Quasigroups and Related Systems **22** (2014), 165 – 178

Successively orthogonal systems of k-ary operations

Galina B. Belyavskaya

Abstract. Systems of k-ary operations, $k \geqslant 2$, generalizing orthogonal sets are considered. These systems have the following property: every k successive k-ary operations of the system are orthogonal. We call these systems successively orthogonal, establish some properties, give examples and methods of construction of these systems.

1. Introduction

It is known that k-ary operations correspond to k-dimensional hypercubes, $k \geqslant 2$, which are objects of combinatorial analysis. A binary quasigroup is an algebraic equivalent of a Latin square and a k-ary quasigroup respects to a permutation cube of the dimension k (cf. [6]). The algebraic approach is useful for research of such combinatorial objects. All of these objects and their corresponding orthogonal sets (systems) have many applications in various areas including affine and projective geometries, design of experiments, in error-correcting and error-detecting coding theory and cryptology; see for example [10].

In this article systems of k-ary operations, $k \geqslant 2$, generalizing orthogonal systems of k-operations (of k-dimensional hypercubes) are considered. These systems are ordered and have the property: every k successive k-ary operations of the system are orthogonal. We call such system successively orthogonal (shortly, a SOS).

It is evident that every orthogonal set of k-operations (i.e., a set in which every k-tuple of k-operations is orthogonal) is a SOS.

Such type of systems arose, for example, in the article [11], dealing with powers of row-latin squares (see Example 1) and in the papers [5, 7, 8, 9] under investigation of systems of operations, related to complete recursive MDS-codes. In the last papers a sequence of k-ary operations $f^{(0)} = f, f^{(1)}, \ldots, f^{(s)}, \ldots$, obtained recursively from a function f: $Q^k \to Q$ that corresponds to the complete k-recursive code $K(n/f^{(0)}, f^{(1)}, \ldots, f^{(n-k-1)})$ with the check functions: $f^{(0)}, f^{(1)}, \ldots, f^{(n-k-1)}$ (see Example 2) is considered. A function f is called recursively r-differentiable if all functions $f^{(0)}, f^{(1)}, \ldots, f^{(r)}$ are k-ary quasigroups. In the article [7], the authors prove that r-differentiable quasigroups correspond

2010 Mathematics Subject Classification: 20N05, 20N15, 05B15
Keywords: Ortogonal system, n-ary operation.

to complete recursive codes and they suggest different methods of construction of binary recursively 1-differentiable quasigroups.

V. Izbash and P. Syrbu in [9, Proposition 2] proved that if a k-operation f is a k-ary quasigroup, then $f^{(i)} = f\theta^i, i = 1, 2, \ldots, s, \ldots$, where

$$\theta : Q^k \to Q^k,\ \theta(x_1^k) = (x_2, x_3, \ldots, x_k, f(x_1^k))$$

for all $(x_1^k) \in Q^k$ (this result for $k = 2$ was announced in [4]). In this case, θ is a permutation on the set Q^k. They also proved that any k successive operations of this sequence are orthogonal [9, Proposition 3], i.e., the respective sequence is a successively orthogonal system.

We prove these results for any 1-invertible k-ary operation f. We research in more detail the corresponding recursive sequence and, as a corollary, we establish the number of different k-operations in this sequence for any given 1-invertible k-ary operation f. We consider a notion of a strongly recursively r-differentiable k-ary quasigroup, suggest distinct methods of construction and corresponding examples of successively orthogonal systems of binary and k-ary, $k > 2$, operations.

2. Preliminaries

At first we recall some necessary notions, little-known results with respect to k-ary operations and with respect to their orthogonal systems.

By x_i^j we will denote the sequence $x_i, x_{i+1}, \ldots, x_j$, $i \leqslant j$. If $j < i$, then x_i^j is the empty sequence, $\overline{1,s} = \{1, 2, \ldots, s\}$. Let Q be a finite or an infinite set, $k \geqslant 1$ be a positive integer, and let Q^k denote the Cartesian power of the set Q.

A *k-ary operation* A (briefly, a *k-operation*) on a set Q is a mapping $A : Q^k \to Q$ defined by $A(x_1^k) \to x_{k+1}$. In this case, we write $A(x_1^k) = x_{k+1}$.

A *k-ary groupoid (Q, A) of order n* is a set Q with one k-ary operation A, defined on Q, where $|Q| = n$.

An k-operation A on Q is called *i-invertible* for some $i \in \overline{1,k}$ if the equation

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

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

For an i-invertible k-operation there exists the *i-inverse n-operation* ${}^{(i)}A$, defined in the following way:

$${}^{(i)}A(x_1^{i-1}, x_{k+1}, x_{i+1}^k) = x_i \Leftrightarrow A(x_1^k) = x_{k+1} \text{ for all } x_1^{k+1} \in Q^{k+1}.$$

It is evident that $A(x_1^{i-1}, {}^{(i)}A(x_1^k), x_{i+1}^k) = {}^{(i)}A(x_1^{i-1}, A(x_1^k), x_{i+1}^k) = x_i$ and ${}^{(i)}[{}^{(i)}A] = A$ for $i \in \overline{1,k}$.

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 $i \in \overline{1,k}$ (cf. [3].

Another equivalent definition of a k-quasigroup is the following. A *k-ary quasigroup* is a k-groupoid 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 considered as a k-quasigroup.

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

In the binary case, the selectors are denoted by $E_1 = F$, $E_2 = E$.

Let Ω_k be the set of all n-ary operations on a finite or an infinite set Q. On Ω_k define a binary operation $\underset{i}{\oplus}$ (the *i-multiplication*) as follows:

$$(A \underset{i}{\oplus} B)(x_1^k) = A(x_1^{i-1}, B(x_1^k), x_{i+1}^k), \quad A, B \in \Omega_k,\ x_1^k \in Q^k.$$

Shortly this equality can be written as $A \underset{i}{\oplus} B = A(E_1^{i-1}, B, E_{i+1}^k)$, where E_i is the i-th selector. In [1], it was proved that $(\Omega_k; \underset{i}{\oplus})_Q$ is a semigroup with the identity E_i.

