TRANSFORMATION OF THE CANONICAL DISJUNCTIVE NORMAL FORM OF A BOOLEAN FUNCTION TO ITS ZHEGALKIN-POLYNOMIAL AND BACK

J. Gonda (Budapest, Hungary)

Abstract. A Boolean function can be given in several forms. One of these forms is the canonical disjunctive normal form and another one the Zhegalkin-polynomial. These forms - apart from the order of the terms occurring in them - are uniquely determined by the function. In this article we give a linear algebraic aspect of the connection between these two forms.

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 $^-$. 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; $\mathbb{N}_0$ denotes the non-negative integers, and $\mathbb{N}$ the positive ones.

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* (hereafter abbreviated as CDNF), 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 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 $m_i^{(n)}$ 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 CDNF, so a Boolean function is uniquely determined by a 2^n long series 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 CDNF of the function contains the minterm with the index j, i.e. for $0 \leq k < 2^{2^n}$

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

where $k = \sum_{i=0}^{2^n-1} \alpha_i^{(k)} 2^i$, and $f_k^{(n)}$ denotes the k-th Boolean function of n variables.

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 $i = \sum_{j=0}^{n-1} a_j^{(i)} 2^j$. 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 $0 - 1$ series, and if the i-th member of such a series is k_i then

$$f^{(n)} = \bigoplus_{i=0}^{2^n-1} k_i S_i^{(n)}. \tag{3}$$

Now let us consider the $0 - 1$ series determining a canonical disjunctive normal form of a Zhegalkin polynomial of a Boolean function as elements of the 2^n-dimensional linear space $T^{(n)}$ over the field with two elements. $T^{(n)}$

contains 2^{2^n} vectors. Let $\underline{\alpha}^{(r)}$, where $0 \leq r = \sum_{i=0}^{2^n-1} \alpha_i^{(r)} 2^i < 2^{2^n}$, denote the vector whose i-th component is $\alpha_i^{(r)}$. Each element of the space determines one and only one logical function in the canonical disjunctive normal form and exactly one Zhegalkin polynomial of a logical function, so we can give a bijection $\varphi : T^{(n)} \longrightarrow T^{(n)}$ in such a way, that the vectors corresponding to each other determine the same Boolean function. A given correspondence $\underline{\alpha} \mapsto \underline{k}$, where $\underline{\alpha}$ and $\underline{k}$ determine the CDNF and the Zhegalkin-polynomial respectively can be computed by $m_i^{(n)} + m_j^{(n)} = m_i^{(n)} \oplus m_j^{(n)}$ and $\overline{u} = 1 \oplus u$, and by $S_i^{(n)} \oplus S_j^{(n)} = S_i^{(n)} \overline{S}_j^{(n)} + \overline{S}_i^{(n)} S_j^{(n)}$ in the other direction, but this is a rather long and badly algorithmisable procedure. It is more straightforward to give an easily treatable trasformation rule manipulating directly the vectors.

Let us see an example. If $n = 2$ and $k = 2$ then

$$\begin{aligned} f_2^{(2)} &= 0 \cdot m_0^{(2)} + 1 \cdot m_1^{(2)} + 0 \cdot m_2^{(2)} + 0 \cdot m_3^{(2)} = m_1^{(2)} = \\ &= \left(\overline{0} \oplus X_1\right) \left(\overline{1} \oplus X_0\right) = \overline{X}_1 X_0 = \\ &= (1 \oplus X_1) X_0 = X_0 \oplus X_1 X_0 = \\ &= \left(\overline{0} + X_1\right) \left(\overline{1} + X_0\right) \oplus \left(\overline{1} + X_1\right) \left(\overline{1} + X_0\right) = \\ &= 0 \cdot S_0^{(2)} \oplus 1 \cdot S_1^{(2)} \oplus 0 \cdot S_2^{(2)} \oplus 1 \cdot S_3^{(2)}, \end{aligned}$$

