PUBLIKACIJE ELEKTROTEHNIČKOG FAKULTETA UNIVERZITETA U BEOGRADU
PUBLICATIONS DE LA FACULTÉ D'ÉLECTROTECHNIQUE DE L'UNIVERSITÉ À BELGRADE

SERIJA: MATEMATIKA I FIZIKA — SÉRIE: MATHÉMATIQUES ET PHYSIQUE

№ 410 — № 411 (1972)

410. ANALYTICAL REPRESENTATIONS OF *m*-VALUED LOGICAL FUNCTIONS OVER THE RING OF INTEGERS MODULO *m**

Živko Tošić

1. INTRODUCTION

1.1. This thesis consists of the following parts:

1. Introduction,
2. Polynomial representations of switching functions,
3. Representanions over the field of integers mod p,
4. Representations over the ring of integers mod m,
5. Some unsolved problems and possible generalizations, and
6. References.

1.2. Representations of switching functions over the field J_2 of integers modulo 2 using also operation of complementation are dealt with in Chapter 2.

For the switching function of n variables $f(x_1, \ldots, x_n)=f(X)$ the BOOLEan difference with respect to a variable x_i is defined in the following way (see **[1, 2, 3]**)

$$D_i f(X)=f(x_i=0)\oplus f(x_i=1),$$

where $f(x_i=c)=f(x_1, \ldots, x_{i-1}, c, x_{i+1}, \ldots, x_n)$.

It is shown that the expansion theorem has the following form

$$f(X)=f(x_i=q_i)\oplus(x_i\oplus q_i)\,D_i f(X) \qquad (q_i\in\{0, 1\}),$$

or a matrix form

$$f(X)=\|\,1 \quad x_i\oplus q_i\,\|\begin{Vmatrix} q_i' & q_i \\ 1 & 1 \end{Vmatrix}\begin{Vmatrix} f(x_i=0) \\ f(x_i=1) \end{Vmatrix}, \tag{1.2.1}$$

where q_i' denotes the complement of q_i.

Analytical representations of the switching functions which represent expansion analogous to the TAYLOR series are considered [see **1, 2, 12**] and the name of polarized polynomial forms is used for them. Matrix form of pola-

*This paper is part of a doctoral dissertation submitted by Ž. Tošić to the Faculty of Electronic Engineering, University of Niš.

rized polynomial forms is proveo which is derived using (1.2.1) and is as follows

$$f(X)=(X_1\times\cdots\times X_n)(W_1\times\cdots\times W_n)F_{1\ldots n},$$

where $\times$ denotes the *left-hand* KRONECKER product of matrices (see **[17]**) and the notations are as follows

$$X_i=\|\,1\quad x_i\oplus q_i\,\|,\qquad W_i=\left\|\begin{matrix}q_i' & q_i\\ 1 & 1\end{matrix}\right\|,$$

$$F_{i\ldots jk}=\left\|\begin{matrix}f(x_i=0,\ldots,x_j=0,x_k=0)\\ f(x_i=0,\ldots,x_j=0,x_k=1)\\ \vdots\\ f(x_i=1,\ldots,x_j=1,x_k=1)\end{matrix}\right\|.$$

The way of transition from one polarized polynomial form to another is given.

The results of M. COHN **[12, 22]** on further generalizations of polarized poynomial forms, so called nonpolarized polynomial forms, are quoted and the minimization problem of polarized and nonpolarized polynomial form is mentioned.

At the end of the Chapter the way of deriving arithmetical representations of switching functions (see **[10]**) is shown.

1.3. Representations of p-valued functions over the field of integers modulo p are considered in Chapter 3.

The expansion theorem by means of the characteristic functions is given and one of its generalizations is proved. Analytical representations are considered by means of the spq polynomial form in which the characteristic functions are used.

Representations of the p-valued functions by polynomials modulo p are considered in the second part of the Chapter according to **[12, 19, 24]** and then their generalization as well, which has two matrix forms. The relation between polynomials and generalized polynomials modulo p is shown.

1.4. Chapter 4 deals with the representations of m-valued functions over J_m, the ring of integers modulo m.

For m-valued functions of one variable, representations of the following form are investigated

$$f(x)=\sum_{r=0}^{m-1}a_r h_r(x)\qquad (a_r\in J_m),\tag{1.4.1}$$

where $h_r(x)(r=0,\ldots,m-1)$ is the system of unary m-valued functions which is characterized by the matrix

$$L=\left\|\begin{matrix}h_0(0) & h_1(0) & \cdots & h_{m-1}(0)\\ h_0(1) & h_1(1) & & h_{m-1}(1)\\ \vdots & & & \\ h_0(m-1) & h_1(m-1) & & h_{m-1}(m-1)\end{matrix}\right\|.$$

It is proved that the unique representation of the form (1.4.1) exists if and only if

$$(\det L,\ m)=1, \tag{1.4.2}$$

where $(a,\ b)$ denote the greatest common divisor of the numbers a and b.

The expansion theorem of m-valued functions of n variables by means of $h_r(x_i)\,(r=0,\ldots,\ m-1)$ functions depending on x_i is derived, and the representation

$$f(X)=(H_1\times\cdots\times H_n)(W_1\times\cdots\times W_n)F_{1\ldots n} \tag{1.4.3}$$

is proved, where $H_i=\|\,h_0(x_i)\ \ldots\ h_{m-1}(x_i)\,\|$, $W_1=\cdots=W_n=L^{-1}$ and

$$F_{1\ldots n}=\left\|\begin{array}{l} f(0,\ldots,0,0)\\ f(0\ldots.,0,1)\\ \vdots\\ f(m-1,\ldots,m-1)\end{array}\right\|.$$

Representations of m-valued functions of the (1.4.3) form are called polynomial forms.

In the case when matrix L satisfies (1.4.2) condition for m.valued functions of one variable, (1.4.1) representation generalization of the following form is being proved,

$$f(x)=\sum_{r=0}^{m=1}a_r x_r(x\oplus q)\qquad (q\in J_m). \tag{1.4.4}$$

The relation between representations (1.4.1) and (1.4.4) is shown and then the generalized expansion theorem is derived by means of which the following representations of m-valued functions of n variables are proved

$$f(X)=(H_1^*\times\cdots\times H_n^*)(W_1^*\times\cdots\times W_n^*)F_{1\ldots n}, \tag{1.4.5}$$

$$f(X)=(H_1^*\times\cdots\times H_n^*)(W_1\times\cdots\times W_n)F_{1\ldots n}^*, \tag{1.4.6}$$

where $H_i^*=\|\,h_0(x_i+q_i)\ \ldots\ h_{m-1}(x_i+q_i)\,\|$.

Matrices $W_i^*\,(i=1,\ldots,n)$ in (1.4.5) and (1.4.6) are derived by a cyclic shift of W matrix columns for q_i places to the left and the vector $F_{1\ldots n}^*$ is derived by a cyclic shift of the coordinates of $F_{1\ldots n}$ for q places downwards, where $q=q_1 m^{n-1}+q_2 m^{n-2}+\cdots+q_n$ (real arithmetic).

Representations (1.4.5) and (1.4.6) are called generalized polynomial forms.

The second part of Chapter 4 deals with the m-valued functions of one variable which may be represented by means of polynomials modulo m. The analogy is then pointed out which exists between the representations of m-valued functions by means of polynomial forms and polynomials modulo p with FOURIER transformations as well as the analogy with expansions by orthogonal functions. At the end, it is proved that the polynomial forms considered may also be derived in whatever commutative ring with a unity. It is a con-

dition there that the determinant of matrix L be an element of the ring which is invertible with respect to the multiplication operation in the ring.

1.5. In Chapter 5 some unsolved problems are pointed out as well as possible further uses of polynomial forms.

1.6. References quoted in Chapter 6 cover the literature used during the work on this thesis.

* * *

Particular thanks are due to Professor dr. D. A. POSPELOV who has introdused the author of this thesis into scientific work and under whose guidance at the Department for Computing Technique of the Moscow Power Institute most of the results have been obtained.

The author is grateful to Professor dr D. S. MITRINOVIĆ for his idea of writing his thesis, and for his great support and permanent interest during the work on the text.

Many thanks are also due to Professor dr. R. Ž. ĐORĐEVIĆ for his cordial and unselfish help in writing the thesis.

2. POLYNOMIAL REPRESENTATIONS OF SWITCHING FUNCTIONS

2.1. Boolean difference

Let us denote the field of integers modulo 2 by J_2. Functions defined over J_2 taking values from J_2 will be called switching functions.

Addition over J_2 will be denoted by $\oplus$ and multiplication by $\cdot$ or by juxtaposition of factors.

The switching function *or* (disjunction) will be denoted $\vee$, while $x \vee y = x \oplus y \oplus xy$. The unary switching function of complementation will be denoted by either $1 \oplus x$ or x'.

Addition and subtraction over the field of real numbers will be as usually denoted by $+$ and $-$, respectively.

Let a switching function $f(X)=f(x_1, \ldots, x_n)$ be given. The BOOLEAN difference of $f(X)$ with respect to the variable $x_i (i \in \{1, \ldots, n\})$ is defined by the expression

$$D_i f(X) = f(x_i = 0) \oplus f(x_i = 1) \tag{2.1.1}$$

where $f(x_i = c) = f(x_1, \ldots, x_{i-1}, c, x_{i+1}, \ldots, x_n)$.

The BOOLEAN difference has ben introduced by S. B. AKERS [1] who has considered in detail the characteristics and applications of this operator. A few years later, independently of S. B. AKERS, the same operator was introduced by R. D. BOCHMANN [2].

S. B. AKERS proved that, equivalently to (2.1.1), the BOOLEAN difference may also be defined as follows

$$D_i f(X) = f(x_1, \ldots, x_i, \ldots, x_n) \oplus f(x_1, \ldots, x_i', \ldots, x_n). \tag{2.1.2}$$

The BOOLEan difference defined that way had been used before S. B. AKERS by I. S. REED [3] in reference with the error correcting codes.

The BOOLEan difference of higher degree is inductively defined as follows

$$D_{i\ldots jk} f(X) = D_k [D_{i\ldots j} f(X)]. \tag{2.1.3}$$

Let us mention that, in reference with some technical applications, another definition of BOOLEan difference of higher degree is considered [4, 5, 6],

$$D^*_{1\ldots k} f(X) = f(x_1, \ldots, x_k, x_{k+1}, \ldots, x_n) \oplus f(x'_1, \ldots, x'_k, x_{k+1}, \ldots, x_n).$$

This operator will not be considered further.

Some characteristics of the BOOLEan difference will be mentioned without proofs. Proofs can be found in references [1, 2, 4, 5].

$$D_i C = 0 \ (C \text{ constant}), \ D_i f'(X) = D_i f(X),$$

$$D_{ij} f(X) = D_{ji} f(X), \ D_{ii} f(X) = 0,$$

$$D_i [f(X) \oplus g(X)] = D_i f(X) \oplus D_i g(X)$$

$$D_i [f(X) g(X)] = f(X) D_i g(X) \oplus g(X) D_i f(X) \oplus D_i f(X) D_i g(X),$$

$$D_i [f(X) \vee g(X)] = f'(X) D_i g(X) \oplus g'(X) D_i f(X) \oplus D_i f(X) D_i g(X),$$

$$D_i f[g(X)] = D_g f(g) D_i g(X),$$

where $D_g f(g)$ is the BOOLEan difference of the function $f(g)$ with respect to the variable g.

Some works in which operators equivalent to the BOOLEan difference are ntroduced and used can also be found in literature.

In reference with the synthesis of the majority switching functions by means of be cascade method, the BOOLEan difference is introduced in [8], which is equivalent to the expression (2.1.1) and is used for determination of the sequence of the variables by means of which the expansion is being performed.

An operator equivalent to the BOOLEan difference defined by expression (2.1.2) is introduced into the works [4, 5, 9] and is used for diagnosis of the switching circuits.

If a switching function is interpolated by a polynomial whose variables take their values from the set $\{0, 1\}$, that polynomial will be called the arithmetical representation of the given switching function. In this case the BOOLEan difference can be introduced in the following way as well

$$D_i f(X) = f(x_i = 1) - f(x_i = 0). \tag{2.1.5}$$

The expression is derived from the well known general definition of the finite difference.

