Annales Univ. Sci. Budapest., Sect. Comp. 26 (2006) 91-104

POLYNOMIAL–LIKE BOOLEAN FUNCTIONS AND THE MAXIMAL CLOSED CLASSES

J. Gonda (Budapest, Hungary)

Abstract. A Boolean function f is polynomial-like if the coefficients in its canonical disjunctive normal form are equal to the coefficients in its Zhegalkin polynomial, that is if the vector of the coefficients of one of the two representations is the eigenvector of the transformation to the other form. In the following article we investigate how are these functions related to the maximal closed classes of the 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; $\mathbf{N}_0$ denotes the set of the non-negative integers, and $\mathbf{N}$ denotes the set of the positive integers.

1. Introduction

Let $f(x_0, \ldots, x_{n-1})$ be a Boolean function of n variables, that is $f : \{0,1\}^n \longrightarrow \{0,1\}$. If $(u_0, \ldots, u_{n-1}) \in \{0,1\}^n$, $i = \sum_{j=0}^{n-1} u_j 2^j$, $f(u_0, \ldots, u_{n-1}) =$

The research was supported by the Hungarian National Foundation for Scientific Research under grant OTKA T-043657.

Mathematics Subject Classification: 06E30, 94C10

$= \alpha_i$ and $l = \sum_{j=0}^{2^n-1} \alpha_j 2^j$, then f can be denoted by $f_l^{(n)}$, and it is uniquely determined by a 2^n-long series composed by the α_i-s ordered by their indices. If $(a_0, \ldots, a_{n-1}) \in \{0,1\}^n$ is a given n-tuple and $f(x_0, \ldots, x_{n-1}) = \prod_{j=0}^{n-1} (\overline{a_j} \oplus x_j)$ then $\alpha_i = f(u_0, \ldots, u_{n-1}) = 1$ if and only if $(u_0, \ldots, u_{n-1}) = (a_0, \ldots, a_{n-1})$. This function is denoted by $m_k^{(n)}$, that is

$$m_k^{(n)} = \prod_{j=0}^{n-1} (\overline{a_j} \oplus x_j), \tag{1}$$

where $k = \sum_{j=0}^{n-1} a_j 2^j$ and it is called the k-th minterm of n variables. Then

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

and this sum of the minterms is the canonical disjunctive normal form of $f_l^{(n)}$. The series of the α_i-s ordered by their indices is the spectrum of the canonical disjunctive normal form of the l-th Boolean function $f_l^{(n)}$ of n variables.

Another possibility to determine a Boolean function is the so called Zhegalkin polynomial. If $(a_0, \ldots, a_{n-1}) \in \{0,1\}^n$ is a given n-tuple, again, and $k = \sum_{j=0}^{n-1} a_j 2^j$, then

$$S_k^{(n)} = \prod_{j=0}^{n-1} (\overline{a_j} + x_j) \tag{3}$$

is the k-th monom of n variables. Let $k_0, \ldots, k_{2^n-1}$ be a 2^n-long series of 0-s and 1-s, then

$$f = \bigoplus_{i=0}^{2^n-1} k_i S_i^{(n)} \tag{4}$$

is a uniquely determined Boolean function of n variables, and conversely, to every Boolean function f of n variables belongs a uniquely determined 2^n-long series $k_0, \ldots, k_{2^n-1}$ of 0-s and 1-s so that $f = \bigoplus_{i=0}^{2^n-1} k_i S_i^{(n)}$. Now the series of

the coefficients of $k_0, \ldots, k_{2^n-1}$ is the spectrum of the Zhegalkin polynomial of the function.

