0 \end{pmatrix} = \begin{pmatrix} 0 \\ 1 \\ 1 \\ 1 \\ 1 \\ 1 \\ 1 \\ 0 \end{pmatrix}. \tag{23}$$

This function is zero preserving (and this is the only zero preserving conjunctively polynomial-like Boolean function of three variables not equal to the zero function), so $\left\{f_1^{(0)}, f_{126}^{(3)}\right\}$ is a basis of the set of all of the Boolean functions. Really,

$$\begin{aligned} f_{126}^{(3)}(x_2, x_1, x_0) &= M_0^{(3)} M_7^{(3)} = \\ &= (\overline{x}_2 + \overline{x}_1 + \overline{x}_0)(x_2 + x_1 + x_0). \end{aligned} \tag{24}$$

Let $g(x_1, x_0) = f_{126}^{(3)}(1, x_1, x_0)$. Then

$$\begin{aligned} g(x_1, x_0) &= f_{126}^{(3)}\left(f_1^{(0)}(), x_1, x_0\right) = \\ &= \left(\overline{f_1^{(0)}}() + \overline{x}_1 + \overline{x}_0\right)\left(f_1^{(0)}() + x_1 + x_0\right) = \\ &= (\overline{1} + \overline{x}_1 + \overline{x}_0)(1 + x_1 + x_0) = \\ &= (0 + \overline{x}_1 + \overline{x}_0)(1 + x_1 + x_0) = \\ &= (\overline{x}_1 + \overline{x}_0) \cdot 1 = \overline{x}_1 + \overline{x}_0 = \overline{x_1 x_0} = x_1 | x_0, \end{aligned}$$

where $|$ denotes the Sheffer function, that is, the NAND-operation which is a universal Boolean function.

3. Conclusion

In the article above we examined some properties, namely the zero and one preserving characteristic, the self-duality, the linearity and the monotonicity of the so-called conjunctively polynomial-like Boolean functions, defined in [7]. The properties examined are those characterizing a set of Boolean functions making up a basis of the switching functions. It is well-known that a basis consists of at most four Boolean functions, and there are bases containing only one Boolean function. Now it was proven that there exist bases consisting only of two Boolean functions of which one is the constant 1 function and the other is a conjunctively polynomial-like Boolean function, too. As these functions are invariant with respect to a linear transform, the construction of a given Boolean function on the base of these functions can be more flexible in some aspects than in the case of the use of the functions of other bases.

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, *34.IEEE Foundations of Computer Science, 1995,* 82-95.

[3] **Calingaert P.,** Switching functions: Canonical form based on commutative and associative binary operations, *Trans. AIEE,* **80** (1961), 808-814.

[4] **Davio M., Deschamps J.-P. and Thayse A.,** *Discrete and switching functions,* McGraw-Hill, 1978.

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

[6] **Gonda J.,** Polynomial-like Boolean functions, *Annales Univ. Sci. Budapest. Sect. Comp.,* **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, *Recent Developments in Switching Theory,* ed. A. Mukhodpadhyay, Academic Press, 1971, 121-228.

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

[10] **Post E.L.,** *Two-valued iterative systems of mathematical logic,* Princeton Univ. Press, 1941.

[11] **Яблонский С.В., Гаврилов Г.П. и Кудрявцев В.Б.,** *Функции алгебры логики и классы Поста,* Наука, Москва, 1966. (Yablonsky S.V., Gavrilov G.P. and Kudryavtsev V.B., *Functions of the algebra of logics and Post classes,* Nauka, Moscow, 1966.)

(Received July 13, 2007)

J. Gonda
Department of Computer Algebra
Eötvös Loránd University
Pázmány Péter sét. 1/C
andog@compalg.inf.elte.hu