Annales Univ. Sci. Budapest., Sect. Comp. 26 (2006) 17-24

SOME PROPERTIES OF POLYNOMIAL–LIKE BOOLEAN FUNCTIONS

J. Gonda (Budapest, Hungary)

Abstract. In [3] a linear algebraic aspect is given for the transformation of a Boolean function to its Zhegalkin representation, and in [4] we determined the eigenvectors of that transform. In [5] we introduced the notion of the polynomial-like Boolean functions as the Boolean functions belonging to the eigenvectors of the transform mentioned above. In this article some simple properties of that type of Boolean functions are given.

In this article the elements of the field with two elements are denoted by 0 and 1; $\mathbf{N}_0$ denotes the non-negative integers, and $\mathbf{N}$ the positive ones.

In [3] we pointed out that if we consider the coefficients of a Boolean function of n variables and the coefficients of the Zhegalkin polynomial of n variables, respectively, as the components of an element of a 2^n-dimensional linear space over $\mathbf{F}_2$, then the relation between the vectors belonging to the two representations of the same Boolean function of n variables could 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 Boolean representation of the given function, and $\mathbf{A}^{(n)}$ is the matrix of the transform in the natural basis. In the article mentioned above it is proved that

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

and as consequence that

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

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 [4] it is pointed out that the minimal polynomial of $\mathbf{A}^{(n)}$ is λ^2+1, except for the case of $n=0$, when the minimal polynomial is equal to $\lambda+1$. The only eigenvector of the transform is 1, and the nullspace of the unique eigenvector of $\mathbf{A}^{(n)}$ is a 2^{n-1}-dimensional space, if $n>0$. $\underline{u}\in\mathbf{F}_2^{2^n}$ is an eigenvector of the transform if and only if $\underline{u}=\begin{pmatrix}\underline{u}^{(0)}\\ \underline{u}^{(1)}\end{pmatrix}$, where $\underline{u}^{(1)}$ is an arbitrary vector of the 2^{n-1}-dimensional linear space over $\mathbf{F}_2$, and $\underline{u}^{(0)}=\left(\mathbf{A}^{n-1}+\mathbf{I}^{n-1}\right)\underline{u}^{(1)}$.

The definition of the polynomial-like Boolean functions can be found in [5]. If f is a Boolean function of n variables, $\underline{\alpha}$ is the spectrum of its canonical disjunctive normal from, and $\underline{k}$ is the vector of the coefficients of its Zhegalkin polynomial, then f is polynomial-like if and only if $\underline{\alpha}=\underline{k}$.

In the following part of our article, we apply the results stated in [3], [4] and [5] to the Boolean functions.

Notation. Let $n\in\mathbf{N}_0$, let $\mathbf{T}^{(n)}$ be the 2^n-dimensional linear space over $\mathbf{F}_2$, for $2^n>i\in\mathbf{N}_0$ let $m_i^{(n)}$ be the i-th minterm of n variables and $S_i^{(n)}$ the i-th elementary Zhegalkin polynomial of n indeterminates, that is $m_i^{(n)}=\prod_{j=0}^{n-1}\left(\overline{a}_j^{(i)}\oplus x_j\right)$ and $S_i^{(n)}=\prod_{j=0}^{n-1}\left(\overline{a}_j^{(i)}+x_j\right)$, where $i=\sum_{j=0}^{n-1}a_j^{(i)}2^j$, and $\oplus$ is the Exclusive Or, and $+$ denotes the logical sum. If $\underline{\alpha}\in\mathbf{T}^{(n)},\underline{k}=\mathbf{A}^{(n)}\underline{\alpha}$, and $f=\sum_{i=0}^{2^n-1}\alpha_i m_i^{(n)}$ is a Boolean-function of n variables, then $\varphi(f)=p=\bigoplus_{i=0}^{2^n-1}k_iS_i^{(n)}$. For the previous f and p, $f=f_r^{(n)}$ and $p=p_s^{(n)}$, where $r=\sum_{i=0}^{2^n-1}\alpha_i2^i$ and $s=\sum_{i=0}^{2^n-1}k_i2^i$.