For the sake of analysis of the switching functions behaviour when the variable x_i changes, R. D. BOCHMANN [2, 6] introduced into consideration the so salled *directed* BOOLEan differences.

Let a switching function of n variables $f(X) = f(x_1, \ldots, x_i, \ldots, x_n)$ be given.

The switching function which equals 1 if and only if with the change of the variable x_i from 0 to 1, $f(X)$ also changes from 0 to 1, is called the BOOLEAN difference in the *forward* direction with respect to the variable x_i, and is defined by the expression

(2.1.6) $$D_i^d f(X) = f'(x_i = 0) f(x_i = 1).$$

The switching function which equals 1 if and only if with the change of the variable x_i from 0 to 1, $f(X)$ changes from 1 to 0, is called the BOOLEAN difference in the *opposite* direction with respect to the variable x_i, and is defined by the expression

(2.1.7) $$D_i^s f(X) = f(x_i = 0) f'(x_i = 1).$$

The following relations between the BOOLEAN difference and the *directed* BOOLEAN differences hold (see [2])

$$D_i f(X) = D_i^d f(X) \oplus D_i^s f(X) = D_i^d f(X) \vee D_i^s f(X),$$
$$D_i^d f(X) = f(x_i = 1) D_i f(X), \quad D_i^s f(X) = f(x_i = 0) D_i f(X).$$

2.2. Expansion theorem

Any swiching function can be represented in the following way (see [1])

(2.2.1) $$f(X) = x_i' f(x_i = 0) \oplus x_i f(x_i = 1).$$

The representation (2.2.1) is called the expansion theorem of the function $f(X)$ with respect to the variable x_i. It is proved by replacing for x_i values of 0 and 1.

The expansion theorem is analogous to the corresponding theorem of C. E. SHANNON [11].

I. S. REED in [3] proved that the set of all switching functions of n variables form 2^n-dimensional vector space over the field J_2. Such a consideration of the set of the switching functions will further be used very often for their representations. Matrices and vectors over J_2 will be denoted by Latin capitals. All the operations with the matrices over J_2 are analogous to the corresponding operations over the field of real numbers.

The expression for the expansion theorem (2.2.1) in the matrix form is as follows

(2.2.2) $$f(X) = \| x_i' \quad x_i \| \begin{Vmatrix} 1 & 0 \\ 0 & 1 \end{Vmatrix} \begin{Vmatrix} f(x_i = 0) \\ f(x_i = 1) \end{Vmatrix}.$$

If replacing of $x_i' = 1 \oplus x_i$ and $x_i = 1 \oplus x_i'$, reprectively, is performed in (2.2.1), two forms of the expansion theorem will be derived (see [12, 13])

(2.2.3) $$f(X) = f(x_i = q_i) \oplus (x_i \oplus q_i) D_i f(X) \quad (q_i = 0, 1).$$

The corresponding matrix expression for (2.2.3) will be (see [15])

(2.2.4) $$f(X) = \| 1 \quad x_i \oplus q_i \| \begin{Vmatrix} q' & q_i \\ 1 & 1 \end{Vmatrix} \begin{Vmatrix} f(x_i = 0) \\ f(x_i = 1) \end{Vmatrix}.$$

In transition from (2.2.3) to (2.2.4) the equation $f(x_i=q_i)=q_i' f(x_i=0\oplus \oplus q_i f(x_i=1)$ is used which is derived from (2.2.1).

Using all these tree forms of the expansion theorem, synthesis of the switching functions by means of so called cascade method of G. N. POVAROV **[14]** may be carried out with the elements which realize the sum and product functions modulo 2 **[13]**.

Let the function $f[g(X)]$ be a composition function. Using (2.2.3) the expansion of $f(g)$ by g and then of $g(X)$ by x is done by

$$f[g(X)]=f(g=q)\oplus[g(x_i=q_i)\oplus(x_i\oplus q_i)D_i g(X)\oplus q]D_g f(g) \tag{2.2.5}$$
$$=f(g=0)\oplus g(x_i=q_i)D_g f(g)\oplus(x_i\oplus q_i)D_i f[g(X)].$$

The expression (2.2.5) represents the expansion theorem of the composition function.

2.3. Basic polynomial representations

Representations of the switching functions over the field J_2, using, besides the field operations and constants 0, 1, the unary operation of complementation as well, will be called polynomial forms. A particular case of the polynomial forms are representations by the polynomials modulo 2.

Let $0\leqq j\leqq 2^n-1$ and

$$j=j_n 2^{n-1}+j_{n-1}2^{n-2}+\cdots+j_2 2+j_1 \tag{2.3.1}$$

be the representation of the number j over the dyadic number system.

Let us put the following functions into the one-to-one correspodence to j

$$p_j(X)=\prod_{i=1}^{n}(x_i\oplus j_i'), \tag{2.3.2}$$

$$r_j(X)=\prod_{j_i=1}x_i,\quad r_j^*(X)=\prod_{j\,i=1}(x_i\oplus q_i)\quad (q_i\in J_2), \tag{2.3.3}$$

$$r_0(X)=r_0^*(X)=1,$$

$$c(j)=c(j_1)\ldots c(j_n),\quad c(j_i)=\begin{cases} i, & j_i=1,\\ \varnothing, & j_i=0,\end{cases} \tag{2.3.4}$$

where $\varnothing$ denotes the empty set.

Using the definitions introduced above, the expansion theorem (2.2.3) can be represented in the following form

$$f(X)=D_\varnothing f(x_i=q_i)\oplus(x_i\oplus q_i)D_i f(x_i=q_i) \tag{2.3.5}$$
$$=r_0^*(X)D_{c(0)}f(x_i=q_i)\oplus r_{2^i}^*(X)D_{c(2^i)}f(x_i=q_i),$$

where $D_\varnothing f(X)=f(X)$.

As x_i is a dummy variable (see **[1]**) for the BOOLEan difference $D_i f(X)$ the equation $D_i f(X)=D_i f(x_i=q_i)$ has been used.

Every switching function may be represented in the following form (see [1, 12])

$$f(X) = \circ\sum_{j=0}^{2^n-1} p_j(X) f(j), \tag{2.3.6}$$

where $f(j)=f(j_1, \ldots, j_n)$ and $\circ\Sigma$ denotes addition modulo 2.

The representation (2.3.6) will be called the full polynomial normal form. It is analogous to the full disjunctive normal form.

By mathematical induction it is proved that every switching function has the following representation (see [1, 2])

$$f(X) = \circ\sum_{j=0}^{2^n-1} r_j^*(X)\, D_{c(j)} f(q_1, \ldots, q_n) \quad (q_i \in J_2). \tag{2.3.7}$$

This representation is derived by the application of the expansion theorem (2.3.5).

The representation of the form (2.3.7) will be called the polarized polynomial form. As the values of $q_i (i=1, \ldots, n)$ can be taken optionally there are 2^n polarized polynomial forms for every switching function of n variables. Their characteristic is that the same variable within them can only be either complemented or uncomplemented.

The polynomial forms (2.3.7) are analogous to the expansion of analytical functions into the TAYLOR series and that is why S. B. AKERS has used in [1] the term „series expansion" for them.

As a particular case of the representations (2.3.7) polynomials modulo 2 are obtained if $q_i = 0\,(i=1, \ldots, n)$ is put,

$$f(X) = \circ\sum_{j=0}^{2^n-1} r_j(X)\, D_{c(j)} f(0, \ldots, 0). \tag{2.3.8}$$

The possibility of using polynomials modulo 2 for representation of switching functions was proved in 1927 by I. I. ŽEGALKIN [16]. The representation (2.3.8) has been proved by I. S. REED [3] and D. E. MULLER [28].

The above considered representations may be very suitably expressed by matrices [12]. The expression (2.2.4) can be written in the following may

$$f(X) = X_i W_i F_i. \tag{2.3.9}$$

Theorem 2.1. *Every switching function of n variables is representable in the form*

$$f(X) = (X_1 \times \cdots \times X_n)(W_1 \times \cdots \times W_n) F_{1 \ldots n}. \tag{2.3.10}$$

PROOF. The proof is by induction on n. For $n=1$ (2.3.10) holds good by (2.3.9). Let us assume that the Theorem 2.1 holds for $n-1$ and let us prove that it holds for n too.

By the expansion of the function $f(X)$ with respect to the variable x_n on the basis of (2.3.9) we have

$$f(X) = X_n W_n F_n. \tag{2.3.11}$$

For the induction step the switching functions $f(x_n=0)$ and $f(x=1)$ in F_n can be written in the following way

$$f(x_n=0)=YWF^0, \qquad f(x_n=1)=YWF^1, \tag{2.3.12}$$

where $Y=X_1\times\cdots\times X_{n-1}$, $W=W_1\times\cdots\times W_{n-1}$, and F^0 and F^1 are vectors, derived from the vector $F_{1\ldots n-1}$ by replacing in all its elements the variable x_n by values 0 and 1, respectively.

Replacing (2.3.12) into (2.3.11) we have

$$\begin{aligned} f(X)&=\| 1 \quad x_n\oplus q_n\| \begin{Vmatrix} q_n' & q_n \\ 1 & 1 \end{Vmatrix} \begin{Vmatrix} YWF^0 \\ YWF^1 \end{Vmatrix} \\ &=\| Y \quad Y\cdot(x_n\oplus q_n)\| \begin{Vmatrix} q_n' W & q_n W \\ W & W \end{Vmatrix} \begin{Vmatrix} F^0 \\ F^1 \end{Vmatrix} \\ &=(X_1\times\cdots\times X_n)(W_1\times\cdots\times W_n)F_{1\ldots n}, \end{aligned}$$

hence Theorem 2.1 is proved.

The representation (2.3.10) is a matrix form for the polarized polynomial forms and is identical to (2.3.7).

The matrix form for the polynomials modulo 2 is derived as a particular case of (2.3.10) if $q_i=0$ is put for all $i=1,\ldots,n$. Then $W_1=\cdots=W_n$. Such mode of representation has ben considered by many authors **[12, 18, 19, 20]** and it should be particularly pointed out that the matrix $W_1\times\cdots\times W_n$ can be derived from the matrix of binomial coefficients modulo 2 (see **[19, 20]**).

2.4. Generalized polynomial forms

As it is said in the preceding text, the characteristic of the polarized polynomial forms is that the same variable in all their elements may be either complemented or uncomplemented. However, M. COHN has proved in **[12, 22]** that there are more general polynomial forms by means of which switching functions can be represented.

If the set of all switching functions of n variables is considered as a 2^n-dimensional vector space over J_2 then bases of the vector space consist of the following vector systems in the representations (2.3.6) and (2.3.7), respectively

$$p_j(X) \qquad (j=0,\ldots,2^n-1), \tag{2.4.1}$$

$$r_j^*(X) \qquad (j=0,\ldots,2^n-1). \tag{2.4.2}$$

The basis (2.4.1) is orthogonal. There are 2^n bases of the form (2.4.2) in all and they consist of vectors

$$1, x_1^*, x_2^*, x_1^*x_2^*, \ldots, x_1^*x_2^*\cdots x_n^*, \tag{2.4.3}$$

were for all i $(i=1,\ldots,n)$ $x_i^*=x_i$ or $x_i^*=x_i'$.

For deriving polynomials modulo 2, the basis consists of the vectors

$$1, x_1, x_2, x_1x_2, \ldots, x_1x_2\cdots x_n. \tag{2.4.4}$$

All basis vectors of the system (2.4.3) may be derived from the vector system (2.2.4) if a certain number of variables are complemented in all vectors.

The matrix composed of the coordinates of the vector system (2.4.3) may be represented as the KRONECKER product of matrices of order two which can be seen from (2.3.10).

M. COHN has shown that if variables are complemented optionally in each of the vectors of the system (2.4.4), a new basis will be derived. Switching functions representations by means of that new basis represent generalisaiion of the polarized polynomial forms and they will be called nonpolarized polynomial forms.

The matrix composed of the coordinates of the basis vectors of the nonpolarized polynomial forms can no more be represented as the KRONECKER product of the matrices of the order two (see **[12]**).

