Annales Univ. Sci. Budapest., Sect. Comp. 32 (2010) 189-200

THREE REMARKS ON THE CONJUCTIVELY POLYNOMIAL–LIKE BOOLEAN FUNCTIONS

J. Gonda (Budapest, Hungary)

Abstract. A Boolean function is conjunctively polynomial-like if the spectra of its modified conjunctive normal form and its Zhegalkin polynomial are equal. In the following article some equivalent forms of the previous definition are given and furthermore it is pointed out that the given definition is the natural equivalent of the similar notion of the polynomial-like Boolean functions.

In this article disjunction and logical sum, conjunction and logical product, exclusive or and modulo two sum, as well as complementation and negation are used in the same sense and they are denoted respectively by $+$, $\cdot$ (or simply without any operation sign), $\oplus$ and $\bar{}$. The elements of the field with two elements and the elements of the Boolean algebra with two elements are denoted by the same signs, namely by 0 and 1; $\mathbf{N}$ denotes the non-negative integers, and $\mathbf{N}^+$ the positive ones.

1. Introduction

1.1. It is well-known that an arbitrary two-valued logical function of n variables can be written in the uniquely determined canonical disjunctive normal form, i.e. as a logical sum whose members are pairwise distinct logical products of n factors, where all of such logical products contain every logical

The European Union and the European Social Fund have provided financial support to the project under the grant agreement TÁMOP-4.2.1/B-09/1/KMR-2010-003.

variable exactly once, either negated or not negated exclusively. Clearly, there exist exactly 2^n such products. Supposing that the variables are indexed by the integers $0 \leq j < n$, these products can be numbered by the numbers $0 \leq i < 2^n$ in such a way that we consider the non-negative integer containing 0 in the j-th position of its binary expansion if the j-th variable of the given product is negated, and 1 in the other case. Of course, this is a one to one correspondence between the 2^n distinct products and the integers of the interval $[0..2^n - 1]$, and if $i = \sum_{j=0}^{n-1} a_j^{(i)} 2^j$, where $a_j^{(i)}$ is either 0 or 1, then the product belonging to it is

$$m_i^{(n)} = \prod_{j=0}^{n-1} \left(\overline{a_j^{(i)}} \oplus X_j \right). \tag{1}$$

Such a product is called *minterm* (with 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 $m_j^{(n)}$ does not occur in that function, and 1 means that the canonical disjunctive normal form of the function contains the minterm of the index j, i.e. for $k = \sum_{i=0}^{2^n-1} \alpha_i^{(k)} 2^i$ with $\alpha_i^{(k)} \in \{0, 1\}$

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

Now $f_k^{(n)}$ denotes the k-th Boolean function of n variables.

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

$$M_i^{(n)} = \sum_{j=0}^{n-1} \left(a_j^{(i)} \oplus X_j \right) \tag{3}$$

for $2^n > i \in \mathbf{N}$. This function, the i-th *maxterm* of n variables is equal to 0 if and only if $X_j = a_j^{(i)}$ for every $0 \leq j < n$. By these maxterms a Boolean function can be expressed as

$$f^{(n)} = \prod_{i=0}^{2^n-1} \left(\alpha_i + M_i^{(n)} \right), \tag{4}$$

where $\alpha_i = f^{(n)}\left(a_{n-1}^{(i)}, \ldots, a_0^{(i)}\right)$, and

$$f_k^{(n)} = \prod_{i=0}^{2^n-1} \left(\alpha_i^{(k)} + M_i^{(n)}\right). \tag{5}$$

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

$$M_i^{(n)\prime} = \sum_{j=0}^{n-1} \left(\overline{a_j^{(i)}} \oplus x_j\right). \tag{6}$$

