Proceedings of Fourth International Conference «Computer-Aided Design of Discrete Devices» (CAD DD'2001), Mink, 2001, vol. 1, pp. 69-76.

FUNDAMENTAL THEOREMS FOR POLYNOMIAL REPRESENTAION OF DISCRET FUNCTIONS

VALERY VYKHOVANETS

Bureau of Computer Science, Trans-Dniester State University, Tiraspol, Moldova, vykhovanets@ucsd.com

Abstract. This paper considers the sum-of-product expansions of discrete functions over various algebraic systems. Decomposition theorem over logic algebra, multiplicative algebra, additive algebra, finite field and integral domain are discussed. Synthesis of generalized polynomial form is developed. An algorithm for computing the coefficients of polynomial form over such algebraic systems, based on matrix manipulation, is given.

Key Words. Discrete function, various valency, sum-of-product expansion, spectral decomposition, polynomial form.

1. INTRODUCTION

The development of digital circuits by means of CAD (Computer-Aided Design) systems has a strong influence on many areas of computer science. Applications in information processing, telecommunication or in industrial control systems permanently require the construction of more and more powerful high-speed circuits. One of the main problems here is to get the immensely increasing complexity of mathematical objects, the so-called *combinatorial explosion*, under control.

A central problem in the design of CAD systems for VLSI (Very Large Scale Integration) is to represent functional behavior of a circuit based on discrete function decomposition. Logic design is normally thought of in terms of binary signals; however for high level design it is natural to think of variables with many values. The process of converting these multi-valued variables to binary signals is called *encoding*.

The binary signals are often associated with binary functions of binary variables. In many cases the encoding is done initially, mostly arbitrary, and then binary valued logic synthesis is applied to the resulting circuit. An alternative is to first manipulate and optimize the discrete function directly. Then the resulting form of the network can be used to select a good encoding.

Many problems in computer-aided design of highly integrated circuits can be transformed to the task of manipulation objects over finite domain. The efficiency of these operations depends substantially on the chosen formal representation of discrete functions.

2. NOTATION

Let a *domain* N_k is a finite set of integers $\{0,1,\ldots,k-1\}$ and a multiple-valued variable x_i can take on values from N_{k_i}; x_i is called the variable with valency k_i.

Definition 1. A *discrete function* or k_f-valued m-function f is a function, which maps domain N_m to domain N_{k_f}, formally, $f : N_m \to N_{k_f}$. The valency of this function is k_f.

If $m = k_0 k_1 \ldots k_{n-1}$ then any m-function f can be represented as

$$f : N_{k_0} \times N_{k_1} \times \ldots \times N_{k_{n-1}} \to N_{k_f}.$$

We determine a linkage between value i of variable x and values i_j of variables x_j ($j=\overline{0,n-1}$) by the $k_{n-1}\ldots k_1k_0$-ary expansion of i,

$$i=(i_{n-1},\ldots,i_1,i_0)_{k_{n-1}\ldots k_1k_0}, \qquad (1)$$

where i_0 is the least significant digit.

Example 1. An example of discrete function $F=[3\,0\,1\,2\,2\,1]$ is shown in Table 1. Assume that $k_0=2$, $k_1=3$, $k_f=4$, $N_{k_0}=\{0,1\}$ $N_{k_1}=\{0,1,2\}$ and $N_{k_f}=\{0,1,2,3\}$.

Table 1. A 4-valued 6-finction

x_1	x_0	$f(x_0,x_1)$
0	0	3
0	1	0
0	2	1
1	0	2
1	1	2
1	2	1

Definition 2. A *discrete operation* is a discrete function that essentially depends on its variables.

3. DECOMPOSITION THEOREMS

Let $R=\langle N_k,+,\cdot\rangle$ is an algebraic system, where k is the valency of algebra and $+$ ($\cdot$) is called addition (multiplication). Let a m-function f be depended on two variables: $x'\in N_{k'}$ and $x''\in N_{k''}$, such that $k'k'''=m$. We write the function f in the form of a sum-of-product expansion over R,

$$f(x',x'')=\sum_{i=0}^{k'-1}\theta_i(x')\cdot a_i(x''), \qquad (2)$$

where $k_f\le k$; $a_i\in N_k$ are coefficients (k-valued k''-functions); $\theta_i\in N_k$ are spectral functions (k-valued k''-functions). Equation (2) can be written for each of x' values:

$$\begin{cases} f(0,x'')=\theta_0(0)\cdot a_0(x'')+\ldots+\theta_{k'-1}(0)\cdot a_{k'-1}(x''); \\ f(1,x'')=\theta_0(1)\cdot a_0(x'')+\ldots+\theta_{k'-1}(1)\cdot a_{k'-1}(x''); \\ \dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots \\ f(k'-1,x'')=\theta_0(k'-1)\cdot a_0(x'')+\ldots+\theta_{k'-1}(k'-1)\cdot a_{k'-1}(x'') \end{cases}$$