Proposition 1. *The EXCLUSIVE OR of polynomial-like Boolean functions of the same variables is a polynomial-like Boolean function of these variables.*

Proof. This statement is obvious, as $\underline{k}=\mathbf{A}\underline{\alpha}$, and then

$$\sum_{i=1}^{m}\underline{k}_1=\sum_{i=1}^{m}\mathbf{A}^{(n)}\underline{\alpha}_i=\mathbf{A}^{(n)}\sum_{i=1}^{m}\underline{\alpha}_i.$$

Proposition 2. *The logical product (that is the And operation) of polynomial-like Boolean functions over pairwise disjunctive sets of variables is polynomial-like Boolean function over the union of these sets of variables.*

Proof. Let $f=f(x_0,\ldots,x_{r-1})$ and $g=g(x_r,\ldots,x_{r+s-1})$ be polynomial-like Boolean functions, where $\{x_0,\ldots,x_{r-1}\}\bigcap\{x_r,\ldots,x_{r+s-1}=\emptyset$, and $f=$

$= \sum_{i=0}^{2^r-1} \alpha_i^{(f)} m_i^{(r)}$, $g = \sum_{i=0}^{2^s-1} \alpha_i^{(g)} m_i^{(s)}$. Then $\varphi(f) = \bigoplus_{i=0}^{2^r-1} \alpha_i^{(f)} S_i^{(r)}$ and $\varphi(g) = \bigoplus_{i=0}^{2^s-1} \alpha_i^{(g)} S_i^{(s)}$. As

$$m_i^{(x_0,\ldots,x_{r-1})} m_j^{(x_r,\ldots,x_{r+s-1})} = \prod_{k=0}^{r-1} \left(\overline{a}_k^{(i)} \oplus x_k\right) \prod_{l=0}^{s-1} \left(\overline{a}_l^{(j)} \oplus x_{r+l}\right) =$$

$$= \prod_{k=0}^{r-1} \left(\overline{a}_k^{(i)} \oplus x_k\right) \prod_{l=r}^{r+s-1} \left(\overline{a}_l^{(2^r j)} \oplus x_l\right) = \prod_{t=0}^{r+s-1} \left(\overline{a}_t^{(i+2^r j)} \oplus x_t\right) =$$

$$= m_{i+2^r j}^{(x_0,\ldots,x_{r-1},x_r,\ldots,x_{r+s-1})}$$

and

$$S_i^{(x_0,\ldots,x_{r-1})} S_j^{(x_r,\ldots,x_{r+s-1})} = \prod_{k=0}^{r-1} \left(\overline{a}_k^{(i)} + x_k\right) \prod_{l=0}^{s-1} \left(\overline{a}_l^{(j)} + x_{r+l}\right) =$$

$$= \prod_{k=0}^{r-1} \left(\overline{a}_k^{(i)} + x_k\right) \prod_{l=r}^{r+s-1} \left(\overline{a}_l^{(2^r j)} + x_l\right) = \prod_{t=0}^{r+s-1} \left(\overline{a}_t^{(i+2^r j)} + x_t\right) =$$

$$= S_{i+2^r j}^{(x_0,\ldots,x_{r-1},x_r,\ldots,x_{r+s-1})},$$

so $(\alpha_i^{(f)} m_i^{(x_0,\ldots,x_{r-1})})(\alpha_j^{(g)} m_j^{(x_0,\ldots,x_{s-1})}) = \alpha_i^{(f)} \alpha_j^{(g)} m_{i+2^r j}^{(x_0,\ldots,x_{r-1},x_r,\ldots,x_{r+s-1})}$, and a similar equality is true substituting m by S. Then, considering that the logical product is distributive over both the OR and the EXCLUSIVE OR operation, we get that

$$fg = f(x_0,\ldots,x_{r-1}) \cdot g(x_r,\ldots,x_{r+s-1}) =$$

$$= \left(\sum_{i=0}^{2^r-1} \alpha_i^{(f)} m_i^{(x_0,\ldots,x_{r-1})}\right) \left(\sum_{j=0}^{2^s-1} \alpha_j^{(g)} m_j^{(x_r,\ldots,x_{r+s-1})}\right) =$$

$$= \sum_{i=0}^{2^r-1} \sum_{j=0}^{2^s-1} \alpha_i^{(f)} \alpha_j^{(g)} m_i^{(x_0,\ldots,x_{r-1})} m_j^{(x_r,\ldots,x_{r+s-1})} =$$

$$= \sum_{k=0}^{2^{r+s}-1} \alpha_{(k \bmod 2^r)}^{(f)} \alpha_{\lfloor \frac{k}{2^r} \rfloor}^{(g)} m_k^{(x_0\ldots,x_{r-1},x_r,\ldots,x_{r+s-1})} =$$