It is easy to see that $M_i^{(n)} = M_{2^n-1-i}^{(n)\prime}$. Now if $f^{(n)} = \prod_{i=0}^{2^n-1} \left(\beta_i + M_i^{(n)\prime}\right) = f_k^{(n)}$ then $\alpha_i = f^{(n)}\left(a_{n-1}^{(i)}, \ldots, a_0^{(i)}\right) = \beta_{2^n-1-i}$. This form of the function given by the modified maxterms is the *modified conjunctive normal form* of the function. For $\overline{u} \oplus v = u \oplus \overline{v}$, so $\overline{a_j^{(i)}} \oplus x_j = a_j^{(i)} \oplus \overline{x}_j$ and $M_i^{(n)\prime} = \sum_{j=0}^{n-1} \left(a_j^{(i)} \oplus \overline{x}_j\right)$. If $g^{(n)} = \prod_{i=0}^{2^n-1} \left(\beta_i + M_i^{(n)}\right)$, then

$$\begin{aligned}
f^{(n)}(x_{n-1}, \ldots, x_0) &= \prod_{i=0}^{2^n-1} \left(\alpha_i + \sum_{j=0}^{n-1} \left(a_j^{(i)} \oplus x_j\right)\right) = \\
&= \prod_{i=0}^{2^n-1} \left(\alpha_i + M_i^{(n)}\right) = \prod_{i=0}^{2^n-1} \left(\beta_i + M_i^{(n)\prime}\right) = \\
&= \prod_{i=0}^{2^n-1} \left(\beta_i + \sum_{j=0}^{n-1} \left(a_j^{(i)} \oplus \overline{x}_j\right)\right) = \\
&= g^{(n)}(\overline{x}_{n-1}, \ldots, \overline{x}_0) = \overline{\overline{g^{(n)}}}(\overline{x}_{n-1}, \ldots, \overline{x}_0) = \\
&= \overline{g^{(n)D}}(x_{n-1}, \ldots, x_0),
\end{aligned} \tag{7}$$

where ^{D} denotes the dual of the function. As if $f = \overline{g^D}$ then $g = \overline{f^D}$, so $g^{(n)}$ is the complement of the dual of $f^{(n)}$ in (7).

Another possibility for giving a Boolean function is the so-called Zhegalkin-polynomial. Let $S_i^{(n)} = \prod_{j=0}^{n-1} \left(\overline{a_j^{(i)}} + X_j\right)$, where $i = \sum_{j=0}^{n-1} a_j^{(i)} 2^j$ again. This

product contains only non-negated variables, and the j-th variable is contained in it if and only if the j-th digit is 1 in the binary expansion of i. There exist exactly 2^n such products which are pairwise distinct. Now any Boolean function of n variables can be written as a modulo two sum of such terms, and the members occurring in the sum are uniquely determined by the function. This 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

$$f^{(n)} = \bigoplus_{i=0}^{2^n-1} k_i S_i^{(n)}. \tag{8}$$

Between the first and third representations of the same Boolean function there is a very simple linear algebraic transform. In [3] it is pointed out that considering 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 $\mathbf{F}_2$, 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 disjunctive 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

$$\mathbf{A}^{(n)} = \begin{cases} (1) & \text{if } n = 0, \\ \begin{pmatrix} \mathbf{A}^{(n-1)} & \mathbf{0}^{(n-1)} \\ \mathbf{A}^{(n-1)} & \mathbf{A}^{(n-1)} \end{pmatrix} & \text{if } n \in \mathbf{N} \end{cases} \tag{9}$$

and as a consequence that

$$\mathbf{A}^{(n)^2} = \mathbf{I}^{(n)}, \tag{10}$$

where $\mathbf{I}^{(n)}$ and $\mathbf{0}^{(n)}$ denote the 2^n-dimensional identity and zero matrix, respectively. From this follows that if $\underline{k} = \mathbf{A}^{(n)}\underline{\alpha}$, then $\underline{\alpha} = \mathbf{A}^{(n)}\underline{k}$. In the special case when $\underline{\alpha} = \underline{k}$, the corresponding function is a *polynomial-like Boolean function*, defined in [6].

