BULETINUL ACADEMIEI DE ŞTIINŢE
A REPUBLICII MOLDOVA. MATEMATICA
Number 1(86), 2018, Pages 24–33
ISSN 1024–7696

Orthogonality and retract orthogonality of operations

Iryna Fryz

Abstract. In this article, we study connections between orthogonality and retract orthogonality of operations. We prove that if a tuple of operations is retractly orthogonal, then it is orthogonal. However, orthogonality of operations doesn't provide their retract orthogonality. Consequently, every k-tuple of orthogonal k-ary operations is prolongable to a k-tuple of orthogonal n-ary operations. Also, we give some specifications for central quasigroups. In particular for central quasigroups over finite field of prime order, retract orthogonality is the necessary and sufficient condition for orthogonality. The problem of coincidence of orthogonality and retract orthogonality remains open.

Mathematics subject classification: 20N05, 05B15.
Keywords and phrases: orthogonality of operations, retract orthogonality of operations, block-wise recursive algorithm, linear operation, central quasigroup.

Introduction

In quasigroup theory, the term "orthogonality" refers to several different notions which are generalizations of orthogonality of binary operations. Here, we will follow the definition of orthogonality of n-ary operations from [1]. For a description of various notions of orthogonality, see also [2, 3] or [4] and the references therein. Some algorithms for constructing orthogonal operations are described in [1, 5–7] and some relations with MDS-codes are given in [2–4, 8].

The detailed review of the theory of orthogonal binary operations ($n = 2$) is considered in [9]. But if $n > 2$, then many questions remain beyond attention, especially those which don't have analogues in the binary case. One of these questions is the orthogonality of retracts of operations.

In article [7], retract orthogonality concept was introduced as a tool of a block-wise recursive algorithm for constructing orthogonal n-ary operations. That is why, our purpose is to establish a connection between orthogonality and retract orthogonality.

In Section 2, we prove that if a tuple of operations is retractly orthogonal, then it is orthogonal (Theorem 5). However, the inverse statement is not true (Proposition 1). Consequently, Theorem 5 implies that every k-tuple of orthogonal k-ary operations is prolongable to a k-tuple of orthogonal n-ary operations (Lemma 1) and composition algorithm proposed in [7] constructs orthogonal operations which are retractly orthogonal (Theorem 3). We give some specifications for retractly orthogonal permutably reducible operations (Lemma 2 and Corollary 1).

In Section 3, we give some specifications of the obtained results for linear operations over an abelian group. In particular, Corollary 3 states that for central quasigroups over finite field of prime order, retract orthogonality is the necessary and sufficient condition for orthogonality. The problem of coincidence of orthogonality and retract orthogonality remains open.

1 Preliminaries

Throughout the article all operations are defined on the same arbitrary fixed set which is called carrier and is denoted by Q.

An operation f is called *i-invertible* if for arbitrary elements $a_1, \ldots, a_{i-1}, b, a_{i-1}, \ldots, a_n$ there exists a unique element x such that

$$f(a_1, \ldots, a_{i-1}, x, a_{i+1}, \ldots, a_n) = b. \tag{1}$$

If f is i-invertible for all $i \in \overline{1, n} := \{1, \ldots, n\}$, then it is called *an invertible* (*a quasigroup*) operation.

For each invertible operation f, *σ-parastrophe* ${}^{\sigma}\!f$ is defined by

$${}^{\sigma}\!f(x_{1\sigma}, \ldots, x_{n\sigma}) = x_{(n+1)\sigma} :\Longleftrightarrow f(x_1, \ldots, x_n) = x_{n+1},$$

where σ is a permutation of the set $\overline{1, n+1}$. In particular, a σ-parastrophe is called

- an *i-th division* if $\sigma = (i, n+1)$;
- *principal* if $(n+1)\sigma = n+1$.