There is a simple connection between the two above mentioned representations of the same Boolean function: if $\underline{\alpha}$ is the spectrum of the disjunctive normal form of the function and $\underline{k}$ is the spectrum of the Zhegalkin polynomial of the same function then

$$\underline{k} = \mathbf{A}^{(n)}\underline{\alpha}, \tag{5}$$

where

$$\mathbf{A}^{(n)} = \begin{cases} [\ 1\ ] & \text{if } n = 0, \\ \begin{bmatrix} \mathbf{A}^{(n-1)} & \mathbf{0}^{(n-1)} \\ \mathbf{A}^{(n-1)} & \mathbf{A}^{(n-1)} \end{bmatrix} & \text{if } n \in \mathbf{N} \end{cases} \tag{6}$$

($\mathbf{A}^{(n)}$ is a $2^n \times 2^n$ matrix and $\mathbf{0}^{(n)}$ is the $2^n \times 2^n$ zero matrix), and

$$\left(\mathbf{A}^{(n)}\right)^{-1} = \mathbf{A}^{(n)} \tag{7}$$

for any nonnegative integer n.

Let $f(x_0, \ldots, x_{n-1})$ be a Boolean function of n variables. Then f is

- 0-preserving if and only if $f(0, \ldots, 0) = 0$;
- 1-preserving if and only if $f(1, \ldots, 1) = 1$;
- self-dual if and only if $f(\overline{u_0}, \ldots, \overline{u_{n-1}}) = \overline{f(u_0, \ldots, u_{n-1})}$ for any $(u_0, \ldots, u_{n-1}) \in \{0,1\}^n$;
- monotone if and only if $f(u_0, \ldots, u_{n-1}) \leq f(v_0, \ldots, v_{n-1})$ in all of the cases when $u_i \leq v_i$ for every $n > i \in \mathbf{N}_0$;
- affine if and only if $f = c \oplus \bigoplus_{i=0}^{n-1} c_i x_i$ where c and the c_i-s are either 0 or 1 and linear if and only if affine and $c = 0$.

Let T_0, T_1, SF, M and A denote the set of zero preserving, one preserving, self-dual, monotone and affine Boolean functions, respectively. As these sets are closed classes of the set B of all of the Boolean functions, so if C is such a subset of B that its closure is B, then C has to contain a not 0 preserving, a not 1 preserving, a not self-dual, a nonmonotone and a nonaffine function (not unconditionally different from each other). The before-mentioned classes of the Boolean functions are maximal, and 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 C is minimal with respect to the property generating B, then C 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 Peirce function, that is the NAND and the NOR functions.

We refer to a Boolean function as a polynomial-like Boolean function if and only if the spectra belonging to its canonical disjunctive normal form and its Zhegalkin polynomial are identical, that is, if $\underline{k} = \underline{\alpha}$. Both of the Boolean functions of zero variables are polynomial-like. If n is a positive integer then the set of the polynomial-like Boolean functions of n variables is a 2^{n-1}-dimensional subspace of the 2^n-dimensional space of all of the Boolean functions of n variables, so there are altogether $2^{2^{n-1}}$ polynomial-like Boolean functions of n variables. The Boolean function f of n variables determined by $\underline{\alpha}$ as the spectrum of its canonical disjunctive normal form is polynomial-like if and only if

$$\underline{\alpha} = \begin{bmatrix} \mathbf{A}^{(n-1)} + \mathbf{I}^{(n-1)} \\ \mathbf{I}^{(n-1)} \end{bmatrix} \underline{u}, \tag{8}$$

where $\mathbf{I}^{(n)}$ is the $2^n \times 2^n$ identity matrix, and $\underline{u}$ is an arbitrary element of the 2^{n-1}-dimensional linear space over $\mathbf{F}_2$, that is $\underline{u}$ is the spectrum of the canonical disjunctive normal form of an arbitrary Boolean function of $n-1$ variables [3]. In another way, if the spectrum of the canonical disjunctive normal form of the Boolean function f of n variables is

$$\underline{\alpha} = \begin{bmatrix} \alpha_0 \\ \vdots \\ \alpha_{2^{n-1}-1} \\ \alpha_{2^{n-1}} \\ \vdots \\ \alpha_{2^n-1} \end{bmatrix} = \begin{bmatrix} \underline{\alpha}^{(0)} \\ \underline{\alpha}^{(1)} \end{bmatrix}, \tag{9}$$