Total number of the nonpolarized polynomial forms for the switching functions of n variables equals 2^K **[22]**, where $K=2^{n2^n-1}$. However, there are only 2^n bases among them which are polarized polynomial forms.

The problem of obtaining the minimum number of realizations is true for the polynomial forms as well. Althoungh there are a lot of works dealing with the minimization of the polynomial forms so far there is no a method which could find wide application in practice. Besides the generalization of the well known classical minimization methods, specific ones are being developed for minimization of the polynomial forms dealing with the characteristics of the considered set of functions (see works **[7, 12, 13, 23—31]** on the minimization of polynomial forms).

2.5. Arithmetical representations

For the sake of the switching functions representation any of the interpolation methods (see **[32]**) may also be used, the values of the variables being taken from the set $\{0, 1\}$.

A more general approach to the switching functions representation by means of the arithmetical operations will be considered here **[10]**. These representations will be called arithmetical representations in order to distinguish them from the representations over J_2.

It should be mentioned first that the unary switching function complement has the following arithmetical representation: $x'=1-x$.

Let us consider under which conditions each switching function of one variable has representation of the form

$$f(x)=a_0 h_0(x)+a_1 h_1(x), \tag{2.5.1}$$

where $x\in\{0, 1\}$, a_0 and a_1 are integer coefficients while $h_0(x)$ and $h_1(x)$ are the switching functions of one variable.

Replacing the values $x=0$ and $x=1$ into (2.5.1) the following system of equations is derived

$$f(k)=a_0 h_0(k)+a_1 h_1(k) \qquad (k=0,\ 1). \tag{2.5.2}$$

In order that an integer solution should exist for a_0 and a_1, it is necessary and sufficient that the determinant of the system (2.5.2) has the value $+1$ or -1. Since there are only four switching functions of one variable, investigating all the possible cases it is easily determined that the system (2.5.2) is satisfied by the following three sets (solutions obtained by a mere replacing of indexes are considered as one) and the same:

1) $h_0(x)=x'$, $h_1(x)=x$;

2) $h_0(x)=1$, $h_1(x)=x$;

3) $h_0(x)=x'$, $h_1(x)=1$.

For these three systems of functions each switching function of n variables will have the following three expansions

$$f(X)=x_i' f(x_i=0)+x_i f(x_i=1)$$
$$=f(x_i=0)+x_i D_i f(X)$$
$$=f(x_i=1)-x_i' D_i f(X), \tag{2.5.3}$$

where $D_i f(X)$ is defined by (2.2.5).

Let us denote

$$H_i^1=\|x_i' \;\; x_i\|, \quad H_i^2=\|1 \;\; x_i\|, \quad H_i^3=\|x_i' \;\; 1\|,$$

$$R_i^1=\begin{Vmatrix}1 & 0\\ 0 & 1\end{Vmatrix}, \quad R_i^2=\begin{Vmatrix}1 & 0\\ -1 & 1\end{Vmatrix}, \quad R_i^3=\begin{Vmatrix}1 & -1\\ 0 & 1\end{Vmatrix},$$

The matrix form of the expansion (2.5.3) will be as follows

$$f(X)=H_i^u R_i^u F_i \qquad (u=1,\ 2,\ 3). \tag{2.5·2}$$

In the same way as with the Theorem 2.1, it may be proved that each switching function of n variables has the following representation

$$f(X)=(H_1^{u_1}\times\cdots\times H_n^{u_n})(R_1^{u_1}\times\cdots\times R_n^{u_n})F_{1\ldots n} \quad (u_i\in\{1,\ 2,\ 3\}). \tag{2.5.2}$$

Arithmetical representations are used in $0-1$ integer linear programming [33, 34]. In addition, transition from arithmetical representations to polynomial forms is being done by replacing the coefficients $a_j\,(j=0,\ldots,\ 2^n-1)$ by their values modulo 2.

3. REPRESENTATIONS OVER THE FIELD OF INTEGERS mod p

3.1. Notations and introductory notes

Let J_p denote the field of integers mod p, p a prime. Functions defined over J_p with the values from J_p will be called p-valued functions. Besides this term, terms p-valued switching functions or p-valued logical functions may be found in literature.

Addition over the field J_p will be denoted by $+$ and multiplication by $\cdot$ or by juxtaposition of factors. The inverse element to the element $t \in J_p$ with respect to the operation $+$ will be denoted $-t$.

The term polynomials modulo p will be used in the usual sense. These polynomials will be considered below and used for representation of p-valued functions. In comparison to the representations by means of other complete sets of p-valued functions, polynomials modulo p have some advantages which are as follows:

— similarity to the ordinary algebra which facilitates work on synthesis and simplification of the circuits (see [35, 36]),

— in comparison to other complete sets, the set considered provides more economical realizations (see [35]).

Except for the representation of p-valued functions, polynomials modulo p are used in the theory of error correcting codes (see [37, 40]), theory of linear sequential switching circuits (see [39, 40]), etc. By means of polynomials over the field $GF(2^n)$ a number of digital proccesses such as the identification of twotone patterns, the decoding of binary block codes, the addressing of "files" in the memory of a computer, etc. may be described (see [41, 42]).

3.2. spg polynomial forms

The functions of the forms to follow will be called the characteristic p-valued functions of one variable

$$g_r(x) = \begin{cases} 1, & x = r \\ 0, & x \neq r \end{cases} \qquad (r = 0, \ldots, p-1). \tag{3.2.1}$$

The following theorem will be proved.

Theorem 3.1. *All characteristic functions of one variable can be expressed by means of the given characteristic function $g_t(x)$ $(t \in J_p)$ in the following way*

$$g_r(x) = g_t(x + t - r) \qquad (r = 0, \ldots, p-1). \tag{3.2.2}$$

Proof. For $x = r$ we have $g_r(r) = g_t(r + t - r) = g_t(t) = 1$. For $x = r_1 \neq r$ we have $r_1 + t - r \neq t$, and then $g_r(r) = g_t(r_1 + t - r) = 0$. Thus Theorem 3.1 has been proved.

The characteristic functions (3.2.1) have the following polynomial representation (see [36])

$$g_0(x) = (p-1)x^{p-1} + 1, \quad g_r(x) = (p-1)\sum_{k=0}^{p-2} r^k x^{p-1-k} \quad (r = 1, \ldots, p-1) \tag{3.2.3}$$

or in a general form (see [19])

$$g_r(x) = 1 + (p-1)\sum_{k=0}^{p-1} r^k x^{p-1-k} \quad (r = 0, \ldots, p-1). \tag{3.2.4}$$

Theorem 4.2. (M. J. GAZALE [19], D. A. POSPELOV [7]). *Any p-valued function of n variables has a representation of the form*

$$f(X) = \sum_{r=0}^{p-1} f(x_i = r)\, g_r(x_i). \tag{3.2.5}$$

The expression (3.2.5) will be called the expansion theorem of the p-valued functions for the characteristic functions of the variable x_i.

As a generalization of theorem 3.2, the following theorem will be proved.

Theorem 3.3. *Every p-valued function of n variables has a representation of the form*

$$f(X)=\sum_{r=0}^{p-1} f(x_i=r-q)\,g_r(x_i+q) \qquad (q\in J_p). \tag{3.2.6}$$

Proof. For every value of $x_i=t\,(t\in J_p)$ on the right-hand side of the equation (3.2.6) only one characteristic function will get the value 1. That will be for $r=t+q$ and then (3.2.6) yields $f(x_i=t)=f(x_i=t+q-q)\,g_r(r)=f(x_i=t)$, hence Theorem 3.3 is proved.

Representation (3.2.6) will be called the generalized expansion theorem for the characteristic functions of the variable x_i.

Let $0\leqq r\leqq p^n-1$ and let

$$r=r_1p^{n-1}+r_2p^{n-2}+\cdots+r_n \tag{3.2.7}$$

be the representation of the number r over the p-adic number system (real arithmetic).

The characteristic functions of the p-valued functions of n variables are defined in the following may

$$g_r(x_1,\ldots,x_n)=\begin{cases}1, & (x_1,\ldots,x_n)=(r_1,\ldots,r_n),\\ 0, & (x_1,\ldots,x_n)\neq(r_1,\ldots,r_n),\end{cases} \tag{3.2.8}$$

where the relation

$$g_r(x_1,\ldots,x_n)=g_{r_1}(x_1)\cdots g_{r_n}(x_n) \tag{3.2.9}$$

holds (see [7, 19, 36]).

Theorem 3.5. (*see* [19]). *Every p-valued function of n variacles has the representation of the form*

$$f(x_1,\ldots,x_n)=\sum_{r=0}^{p-1} f(r_1,\ldots,r_n)\,g_{r_1}(x_1)\cdots g_{r_n}(x_n). \tag{3.2.10}$$

Representation (3.2.10) will be called the spg polynomial form. A generalization of the preceding theorem is provided by the following theorem.

Theorem 3.5. *Every switching p-valued function of n variables has a representation of the form*

$$f(x_1,\ldots,x_n)=\sum_{r=0}^{p^n-1} f(r_1-q_1,\ldots,r_n-q_n)\,g_{r_1}(x_1+q_1)\cdots g_{r_n}(x_n+q_n) \tag{3.2.11}$$

$$(q_i\in J_p).$$

Proof. The proof is by mathematical induction on n. For $n=1$ the theorem holds by (3.2.6). Assume that the theorem holds for $n-1$, and let us prove that the theorem will also hold for n.

According to the inductive assumption it is true that

$$f(X)=\sum_{r=0}^{p^{n-1}-1} f(r_1-q_1,\ldots,r_{n-1}-q_{n-1},x_n)\,g_{r_1}(x_1+q_1)\cdot\cdot\cdot g_{r_n}(x_{n-1}+q_{n-1}).$$

By the application of (3.2.6) we have now

$$\begin{aligned} f(X)&=\sum_{r=0}^{p^{n-1}-1} g_{r_1}(x_1+q_1)\cdot\cdot\cdot g_{r_n}(x_{n-1}+q_{n-1})\\ &\quad\times\sum_{r_n=0}^{p-1} f(r_1-q_1,\ldots,r_n-q_n)\cdot g_{r_n}(x_n+q_n)\\ &=\sum_{r=0}^{p^n-1} f(r_1-q_1,\ldots,r_n-q_n)\,g_{r_1}(x_1+q_1)\cdot\cdot\cdot g_{r_n}(x_n+q_n), \end{aligned}$$

which completes the proof.

The representation (3.2.11) will be called spg generalized polynomial form.

Put $G_i=\|\,g_0(x_i)\ \ldots\ g_{p-1}(x_i)\,\|$, $G_i^*=\|\,g_0(x_i+q_i)\ \ldots\ g_{p-1}(x_i+q_i)\,\|$,

$$F_{i\ldots jk}=\begin{Vmatrix} f(x_i=0,\ldots,x_j=0,x_k=0)\\ f(x_i=0,\ldots,x_j=0,x_k=1)\\ \vdots\\ f(x_i=p-1,\ldots,x_k=p-1)\end{Vmatrix}.$$

Let $q=q_1p^{n-1}+q_2p^{n-2}+\cdots+q_n$ (real arithmetic) be the number which is put into the one-to-one correspondence to the vector $Q=(q_1,\ldots,q_n)$. If the identity matrix of order p^n is denoted by I, then the expansion theorem (3.2.5) will have the following matrix form

$$f(X)=G_iIF_i. \tag{3.2.12}$$

Let I^* be the matrix which is derived by the cyclic shift of the rows of the matrix I for q places to left and $F^*_{i\ldots jk}$ the vector which is derived by the cyclic shift of the $F_{i\ldots jk}$ vector coordinates for q places downwards. The generalized expansion theorem (3.2.6) then has the matrix form

$$f(X)=G_i^*IF_i^*=G_i^*I^*F_i. \tag{3.2.13}$$

The corresponding matrix expressions can also be written for the spg polynomial form (3.2.10) and the generalized polynomial form (3.2.11).