It is clear that a principal σ-parastrophe can be defined by

$${}^{\sigma}\!f(x_1, \ldots, x_n) = f(x_{1\sigma^{-1}}, \ldots, x_{n\sigma^{-1}}). \tag{2}$$

Definition (see [1]). A tuple of n-ary operations $f_1, \ldots, f_k$ $(n \geqslant 2, k \leqslant n)$ defined on Q $(m := |Q|)$ is called *orthogonal* if for arbitrary $b_1, \ldots, b_k \in Q$ the system

$$\begin{cases} f_1(x_1, \ldots, x_n) = b_1, \\ \ldots\ldots\ldots\ldots\ldots\ldots \\ f_k(x_1, \ldots, x_n) = b_k \end{cases} \tag{3}$$

has exactly m^{n-k} solutions. For $n = k$, the tuple $f_1, \ldots, f_k$ is called *orthogonal* if the system (3) has a unique solution. For $k > n$, the tuple of operations is called orthogonal if every its n-subtuple is orthogonal.

Note if $k = 1$, then orthogonality concept coincides with completeness of operation, i. e., an operation f_1 is called *complete* if for all $b_1 \in Q$ the equation

$$f_1(x_1, \ldots, x_n) = b_1$$

has m^{n-1} solutions.

It is well known that an operation has an orthogonal mate if and only if it is complete.

Theorem 1 (see [1]). *A k-tuple ($k < n$) of orthogonal n-ary operations can be embedded into an n-tuple of orthogonal n-ary operations.*

Definition (see [1]). A t-tuple ($t \geqslant k$) of n-ary operations is called *k-wise orthogonal* if every k-tuple of distinct n-ary operations from this tuple is orthogonal.

Theorem 2 (see [1]). *If a t-tuple ($t \geqslant k$) of finite n-ary operations is k-wise orthogonal, then the tuple is ℓ-wise orthogonal for all ℓ such that $1 < \ell \leqslant k$.*

Let f be an n-ary operation defined on a set Q and let

$$\delta := \{i_1, \dots, i_k\} \subseteq \overline{1,n}, \quad \{j_1, \dots, j_{n-k}\} := \overline{1,n} \setminus \delta, \quad \bar{a} := (a_{j_1}, \dots, a_{j_{n-k}}) \in Q^{n-k}.$$

An operation $f_{(\bar{a},\delta)}$ which is defined by

$$f_{(\bar{a},\delta)}(x_{i_1}, \dots, x_{i_k}) := f(y_1, \dots, y_n),$$

where

$$y_i := \begin{cases} x_i \text{ if } i \in \delta, \\ a_i \text{ if } i \notin \delta, \end{cases}$$

is called an $(\bar{a},\delta)$-*retract* or a δ-*retract* of f.

Operations $f_{1;(\bar{a}_1,\delta)}$, $f_{2;(\bar{a}_2,\delta)}$, $\dots$, $f_{k;(\bar{a}_k,\delta)}$ are called *similar* δ-retracts of n-ary operations $f_1, f_2, \dots, f_k$ if $\bar{a}_1 = \bar{a}_2 = \dots = \bar{a}_k$.

Definition (see [7]). Let $\delta \subseteq \overline{1,n}$ and $|\delta| = k$. A k-tuple of n-ary operations is called *δ-retractly orthogonal*, if all tuples of similar δ-retracts of these operations are orthogonal.

If $\delta = \{i\}$, then δ-retract orthogonality of operation f degenerates into its i-invertibility. If $\delta = \overline{1,n}$, then retract orthogonality of $f_1, \dots, f_n$ is orthogonality.

The following algorithm constructs retractly orthogonal operations.

***Composition algorithm* [7].** *Let $\delta \subseteq \overline{1,n}$, $n \geqslant k$ and let $h_1, \dots, h_k$ be k-ary operations, $p_1, \dots, p_k$ be $(n-k+1)$-ary operations, $\sigma \in \mathrm{S}_n$.*

Operations ${}^{\sigma}\!f_1, \dots, {}^{\sigma}\!f_k$ are constructed by the following steps:

1) operations $f_1, \dots, f_k$ are defined by

$$\begin{cases} f_1(x_1, \dots, x_n) := p_1(h_1(x_1, \dots, x_k), x_{k+1}, \dots, x_n), \\ \dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots \\ f_k(x_1, \dots, x_n) := p_k(h_k(x_1, \dots, x_k), x_{k+1}, \dots, x_n); \end{cases} \tag{4}$$

2) operations ${}^{\sigma}\!f_1, \dots, {}^{\sigma}\!f_k$ are obtained from $f_1, \dots, f_k$ using (2).