$$= \sum_{k=0}^{2^{r+s}-1} \alpha_k^{(fg)} m_k^{(x_0 \ldots, x_{r-1}, x_r, \ldots, x_{r+s-1})}$$

and

$$\varphi(f)\varphi(g) = p^{(f)}(x_0, \ldots, x_{r-1}) \cdot p^{(g)}(x_r, \ldots, x_{r+s-1}) =$$

$$= \left(\sum_{i=0}^{2^r-1} \alpha_i^{(f)} S_i^{(x_0,\ldots,x_{r-1})} \right) \left(\sum_{j=0}^{2^s-1} \alpha_j^{(g)} S_j^{(x_r,\ldots,x_{r+s-1})} \right) =$$

$$= \sum_{i=0}^{2^r-1} \sum_{j=0}^{2^s-1} \alpha_i^{(f)} \alpha_j^{(g)} S_i^{(x_0,\ldots,x_{r-1})} S_j^{(x_r,\ldots,x_{r+s-1})} =$$

$$= \sum_{k=0}^{2^{r+s}-1} \alpha_{(k \bmod 2^r)}^{(f)} \alpha_{\lfloor \frac{k}{2^r} \rfloor}^{(g)} S_k^{(x_0,\ldots,x_{r-1},x_r,\ldots,x_{r+s-1})} =$$

$$= \sum_{k=0}^{2^{r+s}-1} \alpha_k^{(fg)} S_k^{(x_0,\ldots,x_{r-1},x_r,\ldots,x_{r+s-1})},$$

where for any $2^{r+s} > k \in \mathbf{N}_0$ $\alpha_k^{(fg)} = \alpha_{(k \bmod 2^r)}^{(f)} \alpha_{\lfloor \frac{k}{2^r} \rfloor}^{(g)}$, so fg is a polynomial-like Boolean function of the variables belonging to $\{x_0, \ldots, x_{r-1}\} \cup \cup \{x_r, \ldots, x_{r+s-1}\}$. From here we get the stated property by induction on the number of the Boolean functions.

Remark. In Proposition 1 it is important, that the set of the variables of the functions are the same, while for the product in Proposition 2 the disjunctivity of these sets is important. For instance, both $x_0 \oplus x_1$ and x_2 are polynomial-like Boolean functions, but $x_0 \oplus x_1 \oplus x_2$ is not, and $x_0 \oplus x_1 \oplus x_1 x_2$ is not a polynomial-like Boolean function, too, although $x_1 x_2$ is a polynomial-like Boolean function of two variables. For the product let us consider as first example again the polynomial-like Boolean functions $x_0 \oplus x_1$ and $x_1 x_2$. Their product is $(x_0 \oplus x_1)x_1 x_2 = x_1 x_2 \oplus x_0 x_1 x_2$, and the right hand side is equal to $x_1 x_2 \oplus x_0 x_1 x_2 = (1 \oplus x_0) x_1 x_2 = \overline{x}_0 x_1 x_2$. Now we can see, that the Zhegalkin polynomial of the product is a binomial, while the canonical disjunctive normal from of the same function contains only one term, so the function is obviously not a polynomial-like Boolean function. Similarly, the product of the polynomial-like Boolean functions $x_0 x_1 \oplus x_0 x_2$ and $x_0 x_1 \oplus x_1 x_2$ is not polynomial-like, as the product function is equal to $x_0 x_1 \oplus x_0 x_1 x_2 = x_0 x_1 \overline{x}_2$.

Proposition 3. *If $f = f_i^{(n)}$ is a polynomial-like Boolean function of n variables, where n is a positive integer, and $2^{2^n} > i \in \mathbf{N}_0$, then i is an even number.*

Proof. Every element of the first column and the diagonal of $\mathbf{A}^{(n)}$ is equal to 1. If $i = 1$ then $\underline{k}$ is equal to the first column of $\mathbf{A}^{(n)}$, so $w(\underline{\alpha}) = = 1 \neq 2^n = w(\underline{k})$, where w is the weight of a vector, that is the number of the components of the vector equal to 1. Now suppose i is an odd number greater than 1. Then $\alpha_0 = 1$, and there is at least one index j so, that $0 < j < 2^n$, and $\alpha_j = 1$. Let l be the smallest index with the previous property. Then $k_l = \left(\mathbf{A}^{(n)}\underline{\alpha}\right)_l = a_{l,0} \oplus a_{l,l} = 1 \oplus 1 = 0 \neq 1 = \alpha_l$, so $\underline{\alpha} \neq \underline{k}$.

