Ashdin Publishing
Journal of Generalized Lie Theory and Applications
Vol. 4 (2010), Article ID G100301, 8 pages
doi:10.4303/jglta/G100301

Polynomial k-ary operations, matrices, and k-mappings

G. BELYAVSKAYA

Institute of Mathematics and Computer Science, Academy of Sciences of Moldova
Academiei str. 5, Chishinau MD-2028, Republic of Moldova
E-mail: gbel1@rambler.ru

Abstract

We establish connection between product of two matrices of order $k \times k$ over a field and the product of the k-mappings corresponding to the k-operations, defined by these matrices. It is proved that, in contrast to the binary case, for arity $k \geq 3$ the components of the k-permutation inverse to a k-permutation, all components of which are polynomial k-quasigroups, are not necessarily k-quasigroups although are invertible at least in two places. Some transformations with the help of permutations of orthogonal systems of polynomial k-operations over a field are considered.

2000 MSC: 20N05, 20N15, 05B15

1 Introduction

It is known that polynomial k-ary operations (shortly, polynomial k-operations), that is, the operations of the form $A(x_1, x_2, \ldots, x_k) = a_1x_1 + a_2x_2 + \cdots + a_kx_k$ over a field and systems of $t \geq k$ of such operations are used in different applications, in particular in coding theory and cryptography. If $t = k$, then we have a matrix $A = (a_{ij})$ of order $k \times k$. However, any k-tuple $(A_1, A_2, \ldots, A_k)$ of k-operations given on a set Q defines some mapping $\bar{\theta}$ of the set Q^k into Q^k (shortly, a k-mapping):

$$\bar{\theta}\big(x_1, x_2, \ldots, x_k\big) = \big(A_1\big(x_1, x_2, \ldots, x_k\big), A_2\big(x_1, x_2, \ldots, x_k\big), \ldots, A_k\big(x_1, x_2, \ldots, x_k\big)\big),$$

and conversely, any mapping of a set Q^k into Q^k defines some k-tuple of k-operations [1].

We establish connection between product of two matrices of order $k \times k$ over a field and the product of the k-mappings corresponding to the k-operations, defined by these matrices. As a corollary, we obtain that the inverse matrix A^{-1} to a nonsingular matrix A is defined by the components of the k-permutation (that is the bijective k-mapping) $\bar{\theta}^{-1}$ inverse to the k-permutation $\bar{\theta}$ with the components which are polynomial k-operations, defined by the matrix A.

In [2], Belousov proved that if A and B are binary quasigroups given on a set Q such that (A, B) is a permutation of Q^2, then the operations C and D, where $(C, D) = (A, B)^{-1}$, are quasigroups as well. We prove that, in contrast to the binary case, for arity $k \geq 3$ the components of the k-permutation inverse to a k-permutation, all components of which are polynomial k-quasigroups, are not necessarily k-quasigroups although are invertible at least in two places.

In different applications, using orthogonal systems of operations, quasigroups, Latin squares, or hypercubes, especially by coding and ciphering of information, necessity to obtain

distinct orthogonal systems of operations from one orthogonal system is arisen. In the theory of binary and k-ary operations, some transformations of orthogonal systems of operations (which lead to orthogonal systems) with the help of permutations are known. These transformations we use for the most known and often used orthogonal systems of polynomial k-operations (in particular, of polynomial k-quasigroups) over a field.

2 Preliminaries

Recall some necessary designations, definitions, and results.

Let Q be a finite or an infinite set, let $k \geq 2$ be a positive integer, and let Q^k denote the kth Cartesian power of Q.

A k-groupoid (Q, A) is a set Q with one k-ary operation A defined on Q.

A k-operation B given on a set Q is called *isotopic* to a k-operation A if there exists a $(k+1)$-tuple of permutations $T = (\alpha_1, \alpha_2, \ldots, \alpha_k, \alpha_{k+1})$ of Q such that $B(x_1^k) = \alpha_{k+1}^{-1} A(\alpha_1 x_1, \alpha_2 x_2, \ldots, \alpha_k x_k)$, where $(x_1^k) = (x_1, x_2, \ldots, x_k)$, shortly $B = A^T$.

A *k-ary quasigroup (or a k-quasigroup)* is a k-groupoid (Q, A), such that in the equality $A(x_1^k) = x_{k+1}$, each set of k elements from x_1^{k+1} uniquely defines the $(k+1)$th element. Sometimes a quasigroup k-operation A is itself considered as a k-quasigroup.

An i-invertible k-operation A defined on Q is a k-operation for which the equation:

$$A\big(a_1^{i-1}, x, a_{i+1}^k\big) = a_{k+1}$$

has a unique solution for each fixed k-tuple $(a_1^{i-1}, a_{i+1}^k, a_{k+1})$ of Q^k.