The expression (2) also can be written as a matrix equation $F=D\times A$ (if there exist Q such that $A=Q\times F$, $Q\times D=I$ we have orthogonal transformation), where F (A) is a $k'\times k''$-matrix, D (Q, I) is a direct (inverse, unit) $k'\times k'$-matrix. We will designate a computation of the matrix Q by the unary matrix operation μ: $Q=\mu D$.

One can see that a column of matrix D is a characteristic vector of some function θ_i. In turn a column of matrix Q is a characteristic vector of some function ϑ_i. The functions ϑ_i are orthogonal to θ_i in restricted sense.

Definition 3. A function system θ_i ($i=\overline{0,k'-1}$) is a *fundamental* over R if adding and multiplication of those functions are commutative, associative and distributive: i.e. for all x, y, $z\in N_{k'}$,

$$\theta_i(x)*\theta_j(y)=\theta_j(y)*\theta_i(x);$$
$$\theta_i(x)*\{\theta_j(y)*\theta_t(z)\}=\{\theta_i(x)*\theta_j(y)\}*\theta_t(z);$$
$$\theta_i(x)\cdot\{\theta_j(y)+\theta_t(z)\}=\theta_i(x)\cdot\theta_j(y)+\theta_i(x)\cdot\theta_t(z),$$

where * is addition or multiplication.

Note the fundamental function is a homomorphism N_k into some subset of N_k, where addition and multiplication are commutative, associative and distributive.

There are a few algebraic systems, which allow finding a_i from (2). The type of sum-of-product expansion is defined by formative operation $\{+,\cdot\}$. For Boolean function it is used the operations of canonical bases Bool [1], Zhegalkin [2], arithmetical [3]. For multiple-valued function it is used such formative operations as maximum and minimum [4], addition modulo k and minimum [5], arithmetic addition and digit-to-digit operation [6], operations of ring of integers [7] and finite field [8].

3.1. Logic algebra

Let $R_L=\langle N_k,+,\cdot\rangle$ be a *logic algebra* and there exists $\sigma\in N_k$ and $\imath\in N_k$ ($\imath\ne\sigma$) such that $a+\sigma=a$, $\sigma+a=a$ and $\sigma\cdot a=\sigma$, $\imath\cdot a=\imath$ for all $a\in N_k$. Element σ is called zero and element $\imath$ is called unit.

Definition 4. A *permutation matrix* $P_{k'}$ is a $k'\times k'$-matrix, each of whose rows and columns has only one nonzero element and this element is unit.

Theorem 1. A function f can be decomposed in the form (2) over R_L if D is a permutation matrix $P_{k'}$.

Then $Q = D^T$ and $Q \times D = I$, where T denotes a transposition operation of matrix.

Example 1. Let a addition and a multiplication are operations defined by matrix S and P such that $s_{ij} = i + j$ and $p_{ij} = i \cdot j$,

$$S = \begin{bmatrix} 0 & 1 & 2 & 3 \\ 1 & * & * & * \\ 2 & * & * & * \\ 3 & * & * & * \end{bmatrix}, \; P = \begin{bmatrix} 0 & 0 & 0 & 0 \\ * & * & * & * \\ * & * & * & * \\ 0 & 1 & 2 & 3 \end{bmatrix},$$

where * is an indifference value. Obviously $\sigma = 0$ and $\imath = 3$. Then for the function from Example 1 we have

$$D = \begin{bmatrix} \theta_0(0) & \theta_1(0) & \theta_2(0) \\ \theta_0(1) & \theta_1(1) & \theta_2(1) \\ \theta_0(2) & \theta_1(2) & \theta_2(2) \end{bmatrix} = \begin{bmatrix} 0 & 0 & 3 \\ 3 & 0 & 0 \\ 0 & 3 & 0 \end{bmatrix},$$