3.3. Polynomials mod p

It is known (see **[53, 54]**) that every one-variable p-valued function may be represented by the polynomial

$$f(x)=\sum_{r=0}^{p-1} a_rx^r, \tag{3.3.1}$$

where (see **[19]**)

$$a_r = \sum_{k=0}^{p-1} f(k)\,(1 - r^{p-1} - k^{p-1-r}) \quad (r = 0 \ \dots \ p-1). \tag{3.3.2}$$

Theorem 3.6. *Every p-valued function of n variables has a representation of the form*

$$f(X) = \sum_{r=0}^{p-1} x_i \sum_{k=0}^{p-1} f(x_i = k)\,(1 - r^{p-1} - k^{p-1-r}). \tag{3.3.3}$$

Proof. Let us investigate a representation of the from

$$f(X) = \sum_{r=0}^{p-1} x_i^r a_r(x_1, \dots, x_{i-1}, x_{i+1}, \dots, x_n). \tag{3.3.4}$$

Replacing for the variable x_i the values $0, \dots, p-1$ into (3.3.4) the following system of congruences will be obtained

$$f(k) = \sum_{r=0}^{p-1} k^r a_r(x_1, \dots \ x_{i-1}, x_{i+1}, \dots, x_n) \quad (k = 0, \dots, p-1). \tag{3.3.5}$$

The matrix of this system has the from

$$V = \left\| \begin{matrix} 1 & 0 & 0 & \cdots & 0 \\ 1 & 1 & 1 & & 1 \\ 1 & 2 & 2^2 & & 2^{p-1} \\ \vdots & & & & \\ 1 & p-1 & (p-1)^2 & & (p-1)^{p-1} \end{matrix} \right\|.$$

The determinant of the matrix V is known as VANDERMONDE's determinant whose value is $\det V = 1!\,2! \cdots (p-1)!$.

If we denote $H_i = \| 1 \ x_i \ \dots \ x_i^{p-1} \|$, $F_i^T = \| f(x_i = 0) \ \dots \ f(x_i = p-1) \|$,

$$A_i^T = \| a_0(x_1, \dots, x_{i-1}, x_{i+1}, \dots, x_n) \ \dots \ a_{p-1}(x_1, \dots, x_{i-1}, x_{i+1}, \dots, x_n) \|$$

then the system (3.3.9) will have the matrix from $VA_i = F_i$ from which it follows

$$A_i = V^{-1} F_i. \tag{3.3.6}$$

The matrix V^{-1} has the form (see **[19, 43, 44, 46]**)

$$V^{-1} = \left\| \begin{matrix} 1 & 0 & 0 & \cdots & 0 \\ 0 & -1^{-1} & -2^{-1} & & -(p-1)^{-1} \\ 0 & -1^{-2} & -2^{-2} & & -(p-1)^{-2} \\ \vdots & & & & \\ 0 & -1^{-(p-2)} & -2^{-(p-2)} & & -(p-1)^{-(p-2)} \\ p-1 & -1^{-(p-1)} & -2^{-(p-1)} & & -(p-1)^{-(p-1)} \end{matrix} \right\|.$$

The elements $w_{rk}(r, k = 0, \dots, p-1)$ of the matrix V^{-1} may be expressed in the following way (see **[19]**)

$$w_{rk} = 1 - r^{p-1} - k^{p-1-r} \tag{3.3.7}$$

The matrix form for (3.3.4) is $f(X)=H_iA_i$ from which replacing A_i from (3.3.6) will be derived (3.3.3), that is, the matrix from

$$f(X)=H_iV^{-1}F_i. \tag{3.3.8}$$

The representation (3.3.8) (or (3.3.3)) will be called the expansion theorem of p-valued functions of n variables about the variable x_i.

Starting from (3.3.8) we will prove by mathematical induction the existence of the following representation (see **[19, 22]**).

Theorem 3.7. *Every p-valued function of n variables has a representatinn of the form*

$$f(X)=(H_1\times\cdots\times H_n)\,(V_1^{-1}\times\cdots\times V_n^{-1})\,F_{1\dots n}, \tag{3.3.9}$$

where $V_1^{-1}=\cdots=V_n^{-1}=V^{-1}$. *The left-hand Kronecker product of matrices is denoted by* $\times$.

Proof. The proof is by induction on n. For $n=1$ the theorem holds by (3.3.8). Assume that the theorem holds for $n-1$, and let us prove that it will then also hold for n.

By the expansion of the function $f(X)$ about the variable x_n from (3.3.8) we will have

$$f(X)=H_nV^{-1}F_n. \tag{3.3.10}$$

All the coordinates of the vector F_n are functions of $n-1$ variable. According to the induction assumption every of those coordinates has the representation of the form (3.3.9)

$$f(x_i=k)=YWF_{1\dots n-1}(x_n=k)\quad(k=0,\dots,p-1), \tag{3.3.11}$$

where $Y=H_1\times\cdots\times H_{n-1}$, $W=V_1^{-1}\times\cdots\times V_{n-1}^{-1}=V^{-1}\times\cdots\times V^{-1}$ and where it has been denoted by $F_{1\dots n-1}(x_n=k)$ that the variable x_n in all cooroinates of the vector $F_{1\dots n-1}$ should be replaced by k.

By the expansion of (3.3.10) and replacement of $f(x_n=k)$ according to (3.3.11), it follows:

$$f(X)=\sum_{r=0}^{p-1}\sum_{k=0}^{p-1}x_n^r w_{rk}f(x_n=k)=\sum_{r=0}^{p-1}\sum_{k=0}^{p-1}x_n^r w_{rk}\,[YWF_{1\dots n-1}(x_n=k)]$$

$$=\sum_{r=0}^{p-1}\sum_{k=0}^{p-1}(x_n^rY)\,(w_{rk}W)\,F_{1\dots n-1}(x_n=k)=(Y\times H_i)\,(W\times V^{-1})\,F_{1\dots n}$$

and (3.3.9) follows immediately.

3.4. Generalized polynomials mod p

A generalization of the following form may be considered for the polynomials (3.3.1)

$$f(x)=\sum_{r=0}^{p-1}a_r(x+q)^r\quad(q\in J_p). \tag{3.4.1}$$

First, the following lemma will be proved.

Let L be a square nonsingular matrix of the order p over J_p and let L^{-1} be its inverse matrix. The matrix which is obtained from the matrix L by the cyclic shift of the rows for q places upwards ($q<p$) will be denoted by L_q.

Lemma. *The inverse matrix L_q^{-1} of the matrix L_q is derived from the inverse matrix L^{-1} by the cyclic shift of the columns for q places to the left.*

Proof. Let P_q be the following permutation matrix of the order p

$$P_q = \begin{Vmatrix} & & & & \overset{q}{\overbrace{}} & & \\ 0 & \cdots & 0 & 1 & 0 & \cdots & 0 \\ 0 & & 0 & 0 & 1 & & 0 \\ \vdots & & & & & & \\ 0 & & 1 & 0 & 0 & & 0 \end{Vmatrix}.$$

It is easy to establish that the inverse matrix of P_q will be the following permutation matrix

$$P_q^{-1} = \begin{Vmatrix} & & & & \overset{p-q}{\overbrace{}} & & \\ 0 & \cdots & 0 & 1 & 0 & \cdots & 0 \\ 0 & & 0 & 0 & 1 & & 0 \\ \vdots & & & & & & \\ 0 & & 1 & 0 & 0 & & 0 \end{Vmatrix}.$$

Cyclic shift of the rows of the matrix M of order p for q places upwards is performed by multiplying from the left-hand side by the permutation matrix P_q. The cyclic shift of the columns of the matrix M for q places to the left is performed by multiplying from the righthand side by the matrix P_q^{-1} (see [46]).

The equation $(L^{-1}P_q^{-1})(P_qL)=I$ follows from the equation $L^{-1}L=I$, and the proof of the lemma follows immediately.

Replacing the values for x in (3.3.1), the following system of congruences is oatained.

$$\sum_{r=0}^{p-1} a_r(k+q)^r = f(k) \qquad (k=0\ \ldots, p-1), \tag{3.4.2}$$

or in the matrix form $V^*A=F$, where

$$V^* = \begin{Vmatrix} 1 & q & q^2 & \cdots & q^{p-1} \\ 1 & (1+q) & (1+q)^2 & & (1+q)^{p-1} \\ \vdots & & & & \\ 1 & (q-1) & (q-1)^2 & & (q-1)^{p-1} \end{Vmatrix}.$$

It is seen that the matrix V^* is derived from the matrix V of the system (3.3.5) by the cyslic shift of the rows for q places upwards.

By the proved lemma the inverse matrix of the matrix V^* exists and is derived from the inverse matrix V^{-1} by the cyclic shift of the columns for q places to the left. From (3.3.7) then follows that

$$w_{rk} = 1 - r^{p-1} - (k+q)^{p-1-r}. \tag{3.4.3}$$

If we put $(V^*)^{-1}=W^*$ then the matrix form of the representation (3.4.1) will be as follows

$$f(x)=H^*W^*F, \tag{3.4.4}$$

where $H^*=\| 1 \quad x+q \quad \dots \quad (x+q)^{p-1} \|$.

The system (3.4.2) can be represented in other form

$$\sum_{r=0}^{p-1} a_r k^r = f(k-q) \qquad (k=0,\dots,p-1),$$

and its matrix form will be $VA=F^*$, where F^* is derived from the vector F by the cyclic shift of the coordinates for q places downwards. From this one more matrix form for the representation (3.4.1) is derived

$$f(x)=H^*WF^*. \tag{3.4.5}$$

The representation (3.4.1) in expansion form will be written using (3.4.4) and (3.4.3)

$$f(x)=\sum_{r=0}^{p-1}(x+q)^r \sum_{k=0}^{p-1} f(k)\,[1-r^{p-1}-(k-q)^{p-1-r}]. \tag{3.4.6}$$

The representation of the form (3.4.6) will be called a generalized polynomial modulo p.

Analogous relations hold for the generalized polynomials of n variables as well as for the polynomials modulo p. They will be mentioned here without proofs since they are performed in the same way.

Theorem 3.8. *Every p-valued function of n variables has a representation of the form*

$$f(X)=\sum_{r=0}^{p-1}(x_i+q_i)^r \sum_{k=0}^{p-1} f(x_i=k)\,[1-r^{p-1}-(k-q)^{p-1-r}]. \tag{3.4.7}$$

The representation (3.4.7) will be called the expansion theorem of p-valued functions about powers $(x_i+q_i)^r$ $(r=0,\dots,p-1)$.

Theorem 3.9. *Every p-valued function of n variables has a representation of the form*

$$f(X)=(H_1^*\times\cdots\times H_n^*)(W_1^*\times\cdots\times W_n^*)F_{1\dots n}, \tag{3.4.8}$$

$$f(X)=(H_1^*\times\cdots\times H_n^*)(W_1\times\cdots\times W_n)F_{1\dots n}^*. \tag{3.4.9}$$

Matrix forms of the generalized polynomials modulo p are given by (3.4.8) and (3.4.9). These polynomials are generalizations of the polarized polynomial forms over the field J_2. Therefore they can also be called polarized polynomials mod p unlike the polynomials mod p of more general form which will be considered later.

The possibility of representing p-valued functinns by the generalized polynomials has been proved by M. COHN **[46]** and they were called T-forms because they are analogous to the expansion of the polynomials into the TAYLOR

series. Then the representations by polynomials mod p correspond to the expansion into the MACLAURIN series. These representations are called M-forms by M.COHN.

There are polynomials of more general form than the generalized (polarized) polynomials. An example of the polynomials generalization (3.3.1) is represented by the polynomials

$$f(x)=a_0+\sum_{r=1}^{P-1} a_r\cdot(x+q_{r1})\cdot\ldots\cdot(x+q_{rr})\ (q_{rj}\in J_p). \tag{3.4.10}$$

Generalization for the p-valued functions of n variables can be performed in the same way. Namely, considering the set of these functions as the p^n-dimensional vector space over the field J_p from (3.3.9) it is seen that for polynomials the basis consists of the system of vectors

$$1,\ x_1,\ \ldots,\ x_1^{p-1},\ x_2,\ x_1x_2,\ \ldots,\ x_1^{p-1}\cdot\ldots\cdot x_n^{p-1}. \tag{3.4.11}$$

If the power $(x_i+q_i)^{s_i}(x_i+q_i)^{s_i-s_i'}\ (s_i'<s_i)$ is taken instead of the power $x_i^{s_i}$ in (3.4.11) a new basis is derived. This is the consequence of the theorem of M. COHN [12] which is as follows:

Theorem 3.10. *Every generalized basis is the basis of the vector space which consists of the p-valued functions of one variable.*

As a generalized basis in the Theorem 3.10 the system of vectors $h_r(x)\ (r=0,\ldots,p-1)$ is considered of such a kind that each of them is represented by the polynomial mod p of the form (3.3.1) whose power equals r.

