Annales Univ. Sci. Budapest., Sect. Comp. 25 (2005) 13-23

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 the following we introduce the notion of the polynomial-like Boolean functions as the Boolean functions belonging to the eigenvectors of the transform mentioned above.

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 a consequence that

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

The research was partially supported by the Hungarian National Foundation for Scientific Research under grant OTKA T043657.

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 of 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 $\underline{u}^{(0)} = \left(\mathbf{A}^{(n-1)} + \mathbf{I}^{(n-1)}\right)\underline{u}^{(1)}$.

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

Notation. Let $n \in \mathbf{N}_0$, $\mathbf{T}^{(n)}$ the 2^n-dimensional linear space over $\mathbf{F}_2$, for $2^n > i \in \mathbf{N}_0$ let $m_i^{(n)}$ the i-th minterm of n variables, and $S_i^{(n)}$ the i-th elementary Zhegalkin polynomial of n indeterminates. If $\underline{\alpha} \in \mathbf{T}^{(n)}$, $\underline{k} = \mathbf{A}^{(n)}\underline{\alpha}$, and $f = \sum_{i=0}^{2^n-1} \alpha_i m_i^{(n)}$ a Boolean function of n variables, then $\tau_f(f) = \sum_{i=0}^{2^n-1} k_i m_i^{(n)}$, $\varphi(f) = \bigoplus_{i=0}^{2^n-1} k_i S_i^{(n)}$, and $\tau_p(p) = \bigoplus_{i=0}^{2^n-1} \alpha_i S_i^{(n)}$. For the previous f and p, $f = f_r^{(n)}$ and $p = p_s^{(n)}$, where $r = \sum_{i=0}^{2^n-1} \alpha_i 2^i$ and $s = \sum_{i=0}^{2^n-1} k_i 2^i$.

Remark. As both φ, τ_f and τ_p are bijective mappings, there exist the inverses of all of these mappings. It can also be seen immediately that τ_f and τ_p are involutions.

Proposition 1. *For any* $n \in \mathbf{N}_0$ $\varphi\tau_f = \tau_p\varphi$.

Proof. Let $f = \sum_{i=0}^{2^n-1} \alpha_i m_i^{(n)}$. Then

$$(\varphi\tau_f)(f) = \varphi\left(\tau_f(f)\right) = \varphi\left(\sum_{i=0}^{2^n-1} k_i m_i^{(n)}\right) =$$

$$= \bigoplus_{i=0}^{2^n-1} \alpha_i S_i^{(n)} =$$

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

As f is an arbitrary Boolean function of n variables for any $n \in \mathbf{N}_0$, the statement of the proposition is true.

For all the three mappings mentioned in the proposition are invertible, from the statement immediately follows that for any $n \in \mathbf{N}_0$ $\varphi^{-1}\tau_p = \tau_f\varphi^{-1}$ (of course for this equality it is enough that φ is invertible).

Proposition 2. *Let $n \in \mathbf{N}$, the index of the Boolean function f of n variables is equal to l, and the index of $\varphi(f)$ is equal to l'. Then*

a) if $l > 0$ then

$$\min\left\{ i \mid 2^n > i \in \mathbf{N}_0 \wedge \alpha_i = 1 \right\} = \min\left\{ i \mid 2^n > \mathbf{N}_0 \wedge k_i = 1 \right\};$$

b) $n > i \in \mathbf{N}_0$:

$$k_{2^i-1} \equiv w\left(\left(l \bmod 2^{2^i} \right)\right) \pmod 2 \bigwedge \alpha_{2^i-1} \equiv w\left(\left(l' \bmod 2^{2^i} \right)\right) \pmod 2;$$

c) $l \equiv l' \pmod 2$,

where $w(l)$ is the weight of l, that is the number of 1-s in its binary representation.