so $\varphi((0,1,0,0)) = (0,1,0,1)$. If $n = 2$ and $k = 8$ then

$$f_8^{(2)} = m_3^{(2)} = X_1 X_0 = S_3^{(2)},$$

that is $\varphi((0,0,0,1)) = (0,0,0,1)$. Finally

$$\begin{aligned} f_2^{(2)} \oplus f_8^{(2)} &= m_1^{(2)} \oplus m_3^{(2)} = m_1^{(2)} + m_3^{(2)} = \overline{X}_1 X_0 + X_1 X_0 = X_0 = \\ &= S_1^{(2)} = \left(S_1^{(2)} \oplus S_3^{(2)}\right) \oplus S_3^{(2)} \end{aligned}$$

that means that

$$\begin{aligned} &\varphi((0,1,0,0) +_T (0,0,0,1)) = (0,1,0,0) = \\ &=(0,1,0,1) +_T (0,0,0,1) = \varphi((0,1,0,0)) +_T \varphi((0,0,0,1)), \end{aligned}$$

where $+_T$ denotes the addition on $T^{(n)}$.

From the last result we get the following

Theorem 1. *The mapping* $\varphi : T^{(n)} \longrightarrow T^{(n)}$, *where* $\sum_{i=0}^{2^n-1} \alpha_i m_i^{(n)} = = \bigoplus_{i=0}^{2^n-1} (\varphi(\alpha))_i S_i^{(n)}$, *is a homomorphism.*

Proof. As $T^{(n)}$ is a linear space over the field of two elements, we only have to show that the mapping is sum preserving. Let $+_T$ denote the addition on $T^{(n)}$. If $\underline{\alpha}$ and $\underline{\beta}$ belong to $T^{(n)}$, then $(\underline{\alpha} +_T \underline{\beta})_i = \alpha_i \oplus \beta_i$ for $2^n > i \in \mathbb{N}_0$, so

$$\bigoplus_{i=0}^{2^n-1} (\varphi(\underline{\alpha} +_T \underline{\beta}))_i S_i^{(n)} = \sum_{i=0}^{2^n-1} (\underline{\alpha} +_T \underline{\beta})_i m_i^{(n)} = \sum_{i=0}^{2^n-1} (\alpha_i \oplus \beta_i) m_i^{(n)} =$$

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

$$= \bigoplus_{i=0}^{2^n-1} (\varphi(\underline{\alpha}))_i S_i^{(n)} \oplus \bigoplus_{i=0}^{2^n-1} (\varphi(\underline{\beta}))_i S_i^{(n)} =$$

$$= \bigoplus_{i=0}^{2^n-1} ((\varphi(\underline{\alpha}))_i \oplus (\varphi(\underline{\beta}))_i) S_i^{(n)} = \bigoplus_{i=0}^{2^n-1} (\varphi(\underline{\alpha}) +_T \varphi(\underline{\beta}))_i S_i^{(n)}.$$

This means that $\varphi(\underline{\alpha} +_T \underline{\beta}) = \varphi(\underline{\alpha}) +_T \varphi(\underline{\beta})$, so φ preserves the sums.

From Theorem 1 and from the fact that φ is bijective follows that φ is an automorphism, so choosing a basis, the mapping can be given by a matrix. Let $b_j^{(i)} = \delta_{i,j}$ for the j-th component of the i-th vector of a basis, where $\delta_{i,j}$ is the Kronecker symbol and let $A^{(n)}$ denote the matrix of the transformation of the Boolean functions of n variables and $0^{(n)}$ the zero matrix of order 2^n.

The vectors of the basis given above belong to the minterms, so the i-th column of $A^{(n)}$ gives the Zhegalkin-polynomial of $m_i^{(n)}$. For instance if $n = 2$ than

$$\begin{aligned} m_0^{(2)} &= \overline{X}_1 \overline{X}_0 = \\ &= 1 \oplus X_0 \oplus X_1 \oplus X_1 X_0 = \\ &= 1 \cdot S_0^{(2)} \oplus 1 \cdot S_1^{(2)} \oplus 1 \cdot S_2^{(2)} \oplus 1 \cdot S_3^{(2)}, \end{aligned}$$