4. REPRESENTATIONS OVER THE RING OF INTEGERS mod m

4.1. sph polynomial forms

Let J_m be the ring of integers modulo m. Functions defined over J_m by the values from J_m will be called m-valued functions.

Addition over the ring J_m will by denoted bu $+$ and multiplication by $\cdot$ or with juxtaposition of factors.

An inverse element to the element $t\in J_m$ will be denoted by $-t$.

It is known that (see [53, 54]) for the case of the ring J_m all m-valued functions cannot be represented by the polynomials, for the operations $+$ and $\cdot$ together with the constants $0,\ldots,m-1$ do not form a complete set. In this chapter it will be shown that by adding of certain numbers of unary functions to the above mentioned set of functions a complete set of functions is derived and the representations of m-valued functions with that complete set will be given.

All the theorems on the representations of the p-valued functions by means of the characteristic functions, which were proved in the preceding chapter for the field J_p, are also proved in the same way for the ring J_m. That is why all the considerations from 3.1 are completely transfered here as well, replacing p by m. Further generalization is given below.

Let $h_0(x), \ldots, h_{m-1}(x)$ be a certain defined system of m-valued functions of one variable. Let us investigate the conditions which should be satisfied by this system so that any m-valued function of one variable could have the representation of the form

$$f(x) = \sum_{r=0}^{m-1} a_r h_r(x) \qquad (a_r \in J_m). \tag{4.1.1}$$

Put $A^T = \|a_0, \ldots, a_{m-1}\|$, $F^T = \|f(0), \ldots, f(m-1)\|$, $H = \|h_0(x), \ldots, h_{m-1}(x)\|$. Then (4.1.1) has the following matrix form

$$f(x) = HA. \tag{4.1.2}$$

Replacing the values for the variable x in (4.1.1), the following system of congruences is derived

$$\sum_{r=0}^{m-1} a_r h_r(k) = f(k) \qquad (k = 0, \ldots, m-1), \tag{4.1.3}$$

or in matrix form

$$LA = F, \tag{4.1.4}$$

where L is the matrix of the system, that is

$$L = \begin{Vmatrix} h_0(0) & h_1(0) & \cdots & h_{m-1}(0) \\ h_0(1) & h_1(1) & & h_{m-1}(1) \\ \vdots & & & \\ h_0(m-1) & h_1(m-1) & & h_{m-1}(m-1) \end{Vmatrix}.$$

The following theorem will be proved.

Theorem 4.1. *Necessary and sufficient condition of the existence of the unique representation of the form* (4.1.1) *is*

$$(\det L, m) = 1. \tag{4.1.5}$$

Proof. The system (4.1.3) may be written in the following form (see **[47]** $\Delta a_r = \Delta_r (r = 0, \ldots, m-1)$, where $\Delta = \det L$ and Δ_r is derived replacing in the r-th column by the column of the function value.

In order that a unique solution for a_r would exist it is necessary and sufficient that $(\Delta, m) = 1$ (see **[49]**). This completes the theorem.

Represeotations of m-valued functions of the form (4.1.1) will be called polynomial forms mod m (or in short: polynomial forms).

Polynomial forms may be considered as a generalization of polynomials which were previously considered in the same sense as was the case with the representations of the functions over the field of real numbers by means of the system of orthogonal functions (see **[48]**).

By Teorem 4.1 it was proved that, by adding m unary functions to the operations $+$, $\cdot$ and the constants $0, \ldots, m-1$, representations of m-valued functions of one variable are obtained. It will now be proved that thus a complete set of m-valued functions is obtained.

Let $h_0(x)=g_0(x)$. According to Theorems 3.1 and 4.1 it follows that it is sufficient to add only one unary function to get, in a case of a nonprime nunber m, a complete set of m-valued functions which consists of $+$, $\cdot$ (mod m) the constants $0, \ldots, m-1$ and $g_0(x)$. The matrix L in the given case is an identity matrix I of the order m. In general, if the matrix L is circulant, the same case will follow.

The question arises how many different possible sets of functions $h_r(x)\,(r=0, \ldots, m-1)$ for the given m satisfy the condition of Theorem 4.1. That condition is reduced to the investigation of matrices whose determinant is relatively prime to m. For the sake of deriving a solution, the total number of such matrices should be divided by $m!$, for matrices obtained from each other by permutations of columns are considered as one and the same solution.

The number of square matrices of order m whose determinant mod m is relatively prime to m is determined in references **[50, 51]**.

From the condition $(\det L, m)=1$ it follows that the matrix L will have an inverse matrix $L^{-1}=W$. Then from (4.1.1) it follows that $A=WF$. Replacing in (4.1.2) we will have

$$f(x)=HWF. \tag{4.1.6}$$

If $w_{rk}\,(r, k=0, \ldots, m-1)$ are the elements of the matrix W then from (4.1.6) it follows that

$$f(x)=\sum_{r=0}^{m-1} h_r(x) \sum_{k=0}^{m-1} w_{rk} f(k). \tag{4.1.7}$$

Let $f(X)$ be an m-valued function of n variables. If we denote

$$F_i^T=\|f(x_i=0) \quad \ldots \quad f(x_i=m-1)\|$$

then, performing the same procedure as while proving the representations (4.1.6) and (4.1.7), respectively, the following theorem is proved.

Theorem 4.2. *Every m-valued function of n variables has a representation of the from*

$$f(X)=H_iWF_i, \tag{4.1.8}$$

or

$$f(X)=\sum_{r=0}^{m-1} h_r(x_i) \sum_{k=0}^{m-1} w_{rk} f(x_i=k). \tag{4.1.9}$$

The representations (4.1.8) and (4.1.9), respectively, will be called the expansion theorem of the m-valued functions of n variables about the functions $h_r(x_i)$ $(r=0, \ldots, m-1)$ of the variable x_i.

Starting from (4.1.8) by mathematical induction method in the same way as in the proof of the Theorem 3.7 of the preceding chapter, the following theorem is proved.

Theorem 4.3. *Every m-valued function of n variables has a representation of the form*

$$f(X)=(H_1\times\cdots\times H_n)(W_1\times\cdots\times W_n)F_{1\ldots n}, \tag{4.1.10}$$

where $W_1=\cdots=W_n=W$.

The representations (4.1.10) will be called the polynomial forms for m-valued functions of n variables.

4.2. Generalized polynomial forms

The polynomial forms from the preceding passage will be generalized in the following way. Let us invetsigate the possibility of represen'ing m-valued functions of one variable in the form

$$f(x)=\sum_{r=0}^{m-1} a_r h_r(x+q) \quad (q\in J_m). \tag{4.2.1}$$

The representation (4.2.1) represents, from one side, a generalization of the polynomial form (4.1.1) for the system $h_r(x+q)$ $(q\in J_m)$ is used instead of the system $h_r(x)$ $(r=0,\ldots,m-1)$. The same complete set of functions as for (4.1.1) is being used for the functions $h_r(x+q)$ may be obtained from the functions $h_r(x)$ so that the variable $x+q$ is first realized. On the other hand, the representation (4.2.1) is a generalization of the polynomial representation (3.4.1) for the system $h_r(x+q)$ used instead of the system of functions $(x+q)^r$. Therefore the polynomial representations may be regarded as a particular case of the representation (4.2.1) when $h_r(x+q)=(x+q)^r$.

The proofs of the theorems in this chapter are analogous to the previous ones, but they will nevertheless be given because this will be the most general case of the representations which will be considered in this thesis.

Put $H^*=\|h_0(x+q),\ldots,h_{m-1}(x+q)\|$. Then (4.2.1) will have the following matrix form

$$f(x)=H^*A. \tag{4.2.2}$$

Replacing the values for the variable x in (4.2.1) the following system of congruences will be obtained

$$\sum_{r=0}^{m-1} a_r h_r(k+q)=f(k) \quad (k=0,\ldots,m-1), \tag{4.2.3}$$

or in matrix form

$$L^*A=F, \tag{4.2.4}$$

where L^* is the matrix of the system (4.2.3) and

$$L^*=\begin{Vmatrix} h_0(q) & h_1(q) & \cdots & h_{m-1}(q) \\ h_0(q+1) & h_1(q+1) & & h_{m-1}(q+1) \\ \vdots & & & \\ h_0(q-1) & h_1(q-1) & & h_{m-1}(q-1) \end{Vmatrix}$$

Confering the matrix L^* to the matrix L from the proceding passage it can be seen that L^* is derived from L by a cyclic shift of the rows for q places upwards.

The lemma from the passage 3.4 holds for the ring J_m if the determinant of the matrix satisfies the condition of Theorem 4.1. Thus, in order that there exist a unique solution of the sustem (4.2.3) it is necessary and sufficient that

the matrix L or L^* has an inverse matrix for any value of $q \in J_m$. If we denote $(L^*)^{-1} = W^*$ then from (4.2.4) it follows that $A = W^* F$ and replacing in (4.2.2)

$$f(x) = H^* W^* F. \tag{4.2.5}$$

The system (4.2.2) can also be written in the following way

$$\sum_{r=0}^{m-1} a_r h_r(k) = f(k-q) \qquad (k = 0, \ldots, m-1),$$

or in matrix form $LA = F^*$, where $(F^*)^T = \| f(m-q) \ \ldots \ f(m-q-1) \|$ and is obtained from the vector F by a cyclic shift of the coordinates for q places downwards.

It is now $A = L^{-1} F^* = WF^*$ and replacing A in (4.2.2) one more matrix form for the representation (4.2.1) is obtained

$$f(x) = H^* WF^*. \tag{4.2.6}$$

The representations (4.2.5) and (4.2.6), respectively, will be called the generalized forms for m-valued functions of one variable.

Now let $f(X)$ be a m-valued function of n variables. Let the system of functions $h_r(x)$ satisfy the conditions of Theorem 4.1. The following theorem will be proved.

Theorem 4.4. *Every m-valued function of n variables has a representation of the form*

$$f(X) = H_i^* W_i^* F_i, \tag{4.2.7}$$

$$f(X) = H_i^* W_i F_i^*, \tag{4.2.8}$$

Proof. Let us investigate the conditions of existence for $f(X)$ of the following representation

$$f(X) = \sum_{r=0}^{m-1} h_r(x_i + q_i)\, a_r(x_1, \ldots, x_{i-1}, x_{i+1}, \ldots, x_n). \tag{4.2.9}$$

Replacing the values of the variable x_i in (4.2.9) and repeating the same procedure as with obtaining the representations (4.2.5) and (4.2.6), the representations (4.2.5) and (4.2.6), the representations (4.2.7) and (4.2.8) follow (see [52]).

The representations (4.2.7) and (4.2.8) will be called the generalized expansion theorem of m-valued functions of n variables about the functions $h_r(x_i + q_i)$ of the variable x_i.

Starting from the representations (4.2.7) and (4.2.8) the following theorem will be proved.

Theorem 4.5. *Every m-valued function of n variables has a representation of the form*

$$f(X) = (H_1^* \times \cdots \times H_n^*)(W_1^* \times \cdots \times W_n^*) F_{1\ldots n}, \tag{4.2.10}$$

$$f(X) = (H_1^* \times \cdots \times H_n^*)(W_1 \times \cdots \times W_n) F_{1\ldots n}^*, \tag{4.2.11}$$

where the matrix W_i^* *is derived from the matrix* $W_i (i = 1, \ldots, n)$ *by a cyclic shift of the columns for* q *places to the left.* $F_{1\ldots n}^*$ *is derived from the vector* $F_{1\ldots n}$ *by a cyclic shift of the coordinates for* q *places downwards. The value* q *is determined by* $q = q_1 m^{n+1} + q_2 m^{n-2} + \cdots + q_n$ *(real arithmetic).*

Proof. The proof will be given for (4.2.10). The proof for (4.2.11) is analogous to that for (4.2.10).