Let $\mathrm{S}_n^{\delta} := \big\{\sigma \in \mathrm{S}_n \mid (\delta)\sigma = \{1, \dots, |\delta|\}\big\}$.

Theorem 3. *Let $p_1, \ldots, p_k$ be 1-invertible $(n-k+1)$-ary operations and $h_1, \ldots, h_k$ be k-ary orthogonal operations, $\sigma^{-1} \in \mathrm{S}_n^{\delta}$. Then operations ${}^{\sigma}\!f_1, \ldots, {}^{\sigma}\!f_n$ being constructed by composition algorithm are δ-retractly orthogonal.*

The symbol S_A refers to the set of all permutations of the set $A \subset \overline{1,n}$.

π-block-wise recursive algorithm [7]. *Let $\pi := \{\pi_1, \ldots, \pi_k\}$ be a partition of $\overline{1,n}$ and $f_1, \ldots, f_n$ be n-ary operations, $\tau_1 \in \mathrm{S}_{\pi_1}$, $\tau_2 \in \mathrm{S}_{\pi_1 \cup \pi_2}$, $\ldots$, $\tau_{k-1} \in \mathrm{S}_{\pi_1 \cup \cdots \cup \pi_{k-1}}$.*

Operations $g_1, \ldots, g_n$ are constructed by the following steps:

1) *the first block of operations is*

$$g_j(x_1, \ldots, x_n) := f_j(x_1, \ldots, x_n), \quad j \in \pi_1;$$

2) *for every $i = 2, \ldots, k$, the i-th block of operations is*

$$g_j(x_1, \ldots, x_n) := f_j(t_1, \ldots, t_n), \quad j \in \pi_i,$$

where

$$t_s := \begin{cases} g_{s\tau_{i-1}}(x_1, \ldots, x_n) & \text{if } s \in \pi_1 \cup \cdots \cup \pi_{i-1}, \\ x_s & \text{otherwise.} \end{cases}$$

A tuple of operations $f_1, \ldots, f_n$ is called π-*block retractly orthogonal* if for all $i \in \overline{1,k}$ a tuple $\{f_j \mid j \in \pi_i\}$ is π_i-retractly orthogonal.

Theorem 4 (see [7])**.** *Let operations $f_1, \ldots, f_n$ be π-block retractly orthogonal. Then the operations $g_1, \ldots, g_n$ constructed by π-block-wise recursive algorithm are orthogonal.*

2 Retract orthogonality and orthogonality

In this section, we establish some connections between orthogonality and retract orthogonality.

In article [7], the authors give only the definition of δ-retract orthogonality for the case when $|\delta|$ coincides with the number of operations in the tuple. Here we consider other cases.

Definition 1. Let $m := |Q|$, $\delta \subset \overline{1,n}$, $|\delta| = k$ and $t \in \overline{1,n}$ be such that $t < k < n$. A t-tuple of n-ary operations $f_1, \ldots, f_t$ on a set Q will be called *δ-retractly orthogonal* if all similar δ-retracts of the operations are orthogonal, i.e., for an arbitrary sequence $\bar{a} \in Q^{n-k}$ and arbitrary elements $b_1, \ldots, b_t \in Q$, the system

$$\begin{cases} f_{1;(\bar{a},\delta)}(x_{i_1}, \ldots, x_{i_k}) = b_1, \\ \dots\dots\dots\dots\dots\dots\dots\dots \\ f_{t;(\bar{a},\delta)}(x_{i_1}, \ldots, x_{i_k}) = b_t \end{cases}$$

has m^{k-t} solutions.

Definition 2. Let $\delta \subset \overline{1,n}$, $|\delta| = k$ and s be an integer such that $s > k$. An s-tuple of n-ary operations will be called *δ-retractly orthogonal* if each of its k-subtuples is δ-retractly orthogonal.