$$Q = \begin{bmatrix} 0 & 3 & 0 \\ 0 & 0 & 3 \\ 3 & 0 & 0 \end{bmatrix}, \; A = Q \times \begin{bmatrix} f(0, x'') \\ f(1, x'') \\ f(2, x'') \end{bmatrix},$$

$$A = \begin{bmatrix} a_0(x'') \\ a_1(x'') \\ a_2(x'') \end{bmatrix} = \begin{bmatrix} 0 & 3 & 0 \\ 0 & 0 & 3 \\ 3 & 0 & 0 \end{bmatrix} \times \begin{bmatrix} 3 & 2 \\ 0 & 2 \\ 1 & 1 \end{bmatrix} = \begin{bmatrix} 0 & 2 \\ 1 & 1 \\ 3 & 2 \end{bmatrix},$$

$$f(x', x'') = \begin{bmatrix} 0 \\ 3 \\ 0 \end{bmatrix}(x') \cdot \begin{bmatrix} 0 \\ 2 \end{bmatrix}(x'') + \begin{bmatrix} 0 \\ 0 \\ 3 \end{bmatrix}(x') \cdot \begin{bmatrix} 1 \\ 1 \end{bmatrix}(x'') + \begin{bmatrix} 3 \\ 0 \\ 0 \end{bmatrix}(x') \cdot \begin{bmatrix} 3 \\ 2 \end{bmatrix}(x'').$$

where $[y_i](x) = y_x$ is a unary operation defined by a vector $[y_i]$.

There are two algebraic subsystems in the logic algebra: Boolean algebra $B_L = \langle B, \vee, \& \rangle$ [1] (if $\tau + \tau = \tau$) and Zhegalkin algebra $P_L = \langle B, \oplus, \& \rangle$ [2] (if $\tau + \tau = \sigma$), where $B = \{\sigma, \tau\}$; $\vee$, & and $\oplus$ are Boolean conjunction, disjunction and nonequivalence correspondingly. It is easy to prove if R_L includes B_L or P_L, then arbitrary matrix consist of zero or unit elements is fundamental. Otherwise a permutation matrix is fundamental only.

In the logic algebra R_L there are the following operations: addition modulo k, maximum, digit-to-digit disjunction (nonequivalence) as addition; and multiplication modulo k, minimum, digit-to-digit conjunction as multiplication. For digit-to-digit operations k must be a power of 2 (power of prime integer).

3.2. Multiplicative algebra

Let $R_M = \langle N_k, +, \cdot \rangle$ be a *multiplicative algebra* such as R_L. In addition to R_L, let $G_M = \langle N_k \setminus \{\sigma\}, \cdot \rangle$ is a group. In this case for all $a \in G_M$ there exists an inverse element $a^{-1} \in G_M$ such that $a \cdot a^{-1} = \imath$ and $a^{-1} \cdot a = \imath$.

Definition 5. A *monomial matrix* $M_{k'}$ is a $k' \times k'$-matrix; each of whose rows and columns has only one nonzero element.

Theorem 2**.** A function f can be decomposed in the form (2) over R_M if D is a monomial matrix $M_{k'}$. Then $Q = \tilde{D}^T$ and $Q \times D = I$, where $\tilde{D}$ is a matrix each of whose nonzero elements are replaced by its inverse elements.

Example 2. Let operations of R_M are

$$S = \begin{bmatrix} 0 & 1 & 2 & 3 \\ 1 & * & * & * \\ 2 & * & * & * \\ 3 & * & * & * \end{bmatrix}, \; P = \begin{bmatrix} 0 & 0 & 0 & 0 \\ 0 & 2 & 3 & 1 \\ 0 & 3 & 1 & 2 \\ 0 & 1 & 2 & 3 \end{bmatrix}.$$

The function from Example 1 can be written

$$f(x', x'') = \begin{bmatrix} 0 \\ 3 \\ 0 \end{bmatrix}(x') \cdot \begin{bmatrix} 0 \\ 2 \end{bmatrix}(x'') + \begin{bmatrix} 0 \\ 0 \\ 2 \end{bmatrix}(x') \cdot \begin{bmatrix} 2 \\ 2 \end{bmatrix}(x'') + \begin{bmatrix} 1 \\ 0 \\ 0 \end{bmatrix}(x') \cdot \begin{bmatrix} 2 \\ 1 \end{bmatrix}(x'').$$

Obviously, a function system and its matrix $M_{k'}$ are fundamental if multiplication of R is commutative.