So *a k-ary quasigroup* (or simply, a k-quasigroup) is a k-groupoid (Q, A), such that the k-operation A is i-invertible for each $i = 1, 2, \ldots, k$ (briefly, $i \in \overline{1,k}$).

The k-operation E_i, $1 \leq i \leq k$, on Q with $E_i(x_1^k) = x_i$ is called *the ith identity operation (or the ith selector) of arity k.*

Recall also the following information of [1] (for the case $k = 2$ see [2]).

Let $(A_1, A_2, \ldots, A_k)$ (briefly, (A_1^k)) be a k-tuple of k-operations defined on a set Q. This k-tuple defines the unique mapping $\bar{\theta} : Q^k \to Q^k$ in the following way:

$$\bar{\theta} : \big(x_1^k\big) \longrightarrow \big(A_1\big(x_1^k\big), A_2\big(x_1^k\big), \ldots, A_k\big(x_1^k\big)\big),$$

(briefly, $\bar{\theta} : (x_1^k) \to (A_1^k)(x_1^k)$ or $\bar{\theta} = (A_1, A_2, \ldots, A_k)$). These mappings we will call *k-mappings*.

Conversely, any mapping Q^k into Q^k uniquely defines a k-tuple (A_1^k) of k-operations on Q: if $\bar{\theta}(x_1^k) = (y_1^k)$, then we define $A_i(x_1^k) = y_i$ for all $i \in \overline{1,k}$. Thus, we obtain the following:

$\bar{\theta} = (A_1^k)$ where $\bar{\theta}(x_1^k) = (A_1^k)(x_1^k) = (A_1^k(x_1^k))$.

If C is a k-operation on Q and $\bar{\theta}$ is a mapping of Q^k into Q^k, then the operation $C\bar{\theta}$ defined by the equality $C\bar{\theta}(x_1^k) = C(\bar{\theta}(x_1^k))$ is also a k-operation. Let $C\bar{\theta} = D$ and $\bar{\theta} = (A_1^k)$, then $D(x_1^k) = C(A_1^k(x_1^k))$ or briefly, $D = C(A_1^k)$. If $\bar{\theta} = (B_1^k)$ and $\bar{\varphi} = (A_1^k)$ are mappings of Q^k into Q^k, then according to [1]:

$$\bar{\varphi}\bar{\theta} = \big(A_1^k\big)\bar{\theta} = \big(A_i\bar{\theta}\big)_{i=1}^k = \big(A_1\bar{\theta}, A_2\bar{\theta}, \ldots, A_k\bar{\theta}\big) = \big(A_1\big(B_1^k\big), A_2\big(B_1^k\big), \ldots, A_k\big(B_1^k\big)\big).$$

If $\bar{\theta} = (B_1^k)$ is a permutation of Q^k, then $B_i = E_i\bar{\theta}$ and $B_i\bar{\theta}^{-1} = B_i(B_1^k)^{-1} = E_i$, $i \in \overline{1,k}$.

Definition 2.1 [1]**.** A k-tuple (A_1^k) of (different) k-operations given on a set Q is called orthogonal if the system $\{A_i(x_1^k) = a_i\}_{i=1}^k$ has a unique solution for all $a_1^k \in Q^k$.

The k-tuple $(E_1^k) = (E_1, E_2, \dots, E_k)$ of the selectors of arity k is the identity permutation of Q^k and is orthogonal.

There is a close connection between orthogonal k-tuples of k-operations given on a set Q and permutations of Q^k (such permutations we will call *k-permutations*) by virtue of the following

Proposition 2.2 [1]**.** *A k-tuple (A_1^k) of k-operations defined on a set Q is orthogonal if and only if the mapping $\bar{\theta} = (A_1^k)$ is a permutation of Q^k.*

Definition 2.3 [1]**.** A system $\Sigma = \{A_1, A_2, \dots, A_t\} = \{A_1^t\}$, $t \geq k$, of k-operations is called orthogonal if any k-tuple of k-operations of Σ is orthogonal.

Definition 2.4 [1]**.** A system $\Sigma = \{A_1, A_2, \dots, A_t\}$, $t \geq 1$, of k-operations, given on a set Q, is called strongly orthogonal if the system $\bar{\Sigma} = \{E_1^k, A_1^t\}$ is orthogonal.

In a strongly orthogonal system $\Sigma = \{A_1^t\}$, all k-operations A_i, $i \in \overline{1,t}$, of Σ are k-quasigroups since a k-operation A is i-invertible if and only if the mapping $(E_1, E_2, \dots, E_{i-1}, A, E_{i+1}, \dots, E_k)$ is a k-permutation. So the system $\bar{\Sigma}$ is called *an orthogonal system of k-quasigroups (a k-OSQ)* [1].