Definition 3. Let $\delta \subset \overline{1,n}$, $|\delta| = k$ and $\ell \in \overline{1,n}$ be such that $\ell < k$. A k-tuple of n-ary operations will be called *ℓ-wise δ-retractly orthogonal* if each of their ℓ-subtuples is δ-retractly orthogonal.

Theorem 5. *If for some $\delta \subset \overline{1,n}$, a tuple of n-ary operations is δ-retractly orthogonal, then the tuple is orthogonal.*

Proof. Suppose n-ary operations $f_1, \ldots, f_k$ are δ-retractly orthogonal. If $|\delta| =: k$, then consider a partition $\pi = \{\delta, \pi_2, \ldots, \pi_r\}$ of the set $\overline{1,n}$, where $\pi_2, \ldots, \pi_r$ are arbitrary pairwise disjoint subsets of the set $\overline{1,n} \backslash \delta$. By virtue of the π-block-wise recursive algorithm, the operations $f_1, \ldots, f_k$ can be taken as the first block of input operations. Then output operations are $f_1, \ldots, f_k, g_{k+1}, \ldots, g_n$, where $g_{k+1}, \ldots, g_n$ are n-ary operations obtained by items 2) – r) of the algorithm from blocks of arbitrary π_2-,…, π_r-retractly orthogonal operations. By Theorem 4, the operations $f_1, \ldots, f_k, g_{k+1}, \ldots, g_n$ are orthogonal, i.e., they are n-wise orthogonal. By Theorem 2, they are also ℓ-wise orthogonal for all $\ell < n$, consequently, for $\ell = k$ as well. From this, the tuple $f_1, \ldots, f_k, g_{k+1}, \ldots, g_n$ is k-wise orthogonal, i.e., each of its k-subtuples of operations is orthogonal, so the tuple $f_1, \ldots, f_k$ is also orthogonal.

If $|\delta| =: t$, where $k < t < n$, then by Theorem 1, every k-tuple of δ-retractly orthogonal n-ary operations can be embedded in a t-tuple of δ-retractly orthogonal n-ary operations. Therefore, there exists a $(t-k)$-tuple of n-ary operations $f_{k+1}, \ldots, f_t$ such that the t-tuple $f_1, \ldots, f_k, f_{k+1}, \ldots, f_t$ is δ-retractly orthogonal. As we have shown above, this tuple is orthogonal. Then by Theorem 2, each of its k-subtuples is orthogonal. $\square$

Let $|\delta| = k$ and $\ell < k$. By Theorem 5, retract orthogonality provides orthogonality, so ℓ-wise δ-retract orthogonality of a k-tuple of n-ary operations implies ℓ-wise orthogonality of the tuple, and δ-retract orthogonality of n-tuple of n-ary operations implies its k-wise orthogonality.

Let us show that the converse of Theorem 5 is not true.

Proposition 1. *There exist k-tuples of orthogonal n-ary operations ($k < n$) such that for some $\delta \subset \overline{1,n}$, where $|\delta| = k$, they are not δ-retractly orthogonal.*

Proof. Suppose the orthogonality of a k-tuple of n-ary operations implies that for all $|\delta| = k$ the tuple is δ-retractly orthogonal. i.e., orthogonality and δ-retract orthogonality are the same. If $k = 1$, then orthogonality of an operation means its completeness. On the other hand according to our assumption, for all $i \in \overline{1,n}$, the operation is $\{i\}$-retractly orthogonal, i.e. it is i-invertible, for all $i \in \overline{1,n}$. From this, a complete operation is a quasigroup operation, a contradiction.

Consider a counterexample for non-trivial case.

Example 1. Let g, h, t and p be 4-ary operations:

$$\begin{aligned} g(x_1,x_2,x_3,x_4) &= 2x_1 - 4x_2 + 2x_3 + 5x_4,\\ h(x_1,x_2,x_3,x_4) &= 4x_1 + 6x_2 + x_3 + 5x_4,\\ t(x_1,x_2,x_3,x_4) &= x_1 - x_2 + x_3 + x_4,\\ p(x_1,x_2,x_3,x_4) &= -x_1 + 2x_2 - 7x_3 + x_4 \end{aligned}$$

on $\mathbb{Z}_{20}$. It is easy to verify that they are orthogonal, therefore by Theorem 2 operations g and h are orthogonal as well. However, they are not δ-retractly orthogonal for each δ such that $|\delta| = 2$, because all corresponding to them determinants are not relatively prime to 20. Besides, all similar ternary retracts of g and h are not orthogonal either. But orthogonal operations h and t are not $\{1,2\}$-, $\{3,4\}$-retractly orthogonal and they are δ-retractly orthogonal for other possible cases.