If Λ_i is the set of all i-invertible k-operations from Ω_k for some $i \in \overline{1,k}$, then $(\Lambda_i; \underset{i}{\oplus})_Q$ is a group. In this group E_i is the identity, the inverse element for A is the operation ${}^{(i)}A \in \Lambda_i$ since $A \underset{i}{\oplus} E_i = E_i \underset{i}{\oplus} A = A$, $A \underset{i}{\oplus} {}^{(i)}A = {}^{(i)}A \underset{i}{\oplus} A = E_i$.

All 2-invertible binary operations, given on a set Q, form the group $(\Lambda_2; \cdot)$ under the multiplication $(A \cdot B)(x, y) = A(x, B(x, y))$.

Let $\sigma \in S_{k+1}$ be a permutation of degree $k+1$. The k-operation ${}^{\sigma}A$ defined by the equality ${}^{\sigma}A(x_{\sigma_1}^{\sigma_k}) = x_{\sigma_{k+1}}$ which is equivalent to the equality $A(x_1^k) = x_{k+1}$ is called a *σ-parastrophe of a quasigroup* A and is a quasigroup. Any i-inverse operation for a quasigroup A is its parastrophe.

If $\sigma(k+1) = k+1$, a parastrophe is called *principal*. A principal parastrophe exists for any k-operation.

Recall some useful information from [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 $\theta : Q^k \to Q^k$ in the following way:

$$\theta : (x_1^k) \to (A_1(x_1^k), A_2(x_1^k), \ldots, A_k(x_1^k)), \text{ (or briefly, } \theta : (x_1^k) \to (A_1^k)(x_1^k)\,).$$

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

$$\theta(x_1^k) = (A_1^k)(x_1^k) = (A_1^k(x_1^k)).$$

If C is a k-operation on Q and θ is a mapping Q^k into Q^k, then the operation $C\theta$, defined by the equality $C\theta(x_1^k) = C(\theta(x_1^k))$, is also a k-operation.

Let $C\theta = D$ and $\theta = (A_1^k)$, then $D(x_1^k) = C(A_1^k(x_1^k))$ or briefly, $D = C(A_1^k)$. If $\theta = (B_1^k)$ and $\varphi = (A_1^k)$ are mappings from Q^k into Q^k, then

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

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

Definition 1. [1]. A k-tuple $< A_1^k >$ of k-operations 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 $< E_1^k >$ of selectors of arity k is the identity permutation on Q^k and is orthogonal.

There is a close connection between orthogonal k-tuples of k-operations on Q and permutations on Q^k by virtue of the following result of [1]:

A k-tuple $< A_1^k >$ of k-operations is orthogonal if and only if the mapping $\theta = (A_1^k)$ is a permutation on Q^k.

Some properties of k-operations can be expressed by means of orthogonality. For example, a k-operation A is i-invertible ($1 \leqslant i \leqslant k$) if and only if the k-tuple $< E_1^{i-1}, A, E_{i+1}^k >$ is orthogonal (or equivalently, the mapping $\theta = (E_1^{i-1}, A, E_{i+1}^k)$ is a permutation). A k-operation A is a k-quasigroup if and only if the k-tuple $< E_1^{i-1}, A, E_{i+1}^k >$ is orthogonal for any $i \in \overline{1,k}$ [1].

Definition 2. [1] A set $\{A_1, A_2, \ldots, A_t\}$, $t \geqslant k$, of k-operations on a set Q is called *orthogonal* if every k-tuple of k-operations of the set is orthogonal.

Definition 3. [1] A set $\Sigma = \{A_1^t\}$, $t \geqslant 1$, of k-ary operations on a set Q is called *strongly orthogonal* if the set $\overline{\Sigma} = \{E_1^k, A_1^t\}$ is orthogonal.

Note that in a strongly orthogonal set $\Sigma = \{A_1^t\}$ all k-ary operations are k-ary quasigroups, and the number t of k-operations in Σ can be smaller than arity k.

Definition 4. [6] Two finite k-ary operations A and B on a set Q of order $q \geqslant 3$ is called *orthogonal* if the system of equations $\{A(x_1^k) = a,\ B(x_1^k) = b\}$ has exactly q^{k-2} solutions for any $a, b \in Q$.

3. Successively orthogonal systems

In this section we consider systems of k-operations that generalize orthogonal sets.

Definition 5. An ordered system $\Sigma = \{A_1^t\}$ of k-ary operations, $k \geqslant 2$, $t \geqslant k$, given on a set Q, is called *successively orthogonal system* (briefly, a SOS), if any successive k operations are orthogonal.

It is evident that every (strongly) orthogonal set of k-operations is a successively orthogonal system. Give some other examples of a SOS.

Example 1. In [11], Donald A. Norton studies power sets of row-latin squares of order $n \geqslant 3$, i.e., squares all rows of which are permutations. A finite 2-invertible

binary groupoid (Q, A) corresponds to a row-latin square $\overline{A}$, defined on a set $Q = \{a_1, a_2, \ldots, a_n\}$, the operation $A^i(x, y) = A(x, A^{i-1}(x, y))$ respects to the power $\overline{A}^i$ of a row-latin square $\overline{A}$. The identity square I (all its rows are identical permutations) corresponds to the selector $E_2(x, y) = E(x, y) = y$, the a_i-th row of the square $\overline{A}$ is the translation $L_{a_i}x = A(a_i, x)$ of the groupoid (Q, A).

