Annales Univ. Sci. Budapest., Sect. Comp. 52 (2021) 147–161

SOME RESULTS ON HOMOGENEOUS SYMMETRIC POLYNOMIAL-LIKE BOOLEAN FUNCTIONS

János Gonda (Budapest, Hungary)

Communicated by Imre Kátai

(Received April 27, 2021; accepted July 29, 2021)

Abstract. 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. Another special set of the Boolean-functions are the set of the symmetric functions. In earlier articles we introduced the class of the symmetric polynomial-like Boolean functions, investigated some elementary properties of such functions and dealt with the special case of the homogeneous symmetric polynomial-like Boolean functions. One of our results determined the integers n for a given nonnegatíve integer k so that the Boolean function belonging to $p^{(n;k)}$ is polynomial-like. Now we continue the investigation of the homogeneous symmetric polynomial-like Boolean functions, and among others we deal with the reverse problem, that is, we determine the number of the homogeneous symmetric, n-indeterminate polynomials for which the Boolean functions are polynomial-like.

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; $\mathbb{N}$ denotes the non-negative integers, and $\mathbb{N}^+$ the positive ones.

Key words and phrases: Boolean function, normal form, Zhegalkin polynomial, polynomial-like Boolean function, symmetric polynomial, symmetric function, homogeneous polynomial.
2010 Mathematics Subject Classification: Please use the *06E30, 94C10, 15A18.*
https://doi.org/10.71352/ac.52.147

1. Introduction

Logical functions and especially the two-valued ones have important role in our everyday life, so it is easy to understand why they are widely investigated. A scope of the investigations is the representations of these functions and the transforms from one representation to another ([3], [4], [5]). 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 [12], but there are a lot of other classes of the Boolean functions invariant with respect to some property. Such properties can be for example linear transforms. In [6] the author of the present paper introduced a class of the Boolean functions invariant under a special linear transform. The functions of that class are called polynomial-like Boolean functions. An important subclass in this class is the set of the symmetric functions, and within this, as a narrower subset, the collection of the homogeneous symmetric polynomial-like Boolean functions. In general, we dealt with the symmetric polynomial-like Boolean functions in [8] and then with the homogeneous case in [9]. In that article Theorem 2.4. has given the integers n for which $p^{(n,k)}$ is polynomial with the given nonnegative integer k. Further results on homogeneous functions are presented in this paper. One of our present results gives for a given nonnegative integers n the number of the n-indeterminate homogeneous symmetric polynomials belonging to polynomial-like Boolean functions.

1.1. Represantations 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 each of such logical products contains 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 to 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 $\alpha_i^{(l)} \in \{0, 1\}$

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

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

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

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 $\mathbb{F}_2$, 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

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

(this form of the matrix shows that for every $n \in \mathbb{N}$, $\mathbf{A}^{(n)}$ 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

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

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

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.

1.2. 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

$$\begin{pmatrix} \underline{u}_0 \\ \underline{u}_1 \end{pmatrix} = \begin{pmatrix} \mathbf{A}^{(n)} & \mathbf{0}^{(n)} \\ \mathbf{A}^{(n)} & \mathbf{A}^{(n)} \end{pmatrix} \begin{pmatrix} \underline{u}_0 \\ \underline{u}_1 \end{pmatrix} \tag{1.8}$$

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

$$\begin{pmatrix} \mathbf{A}^{(n)} + \mathbf{I}^{(n)} \\ \mathbf{I}^{(n)} \end{pmatrix}. \tag{1.9}$$

1.3. Symmetric functions and symmetric polynomials

Let $n \in \mathbb{N}$, let X and Y be sets, $f : X^n \to Y$ and π an arbitrary element of the symmetric group S_n. The function f is symmetric, if for any $(u_0, \cdots, u_i, \cdots, u_{n-1}) \in X^n$

$$f(u_0, \cdots, u_i, \cdots, u_{n-1}) = f\left(u_{\pi(0)}, \cdots, u_{\pi(i)}, \cdots, u_{\pi(n-1)}\right). \tag{1.10}$$

If $\mathcal{K}$ is a field, and $p \in K[x_0, \cdots, x_i, \cdots, x_{n-1}]$, then p is a symmetric polynomial over $\mathcal{K}$, if

$$p = p \circ \left(x_{\pi(0)}, \cdots, x_{\pi(i)}, \cdots, x_{\pi(n-1)}\right), \tag{1.11}$$

where $\circ$ denotes the composition.