Proof. a) $a^{(n)}_{i,i} = 1$ and for $j > i$ $a^{(n)}_{i,j} = 0$, so, if $\min\left\{ i \mid 2^n > i \in \right.$ $\left. \in \mathbf{N}_0 \wedge \alpha_i = 1 \right\} = t$, then $k_i = \bigoplus_{j=0}^{2^n-1} a^{(n)}_{t,j}\alpha_j = \bigoplus_{j=t}^{2^n-1} a^{(n)}_{t,j}\alpha_j = \alpha_t = 1$, but for all of the $t > i \in \mathbf{N}_0$ indices $k_i = \bigoplus_{j=0}^{2^n-1} a^{(n)}_{i,j}\alpha_j = \bigoplus_{j=t}^{2^n-1} a^{(n)}_{i,j}\alpha_j = 0$. Similarly, it is true in the opposite direction, too.

b) If $l = \sum_{i=0}^{2^n-1} \alpha_i 2^i$, then $\left(l \bmod 2^r \right) = \sum_{i=0}^{r-1} \alpha_i 2^i$. As all of the α_i coefficients are equal to either zero or one, we get that $w\left(\left(l \bmod 2^r \right)\right) = \sum_{i=0}^{r-1} \alpha_i$, and then $w\left(\left(l \bmod 2^r \right)\right) \pmod 2 = \sum_{i=0}^{r-1} \alpha_i \pmod 2 = \bigoplus_{i=0}^{r-1} \alpha_i$. For $2^i > j \in \mathbf{N}_0$ $a^{(n)}_{2^i-1,j} = 1$, so $k_{2^i-1} = \bigoplus_{j=0}^{2^n-1} a^{(n)}_{i,j}\alpha_j = \bigoplus_{j=0}^{2^i-1} \alpha_j$. The other congruence can be proved in the same way.

c) This is a direct consequence of b) by $t = 0$.

Now we define the polynomial-like Boolean functions.

Definition. Let $n \in \mathbf{N}_0$. The Boolean function f of n variables is a polynomial-like Boolean function if $\tau_f(f) = f$.

By the definition, the Boolean function f is polynomial-like if and only if the coefficients of its canonical disjunctive normal form and its Zhegalkin polynomial with the same indices are equal to each other, that is if $\underline{\alpha}$ is an eigenvector of $\mathbf{A}^{(n)}$. From this follows that both of the Boolean functions of zero variables are polynomial-like Boolean functions, and if $f = f_i^{(n)}$, then $\varphi(f) = p = p_i^{(n)}$.

Proposition 3. *$f = \tau_f(f)$ if and only if $\varphi(f) = \tau_p(\varphi(f))$.*

Proof. As φ is invertible, $f = \tau_f(f)$ is fulfilled if and only if $\varphi(f) = \varphi(\tau_f(f))$. But by Proposition 1 $\varphi(\tau_f(f)) = \tau_p(\varphi(f))$, so $\varphi(f) = \varphi(\tau_f(f))$ is true if and only if $\varphi(f) = \tau_p(\varphi(f))$ is true, too.

Proposition 4. *Let $n \in \mathbf{N}$. If $f = f_j^{(n-1)}$ is an arbitrary Boolean function of $n-1$ variables, then $x_{n-1}f \oplus \overline{x}_{n-1}(\tau_f(f) \oplus f)$ is a polynomial-like Boolean function (the variables are indexed from zero).*

Proof. For an arbitrary 2^{n-1}-dimensional $\underline{\alpha}$ vector

$$\begin{pmatrix} \underline{\alpha}^{(0)} \\ \underline{\alpha}^{(1)} \end{pmatrix} = \begin{pmatrix} \left(\mathbf{A}^{(n-1)} + \mathbf{I}^{(n-1)}\right)\underline{\alpha} \\ \underline{\alpha} \end{pmatrix}$$

is an eigenvector of the transform of the 2^n-dimensional linear space over the field of two elements. Let $f = \sum_{i=0}^{2^{n-1}-1} \alpha_i m_i^{(n-1)}$, then

$$g = \sum_{i=0}^{2^{n-1}-1} \alpha_i^{(0)} \left(\overline{x}_{n-1} m_i^{(n-1)}\right) + \sum_{i=0}^{2^{n-1}-1} \alpha_i^{(1)} \left(x_{n-1} m_i^{(n-1)}\right) =$$

$$= \overline{x}_{n-1} \sum_{i=0}^{2^{n-1}-1} \alpha_i^{(0)} m_i^{(n-1)} \oplus x_{n-1} \sum_{i=0}^{2^{n-1}-1} \alpha_i^{(1)} m_i^{(n-1)}$$

is a polynomial-like Boolean function of n variables. But,

$$\underline{\alpha}^{(0)} = \left(\mathbf{A}^{(n-1)} + \mathbf{I}^{(n-1)}\right)\underline{\alpha} = \mathbf{A}^{(n-1)}\underline{\alpha} + \underline{\alpha} = \underline{k} + \underline{\alpha},$$

so

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

$$= \sum_{i=0}^{2^{n-1}-1} k_i^{(n-1)} m_i^{(n-1)} \oplus \sum_{i=0}^{2^{n-1}-1} \alpha_i m_i^{(n-1)} = \tau_f(f) \oplus f$$

and then $x_{n-1}f \oplus \overline{x}_{n-1}(\tau_f(f) \oplus f)$ is a polynomial-like Boolean function.