Thus, we have shown that there exists a k-tuple of orthogonal n-ary operations such that for all $\delta \subset \overline{1,n}$, the tuple is not δ-retractly orthogonal. $\square$

A k-tuple of n-ary operations $f_1, \ldots, f_k$ $(k < n)$ constructed by (4) will be called *prolongation* of a k-tuple of orthogonal k-ary operations $h_1, \ldots, h_k$ to a k-tuple of n-ary operations, where $p_1, \ldots, p_k$ are arbitrary 1-invertible $(n-k+1)$-ary operations.

Lemma 1. *Every k-tuple of orthogonal k-ary operations is prolongable to a k-tuple of orthogonal n-ary operations.*

Proof. By Theorem 3, every prolongation of a k-tuple of orthogonal k-ary operations is $\overline{1,k}$-retractly orthogonal and by Theorem 5 the prolongation is orthogonal. Since there exists a k-tuple of 1-invertible $(n-k+1)$-ary operations, every k-tuple of orthogonal k-ary operations can be *prolonged* to a k-tuple of orthogonal n-ary operations. $\square$

Remark 1. Let $p_1, \ldots, p_k$ be arbitrary 1-invertible $(n-k+1)$-ary operations, $h_1, \ldots,$ h_k be arbitrary k-ary operations. According to Theorem 3 and Theorem 5,

1) operations $f_1, \ldots, f_k$ constructed by (4) are orthogonal, besides they are $\overline{1,k}$-retractly orthogonal if and only if $h_1, \ldots, h_k$ are orthogonal;

2) operations ${}^{\sigma}f_1, \ldots, {}^{\sigma}f_k$ being constructed by composition algorithm are δ-retractly orthogonal and they are orthogonal.

Remark 2. If we put bijective mappings $\alpha_1, \ldots, \alpha_k$ of Q onto Q instead of $p_1, \ldots,$ p_k in (4) respectively, the well-known statement follows: operations $\alpha_1 h_1, \ldots, \alpha_k h_k$ are orthogonal if and only if $h_1, \ldots, h_k$ are orthogonal.

Retract orthogonality of permutably reducible operations. An n-ary operation f will be called *δ-permutably reducible*, where $\delta = \{i_1, \dots, i_k\} \subset \overline{1,n}$, if there exist an s-invertible $(n-k)$-ary operation g and a k-ary operation h such that f can be represented as

$$f(x_1, \dots, x_n) = g(x_{j_1}, \dots, x_{j_{s-1}}, h(x_{i_1}, \dots, x_{i_k}), x_{j_{s+1}}, \dots, x_{j_{n-k+1}}).$$

Lemma 2. *Let $\delta \subset \overline{1,n}$, $|\delta| = k$ and each of the operations from a k-tuple of orthogonal n-ary operations be δ-permutably reducible. If there exists a tuple of similar orthogonal δ-retracts of operations of the tuple, then the k-tuple is δ-retractly orthogonal.*

Proof. Let

$$\delta = \{i_1, \dots, i_k\} \subseteq \overline{1,n}, \qquad \overline{1,n} \setminus \delta = \{j_1, \dots, j_{s-1}, j_{s+1}, \dots, j_{n-k+1}\}$$

and for all $i \in \overline{1,k}$, an n-ary operation f_i be δ-permutably reducible, i.e., there exist an s-invertible $(n-k)$-ary operation g_i and a k-ary operation h_i such that f_i can be represented as

$$f_i(x_1, \dots, x_n) = g_i(x_{j_1}, \dots, x_{j_{s-1}}, h_i(x_{i_1}, \dots, x_{i_k}), x_{j_{s+1}}, \dots, x_{j_{n-k+1}}).$$

