Methods of construction of successively orthogonal systems of k-operations

Galina B. Belyavskaya

IMI - 2015, V.D. Belousov - 90

Abstract

We continue the study of successively orthogonal systems of k-operations (SOS) which generalize orthogonal sets. These systems have the following property: every k successive k-ary operations of the system are orthogonal. We suggest new methods of construction of such systems, in particular, method of continuation of an orthogonal system of k-operations to a SOS.

Introduction

It is known that k-ary operations, $k \geq 2$, correspond to k-dimensional hypercubes 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.

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, designs of experiments, error-correcting and error-detecting coding theory and cryptology.

Preliminaries

A k-ary operation A (briefly, a k-operation) on a set Q is a mapping $A : Q^k \to Q$, defined by $A(x_1^k) \to x_{k+1}$, where $(x_1^k) = (x_1, x_2, ..., x_k)$. In this case write $A(x_1^k) = x_{k+1}$.

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

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

In the binary case, $E_1 = F$, $E_2 = E$.

An i-invertible k-operation A, defined on Q, is a k-operation with the following property: the equation $A(a_1^{i-1}, x, a_{i+1}^k) = a_{k+1}$ has a unique solution for each fixed k-tuple $(a_1^{i-1}, a_{i+1}^k, a_{k+1})$ of Q^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 $i = 1, 2, \ldots, k$.

The following three definitions generalize the corresponding notions for the binary case (V.D.Belousov for $k = 2$), were introduced by Bektenov A.S., Yacubov T. (1974).

Definition 1. *A k-tuple $< A_1, A_2, ..., A_k >=< A_1^k >$ of 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 $a_1^k \in Q^k$.*

Definition 2. *A set $\{A_1, A_2, \ldots, A_t\}$, $t \geq k$, of k-operations is called orthogonal if every k-tuple of these k-operations is orthogonal.*

Definition 3. *A set $\Sigma = \{A_1^t\}$, $t \geq 1$, of k-ary operations, given on a set Q, is called strongly orthogonal if the set $\overline{\Sigma} = \{A_1^t, E_1^k\}$ 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 A. S. Bektenov, T. Yacubov (V.D. Belousov for $k = 2$):

A k-tuple $< A_1^k >$ of k-operations is orthogonal if and only if the mapping $\theta = (A_1^k) : Q^k \to Q^k$, $(x_1^k) \to (A_1(x_1^k), A_2(x_1^k), ..., A_k(x_1^k)) = (A_1^k)(x_1^k)$ 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 ($1 \leq i \leq k$) 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 $i \in \overline{1,k}$.

Methods of construction of SOS

The concept of successively orthogonal systems of k-operations was introduced in the article [gbel] published in 2014.

Some examples of these quasigroups arose in the investigation of row-complete latin squares and recursively differentiable quasigroups connected with recursive MDS-codes.

Definition 4 [gbel]. *An ordered system $\Sigma = \{A_1^t\}$ of k-ary operations, $k \geq 2$, $t \geq k$, given on a set Q, is called a 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.

In the article [gbel] it were given the following methods of the construction of a SOS, using one or more 1-invertible k-operations.

Theorem 1 [gbel]. *Let $A \neq E_1$ be an 1-invertible k-operation on a set Q, $k \geq 2$, $\theta = (E_2^k, A)$, s_0 be the order of the permutation θ in the group S_{Q^k}, then $s_0 > k$ and the sequence of k-operations*

$$E_1, E_2, ..., E_k, A, A\theta, A\theta^2, ..., A\theta^{k-1}, A\theta^k, ..., A\theta^{s_0-k-1}$$

is a SOS.

Remark 1. Note that from the proof of this theorem it follows that this fragment of the SOS is repeated, that is $A\theta^{s_0-k} = E_1, A\theta^{s_0-k+1}, ..., A\theta^{s_0-1} = E_k$. $A\theta^{s_0} = A...$.

Theorem 2 [gbel]. *Let $A_1, A_2, ..., A_t$ be 1-invertible k-operations and the permutations $\theta_1 = (E_2^k, A_1)$, $\theta_2 = (E_2^k, A_2)$, $\theta_3 = (E_2^k, A_3)$,..., $\theta_t = (E_2^k, A_t)$ have the orders $s_1, ..., s_t$ respectively, then the system*

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

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

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

is successively orthogonal.

The following theorem of [gbel] points out the number of different operations in the SOS of Theorem 1 [gbel] for a given 1-invertible k-operation A.

Theorem 3 [gbel]. *Let a permutation (E_2^k, A) have the order s_0, then a successively orthogonal system of Theorem 2 contains s_0 different k-operations, which are repeated. If $s_0 = k+1$, then the k-operation A is a k-quasigroup. For any 1-invertible k-operation $s_0 \geq k+1$.*

Now we suggest a new more general recursive method of the construction of a SOS, using any 1-invertible k-operations.