Remark. In the proof above we used and later in this article we shall use the fact that $\sum_{i=0}^{2^n-1} \alpha_i m_i^{(n)} = \bigoplus_{i=0}^{2^n-1} \alpha_i m_i^{(n)}$, as for any $2^n > j > i \in \mathbf{N}_0$ $m_i^{(n)} m_j^{(n)} = 0$.

Proposition 5. *Let $n > 0$, and let f be a polynomial-like Boolean function of n variables. If $f = f_j^{(n)}$ and*

$$j = \sum_{i=0}^{2^n-1} \alpha_i 2^i = \sum_{i=0}^{2^{n-1}-1} \alpha_i 2^i + 2^{2^{n-1}} \sum_{i=0}^{2^{n-1}-1} \alpha_{i+2^{n-1}} 2^i = j^{(0)} + j^{(1)} 2^{2^{n-1}},$$

then

$$\varphi(f) = p = p_j^{(n)} = x_{n-1} p_{j^{(1)}}^{(n-1)} \oplus \left(\tau_p\left(p_{j^{(1)}}^{(n-1)}\right) \oplus p_{j^{(1)}}^{(n-1)}\right)$$

(the variables are indexed from zero).

Proof. The vector of the coefficients of $x_{n-1} f_{j^{(1)}}^{(n-1)}$ is equal to $\begin{pmatrix} \underline{0} \\ \underline{\alpha}^{(1)} \end{pmatrix}$, and the transformed vector is equal to

$$\mathbf{A}^{(n)}\underline{\alpha} = \begin{pmatrix} \mathbf{A}^{(n-1)} & \mathbf{0}^{(n-1)} \\ \mathbf{A}^{(n-1)} & \mathbf{A}^{(n-1)} \end{pmatrix} \begin{pmatrix} \underline{0} \\ \underline{\alpha}^{(1)} \end{pmatrix} = \begin{pmatrix} \underline{0} \\ \mathbf{A}^{(n-1)}\underline{\alpha}^{(1)} \end{pmatrix}.$$

This implies that $\varphi\left(x_{n-1} f_{j^{(1)}}^{(n-1)}\right) = x_{n-1}\varphi\left(f_{j^{(1)}}^{(n-1)}\right) = x_{n-1} p_{j^{(1)}}^{(n-1)}$. As the mapping $\underline{\alpha} \to \mathbf{A}^{(n)}\underline{\alpha}$ is linear, so

$$\varphi\left(f_j^{(n)}\right) = \varphi\left(x_{n-1} f_{j^{(1)}}^{(n-1)} \oplus \left(\tau_f\left(f_{j^{(1)}}^{(n-1)}\right) \oplus f_{j^{(1)}}^{(n-1)}\right)\right) =$$
$$= x_{n-1} p_{j^{(1)}}^{(n-1)} \oplus \left(\varphi\left(\tau_f\left(f_{j^{(1)}}^{(n-1)}\right)\right) \oplus p_{j^{(1)}}^{(n-1)}\right).$$

By Proposition 1 $\varphi\left(\tau_f\left(f_{j^{(1)}}^{(n-1)}\right)\right) = \tau_p\left(\varphi\left(f_{j^{(1)}}^{(n-1)}\right)\right) = \tau_p\left(p_{j^{(1)}}^{(n-1)}\right)$, and so we proved that $\varphi(f) = x_{n-1} p_{j^{(1)}}^{(n-1)} \oplus \left(\tau_p\left(p_{j^{(1)}}^{(n-1)}\right) \oplus p_{j^{(1)}}^{(n-1)}\right)$.

Let us consider some examples.