Now the Boolean function f is symmetric if and only if its Zhegalkin-polynomial is symmetric.

The polynomial function for a symmetric polynomial is a symmetric function, but the converse is not necessarily true. There are infinitely many polynomials with the same polynomial function over a finite field, most of which are not symmetric even when the corresponding polynomial function is symmetric. For example, the polynomial function for the polynomials $p^{(1)} = x_0x_1^2$ and $p^{(2)} = x_0x_1$ over the field of two elements is the symmetric function $\hat{p} = x_0x_1$, but $p^{(1)}$ is not a symmetric polynomial, since $p^{(1)} = x_0x_1^2 \neq x_0^2x_1 = p^{(3)}$.

It is worth to mention that if k is a nonnegative integer and $k \leq n \in \mathbb{N}$, then the k-degree homogeneous symmetric Zhegalkin-polynomial in n indeterminates is the k-degree elementary symmetric polynomial in n indeterminates over $\mathbb{F}_2$ (see Theorem 1.2. in [8]).

By this result we can determine a homogeneous symmetric Zhegalkin-polynomial by fixing the number of the indeterminates and the degree of the polynomial, that is by the ordered pair of $(n;k)$ where n is the number of the indeterminates and k is the degree of the monomials occuring in the polynomial. Similarly, if A is a set of nonnegative integers not greater than n then $(n;A)$ determines a symmetric Zhegalkin-polynomial containing the k-degree monomial if and only if $k \in A$.

Let n be a nonnegative integer, $n \geq k \in \mathbb{N}$ and A is a subset of the nonnegative integers not greater than n. Then $p^{(n;k)}$ is the k-degree homogeneous symmetric Zhegalkin-polynomial in n indeterminates and $p^{(n;A)} = \sum_{k \in A} p^{(n;k)}$.

As $2a = 0$ for any $a \in \mathbb{F}_2$, so $p^{(n;A_1)} + p^{(n;A_2)} = p^{(n;A_1 \Delta A_2)}$, where Δ denotes the symmetric difference, that is, $A_1 \Delta A_2 = (A_1 \cap \bar{A}_2) \cup (\bar{A}_1 \cap A_2)$.

If $p^{(n;k)}$ is polynomial-like, then the Boolean-function f belonging to that polynomial is the logical sum of the minterms containing exactly $n-k$ negated variables, as the spectra of the function and the polynomial are identical.

It is easy to see that for any $n \in \mathbb{N}$ the n-variable AND-function is polynomial-like and symmetric, so for any $n \in \mathbb{N}$ there is at least one symmetric polynomial-like n-variable Boolean function.

For any $n \in \mathbb{N}$ the spectra of the symmetric polynomial-like Boolean functions of n-variables form a linear space.

According to Corollary 2.1. and Theorem 2.4. in [8] for any $3 \leq n \in \mathbb{N}$ the collection of the symmetric polynomial-like Boolean functions is a proper subspace of the space of the polynomial-like Boolean functions.

2. Homogeneous symmetric polynomial-like Boolean functions

This section is based on the results contained in [9].

In the following, unless we say otherwise, polynomial means a polynomial over $\mathbb{F}_2$ of degree at most one in every indeterminate, and if p is the Zhegalkin polynomial of a polynomial-like Boolean function then also the polynomial itself is called as polynomial-like. The zero polynomial has no degree.

The next two statements are straightforward so we omit the proofs.