A k-operation A is a k-quasigroup if and only if the set $\Sigma = \{A\}$ is strongly orthogonal. A set $\Sigma = \{A_1^t\}$ of k-quasigroups when $k > 2$, $t \geq k$, can be orthogonal but not strongly orthogonal in contrast to the binary case ($k = 2$) [1].

Note that in the case of a strongly orthogonal set $\Sigma = \{A_1, A_2, \dots, A_t\}$ of k-operations, the number t of k-operations in Σ can be less than arity k.

3 Product of $(k \times k)$-matrices and product of k-mappings

Consider k-operations of a special kind (*polynomial k-operations*), that is k-operations of the form $A(x_1^k) = a_1x_1 + a_2x_2 + \dots + a_kx_k$ over a field.

A polynomial k-operation is a polynomial k-quasigroup if and only if $a_i \neq 0$ for all $i \in \overline{1,k}$.

If a k-operation B is isotopic to a polynomial k-operation $A(x_1^k) = a_1x_1 + a_2x_2 + \dots + a_kx_k$, that is $B = A^T$, where $T = (\alpha_1, \alpha_2, \dots, \alpha_k, \alpha_{k+1})$, then

$$B(x_1^k) = \alpha_{k+1}^{-1}(a_1\alpha_1x_1 + a_2\alpha_2x_2 + \dots + a_k\alpha_kx_k).$$

Note that the selectors E_i of arity k can be also considered as polynomial k-operations over a field:

$E_i(x_1^k) = a_1x_1 + a_2x_2 + \dots + a_ix_i + \dots + a_kx_k$, where $a_i = 1$, $a_j = 0$, $j \neq i$.

Let a set $\Sigma = \{A_1, A_2, \dots, A_t\}$, $k \geq 2$, $t \geq k$, be a set of k-operations each of which is a polynomial k-operation over a field, that is

$$\begin{aligned} A_1(x_1^k) &= a_{11}x_1 + a_{12}x_2 + \dots + a_{1k}x_k, \\ A_2(x_1^k) &= a_{21}x_1 + a_{22}x_2 + \dots + a_{2k}x_k, \\ &\vdots \\ A_t(x_1^k) &= a_{t1}x_1 + a_{t2}x_2 + \dots + a_{tk}x_k. \end{aligned} \tag{3.1}$$

These polynomial operations define corresponding rows of the $(t \times k)$-matrix A. It is easy to see from Definition 2.1 that the following statement is valid, where a k-minor is the determinant of a $(k \times k)$-subarray of a matrix A.

Proposition 3.1 [3]. *A system $\Sigma = \{A_1^t\}$, $k \geq 2$, $t \geq k$, of polynomial k-operations of (3.1) is orthogonal if and only if all k-minors of the matrix A defined by these k-operations are different from* 0.

Let in (3.1) $t = k$, $A = (a_{ij})$, $i, j \in \overline{1,k}$, be the $(k \times k)$-matrix the rows of which are defined by the k-operations $A_1, A_2, \ldots, A_k$ and $\bar{\theta}_A = (A_1, A_2, \ldots, A_k)$. It is clear that the mapping $\bar{\theta}_A$ is a k-permutation if and only if the matrix A is nonsingular.

The following statement establishes a connection between product of matrices and product of k-mappings.

Theorem 3.2. *Let A and B be $(k \times k)$-matrices over a field, $\bar{\theta}_A = (A_1, A_2, \ldots, A_k)$, let $\bar{\theta}_B = (B_1, B_2, \ldots, B_k)$ be the k-mappings defined by the polynomial k-operations corresponding to the rows of these matrices, $\bar{\theta}_A\bar{\theta}_B = (C_1, C_2, \ldots, C_k)$. Then the k-operations $C_1, C_2, \ldots, C_k$ are polynomial and define the matrix $C = AB$, that is $\bar{\theta}_A\bar{\theta}_B = \bar{\theta}_{AB}$.*

Proof. Let $\bar{\theta}_A\bar{\theta}_B = (A_1, A_2, \ldots, A_k)(B_1, B_2, \ldots, B_k) = (C_1, C_2, \ldots, C_k)$, $i \in \overline{1,k}$, then by the definition,