Examples. a) Let $n = 3$ and $f = f_{149}^{(3)}$. $149 = 1 + 4 + 16 + 128 = 2^0 + 2^2 + 2^4 + 2^7$, and so $f = m_0^{(3)} + m_2^{(3)} + m_4^{(3)} + m_7^{(3)} = \overline{x}_2\overline{x}_1\overline{x}_0 + \overline{x}_2 x_1 \overline{x}_0 + x_2\overline{x}_1\overline{x}_0 +$

$+x_2x_1x_0$. The spectrum of this function is $\underline{\alpha}^T = (1,0,1,0,1,0,0,1)$. From $\underline{\alpha}$ we get $\underline{k}$:

$$\underline{k} = \mathbf{A}^{(3)}\underline{\alpha} = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 \\ 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \end{pmatrix} \begin{pmatrix} 1 \\ 0 \\ 1 \\ 0 \\ 1 \\ 0 \\ 0 \\ 1 \end{pmatrix} = \begin{pmatrix} 1 \\ 1 \\ 0 \\ 0 \\ 0 \\ 0 \\ 1 \\ 0 \end{pmatrix}.$$

Now

$$\begin{aligned} f &= m_0^{(3)} + m_2^{(3)} + m_4^{(3)} + m_7^{(3)} = \\ &= \overline{x}_2\overline{x}_1\overline{x}_0 + \overline{x}_2x_1\overline{x}_0 + x_2\overline{x}_1\overline{x}_0 + x_2x_1x_0, \\ \tau_f(f) &= m_0^{(3)} + m_1^{(3)} + m_6^{(3)} = \overline{x}_2\overline{x}_1\overline{x}_0 + \overline{x}_2\overline{x}_1x_0 + x_2x_1\overline{x}_0, \\ \varphi(f) &= S_0^{(3)} \oplus S_1^{(3)} \oplus S_6^{(3)} = 1 \oplus x_0 \oplus x_2x_1, \\ \tau_p(\varphi(f)) &= S_0^{(3)} \oplus S_2^{(3)} \oplus S_4^{(3)} \oplus S_7^{(3)} = 1 \oplus x_1 \oplus x_2 \oplus x_2x_1x_0 \end{aligned}$$

and $\tau_f(f) = f_{67}^{(3)}$, $p = \varphi(f) = p_{67}^{(3)}$ and $\tau_p(\varphi(f)) = \tau_p(p) = p_{149}^{(3)}$.

b) Let $n = 4$ and $\underline{\alpha}^T = (0,1,1,0,1,0,1,1,1,0,1,0,1,0,0,1)$, then

$$\underline{k} = \mathbf{A}^{(4)}\underline{\alpha} =$$

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

As $\underline{\alpha} = \underline{k}$, f belonging to $\underline{\alpha}$ is a polynomial-like Boolean function of 4 variables. This is not surprising. The last part of $\underline{\alpha}$ is $\underline{\alpha}^{(1)^T} = (1,0,1,0,1,0,0,1)$, which is equal to $\underline{\alpha}$ in the previous example in a). Then

$$\left(\mathbf{A}^{(3)} + \mathrm{I}^{(3)}\right)\underline{\alpha}^{(1)} = \begin{pmatrix}1\\1\\0\\0\\0\\0\\1\\0\end{pmatrix} + \begin{pmatrix}1\\0\\1\\0\\1\\0\\0\\1\end{pmatrix} = \begin{pmatrix}0\\1\\1\\0\\1\\0\\1\\1\end{pmatrix}$$

which is exactly the first part of $\underline{\alpha}$. Particularly,

$$\begin{aligned} f = f^{(4)}_{38358} =& m^{(4)}_1 + m^{(4)}_2 + m^{(4)}_4 + m^{(4)}_6 + m^{(4)}_7 + m^{(4)}_8 + m^{(4)}_{10} + m^{(4)}_{12} + m^{(4)}_{15} = \\ =& \overline{x}_3\overline{x}_2\overline{x}_1x_0 + \overline{x}_3\overline{x}_2x_1\overline{x}_0 + \overline{x}_3x_2\overline{x}_1\overline{x}_0 + \overline{x}_3x_2x_1\overline{x}_0 + \overline{x}_3x_2x_1x_0 + \\ &+ x_3\overline{x}_2\overline{x}_1\overline{x}_0 + x_3\overline{x}_2x_1\overline{x}_0 + x_3x_2\overline{x}_1\overline{x}_0 + x_3x_2x_1x_0, \end{aligned}$$