$$\begin{aligned} m_1^{(2)} &= \overline{X}_1 X_0 = \\ &= X_0 \oplus X_1 X_0 = \\ &= 0 \cdot S_0^{(2)} \oplus 1 \cdot S_1^{(2)} \oplus 0 \cdot S_2^{(2)} \oplus 1 \cdot S_3^{(2)}, \end{aligned}$$

$$\begin{aligned} m_2^{(2)} &= X_1\overline{X}_0 = \\ &= X_1 \oplus X_1X_0 = \\ &= 0\cdot S_0^{(2)} \oplus 0\cdot S_1^{(2)} \oplus 1\cdot S_2^{(2)} \oplus 1\cdot S_3^{(2)}, \\ m_3^{(2)} &= X_1X_0 = \\ &= 0\cdot S_0^{(2)} \oplus 0\cdot S_1^{(2)} \oplus 0\cdot S_2^{(2)} \oplus 1\cdot S_3^{(2)} \end{aligned}$$

and in a concise form

$$\begin{array}{cccccc} & & \varphi\left(m_0^{(2)}\right) & \varphi\left(m_1^{(2)}\right) & \varphi\left(m_2^{(2)}\right) & \varphi\left(m_3^{(2)}\right) \\ & & \downarrow & \downarrow & \downarrow & \downarrow \\ S_0^{(2)} & \rightarrow & 1 & 0 & 0 & 0 \\ S_1^{(2)} & \rightarrow & 1 & 1 & 0 & 0 \\ S_2^{(2)} & \rightarrow & 1 & 0 & 1 & 0 \\ S_3^{(2)} & \rightarrow & 1 & 1 & 1 & 1 \end{array}$$

The structure of $A^{(n)}$ is very simple.

Theorem 2.

$$A^{(n)} = \begin{cases} (1), & \text{if } n = 0, \\ \begin{pmatrix} A^{(n-1)} & 0^{(n-1)} \\ A^{(n-1)} & A^{(n-1)} \end{pmatrix}, & \text{if } n \in \mathbb{N}. \end{cases} \tag{4}$$

Proof. As the empty product is 1 and $2^0 = 1$, so $m_0^{(0)} = 1 = S_0^{(0)}$. Then

$$\bigoplus_{i=0}^{0} (\varphi(\underline{\alpha}))_i S_i^{(0)} = \sum_{i=0}^{0} \alpha_i m_i^{(0)} = \alpha_0 \cdot 1 = \bigoplus_{i=0}^{0} \alpha_0 S_i^{(0)}.$$

That means, that $\underline{\alpha} = \varphi(\underline{\alpha}) = A^{(0)}\underline{\alpha}$, i.e. $A^{(0)} = I^{(0)}$, where $I^{(n)}$ denotes the unit matrix of order 2^n for any non-negative integer n.

Now let $f^{(n+1)} = \sum_{i=0}^{2^{n+1}} \alpha_i m_i^{(n+1)} = \bigoplus_{i=0}^{2^{n+1}} k_i S_i^{(n+1)}$ be a Boolean function of $n+1$ variables, where $\underline{k} = \varphi(\underline{\alpha}) = A^{(n+1)}\underline{\alpha}$. Then both $\underline{\alpha}$ and $\underline{k}$ are vectors of dimension 2^{n+1}. Let $\underline{\alpha}^{[0]}$ and $\underline{\alpha}^{[1]}$ denote the first 2^n and the last 2^n components of $\underline{\alpha}$ respectively, and let $A^{(n+1)} = \begin{pmatrix} P & Q \\ R & T \end{pmatrix}$, where the submatrices are of order 2^n. With these notations $A^{(n+1)}\underline{\alpha} = \begin{pmatrix} P\underline{\alpha}^{[0]} & + & Q\underline{\alpha}^{[1]} \\ R\underline{\alpha}^{[0]} & + & T\underline{\alpha}^{[1]} \end{pmatrix}$, so $\left(A^{(n+1)}\underline{\alpha}\right)_i = \left(P\underline{\alpha}^{[0]} + Q\underline{\alpha}^{[1]}\right)_i$, when $0 \le i < 2^n$, and $\left(A^{(n+1)}\underline{\alpha}\right)_i = = \left(R\underline{\alpha}^{[0]} + T\underline{\alpha}^{[1]}\right)_{i-2^n}$, when $2^n \le i < 2^{n+1}$. On the other hand

