

Iryna V. Fryz

Algorithm for the complement of orthogonal operations

Commentationes Mathematicae Universitatis Carolinae, Vol. 59 (2018), No. 2, 135–151

Persistent URL: <http://dml.cz/dmlcz/147247>

Terms of use:

© Charles University in Prague, Faculty of Mathematics and Physics, 2018

Institute of Mathematics of the Czech Academy of Sciences provides access to digitized documents strictly for personal use. Each copy of any part of this document must contain these *Terms of use*.



This document has been digitized, optimized for electronic delivery and stamped with digital signature within the project *DML-CZ: The Czech Digital Mathematics Library* <http://dml.cz>

Algorithm for the complement of orthogonal operations

IRYNA V. FRYZ

Abstract. G. B. Belyavskaya and G. L. Mullen showed the existence of a complement for a k -tuple of orthogonal n -ary operations, where $k < n$, to an n -tuple of orthogonal n -ary operations. But they proposed no method for complementing. In this article, we give an algorithm for complementing a k -tuple of orthogonal n -ary operations to an n -tuple of orthogonal n -ary operations and an algorithm for complementing a k -tuple of orthogonal k -ary operations to an n -tuple of orthogonal n -ary operations. Also we find some estimations of the number of complements.

Keywords: orthogonality of operations; retract orthogonality of operations; complement of orthogonal operations; block-wise recursive algorithm

Classification: 05B15, 20N05, 20N15

Introduction

Often 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 [3]. For a description of various notions of orthogonality, see also [4], [5] or [6] and the references therein.

The detailed review of the theory of orthogonal binary operations, i.e., for $n = 2$, is considered in [10]. But if $n > 2$, then many questions remain beyond attention, especially those which do not have analogues in binary case. One of these questions is orthogonality of retracts of operations which was given in [9] and described in [8]. Another important question is finding the complements of a k -tuple of orthogonal n -ary operations to an n -tuple of orthogonal n -ary operations, where $k < n$. In binary case, this problem has been solved. Besides, it has been shown that an operation has an orthogonal mate (an orthogonal complement) if and only if it is complete, therefore every method for constructing an orthogonal mate for an operation is a method of its complementing. In addition, if an operation is invertible (quasigroup), then it has an orthogonal quasigroup mate if and only if this quasigroup is admissible, see [10].

G. B. Belyavskaya and G. L. Mullen in [3] proved that for every k -tuple of orthogonal n -ary operations, where $k < n$, there exists a complement to an n -tuple of orthogonal n -ary operations. They proposed an algorithm for constructing

an n -tuple of orthogonal n -ary operations, however, no method for complementing was given. Also, other methods known to the author (see [2], [7], [13]) do not allow to find an orthogonal complement for a given tuple of orthogonal operations. The author and F. M. Sokhatsky in [9] suggested a generalization of G. B. Belyavskaya and G. L. Mullen’s algorithm, namely a block-wise recursive algorithm. This algorithm gives a possibility to construct a complement for a k -tuple of orthogonal n -ary operations to an n -tuple of orthogonal n -ary operations.

In Section 2, we give an algorithm for complementing a k -tuple of orthogonal n -ary operations to an n -tuple of orthogonal n -ary operations (Algorithm 1).

In Section 3, we describe retract orthogonality concept for hypercubes and illustrate the construction of orthogonal complements for orthogonal hypercubes (operations).

In Section 4, we prove necessary statements for finding some estimations of the number of complements for orthogonal operations of finite order, in particular, we find the number of all i -invertible n -ary operations (Lemma 8).

In Section 5, we find estimations for the number of trivial complements of a k -tuple of δ -retractly orthogonal n -ary operations, where $|\delta| = k$, to a $(k + r)$ -tuple of orthogonal n -ary operations (Theorem 11, Corollary 12, Corollary 13, Corollary 14), where $1 \leq r \leq n - k$.

In Section 6, we give an algorithm for complementing a k -tuple of orthogonal k -ary operations to an n -tuple of orthogonal n -ary operations (Algorithm 3) and we find the lower bound of the number of complements constructed by Algorithm 3.