$$\begin{aligned} p = p^{(4)}_{38358} =& S^{(4)}_1 \oplus S^{(4)}_2 \oplus S^{(4)}_4 \oplus S^{(4)}_6 \oplus S^{(4)}_7 \oplus S^{(4)}_8 \oplus S^{(4)}_{10} \oplus S^{(4)}_{12} \oplus S^{(4)}_{15} = \\ =& x_0 \oplus x_1 \oplus x_2 \oplus x_2x_1 \oplus x_2x_1x_0 \oplus x_3 \oplus x_3x_1 \oplus x_3x_2 \oplus x_3x_2x_1x_0. \end{aligned}$$

c) Let $f = f^{(4)}_{38358}$. Now $j^{(1)} = \left\lfloor \dfrac{38358}{2^{2^4-1}} \right\rfloor = 149 = 2^0 + 2^2 + 2^4 + 2^7$, so the right side part of $\underline{\alpha}$ is $\underline{\alpha}^{(1)^T} = (1,0,1,0,1,0,0,1)$, and $\underline{k}$ belonging to $\underline{\alpha}^{(1)}$ is equal to $\underline{k}^T = (1,1,0,0,0,0,1,0)$. Then

$$x_3p^{(3)}_{149} \oplus \left(\tau_p\left(p^{(3)}_{149}\right) \oplus p^{(3)}_{149}\right) =$$

$$= x_3\left(1 \oplus x_1 \oplus x_2 \oplus x_2x_1x_0\right) \oplus \left(\left(1 \oplus x_0 \oplus x_2x_1\right) \oplus \left(1 \oplus x_1 \oplus x_2 \oplus x_2x_1x_0\right)\right) =$$

$$= x_0 \oplus x_1 \oplus x_2 \oplus x_2x_1 \oplus x_2x_1x_0 \oplus x_3 \oplus x_3x_1 \oplus x_3x_2 \oplus x_3x_2x_1x_0 =$$

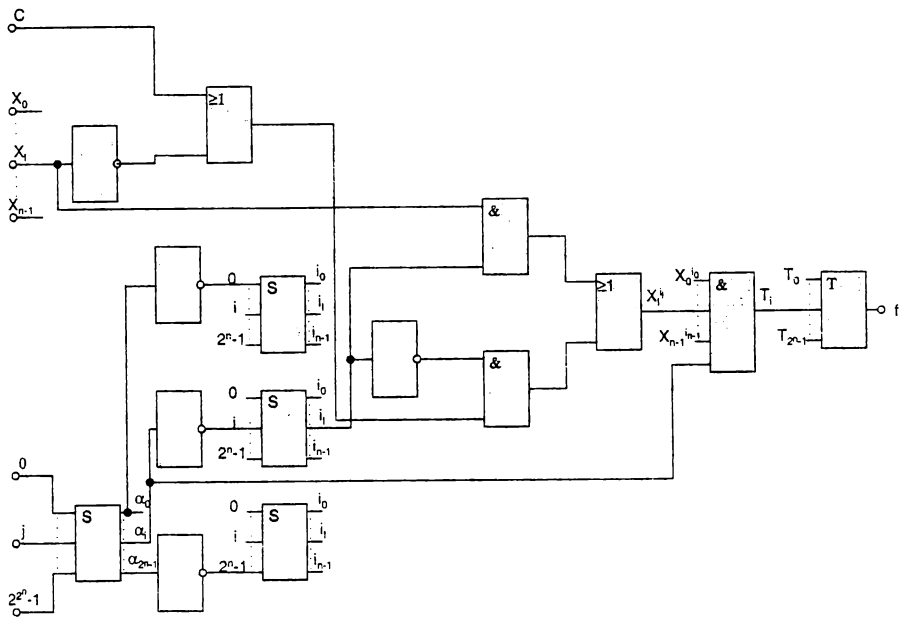
$$= S^{(4)}_1 \oplus S^{(4)}_2 \oplus S^{(4)}_4 \oplus S^{(4)}_6 \oplus S^{(4)}_7 \oplus S^{(4)}_8 \oplus S^{(4)}_{10} \oplus S^{(4)}_{12} \oplus S^{(4)}_{15} =$$

$$= p^{(4)}_{38358} = \varphi(f).$$

Let us consider the figure on the next page.