The proof is by induction on n. For $n = 1$ the theorem holds by (4.2.7) Assume that it holds for $n-1$ and let us prove that then it will also hold for n.

Let us express the function $f(X)$ about the functions $h_r(x_n + q_n) (r = 0, \ldots, m-1)$ of the variable x_n according to (4.2.7). All the coordinates of the vector F_i are functions of $n-1$ variables. According to the inductive assumption each of these coordinates for the variables $x_1, \ldots, x_{n-1}$ has a representation of the form

$$f(X) = Y^* Z^* F_{1\ldots n-1}(x_n = k) \qquad (k = 0, \ldots, m-1), \tag{4.2.12}$$

where $Y^* = H_1^* \times \cdots \times H_{n-1}^*$, $Z^* = W_1^* \times \cdots \times W_{n-1}^*$ and where $F_{1\ldots n-1}(x_n = k)$ denotes that in each coordinate of the vector $F_{1\ldots n-1}$ the variable x_n should be replaced by the value k.

Expanding (4.2.7) and replacing $f(x_n = k)$ according to (4.2.12) it will be obtained that

$$\begin{aligned} f(X) &= \sum_{r=0}^{m-1} \sum_{k=0}^{m-1} h_r(x_n + q_n)\, w_{rk}\, f(x_n = k) \\ &= \sum_{r=0}^{m-1} \sum_{k=0}^{m-1} h_r(x_n + q_n) [Y^* Z^* F_{1\ldots n-1}(x_n = k)] \\ &= \sum_{r=0}^{m-1} \sum_{k=0}^{m-1} [h_r(x_n + q_n)\, Y^*] (w_{rk} Z^*) F_{1\ldots n}(x_n = k) \\ &= (Y^* \times H_n^*)(Z^* \times W_n^*) F_{1\ldots i}. \end{aligned}$$

whence the proof of (4.2.10) follows immediately.

The representations (4.2.10) and (4.2.11) will be called the generalized polynomial form for m-valued functions of n variables.

One more further generalization of the polynomial forms will be given. Let the system of vectors

$$h_r(x) \qquad (r = 0, \ldots, m-1), \tag{4.2.13}$$

satisfy the conditions of theorem 4.1. Then every m-valued function can be represented by polynomial forms (4.2.5) or (4.2.6).

If the system of vectors

$$h_r(x + q) \qquad (r = 0, \ldots, m-1) \tag{4.2.14}$$

is used then each m-valued function will have from one to m^n different representations by means of the generalized polynomial forms (4.2.10) or (4.2.11)

(for $q_i = 0, \ldots, m-1$, $i = 1, \ldots, n$). The particular case of these representations are the polynomial forms which are obtained for $q_i = 0$. If the matrix of the system of vectors is circulant then there is only one polynomial form.

Furter generalization of polarized polynomial form are representations with the system of vectors

$$h_r(x + \bar{q_r}) \qquad (r = 0, \ldots, m-1;\ q \in J_m). \tag{4.2.15}$$

These representations will be called nonpolarized polynomial forms. Matrices which characterize these forms for m-valued functions of one variable are derived by the cyclic shift of each column particularly for q_r places upwards but not by the cyclic shift of rows as with the generalized polynomial forms. For a given matrix of the order m, m^m different matrices can be derived by means of this shift. However, the determinants of all these matrices will not satisfy the condition of the Theorem 4.1.

From the results of M. COHN it follows that, for the case of the field J_p, every p-valued function of one variable has p^{p-1} nonpolarized polynomial forms. However, there are matrices of the order p which allow obtaining a still greater number of nonpolarized polynomial forms. Thus, investigating on the computer all the matrices of the order 3×3 over the field J_3 it has been established that there are matrices which allow obtaining 24 nonpolarized polynomial forms which is significantly more than it has been known so far.

The problem of investigation of the number of nonpolarized polynomial forms for the matrices of the order m over the ring J_m has not been considered so far and remains unsolved.

4.3. Polynomial functions mod m

If an m-valued function of one variable is representable by the polynomial

$$f(x) = \sum_{r=0}^{s(m)-1} a_r x^r \quad (a_r \in J_m), \tag{4.3.1}$$

it will be called a polynomial function.

When $m = p$ (p a prime), then every m-valued function is polynomial and $s(m) = p$ (see **[53, 54]**). All the functions over the ring J_m are not polynomial ones and the power $s(m) < m$ and is defined by the expression (see **[55, 56]**)

$$s(m) = \min_j \{m \mid j!\}. \tag{4.3.2}$$

Let us mention that the value for $s(m)$, as derived from the generalized FERMÀT theorem (see **[57, 58]**) in most cases is considerably greater than the value defined by (4.3.2).

Replacing the values for the variable x in (4.3.1) the following system of congruences is obtained:

$$\sum_{r=0}^{s(m)-1} a_r k^r = f(k) \qquad (k = 0, \ldots, m-1). \tag{4.3.3}$$

The extended matrix of the sistem (4.3.6) has the following form

$$L' = \left\| \begin{array}{cccccc} 1 & 0 & 0 & \cdots & 0 & f(0) \\ 1 & 1 & 1^2 & & 1^{s(m)-1} & f(1) \\ 1 & 2 & 2^2 & & 2^{s(m)-1} & f(2) \\ \vdots & & & & & \\ 1 & m-1 & (m-1)^2 & & (m-1)^{s(m)-1} & f(m-1) \end{array} \right\|.$$

The rows of the matrix L' will be denoted by the numbers from 0 to $m-1$ and the columns from 0 to $s(m)$.

If the notion of the finite difference is defined over J_m as over the field of real numbers (see [**32**]), the following relation can be proved as well

$$D^r f(0) = f(r) - \sum_{i=0}^{r-1} \binom{r}{i} D^i f(0). \tag{4.3.4}$$

The following equivalent transformations will be performed over the matrix L' (see [**59, 60**]).

The row denoted by zero previously multiplied by $\binom{r}{0}$ is subtracted from the r-th row ($r = 1, \ldots, m-1$) (It is defined that $0! = 1$ and $\binom{n}{0} = \binom{0}{0} = 1$ ($n = 1, 2, \ldots$) over the ring J_m). Then the corresponding elements of the $s-1$-th column previously multiplied by 1 are subtracted from the elements of the r-th column ($s = 2, \ldots, S-1$) (the notation $S = s(m)$ will be used as a short from). Then the first row, previously multiplied by $\binom{r}{1}$, is subtracted from the t-th row ($r = 2, \ldots, m-1$). Transformations of the rows from the S-th to the m-th step only are being preformed. As a result the following matrix is obtained (at every step of the transformation on the matrix L', replacing in the S-th column has been done according to the formula 4.3.4).)

$$L'_d = \left\| \begin{array}{cccccc} 0! & 0 & 0 & \cdots & 0 & D^0 f(0 \\ 0 & 1! & 0 & & 0 & Df(0) \\ \vdots & & & & & \\ 0 & 0 & 0 & & (S-1)! & D^{S-1} f(0) \\ 0 & 0 & 0 & & 0 & D^S f(0) \\ \vdots & & & & & \\ 0 & 0 & 0 & & 0 & D^{m-1} f(0) \end{array} \right\|.$$

Let L be a matrix of the system of congruences (4.3.3). Then it has the following matrix from

$$LA = F. \tag{4.3.5}$$

The transformation of the rows of the extended matrix L' at the k-th step ($k = 1, \ldots, m-2$) may be represented as the product of the left-hand and right-hand side of the (4.3.5) by the square matrix of the order m which

has ones on the main diagonal and at the i-th place of k-th column elements

$$-\binom{r}{i} \quad (i=k+1, \ldots, m-1).$$

Transformations of the columns at the k-th step ($k=1, \ldots, S-2$) may be represented as the multiplication of the matrix L' from the right-hand side by the square matrix of the order S which has ones on the main diagonal and elements — k on the diagonal $j-i=1$ (i, j ordinal numbers of the row and column of a certain element of the matrix), beginning from the k-th to the $S-1$-th column.

Then the system (4.3.5) may be replaced by the equivalent system

$$(ULV)(V^{-1}A)=UF, \tag{4.3.6}$$

where the matrices U and V represent the product of all matrices by which the transformations of the rows and columns have been done.

Put $ULV=L_d$, $V^{-1}A=B$, $F_D^T=\| D^0f(0), \ldots, D^{m-1}f(0) \|$. Then the system of congruences (4.3.6) takes the following form

$$L_dB=F_D. \tag{4.3.7}$$

The two known results from the theory of numbers will be required which will be quoted as lemmas (see proofs in [**49**]).

Lemma 4.1. *Let $(a, m)=d$. The congruence $ax=b \pmod m$ has no solution if b cannot be divided by d. If b is divisible by d then the congruence has d solutions.*

Lemma 4.2. *If x takes the values from the complete set of the residues modulo m, then $x+b$, b being any prime, takes the values from the complete set of the residues modulo m as well.*

The following theorems will be proved.

Theorem 4.6. *The m-valued function of one variable is polynomial if and only if for all values $r=0, \ldots, m-1$*

$$D^rf(0)=0 \ (\mathrm{mod}\,(r!, m)). \tag{4.3.8}$$

Proof. The matrix equation may be written in the following form

$$\begin{aligned} r!\,b_r &= D^rf(0) \quad (r=0, \ldots, s(m)-1) \\ Ob_r &= D^rf(0) \quad (r=s(m), \ldots, m-1). \end{aligned} \tag{4.3.9}$$

In order that the system (4.3.9) should have, according to Lemma 4.1, a unique solution with respect to b_r, it is necessary and sufficient that for all $r=0, \ldots, m-1$ $D^rf(0)$ is divisible by $(r!, m)$. This completes the theorem.

The condition when a function over the ring J_m will be polynomial has been considered in references [**61**, **62**]. Another case, analogous to Theorem 4.6, when a function will be polynomial, has been proved in [**61**].

For the case when $m=p_1 \cdots p_k$, the condition for a function to be polynomial has been given in [**63**].

A. J. KEMPNER has proved in [55] how many m-valued polynomial functions of one variable there are for a given m. It will be proved here using the equivalent system of congruences (4.3.7) obtained the folloving theorem.

Theorem 4.7. *The total number $N(m)$ of the polynomial m-valued functions of one variable is*

$$N(m)=\frac{m^{s(m)}}{(0!,m)\cdots([s(m)-1]!,m)}. \tag{4.3.10}$$

Proof. The system (4.3.9) can be written, according to (4.3.5), in the following way

$$\begin{aligned} r!\,b_r &= f(r)-f_r \quad (r=0,\ldots,s(m)-1),\\ 0\,b_r &= f(r)-f_r \quad (r=s(m),\ldots,m-1), \end{aligned} \tag{4.3.11}$$

where

$$f_r=\sum_{i=0}^{r-1}\binom{r}{i}D^i f(0).$$

For every r, $f(r)$ can take one of the values from J_m. When $f(r)$ takes all possible values from J_m then, according to the Lemma 4.2, $f(r)-f_r$ will also take all possible values from J_m. However, $f(r)$ will satisfy the condition (4.3.8) only for those values for which $f(r)-f_r$ is divisible by $(r!, m)$. Hence, the proof of the theorem follows immediately.

On the basis of the known concepts from the theory of numbers, the equation (4.3.10) can also be written in the following way

$$N(m)=\prod_{i=1}^{k}N\left(p_i^{e_i}\right), \tag{4.3.12}$$

where $m=p_1^{e_1}\cdots p_k^{e_k}$.

4.4 Transformations of the m-valued functions

The analogy be pointed out existing between the representations of m-valued functions by polynomial forms and transformations, particularly FOURIER transformation. K. S. MENGER has shown in [45] how the polynomial representatios of p-valued functions of one variable can be interpreted as FOURIER transformation for the case when $f(0)=0$.