1. Preliminaries

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

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

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

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

For each invertible operation f , a σ -parastrophe \mathcal{f} is defined by

$$\mathcal{f}(x_{1\sigma}, \dots, x_{n\sigma}) = x_{(n+1)\sigma} \iff f(x_1, \dots, x_n) = x_{n+1},$$

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

- an *ith 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

$$(2) \quad \mathcal{f}(x_1, \dots, x_n) = f(x_{1\sigma^{-1}}, \dots, x_{n\sigma^{-1}}).$$

Definition 1 ([3]). A tuple of n -ary operations f_1, \dots, f_k defined on Q , where $n \geq 2$, $k \leq n$, and $m := |Q|$, is called *orthogonal*, if a system

$$(3) \quad \begin{cases} f_1(x_1, \dots, x_n) = b_1, \\ \vdots \\ f_k(x_1, \dots, x_n) = b_k \end{cases}$$

has exactly m^{n-k} solutions for arbitrary $b_1, \dots, b_k \in Q$. If $n = k$, then the system (3) has a unique solution. For $k > n$, the operations are called *orthogonal*, if every n -subtuple of f_1, \dots, f_k is orthogonal.

If $k = 1$, then orthogonality concept coincides with completeness concept, i.e., an operation f_1 is called *complete*, if an equation

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

has m^{n-1} solutions for all $b_1 \in Q$.

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

Theorem 1 ([3]). *Every k -tuple of orthogonal n -ary operations ($k < n$) can be embedded into an n -tuple of orthogonal n -ary operations.*

Definition 2 ([3]). Let $k \leq n < s$. An s -tuple 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 ([3]). *Let $1 \leq k \leq n$. If k -tuple of n -ary operations is k -wise orthogonal, then the tuple is ℓ -wise orthogonal for all ℓ such that $1 \leq \ell < k$.*

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

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

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}, δ) -*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 3 ([9]). A k -tuple of n -ary operations, where $k > n$, 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_i degenerates into its i -invertibility. If $\delta = \overline{1, n}$, then retract orthogonality of f_1, \dots, f_n is orthogonality.

Theorem 5 ([8]). *If for some $\delta \subset \overline{1, n}$ a tuple of n -ary operations is δ -retractly orthogonal, then the tuple is orthogonal.*

Proposition 6 ([8]). *Let $k < n$. Then there exist k -tuples of orthogonal n -ary operations such that for some $\delta \subset \overline{1, n}$, $|\delta| = k$, they are not δ -retractly orthogonal.*

2. Construction of complements for orthogonal operations

Theorem 1 and Theorem 2 mean that for every k -tuple of orthogonal n -ary operations f_1, \dots, f_k there exists an $(n - k)$ -tuple of orthogonal n -ary operations f_{k+1}, \dots, f_n such that n -tuple f_1, \dots, f_n is orthogonal. By virtue of Definition 1, every complete n -ary operation can be embedded into an n -tuple of orthogonal n -ary operations. For the complement of orthogonal operations, the method proposed in [3] can be used, but only in the case $k = 1$ and this complete operation has to be n -invertible. An algorithm for complementing a k -tuple of orthogonal n -ary operations is unknown. However for a k -tuple of retractly orthogonal n -ary operation, the algorithm from [9] is successfully applicable. Remark that the difference between orthogonality and retract orthogonality is described in Theorem 5 and Proposition 6, namely, retract orthogonality implies orthogonality, but the inverse statement is not true.

An arbitrary k -tuple of δ -retractly orthogonal n -ary operations, where $|\delta| = k$, can be complemented to an n -tuple of orthogonal n -ary operations using a block-wise recursive algorithm.

Algorithm 1. Let $\delta = \{i_1, \dots, i_k\} \subset \overline{1, n}$, $|\delta| = k$ and g_{i_1}, \dots, g_{i_k} be δ -retractly orthogonal n -ary operations.