Suppose there exists a tuple of orthogonal δ-retracts of operations $f_1, \dots, f_k$, i.e., there exists a tuple $\bar{a} = (a_{j_1}, \dots, a_{j_{s-1}}, a_{j_{s+1}}, \dots, a_{j_{n-k+1}}) \in Q^{n-k}$ such that for all $b_1, \dots, b_k$ the system

$$\begin{cases} g_1(a_{j_1}, \dots, a_{j_{s-1}}, h_1(x_{i_1}, \dots, x_{i_k}), a_{j_{s+1}}, \dots, a_{j_{n-k+1}}) = b_1, \\ \dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots \\ g_k(a_{j_1}, \dots, a_{j_{s-1}}, h_k(x_{i_1}, \dots, x_{i_k}), a_{j_{s+1}}, \dots, a_{j_{n-k+1}}) = b_k \end{cases} \tag{5}$$

has a unique solution. Since $g_1, \dots, g_k$ are s-invertible, their s-translations are bijective mappings of Q onto Q, i.e., for all $i \in \overline{1,k}$ a transformation α_i defined by

$$\alpha_i u := g_i(a_{j_1}, \dots, a_{j_{s-1}}, u, a_{j_{s+1}}, \dots, a_{j_{n-k+1}})$$

is a bijection of Q onto Q. Hence, the system (5) can be written as

$$\begin{cases} h_1(x_{i_1}, \dots, x_{i_k}) = \alpha_1^{-1} b_1, \\ \dots\dots\dots\dots\dots\dots\dots\dots \\ h_k(x_{i_1}, \dots, x_{i_k}) = \alpha_k^{-1} b_k. \end{cases}$$

Note that $\alpha_1^{-1} b_1, \dots, \alpha_k^{-1} b_k$ take all values on Q with $b_1, \dots, b_k$ simultaneously. This means that the uniqueness of solution of (5) doesn't depend on $\bar{a}$. Therefore, the system has a unique solution for all $\bar{a} \in Q^{n-k}$. Thus, the operations $f_1, \dots, f_k$ are δ-retractly orthogonal. $\square$

Summarizing Lemma 2 and Theorem 5, we have the following assertion.

Corollary 1. *Let $\delta \subset \overline{1,n}$, $|\delta| = k$ and each operation of a k-tuple of n-ary operations be δ-permutably reducible. Then if there exists a tuple of similar orthogonal δ-retracts of operations of the tuple, then the k-tuple is orthogonal.*

3 Orthogonality of linear operations

A *linear transformation* of a group is defined as a composition of its translations and automorphisms. An n-ary quasigroup (Q, f) is called an isotope of a binary group $(Q;+)$ if $(Q;f)$ is isotopic to $(Q;d)$, where $d(x_1,\ldots,x_n) := x_1+\cdots+x_n$. If all components of the isotopism are linear transformations over $(Q;+)$, then $(Q;f)$ is called *linear on* $(Q;+)$.

If an n-ary quasigroup f is linear on a group $(Q;+)$, then it has decomposition

$$f(x_1,\ldots,x_n) = \alpha_1 x_1 + \cdots + \alpha_n x_n + a,$$

where $a \in Q$ and $\alpha_1,\ldots,\alpha_n$ are automorphisms of $(Q;+)$. The decomposition is called *canonical* and $\alpha_1,\ldots,\alpha_n$ are called *decomposition automorphisms* [10]. A linear isotope of an abelian group is called a *central quasigroup* (or a T-quasigroup).

It is easy to verify that every linear operation over an abelian group is permutably reducible, i.e., it is a repetition-free composition of two linear operations over this group. Besides, each of the two variables can be separated. Thus, Lemma 2 and Corollary 1 are performed for linear operations over an abelian group.