then f is polynomial-like if and only if $\underline{\alpha}^{(0)} = \left(\mathbf{A}^{(n-1)} + \mathbf{I}^{(n-1)}\right) \underline{\alpha}^{(1)}$. This means that if $\underline{\alpha}$ is the spectrum of the canonical disjunctive normal form of an arbitrary Boolean function f_1 of $n-1$ variables, and f_0 is the Boolean function with $\left(\mathbf{A}^{(n-1)} + \mathbf{I}^{(n-1)}\right) \underline{\alpha}$ as the spectrum of its canonical disjunctive normal form, then $f = \overline{x}_{n-1} f_0 + x_{n-1} f_1$ is a polynomial-like Boolean function of n variables (x_{n-1} is the new variable). Of course if f is a polynomial-like Boolean function and $\underline{\alpha}$ is the spectrum of its canonical disjunctive normal form, then $\underline{\alpha}$ is the spectrum of its Zhegalkin polynomial, too. From the previous results follows that for any positive integer n, $f_0^{(n)}$, $f_{2^{2^n-1}-2}^{(n)}$, $f_{2^{2^n-1}}^{(n)}$ and $f_{2^{2^n}-2}^{(n)}$

are polynomial-like Boolean functions of n variables. If f is a polynomial-like Boolean function then all of its variables are essential.

2. Development

Theorem 1. *The index of a polynomial-like Boolean function of at least one variable is even.*

Proof. This statement was proved in [4].

Corollary 1. *A polynomial-like Boolean function of at least one variable is zero preserving.*

Proof. This corollary is an almost obvious consequence of the previous theorem, but we give a formal proof for the sake of the completeness. Let $f = \sum_{i=0}^{2^n-1} \alpha_i m_i^{(n)}$, where $m_i^{(n)} = \prod_{j=0}^{n-1} \left(\overline{a}_i^{(i)} \oplus x_j\right)$ and $i = \sum_{j=0}^{n-1} a_j^{(i)} 2^j$ for every $2^n > i \in \mathbf{N}_0$. Then $t = \sum_{j=0}^{2^n-1} \alpha_j 2^j$ is the index of f. A Boolean function is zero preserving if and only if $\alpha_0 = 0$, and t is even if and only if $\alpha_0 = 0$. In Theorem 1 it was stated that the index of a polynomial-like Boolean function depending on at least one variable is even, so a polynomial-like Boolean function of $n > 0$ variables is zero preserving.

Theorem 2. *Exactly half of the polynomial-like Boolean functions is 1 preserving.*

Proof. $f_{2^{2^n-1}}^{(n)}$ is a polynomial-like Boolean function of n variables, and $\widetilde{f} = f \oplus f_{2^{2^n-1}}^{(n)}$ if and only if $f = \widetilde{f} \oplus f_{2^{2^n-1}}^{(n)}$, furthermore $\widetilde{f}$ is the function of the variables of the two functions so $f \mapsto f \oplus f_{2^{2^n-1}}^{(n)}$ is a bijective involution on the set of the Boolean functions of n variables. In [4] it was proved that the EXCLUSIVE OR of two polynomial-like Boolean functions is a polynomial-like Boolean function, too, so $\widetilde{f}$ is polynomial-like if and only if f has the same property. But in $\underline{\alpha}$ belonging to $f_{2^{2^n-1}}^{(n)}$ there is only one component with the value of 1, namely α_{2^n-1}, so all of the components of f and $f \oplus f_{2^{2^n-1}}^{(n)}$ are equal with the exception of that belonging to the index of $2^n - 1$. This means that one and exactly one of the two functions is 1 preserving, and then the mapping $f \mapsto f \oplus f_{2^{2^n-1}}^{(n)}$ is one to one from the set of the 1 preserving polynomial-like Boolean functions of n variables onto the set of the polynomial-like Boolean functions of the same variables not preserving 1.