Let (Q, A) be a finite 2-invertible operation of order n, $p(a_i)$, $a_i \in Q$, be the order of the translation L_{a_i} of (Q, A) in S_Q,

$$p = l.c.m.[p(a_1), p(a_2), \ldots, p(a_n)].$$

Then from the results of [11] it follows that $A^p = E$ (the same, $\overline{A}^p = I$), but $A^q \neq E$ for $0 < q < p$, the operations $A, A^2, \ldots, A^{p-1}$ form a series of 2-invertible operations. If (Q, A) is a quasigroup, then each two adjacent operations in the series are orthogonal and we have a SOS. □

Note that if m is the smallest power for a quasigroup (Q, A) such that A^m is not a quasigroup $(2 \leqslant m \leqslant p)$, then any m successive powers of A form an orthogonal set of 2-invertible operations (follows from Theorem 4 of [11] for row-latin squares). Thus we have a SOS of powers of the quasigroup A as well.

Example 2. In [7, 8], it was considered a complete k-recursive code $C(n, f) = (x_1, x_2, \ldots x_k, f^{(0)}(x_1^k), f^{(1)}(x_1^k), \ldots, f^{(n-k-1)}(x_1^k) \mid (x_1^k) \in Q^k)$ over an alphabet Q with words of length n, $2 \leqslant k \leqslant n$, defined by a k-operation f: $Q^k \to Q$. The functions $f^{(0)}, f^{(1)}, \ldots, f^{(n-k-1)}$ are called k-recursive derivatives of f and are defined as follows:

$$f^{(0)}(x_1^k) = f(x_1^k),$$
$$f^{(1)}(x_1^k) = f(x_2^k, f^{(0)}(x_1^k)),$$
$$f^{(2)}(x_1^k) = f(x_3^k, f^{(0)}(x_1^k), f^{(1)}(x_1^k)), \ldots,$$
$$f^{(t)}(x_1^k) = f(x_{t+1}^k, f^{(0)}(x_1^k), \ldots, f^{t-1}(x_1^k)) \text{ if } t < k,$$
$$f^{(t)}(x_1^k) = f(f^{(t-k)}(x_1^k), f^{(t-k+1)}(x_1^k), \ldots, f^{(t-1)}(x_1^k)) \text{ if } t \geqslant k.$$

V. Izbash and P. Syrbu in [9, Proposition 3], proved that if a k-operation f is a k-quasigroup, then every k successive k-recursive derivatives $f^{(i)}, f^{(i+1)}, \ldots, f^{(i+k-1)}$ of a k-quasigroup f are orthogonal. Hence, the system $\Sigma = \{f^{(0)}, f^{(1)}, \ldots, f^{(t)}, \ldots\}$ is a SOS. □

4. Methods of construction of SOS

Below we suggest some methods of construction of successively orthogonal sets of k-ary operations, $k \geqslant 2$, using k-quasigroups or invertible k-operations.

At first we consider the binary case, based on Example 1.

Let $(\Lambda_2; \underset{2}{\oplus})_Q = (\Lambda_2; \cdot)_Q$ be the group of all 2-invertible binary operations, given on a set Q, where $(A \cdot B)(x, y) = A((x, B(x, y))$.

Theorem 1. *Let $A_1, A_2, \ldots, A_t$ be binary quasigroups with the order $s_1, \ldots, s_t$ respectively in the group $(\Lambda_2; \cdot)_Q$. Then the system*

$$F, E, A_1, A_1^2, \ldots, A_1^{s_1-1}, F, E, A_2, A_2^2, \ldots, A_2^{s_2-1}, \ldots, \ F, E, A_t, A_t^2, \ldots, A_t^{s_t-1}$$

is a SOS.

Proof. Consider the system $\Sigma_1 = \{F, E, A_1, A_1^2, \ldots, A_1^{s_1-1}\}$, where $A_1^i(x,y) = A_1(x, A_1^{i-1}(x,y))$. Each operation of Σ_1 is orthogonal to its predecessor since A_1 is a quasigroup, and A_1^{i-1} is a 2-invertible operation. But s_1 is the order of the quasigroup A_1 in the group $(\Lambda_2; \cdot)_Q$ ($A_1^{s_1} = E$), so all operations $A_1, A_1^2, \ldots, A_1^{s_1-1}$ are distinct 2-invertible operations and the operation $A_1^{s_1-1}$ is orthogonal to the selector F. The selectors F and E are orthogonal as well. Analogously, using binary quasigroups $A_2, \ldots, A_t$ we obtain a *SOS*. □

Remark. Analogously, we can use the powers of quasigroups under the left multiplication $(A \circ B)(x,y) = A(B(x,y), y)$ of 1-invertible operations, if $A^{(i)}(x,y) = A(A^{(i-1)}(x,y), y)$. In this case, we obtain the following *SOS*:

$$E, F, A_1, A_1^{(2)}, \ldots, A_1^{(s_1-1)},$$

$$E, F, A_2, A_2^{(2)}, \ldots, A_2^{(s_2-1)}, \ldots, \ E, F, A_t, A_t^{(2)}, \ldots, A_t^{(s_t-1)},$$

where s_i is the order of the respective quasigroup in the group $(\Lambda_1; \circ)_Q$.

Example 3. Consider the binary quasigroup $A_1(x,y) = (1-a)x + ay$ over the field GF(11), where 1 is the identity of the field and the element a has order 5 in the multiplicative group of GF(11). Then $A_1^2(x,y) = A(x, A(x,y)) = (1-a)x + a((1-a)x + ay) = (1-a)x + ax - a^2x + a^2y = (1-a^2)x + a^2y$, $A_1^3(x,y) = (1-a^3)x + a^3y$, $A_1^4(x,y) = (1-a^4)x + a^4y$, $A_1^5(x,y) = (1-a^5)x + a^5y = y = E(x,y)$.