Proposition 2. *Let $\delta = \{i_1,\ldots,i_k\} \subset \overline{1,n}$ and $\overline{1,n} \setminus \delta = \{j_1,\ldots,j_{n-k}\}$. Then n-ary linear operations $f_1,\ldots,\ f_k$ over an abelian group $(Q;+)$ are δ-retractly orthogonal if and only if for all $q \in \overline{1,k}$, each of these operations can be represented as*

$$f_q(x_1,\ldots,x_n) = p_q(h_q(x_{i_1},\ldots,x_{i_k}), x_{j_1},\ldots,x_{j_{n-k}}), \tag{6}$$

where $h_1,\ldots,\ h_k$ are orthogonal and $p_1,\ldots,\ p_k$ are 1-invertible.

Proof. Let for all $q \in \overline{1,k}$,

$$f_q(x_1,\ldots,x_n) := \alpha_{q1}x_1 + \cdots + \alpha_{qn}x_n + a_q, \tag{7}$$

where $\alpha_{q1},\ldots,\alpha_{qn}$ are linear transformations of $(Q;+)$ and $a_q \in Q$.

Suppose $f_1,\ldots,\ f_k$ are δ-retractly orthogonal. Since $(Q;+)$ is abelian, the equality (7) can be rewritten as

$$\begin{aligned} f_q(x_1,\ldots,x_n) = {} & \alpha_{qi_1}x_{i_1} + \cdots + \alpha_{qi_k}x_{i_k} + \\ & + \alpha_{qj_1}x_{j_1} + \cdots + \alpha_{qj_{n-k}}x_{j_{n-k}} + a_q. \end{aligned}$$

We can rewrite the last equality:

$$\begin{aligned} f_j(x_1,\ldots,x_n) = {} & \beta(\beta^{-1}\alpha_{qi_1}x_{i_1} + \cdots + \beta^{-1}\alpha_{qi_k}x_{i_k}) + \\ & + \alpha_{qj_1}x_{j_1} + \cdots + \alpha_{qj_{n-k}}x_{j_{n-k}} + a_q, \end{aligned}$$

where β is an arbitrary automorphism of $(Q;+)$. Hence for all $q \in \overline{1,k}$, the operation f_q has the form (6), where

$$h_q(x_{i_1},\ldots,x_{i_k}) := \beta^{-1}\alpha_{qi_1}x_{i_1} + \cdots + \beta^{-1}\alpha_{qi_k}x_{i_k},$$
$$p_q(u, x_{j_1},\ldots,x_{j_{n-k}}) := \beta u + \alpha_{qj_1}x_{j_1} + \cdots + \alpha_{qj_{n-k}}x_{j_{n-k}} + a_q.$$

Orthogonality of $h_1,\ldots,\ h_k$ follows from δ-retract orthogonality of $f_1,\ldots,\ f_k$ and Remark 2.

Sufficiency follows from Remark 1. □

Corollary 2. *Let $k \leqslant n$ and $f_1,\ \ldots,\ f_k$ be n-ary linear operations over $(\mathbb{Z}_m;+)$. If there exists a minor of the order k of the corresponding matrix for $f_1,\ \ldots,\ f_k$ which is relatively prime to m, then the operations are orthogonal.*

Proof. Suppose there exists a minor of order k of the corresponding matrix for operations $f_1,\ldots,\ f_k$ which is relatively prime to m. This minor is the corresponding determinant for some k-ary retracts of operations $f_1,\ \ldots,\ f_k$, i.e., $f_1,\ \ldots,\ f_k$ are retractly orthogonal. Then by Theorem 5, the operations $f_1,\ \ldots,\ f_k$ are orthogonal. □

Note there exist orthogonal linear operations over an abelian group which are not retractly orthogonal (see, Example 1). In particular, there exist such orthogonal central quasigroups over a group of non-prime order.

Corollary 3. *Let $k \leqslant n$ and p be a prime number. n-ary central quasigroups $f_1,\ \ldots,$ f_k over field $(\mathbb{Z}_p;+,\cdot)$ are orthogonal if and only if there exists δ such that $|\delta| = k$ and $f_1,\ \ldots,\ f_k$ are δ-retractly orthogonal.*

Proof. For all $i \in \overline{1,k}$, the quasigroup f_i has the form

$$f_i(x_1,\ldots,x_n) = a_{i1}x_1 + a_{i2}x_2 + \cdots + a_{in}x_n + a_i,$$

where $a_{i1}, a_{i2},\ldots,a_{in}$ are arbitrary invertible elements from $(\mathbb{Z}_p;+,\cdot)$ and $a_i \in \mathbb{Z}_p$.