Theorem 3. *The only self-dual polynomial-like Boolean function is the identity function of one variable.*

Proof.

$$\left(f_2^{(1)}(x_0)\right)^D = \overline{f}_2^{(1)}(\bar{x}_0) = \overline{\bar{x}}_0 = x_0 = f_2^{(1)}(x_0), \tag{10}$$

so the identity function of one variable, that is the only proper polynomial-like Boolean function of one variable is self-dual.

$$\overline{f}_0^{(0)}() = \bar{0} = 1 \neq 0 = f_0^{(0)}(), \tag{11}$$

and similarly

$$\overline{f}_1^{(0)}() = \overline{1} = 0 \neq 1 = f_1^{(0)}(), \tag{12}$$

so none of the Boolean functions of 0 variables is self-dual. Now let $n \geq 2$, and let $\underline{\alpha}$ be the spectrum of the Boolean function f of n variables.

$$\underline{\alpha} = \begin{bmatrix} \underline{\alpha}^{(0)} \\ \underline{\alpha}^{(1)} \end{bmatrix}, \tag{13}$$

where both $\underline{\alpha}^{(0)}$ and $\underline{\alpha}^{(1)}$ are vectors of the 2^{n-1}-dimensional linear space. If f is self-dual, then for $0 \leq i < 2^{n-1}$

$$\alpha_i^{(0)} = \overline{\alpha}_{2^{n-1}-1-i}^{(1)} = 1 \oplus \alpha_{2^{n-1}-1-i}^{(1)}, \tag{14}$$

so

$$\begin{aligned} w(\underline{\alpha}) &= w\left(\underline{\alpha}^{(0)}\right) + w\left(\underline{\alpha}^{(1)}\right) = \\ &= \sum_{i=0}^{2^{n-1}-1} \left(\left(1 \oplus \alpha_{2^{n-1}-i}^{(1)}\right) + \alpha_{2^{n-1}-i}^{(1)}\right) = \\ &= \sum_{i=0}^{2^{n-1}-1} \left(\left(1 + \alpha_{2^{n-1}-i}^{(1)} - 2 \cdot 1 \cdot \alpha_{2^{n-1}-i}^{(1)}\right) + \alpha_{2^{n-1}-i}^{(1)}\right) = \\ &= \sum_{i=0}^{2^{n-1}-1} \left(1 - \alpha_{2^{n-1}-i}^{(1)} + \alpha_{2^{n-1}-i}^{(1)}\right) = \sum_{i=0}^{2^{n-1}-1} 1 = 2^{n-1} \end{aligned} \tag{15}$$

and as $n \geq 2$, so $2 \mid 2^{n-1}$, that is $w(\underline{\alpha})$ is even. Now let f be polynomial-like. Then $\alpha_0 = 0$, because f is zero preserving, so $\alpha_{2^n-1} = 1$, because f is self-dual. But f is polynomial-like, so

$$\bigoplus_{i=0}^{2^n-1} \alpha_i = \left(\mathbf{A}^{(n)}\underline{\alpha}\right)_{2^n-1} = k_{2^n-1} = \alpha_{2^n-1} = 1, \tag{16}$$

and then

$$1 = \bigoplus_{i=0}^{2^n-1} \alpha_i = \left(\sum_{i=0}^{2^n-1} \alpha_i \bmod 2\right) = (w(\underline{\alpha}) \bmod 2), \tag{17}$$

that means $w(\underline{\alpha})$ is odd. But earlier we saw that this is impossible if f is a self-dual function.

Theorem 4. *The zero-function, the identity function of one variable and $x_1 \oplus x_0$ as a function of two variables are linear polynomial-like Boolean functions, and there is no other linear polynomial-like Boolean function. The only affine polynomial-like Boolean function, which is not linear, is the 1-function of zero variables.*

Proof. All of the enumerated functions are affine and polynomial-like. Now let f be a polynomial-like Boolean function of at least one variable. Then f is not degenerative and f is zero preserving, so if f is an affine function, then it is linear, too, and $f = \bigoplus_{i=0}^{n-1} x_i$, so the weight of f is equal to n. As f is polynomial-like, so the spectrum of the function has the form of

$$\begin{bmatrix} \left(\mathbf{A}^{(n-1)} + \mathbf{I}^{(n-1)}\right)\underline{\alpha} \\ \underline{\alpha} \end{bmatrix}, \tag{18}$$

where $\underline{\alpha}$ belongs to the 2^{n-1}-dimensional linear space.