Theorem 2.1. *Let n be a nonnegative integer. The degree of the Zhegalkin polynomial of an n-variable $f \neq 0$ Boolean function is at most n.*

Theorem 2.2. *For every nonnegative integer n the Boolean function belonging to the homogeneous Zhegalkin polynomial of degree n in n indeterminates is polynomial-like.*

Theorem 2.3. *Let k be a nonnegative integer and let $k \leq n \in \mathbb{N}$. If the Boolean function of a homogeneous symmetric Zhegalkin-polynomial of degree k in n indeterminates is not polynomial-like then the Boolean function of a homogeneous symmetric Zhegalkin-polynomial of degree k in $n+1$ indeterminates is not polynomial-like, either.*

Proof. If the polynomial $0 \neq p = p^{(0)} + x_n p^{(1)}$ in $n+1$ indeterminates, where $p^{(0)}$ and $p^{(1)}$ are polynomials of the indeterminates $x_0, \ldots, x_{n-1}$, is

- a polynomial of degree $n \geq k$, then $p^{(0)}$ is a polynomial of degree at most k, as every term of p and then every term of $p^{(0)}$, too, is of degree maximum k;
- homogeneous, then also $p^{(0)}$ is homogeneous, because $p^{(0)}$ and $x_n p^{(1)}$ have no common terms;
- symmetric, then $p^{(0)}$ is symmetric, too, since for any permutation of the indeterminates $x_0, \cdots, x_{n-1}$ there is no common term in $p^{(0)}$ and $x_n p^{(1)}$;
- the Zhegalkin polynomial of an $n+1$-variable polynomial-like Boolean function, then $p^{(0)}$ is the Zhegalkin polynomial of an n-variable polynomial-like Boolean function. Indeed, if the spectrum of p is $\mathbf{u} = \begin{pmatrix} \mathbf{u}^{(0)} \\ \mathbf{u}^{(1)} \end{pmatrix}$, where $\mathbf{u}^{(0)}$ is the vector composed of the first 2^n components of $\mathbf{u}$, then $\mathbf{u}^{(0)}$ and $\mathbf{u}^{(1)}$ is the spectrum of $p^{(0)}$ and $p^{(1)}$, respectively. If p is polynomial-like, then from $\begin{pmatrix} \mathbf{u}^{(0)} \\ \mathbf{u}^{(1)} \end{pmatrix} = \mathbf{u} = \mathbf{A}^{(n+1)}\mathbf{u} = \begin{pmatrix} \mathbf{A}^{(n)} & \mathbf{0}^{(n)} \\ \mathbf{A}^{(n)} & \mathbf{A}^{(n)} \end{pmatrix} \begin{pmatrix} \mathbf{u}^{(0)} \\ \mathbf{u}^{(1)} \end{pmatrix}$ follows that $\mathbf{u}^{(0)} = \mathbf{A}^{(n)}\mathbf{u}^{(0)}$, so $p^{(0)}$ is polynomial-like.

Based on the above properties, if p is an $n+1$ indeterminate k-degree homogeneous symmetric polynomial which is the Zhegalkin polynomial of an $n+1$-variable polynomial-like Boolean function, then $p^{(0)}$ is a k-degree homogeneous symmetric polynomial in n indeterminates belonging to an n-variable polynomial-like Boolean function. From this follows that the theorem holds. ■

Corollary 2.1. *If for an integer n not less than the nonnegative integer k the Boolean function belonging to a k-degree homogeneous symmetric Zhegalkin-polynomial in n indeterminates is not polynomial-like and $n \leq m$ is an integer then the Boolean function belonging to a k-degree homogeneous symmetric Zhegalkin-polynomial in m indeterminates is not polynomial-like, either.*

Proof. It follows immediately from the previous theorem by induction on m. ■

Definition 2.1. Let $n \in \mathbb{N}$ and $2^n > i \in \mathbb{N}$. i can be written in a unique way in the form $i = \sum_{l=0}^{n-1} i_l 2^i$ where for any nonnegative index l less then n $i_l \in \{0,\ 1\}$ and $i_0 \cdots i_{n-1} = \mathbf{i} \in \{0,\ 1\}^n$. Then $w(\mathbf{i}) = w(i) = \sum_{l=0}^{n-1} i_l$ is the weight of i and $\mathbf{i}$ covers the vector $j_0 \cdots j_{n-1} = \mathbf{j} \in \{0,\ 1\}^n$ belonging to the nonnegative integer $2^n > \sum_{l=0}^{n-1} j_l = j$, if for each of the indices l $i_l \geq j_l$. The fact that $\mathbf{i}$ covers $\mathbf{j}$ is denoted by $\mathbf{i} \succcurlyeq \mathbf{j}$. In the case of $\mathbf{i} \succcurlyeq \mathbf{j}$ we also say that i covers j.