$$\bigoplus_{i=0}^{2^{n+1}-1} \left(A^{(n+1)}\underline{\alpha}\right)_i S_i^{(n+1)} = \sum_{i=0}^{2^{n+1}-1} \alpha_i m_i^{(n+1)} = \bigoplus_{i=0}^{2^{n+1}-1} \alpha_i m_i^{(n+1)} =$$

$$= \bigoplus_{i=0}^{2^n-1} \alpha_i \left(m_i^{(n)}\overline{X}_{n+1}\right) \oplus \bigoplus_{i=2^n}^{2^{n+1}-1} \alpha_i \left(m_{i-2^n}^{(n)} X_{n+1}\right) =$$

$$= (1 \oplus X_{n+1}) \bigoplus_{i=0}^{2^n-1} \alpha_i m_i^{(n)} \oplus X_{n+1} \bigoplus_{i=0}^{2^n-1} \alpha_{2^n+i} m_i^{(n)} =$$

$$= \bigoplus_{i=0}^{2^n-1} \alpha_i m_i^{(n)} \oplus X_{n+1} \bigoplus_{i=0}^{2^n-1} (\alpha_i \oplus \alpha_{2^n+i})\, m_i^{(n)} =$$

$$= \bigoplus_{i=0}^{2^n-1} \left(A^{(n)}\underline{\alpha}^{[0]}\right)_i S_i^{(n)} \oplus \bigoplus_{i=0}^{2^n-1} \left(A^{(n)}\left(\underline{\alpha}^{[0]} + \underline{\alpha}^{[i]}\right)\right)_i \left(S_i^{(n)} X_{n+1}\right) =$$

$$= \bigoplus_{i=0}^{2^n-1} \left(A^{(n)}\underline{\alpha}^{[0]} + 0^{(n)}\underline{\alpha}^{[1]}\right)_i S_i^{(n+1)} \oplus \bigoplus_{i=2^n}^{2^{n+1}-1} \left(A^{(n)}\underline{\alpha}^{[0]} + A^{(n)}\underline{\alpha}^{[1]}\right)_{i-2^n} S_i^{(n+1)}$$

and with the previous result for $A^{(n+1)}\underline{\alpha}$ we can see, that

$$A^{(n+1)} = \begin{pmatrix} A^{(n)} & 0^{(n)} \\ A^{(n)} & A^{(n)} \end{pmatrix}.$$

As the mapping detemined by $A^{(n)}$ is an automorphism, it has an inverse. Now we give the inverse of $A^{(n)}$. First of all we consider again the case of $n = 2$:

$$\begin{aligned} S_0^{(2)} &= 1 = \\ &= \overline{X}_1\overline{X}_0 + \overline{X}_1 X_0 + X_1\overline{X}_0 + X_1 X_0 = \\ &= 1 \cdot m_0^{(2)} + 1 \cdot m_1^{(2)} + 1 \cdot m_2^{(2)} + 1 \cdot m_3^{(2)}, \end{aligned}$$

$$\begin{aligned} S_1^{(2)} &= X_0 = \\ &= \overline{X}_1 X_0 + X_1 X_0 = \\ &= 0 \cdot m_0^{(2)} + 1 \cdot m_1^{(2)} + 0 \cdot m_2^{(2)} + 1 \cdot m_3^{(2)}, \end{aligned}$$

$$\begin{aligned} S_2^{(2)} &= X_1 = \\ &= X_1\overline{X}_0 + X_1 X_0 = \\ &= 0 \cdot m_0^{(2)} + 0 \cdot m_1^{(2)} + 1 \cdot m_2^{(2)} + 1 \cdot m_3^{(2)}, \end{aligned}$$

$$\begin{aligned} S_3^{(2)} &= X_1 X_0 = \\ &= 0 \cdot m_0^{(2)} + 0 \cdot m_1^{(2)} + 0 \cdot m_2^{(2)} + 1 \cdot m_3^{(2)} \end{aligned}$$