There is a similar relationship between the modified conjunctive normal form and the Zhegalkin polynomial of the same Boolean function, namely $\underline{k} = \left(\mathbf{A}^{(n)}\mathbf{P}^{(n)}\right)\underline{\alpha}$, if $\underline{\alpha}$ is the spectrum of the modified conjunctive normal form of the function and $\mathbf{P}^{(n)}$ is a $2^n \times 2^n$ matrix with the elements $P_{i,j} = \delta_{2^n-1-i,j}$, that is with 1 in the side diagonal and with 0 at the other positions of the matrix. In [7] the notation $\mathbf{U}^{(n)} = \mathbf{A}^{(n)}\mathbf{P}^{(n)}$ was applied. Now if $\underline{\alpha} = \underline{k}$, then the corresponding function is a *conjunctively polynomial-like Boolean function.*

1.2. Let $\mathbf{T}$ be an $n \times m$ matrix, and let $\mathbf{T}^*$ be such a matrix that $(\mathbf{T}^*)_{i,j} = T_{m-1-j,n-1-i}$ for every $n > i \in \mathbf{N}$ and $m > j \in \mathbf{N}$, that is, $\mathbf{T}^*$ is the transpose of $\mathbf{T}$ with respect to the side diagonal of the matrix. Then the following properties are valid:

(1) (a) $(\mathbf{T}^*)^* = \mathbf{T}$;

(b) $\left(\mathbf{T}^T\right)^* = (\mathbf{T}^*)^T$;

(c) $(c\mathbf{T})^* = c\mathbf{T}^*$;

(d) $(\mathbf{T}_1 + \mathbf{T}_2)^* = \mathbf{T}_1^* + \mathbf{T}_2^*$;

(e) $(\mathbf{T}_1\mathbf{T}_2)^* = \mathbf{T}_2^*\mathbf{T}_1^*$.

(2) If $\mathbf{P}^{[t]}$ is a $t \times t$ matrix so that $P_{i,j}^{[t]} = \delta_{t-1-i,j}$ for any $t > i \in \mathbf{N}$ and $t > j \in \mathbf{N}$, then

(a) $\left(\mathbf{P}^{[t]}\right)^2 = \mathbf{I}^{(t\times t)}$;

(b) $\left(\mathbf{P}^{[t]}\right)^* = \mathbf{P}^{[t]} = \left(\mathbf{P}^{[t]}\right)^T$;

(c) $\mathbf{P}^{[n]}\mathbf{T}\mathbf{P}^{[m]} = (\mathbf{T}^*)^T$.

(3) From the last property we get that

(a) $\mathbf{T}^*\mathbf{P}^{[n]} = \mathbf{P}^{[m]}\mathbf{T}^T$;

(b) if $\mathbf{T}^* = \mathbf{T}$ (and then necessarily $m = n$) then $\mathbf{P}^{[n]}\mathbf{T}\mathbf{P}^{[n]} = \mathbf{T}^T \wedge \mathbf{T}\mathbf{P}^{[n]} = \mathbf{P}^{[n]}\mathbf{T}^T$.

From now on let $\mathbf{P}^{(n)} = \mathbf{P}^{[2^n]}$.

2. Development

2.1. As $\mathbf{A}^{(0)} = (1)$, so $\left(\mathbf{A}^{(0)}\right)^* = \mathbf{A}^{(0)}$. Supposing that $\left(\mathbf{A}^{(n)}\right)^* = \mathbf{A}^{(n)}$ we get that

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

$$
\begin{aligned}
&= \begin{pmatrix} \left(\mathbf{A}^{(n)}\right)^* & \left(\mathbf{0}^{(n)}\right)^* \\ \left(\mathbf{A}^{(n)}\right)^* & \left(\mathbf{A}^{(n)}\right)^* \end{pmatrix} = \\
&= \begin{pmatrix} \mathbf{A}^{(n)} & \mathbf{0}^{(n)} \\ \mathbf{A}^{(n)} & \mathbf{A}^{(n)} \end{pmatrix} = \mathbf{A}^{(n+1)},
\end{aligned} \tag{11}
$$

so $\left(\mathbf{A}^{(n)}\right)^* = \mathbf{A}^{(n)}$ for any $n \in \mathbf{N}$. With 3b in 1.2 in the Introduction we get that