And let b be the generating element of the multiplication group of the field and $A_2(x,y) = (1-b)x + by$, then we obtain the following *SOS* containing 13 quasigroups:

$$F, E, A_1, A_1^2, A_1^3, A_1^4, F, E, A_2, A_2^2, \ldots, A_2^9. \qquad \square$$

Let A^{-1} be the inverse element for a binary 2-invertible operation A in the group $(\Lambda_2; \cdot)_Q$. Simultaneously this operation is the right inverse quasigroup for (Q, A), if (Q, A) is a quasigroup.

Proposition 1. *Let (Q, A) be a binary quasigroup, s be the order of A in the group $(\Lambda_2; \cdot)_Q$, $A^{-(i)} = (A^i)^{-1}$. Then the system*

$$\Sigma = \{A^{-(s-1)}, A^{-(s-2)}, \ldots, A^{-1}, E, A, A^2, \ldots, A^{s-1}\}$$

is a SOS of 2-invertible binary operations.

Proof. Indeed, in this case, A (A^{-1}) is a quasigroup, so it is orthogonal to the selector E (F, if instead E in the *SOS* to use F. In this *SOS* we can use also both

selectors). It is easy to see that any two successive operations are also orthogonal since A and A^{-1} are quasigroups, and the rest operations are 2-invertible. □

Let $k \geqslant 3$. Consider k-invertible k-operations A and B on a set Q and the k-th multiplication of these operations:

$$C(x_1^k) = (A \oplus_k B)(x_1^k) = A(x_1^{k-1}, B(x_1^k)).$$

In this case, the k-operation C is also k-invertible, and all k-invertible operations on Q consist the group $(\Lambda_k; \underset{k}{\oplus})_Q$ under the multiplication $A \oplus_k B$. The identity of this group is the selector $E_k : E_k(x_1^k) = x_k$.

Now consider the following power set $\Sigma_A = \{A, A^2, \dots A^{s-1}\}$, generated by a k-invertible k-operation A of order s ($A^s = E_k$) in the group $(\Lambda_k; \oplus_k)_Q$, where $A^i(x_1^k) = A(x_1^{k-1}, A^{i-1}(x_1^k)), i = 2, 3, \dots, s-1$. The number of distinct finite k-operations in Σ_A is equal $s-1$.

In contrast to the binary case, for $k \geqslant 3$ the set Σ_A is not a SOS since the following statement is valid.

Proposition 2. *For each integer $k \geqslant 3$ and for any k-invertible k-operation A of order $s > k$ in the group $(\Lambda_k; \oplus_k)_Q$, $\mid Q \mid \geqslant 3$, the k-tuple $< A^i, A^{i+1}, A^{i+k-1} >$ of successive powers of A, $i \in \overline{1, s-k}$, is not orthogonal.*

Proof. Let $k \geqslant 3$, $\Sigma_A = \{A, A^2, \dots, A^{s-1}\}$ be the power set, generated by a k-invertible k-operation A, where $A^i(x_1^k) = A(x_1^{k-1}, A^{i-1}(x_1^k))$, $i = 2, 3, \dots, s-1$. Consider the k-tuple $< A^i, A^{i+1}, \dots, A^{i+k-1} >$ and the respective system of equations if $a \neq b$ $(a, b \in Q)$:

$$A^i(x_1^k) = a, A^{i+1}(x_1^k) = a, A^{i+2}(x_1^k) = a, \dots, A^{i+k-1}(x_1^k) = b.$$

Then $A^i(x_1^k) = a, A(x_1^{k-1}, a) = a, \dots, A(x_1^{k-1}, a) = a, A(x_1^{k-1}, a) = b$. This system has not a solution for the k-tuple $< a, a, \dots, a, b >$ when $a \neq b$ and $k \geqslant 3$. Thus the tuple $< A^i, A^{i+1}, \dots, A^{i+k-1} >$ is not orthogonal. □

But the set $\Sigma_A = \{A, A^2, \dots, A^{s-1}\}$, $s > k$, has one good property when (Q, A) is a finite k-quasigroup of order q ($\mid Q \mid = q$).

Proposition 3. *Let (Q, A) be a k-quasigroup of order q, s be the order of A in the group $(\Lambda_k; \oplus_k)_Q$, $\Sigma_A = \{A, A^2, \dots, A^{s-1}\}$, $s > k$. Then every two successive k-operations A^i and A^{i+1} of Σ_A, $i \in \overline{1, s-2}$, are orthogonal.*

Proof. From the system $\{A^i(x_1^k) = a,\ A^{i+1}(x_1^k) = A(x_1^{k-1}, A^i(x_1^k)) = b\}$ it follows that $A(x_1^{k-1}, a) = b$. But this equation has exactly q^{k-2} solutions for any $a, b \in Q$ since the $(k-1)$-ary operation $A_a(x_1^{k-1}) = A(x_1^{k-1}, a)$ is a $(k-1)$-quasigroup, so in it every element b of Q appears exactly q^{k-2} times. Hence, the equation $A(x_1^{k-1}, a) = b$ has exactly q^{k-2} solutions. For any solution c_1^{k-1} the equation $A^i(c_1^{k-1}, x_k) = a$ has unique solution since the k-operation A^i is k-invertible. Thus the k-operations A^i and A^{i+1} are orthogonal. □

Proposition 4. *Let A be a k-invertible k-operation, given on a set Q and s be the order of A in the group $(\Lambda_k; \underset{k}{\oplus})_Q$. Then the system*

$$E_1, E_2, \ldots, E_{k-1}, A, E_1, E_2, \ldots, E_{k-1}, A^2, E_1, E_2, \ldots, E_{k-1}, A^3, \ldots,$$

$$E_1, E_2, \ldots, E_{k-1}, A^s = E_k$$

is a SOS, where $A^i(x_1^k) = A(x_1^{k-1}, A^{i-1}(x_1^k))$, $i = 2, 3, \ldots, s$.