Proposition 4. *$f_0^{(n)}, f_{2^{2^n-1}-2}^{(n)}, f_{2^{2^n-1}}^{(n)}$ and $f_{2^{2^n}-2}^{(n)}$ are polynomial-like Boolean functions of n-variables.*

Proof. If $\underline{\alpha} = \underline{0}$, then $\mathbf{A}^{(n)}\underline{\alpha} = \underline{0}$, too. For $\underline{\alpha} = (0, 0, ..., 0, 1)$, $\mathbf{A}^{(n)}\underline{\alpha}$ is the last column of $\mathbf{A}^{(n)}$, which is equal to $(0, 0, ..., 0, 1)^T$. As the number of ones in all of the rows of $\mathbf{A}^{(n)}$ with a positive indices is even, and the first element of any row is equal to one, too, furthermore the first row of the matrix contains exactly one 1, the image of $\underline{\alpha} = (0, 1, ..., 1, 1)$ is equal to the original vector. Finally, as $(0, 1, ..., 1, 0)$ is the sum of $(0, 1, ..., 1, 1)$ and $(0, 0, ..., 0, 1)$, and the transform is closed for the addition of the vectors, from the previous results we get that the image of $(0, 1, ..., 1, 0)$ is equal to itself.

Proposition 5. *$f_i^{(n)}$ is a polynomial-like Boolean function if and only if $\overline{f}_{i+1}^{(n)}$ is a polynomial-like Boolean function, too.*

Proof. As the set of the polynomial-like Boolean functions of the same variables is closed for the EXCLUSIVE OR, and $f_{2^{2^n}-2}^{(n)}$ is a polynomial-like Boolean function of n variables, the Boolean function f of n variables is polynomial-like if and only if $f^* = f \oplus f_{2^{2^n}-2}^{(n)}$ is polynomial-like. In the spectrum of the canonical disjunctive normal form of $f_{2^{2^n}-2}^{(n)}$ every coefficient but the one belonging to the index of 0 is equal to 1, so in the spectra of f and $f \oplus f_{2^{2^n}-2}^{(n)}$ the members belonging to the index of 0 are identical, while all other coefficients are different. If f is polynomial-like, then $\alpha_0 = 0$ and so $f_1^{(n)} \oplus f \oplus f^* = f_1^{(n)} \oplus f_{2^{2^n}-2}^{(n)} = f_{2^{2^n}-1}^{(n)}$, that is $f^* = \overline{f_1^{(n)} \oplus f}$, and if $f = f_i^{(n)}$, then - considering that $\alpha_0 = 0$ - $f_1^{(n)} \oplus f = f_{i+1}^{(n)}$.

Proposition 6. *If $f(x_{n-1}, \ldots, x_{i+1}, x_i, x_{i-1}, \ldots, x_0)$ is a polynomial-like Boolean function, then $f(x_{n-1}, \ldots, x_{i+1}, \overline{x}_i, x_{i-1}, \ldots, x_0)$ is a polynomial-like Boolean function if and only if $f = 0$ or $f = 1$.*

Remark. $f = 1$ is a polynomial-like Boolean function if and only if f is a Boolean function of 0 variables.

Proof. As the polynomial-like-property is invariant with respect to the permutation of the indices of the variables, it is enough to prove, that if $f(x_{n-1}, x_{n-2}, \ldots, x_0)$ polynomial-like, then $f(\overline{x}_{n-1}, x_{n-2}, \ldots, x_0)$ is not polynomial-like, except of the case when f is a constant function.

If f is a Boolean function of zero variables, then it is obvious that inverting any variable of the function we get the same function, so the new function is polynomial-like if and only if the original one is polynomial-like, and both of the Boolean functions of zero variables are polynomial-like.