$$\begin{aligned}
C_i(x_1^k) &= A_i\bar{\theta}_B(x_1^k) = A_i\big(B_1, B_2, \ldots, B_k\big)\big(x_1^k\big) = A_i\big(B_1\big(x_1^k\big), B_2\big(x_1^k\big), \ldots, B_k\big(x_1^k\big)\big) \\
&= a_{i1}\big(b_{11}x_1 + b_{12}x_2 + \cdots + b_{1k}x_k\big) + a_{i2}\big(b_{21}x_1 + b_{22}x_2 + \cdots + b_{2k}x_k\big) \\
&\quad + \cdots + a_{ik}\big(b_{k1}x_1 + b_{k2}x_2 + \cdots + b_{kk}x_k\big) \\
&= \big(a_{i1}b_{11} + a_{i2}b_{21} + \cdots + a_{ik}b_{k1}\big)x_1 + \big(a_{i1}b_{12} + a_{i2}b_{22} + \cdots + a_{ik}b_{k2}\big)x_2 \\
&\quad + \cdots + \big(a_{i1}b_{1k} + a_{i2}b_{2k} + \cdots + a_{ik}b_{kk}\big)x_k \\
&= c_{i1}x_1 + c_{i2}x_2 + \cdots + c_{ik}x_k,
\end{aligned}$$

where $c_{il} = a_{i1}b_{1l} + a_{i2}b_{2l} + \cdots + a_{ik}b_{kl}$, $l \in \overline{1,k}$.

It means that $C_i = A_i\bar{\theta}_B$ is the polynomial k-operation defined by the ith row of the matrix AB, so $C = AB$. □

Theorem 3.2 can be formulated otherwise.

Corollary 3.3. *Let $A_1, A_2, \ldots, A_k$ and $B_1, B_2, \ldots, B_k$ be polynomial k-operations over a field, $\bar{\theta}_B = (B_1, B_2, \ldots, B_k)$, then the k-operations $A_1\bar{\theta}_B, A_2\bar{\theta}_B, \ldots, A_k\bar{\theta}_B$ are polynomial, and the matrix AB is the coefficient matrix for them.*

Corollary 3.4. *Let $\bar{\theta}_A = (A_1, A_2, \ldots, A_k)$, where A is a nonsingular matrix, and the matrix A^{-1} is inverse to A. Then $\bar{\theta}_A$ is a k-permutation and $\bar{\theta}_A^{-1} = \bar{\theta}_{A^{-1}}$.*

Proof. Let $(B_1, B_2, \ldots, B_k) = \bar{\theta}_{A^{-1}}$. Show that $\bar{\theta}_A\bar{\theta}_{A^{-1}}$ is the identity permutation of Q^k, that is $(A_1, A_2, \ldots, A_k)(B_1, B_2, \ldots, B_k) = (E_1, E_2, \ldots, E_k)$. Let

$$A_i\big(x_1^k\big) = a_{i1}x_1 + a_{i2}x_2 + \cdots + a_{ik}x_k, B_i\big(x_1^k\big) = b_{i1}x_1 + b_{i2}x_2 + \cdots + b_{ik}x_k.$$

Then as it follows from the proof of Theorem 3.2 in the k-operation $A_i(B_1, B_2, \ldots, B_k)$ the multipliers by x_j, $j \neq i$, are equal to 0, and the multiplier $(a_{i1}b_{1i} + a_{i2}b_{2i} + \cdots + a_{ik}b_{ki})$ by x_i is equal 1, since the operations $B_1, B_2, \ldots, B_k$ are defined by the matrix A^{-1}. It means that $A_i(B_1, B_2, \ldots, B_k) = E_i$, $i \in \overline{1,k}$, but k-selectors $E_1, E_2, \ldots, E_k$ define the rows of the identity matrix of order $k \times k$ the rows of which correspond to the selectors $E_1, E_2, \ldots, E_k$. Hence, $\bar{\theta}_A\bar{\theta}_{A^{-1}} = (A_1, A_2, \ldots, A_k)(B_1, B_2, \ldots, B_k) = (E_1, E_2, \ldots, E_k)$, so $\bar{\theta}_A^{-1} = \bar{\theta}_{A^{-1}}$. □

Corollary 3.4 at once implies.

Corollary 3.5. *If A is a nonsingular $(k \times k)$-matrix and $A_1, A_2, \ldots, A_k$ are the polynomial operations defined by the rows of A, respectively, then $\bar{\theta} = (A_1, A_2, \ldots, A_k)$ is a k-permutation, and the permutation $\bar{\theta}^{-1} = (B_1, B_2, \ldots, B_k)$ defines the polynomial operations corresponding to the rows of the matrix A^{-1} inverse to A.*

It is known that if A and B are orthogonal binary quasigroups given on a set Q, that is (A, B) is a permutation of Q^2, then the operations C and D, where $(C, D) = (A, B)^{-1}$, are quasigroups as well (see [2, Lemma 3]). Taking into account this fact and Corollary 3.5, we obtain that if in a nonsingular matrix A of order 2×2 there is no the element 0, then in the inverse matrix A^{-1} the element 0 absents also. Below we will show that in the case of arity $k \geq 3$ this statement in general is not true.