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

and

$$
\left(\mathbf{A}^{(n)}\right)^T \mathbf{P}^{(n)} = \mathbf{P}^{(n)}\mathbf{A}^{(n)}. \tag{13}
$$

In [7] it was proved that $\left(\mathbf{A}^{(n)}\mathbf{P}^{(n)}\right)^3 = \mathbf{I}^{(n)}$, so

$$
\mathbf{P}^{(n)}\mathbf{A}^{(n)} = \left(\mathbf{A}^{(n)}\mathbf{P}^{(n)}\right)^2 = \mathbf{A}^{(n)} \left(\mathbf{P}^{(n)}\mathbf{A}^{(n)}\mathbf{P}^{(n)}\right) \tag{14}
$$

and then

$$
\begin{aligned}
\mathbf{A}^{(n)}\mathbf{P}^{(n)}\mathbf{A}^{(n)} &= \mathbf{P}^{(n)}\mathbf{A}^{(n)}\mathbf{P}^{(n)} = \\
&= \left(\left(\mathbf{A}^{(n)}\right)^*\right)^T = \left(\mathbf{A}^{(n)}\right)^T.
\end{aligned} \tag{15}
$$

From the last result we get that $\mathbf{A}^{(n)} \left(\mathbf{A}^{(n)}\right)^T \mathbf{A}^{(n)} = \mathbf{P}^{(n)}$, and then

$$
\mathbf{A}^{(n)} \left(\mathbf{A}^{(n)}\right)^T = \mathbf{P}^{(n)}\mathbf{A}^{(n)} = \left(\mathbf{A}^{(n)}\right)^T \mathbf{P}^{(n)} \tag{16}
$$

and

$$
\left(\mathbf{A}^{(n)}\right)^T \mathbf{A}^{(n)} = \mathbf{A}^{(n)}\mathbf{P}^{(n)} = \mathbf{P}^{(n)} \left(\mathbf{A}^{(n)}\right)^T. \tag{17}
$$

With the previous results we proved the following theorem.

Theorem 1. *The following statements are equivalent:*

(1)

(a) $\underline{v} = \left(\mathbf{A}^{(n)}\mathbf{P}^{(n)}\right)\underline{u}$;

(b) $\underline{v} = \left(\mathbf{P}^{(n)}\left(\mathbf{A}^{(n)}\right)^T\right)\underline{u}$;

(c) $\mathbf{P}^{(n)}\underline{v} = \left(\mathbf{A}^{(n)}\right)^T\underline{u}$;

(d) $\mathbf{A}^{(n)}\underline{v} = \mathbf{P}^{(n)}\underline{u}$.

(2)

(a) $\underline{u} = \left(\left(\mathbf{A}^{(n)}\right)^T\mathbf{P}^{(n)}\right)\underline{u}$;

(b) $\underline{u} = \left(\mathbf{P}^{(n)}\mathbf{A}^{(n)}\right)\underline{u}$;

(c) $\underline{u} = \left(\mathbf{A}^{(n)}\mathbf{P}^{(n)}\right)\underline{u}$;

(d) $\underline{u} = \left(\mathbf{P}^{(n)}\left(\mathbf{A}^{(n)}\right)^T\right)\underline{u}$;

(e) $\underline{u} = \left(\left(\mathbf{A}^{(n)}\right)^T\mathbf{A}^{(n)}\right)\underline{u}$;

(f) $\underline{u} = \left(\mathbf{A}^{(n)}\left(\mathbf{A}^{(n)}\right)^T\right)\underline{u}$;

(g) $\mathbf{P}^{(n)}\underline{u} = \mathbf{A}^{(n)}\underline{u}$;

(h) $\mathbf{P}^{(n)}\underline{u} = \left(\mathbf{A}^{(n)}\right)^T\underline{u}$;

(i) $\mathbf{A}^{(n)}\underline{u} = \left(\mathbf{A}^{(n)}\right)^T\underline{u}$;

(j) $\left(\mathbf{A}^{(n)}\mathbf{P}^{(n)}\right)\underline{u} = \left(\mathbf{P}^{(n)}\mathbf{A}^{(n)}\right)\underline{u}$.