$$f = \bigoplus_{i=0}^{n-1} x_i = x_{n-1} \cdot 1 \oplus \bigoplus_{i=0}^{n-2} x_i, \tag{19}$$

so $\alpha_i = 1$ is true only if $i = 0$, and then

$$\begin{bmatrix} \left(\mathbf{A}^{(n-1)} + \mathbf{I}^{(n-1)}\right)\underline{\alpha} \\ \underline{\alpha} \end{bmatrix} = \begin{bmatrix} \left(\mathbf{A}^{(n-1)} + \mathbf{I}^{(n-1)}\right)\underline{e}_0^{(n-1)} \\ \underline{e}_0^{(n-1)} \end{bmatrix} =$$

$$= \sum_{i=1}^{2^{n-1}} \underline{e}_i^{(n)}. \tag{20}$$

From this follows that $w(f) = 2^{n-1}$, and so $n = 2^{n-1}$. But this is true if and only if $n = 1$ or $n = 2$.

Theorem 5. *Every polynomial-like Boolean function of less than two variables is monotone, but in the case when $n \geq 2$, for any n there are both monotone and nonmonotone polynomial-like Boolean functions of n variables.*

Proof. The zero function, the one function of zero variables and the identity function of one variable $f_2^{(1)}(x_0) = x_0$ are polynomial-like monotone Boolean functions. As α_{2^n-1} is the only component with the value of 1 in the spectrum of the canonical disjunctive normal form of $f_{2^{2^n}-1}^{(n)}$ (and also in the spectrum of its Zhegalkin polynomial as $f_{2^{2^n}-1}^{(n)}$ is polynomial-like for any nonnegative integer n), this function is a monotone polynomial-like Boolean function. But f is polynomial-like if and only if $f \oplus f_{2^{2^n}-1}^{(n)}$ is polynomial-like, too, and in the spectra of these two functions differ only the components belonging to the greatest index, so at most one of the two functions can be monotone, if f is not the zero function.

Remark 1. Let g be an arbitrary Boolean function of n variables indexed from 0 to $n-1$ and let $f = x_n g \oplus h$ be the polynomial-like Boolean function of $n+1$ variables generated by g. $g \mapsto f$ is a one to one mapping of the set of the Boolean functions of n variables onto the set of the polynomial-like Boolean functions of $n+1$ variables. If g is nonmonotone, then f is nonmonotone, too. A Boolean function not preserving the 1 is nonmonotone with exception of the 0 function. Similarly, the Boolean functions containing all of the minterms with exception of at least one of those minterms having exactly one negated variable are nonmonotone, but one preserving if the polynomial is of at least two variables. The number of these latter type of the nonmonotone Boolean functions is $2^n - 1$. As half of the polynomial-like Boolean functions are not 1 preserving, and $2^n - 1 > 1$ if $n \geq 2$, so more than half of the polynomial-like Boolean functions of at least three variables are nonmonotone.

Theorem 6. *The closure of the set of the polynomial-like Boolean functions is the set of all of the Boolean functions.*

Proof. By the earlier results in the set of the polynomial-like Boolean functions there exist not 1 preserving functions, not self-dual functions, non-affine functions and nonmonotone functions, and the 1-function of zero variables is polynomial-like and it is not zero preserving, so the closure of the polynomial-like Boolean functions is the whole set B of the Boolean functions.

Remark 2. The previous theorem is a direct consequence of the fact that the 1 function of zero variables, the AND function and the EXCLUSIVE OR function of two variables are polynomial-like and the set of these three Boolean functions is a basis of the set B of all of the Boolean functions.