and then

$$\begin{array}{ccccccc} & & \varphi^{-1}\left(S_0^{(2)}\right) & \varphi^{-1}\left(S_1^{(2)}\right) & \varphi^{-1}\left(S_2^{(2)}\right) & \varphi^{-1}\left(S_3^{(2)}\right) \\ & & \downarrow & \downarrow & \downarrow & \downarrow \\ m_0^{(2)} & \longrightarrow & 1 & 0 & 0 & 0 \\ m_1^{(2)} & \longrightarrow & 1 & 1 & 0 & 0 \\ m_2^{(2)} & \longrightarrow & 1 & 0 & 1 & 0 \\ m_3^{(2)} & \longrightarrow & 1 & 1 & 1 & 1 \end{array}$$

Comparing this table with the one on page 151 we see that in that special case the inverse of the matrix of the transformation is the same as the matrix of the original mapping. This is no accident:

Theorem 3. *For any non-negative integer n the inverse of $A^{(n)}$ is itself, that is*

$$A^{(n)^{-1}} = A^{(n)}, \tag{5}$$

Proof. $A^{(0)^{-1}} = I^{(0)^{-1}} = I^{(0)} = A^{(0)}$; if $n \in N_0$, and $A^{(k)}A^{(k)} = I^{(k)}$ for any non-negative integer k less than or equal to n then

$$A^{(n+1)}A^{(n+1)} = \begin{pmatrix} A^{(n)} & 0^{(n)} \\ A^{(n)} & A^{(n)} \end{pmatrix} \begin{pmatrix} A^{(n)} & 0^{(n)} \\ A^{(n)} & A^{(n)} \end{pmatrix} = \begin{pmatrix} I^{(n)} & 0^{(n)} \\ 0^{(n)} & I^{(n)} \end{pmatrix} = I^{(n+1)},$$

because $A^{(n)}A^{(n)} + A^{(n)}A^{(n)} = 0^{(n)}$, so the proposition is true for any $n \in N_0$.

$A^{(n)}$ is a $2^n \times 2^n$ matrix, and $2^n \times 2^n = 2^{2n}$ is a big number even if n is relatively small. That fact can cause problems in storing the matrix. However, the elements of $A^{(n)}$ can be calculated directly from the indices.

Theorem 4. $A_{i,k}^{(n)} = \prod\limits_{j=0}^{n-1} \left(a_j^{(i)} + \overline{a}_j^{(k)}\right)$, *where $a_r^{(s)}$ is the r-th digit in the binary expansion of the non-negative integer s, and + denotes the logical sum.*

Proof.

$$\bigoplus_{i=0}^{2^n-1}\left(\bigoplus_{k=0}^{2^n-1} A_{i,k}^{(n)}\alpha_k\right) S_i^{(n)} = \bigoplus_{i=0}^{2^n-1} k_i S_i^{(n)} = \sum_{k=0}^{2^n-1}\alpha_k m_k^{(n)} = \bigoplus_{k=0}^{2^n-1}\alpha_k m_k^{(n)} =$$

$$= \bigoplus_{k=0}^{2^n-1}\left(\alpha_k \prod_{j=0}^{n-1}\left(\overline{a}_j^{(k)}\oplus X_j\right)\right) =$$

$$= \bigoplus_{k=0}^{2^n-1}\left(\alpha_k\left(\bigoplus_{i=0}^{2^n-1}\prod_{j=0}^{n-1}\left(\left(a_j^{(i)}+\overline{a}_j^{(k)}\right)\left(\overline{a}_j^{(i)}+X_j\right)\right)\right)\right) =$$

$$= \bigoplus_{i=0}^{2^n-1}\left(\left(\bigoplus_{k=0}^{2^n-1}\left(\alpha_k\prod_{j=0}^{n-1}\left(a_j^{(i)}+\overline{a}_j^{(k)}\right)\right)\right)\prod_{j=0}^{n-1}\left(\overline{a}_j^{(i)}+X_j\right)\right) =$$

$$= \bigoplus_{i=0}^{2^n-1}\left(\bigoplus_{k=0}^{2^n-1} c_{i,k}\alpha_k\right) S_i^{(n)},$$