2.2. From the results in Theorem 1 we emphasize the following.

Theorem 2. *If $\underline{u}$ is the spectrum of the modified conjunctive normal form of a conjunctively polynomial-like Boolean function then the Boolean function determined by $\underline{u}_{\leftarrow} = \mathbf{P}\underline{u}$ as the spectrum of the modified conjunctive normal form of the function is conjunctively polynomial-like, too.*

Proof. As we saw (2g), if $\underline{u} = \left(\mathbf{A}^{(n)}\mathbf{P}^{(n)}\right)\underline{u}$, then $\mathbf{P}^{(n)}\underline{u} = \mathbf{A}^{(n)}\underline{u}$, and then

$$\begin{aligned}\mathbf{P}^{(n)}\underline{u} &= \mathbf{A}^{(n)}\underline{u} = \mathbf{A}^{(n)}\left(\mathbf{I}^{(n)}\underline{u}\right) = \\ &= \mathbf{A}^{(n)}\left(\left(\mathbf{P}^{(n)}\mathbf{P}^{(n)}\right)\underline{u}\right) = \mathbf{A}^{(n)}\left(\mathbf{P}^{(n)}\left(\mathbf{P}^{(n)}\underline{u}\right)\right) = \\ &= \left(\mathbf{A}^{(n)}\mathbf{P}^{(n)}\right)\left(\mathbf{P}^{(n)}\underline{u}\right).\end{aligned} \tag{18}$$

2.3. Let $\underline{\gamma} \in \mathbf{F}_2^{2^n}$, and let $f^{(n)}$ such a Boolean-function that its modified conjunctive normal form contains $M_i^{(n)\prime}$, where $2^n > i \in \mathbf{N}$, if and only if $\gamma_i = 1$. Then

$$f^{(n)} = \prod_{i=0}^{2^n-1}\left(\overline{\gamma_i} + M_i^{(n)\prime}\right) = \prod_{i=0}^{2^n-1}\left(\alpha_i + M_i^{(n)\prime}\right) \tag{19}$$

and so $\underline{\alpha} = \overline{\underline{\gamma}} = \underline{1}^{(n)} + \underline{\gamma}$, where $\underline{1}^{(n)} \in \mathbf{F}_2^{2^n}$ is such a vector, that $1_i = 1$ for every $2^n > i \in \mathbf{N}$ (briefly we consider the complement of a given Boolean function). Now we could consider those functions, for which $\underline{\gamma} = \underline{k}$, that is those functions which contain the term indexed by i in their Zhegalkin-polynomials exactly in those cases if the term belonging to the same index occurs in the spectra of the modified conjunctive normal forms of the functions. Even more in some respect could be rather these functions considered conjunctively polynomial-like Boolean functions, but this is impossible by the following theorem.

Theorem 3. *The only Boolean function with equal spectra belonging to the Zhegalkin polynomial and to the modified conjunctive normal form of the complement of the function is $f_2^{(1)}$, that is the identity function of one variable.*

Before the proof of the previous theorem we would like to remind of $\mathbf{U}^{(n)} = \mathbf{A}^{(n)}\mathbf{P}^{(n)}$:

$$\mathbf{U}^{(n)} = \begin{cases} (1) & n = 0, \\ \begin{pmatrix} \mathbf{0}^{(n-1)} & \mathbf{U}^{(n-1)} \\ \mathbf{U}^{(n-1)} & \mathbf{U}^{(n-1)} \end{pmatrix} & n > 0. \end{cases} \tag{20}$$

From the structure of the matrix it is easy to see that

- all of the elements of the side diagonal of the matrix are equal to 1;
- the elements above of the side diagonal are equal to 0 (that is $\mathbf{U}^{(n)}$ is a bottom triangle matrix with respect to the side diagonal);

- the matrix is symmetrical to the main diagonal;
- the last row and the last column contain only 1-s;
- the number of the 1-s contained in a row (or in a column) is even with the exception of the first row (and the first column).