Proof. Indeed, any k-tuple $< E_j, E_{j+1}, \ldots, E_{k-1}, A^i, E_1, E_2, \ldots, E_{j-1} >$, $j = 2, \ldots, k-1$, and any k-tuple $< A^i, E_1, E_2, \ldots, E_{k-1} >$ are orthogonal since every of the k-operation A^i, $i = 1, 2, 3, \ldots, s$, is k-invertible. □

Corollary 1. *If A is a binary 2-invertible operation, given on a set Q, has the order s in the group $(\Lambda_2; \cdot)_Q$, then the system*

$$F, A, F, A^2, \ldots, F, A^{s-1}, F, A^s = E$$

is a SOS, where $A^i(x, y) = A(x, A^{i-1}(x, y))$, $i = 2, 3, \ldots, s$. □

Proposition 5. *Let $\Sigma_1 = \{A_1, A_2, \ldots, A_{t_1}\}$ and $\Sigma_2 = \{B_1, B_2, \ldots, B_{t_2}\}$ be strongly orthogonal sets of k-operations. Then the system*

$$\Sigma_3 = \{E_1, E_2, \ldots, E_k, A_1, A_2, \ldots, A_{t_1}, E_1, E_2, \ldots, E_k, B_1, B_2, \ldots, B_{t_2}\}$$

is a SOS.

Proof. It easy to see that every k-tuple of successive k-operations is orthogonal since the systems Σ_1 and Σ_2 of k-ary quasigroups are strongly orthogonal. □

Theorem 2. *Let $A \neq E_1$ be an 1-invertible k-operation on a set Q, $k \geqslant 2$, $\theta = (E_2^k, A)$ and let s be the order of the permutation θ in the group S_{Q^k}. Then $s > k$ and the sequence of k-operations*

$$E_1, E_2, \ldots, E_k, A, A\theta, A\theta^2, \ldots, A\theta^{k-1}, A\theta^k, \ldots, A\theta^{s-k-1}$$

is a SOS.

Proof. From the 1-invertibility of an k-operation A it follows that the mapping $\theta = (E_2^k, A)$ is a permutation on the set Q^k, and $A \neq E_2, E_3, \ldots, E_k$.

Consider the following mappings which are also permutations:

$$\theta = (E_2^k, A) = (E_2, \ldots, E_k, A),$$

$$\theta^2 = \theta(\theta) = (E_2^k, A)(E_2, \ldots, E_k, A) = (E_3, \ldots, E_k, A, A\theta), \ldots,$$

$$\theta^{k-1} = \theta(\theta^{k-2}) = (E_k, A, A\theta, \ldots, A\theta^{k-2}),$$

$$\theta^k = \theta\theta^{k-1} = (A, A\theta, \ldots, A\theta^{k-1}), \ldots,$$

$$\theta^t = (A\theta^{t-k}, A\theta^{t-k+1}, \ldots, A\theta^{t-1}),\ t > k.$$

These permutations mean that the k-tuples of k-operations corresponding to them are orthogonal. Let s be the order of the k-permutation θ, i. e., $\theta^s = \varepsilon = (E_1, E_2, \ldots, E_k)$, then

$$\theta^s = (A\theta^{s-k}, A\theta^{s-(k-1)}, \ldots, A\theta^{s-2}, A\theta^{s-1}) =$$

$$(A\theta^{-k}, A\theta^{-(k-1)}, \ldots, A\theta^{-2}, A\theta^{-1}) = (E_1, E_2, \ldots, E_k).$$

From these equalities it follows that $A\theta^{s-k} = A\theta^{-k} = E_1$, $A\theta^{s-(k-1)} = A\theta^{-k+1} = E_2, \ldots, A\theta^{s-1} = A\theta^{-1} = E_k$.

It is evident that $s > k$ since $A \neq E_1$, and $\theta^k = (A, A\theta, A\theta^2, \ldots, A\theta^{k-1})$.

Thus we have the following sequence of k-permutations:

$$\varepsilon, \theta, \theta^2, \ldots, \theta^{s-1}, \theta^s = \varepsilon, \theta, \theta^2, \ldots, \theta^s = \varepsilon, \ldots.$$

This sequence corresponds to the following successively orthogonal system, where s k-operations are repeated:

$$E_1, E_2, \ldots, E_k, A, A\theta, A\theta^2, \ldots, A\theta^{k-1}, A\theta^k, \ldots, A\theta^{s-k-1}, \tag{1}$$

$$E_1, E_2, \ldots, E_k, A, A\theta, A\theta^2, \ldots, A\theta^{k-1}, A\theta^k, \ldots, A\theta^{s-k-1}, \ldots \qquad \square$$

Corollary 2. *In Theorem* 2 *the k-operation $A\theta^{s-k-1}$ is k-invertible.*

Proof. Indeed, from the above we get that the k-mapping

$$\theta^{s-1} = (A\theta^{s-k-1}, A\theta^{s-k}, \ldots, A\theta^{s-2}) = (A\theta^{s-k-1}, E_1, E_2, \ldots, E_{k-1})$$

is a permutation, so the k-tuple $< A\theta^{s-k-1}, E_1, E_2, \ldots, E_{k-1} >$ of operations is orthogonal, and the k-operation $A\theta^{s-k-1}$ is k-invertible. $\square$

In [7], for a function f: $Q^k \to Q$ it was defined a complete k-recursive code $K(n/f^{(0)}, f^{(1)}, \ldots, f^{(n-k-1)})$, $f^{(0)} = f$, with the check functions: $f^{(0)}, f^{(1)}, \ldots, f^{(n-k-1)}$, defined in Example 2.

The function $f^{(i)}$ is called the *i-th recursive derivative* of a function f.