The following statement is valid for a k-permutation $(A_1, A_2, \ldots, A_k)$ all components A_i, $i \in \overline{1,k}$, of which are polynomial k-ary quasigroups over a field.

Theorem 3.6. *If all polynomial k-operations $A_1, A_2, \ldots, A_k$ over a field are k-quasigroups, $\bar{\theta} = (A_1, A_2, \ldots, A_k)$ is a k-permutation and $\bar{\theta}^{-1} = (B_1, B_2, \ldots, B_k)$, then each k-operation of $B_1, B_2, \ldots, B_k$ is invertible at least in two places.*

Proof. A polynomial k-operation A_i: $A_i(x_1^k) = a_{i1}x_1 + a_{i2}x_2 + \cdots + a_{ik}x_k$, $i \in \overline{1,k}$, is a k-quasigroup if and only if all coefficients a_{ij}, $j \in \overline{1,k}$, are distinct from 0. Since $(B_1, B_2, \ldots, B_k)(A_1, A_2, \ldots, A_k) = (E_1, E_2, \ldots, E_k)$, then $(b_{i1}a_{1i} + b_{i2}a_{2i} + \cdots + b_{ik}a_{ki}) = 1$ for any $i \in \overline{1,k}$ and $(b_{j1}a_{1i} + b_{j2}a_{2i} + \cdots + b_{jk}a_{ki}) = 0$ for all $j \neq i$ (see the proof of Corollary 3.4). By Corollary 3.5, all elements of the jth row of the matrix $A^{-1} = B$ cannot simultaneously be equal to 0 as the matrix $A^{-1} = B$ is nonsingular (by the conditions of the theorem $\bar{\theta}$ is a k-permutation).

If $k-1$ of the coefficients $b_{j1}, b_{j2}, \ldots, b_{jk}$ is equal 0, then the last coefficient is also equal 0. Thus, there exist at least two elements which are not equal 0 in every row $j \neq i$ of the matrix B and the k-operation B_j, corresponding to it is invertible at least in two places. Changing i, $i \in \overline{1,k}$, we obtain that the statement is true for any k-operations of $B_1, B_2, \ldots, B_k$. □

Using the matrices corresponding to the k-permutations of Theorem 3.6 we obtain the following corollary.

Corollary 3.7. *If a nonsingular $(k \times k)$-matrix A has not zero elements, then every row (every column) of the matrix A^{-1} contains at least two nonzero elements.*

Proof. This statement for rows follows from Corollary 3.5 and Theorem 3.6. The statement with respect to columns we can obtain from the proof of Theorem 3.6 considering the product $(A_1, A_2, \ldots, A_k)(B_1, B_2, \ldots, B_k) = (E_1, E_2, \ldots, E_k)$, the elements $a_{i1}b_{1j} + a_{i2}b_{2j} + \cdots + a_{ik}b_{kj} = 0$, $j \neq i$, and reasoning similarly. □

Below we will show that the result of Belousov for the binary case, in general, is not true with respect to arity $k > 2$ (i.e., the result of Theorem 3.6 for $k > 2$, in general, is not improved) constructing the following two counterexamples of k-permutations for ternary case.

Consider three ternary polynomial operations over the field GF(7):

$$A_1(x, y, z) = x + y + z, \quad A_2(x, y, z) = x + y + 2z, \quad A_3(x, y, z) = x + 3y + 3z,$$

and three operations:

$$B_1(x, y, z) = x + 2y + 4z, \quad B_2(x, y, z) = x + 3y + 2z, \quad B_3(x, y, z) = x + 4y + 2z.$$

The following nonsingular (3×3)-matrices A, A^{-1} (B, B^{-1}) correspond to these ternary operations:

$$A = \begin{pmatrix} 1 & 1 & 1 \\ 1 & 1 & 2 \\ 1 & 3 & 3 \end{pmatrix}, \quad A^{-1} = \begin{pmatrix} 5 & 0 & 3 \\ 4 & 6 & 4 \\ 6 & 1 & 0 \end{pmatrix}, \quad B = \begin{pmatrix} 1 & 2 & 4 \\ 1 & 3 & 2 \\ 1 & 4 & 2 \end{pmatrix}, \quad B^{-1} = \begin{pmatrix} 6 & 6 & 3 \\ 0 & 6 & 1 \\ 4 & 6 & 4 \end{pmatrix}.$$

The inverse matrix $C = A^{-1}$ $(D = B^{-1})$ defines the following 3 operations: $C_1(x, y, z) = 5x + 0y + 3z$, $C_2(x, y, z) = 4x + 6y + 4z$, $C_3(x, y, z) = 6x + y + 0z$ $(D_1(x, y, z) = 6x + 6y + 3z$, $D_2(x, y, z) = 0x + 6y + z$, $D_3(x, y, z) = 4x + 6y + 4z)$. The k-operations C_1, C_3, D_2 are not 3-quasigroups, but every from them is invertible in two places. The permutation $\bar{\theta}_C = (C_1, C_2, C_3)$ $(\bar{\theta}_D = (D_1, D_2, D_3))$, not all components of which are 3-quasigroups, is inverse to the 3-permutations $\bar{\theta}_A = (A_1, A_2, A_3)$ $(\bar{\theta}_B = (B_1, B_2, B_3))$ with quasigroup components.