Now let us see the proof of the theorem.

Proof. If $\underline{\gamma} \in \mathbf{F}_2^n$ is the vector containing a 1 at the position indexed by i, where $2^n > i \in \mathbf{N}$, exactly in the case if the modified conjunctive normal form of the Boolean function of n variables contains $M_i^{(n)\prime}$ then the spectrum of the Zhegalkin-polynomial of the same function is equal to

$$\begin{aligned} \underline{k} &= \left(\mathbf{A}^{(n)}\mathbf{P}^{(n)}\right)\left(\underline{1}^{(n)} + \underline{\gamma}\right) = \left(\mathbf{A}^{(n)}\mathbf{P}^{(n)}\right)\underline{1}^{(n)} + \left(\mathbf{A}^{(n)}\mathbf{P}^{(n)}\right)\underline{\gamma} = \\ &= \underline{e}_0^{(n)} + \left(\mathbf{A}^{(n)}\mathbf{P}^{(n)}\right)\underline{\gamma}, \end{aligned} \tag{21}$$

where $\underline{e}_0^{(n)}$ is the 2^n-dimensional vector over $\mathbf{F}_2$ with 1 exactly at the position belonging to the index $i = 0$. Thus if $\underline{k} = \underline{\gamma}$, then

$$\underline{e}_0^{(n)} + \underline{\gamma} = \left(\mathbf{A}^{(n)}\mathbf{P}^{(n)}\right)\underline{\gamma} = \mathbf{U}^{(n)}\underline{\gamma}. \tag{22}$$

If $\underline{u} \in \mathbf{F}_2^{2^n}$ is the solution of the previous equation then

$$\begin{aligned} 1 \oplus \bigoplus_{i=0}^{2^n-1} u_i &= (1 \oplus u_0) \oplus \bigoplus_{i=1}^{2^n-1} (0 \oplus u_i) = \\ &= \bigoplus_{i=0}^{2^n-1} \left(\left(\underline{e}_0^{(n)}\right)_i \oplus u_i\right) = \bigoplus_{i=0}^{2^n-1} \left(\underline{e}_0^{(n)} + \underline{u}\right)_i = \\ &= \bigoplus_{i=0}^{2^n-1} \left(\mathbf{U}^{(n)}\underline{u}\right)_i = \bigoplus_{i=0}^{2^n-1} \bigoplus_{j=0}^{2^n-1} U_{i,j}^{(n)} u_j = \bigoplus_{j=0}^{2^n-1} u_j \bigoplus_{i=0}^{2^n-1} U_{i,j}^{(n)} = \\ &= \bigoplus_{j=0}^{2^n-1} u_j \delta_{0,j} = u_0 \end{aligned} \tag{23}$$

and from here we get that

$$1 = u_0 \oplus \bigoplus_{i=0}^{2^n-1} u_i = \bigoplus_{i=1}^{2^n-1} u_i. \tag{24}$$

If $n=0$, then $1=\bigoplus_{i=1}^{2^0-1}u_i=\bigoplus_{i=1}^{0}u_i=0$, which is a contradiction. If $n=1$, then with $1=\bigoplus_{i=1}^{2^1-1}u_i=\bigoplus_{i=1}^{1}u_i=u_1$

$$
\begin{aligned}
1\oplus u_0 &= \left(\underline{e}_0^{(1)}+\underline{u}\right)_0=\left(\mathbf{U}^{(1)}\underline{u}\right)_0=\bigoplus_{j=0}^{2^1-1}U_{0,j}^{(1)}u_j= \\
&= 0\cdot u_0\oplus 1\cdot u_1=u_1=1,
\end{aligned}
\tag{25}
$$