A k-quasigroup operation f ($k \geqslant 2$) is called *recursively r-differentiable* if all its k-recursive derivatives $f^{(0)}, f^{(1)}, \ldots, f^{(r)}$ are k-quasigroups.

By Proposition 7 of [7], the system of operations

$$\Sigma = \{E_1, E_2, \ldots, E_k, f^{(0)}, f^{(1)}, f^{(2)}, \ldots, f^{(r)}\}$$

is orthogonal.

V. Izbash and P. Syrbu in [9, Proposition 2] proved that if a k-operation f is a k-quasigroup, then $f^{(i)} = f\theta^i, i = 1, 2, \ldots$, where

$$\theta : Q^k \to Q^k, \quad \theta(x_1^k) = (x_2, x_3, \ldots, x_k, f(x_1^k))$$

for all $(x_1^k) \in Q^k$. In this case, $\theta = (E_2, E_3, \ldots, E_k, f)$ and is a permutation since f is a quasigroup.

Corollary 3. *If a function f is an r-differentiable k-quasigroup, then $r \leqslant s-k-1$, where s is the order of the permutation $\theta = (E_2^k, f)$.* □

Lemma 1. *Let A be an 1-invertible k-operation, $\theta = (E_2^k, A)$. Then*

$$\theta^{-1} = ({}^{\sigma}({}^{(1)}A), E_1, E_2, \ldots E_{k-1}), \tag{2}$$

$$A({}^{\sigma}({}^{(1)}A)(x_1^k), x_1, x_2, \ldots, x_{k-1}) = x_k,$$

where ${}^{(1)}A$ is the 1-inverse operation for the k-operation A, and the principal parastrophe σ is defined by the permutation

$$\sigma(x_1, x_2, \ldots, x_k) = (x_{\sigma 1}, x_{\sigma 2}, \ldots, x_{\sigma k}) = (x_k, x_1, x_2, \ldots, x_{k-1}).$$

Proof. Let $\theta^{-1} = (D_1, D_2, \ldots, D_k)$, find the k-operations $D_1, D_2, \ldots, D_k$:

$$(E_2^k, A)(E_2^k, A)^{-1} = (E_1, E_2, \ldots E_k),\ (E_2^k, A)(D_1, D_2, \ldots, D_k) =$$

$$(D_2, D_3, \ldots D_k, A(D_1, D_2, \ldots, D_k)) = (E_1, E_2, \ldots E_k).$$

Hence, $D_2 = E_1, D_3 = E_2, \ldots, D_k = E_{k-1}$, $A(D_1, D_2, \ldots, D_k) = E_k$ or

$$A(D_1, E_1, E_2, \ldots, E_{k-1}) = E_k, \quad A(D_1(x_1^k), x_1, x_2, \ldots, x_{k-1}) = x_k,$$

whence

$$D_1(x_1^k) = {}^{(1)}A(x_k, x_1, x_2, \ldots, x_{k-1}).$$

Here ${}^{(1)}A$ is the 1-inverse operation for the 1-invertible k-operation A. Hence, $D_1(x_1^k) = {}^{\sigma}({}^{(1)}A)(x_1^k)$, where σ is the principal parastrophe of ${}^{(1)}A$ defined by the cyclic permutation $\sigma(x_1, x_2, \ldots, x_k) = (x_k, x_1, x_2, \ldots, x_{k-1})$. Thus $\theta^{-1} = ({}^{\sigma}({}^{(1)}A), E_1, E_2, \ldots E_{k-1})$. □

As a corollary we obtain the result of V.D. Belousov from [2] for a binary quasigroup A: $D_1(x, y) = {}^{-1}A(y, x) = {}^{-1}(A^{-1})(x, y)$ and $(E, A)^{-1} = ({}^{-1}(A^{-1}), F)$.

Theorem 3. *Let a permutation (E_2^k, A) have the order s, then a successively orthogonal system of Theorem 2 contains s different k-operations, which are repeated. If $s = k+1$, then the k-operation A is a k-quasigroup. For any 1-invertible k-operation $s \geqslant k+1$.*

Proof. Prove that in (1) all operations are distinct. Let $A^{(i)} = A^{(j)}$, $i, j < s$, $j > i$, then $A\theta^t = A$, where $t = j - i < s$. But then $A^{(t-1)}\theta = A$ and by Lemma 1,

$$A^{(t-1)}(x_1^k) = A\theta^{-1}(x_1^k) = A({}^{\sigma}({}^{(1)}A)(x_1^k), x_1, x_2, \ldots, x_{k-1}) = x_k.$$

Thus $A^{(t-1)} = E_k$.

Further, from $A^{(t-1)} = A^{(t-2)}\theta = E_k$ according to (2) it follows

$$A^{(t-2)} = E_k\theta^{-1} = E_k({}^{\sigma}({}^{(1)}A), E_1, E_2, \dots E_{k-1}) = E_{k-1}.$$

Analogously, taking into account that $A^{(i)} = A^{(i-1)}\theta$, we obtain

$$\theta^t = (A\theta^{t-k}, A\theta^{t-(k-1)}, \dots, A\theta^{t-2}, A\theta^{t-1}) = (E_1, E_2, \dots, E_k) = \theta^s.$$

But s is the least number such that $\theta^s = \varepsilon$. We have the contradiction since $t = j - i < s$.