3.3. Additive algebra

Let $R_A = \langle N_k, +, \cdot \rangle$ be an *additive algebra* such as R_L. In addition to R_L, let $G_A = \langle N_k, + \rangle$ is a commutative group.

Definition 6**.** A *cyclic order of element* $a \in G_A$ is a minimal whole number $c_a > 0$, such that cyclic sum

$$c_a \circ a = \underbrace{a + a + \ldots + a}_{c_a} = \sigma,$$

where σ is an identity element of G_A. Let $0 \circ a = \sigma$ and let $(-\lambda) \circ a = \lambda \circ (-a)$ where λ is an integer.

Definition 7. A *cyclic order of group* G_A is a minimal order of its elements except σ.

Lemma 3. Equation $\lambda \circ a = b$ has unique solution for all $a, b \in G_A$ if and only if $c < |\lambda|$, where c is a cyclic order of commutative group G_A.

Definition 8. A *logical matrix* $L_{k'}$ is a $k' \times k'$-matrix; each of whose elements is zero or unit. If we replace the elements of $L_{k'}$ with 0 and 1 respectively, we find matrix $\hat{L}_{k'}$. $\hat{L}_{k'}$ is called a conjugate matrix of $L_{k'}$.

Theorem 4. A function f can be decomposed in the form (2) over R_A if D is a logical matrix $L_{k'}$ and if the modulo of determinant of conjugate matrix $\hat{L}_{k'}$ less then a cyclic order of group G_A. Then $\Delta \circ A = \overline{D}^T \circ F$ where $\overline{D}$ is an algebraic complement $\hat{L}_{k'}$, Δ is a determinant of $\hat{L}_{k'}$.

Example 2. Let operations of R_A are

$$S = \begin{bmatrix} 0 & 1 & 2 & 3 \\ 1 & 0 & 3 & 2 \\ 2 & 3 & 0 & 1 \\ 3 & 2 & 1 & 0 \end{bmatrix}, \quad P = \begin{bmatrix} 0 & 0 & 0 & 0 \\ * & * & * & * \\ * & * & * & * \\ 0 & 1 & 2 & 3 \end{bmatrix}.$$

The function from Example 1 can be written

$$f(x', x'') = \begin{bmatrix} 3 \\ 3 \\ 0 \end{bmatrix}(x') \cdot \begin{bmatrix} 2 \\ 3 \end{bmatrix}(x'') + \begin{bmatrix} 3 \\ 0 \\ 3 \end{bmatrix}(x') \cdot \begin{bmatrix} 2 \\ 2 \end{bmatrix}(x'') + \begin{bmatrix} 0 \\ 3 \\ 0 \end{bmatrix}(x') \cdot \begin{bmatrix} 1 \\ 2 \end{bmatrix}(x'').$$

Obviously, if G_A is a cyclic group, then transform (2) is orthogonal when Δ is a divisor of number divisible by k. In this case equation $\Delta \circ a = b$ has unique solution $a = (qk/\Delta) \circ b$, $q \in Z$, and there exists a matrix $Q = (qk/\Delta)\overline{D}^T$. For all groups G_A, when $|\Delta| = 1$, we always have $Q = \Delta \overline{D}^T$.

Note the multiplication of R_A is used only for function computation, whereas for coefficients computation is used the cyclic sum of group G_A.

In the additive algebra R_L there are the following operations: addition modulo k, digit-to-digit nonequivalence as addition; and multiplication modulo k, minimum, digit-to-digit conjunction as multiplication.

3.4. Finite field

Let $R_F = \langle N_k, +, \cdot \rangle$ be a *finite field* of characteristic p. It is known the field R_F has p^q elements for some positive integer q, if p is a prime number, i.e. $k = p^q$.

Theorem 5. A function f can be decomposed in the form (2) over R_F if matrix D consist of elements from N_k and if a determinant of D over R_F is not equal to σ. Then $Q = D^{-1}$ and $Q \times D = I$, where D^{-1} is an inverse matrix of D calculated over R_F.