that is $\underline{u}=01$ is a solution. If $\underline{\gamma}=\underline{u}$, then the appropriate Boolean function is the following:

$$
\begin{aligned}
f^{(1)}(x_0) &= \prod_{i=0}^{2^1-1}\left(\overline{\gamma}_i+M_i^{(n)\prime}\right)= \\
&= \left(\overline{0}+M_0^{(1)\prime}\right)\left(\overline{1}+M_1^{(1)\prime}\right)= \\
&= (1+\overline{x}_0)(0+x_0)=1\cdot x_0=x_0.
\end{aligned}
\tag{26}
$$

Finally let $n\geq 2$. Then

$$
\begin{aligned}
\bigoplus_{i=1}^{2^{n-1}-2}u_i\oplus u_{2^{n-1}} &= \bigoplus_{i=1}^{2^{n-1}-2}(0\oplus u_i)\oplus(0\oplus u_{2^{n-1}})= \\
&= \bigoplus_{i=1}^{2^{n-1}-2}\left(\left(\underline{e}_0^{(n)}\right)_i\oplus u_i\right)\oplus\left(\left(\underline{e}_0^{(n)}\right)_{2^{n-1}}\oplus u_{2^{n-1}}\right)= \\
&= \bigoplus_{i=1}^{2^{n-1}-2}\left(\underline{e}_0^{(n)}+\underline{u}\right)_i\oplus\left(\underline{e}_0^{(n)}+\underline{u}\right)_{2^{n-1}}= \\
&= \bigoplus_{i=1}^{2^{n-1}-2}\left(\mathbf{U}^{(n)}\underline{u}\right)_i\oplus\left(\mathbf{U}^{(n)}\underline{u}\right)_{2^{n-1}}= \\
&= \bigoplus_{i=1}^{2^{n-1}-2}\bigoplus_{j=0}^{2^n-1}U_{i,j}^{(n)}u_j\oplus\bigoplus_{j=0}^{2^n-1}U_{2^{n-1},j}^{(n)}u_j= \\
&= \bigoplus_{j=0}^{2^n-1}\left(\bigoplus_{i=1}^{2^{n-1}-2}U_{i,j}^{(n)}\right)u_j\oplus\bigoplus_{j=0}^{2^n-1}U_{2^{n-1},j}^{(n)}u_j= \\
&= \bigoplus_{j=2^{n-1}+1}^{2^n-2}u_j\oplus(u_{2^{n-1}-1}\oplus u_{2^n-1})= \\
&= \bigoplus_{j=2^{n-1}-1}^{2^n-1}u_j\oplus u_{2^{n-1}},
\end{aligned}
\tag{27}
$$

so $\bigoplus_{i=1}^{2^{n-1}-2} u_i = \bigoplus_{i=2^{n-1}-1}^{2^n-1} u_i$ and rearranging we get $\bigoplus_{i=1}^{2^n-1} u_i = 0$. Comparing this result with the earlier result in (24) that is $\bigoplus_{i=1}^{2^n-1} u_i = 1$ we get that $0 = 1$, which is an obvious impossibility.

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, *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*, **79** (1961), 808-814.

[4] **Davio M., Deschamps J.-P. and Thayse A.,** *Discrete and switching functions*, Georgi Publishing Co., St., 1978. (with a foreword by Raymond T. Yeh)

[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.,** Conjunctively polynomial-like Boolean functions. *Acta Mathematica Academiae Paedagogicae Nyíregyháziensis*, **23** (2) (2007), 89-103.

[8] **Lechner R.J.,** Harmonic analysis of switching functions, *Recent Developments in Switching Theory*, Academic Press, New York, 1971, 121-228.

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

[10] **Post E.L.,** *Two-valued iterative systems of mathematical logic,* Annals of Mathematics Studies **5**, Princeton University Press, Princeton, N. Y., 1941.

(Received August 29, 2010)

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