If $A^{(t)} = E_i$, $1 \leqslant i \leqslant k$, then $t < s - k + i - 1$ since $A^{(t)} = A^{(t-1)}\theta = E_i = A^{s-k+i-1}$ (it is the i-th component in $\theta^s = (A\theta^{s-k}, A\theta^{s-(k-1)}, \dots, A\theta^{s-2}, A\theta^{s-1})$). Use the equality (2):

$$A^{(t-1)} = E_i\theta^{-1} = E_i({}^{\sigma}({}^{(1)}A), E_1, E_2, \dots E_{k-1}) = E_{i-1},$$

$$A^{(t-2)} = E_{i-1}\theta^{-1} = E_{i-1}({}^{\sigma}({}^{(1)}A), E_1, E_2, \dots E_{k-1}) = E_{i-2}, \dots,$$

$$A^{(t-(i-1))} = E_{i-(i-2)}({}^{\sigma}({}^{(1)}A), E_1, E_2, \dots E_{k-1}) = E_1,$$

$$A^{(t+1)} = E_i\theta = E_i(E_2^k, A) = E_{i+1},$$

$$A^{(t+2)} = E_{i+1}\theta = E_{i+1}(E_2^k, A) = E_{i+2}, \dots,$$

$$A^{(t+(k-i))} = E_{k-1}\theta = E_{k-1}(E_2^k, A) = E_k.$$

It means that

$\theta^{t-i+k+1} = (A^{(t-(i-1))}, A^{(t-i+2)}, \dots, A^{(t-1)}, A^{(t)}, A^{(t+1)}, \dots, A^{t+(k-i)}) =$
$(E_1, E_2, \dots, E_k) = \theta^s$. But $t < s - k + i - 1$, so $t - i + k + 1 < s$.

If $s = k + 1$, $\theta = (E_2^k, A)$, then $\theta^{k+1} = (A\theta, A\theta^2, \dots, A\theta^k) = (E_1, E_2, \dots, E_k)$ and we get the successively orthogonal sequence

$$E_1, E_2, \dots, E_k, A, E_1, E_2, \dots, E_k, A, \dots.$$

Hence, the mappings (E_2^k, A), (E_3^k, A, E_1), (E_4^k, A, E_1, E_2),..., (A, E_1^{k-1}) are permutations. It means that the k-operation A is i-invertible for any $i = 1, 2, \dots, k$, i. e., A is a k-quasigroup. □

Above we established that, in general case, $r \leqslant s - k - 1$ for an r-differentiable k-quasigroup A, where s is the order of the permutation $\theta = (E_2^k, A)$. Now consider r-differentiable k-quasigroups with $r = s - k - 1$.

A k-quasigroup (Q, A) we shall call *strongly recursively r-differentiable* if $r = s - k - 1$, where s is the order of the permutation $\theta = (E_2^k, A)$. In this case, $A^{(r+1)} = E_1$. For the binary quasigroups this notion was introduced in [5].

By Theorem 3, all $r = s - k - 1$ derivatives of a strongly recursively r-differentiable quasigroup are different.

From Theorems 2 and 3 we obtain the following corollary for any 1-invertible k-function (k-operation) f.

Corollary 4. *If f is an 1-invertible k-function, then $f^{(i)} = f\theta^{(i)}$, $i = 1, 2, \ldots$, where $\theta = (E_2^k, f)$. The sequence of the recursive derivatives has the form*

$$E_1, E_2, \ldots, E_k, f, f\theta, f\theta^2, \ldots, f\theta^{k-1}, f\theta^k, \ldots, f\theta^{s-k-1},$$

$$E_1, E_2, \ldots, E_k, f, f\theta, f\theta^2, \ldots, f\theta^{k-1}, f\theta^k, \ldots, f\theta^{s-k-1}, \ldots,$$

where s is the order of the permutation θ. For a strongly recursively r-differentiable k-quasigroup $s = r + k + 1$. For an 1-differentiable k-quasigroup $s \geqslant k + 2$. For a 0-differentiable k-quasigroup $s \geqslant k + 1$. □

Example 4. Give an example of a strongly recursively r-differentiable binary quasigroup (Q, A) of order 7 (Example 2 of [5]) over the field $GF(7)$ (in this case, $E_1 = F, E_2 = E$):

$A(x, y) = 2(y - x) + x = 6x + 2y$;
$A^{(1)}(x, y) = 5x + 3y$;
$A^{(2)}(x, y) = 4x + 4y$;
$A^{(3)}(x, y) = 3x + 5y$;
$A^{(4)}(x, y) = 2x + 6y$;
$A^{(5)}(x, y) = F(x, y) = x$.

This quasigroup is strongly recursively 4-differentiable and generates the orthogonal system $\Sigma = \{F, E, A, A^{(1)}, A^{(2)}, A^{(3)}, A^{(4)}\}$. By Corollary 4, the permutation $\theta = (E, A)$ has the order $s = 4 + 2 + 1 = 7$ in the group S_{49}. □

Example 5. For an illustration of Corollary 4 consider one small example when k=2, $A_1(x, y) = x + y \pmod 3$, $\theta_1 = (E, A_1)$. Taking into account that A_1 is an abelian group, we obtain the following successively orthogonal sequence (modulo 3) with repetition:

$$F, E, A_1(x, y) = x + y, A_1\theta_1(x, y) = x + 2y, A_1\theta_1^2(x, y) = 2x,$$

$$A_1\theta_1^3(x, y) = 2y, A_1\theta_1^4(x, y) = 2x + 2y, A_1\theta_1^5(x, y) = 2x + y,$$

$$A_1\theta_1^6(x, y) = x = F(x, y), A_1\theta_1^7(x, y) = y = E(x, y), A_1\theta_1^8(x, y) = x + y, \ldots$$

The permutation θ_1 has the order 8 since $\theta_1^8 = (A_1\theta_1^6, A_1\theta_1^7) = (F, E)$ in the group S_9 and the sequence contains eight different operations. □

Now we change the construction of a successively orthogonal system of Theorem 2, beginning with the first repetition and using other 1-invertible k-operations.