so $\bigoplus_{i=0}^{2^n-1}\left(\bigoplus_{k=0}^{2^n-1}\left(A_{i,k}^{(n)}-c_{i,k}\right)\alpha_k\right) S_i^{(n)} = 0$. In the Zhegalkin-polynomial of a Boolean function the coefficients are uniquely determined, that means each coefficient of $S_i^{(n)}$ is 0 in the previous sum, so $\bigoplus_{k=0}^{2^n-1}\left(A_{i,k}^{(n)}-c_{i,k}\right)\alpha_k = 0$ for every non-negative integer t less than 2^n. Since that equality must be fulfilled for every vector $\underline{\alpha}$, so for every non-negative integers i and k less than 2^n

$$A_{i,k}^{(n)} = c_{i,k} = \prod_{j=0}^{n-1}\left(a_j^{(i)}+\overline{a}_j^{(k)}\right)$$

which is exactly the proposition formulated in the theorem.

Corollary. *Let* $0 \le 0 \le 1 \le 1$ *for the two elements of the field of two elements, and* $\underline{\alpha} \preceq \underline{\beta}$ *for the vectors* $\underline{\alpha}$ *and* $\underline{\beta}$ *of the n-dimensional linear space over that field if and only if for every index i, where* $0 \le i < n$, $\alpha_i \le \beta_i$. *Then* $A_{i,k}^{(n)} = 1$ *exactly in that case, when* $\underline{a}^{(k)} \preceq \underline{a}^{(i)}$, *where* $t = \sum_{j=0}^{n-1} a_j^{(t)}2^j$ *for every non-negative integer t less than* 2^n.

Proof. $A_{i,k}^{(n)} = \prod_{j=0}^{n-1}\left(a_j^{(i)}+\overline{a}_j^{(k)}\right) = 1$ if and only if in the logical product the value of each term is equal to 1. However $a_j^{(i)}+\overline{a}_j^{(k)} = 1$ is true exactly in that case, if in all cases when $\overline{a}_j^{(k)} = 0$, i.e. when $a_j^{(k)} = 1$, $a_j^{(i)} = 1$ is fulfilled, too. Considering that the value of every $a_u^{(v)}$ is 0 or 1, this means that $a_j^{(k)} \leq a_j^{(i)}$ for every index $0 \leq j < n$.

With the help of Theorem 4 and the subsequent corollary we can give an algorithm generating the elements of $A_{i,k}^{(n)}$ from the input data i, k and n.

```
procedure gener $(i,k,n,t)$ $[n \in N_0.\ 2^n > i \in \mathbb{N}_0,\ 2^n > k \in \mathbb{N}_0,\ t \in \{0,1\}]$
    $t := 1$
    $u := 2^{n-1}$
    while $u \geq 1$
        if $i < k$ then
            $t := 0$
            $u := 0$
        elseif $u \leq i$ then
            $i := i - u$
            if $u \leq k$ then
                $k := k - u$
            end if
        end if
        $u := u$ div 2
    end while
end procedure
```

In that procedure **div** denotes the integer division, i.e. if u and $v \neq 0$ are integers, then u **div** $v := \left\lfloor \frac{u}{v} \right\rfloor$; t is the result of the procedure, and $A_{i,k}^{(n)} = t$.

Now we give some simple properties characterising the matrix $A^{(n)}$:

Theorem 5. *$A^{(n)}$ has the following properties:*

1. bottom triangle-matrix;

2. all elements in the main diagonal are 1;

3. the matrix is symmetrical for the subdiagonal;

4. the elements of the subdiagonal are 0 with the exception of the element in the left bottom corner;

5. the elements of the 0. column are 1.

Proof. All of the above mentioned properties are true if $n = 0$, and taking into consideration the structure of $A^{(n)}$, namely that $A^{(n+1)} = \begin{pmatrix} A^{(n)} & 0^{(n)} \\ A^{(n)} & A^{(n)} \end{pmatrix}$, we get the proof by induction on n.

References

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

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

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

(Received October 20, 1999; revised September 22, 2000)

J. Gonda
Department of Computer Algebra
Eötvös Loránd University
P.O.B. 32
H-1518 Budapest, Hungary