Suppose $f_1,\ \ldots,\ f_k$ are orthogonal, this means that for all $b_1,\ldots,b_k \in \mathbb{Z}_p$ the system (3) has p^{n-k} solutions, i.e., $rank(A) = k$, where

$$A = \begin{pmatrix} a_{11} & a_{12} & \ldots & a_{1n} \\ a_{21} & a_{22} & \ldots & a_{2n} \\ \ldots & \ldots & \ldots & \ldots \\ a_{k1} & a_{k2} & \ldots & a_{kn} \end{pmatrix}.$$

Since $f_1,\ldots,\ f_k$ are orthogonal, there exists an invertible submatrix M of order k of matrix A. The matrix M corresponds to some k-tuple of k-ary δ-retracts of $f_1,\ \ldots,$ f_k, where $|\delta| = k$. By virtue of Corollary 2, the quasigroups $f_1,\ldots,\ f_k$ are δ-retractly orthogonal.

The sufficiency follows from Theorem 5. □

Example 2. Let p be a prime number, $a_1,\ \ldots,\ a_k$ be pairwise different and non-zero elements from $\mathbb{Z}_p$. If the corresponding matrix for n-ary central quasigroups $f_1,\ldots,$ f_k over $(\mathbb{Z}_p;+,\cdot)$, where $k \leqslant n$, is the Vandermonde matrix, i.e.,

$$\begin{pmatrix} 1 & a_1 & a_1^2 & \ldots & a_1^{k-1} \\ 1 & a_2 & a_2^2 & \ldots & a_2^{k-1} \\ \ldots & \ldots & \ldots & \ldots & \ldots \\ 1 & a_k & a_k^2 & \ldots & a_k^{k-1} \end{pmatrix},$$

and for every $i, j \in \overline{1,k}$, inequality $a_i \neq a_j$ holds, then $f_1, \ldots, f_k$ are $\overline{1,s}$-retractly orthogonal for all $s = 2, \ldots, n$.

References

[1] Belyavskaya G., Mullen G. L. *Orthogonal hypercubes and n-ary operations*, Quasigroups Related Systems, 2005, **13**, No. 1, 73–86.

[2] Gonzalez S., Couselo E., Markov V., Nechaev A. *Recursive MDS-codes and recursively differentiable quasigroups.* Discrete Math. Appl., 1998, **8**, No. 3 , 217–247.

[3] Dougherty S. T., Szczepanski T. A. *Latin k-hypercubes*, Australas. J. Combin., 2008, **40**, 145–160.

[4] Ethier J. T., Mullen G. L. *Strong forms of orthogonality for sets of hypercubes*, Discrete Math., 2012, **312**, 2050–2061.

[5] Evans T. *The construction of orthogonal k-skeins and latin k-cubes.* Aequationes Math., 1976, **14**, No. 3, 485–491.

[6] Trenkler M. *On orthogonal latin p-dimensional cubes.* Czechoslovak Math. J., 2005, **55(130)**, 725–728.

[7] Fryz I. V., Sokhatsky F. M. *Block composition algorithm for constructing orthogonal n-ary operations*, Discrete Math., 2017, **340**, 1957–1966; doi:10.1016/j.disc.2016.11.012.

[8] Soedarmadji E. *Latin hypercubes and MDS-codes.* Discrete Math., 2006, **306**, 1232–1239.

[9] Keedwell A. D., Denes J. *Latin Squares and their Applications*, Second edition, Amsterdam: North Holland, 2015, 438 p.

[10] Sokhatskyj F., Syvakivskyj P. *On linear isotopes of cyclic groups.* Quasigroups Related Systems, 1994, **1**, No. 1, 66–76.

Iryna Fryz
Vasyl' Stus Donetsk National University
600-richia str. 21
21021 Vinnytsia
Ukraine

E-mail: *iryna.fryz@ukr.net*

Received May 10, 2017
Revised December 2, 2017