Theorem 4. *Let $A_1, A_2, \ldots, A_t$ be 1-invertible k-operations and the permutations $\theta_1 = (E_2^k, A_1)$, $\theta_2 = (E_2^k, A_2)$, $\theta_3 = (E_2^k, A_3), \ldots$, $\theta_t = (E_2^k, A_t)$ have the orders $s_1, \ldots, s_t$ respectively. Then the system*

$$E_1, E_2, \ldots, E_k, A_1, A_1\theta_1, A_1\theta_1^2, \ldots, A_1\theta_1^{k-1}, A_1\theta_1^k, \ldots, A_1\theta_1^{s_1-k-1},$$

$$E_1, E_2, \ldots, E_k, A_2, A_2\theta_2, A_2\theta_2^2, \ldots, A_2\theta_2^{k-1}, A_2\theta_2^k, \ldots, A_2\theta_2^{s_2-k-1}, \ldots,$$

$$E_1, E_2, \ldots, E_k, A_t, A_t\theta_t, A_t\theta_t^2, \ldots, A_t\theta_t^{k-1}, A_t\theta_t^k, \ldots, A_t\theta_t^{s_t-k-1}$$

is successively orthogonal.

Proof. Begin with the first repetition, using an 1-invertible k-operation $A_2 \neq A_1$ and the permutation $\theta_2 = (E_2^k, A_2)$ of order s_2:

$$E_1, E_2, \ldots, E_k, A_1, A_1\theta_1, A_1\theta_1^2, \ldots, A_1\theta_1^{k-1}, A_1\theta_1^k, \ldots, A_1\theta_1^{s_1-k-1},$$

$$E_1, E_2, \ldots, E_k, A_2, A_2\theta_2, A_2\theta_2^2, \ldots, A_2\theta_2^{k-1}, A_2\theta_2^k, \ldots, A_2\theta_1^{s_2-k-1}.$$

It is evident that we obtain a SOS which can be continued if to use distinct 1-invertible k-operations $A_3, A_4, \ldots$. □

Some operations, different from the selectors, in distinct "fragments" of this SOS, in general case, can coincide.

Example 6. Continue the sequence of Example 5, using the following k-operations (k-quasigroups):

$A_1(x,y) = x + y \,(mod\, 3)$, $A_2(x,y) = 2x + y \,(mod\, 3)$, $A_3(x,y) = x + 2y \,(mod\, 3)$. Then $\theta_1 = (E, A_1)$, $\theta_2 = (E, A_2)$, $\theta_3 = (E, A_3)$ and we obtain the following SOS (modulo 3):

$$F, E, A_1(x,y) = x + y,\ A_1^{(1)}(x,y) = x + 2y, A_1^{(2)}(x,y) = 2x, A_1^{(3)}(x,y) = 2y,$$

$$A_1^{(4)}(x,y) = 2x + 2y, A_1^{(5)}(x,y) = 2x + y, A_1^{(6)} = F, A^{(7)} = E,$$

$$A_2(x,y) = 2x + y,\ A_2^{(1)}(x,y) = 2x,\ A_2^{(2)}(x,y) = 2(2x + y) + 2x = 2y,$$

$$A_2^{(3)}(x,y) = x + 2y, A_2^{(4)} = F, A_2^{(5)} = E,$$

$$A_3(x,y) = x + 2y,\ A_3^{(1)}(x,y) = y + 2(x + 2y) = 2x + 2y,$$

$$A_3^{(2)}(x,y) = x + 2y + 2(2x + 2y) = 2x,\ A_3^{(3)}(x,y) = 2x + 2y + 4x = 2y,$$

$$A_3^{(4)}(x,y) = 2x + 4y = 2x + y,\ A_3^{(5)}(x,y) = 2y + 2(2x + y) = x + y,$$

$$A_3^{(6)}(x,y) = 2x + y + 2(x + y) = x,\ A_3^{(7)}(x,y) = x + y + 2x = y. \qquad \square$$

From this example it follows that the order of the permutations θ_1, θ_2 and θ_3 is 8, 6 and 8 respectively. The quasigroups A_1 and A_3 are 1-differentiable, and A_2 is 0-differentiable.

References

[1] **A. S. Bektenov and T. Yacubov**, *Systems of orthogonal n-ary operations*, (Russian), Izv. AN Moldav. SSR, Ser. fiz.-teh. i mat. nauk **3** (1974), 7 – 14.

[2] **V. D. Belousov**, *Systems of orthogonal operations*, (Russian), Matem. sbornik **77** (119), (1968), 38 – 58.

[3] **V. D. Belousov**, *n-Ary quasigroups*, (Russian), Ştiinţa, Kishinev, 1972.

[4] **G. B. Belyavskaya**, *On r-differentiable quasigroups*, Abstracts Int. Conf. Pure and Appl. Math., Kiev, 2002, 11 – 12.

[5] **G. B. Belyavskaya**, *Recursively r-differentiable quasigroups within S-systems and MDS-codes*, Quasigroups and Related Systems **20** (2012), 157 – 168.

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

[7] **E. Couselo, S. Gonsales, V. Markov, A. Nechaev**, *Recursive MDS-codes and recursively differentiable quasigroup*, (Russian), Discret. Mat. **10** (1998), 3 – 29.

[8] **E. Couselo, S. Gonsales, V. Markov, A. Nechaev**, *The parameters of recursive MDS-codes*, (Russian), Discret. Mat. **12** (2000), 3 – 24.

[9] **V. I. Izbash and P. Syrbu**, *Recursively differentiable quasigroups and complete recursive codes*, Comment. Math. Univ. Carolinae **45** (2004), 257 – 263.

[10] **C. F. Laywine and G. L. Mullen**, *Discrete Mathematics Using Latin Squares*, Wiley, New York, 1998.

[11] **D. A. Norton**, *Groups of orthogonal row-latin squares*, Pacific J. Math. **11** (1952), 335 – –341.

Received June 2, 2014

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