Remark 2.1. If $n \in \mathbb{N}$, $2^n > i \in \mathbb{N}$, $2^n > j \in \mathbb{N}$ and $\mathbf{i} \succcurlyeq \mathbf{j}$, then $i \geq j$ and $w(i) \geq w(j)$, since under the given conditions $i = \sum_{l=0}^{n-1} i_l 2^l \geq \sum_{l=0}^{n-1} j_l 2^l = j$ and $w(i) = \sum_{l=0}^{n-1} i_l \geq \sum_{l=0}^{n-1} j_l = w(j)$.

One of the main results of [9] is the following theorem.

Theorem 2.4. *Let n be a nonnegative integer and let $n \geq k \in \mathbb{N}$. Then $p^{(n;k)}$ is polynomial-like if and only if $\binom{w}{k}$ is an even number for every integer $k < w \leq n$.*

Proof. $p^{(n;k)}$ is polynomial-like if and only if $\mathbf{u} = \mathbf{A}\mathbf{u}$, where $\mathbf{u}$ is the spectrum of the polynomial, that is, if $u_i = v_i = (\mathbf{A}\mathbf{u})_i = \sum_{j=0}^{2^n-1} a_{i,j} u_j = \sum_{j=0}^{i} a_{i,j} u_j$ for every nonnegative integer i less than 2^n. The i-th component u_i of $\mathbf{u}$ belonging to $p^{(n;k)}$ is equal to 1 if and only if $w(i) = k$ and $a_{i,j} = 1$ exactly in the case when i covers j (see the Corollary in [5]). By the Remark above $i \geq j$ if $\mathbf{i} \succcurlyeq \mathbf{j}$. Depending from the weight of i we have to distinguish three cases:

1. if $w_i = w(i) < k$, then $u_i = 0$, furthermore if $u_j = 1$ then $a_{i,j} = 0$, so in that case $a_{i,j} u_j = 0$ for every $0 \leq j \leq i$, and then $v_i = \sum_{j=0}^{i} a_{i,j} u_j = 0 = u_i$;

2. if $w_i = w(i) = k$ then there exists one and only one nonnegative integer j not greater than i that $u_j = 1$ and $a_{i,j} = 1$, namely $j = i$, so now in the sum $\sum_{j=0}^{i} a_{i,j} u_j$ there is exactly one nonzero member, $a_{i,i} u_i$, therefor $v_i = \sum_{j=0}^{i} a_{i,j} u_j = a_{i,i} u_i = 1 = u_i$;

3. finally let i be such an integer that $w_i = w(i) > k$. Then there are $\binom{w_i}{k}$ such index j, that $\mathbf{i} \succcurlyeq \mathbf{j}$ and $w_j = w(j) = k$, and then $v_i = \sum_{j=0}^{i} a_{i,j} u_j = \sum_{\mathbf{i} \succcurlyeq \mathbf{j}} u_j = \sum_{\mathbf{i} \succcurlyeq \mathbf{j}} 1 = 0 = u_i$ if and only if $\binom{w_i}{k}$ is an even number. ■

Corollary 2.2. *Let n be a nonnegative integer. Then*

1. *$p^{(n;0)}$ is polynomial-like if and only if $n = 0$;*

2. $p^{(n;n)}$ *is polynomial-like for every nonnegative integer* n*;*

3. $p^{(n+1;n)}$ *is polynomial-like if and only if* n *is an odd number.*

Proof. 1. $w_i = w(i) = 0$ if and only if $i = 0$. Now there is no such i, that $w(i) < 0$, and if $n > 0$, then for instance $\binom{n}{0} = 1$ is not an even number;

2. the weight of the index of a term of a Zhegalkin-polynomial is equal to the number of the indeterminates occuring in that term so an n-indeterminate Zhegalkin polynomial has no member with index $2^n > i \in \mathbb{N}$ such that $w_i = w(i) > n$;

3. in this case it is only true for $n+1$ that $w(i) > n$, and $\binom{n+1}{n} = \binom{n+1}{1} = n+1$ is even exactly in the case when n is odd. ■

Another important result is the next theorem.