Theorem 4. *Let* $A_1, A_2, ..., A_t$, $t \geq 1$, *be arbitrary 1-invertible* k*-operations,* $k \geq 2$, *given on a set* Q, $\theta_1 = (E_2^k, A_1), \theta_2 = (E_2^k, A_2), ..., \theta_t = (E_2^k, A_t)$ *be the corresponding permutations on* Q^k. *Then the system*

$$E_1, E_2, ..., E_k,\ B_1 = A_1,\ B_2 = A_2\theta_1,\ B_3 = A_3(\theta_2\theta_1), ...,$$

$$B_t = A_t(\theta_{t-1}...\theta_2\theta_1)$$

is a SOS.

Corollary 1. *The system of the theorem 4 has the form*

$$E_1, E_2, ..., E_k, B_1, B_2, ..., B_t \text{ where } B_1 = A_1,$$

$$B_s = A_s(E_s^k, B_1, B_2, ..., B_{s-1}), \text{ if } 1 < s \leq k,$$

$$B_s = A_s(B_{s-k}, B_{s-k+1}, ..., B_{s-1}), \text{ if } k < s \leq t.$$

Corollary 2. *Let $A_1, A_2, ..., A_t$ be arbitrary 1-invertible binary operations, given on a set Q, $\theta_1 = (E, A_1), \theta_2 = (E, A_2), ..., \theta_t = (E, A_t)$ be the corresponding permutations on Q^2. Then we have the following SOS:*

$$F, E, B_1 = A_1, B_2 = A_2(E, B_1), B_3 = A_3(B_1, B_2), ...,$$

$$B_t = A_t(B_{t-2}, B_{t-1}).$$

Example 1. Let $A_1, A_2, ..., A_5$ be the following binary quasigroups over the field GF(7) (modulo 7).

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

$$A_4(x,y) = x + 3y,\ A_5(x,y) = 3x + y.$$

By Corollary 2:

$$B_1(x,y) = x+y,\ B_2(x,y) = A_2(y, B_1(x,y)) = 2y+x+y = x+3y,$$

$$B_3(x,y) = A_3(B_1, B_2)(x,y) = 2(x+y) + 2(3y+x) = 4x + y,$$

$$B_4(x,y) = A_4(B_2, B_3)(x,y) = 3y + x + 3(4x+y) = 6x + 6y,$$

$$B_5(x,y) = A_5(B_3, B_4)(x,y) = 3(4x+y) + 6x + 6y = 4x + 2y.$$

We obtain the following SOS of the selectors and five quasigroups (modulo 7):

$$F, E,\ B_1(x,y) = A_1(x,y) = x + y,\ B_2(x,y) = x + 3y,$$

$$B_3(x,y) = 4x + y,\ B_4(x,y) = 6x + 6y,\ B_5(x,y) = 4x + 2y.$$

Note that this SOS is not an orthogonal set (for example, the operations B_1 and B_4 are not orthogonal).

In this example all operations (besides of the selectors) are quasigroups. In the proof of the following proposition we shall give a method of the construction of a SOS containing only binary quasigroups. This method is some modification of the method of Theorem 4 for binary quasigroups.

Proposition 1. *For any prime $p \geq 5$ and any $t \geq 3$ there exists a SOS of t binary quasigroups of order p.*

Remark 2. If in Theorem 4 $A_1 = A_2 = ... = A_t = A$, then $\theta_1 = \theta_2 = ... = \theta_t = \theta$. Let s_0 be the order of the permutation θ in the group S_{Q^k}. Then, as a corollary, we have the sequence of Theorem 1 [gbel], moreover, we obtain the following SOS:

$$E_1, E_2, ..., E_k, B_1, B_2, B_3, ..., B_t \text{ where } B_1 = A,$$

$$B_s = A(E_s^k, B_1, B_2, ..., B_{s-1}), \text{ if } 1 < s \leq k,$$

$$B_s = A(B_{s-k}, B_{s-k+1}, ..., B_{s-1}), \text{ if } k < s \leq t.$$

In this case the k-operations of this SOS are repeated beginning with B_{s_0-k} and contains exactly s_0 different k-operations.

It was be found that any orthogonal system of k-operations can be continued to a SOS.

Theorem 5. *Any orthogonal system of k-operations can be continued to a SOS.*

In the proof of this theorem a method of construction of a SOS from an orthogonal system of k-operations is given.

Corollary 3. *Every orthogonal k-tuple $< C_1, C_2, ..., C_k >$ of k-operations can be continued to a SOS.*

References:

1. Bektenov A.S., Yacubov T. Systems of orthogonal n-ary operations (In Russian) // Izv. AN Moldavskoi SSR, Ser. fiz.-teh. i mat. nauk, no. 3, 1974, 7–14.

2. Belyavskaya G.B. Successively orthogonal systems of k-ary operations // Quasigroups and Related Systems, 22 (2014), 165-178.

3. Couselo E., Gonsales S., Markov V., Nechaev A. Recursive MDS-codes and recursively differentiable quasigroups (in Russian) // Discret. Mat. vol. 10, no.2, 1998, $3 - 29$.

4. Izbash V., Syrbu P. Recursively differentiable quasigroups and complete recursive codes // Commentationes Mathematicae Universitatis Carolinae, Praga, 2004, 45,2, 257-263.

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

6. Belyavskaya G., Mullen Gary L. Orthogonal hypercubes and n-ary operations // Quasigroups and Related Systems, vol. 13, no.1, 2005, 73-86.