Example 3. Let a field R_F has operations

$$S = \begin{bmatrix} 0 & 1 & 2 & 3 \\ 1 & 0 & 3 & 2 \\ 2 & 3 & 0 & 1 \\ 3 & 2 & 1 & 0 \end{bmatrix}, \quad P = \begin{bmatrix} 0 & 0 & 0 & 0 \\ 0 & 2 & 3 & 1 \\ 0 & 3 & 1 & 2 \\ 0 & 1 & 2 & 3 \end{bmatrix}.$$

The function defined above can be written

$$f(x', x'') = \begin{bmatrix} 1 \\ 3 \\ 0 \end{bmatrix}(x') \cdot \begin{bmatrix} 2 \\ 1 \end{bmatrix}(x'') + \begin{bmatrix} 0 \\ 1 \\ 2 \end{bmatrix}(x') \cdot \begin{bmatrix} 3 \\ 2 \end{bmatrix}(x'') + \begin{bmatrix} 2 \\ 0 \\ 3 \end{bmatrix}(x') \cdot \begin{bmatrix} 2 \\ 0 \end{bmatrix}(x'').$$

3.5. Integral domain

A commutative ring $R_I = \langle N_k, +, \cdot \rangle$ with identity is called an *integral domain* if for all $a, b \in N_k$, $a \cdot b = \sigma$ implies $a = \sigma$ or $b = \sigma$. As is well known any finite integral domain must be a field. Let $R_I = \langle Z, +, \cdot \rangle$ is the ring of integers.

Theorem 6. A function f can be decomposed in the form (2) over R_I if matrix D consist of elements from Z and if the determinant of D is not equal to zero. Then $\Delta \cdot A = \overline{D}^T \cdot F$, $Q \times D = \Delta \cdot I$ and

$$f(x', x'') = \frac{1}{\Delta} \sum_{i=0}^{k'-1} \theta_i(x') \cdot \dot{a}_i(x''),$$

where $\overline{D}$ is an algebraic complement D, Δ is a determinant of D, $\dot{a}_j = \Delta \cdot a_j$, $\dot{a}_j \in Z$.

Example 4. Our function over the ring of integers can be written $f(x', x'') =$

$$=\frac{1}{5}\cdot\left(\begin{bmatrix}3\\1\\4\end{bmatrix}(x')\cdot\begin{bmatrix}2\\10\end{bmatrix}(x'')+\begin{bmatrix}-2\\0\\-1\end{bmatrix}(x')\cdot\begin{bmatrix}10\\15\end{bmatrix}(x'')+\begin{bmatrix}1\\2\\3\end{bmatrix}(x')\cdot\begin{bmatrix}-1\\-10\end{bmatrix}(x'')\right).$$

3.6. Functional completeness

As a matter of fact the equation (2) permits to evaluate the function f by calculating the function θ_i and a_i which have the lesser complexity than f has. The decomposition theorems declare conditions when basis $\Omega=\{+,\cdot,\{\theta_i\},\langle a\rangle\}$ has the functional completeness, where $\{\theta_i\}$ is a stated set of k'-functions, $\langle a\rangle$ is a class that includes all k''-functions. In extreme case, when $k'=m$ and $\langle a\rangle$ consists of constants, we have a spectral decomposition.

At the spectral decomposition some m-function expresses by m spectral functions which have the same complexity that the current function has. In the engineering it makes sense when the spectral functions have very effective realization. Therefore we will find such classes of k'-function.

4. POLYNOMIAL FORMS

The polynomial forms of Boolean and multiple-valued functions usually refer to the representation of functions over Boolean logic, the finite field and the integral domain [9]. Generalized polynomial form bases on sum-of-product expansion (2) over some algebraic system R described above. In this case the spectral functions θ_i depend on n variables and can be written so

$$\theta_i(x_0,x_1,\ldots,x_{n-1})=$$
$$=x_0^{i_0}\delta_0 x_1^{i_1}\delta_1\ldots\delta_{n-2}x_{n-1}^{i_{n-1}}\delta_{n-1}c_i \qquad (3)$$

where $x_j^{i_j}=x_j\gamma_j i_j$ are power functions of two variables γ_j, δ_j are connecting functions of two variables, c_i are arbitrary constants, $i=(i_{n-1}\ldots i_0)_{k'}$ is the $k_{n-1}\ldots k_1k_0$-ary expansion (1) of i, $k'=k_{n-1}\ldots k_1k_0$.

The using operation δ_{n-1} and constant c_i is equal unary operation $\gamma^{(i)}(x)=x\delta_{n-1}c_i$, which is defined for every polynomial function θ_i. It is permitted to use everywhere zero polynomial function over additive algebra, finite field and integral domain. In this case $\gamma^{(i)}$ reduces σ to nonzero value $\gamma^{(i)}(\sigma)\neq\sigma$.