Theorem 2.5. *Let* l *be a positive and* t *a nonnegative integer and let* $k = 2^l(2t+1) - 1$. *Then* $p^{(n;k)}$ *is polynomial-like, if* $k \leq n < k + 2^l$, *and* $p^{\left(k+2^l;k\right)}$ *is not polynomial-like.*

Proof. By the previous theorem the only thing to prove is that $\binom{w}{k}$ is an even number if $k < w \leq n < k + 2^l$ but $\binom{k+2^l}{k}$ is an odd number.

Let $2^l \geq r = 2^u(2v+1)$ be a positive integer. r uniquely determines the nonnegative integers u and v. $2^l \geq 2^u(2v+1)$ and $2v+1 \geq 1$ imply that $u \leq l$, and $u = l$ is equivalent to the case that $r = 2^l$. If $w = k + r$ then

$$\binom{w}{k} = \binom{k+r}{k} = \binom{k+r}{r} = \tag{2.1}$$
$$= \frac{\prod_{i=1}^{r}(k+i)}{\prod_{i=1}^{r} i} = \frac{\prod_{i=0}^{r-1}((k+1)+i)}{\prod_{i=1}^{r} i} = \frac{k+1}{r}\prod_{i=1}^{r-1}\frac{(k+1)+i}{i}.$$

Let us write the positive integer i less than r in the form $r = 2^{p_i}(2q_i+1)$. Now $l > p_i \in \mathbb{N}$. Then

$$\frac{k+1}{r} = 2^{l-u}\frac{2t+1}{2v+1}, \tag{2.2}$$

$$\frac{(k+1)+i}{i} = \frac{2^l\,(2t+1)+2^{p_i}\,(2q_i+1)}{2^{p_i}\,(2q_i+1)} = \tag{2.3}$$
$$= \frac{2\left(2^{l-p_i-1}\,(2t+1)+q_i\right)+1}{2q_i+1} = \frac{2w_i+1}{2q_i+1},$$

so

$$\binom{w}{k} = 2^{l-u}\frac{2t+1}{2v+1}\prod_{i=1}^{r-1}\frac{2w_i+1}{2q_i+1} = 2^{l-u}\frac{(2t+1)\prod_{i=1}^{r-1}(2w_i+1)}{(2v+1)\prod_{i=1}^{r-1}(2q_i+1)}. \tag{2.4}$$

Both the numerator and the denominator of the fraction are products of odd integers, so both the numerator and the denominator are odd integers. The binomial coefficient is an integer and the denominator of the fraction is relative prime to 2^{l-u}, hence itself the fraction is an integer. From this follows that $\binom{w}{k}$ is odd for the given w and k if and only if $u = l$, that is, when $r = 2^l$. ■

Theorem 2.6. *Let p be a Zhegalkin polynomial of $x_0, \cdots, x_{n-1}, x_n$ and let $p = p^{(0)} + x_n p^{(1)}$ where $p^{(0)}$ and $p^{(1)}$ are Zhegalkin polynomials of the indeterminates $x_0, \cdots, x_{n-1}$. Then $p = p^{(n+1;k)}$ if and only if $k = 0$, $k = n+1$, or $0 < k \leq n$ and $p^{(0)} = p^{(n;k)}$ and $p^{(1)} = p^{(n;k-1)}$.*

Proof. With the cases $k = 0$ and $k = n+1$ we dealt earlier. Let $0 < k \leq n$ and $p = p^{(n+1;k)}$. We know that in this case $p^{(0)} = p^{(n;k)}$. Now $p^{(n+1;k)}$ is the sum of the k-degree monomials of the $n+1$ indeterminates not containing any other terms. These monomials either contain x_n or not in a mutually exclusive manner. The sum of the latter is the set of the k-degree monomials of the indeterminates $x_0, \cdots, x_{n-1}$, and their sum is $p^{(n;k)}$. Each of the other monomials is the product of x_n and one and only one monomial of degree $k-1$ of the other indeterminates and all of these monomials are in p, so their sum is $x_n p^{(n;k-1)}$. Conversely, if $p = p^{(n;k)} + x_n p^{(n;k-1)}$, then each member of $p^{(n;k)}$ and $x_n p^{(n;k-1)}$ is a k-degree monomial of the $n+1$ indeterminates, and each of such monomial is a member of one of the two preceding polynomials, so $p = p^{(n+1;k)}$. ■

3. New results

The following theorem is a synthesis of some previous results.