In the picture it can be seen a general layout realizing a switching circuit belonging to a Boolean function. At the S-boxes exactly one input is 0. The

boxes denoted by & realize the AND operation, and the boxes with $a \geq 1$ are the OR-gates. The little circles mean the negations. The box on the right side realizes either OR or the modulo 2 sum operation. In the first case $C = 0$, and the circuit realizes the canonical disjunctive normal form of the function, while in the second case $C = 1$, and the output is the Zhegalkin polynomial of the function. When the selected function is a polynomial-like Boolean function, then the result is independent of the type of the last gate.



Proposition 6. *The number of the polynomial-like Boolean functions of n variables for a positive integer n is equal to $2^{2^{n-1}}$.*

Proof. There is a natural bijective mapping between the polynomial-like Boolean functions of n variables and the 2^{n-1}-dimensional nullspace of the unique eigenvalue of $\mathbf{A}^{(n)}$.

Proposition 7. *Let π be a permutation of the set of nonnegative integers less than n, f a Boolean function of n variables, and $(\Pi f)(x_0, \ldots, x_{n-1}) = f(x_{\pi(0)}, \ldots, x_{\pi(n-1)})$. Then $\varphi(\Pi f) = \Pi(\varphi f)$, and f is a polynomial-like Boolean function if and only if Πf is also polynomial-like.*

Proof. For any element of $\{0,1\}^n$

$$f(u_0,\ldots,u_{n-1}) = (\varphi f)(u_{\pi(0)},\ldots,u_{\pi(n-1)}),$$

so if

$$p^{(1)}(x_0,\ldots,x_{n-1}) = \varphi\left(f\left(x_{\pi(0)},\ldots,x_{\pi(n-1)}\right)\right),$$
$$p^{(2)}\left(x_0,\ldots,x_{n-1}\right) = (\varphi f)\left(x_{\pi(0)},\ldots,x_{\pi(n-1)}\right),$$

then

$$p^{(1)}\left(u_0,\ldots,u_{n-1}\right) = f\left(u_{\pi(0)},\ldots,u_{\pi(n-1)}\right) =$$
$$=(\varphi f)\left(u_{\pi(0)},\ldots,u_{\pi(n-1)}\right) = p^{(2)}\left(u_0,\ldots,u_{n-1}\right)$$

is also true, that is the mappings belonging to $p^{(1)}$ and $p^{(2)}$ are equal. In that case even the polynomials are equal, which proves the first statement.

Now suppose f is a polynomial-like Boolean function. Then $\underline{\alpha} = \underline{k}$, which implies $\underline{\alpha}' = \underline{k}'$, where $\underline{\alpha}'$ and $\underline{k}'$ denote the vectors of the coefficients of the permuted variables. From the first part of the proposition follows that $\underline{\alpha}'$ and $\underline{k}'$ belong to the same function, so if f is polynomial-like then the function of the permuted variables is also polynomial-like.

Proposition 8. *Every variable of a nonzero polynomial-like Boolean function is essential.*

Proof. In the case of $n = 0$ this is obvious. Now let $n \in \mathbf{N}$, and let $f \neq 0$ a Boolean function of n variables. On the base of Proposition 7 it is enough to prove that x_{n-1} is an essential variable of f, if the function is a polynomial-like Boolean function. f can be written as $f = \overline{x}_{n-1}g^{(0)} + x_{n-1}g^{(1)}$, and f is independent of x_{n-1} if and only if $g^{(0)} = g^{(1)}$. In that case

$$\begin{pmatrix} \underline{k}^{(0)} \\ \underline{k}^{(1)} \end{pmatrix} = \underline{k} = \mathbf{A}^{(n)}\underline{\alpha} = \begin{pmatrix} \mathbf{A}^{(n-1)} & \mathbf{0}^{(n-1)} \\ \mathbf{A}^{(n-1)} & \mathbf{A}^{(n-1)} \end{pmatrix} \begin{pmatrix} \underline{\alpha}^{(0)} \\ \underline{\alpha}^{(1)} \end{pmatrix} =$$

$$= \begin{pmatrix} \mathbf{A}^{(n-1)} & \mathbf{0}^{(n-1)} \\ \mathbf{A}^{(n-1)} & \mathbf{A}^{(n-1)} \end{pmatrix} \begin{pmatrix} \underline{\alpha}^{(0)} \\ \underline{\alpha}^{(0)} \end{pmatrix} = \begin{pmatrix} \mathbf{A}^{(n-1)}\underline{\alpha}^{(0)} \\ \underline{0} \end{pmatrix},$$

that is $\underline{k}^{(1)} = \underline{0}$. But $\underline{\alpha}^{(1)} = \underline{0}$ if and only if $g^{(1)} = 0$, and then $f = 0$, what was excluded. That means if f does not depend on x_{n-1}, then $\underline{\alpha}^{(1)} \neq \underline{k}^{(1)}$, and then $\underline{\alpha} \neq \underline{k}$, too, so f is not a polynomial-like Boolean function.