Now suppose that n is a positive integer, and f is a polynomial-like Boolean function of n variables. Every Boolean function of n variables can be written as $f = \overline{x}_{n-1} f^{[0]} \oplus x_{n-1} f^{[1]}$, where $f^{[0]}$ and $f^{[1]}$ are Boolean functions of $x_0, \ldots, x_{n-2}$, and $f(\overline{x}_{n-1}, x_{n-2}, \ldots, x_0) = \overline{x}_{n-1} f^{[1]} \oplus x_{n-1} f^{[0]}$. If f is polynomial-like, then $\underline{\alpha}^{[0]} = \left(\mathbf{A}^{(n)} + \mathbf{I}^{(n)} \right) \underline{\alpha}^{[1]}$, and if also $f(\overline{x}_{n-1}, x_{n-2}, \ldots, x_0)$ is polynomial-like, then $\underline{\alpha}^{[1]} = \left(\mathbf{A}^{(n)} + \mathbf{I}^{(n)} \right) \underline{\alpha}^{[0]}$. It means that in the latter case

$$\underline{\alpha}^{[1]} = \left(\mathbf{A}^{(n)} + \mathbf{I}^{(n)} \right) \underline{\alpha}^{[0]} = \left(\mathbf{A}^{(n)} + \mathbf{I}^{(n)} \right)^2 \underline{\alpha}^{[1]} = \underline{0}$$

and then $\underline{\alpha}^{[0]} = \left(\mathbf{A}^{(n)} + \mathbf{I}^{(n)} \right) \underline{\alpha}^{[1]} = \underline{0}$, too, so $f = 0$.

Remark. If f is a Boolean function of n variables, and $n > j > i \geq 0$, then both of the two Boolean functions

$$f\left(x_{n-1}, \ldots, x_{j+1}, x_j, x_{j-1}, \ldots, x_{i+1}, x_i, x_{i-1}, \ldots, x_0 \right)$$

and

$$f\left(x_{n-1}, \ldots, x_{j+1}, \overline{x}_j, x_{j-1}, \ldots, x_{i+1}, \overline{x}_i, x_{i-1}, \ldots, x_0 \right)$$

can be polynomial-like. For instance, if

$$f = f^{(3)}_{158} = \overline{x}_2 \overline{x}_1 x_0 + \overline{x}_2 x_1 \overline{x}_0 + \overline{x}_2 x_1 x_0 + x_2 \overline{x}_1 \overline{x}_0 + x_2 x_1 x_0,$$

then $\underline{\alpha}^{(158)} = (0,1,1,1,1,0,0,1)^T$, and

$$\begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 \\ 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \end{pmatrix} \begin{pmatrix} 0 \\ 1 \\ 1 \\ 1 \\ 1 \\ 0 \\ 0 \\ 1 \end{pmatrix} = \begin{pmatrix} 0 \\ 1 \\ 1 \\ 1 \\ 1 \\ 0 \\ 0 \\ 1 \end{pmatrix}$$

so f is a polynomial-like Boolean function. Now

$$f(\overline{x}_2, x_1, \overline{x}_0) = x_2\overline{x}_1\overline{x}_0 + x_2x_1x_0 + x_2x_2\overline{x}_0 + \overline{x}_2\overline{x}_1x_0 + \overline{x}_2x_1\overline{x}_0 =$$

$$= \overline{x}_2\overline{x}_1x_0 + \overline{x}_2x_1\overline{x}_0 + x_2\overline{x}_1\overline{x}_0 + x_2x_1\overline{x}_0 + x_2x_1x_0 = f_{214}^{(3)}$$

and the spectrum of this function is equal to $\underline{\alpha}^{(214)} = (0,1,1,0,1,0,1,1)^T$. In that case

$$\begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 \\ 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \end{pmatrix} \begin{pmatrix} 0 \\ 1 \\ 1 \\ 0 \\ 1 \\ 0 \\ 1 \\ 1 \end{pmatrix} = \begin{pmatrix} 0 \\ 1 \\ 1 \\ 0 \\ 1 \\ 0 \\ 1 \\ 1 \end{pmatrix}$$

that means, that this function is a polynomial-like Boolean function, too.

References

[1] **Abbott J.C.,** *Sets, lattices and Boolean algebras,* Allyn and Bacon, Boston, Mass., 1964.

[2] **Flegg H.G.,** *Boolean algebra and its application,* Wiley, New York, 1964.

[3] **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.

[4] **Gonda J.,** The structure of the Boolean-Zhegalkin transform, *Annales Univ. Sci. Budapest. Sect. Comp.,* **23** (2004), 25-40.

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

(Received March 26, 2003)

J. Gonda
Department of Computer Algebra
Eötvös Loránd University
Pázmány Péter sét. 1/C
H-1117 Budapest, P.O.B. 32
andog@compalg.inf.elte.hu