Operations $g_{i_{k+1}}, \dots, g_{i_n}$ are constructed by the following items:

- 1) choose arbitrary n -ary operations $f_{i_{k+1}}, \dots, f_{i_n}$ such that for every $r \in \overline{2, q}$ a tuple $\{f_j : j \in \pi_r\}$ is π_r -retractly orthogonal, i.e., the corresponding partition of $\overline{1, n}$ is $\pi := \{\delta, \pi_2, \dots, \pi_q\}$, and permutations $\tau_1 \in S_\delta$, $\tau_2 \in S_{\delta \cup \pi_2}, \dots, \tau_{q-1} \in S_{\delta \cup \pi_2 \cup \dots \cup \pi_{q-1}}$;
- 2) for every $j \in \pi_2$, the operation g_j is constructed by

$$(5) \quad g_j(x_1, \dots, x_n) := f_j(t_1, \dots, t_n),$$

where

$$t_s := \begin{cases} g_{s\tau_1}(x_1, \dots, x_n) & \text{if } s \in \delta, \\ x_s & \text{otherwise;} \end{cases}$$

- r) for every $j \in \pi_r$, $r = 3, \dots, q$, the operation g_j is constructed by (5), where

$$t_s := \begin{cases} g_{s\tau_{r-1}}(x_1, \dots, x_n) & \text{if } s \in \delta \cup \pi_2 \cup \dots \cup \pi_{r-1}, \\ x_s & \text{otherwise.} \end{cases}$$

Theorem 7. *An $(n - k)$ -tuple of n -ary operations $g_{i_{k+1}}, \dots, g_{i_n}$ constructed by Algorithm 1 is a complement of a k -tuple of δ -retractly orthogonal n -ary operations g_{i_1}, \dots, g_{i_k} to an n -tuple of orthogonal n -ary operations.*

PROOF: The proof follows immediately from Theorem 4, if we take δ as the first block of a defining partition of the set $\overline{1, n}$ for a block-wise recursive algorithm. \square

Note that Algorithm 1 gives a possibility to complement a given k -tuple of δ -retractly orthogonal n -ary operations to a $(k + r)$ -tuple of orthogonal n -ary operations for all $r \in \overline{1, n - k}$. This follows from Theorem 2.

3. Orthogonal complements for hypercubes

It is well known that to every n -ary operation of order m there corresponds an n -dimensional hypercube (n -cube) of order m , i.e., an n -dimensional array on m distinct symbols; and to a k -tuple of orthogonal n -ary operations there corresponds a k -tuple of orthogonal n -cubes, $k \leq n$, i.e., under their superimposition, each of the m^n ordered k -sequences of symbols occurs exactly m^{n-k} times, see [3].

Let $\delta \subset \overline{1, n}$ and $|\delta| = k$. A k -cube H_δ is called a δ -subhypercube of an n -cube H , if it is obtained from H by fixing the $n - k$ coordinates with indices from $\overline{1, n} \setminus \delta$. To every k -ary retract of an n -ary operation there corresponds a k -dimensional subhypercube of the corresponding n -cube. If $\delta = \{i, j\}$, then H_δ is called an $\{i, j\}$ -slice of H . If $\delta = \{i\}$, then a δ -subhypercube is called an i -line. For each $i \in \overline{1, n}$, there are m^{n-1} i -lines. If an i -line is a permutation of $\overline{1, n}$, then the line is called *Latin*. If each of the i -lines of a hypercube is Latin one, then the corresponding operation is i -invertible.

For example in a square, 1-lines are columns and 2-lines are rows. There are m rows and m columns in a square of order m . In a cube, 1-lines are obtained when the second and the third coordinates are fixed, 2-lines when the first and the third coordinates are fixed and 3-lines when the first and the second coordinates are fixed. The number of i -lines is m^2 for every $i \in \{1, 2, 3\}$ and the number of $\{1, 2\}$ -slices ($\{1, 3\}$ -slices, $\{2, 3\}$ -slices) is m .