Briefly can be mentioned that Proposition 8 is true for the zero function of zero variables, but false for the zero function with at least one variable.

Proposition 9. *Let* $n \in \mathbf{N}$, $f = f_k^{(n)}$ *and* $f_k^{(n)} = \overline{x}_{n-1} f^{(n-1)}_{(k \bmod 2^{2^{n-1}})} + x_{n-1} f^{(n-1)}_{\left\lfloor \frac{k}{2^{2^{n-1}}} \right\rfloor}$, *where neither* $f^{(n-1)}_{(k \bmod 2^{2^{n-1}})}$, *nor* $f^{(n-1)}_{\left\lfloor \frac{k}{2^{2^{n-1}}} \right\rfloor}$ *depends on* x_{n-1}. *If* f *is polynomial-like, then* $k = 0$ *or* $k \geq 2^{2^{n-1}}$, *and* $\left(k \bmod 2^{2^{n-1}}\right) = 0$ *if and only if* $f^{(n-1)}_{\left\lfloor \frac{k}{2^{2^{n-1}}} \right\rfloor}$ *is a polynomial-like Boolean function of* $n-1$ *variables.*

Proof. The zero function is polynomial-like, and in that case $k = 0$. If $f \neq 0$, then every variable of f is essential, so $f^{(n-1)}_{\left\lfloor \frac{k}{2^{2^{n-1}}} \right\rfloor} \neq 0$. Then $\left\lfloor \frac{k}{2^{2^{n-1}}} \right\rfloor \geq 1$ and $k \geq 2^{2^{n-1}}$.

Now suppose f polynomial-like and $\left(k \bmod 2^{2^{n-1}}\right) = 0$. From this follows that $f^{(n-1)}_{(k \bmod 2^{2^{n-1}})} = 0$ and $\underline{\alpha}^{(0)} = \underline{0}$. Then

$$\begin{pmatrix} \underline{\alpha}^{(0)} \\ \underline{\alpha}^{(1)} \end{pmatrix} = \begin{pmatrix} \underline{k}^{(0)} \\ \underline{k}^{(1)} \end{pmatrix} = \underline{k} = \mathbf{A}^{(n)} \underline{\alpha} = \begin{pmatrix} \mathbf{A}^{(n-1)} & \mathbf{0}^{(n-1)} \\ \mathbf{A}^{(n-1)} & \mathbf{A}^{(n-1)} \end{pmatrix} \begin{pmatrix} \underline{\alpha}^{(0)} \\ \underline{\alpha}^{(1)} \end{pmatrix} =$$

$$= \begin{pmatrix} \mathbf{A}^{(n-1)} & \mathbf{0}^{(n-1)} \\ \mathbf{A}^{(n-1)} & \mathbf{A}^{(n-1)} \end{pmatrix} \begin{pmatrix} \underline{0} \\ \underline{\alpha}^{(1)} \end{pmatrix} = \begin{pmatrix} \underline{0} \\ \mathbf{A}^{(n-1)} \underline{\alpha}^{(1)} \end{pmatrix}$$

and $\underline{\alpha}^{(1)} = \underline{k}^{(1)} = \mathbf{A}^{(n-1)} \underline{\alpha}^{(1)}$, so $f^{(n-1)}_{\left\lfloor \frac{k}{2^{2^{n-1}}} \right\rfloor}$ is a polynomial-like Boolean function of $n-1$ variables.

References

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

[2] **Flegg H.G.,** *Boolean algebra and its application,* J. Wiley and Sons, 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.

(Received February 11, 2003)

J. Gonda
Department of Computer Algebra
Eötvös Loránd University
Pázmány Péter sét. 1/C
H-1117 Budapest, Hungary