The polynomial forms are known under the names of conjunctive (disjunctive), Zhegalkin, arithmetical, Walsh, and so on (see Table 2, 3).

Table 2. Polynomial forms of Boolean function

Form	R	δ_j	$x^i=$
Conjunctive	$\langle N_2,\vee,\&\rangle$	&	$\begin{cases}x, i=0\\ \bar{x}, i=1\end{cases}$
Zhegalkin	$\langle N_2,\oplus,\&\rangle$	&	$\begin{cases}x, i=0\\ \bar{x}, i=1\end{cases}$
Arithmetical	$\langle Z,+,\bullet\rangle$	&	$\begin{cases}1, i=0\\ x, i=1\end{cases}$
Walsh	$\langle Z,+,\bullet\rangle$	$\bullet$	$\begin{cases}1, i=0\\ -1, i=1\end{cases}$

Table 3. Polynomial forms of multi-valued function

Form	R	δ_j	x^i
Post	$\langle N_k,\max,\min\rangle$	min	$\begin{cases}k-1, i=x\\ 0, i\neq x\end{cases}$
Galois	$\langle N_k,+,\bullet\rangle$	$\bullet$	x^i (over R)
Arithmetical	$\langle Z,+,\bullet\rangle$	$\bullet$	x^i (over Z)
Walsh	$\langle Z,+,\bullet\rangle$	$\bullet$	$(-1)^{x+i\,(\mathrm{mod}\ k)}$

Theorem 7**.** A function f can be represented in the polynomial form over some algebraic system R if each of functions γ_j ($j=\overline{0,n-1}$) is operation and the every function δ_l ($l=\overline{0,n-1}$) is operation in domain defined by γ_l and γ_{l+1} ranges of values.

The Theorem 7 asserts that the matrix of the power function γ_j does not contain two equal rows (columns), and the matrix of connection function δ_r does not contain all equal rows (columns).

4.1. Polynomial form synthesis

The synthesis of some polynomial form is reduced to the matrix D construction according to the analytical expression of polynomial function (3). The next step of synthesis is the finding a vector of coefficients A for each characteristic vector of function f. To generalize the method of polynomial

form synthesis [10] we use the generalized kroneker product.

Definition 9**.** Let be a binary function δ and let be two matrices: $n_0 \times m_0$-matrix $A = \|a_{i_0 j_0}\|$ and $n_1 \times m_1$-matrix $B = \|b_{i_1 j_1}\|$. A *kroneker product* of A and B over δ is a matrix $C = A \otimes_\delta B$ with elements $c_{ij} = a_{i_0 j_0} \delta b_{i_1 j_1}$, where $i = (i_1\, i_0)_{n_1 n_0}$ and $j = (j_1\, j_0)_{m_1 m_0}$ are the $n_1 n_0$-ary and $m_1 m_0$-ary expansions (1) of integers i and j correspondingly.

It follows from Definition 9 that the matrix C is a block matrix, which consists of $n_1 \times m_1$ $n_0 \times m_0$-matrices $C_{i_1 j_1} = A \delta b_{i_1 j_1}$. We can also define the kroneker product as $C_{i_0 j_0} = a_{i_0 j_0} \delta B$. In the first case the kroneker product is called the left kroneker product and denoted as $\otimes$ or $\bar{\otimes}$. In the second case it is called the right kroneker product and denoted as $\vec{\otimes}$. The right kroneker product is known earlier as a direct (external) product of matrices.

Taking into account the definition 9 a matrix D can be calculated by the recurrent rule

$$\begin{cases} D_0 = \Gamma_0; \\ D_{j+1} = D_j \otimes_{\delta_j} \Gamma_{j+1} \ (j = \overline{0, n-2}); \\ D = D_{n-1} \delta_{n-1} C, \end{cases} \qquad (4)$$

where Γ_j is the matrix of power operation γ_j, C is a $k' \times k'$-matrix of constants, which consists of k' identical rows of k' arbitrary constants. For orthogonal transformations the matrix Q is calculated by invert conversion of D over R, $Q = \mu D$.

While synthesis occurs the valency of the variables and the valency of the operations must be in complete concordance. In Table 4 it is shown the valency restrictions of polynomial operations with boundary conditions $k^{(\gamma_0)} \le k_0^{(\delta_0)}$ and $k^{(\delta_{n-1})} \ge k$, where $k_0^{(*)}$, $k_1^{(*)}$ are the valencies of left, right operands of operation *, and $k^{(*)}$ is the valency of operation *; k_j is the valency of the variable x_j and k is the valency of the algebra R.