Corollary 2. *The set of the polynomial-like Boolean functions of n given variables is closed if and only if $n \leq 1$.*

Proof. The closure of the set of the 0 and the 1 function of zero variables, as well as the closure of the set of the 0 and the identity function of one variables are themselves, so these sets are closed for the superposition of functions from these sets. At the same time if $n \geq 2$, then $f^{(n)}_{2^{2^n}-2}$ and $f^{(n)}_{2^{2^n}-1}$ are polynomial-like. Substituting x_{n-1} by the latter function in $f^{(n)}_{2^{2^n}-2}$ we get

$$
\begin{aligned}
f^{(n)}_{2^{2^n}-2}\left(f^{(n)}_{2^{2^n}-1}, x_{n-2}, \ldots, x_0\right) &= \sum_{i=0}^{n-2} x_i + \prod_{i=0}^{n-1} x_i = \\
&= \sum_{i=0}^{n-2} \left(x_i + x_i \prod_{j=0}^{n-1} x_j \right) = \\
&= \sum_{i=0}^{n-2} x_i = f^{(n-1)}_{2^{2^{n-1}}-2}\left(x_{n-2}, \ldots, x_0\right)
\end{aligned} \tag{21}
$$

and then we can see that the Boolean function of n variables on the left side of the expression is degenerated in one of its variables, so this function is not polynomial-like.

Theorem 7. *For any $n \geq 3$ there exist polynomial-like Boolean functions which are simultaneously not* 1 *preserving, not self-dual, nonaffine and nonmonotone.*

Proof. All of the polynomial-like Boolean functions of more than two variables are zero preserving, not self-dual, nonaffine, and half of the polynomial-like Boolean functions of these variables are not 1 preserving, so if such a function is not the zero function, then it is nonmonotone. For instance for any n greater than 2 $f^{(n)}_{2^{2^n-1}-2}$ is a polynomial-like Boolean function and it is not the zero function, and as $2^{2^n-1} - 2 < 2^{2^n-1}$, so $\alpha_{2^n-1} = 0$ in the spectrum of the canonical disjunctive normal form of $f^{(n)}_{2^{2^n-1}-2}$. From this follows that $f^{(n)}_{2^{2^n-1}-2}$ is not 1 preserving.

Corollary 3. *There exists a basis of the set of Boolean functions containing two polynomial-like Boolean functions, from which one is the* 1 *function of zero variables.*

Proof. The 1 function of zero variables is a polynomial-like Boolean function not preserving the 0, but preserving the 1 for instance. From Theorem 7 it follows that there exist polynomial-like Boolean functions, which are not

1 preserving, not self-dual, nonaffine and nonmonotone, but these functions must be 0 preserving, so such a function in itself is not a basis, but with the 1 function of zero variables they can generate all of the Boolean functions.

Theorem 8. *The linear part of a polynomial-like Boolean function of n variables is either $l_f = 0$ or $l_f = \bigoplus_{i=0}^{n-1} x_i$. Exactly half of the polynomial-like Boolean functions of at least one variable belong to one of these two groups. The affine part of a Boolean function of at least one variable is equal to the linear part of that function.*

Remark 3. *Let $p = \bigoplus_{i=0}^{2^n-1} k_i S_i^{(n)}$ be the Zhegalkin-polynomial of the Boolean function f of n variables. Then $l_f = \bigoplus_{i=0}^{n-1} k_{2^i} x_i$ is the linear part of f, and the affine part of f is $a_f = k_0 \oplus l_f$.*

Proof. For $n = 0$ the statement is obviously true, so let $n > 0$. $f^{(n)}$ is polynomial-like if and only if its spectrum $\underline{\alpha}$ belongs to the linear space spanned by the columns of the matrix

$$\mathbf{U}^{(n)} = \begin{bmatrix} \mathbf{A}^{(n-1)} + \mathbf{I}^{(n-1)} \\ \mathbf{I}^{(n-1)} \end{bmatrix}. \tag{22}$$