4 Transformations of orthogonal systems of polynomial k-operations

Now we recall some necessary information from [1] with respect to transformations of orthogonal systems of k-operations (k-OSOs) (for the case $k = 2$ see [2]).

Two k-OSOs Σ and Σ' given on a set Q are called *conjugate* if there exists a permutation $\bar{\theta}$ of Q^k such that $\Sigma' = \Sigma\bar{\theta}$, and a k-OSO Σ' is called *parastrophic* to Σ if $\Sigma' = \Sigma\bar{\theta}^{-1}$, where $\bar{\theta} = (A_{i_1}, A_{i_2}, \ldots, A_{i_k})$, $A_{i_j} \in \Sigma$ for any $j \in \overline{1,k}$. In this case,

$$\Sigma' = \Sigma\bar{\theta}^{-1} = \big\{E_1, E_2, \ldots, E_k, A_i\bar{\theta}^{-1} \mid i \in \overline{1,t},\ i \neq i_j,\ j \in \overline{1,k}\big\}.$$

By [1, Theorem 1], every k-OSO is conjugate to a k-OSQ, and by [1, Lemma 3], two k-OSQs are conjugate if and only if they are parastrophic.

Two orthogonal systems of k-operations Σ and Σ' given on a set Q are called *isotopic*, if $\Sigma' = (\Sigma)^T = \{\alpha_1 A_1, \alpha_2 A_2, \ldots, \alpha_t A_t\}$, $A_i \in \Sigma$, where $T = (\alpha_1, \alpha_2, \ldots, \alpha_t)$ is a tuple of permutations of the set Q.

The transformation $\Sigma \to (\Sigma\bar{\theta})^T = \Sigma'$ is called *isostrophy*.

Remark 4.1. Note that if a k-OSO $\Sigma = \{A_1^t\}$ of k-operations on a set Q is strongly orthogonal (i.e. the system $\bar{\Sigma} = \{E_1^k, A_1^t\}$ is orthogonal), and $T = (\alpha_1, \alpha_2, \ldots, \alpha_{t+k})$ is a $(t + k)$-tuple of permutations of Q, then $(\bar{\Sigma})^T = \{\alpha_1 E_1, \alpha_2 E_2, \ldots, \alpha_k E_k, B_1, B_2, \ldots, B_t\}$, where $B_j = \alpha_{k+j} A_j$, $j \in \overline{1,t}$, are k-quasigroups.

According to [1], the equality $(\Sigma\bar{\theta})^T = (\Sigma^T)\bar{\theta}$ is true, that is if $B_i \in \Sigma' = (\Sigma\bar{\theta})^T$, $i \in \overline{1,t}$, then,

$$B_i\big(x_1^k\big) = \big(\alpha_i\big(A_i\bar{\theta}\big)\big)\big(x_1^k\big) = \big(\alpha_i A_i\big)\bar{\theta}\big(x_1^k\big). \tag{4.1}$$

In addition, we consider the following case of the transformation of isostrophy of a k-OSO, namely, $\Sigma' = (\Sigma\bar{\theta}_1)^T$, where $\bar{\theta}_1 = \bar{\theta}\bar{\theta}_0$, $\bar{\theta}_0 = (\beta_1 E_1, \beta_2 E_2, \ldots, \beta_k E_k)$, $\beta_1, \beta_2, \ldots, \beta_k$ are permutations of Q, that is $\bar{\theta}_0(x_1^k) = (\beta_1 E_1, \beta_2 E_2, \ldots, \beta_k E_k)(x_1^k) = (\beta_1 x_1, \beta_2 x_2, \ldots, \beta_k x_k)$.

