On successively orthogonal systems of operations

Galina B. Belyavskaya

Seminar-2014 devoted V.D. Belousov

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

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

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.

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

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 $i = 1, 2, \ldots, k$.

Definition 1 [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 $a_1^k \in Q^k$.*

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 [1].

Definition 2 [1]. *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 [1]. *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.*

Definition 4. *A system $\Sigma = \{A_1^t\}$, $t \geq k$, of k-ary operations, given on a set Q, $\mid Q \mid \geq 3$, is called successively orthogonal system (briefly, a SOS) if any successive k operations are orthogonal.*

Every orthogonal set of k-operations is a successively orthogonal system.

Let (Q, A) be a quasigroup, $A^i(x, y) = A(x, A^{i-1}(x, y))$, $i = 2, \ldots$.

Theorem 1. *If $A, A_1, A_2, ..., A_t$ are binary quasigroups of the order $s_0, s_1, ..., s_t$ respectively, in the group $(\Lambda_2; \cdot)$ of all 2-invertible binary operations, given on a set Q, then the sequence*

$$F, E, A, A^2, ..., A^{s_0-1},\ F, E, A_1, A_1^2, ..., A_1^{s_1-1},$$

$$F, E, A_2, A_2^2, ..., A_2^{s_2-1}, ...,\ F, E, A_t, A_t^2, ..., A_t^{s_t-1}$$

is a SOS.

Proposition 1. *Let $\Sigma_1 = \{A_1, A_2, ..., A_{s_1}\}$, $\Sigma_2 = \{B_1, B_2, ..., B_{s_2}\}$ be strongly orthogonal sets of k-operations. Then the system*

$$\Sigma_3 = \{E_1, E_2, ..., E_k, A_1, A_2, ..., A_{s_1}, E_1, E_2, ..., E_k, B_1, B_2, ..., B_{s_2}\}$$

is a SOS.

Theorem 2. *Let A be an 1-invertible k-operation on a set Q, $\theta = (E_2, E_3, ..., E_k, A) = (E_2^k, A)$, and s_0 be the order of the permutation θ in the group S_{Q^k}, then the system of k-operations*

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

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

is successively orthogonal.

Corollary 1. *In the theorem 2 the k-operation $A\theta^{s_0-k-1}$ is k-invertible.*

In [2] for a function f: $Q^k \to Q$ it was defined a complete k-recursive code $K(n/f^{(0)}, f^{(1)}, ..., f^{(n-k-1)})$ with the check functions: $f^{(0)} = f, f^{(1)}, ..., f^{(n-k-1)}$. The function $f^{(i)}$ is called *the i-th recursive derivative* of a function f and is defined recursively as follows:

$f^{(0)}(x_1^k) = f(x_1^k)$, $f^{(1)}(x_1^k) = f(x_2^k, f^{(0)}(x_1^k)), ...,$
$f^{(i)}(x_1^k) = f(x_{i+1}^k, f^{(0)}(x_1^k), ..., f^{i-1}(x_1^k))$ for $i < k$, and
$f^{(i)}(x_1^k) = f(f^{(i-k)}(x_1^k), f^{(i-k+1)}(x_1^k), ..., f^{(i-1)}(x_1^k))$ for $i \geq k$.

V. Izbash and P. Syrbu in [3, Proposition 2] proved that if a k-operation f is a k-quasigroup, then $f^{(i)} = f\theta^i, i = 1, 2, ...,$ where

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

for all $(x_1^k) \in Q^k$.

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

A k-quasigroup we call *strongly recursively r-differentiable* if it is recursively r-differentiable and $r = s_0 - k - 1$, where s_0 is the order of the permutation $\theta = (E_2^k, A)$. In this case $A^{(r+1)} = E_1$. For the binary case this notion was introduced in [4]. From Theorem 2 we obtain the following corollary for any 1-invertible k-function f.

Corollary 2. *If f is an 1-invertible k-function, then*
$f^{(i)} = f\theta^{(i)}, i = 1, 2, ...,$ where $\theta = (E_2^k, f)$.
The sequence of the recursive derivatives has the form
$E_1, E_2, ..., E_k, f, f\theta, f\theta^2, ..., f\theta^{k-1}, f\theta^k, ..., f\theta^{s_0-k-1},$
$E_1, E_2, ..., E_k, f, f\theta, f\theta^2, ..., f\theta^{k-1}, f\theta^k, ..., f\theta^{s_0-k-1}, ...,$
where s_0 is the order of the permutation θ.
If f is an r-differentiable k-quasigroup, then $r \leq s_0 - k - 1$.
If a k-quasigroup is strongly recursively r-differentiable, then $r = s_0 - k - 1$.
For an 1-differentiable k-quasigroup $s_0 \geq k + 2$.

Theorem 3. *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.*

If $s_0 = k + 1$, then the k-operation A is a quasigroup k-operation.

For any 1-invertible k-operation $s_0 \geq k+1$.

Theorem 4. *Let $A, A_1, ..., A_t$ be 1-invertible k-operations and the permutations $\theta = (E_2^k, A)$, $\theta_1 = (E_2^k, A_1)$,..., $\theta_t = (E_2^k, A_t)$ have the order $s_0, s_1, ..., s_t$ respectively, then the system*

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

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

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

is a SOS.

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

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

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