That analogy will be obtained putting in (3.3.2) $f(0)=0$

$$a(r)=(p-1)\sum_{x=1}^{p-1}f(x)\,x^{-r}, \tag{4.4.1}$$

$$f(x)=\sum_{r=1}^{p-1}a(r)\,x^r. \tag{4.4.2}$$

Conferring with the FOURIER transformation

$$G(\omega)=\frac{1}{2\pi}\int_{-\infty}^{+\infty} f(t)\,e^{-j\omega t}\,dt, \tag{4.4.3}$$

$$f(t)=\int_{-\infty}^{+\infty} G(\omega)\,e^{j\omega t}\,d\omega. \tag{4.4.4}$$

it can be seen that there is the following analogy: x^{-r} corresponds to $e^{-j\omega t}$, x^r corresponds to $e^{j\omega t}$, summation to integration etc. Since the function $f(x)$ is always given either in tabular or in analytical form it will be considered as the original and $a(r)$ as its image.

From these consideradions a conclusion imposes naturaly that, without the limitation $f(0)=0$, the following transformation for the given p-valued function $f(x)$ of one variable should be introduced

$$a(r)=(p-1)\sum_{x=0}^{p-1} f(x)\,(r^{p-1}+x^{p-1-r}-1), \tag{4.4.5}$$

$$f(x)=\sum_{r=0}^{p-1} a(r)\,x^r. \tag{4.4.6}$$

Representations of the m-valued functions by polynomial forms can also be considered as a transformation. The rows of the matrix W in (4.1.6) can be considered as the m-valued functions of one variable, that is

$$W^T=\begin{Vmatrix} w_0(0) & w_1(0) & \cdots & w_{m-1}(0) \\ w_0(1) & w_1(1) & & w_{m-1}(1) \\ \vdots & & & \\ w_0(m-1) & w_1(m-1) & & w_{m-1}(m-1) \end{Vmatrix}.$$

Then it can be written

$$a(r)=\sum_{x=0}^{m-1} w_r(x)\,f(x), \tag{4.4.7}$$

$$f(x)=\sum_{r=0}^{m-1} a(r)\,h_r(x). \tag{4.4.8}$$

Analogous considerations can also be carried out for the functions in several variables.

The way of obtaining coefficients $a_r\,(r=0,\ldots,m-1)$ in polynomial forms for the m-valued functions of one variable can be generalized in the following way.

Let a system of m m-valued functions $u_j(x)$ $(j=0, \ldots, m-1)$ of one variable be given, which will be characterized by the matrix

$$U = \left\| \begin{array}{lll} u_0(0) & u_1(0) & \cdots \; u_{m-1}(0) \\ u_0(1) & u_1(1) & \quad\; u_{m-1}(1) \\ \vdots & & \\ u_0(m-1) & u_1(m-1) & \quad\; u_{m-1}(m-1) \end{array} \right\|,$$

and let $(\det U, m)=1$. If the representation (4.1.6) exists then, according to (4.1.4) it can be written as follows

$$A=[L^{-1}(U^T)^{-1}](U^T F). \tag{4.4.9}$$

The expression (4.4.9) can be considered as the most general one and the coefficients in the polynomial forms can be determined by it. However, the following two cases are of particular importance.

Let $U=L$ and $L^TL=\operatorname{diag}(d_{00}, \ldots, d_{m-1,m-1})$ be a diagonal matrix where $(d_{rr}, m)=1$ is true for all $d_{rr}(r=0, \ldots, m-1)$. Then, according to (4.4.9) and (4.1.2), it follows that

$$a_r = d_{rr}^{-1} \sum_{x=0}^{m-1} h_r(x) f(x) \quad (r=0, \ldots, m-1) \tag{4.4.10}$$

where $d_{rr}=\sum_{x=0}^{m-1} h_r^2(x)$.

If $U=L$ and L is an orthogonal matrix, i.e. $L^TL=I$, then

$$a_r = \sum_{x=0}^{m-1} h_r(x) f(x). \tag{4.4.11}$$

The coefficients a_r in polynomial forms, which represent an analogy of the expansion into the orthogonal series, are determined by the relations (4.4.10) and (4.4.11).

4.5. Algebraic forms

Let $R=\{e_0, e_1, \ldots, e_{m-1}\}$ and let $(R, +, \cdot)$ form an algebraic structure of the commutative ring with unity (unity elements for operations $+$ and $\cdot$, reprectively, are denoted by e_0 and e_1).

It will be shown that results about the representations of m-valued functions which have already been considered may be transferred to the ring R. Those representations will be considered as the generalization of the polynomial forms considered in references [7, **52**, **64 – 67**] and in this chapter.

Let a system of m-valued functions of one variable $h_r(x)$ $(r=0, \ldots, m-1)$ be given. This system will be characterized by the following matrix

$$L = \left\| \begin{array}{lll} h_0(e_0) & h_1(e_0) & \cdots \; h_{m-1}(e_0) \\ h_0(e_1) & h_1(e_1) & \quad\; h_{m-1}(e_1) \\ \vdots & & \\ h_0(e_{m-1}) & h_1(e_{m-1}) & \quad\; h_{m-1}(e_{m-1}) \end{array} \right\|.$$

Let us investigate the condition that every m-valued function of one variable, given by its values $f(e_0), \ldots, f(e_{m-1})$, may be represented over the ring R in the following way

$$f(x)=\sum_{r=0}^{m-1} a_j h_j(x) \quad (a_j \in R), \tag{4.5.1}$$

or in the matrix form

$$f(x)=HA. \tag{4.5.2}$$

Replacing the values for a variable x in (4.5.1) the following system of equations is obtained:

$$f(k)=\sum_{r=0}^{m-1} a_r h_r(k) \quad (k=e_0, \ldots, e_{m-1}). \tag{4.5.3}$$

which has the following matrix form

$$F=LA, \tag{4.5.4}$$

where $F^T=\| f(e_0) \ \ldots \ f(e_{m-1}) \|$.

The following theorem will be proved.

Theorem 4.8. *A necessary and sufficient condition for the existing of a unique representation of the form* (4.5.1) *for every m-valued function of one variable is that the determinant of the matrix L be an element from R which is invertible in reference to the operation* $\cdot$.

Proof. System (4.5.3) may be written in the form (see **[47]**)

$$\Delta a_r=\Delta_r \quad (r=0, \ldots, m-1), \tag{4.5.5}$$

where $\Delta=\det L$ and Δ_r is derived replacing the r-th column by the column of the function values.

In order that a unique solution for a_r exists it is necessary and sufficient that det L be an element from R which is invertible with respect to the operation $\cdot$ (see **[68]**). This completes the proof.

From the invertibility of the determinant over R it follows that the matrix L will be regular, i.e., the matrix L will have over R the inverse matrix L^{-1}. Then, from (4.5.4) $A=L^{-1}F$ and replacing A in (4.5.2) it follows that

$$f(x)=HL^{-1}F. \tag{4.5.6}$$

The representations of the form (4.5.1) (or the matrix form (4.5.6)) will be called the algebraic forms.

Further gereralization of the algebraic forms are the representations

$$f(x)=\sum_{r=0}^{m-1} a_r h_r(x+e_q) \quad (e_q \in R), \tag{4.5.7}$$

or in the matrix form

$$f(x)=H^*A, \tag{4.5.8}$$

where $H^*=\| h_0(x+e_q) \ \ldots \ h_{m-1}(x+e_q) \|$.

Replacing the values for the variable x in (4.6.7) the following system of equations will be derived

$$f(k)=\sum_{r=0}^{m-1} a_r h_r(k+e_q) \quad k=e_0, \ldots, e_{m-1}).$$

This sistem of equations may be represented in the matrix form in the following two ways

(4.5.9) $$F=L^*A,$$

(4.5.10) $$F^*=LA,$$

where $(F^*)^T=\|f(e_{m-q}) \ldots f(e_{m-q-1})\|$ and L^* is the matrix which is obtained from the matrix L by a cyclic shift of the rows for q places upwards.

As $\det L^*=(-1)^{qm}\det L$ and since $\det L$ is an element from R which is invertible in R the inverse matrix $(L^*)^{-1}$ will hence exist, for from the invertibility of $\det L$, the invertibility of element $-\det L$ follows (see **[68]**).

According to (4.5.9) and (4,5.10) it follows that

(4.5.11) $$A=(L^*)^{-1}F=L^{-1}F^*.$$

Replacing (4.5.11) in (4.5.8) it will finally be obtained that

(4.5.12) $$f(x)=H^*(L^*)^{-1}F,$$

(4.5.13) $$f(x)=H^*L^{-1}F^*.$$

The representations (4.5.12) and (4.5.13) will be called the generalized algebraic forms.

For every m-valued function of one variable there are in total m generalized algebraic forms. The particular case for $e_q=e_0$ are the algebraic forms.

The analytical representations by algebraic forms and generalized algebraic forms for m-valued functions of n variables can be obtained in the same way as under 4.2. Therefore they will not be considered here.

5. SOME UNSOLVED PROBLEMS AND POSSIBLE GENERALIZATIONS

5.1. It is of interest in technical applications that a representation of m-valued functions is to be found whose realization is optimal according to a criterion given in advance. As a criterion of that kind, for example, serve the total number of logical elements $+$ and $\cdot$ (mod m) required for the realization of the given function. This problem is known as the minimization of m-valued functions.

The generalized polynomial forms (4.2.1) give a possibility that m different analitical representations by polynomial forms in the general case can be derived for the same m-valued function of one variable. The problem how to select the value q to derive a minimal polynomial form has remained unsolved. D. A. POSPELOV has shown in **[24]** that this problem can be reduced to the linear integer programming but further considerations do not exist.

Still larger optimization of the polynomial forms can be achieved if the vector system (4.2.15) obtained by cyclic shift of certain columns is used for representations. There are two problems left which are worth paying attention.

First, how to establish for the given matrix L of the order m how many of m^m matrices, obtained by cyclic shift of the columns, satisfy the condition of Theorem 4.1.

Secondly, how to find an optimum polynomial form among the possible ones of that kind.

5.2. Instead of using m functions of one variable for the polynomial forms (4.1.1), any subset of those functions and the subset of all possible componentwise products of those functions may be taken. It would be interesting here to find out criteria for determining when the componentwise product of two or more vectors over the ring J_m will be linearly independent with those vectors as well as which and how many of such products will be linearly independent with the given set of vectors and with the rest of the products.

5.3. Polynomial forms may be used for generation of codes over the field J_p or the ring J_m. This was not considered in this thesis as well. Consideration of the codes over the ring J_m represents a particular interest for, as far as the author knows, such codes have not been considered so far.

For the case of the field J_p, codes of the REED-MULLER type for $p=2$ can be generated by polynomials mod p as well (see **[1, 28, 37, 38]**). Such a generalization has not been considered yet.

Consideration of these representations will be interesting as well as the investigation of their deriving.

5.4. Let us point out some more interesting unsolved problems.

In the case of the synthesis of the switching circuits by POVAROV cascade method (see **[14]**) over any complete set of functions, the sequence by means of which the expansion is performed results in complexity of the derived switching circuits. The hypothesis on usage of the BOOLEan difference to determine the sequence of expansion has been given in reference **[8]** in connection with the synthesis of switching circuits with majority functions. It will surely be of interest to try to find out of what significance the BOOLEan difference may be here.

The polynomial functions mod m have been considered under 4.3. It is not known at present how many of all permutations of the set $\{0, 1, \ldots, m-1\}$ may be representen by the polynomials for the case of the ring J_m.

Besides representations by polynomials or polynomial forms, m-valued functions can be representad by other canonical forms as well. Transition from one representation to another for $m \neq 2$ has not been considered so far (for $m=2$, see **[20]**).

The operation $+ \pmod m$ can be aplied to the arithmetic units of a computer and that is why its incorporation into the complete set of functions is of importance (see **[69]**). However, this is not true for the operation $\cdot \pmod m$ so that it would also be interesting to investigate another complete sets into which the operation $+ \pmod m$ is incorporated. Some considerations on this subject can be found in reference **[70]**.