In the rows of $\mathbf{A}^{(n-1)}$ belonging to the indices 2^k, where $n-1 > k \in \mathbf{N}_0$, $A^{(n-1)}_{2^k,0} = 1$ and $A^{(n-1)}_{2^k,2^k} = 1$, and $A^{(n-1)}_{2^k,j} = 0$ for any other $2^{n-1} > j \in \mathbf{N}$, so $A^{(n-1)}_{2^k,j} = 1$ is true in the matrix $\mathbf{A}^{(n-1)} + \mathbf{I}^{(n-1)}$ if and only if $j = 0$. Then it is true in $\mathbf{U}^{(n)}$, too, that $U^{(n)}_{2^k,l} = 1$ if and only if $l = 0$, where now $n > l \in \mathbf{N}_0$, as if $l < n-1$, then in $\mathbf{U}^{(n)}$ the rows with the indices of 2^l are the rows belonging to the indices of 2^l in the matrix $\mathbf{A}^{(n-1)} + \mathbf{I}^{(n-1)}$, and if $l = n-1$ then this row is the row of the identity matrix $\mathbf{I}^{(n-1)}$ indexed by 0. Now suppose $f^{(n)}$ is polynomial-like, and $\alpha_{2^r} = 1$ for a $0 \le r < n$. By the previous results it is possible only if $c_0 = 1$ in $\underline{\alpha} = \mathbf{U}^{(n)}\underline{c} = \sum_{i=0}^{2^{n-1}-1} c_i \underline{U}_i^{(n)}$. But in that case $\alpha_{2^t} = 1$ for all of $n > t \in \mathbf{N}_0$.

If in the spectrum $\underline{\alpha} = \mathbf{U}^{(n)}\underline{c}$ of the polynomial-like Boolean function f of n variables $c_0 = 0$, then the linear part of the function is the 0 function, while in the case when $c_0 = 1$ this linear part is equal to $\bigoplus_{i=0}^{n-1} x_i$. This means that exactly for half of the polynomial-like Boolean functions of n variables 0 is the linear part.

As a polynomial-like Boolean function with at least one variable is 0 preserving, the constant member in its Zhegalkin polynomial is 0, so the linear and the affine part of a polynomial-like Boolean function of at least one variable are equal.

Example 1. Let $n = 3$, then there are altogether $2^{2^{3-1}} = 16$ polynomial-like Boolean functions of three variables. These functions and their properties can be seen in Table 1. Now we can easily give all of the bases consisting of two functions of at most three variables. One of the two functions must be

Table 1.

the one-function of zero variables as this is the only polynomial-like Boolean function not preserving 0. Now we have to find polynomial-like Boolean functions of at most three variables having all of the further properties. The only one variable polynomial-like Boolean function is the identity function

which is 1-preserving. The zero function of two variables, the EXCLUSIVE OR function, the AND and the OR functions of two variables are the two variable polynomial-like Boolean functions. Three of them are monotone and the fourth, the EXCLUSIVE OR function is linear, so none of them can belong to a basis with two functions. The last eight functions in Table 1 are 1-preserving and the first is monotone, but each other function in Table 1 is suitable for our purpose as they are not 1-preserving, not self-dual, nonlinear and nonmonotone. Let us consider these functions. The set of these functions is $A = \left\{ f_{30}^{(3)}, f_{40}^{(3)}, f_{54}^{(3)}, f_{72}^{(3)}, f_{86}^{(3)}, f_{96}^{(3)}, f_{126}^{(3)} \right\}$.

$$
\begin{aligned}
f_{30}^{(3)} &= \overline{x}_2\overline{x}_1x_0 + \overline{x}_2x_1\overline{x}_0 + \overline{x}_2x_1x_0 + x_2\overline{x}_1\overline{x}_0 = \\
&= \overline{x}_2\left(\overline{x}_1x_0 + x_1\overline{x}_0 + x_1x_0\right) + x_2\overline{x}_1\overline{x}_0 = \\
&= \overline{x}_2\left(x_1 + x_0\right) + x_2\overline{x_1 + x_0} = x_2 \oplus \left(x_1 + x_0\right).
\end{aligned} \tag{23}
$$