Theorem 3.1. *Let k be an even nonnegative integer and n be an arbitrary natural number not less than k. Then $p^{(n;k)}$ is polynomial-like if and only if $n = k$.*

Proof. According to 2. in Corollary 2.2 $p^{(k;k)}$ is polynomial-like for each natural number k. On the other hand, by 3. in the same Corollary, $p^{(k+1;k)}$

is polynomial-like if and only if k is odd. According to Theorem 2.3, if $p^{(n;k)}$ is not polynomial-like, then $p^{(n+1;k)}$ is not polynomial-like either, and then for every $m \geq n$, according to Corollary 2.1, $p^{(m;k)}$ is not polynomial-like. ■

According to the above theorem, for an even natural number k there is one and only one natural number n, with which $p^{(n;k)}$ is polynomial-like.

Corollary 3.1. *If $p^{(n;k)}$ is polynomial-like with the natural numbers k and n greater than k, then k is odd.*

Proof. If k is an even natural number and n is a natural number greater than k, then $p^{(n;\ k)}$ cannot be polynomial-like by the former theorem. ■

The following theorem is also a rewording of a previous result.

Theorem 3.2. *Let k be an odd natural number such that $2^l \big| k+1$, but $2^{l+1} \nmid k+1$. Then the number of the natural numbers n for which $p^{(n;k)}$ is polynomial-like is 2^l.*

Proof. According to Theorem 2.5 $p^{(n;k)}$ is polynomial-like for $k \leq n < k+2^l$, but $p^{(k+2^l;k)}$ is not polynomial-like, so the number of the natural numbers n for which $p^{(n;k)}$ is polynomial-like equal to the number of the integers in the interval $\big[k, k+2^l\big[$. ■

Theorem 3.3. *Let n be odd and $k \leq n$ natural numbers. Then $p^{(n+1;k)}$ is polynomial-like if and only if $p^{(n;k)}$ is polynomial-like.*

Proof. If $p^{(n;k)}$ is not polynomial-like, then by Theorem 2.3 $p^{(n+1;k)}$ is not polynomial-like either. Let's look at the other case. If n is odd, $n \geq k$ and $p^{(n;\ k)}$ is polynomial-like, then k is also odd: if $n = k$, then it is obvious, and if $n > k$, then this is true according to Theorem 3.1. Then k can be written in the form $k = 2^l(2v+1) - 1$, where l is a positive and v is a non-negative integer. According to Theorem 2.5 $p^{(n;k)}$ is polynomial-like for $k \leq n < k+2^l$, but $p^{(k+2^l;k)}$ is not polynomial-like, and thus, based on previous results $p^{(n;k)}$ is polynomial-like if and only if $k \leq n < k+2^l$. Now we assume that $p^{(n;k)}$ is polynomial-like, so $k \leq n < k+2^l$. k is odd, 2^l is even, since $l > 0$, so $k+2^l$ is odd. But $n < k+2^l$ and n are odd, so $n+1$ is even, so even $n+1$ is smaller than $k+2^l$, and consequently $p^{(n+1;k)}$ is polynomial-like. ■

Corollary 3.2. *Let n be odd and k not greater than n natural numbers. Then the number of the homogeneous symmetric polynomial-like Boolean functions in $n+1$ indeterminates is one greater than the number of the n-indeterminate homogeneous symmetric polynomial-like Boolean functions.*

Proof. According to the above theorem, the set of the degrees of the homogeneous symmetric Zhegalkin polynomials of degree not greater than n belonging to the $n+1$ variable homogeneous symmetric polynomial-like Boolean functions is equal to the set of the degrees of the homogeneous symmetric Zhegalkin polynomials belonging to the n-variable Boolean functions. But in addition, there is only one $n+1$ indeterminate homogeneous Zhegalkin polynomial, $p^{(n+1;n+1)}$, and this is symmetric and defines a polynomial-like Boolean function, so the number of the polynomials $p^{(n+1;k)}$ is indeed one greater than the number of the n-indeterminate polynomials with this property. ■