REFERENCES

1. S. B. AKERS: *On a theory of Boolean functions.* J. Soc. Ind. and Appll. Math. **7** (1959), 487—498.

2. R. D. BOCHMANN: *Über Aaleitungen in der Schaltalgebra und einen damit formulierbaren Entwicklunssatz.* Wiss. Z. Techn. Univ. Dresden, **14** (1965), 1523—1527.

3. I. S. REED: *A class of multiple-error-correcting codes and the decoding scheme.* IRE Trans. Inform. Theory, PGIT-**4** (1954), 38—49.

4. F. F. SELLERS, et al.: *Analysing errors with the Boolean difference.* IEEE Trans. Computers, C-**17** (1968), 676—683.

5. F. F. SELLERS, et al.: *Error detecting logic for digital computers.* New York, 1968.

6. D. BOHMAN: *Kritičeskie perehody v diskretnyh shemah i strukturnye metody ih lokalizacii.* Dissertacija na soiskkanie učenoj stepeni kandidata tehničeskih nauk. Moskovskij elektrotehničeskij institut svjazi, Moskva, 1968.

7. D. A. POSPELOV: *Logičeskie metody analiza i sinteza shem.* Izd. 2-e Moskva, 1968.

8. V. I. VARŠAVSKIJ, L. Ya. ROZENBLJUM: *O minimizacii piramidaljnyh shem iz mažoritarnyh elementov.* Izvestija AN SSSR, Tehničeskaja kibernetika, No 3, 1964, str. 24—29.

9. V. AMAR, N. COLDULMARI: *Diagnosis of large combinational networks.* IEEE Trans. Electronic Computers, EC-**16** (1967), 675—680.

10. Ž. TOŠIĆ: *Arifmetičeskie predstavlenija logičeskih fuukcij.* Sb. „Diskretnye avtomaty i seti svjazi", Moskva 1970, s. 131—136.

11. C. E. SHANNON: *A symbolic analysis of relay and switcqing circuits.* Trans. AIEE, **57** (1938), 713—722.

12. M. COHN: *Switching function canonical forms over integer fields.* Ph. D. Dissertation, Harvard University, Cambridge, Mass., Theory of switching, Rept. BL-**27**, Dec. 1960.

13. A. HAUSENBLAS: *Schaltungssynthese mit Koinzidenz-nnd Antivalenzgattern.* Elektron. Rechenanlagen **4** (1962), 217—221.

14. G. N. POVAROV: *Matematičeskaja teorija sinteza kontaktnyh (l, k) — poljusnikov.* Dokl. AN SSSR **100** (1955), 909—912.

15. Ž. TOŠIĆ: *Matričnyj zposob opredelenija proizvodnyh v bulevoj algebre.* Sb. „Doklady NTK po itogam NIR za 1968—169 gg. Podsekcija VT". Mosk. energ. in-*t*, Moskva 1970, s. 96—100.

16. I. I. ŽEGALKIN: *O tehnike vyčislenija predloženij v simvoličeskoj logike.* Matem. sbornik **34** (1927), 9—28.

17. A. P. MIŠINA, I. V. PROSKURJAKOV: *Vysšaja algebra (linejnaja algebra, mnogočleny, obščaja algebra).* Moskva, 1962.

18. H. R. MULLER: *Algebraischen Aussagenkalkul.* Akad.. Wien, S. — B. IIa, **149** (1940), 77—115.

19. M. J. GAZALE: *Les structures de communication a m valeurs et les calculatrices numeriques.* Paris, 1959.

20. P. CALINGAERT: *Switching function canonical forms based on comutative and associative binary operations.* Trans. AIEE, **80** (1961), 808—814.

21. R. J. LESHNER: *Transformations among switching function canonical forms.* IEEE Trans. Electronic Computers, EC-**12** (1963), 129—130.

22. M. COHN: *Inconsistent canonical forms of switching functions.* IEEE Trans. Electronic Computers, EC-**11** (1962), 284—285.

23. Ž. TOŠIĆ: *Polinomialjnye predstavlenija bulevyh funkcij i ih minimizacija.* Izv. AN SSSR, Tehn. kibernetika, No **3**, 1967, 141—143.

24. D. A. POSPELOV: *Ob odnoj postanovke zadači minimizacii v mnogoznačnyh logikah.* Sb. „Mnogoznačnye elementy i struktury", Moskva, 1967, s. 112—114.

25. G. E. CEJTLIN: *Realizacija bulevyh funkcij v algebre s sistemoj operacij*: „·", „—", „+" *mod 2*". Sb. „Teorija avtomatov. Trudy seminara", No **3**, 1966, s. 84—92.

26. S. EVEN, et al.: *On minima i modulo 2 sums of products for switching functions.* IEEE Trans. Electronic Computers, EC-**16** (1967), 671—674.

27. A. MUKHOPADHYAY, G. SCHMITZ: *Minimization of exclusive or and logical equivalence switching functions.* IEEE Trans. Computers, C-**19** (1970), 132—140.

28. D. E. MULLER: *Application of Boolean algebra to switching circuit design and to error detection.* IRE Trans. Electronic Computers, EC-**3** (1954), pp. 6—12.

29. C. V. RAMAMOORTHY: *Procedures for minimization of „exclusive-or" and „logical-equivalence" switching circuits.* 6 th IEEE Annual Symp. on Switching Circuit Theory and Logical Design, Oct. 1965, pp. 143—149.

30. V. Y. SHEN, A. C. MCKELLER: *An algorithm for the disjunctive decomposition of switching functions.* IEEE Trans. Computers, C-**19** (1970), 239—248.

31. J. WALLACH: *Bemerkungen zur Schaltunssynthese mit Koinzidenz und Antivalenzgattern* Elektron. Rechenan. **7** (1965), 307—309.

32. B. P. DEMIDOVIČ, I. A. MARON: *Osnovy vyčisliteljnoj matematiki,* izd. 2-e. Moskva, 1963.

33. P. L. HAMMER (Ivanescu), S. RUDEANU: *Boolean methods in operation research and related areas.* Berlin, 1968.

34. P. L. IVANESCU, S. RUDEANU: *Pseudo-Boolean methods for bivalent programming.* Berlin, 1966.

35. O. LOWENSCHUSS: *Non-binary switching theory.* IRE Natl. Conv. Record **6** (1958), No 4, pp. 305—317.

36. P. E. WOOD: *Switching Theory.* New York, 1968.

37. W. E. PETERSON: *Error correcting codes.* New York, 1961.

38. L. F. BORODIN: *Vvedenie v teoriju pomehoustojčivogo kodirovanija.* Moskva, 1960.

39. C. W. GOLOMB: *Shift register sequences.* San Francisko, 1967.

40. *Linear sequential switching circuits.* Ed. by W. K. HAUTZ. San Francisko, 1965.

41. T. C. BARTEE, D. I. SCHEIDER: *Computation with finite fields.* Information and Control **6** (1963), pp. 79—98.

42. A. GILL, L. P. JACOB: *On a mapping polynomials for Galois fields.* Quart. Appl. Math. **24** (1966), 57—62.

43. M. STOJAKOVIČ: *Obraščenie matric, vstrečajuščihsja v teorii sinteza relejnyh kontaktnyh shem.* Žurnal vyčisl. matematiki i matematičeskoj fiziki **6** (1966), 158—161.

44. H. L. ALTHAUS, R. J. LEAKE: *Inverse of a finite-field Vandermonde matrix,* IEEE Trans. Inform. Theory IT-**15** (1969), Pt. 1, p. 173.

45. K. S. MENGER: *A transform for logic networks.* IEEE Trans. Computers, C-**18** (1969), 241—250.

46. M. COHN: *Canonical forms of functions in p-valued logics.* Proc. 2 nd Annual Symp. on Switching Circuit Theory and Logical Design. AIEE Publ. No S-**134**, New York, 1961, pp. 169—177.

47. D. S. MITRINOVIĆ, D. Ž. DJOKOVIĆ: *Polinomi i matrice.* Beograd, 1966.

48. B. P. DEMIDOVIČ, I. A. MARON, E. Z. ŠUVALOVA: *Čislennye metody analiza,* izd. 2-e. Moskva, 1963.

49. I. M. VINOGRADOV: *Osnovy teorii čisel,* izd. 7-e. Moskva, 1965.

50. C. JORDAN: *Sur le nombre des solutions de la congruence* $|a_{ik}| \equiv A \pmod m$. J. Math. Pure Appl. (6) **7** (1911), 409—416.

51. N. J. FINE, I. NIVEN: *The probability that a determinant be congruent to a (mod m).* Bull. Am. Math. Sos. **50** (1944), 89—93.

52. Ž. TOŠIĆ: *Polinomialnye preostavlenija m-značnyh logičeskih funkcij.* Publikacije El.-tehn. Fakulteta Univerziteta u Beogradu ser. matem. i fizika, No 302—319, 1970, s. 43—48.

53. B. A. BERNSTEIN: *Modular representations of finite algebras.* Proc. Intern. Math. Congress, Toronto, 1924, vol. 1. Univ. of Toronto Press, 1928, pp. 207—216.

54. S. V. YABLONSKIJ: *Funkcional'nye postroenija v k-značnoj logike.* Trudy matem. in-ta im Steklova, **51** (1958), s. 5—142.

55. A. J. KEMPNER: *Polynomials and their residue systems.* Trans. Amer. Math. Sos., **22** (1921), pp. 240—288.

56. L. E. DICKSON: *Introduction to the theory of numbers.* Chicago, 1929.

57. V. G. KIRIN: *On the polynomial representation of operations in the n-valued propositional calculi.* Glasnik mat.-fiz. i astronomski, **18** (1963), No 1—2, pp. 3—12.

58. D. A. SINGMASTER: *A maximal generalization of Fermat's theorem.* Math. Mag., **39** (1966), No 2, pp. 102—107.

59. H. J. S. SMITH: *On systems of linear independente equations and congruences.* Phil. Trans. Royal Sos. London, pt. 1 (1861), pp. 293—326.

60. H. J. S. SMITH: *On the arithmetical invariants of a rectangular matrix of which the consituents are integral numbers.* Proc. London Math. Soc., **4** (1871—1873), pp, 236—253.

61. L. CARLITZ: *Functions and polynomials (mod p^n).* Acta arithmetica, **9** (1964), No 9, pp. 67—78.

62. N. N. AJZENBERG, I. V. SEMJON, A. I. CITKIN: *Polynomial'nye predstavlenija funkcij k-značnoj logiki.* Avtomatika i vyčislitel'naja tehnika, No 2, 1971, pp. 6—13.

63. N. N. AJZENBERG: *O predstavlenii funkcij k-značnoj logiki polinomami po mod k* Kibernetika, No 2, 1968, s. 102.

64. D. A. POSPELOV, Ž. TOŠIĆ: *Polinomial'nye predstavlenija v mnogoznačnyh logikah.* Sb. „Mnogoznačnye elemeny i struktury" Moskva, 1967, pp. 115—121.

65. Ž. TOŠIĆ: *Polinomial'nye predstavlenija v odnom klasse trehznačnyh logik.* Izv. AN SSSR, Tehn. Kibernetika, No 2, 1967, 114—118.

66. D. A. POSPELOV, Ž. TOŠIĆ: *Polininomial'nye predstnvlenija v mnogoznačnyh logikah.* Sb. „Sintez diskretnyh avtomatov i upravljajuščih ustrojstv" Moskva, 1968, s. 132—139.

67. YU. L. IVAS'KIV, D. A. POSPELOV, Ž. TOŠIĆ: *Predstavlenija v mnogoznačnyh logikah* Kibernetika, No 2, 1969, s. 35—42.

68. O. ZARISKI, P. SAMUEL: *Commutative algebra,* vol. 1, Princeton, 1958.

69. Z. L. RABINOVIČ: *Voprosy postroenija vyčislitelnyh mašin na elementah s mnogoznačym strukturnym alfavitom.* Sb. „Mnogozračnye elementy i struktury". Moskva, 1967, s. 80—93.

70. N. N. AJZENBERG, Z. L. RABINOVIČ: *Nekotorye klassy funkcional'no polnyh sistem operacij i kanoničeskie formy predstavlenija funkcij mnogoznačnoj logiki.* Kibernetika, No 2, 1965, s. 37—45.

CONTENTS