In this case if $B_i \in \Sigma'$, then from (4.1), we have

$$B_i\big(x_1^k\big) = \big(\alpha_i A_i\big)\bar{\theta}_1\big(x_1^k\big) = \big(\alpha_i A_i\big)\big(\bar{\theta}\bar{\theta}_0\big)\big(x_1^k\big) = \big(\big(\alpha_i A_i\big)\bar{\theta}\big)\bar{\theta}_0\big(x_1^k\big). \tag{4.2}$$

Let $\bar{\theta} = (C_1, C_2, \dots, C_k)$, then $(\bar{\theta}\bar{\theta}_0)(x_1^k) = (C_1, C_2, \dots, C_k)(\beta_1 x_1, \beta_2 x_2, \dots, \beta_k x_k)$ and from (4.2), it follows

$$B_i(x_1^k) = \alpha_i A_i\Big(C_1(\beta_j x_j)_{j=1}^k, C_2(\beta_j x_j)_{j=1}^k, \dots, C_k(\beta_j x_j)_{j=1}^k\Big), \tag{4.3}$$

where $(\beta_j x_j)_{j=1}^k = (\beta_1 x_1, \beta_2 x_2, \dots, \beta_k x_k)$.

Now consider all these transformations for the case of orthogonal systems of polynomial k-ary operations.

Let $A = (a_{ij})$, $i \in \overline{1,t}$, $j \in \overline{1,k}$, be a $(t \times k)$-matrix, let $\Sigma_A = \{A_1, A_2, \dots, A_t\}$ be the orthogonal system of the polynomial k-operations, defined by the corresponding rows of the matrix A (see (3.1)).

Proposition 4.2. *Let $B_i \in (\Sigma_A)^T$, where $T = (\alpha_1, \alpha_2, \dots, \alpha_t)$, α_i, $i \in \overline{1,t}$, are permutations, then,*

$$B_i(x_1^k) = \alpha_i(a_{i1}x_1 + a_{i2}x_2 + \dots + a_{ik}x_k), \quad i \in \overline{1,t}.$$

Indeed, by the definition of isotopic systems, we have

$$B_i(x_1^k) = \alpha_i A_i(x_1^k) = \alpha_i(a_{i1}x_1 + a_{i2}x_2 + \dots + a_{ik}x_k), \quad i \in \overline{1,t}.$$

In this case, the values of the operation A_i are changed according to the permutation α_i, $i \in \overline{1,t}$.

Proposition 4.3. *Let $B_i \in \Sigma_A\bar{\theta}$, where $\bar{\theta} = (C_1, C_2, \dots, C_k)$, then,*

$$B_i(x_1^k) = a_{i1}C_1(x_1^k) + a_{i2}C_2(x_1^k) + \dots + a_{ik}C_k(x_1^k), \quad i \in \overline{1,t}.$$

If the operations C_j, $j \in \overline{1,k}$, are polynomial and define a matrix C, then the operations B_i, $i \in \overline{1,t}$, are polynomial and are defined by the matrix AC.

Indeed, in this case,

$$\begin{aligned} B_i(x_1^k) &= A_i\bar{\theta}(x_1^k) = A_i(C_1, C_2, \dots, C_k)(x_1^k) \\ &= a_{i1}C_1(x_1^k) + a_{i2}C_2(x_1^k) + \dots + a_{ik}C_k(x_1^k), \quad i \in \overline{1,t}. \end{aligned}$$

It is evident that if the operations C_j, $j \in \overline{1,k}$, are polynomial, then the operations B_i, $i \in \overline{1,t}$, are also polynomial. Moreover, in this case, the operation B_i is defined by the ith row of the $(t \times k)$-matrix $B = AC$ (see the form of the operation C_i in the proof of Theorem 3.2 if the matrices B and C change places and $i \in \overline{1,t}$).

Corollary 4.4. *If in Proposition 4.3 $\bar{\theta} = (A_{i_1}, A_{i_2}, \dots, A_{i_k})$, $A_{i_l} \in \Sigma_A$, $l \in \overline{1,k}$, $\bar{\theta}^{-1} = (D_1, D_2, \dots, D_k)$, then $\Sigma_A\bar{\theta}^{-1}$ is an orthogonal system of polynomial k-operations, $B_{i_l} = E_l$, $l \in \overline{1,k}$, and*

$$B_i(x_1^k) = a_{i1}D_1(x_1^k) + a_{i2}D_2(x_1^k) + \dots + a_{ik}D_k(x_1^k), \quad i \in \overline{1,t},\ i \neq i_1, i_2, \dots, i_k$$

are polynomial k-quasigroups.