Theorem 3.4. *Let $l \in \mathbb{N}^+$, $t \in \mathbb{N}$, $n = 2^l(2t+1) - 1$ and $n+1 = \sum_{i=l}^{l+m} a_i 2^i$, where $m \in \mathbb{N}$, $a_{l+m} = 1$ and for all integers $l < i < l+m$, $a_i \in \{0,1\}$. Then for $k \in \mathbb{N}$ $p^{(n;k)}$ is a polynomial-like Boolean function if and only if $k+1 = \sum_{i=l+r}^{l+m} a_i 2^i$ with an $m \geq r \in \mathbb{N}$ such that $a_{l+r} = 1$.*

Proof. $n+1 = 2^l(2t+1)$ and $l \in \mathbb{N}^+$, so $a_l = 1$. If $k > n$, then $p^{(n;k)}$ does not exist, and due to $n > 0$, $p^{(n;0)}$ is not polynomial-like. Since n is odd, so even for even k there is no polynomial-like $p^{(n;k)}$, so we can assume that $0 < k \leq n$ is odd. $p^{(n;n)}$ is polynomial-like, and then $k+1 = n+1 = \sum_{i=l}^{l+m} a_i 2^i = \sum_{i=l+0}^{l+m} a_i 2^i$. But we have already seen that $a_{l+0} = a_l = 1$, and $m \geq 0 \in \mathbb{N}$, that is, for $k = r = 0$, $p^{(n;k)}$ is polynomial-like. Hereinafter, $k < n$. Then $k+1 < n+1$, and in the binary expansions the leftmost bit in k where k and n differ, 0, so $k+1 = \sum_{i=l}^{l+r-1} b_i 2^i + 0 \cdot 2^{l+r} + \sum_{i=l+r+1}^{l+m} a_i 2^i$ with a positive integer r not greater than m for which $a_{l+r} = 1$. We have previously seen that if $k = 2^{l'}(2t'+1) - 1$, then with $n > k$, $p^{(n;k)}$ is polynomial-like if and only if $n < k + 2^{l'}$. If $b = \sum_{i=l}^{l+r-1} b_i 2^i = 0$, then $l' \geq l + r + 1$, and

$$k+1+2^{l'} \geq k+1+2^{l+r+1} > \sum_{i=l}^{l+r} a_i 2^i + \sum_{i=l+r+1}^{l+m} a_i 2^i = n+1, \tag{3.1}$$

that is, $p^{(n;k)}$ is polynomial-like. In the other case, $b \neq 0$. Then $0 < l' < l+r$ (because $k+1$ is even), $b = \sum_{i=l'}^{l+r-1} b_i 2^i$, and consequently

$$\begin{aligned} k+1+2^{l'} = b + \sum_{i=l+r+1}^{l+m} a_i 2^i + 2^{l'} \leq \sum_{i=l'}^{l+r-1} 2^i + 2^{l'} + \sum_{i=l+r+1}^{l+m} a_i 2^i = \\ = 2^{l+r} + \sum_{i=l+r+1}^{l+m} a_i 2^i \leq \sum_{i=l}^{l+m} a_i 2^i = n+1 \end{aligned} \tag{3.2}$$

so now $p^{(n;k)}$ is not polynomial-like. ■

Theorem 3.5. *Let n be an odd natural number. The number of the n-variable nonzero homogeneous symmetric polynomial-like Boolean functions is $w(n+1)$.*

Proof. Let $n = 2^l(2t+1)-1$, where $l \in \mathbb{N}^+$ and $t \in \mathbb{N}$, and let $w(n+1) = q$. Then, by the previous theorem, the number of the n-variable nonzero homogeneous symmetric polynomial-like Boolean functions is equal to the number of the one's in $n+1 = \sum_{i=l}^{l+m} a_i 2^i$. ■

A direct consequence of the theorem is the following corollary.