As polynomial-like Boolean functions are invariant with respect to the permutations of their variables (see in [3]), and the above function is symmetrical in x_1 and x_0, so we have three different polynomial-like Boolean functions of the same form. The weight of these functions is four, and in A there are exactly three functions containing four 1's in their spectra, $f_{30}^{(3)}$, $f_{54}^{(3)}$ and $f_{86}^{(3)}$. The next function in A is $f_{40}^{(3)}$:

$$
\begin{aligned}
f_{40}^{(3)} &= \overline{x}_2x_1x_0 + x_2\overline{x}_1x_0 = \\
&= \left(\overline{x}_2x_1 + x_2\overline{x}_1\right)x_0 = \left(x_2 \oplus x_1\right)x_0
\end{aligned} \tag{24}
$$

and again we have three similar functions, namely $f_{40}^{(3)}$, $f_{72}^{(3)}$ and $f_{96}^{(3)}$. Finally $f_{126}^{(3)}$ is a function the weight of which is equal to 6 and this is the only fuction in A with this property. (By the proof of Theorem 7 the n-variable $f_{2^{2^n-1}-2}^{(n)}$ is always polynomial-like, if $n \geq 3$, and now $n = 3$, so $2^{2^n-1} - 2 = 126$). Now

$$
f_{126}^{(3)} = \overline{\overline{x}_2\overline{x}_1\overline{x}_0 + x_2x_1x_0} = \left(\overline{x}_2 + \overline{x}_1 + \overline{x}_0\right)\left(x_2 + x_1 + x_0\right). \tag{25}
$$

Altogether we have three different classes containing seven different bases consisting of two polynomial-like Boolean functions of at most three variables, more exactly consisting of a zero variable and a three variable polynomial-like Boolean function. These bases are shown in Table 2.

$$\left\{f_1^{(0)}, f_{30}^{(3)}\right\} = \{1, x_2 \oplus (x_1 + x_0)\}$$
$$\left\{f_1^{(0)}, f_{40}^{(3)}\right\} = \{1, (x_2 \oplus x_1)\, x_0\}$$
$$\left\{f_1^{(0)}, f_{54}^{(3)}\right\} = \{1, x_1 \oplus (x_0 + x_2)\}$$
$$\left\{f_1^{(0)}, f_{72}^{(3)}\right\} = \{1, (x_0 \oplus x_2)\, x_1\}$$
$$\left\{f_1^{(0)}, f_{86}^{(3)}\right\} = \{1, x_0 \oplus (x_2 + x_1)\}$$
$$\left\{f_1^{(0)}, f_{96}^{(3)}\right\} = \{1, (x_1 \oplus x_0)\, x_2\}$$
$$\left\{f_1^{(0)}, f_{126}^{(3)}\right\} = \{1, (\overline{x}_2 + \overline{x}_1 + \overline{x}_0)\,(x_2 + x_1 + x_0)\}$$

Table 2.

3. Conclusion

Although there are infinitely many Boolean functions, but the minimal generating systems, the bases of them are always finite and contain at most four functions. In the article above we pointed out that there are bases containing only polynomial-like Boolean functions and among such bases we can find two element ones, too. As all of the nonconstant polynomial-like Boolean functions are zero-preserving, there is no basis containing only one polynomial-like Boolean function, but one of the two functions of a basis consisting of two polynomial-like Boolean functions is always the simplest possible, namely the constant 1-function of zero variables. There are infinitely many such bases, as for instance $\{1, f_{2^{2^n-1}-2}^{(n)}\}$ is a basis for any integer $n \geq 3$ (see Theorem 7).

References

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

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

[3] **Gonda J.,** Polynomial-like Boolean functions, *Annales Univ. Sci. Budapest. Sect. Comp.,* **25** (2005), 13-23.

[4] **Gonda J.,** Some properties of polynomial-like Boolean functions, *Annales Univ. Sci. Budapest. Sect. Comp.,* **26** (2006), 17-24.

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

[6] **Post E.L.,** *The two-valued iterative systems of mathematical logic,* Annals of Mathematics Studies **5**, Princeton University Press, Princeton, N.J., 1941.

[7] **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 December 9, 2005)

J. Gonda
Department of Computer Algebra
Eötvös Loránd University
H-1117 Budapest, P.O.B. 32
andog@compalg.inf.elte.hu