Proof. By the definition of the transformation of parastrophy, we have $B_{i_l}(x_1^k) = A_{i_l}\bar{\theta}^{-1}(x_1^k) = E_l(x_1^k)$, $l \in \overline{1,k}$, since $(A_{i_1}, A_{i_2}, \dots, A_{i_k})(A_{i_1}, A_{i_2}, \dots, A_{i_k})^{-1} = (E_1, E_2, \dots, E_k)$ and $B_i(x_1^k) = A_i\bar{\theta}^{-1}(x_1^k) = A_i(D_1, D_2, \dots, D_k)(x_1^k) = A_i(D_1(x_1^k), D_2(x_1^k), \dots, D_k(x_1^k)) = a_{i1}D_1(x_1^k) + a_{i2}D_2(x_1^k) + \dots + a_{ik}D_k(x_1^k)$, when $i \in \overline{1,t}$, $i \neq i_1, i_2, \dots, i_k$, but by Corollary 3.4, all components D_i, $i \in \overline{1,k}$ of the permutation $\bar{\theta}^{-1}$ are polynomial k-operations, so all k-operations of $\Sigma_A\bar{\theta}^{-1}$ are also polynomial k-operations. Moreover, in this case, we obtain that the system $\Sigma' = \{B_i \mid i \neq i_1, i_2, \dots, i_k\}$ is strongly orthogonal, and so all k-operations of Σ' are polynomial k-quasigroups. □

Proposition 4.5. *If* $B_i \in (\Sigma_A\bar{\theta}\bar{\theta}_0)^T$, *where* $\bar{\theta} = (C_1, C_2, \dots, C_k)$, $\bar{\theta}_0 = (\beta_1E_1, \beta_2E_2, \dots, \beta_kE_k)$, $T = (\alpha_1, \alpha_2, \dots, \alpha_t)$, *then,*

$$B_i(x_1^k) = \alpha_i\Big(a_{i1}C_1\big(\beta_jx_j\big)_{j=1}^k + a_{i2}C_2\big(\beta_jx_j\big)_{j=1}^k + \dots + a_{ik}C_k\big(\beta_jx_j\big)_{j=1}^k\Big), \quad i \in \overline{1,t}.$$

Indeed, according to (4.3), $B_i(x_1^k) = \alpha_iA_i(C_1(\beta_jx_j)_{j=1}^k, C_2(\beta_jx_j)_{j=1}^k, \dots, C_k(\beta_jx_j)_{j=1}^k) = \alpha_i(a_{i1}C_1(\beta_jx_j)_{j=1}^k + a_{i2}C_2(\beta_jx_j)_{j=1}^k + \dots + a_{ik}C_k(\beta_jx_j)_{j=1}^k)$, $i \in \overline{1,t}$.

Proposition 4.6. *If* $B_i \in (\Sigma_A\bar{\theta}^{-1}\bar{\theta}_0)^T$, *where* $\bar{\theta} = (A_{i_1}, A_{i_2}, \dots, A_{i_k})$, $A_{i_l} \in \Sigma_A$, $l \in \overline{1,k}$, $\bar{\theta}^{-1} = (D_1, D_2, \dots, D_k)$, $\bar{\theta}_0 = (\beta_1E_1, \beta_2E_2, \dots, \beta_kE_k)$, *then* $B_{i_l} = \alpha_{i_l}\beta_lE_l$, $l \in \overline{1,k}$,

$$B_i(x_1^k) = \alpha_i\Big(a_{i1}D_1\big(\beta_jx_j\big)_{j=1}^k + a_{i2}D_2\big(\beta_jx_j\big)_{j=1}^k + \dots + a_{ik}D_k\big(\beta_jx_j\big)_{j=1}^k\Big), \quad i \in \overline{1,t},\ i \neq i_1, i_2, \dots, i_k,$$

moreover, the operations B_i, $i \neq i_1, i_2, \dots, i_k$, *are* k*-quasigroups.*

This statement follows from Corollary 4.4, Proposition 4.5, and Remark 4.1 since

$$\begin{aligned} B_{i_l}(x_1^k) &= \big(\alpha_{i_l}A_{i_l}\bar{\theta}^{-1}\big)\bar{\theta}_0\big(x_1^k\big) = \big(\alpha_{i_l}E_l\big)\bar{\theta}_0\big(x_1^k\big) \\ &= \alpha_{i_l}E_l\big(\beta_jx_j\big)_{j=1}^k = \alpha_{i_l}\beta_lE_l\big(x_1^k\big), \quad l \in \overline{1,k}. \end{aligned}$$

References

[1] A. S. Bektenov and T. Jakubov. Systems of orthogonal n-ary operations (Russian). *Bul. Akad. Štiince RSS Moldova, Ser. Phys.-Math. Sci.*, (1974), 7–14.

[2] V. D. Belousov. Systems of orthogonal operations (Russian). *Mat. Sb. (N.S.)*, **77** (1968), 38–58.

[3] G. Belyavskaya and Gary L. Mullen. Orthogonal hypercubes and n-ary operations. *Quasigroups Related Systems*, **13** (2005), 73–86.

[4] J. Dénes and A. D. Keedwell. *Latin Squares and Their Applications.* Academic Press, New York, 1974.

Received March 11, 2010
Revised April 26, 2010