Corollary 3.3. *Let l be a positive integer. Then the number of the nonzero n-indeterminate homogeneous symmetric polynomial-like Boolean functions is equal to 1 if $n = 2^l - 1$ and to l in the case when $n = 2^{(l+1)} - 3$.*

Proof. $n+1 = 2^l = 1\underbrace{0\ldots0}_{l}$ and $n+1 = 2^{(l+1)} - 2 = \underbrace{1\ldots1}_{l}0$, so $w(2^l) = 1$ and $w(2^{(l+1)} - 2) = l$. ■

Example 3.6. Now we consider some homogeneous symmetric polynomial-like Boolean functions. First, we give such functions by Theorem 2.5 supposing that n is odd.

1. If $k = 1, 5, 9, 13$ then $p^{(n;k)}$ is symmetric and polynomial-like if and only if $n = k$, as now $k = 2^1(2u+1)-1$;
2. if $k = 3, 11$ then $p^{(n;k)}$ is symmetric and polynomial-like if and only if $n = k$ or $n = k+2$, as in this case $k = 2^2(2u+1)-1$;
3. if $k = 7$ then $k = 2^3(2\cdot0+1)-1$, so $p^{(n;k)}$ is symmetric and polynomial-like if $n = 7, 9, 11, 13$ and not polynomial-like, when $n > 13$.

It follows from the previous list that for $n = 7, 9, 13$ $p^{(7;7)}$, $p^{(9;7)}$, $p^{(9;9)}$, $p^{(13;7)}$, $p^{(13;11)}$ and $p^{(13;13)}$ are the homogeneous polynomial-like Boolean functions.

The homogeneous symmetric polynomial-like Boolean functions for n = 7,9,13 are then determined using the results found in this paper.

1. Let $n = 7$. Then $n+1 = 8 = 2^3 = 1000_{(2)}$, $w(n+1) = 1$, and the only nonzero homogeneous symmetric polynomial-like Boolean function in 7 indeterminates is $p^{(7;7)} = \prod_{i=0}^{6} x_i$ (now $k = 7$ and $k+1 = 8 = 1000_{(2)}$).
2. Let $n = 13$. Then $n+1 = 14 = 2^4-2 = 1110_{(2)}$, $w(n+1) = 3$, and the 13-indeterminate nonzero homogeneous symmetric polynomial-like Boolean functions are

- $p^{(13;7)} = \sum_{I\subset A,|I|=7} \prod_{i\in I} x_i$ (now $k+1 = 8 = 1000_{(2)}$);
- $p^{(13;11)} = \sum_{I\subset A,|I|=11} \prod_{i\in I} x_i$ ($k+1 = 12 = 1100_{(2)}$);
- $p^{(13;13)} = \prod_{i=0}^{12} x_i$ ($k+1 = 14 = 1110_{(2)}$);

where A is the set of the nonnegative integers less than 13.

3. Let $n = 9$. Then $n+1 = 10 = 1010_{(2)}$, $w(n+1) = 2$, and the 9-indeterminate nonzero homogeneous symmetric polynomial-like Boolean functions are

- $p^{(9;7)} = \sum_{I\subset A,|I|=7} \prod_{i\in I} x_i$ ($k+1 = 8 = 1000_{(2)}$);
- $p^{(9;9)} = \sum_{I\subset A,|I|=9} \prod_{i\in I} x_i$ ($k+1 = 10 = 1010_{(2)}$).

where A is the set of the nonnegative integers less than 9.

As we can see, the sets of functions defined in the two ways are the same, the two calculation methods led to the same result.

There are many interesting questions about symmetric polynomial-like Boolean functions. For example, for a given $n \in \mathbb{N}$, n-indeterminate homogeneous symmetric polynomial-like Boolean functions generate a linear space. In this article, we have considered these functions on their own, so it may be worthwhile to examine the space itself in the future.

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. Comp.*, **20** (2001), 147–156.

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

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

[8] **Gonda, J.,** Symmetric polynomial-like Boolean functions, *Annales Univ. Sci. Budapest., Sect. Comp.*, **49** (2019), 209–218.

[9] **Gonda, J.,** Homogeneous symmetric polynomial-like Boolean functions, *Annales Univ. Sci. Budapest., Sect. Comp.*, **51** (2020), 97–110.

[10] **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.

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

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

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