Table 4. The concordance of the valencies

	γ_j	δ_j
$k_0^{(*)}$	$k_0^{(\gamma_j)} \ge k_j$	$k_0^{(\delta_j)} \ge k^{(\delta_{j-1})}$
$k_1^{(*)}$	$k_1^{(\gamma_j)} \ge k_j$	$k_1^{(\delta_j)} \ge k^{(\gamma_{j+1})}$
$k^{(*)}$	$k^{(\gamma_j)} \le k_1^{(\delta_{j-1})}$	$k^{(\delta_j)} \le k_0^{(\delta_{j+1})}$

Example 5. We realize the function from Example 1 in polynomial form over multiplicative algebra from Example 2. In this case the operation δ_1 may be removed, the other operations we define so:

$$\gamma_0 = \begin{bmatrix} 2 & 3 & 2 \\ 2 & 2 & 0 \\ 1 & 2 & 2 \end{bmatrix}, \ \gamma_1 = \begin{bmatrix} 1 & 0 \\ 3 & 1 \end{bmatrix}, \ \delta_0 = \begin{bmatrix} 3 & 0 & 1 & 2 \\ 2 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 \\ 3 & 0 & 2 & 2 \end{bmatrix}.$$

Then we use the recurrent rule (4) and find:

$$D = \Gamma_0 \otimes_0 \Gamma_1 = \left[\begin{array}{ccc|ccc} 0 & 0 & 0 & 0 & 3 & 0 \\ 0 & 0 & 0 & 0 & 0 & 3 \\ 0 & 0 & 0 & 2 & 0 & 0 \\ \hline 0 & 2 & 0 & 0 & 0 & 0 \\ 0 & 0 & 2 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 \end{array}\right].$$

From Theorem 2 it is issued

$$Q = \mu D = \tilde{D}^T = \left[\begin{array}{ccc|ccc} 0 & 0 & 0 & 0 & 0 & 3 \\ 0 & 0 & 0 & 2 & 0 & 0 \\ 0 & 0 & 0 & 0 & 2 & 0 \\ \hline 0 & 0 & 2 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 \end{array}\right],$$

and, at last, $A = Q \times F = [111310]^T$.

Note that the number of nonzero coefficients of polynomial form over the logic and multiplicative algebra are equal the number of nonzero values of the function. It is allowed us to determine σ by viewing the truth table of the function on conditions that we wish to have the minimum of nonzero coefficients. As opposed to the logic algebra the multiplicative algebra permits to control the values of coefficients, for example, to minimize the memory requirement or to make identical the greatest number of the coefficients.

4.2. Reed-Muller form

Some generalizing of the polynomial representation is Reed-Muller form [11, 12], which have the following spectral functions:

$$\theta_i(x_0, x_1, \ldots, x_{n-1}) = \\ = \omega_0^{i_0}(x_0)\delta_0 \ldots \delta_{n-2}\, \omega_{n-1}^{i_{n-1}}(x_{n-1})\delta_{n-1}\, c_i, \qquad (5)$$

where ω_j ($j = \overline{0, n-1}$) are unary functions called polarity operations. The polarity operations from (5) assign preliminary transformations of the variables and it are in progress before execution the power operations γ_j:

$$\omega_j^{i_j}(x_j) = \omega(x_j)\,\gamma_j\, i_j .$$

Definition 10**.** A unary operation ω is called *reversible* if for each y exists a unique value of x that $\omega(x) = y$.

Theorem 8**.** A function f can be represented in the Reed-Muller form over some algebraic system R if it is fulfilled a requirements of the Theorem 7 and if ω_j ($j = \overline{0, n-1}$) are reversible operations.

The synthesis of Reed-Muller form can be executed by the recurrent rule (4) where it is used modifying matrices of the power operations $\Gamma_j^{\omega} = \omega(\Gamma_j)$.

The operations ω_j divide all k'-function into equivalence classes. It is permitted to synthesize the polynomial form to within one-to-one transformation of the variables. If it is found a compact representation of function f then the same representation will have $k_0!k_1!\ldots k_{n-1}!$ functions, which are gained by the every possible transformation.

4.3. Multiplicative form

The inverse matrix computation over the logic (multiplicative) algebra is reduced to the transposition of matrix, whereas it is very time-consuming over the additive algebra, finite field and integral domain.

Definition 11**.** A *multiplicative operation* is an operation δ_j from (3), which have the same values as well as the multiplication of the algebra R in domain defined by γ_l and γ_{l+1} ranges of values.

Definition 12**.** A *multiplicative form* is called a polynomial form where all (a part of all) operations δ_j are multiplicative.

Generalize well-known equation that ties together ordinary and kroneker products.

Lemma 9**.** For fundamental matrices A, B, C and D over R, which have dimensions $n_a \times m_a$, $n_b \times m_b$, $(n_c = m_a) \times m_c$ and $(n_d = m_b) \times m_d$ correspondingly,

$$(A \otimes B) \times (C \otimes D) = (A \times C) \otimes (B \times D), \qquad (6)$$

where $\times$ is the ordinary product of matrices, $\otimes$ is the left (right) kroneker product over the multiplication of the algebra R.

From 6 we can prove the following

Theorem 10**.** If δ_j ($j = \overline{0, n-2}$) are multiplicative operations and for each fundamental matrices Γ_j there exists inverse matrix $\mu\Gamma_j$ over R, then

$$\mu\left(\bigotimes_{j=0}^{n-1} \Gamma_j\right) = \bigotimes_{j=0}^{n-1} \mu\Gamma_j . \qquad (7)$$

The equation (7) allows us to reduce the inverting of kroneker product of matrices to kroneker product of inverse matrices.

4.4. Special cases of synthesis

There exist special cases of polynomial form synthesis. It is used to increase effectiveness of the function computation (realizing) in polynomial form.

If the last operation δ_{n-1} from (3) is getting value on Boolean domain, then the multiplication of algebra R may be not doing and the computation of function reduces to summing of coefficients a_i which places at nonzero θ_i.

If operations γ_j from (3) or ω_j from (5) are getting values on Boolean domain, i.e. there are converting the multiple-valued variables to Boolean, then after this converting it is using the Boolean computation only.

If $k > k_f$, then the number of polynomial operations increases. On the other equal conditions it is brought to more compact representation of function.

And, at last, the number of required to calculate operations may be decreased if it is defined the operations γ_j so that there exists such y_j that $x_j \gamma_j y_j = x_j$. In this case this operations γ_j do not execute if $i_j = y_j$.

5. CONCLUSION

In this paper, new generalized theorems for various representations and manipulation of discrete functions in polynomial form is introduced and examples for its using are given. Expansion of number analytical constructions of polynomial form allows us taking into account non-trivial properties of discrete functions and getting effective realization of discrete functions.

6. REFERENCES

1. Boole G. The Laws of Thought. London, Macmillan, 1854.
2. Zhegalkin I. I. On the Technique of Computation the Sentences in Symbolic Logic, Matem. Sbornik, vol. 34, 1927, pp. 9-28.
3. Malygin V. D. Representation of Boolean Functions by Arithmetic Polynomials, Automation and Remote Control, vol. 43, 1982, pp. 496-504.
4. Post E. An introduction to a general theory of elementary proposition, Am. Journal Math., vol. 43, 1921, pp. 163-185.
5. Dubrova E. V., Muzio J. C. Generalized Reed-Muller Canonical Form for a Multiple-Valued Algebra, Multiple-Valued Logic, No 1, 1996, pp. 65-84.
6. Vykhovanets V. S., Malyugin V. D. Multiple logic computation, Automation and Remote Control, vol. 59, 1998, pp. 885-891.
7. Tosic Z. Analytical Representation of m-Valued Logical Function over the Ring of Inte-gers modulo m. Ph. D. thesis. Beograd: Univ. of Beograd Press, 1972.
8. Pradhan D. K. A Multi-Valued Algebra Based on Finite Fields, Proc. Int. Symp. on MVL, 1974, pp. 95-112.
9. Strazdins I. J. The Polynomial Algebra of Multivalued Logic, Algebra, Combinatorics, and Logic in Computer Science, vol. 42, 1983, pp. 777-785.
10. Vykhovanets V. S. Parallel computation in time, Automation and Remote Control, vol. 60, No 12, 1999, pp. 1024-1039.
11. Reed L. S. A class of multiple error correction codes and their decoding scheme, IRE Trans. on Inform. Theory, 1954, vol. 4, pp. 38-42.
12. Muller D. E. Application of Boolean algebra to switching circuit design and to error detection, IRE Trans. Electron. Comput.,1954, vol. EC-3, pp. 6-12.