Every cube on Q can be presented by its $\{i, j\}$ -slices for fixed $i, j \in \{1, 2, 3\}$. Let $G_{(\{1,2\},a)}$ refer to the $\{1, 2\}$ -slice of G when the third coordinate is fixed by $a \in Q$. For example, let us present cube G on the set $\{1, 2, 3\}$ by $\{1, 2\}$ -slices:

G :	$G_{(\{1,2\},0)}$	$G_{(\{1,2\},1)}$	$G_{(\{1,2\},2)}$																											
	<table border="1" style="border-collapse: collapse; text-align: center;"> <tr><td>0</td><td>0</td><td>1</td></tr> <tr><td>1</td><td>1</td><td>2</td></tr> <tr><td>2</td><td>0</td><td>2</td></tr> </table>	0	0	1	1	1	2	2	0	2	<table border="1" style="border-collapse: collapse; text-align: center;"> <tr><td>0</td><td>2</td><td>1</td></tr> <tr><td>2</td><td>2</td><td>0</td></tr> <tr><td>1</td><td>0</td><td>1</td></tr> </table>	0	2	1	2	2	0	1	0	1	<table border="1" style="border-collapse: collapse; text-align: center;"> <tr><td>0</td><td>0</td><td>2</td></tr> <tr><td>1</td><td>2</td><td>0</td></tr> <tr><td>1</td><td>2</td><td>1</td></tr> </table>	0	0	2	1	2	0	1	2	1
0	0	1																												
1	1	2																												
2	0	2																												
0	2	1																												
2	2	0																												
1	0	1																												
0	0	2																												
1	2	0																												
1	2	1																												

Subhypercubes $H_{1,\delta}, \dots, H_{k,\delta}$ of order m of hypercubes H_1, \dots, H_k are called *similar*, if each of them is defined by fixing all coordinates from $\overline{1, n} \setminus \delta$ by the same elements.

Definition 3 can be reformulated for hypercubes: hypercubes H_1, \dots, H_k are called δ -retractly orthogonal, if all their similar subhypercubes $H_{1,\delta}, \dots, H_{k,\delta}$ are orthogonal. For example, cube H on $\{1, 2, 3\}$ with its $\{1, 2\}$ -slices:

$$H: \begin{array}{|c|c|c|} \hline 0 & 2 & 2 \\ \hline 0 & 1 & 1 \\ \hline 0 & 1 & 2 \\ \hline \end{array} \quad \begin{array}{|c|c|c|} \hline 0 & 0 & 0 \\ \hline 1 & 2 & 1 \\ \hline 2 & 2 & 1 \\ \hline \end{array} \quad \begin{array}{|c|c|c|} \hline 1 & 0 & 1 \\ \hline 2 & 0 & 2 \\ \hline 0 & 2 & 1 \\ \hline \end{array}$$

and G are $\{1, 2\}$ -retractly orthogonal. Indeed, let us superimpose the similar $\{1, 2\}$ -retracts of G and H :

$$\begin{array}{|c|c|c|} \hline 00 & 02 & 12 \\ \hline 10 & 11 & 21 \\ \hline 20 & 01 & 22 \\ \hline \end{array} \quad \begin{array}{|c|c|c|} \hline 00 & 20 & 10 \\ \hline 21 & 22 & 01 \\ \hline 12 & 02 & 11 \\ \hline \end{array} \quad \begin{array}{|c|c|c|} \hline 01 & 00 & 21 \\ \hline 12 & 20 & 02 \\ \hline 10 & 22 & 11 \\ \hline \end{array}$$

In each of these squares, every pair occurs exactly once, i.e., the similar $\{1, 2\}$ -slices are orthogonal, therefore G and H are $\{1, 2\}$ -retractly orthogonal. G and H are orthogonal because in all these squares of pairs every pair occurs exactly thrice. Their orthogonality follows from Theorem 5 as well.

Note that all given statements can be reformulated for hypercubes. Thus, Algorithm 1 is applicable for the complement of orthogonal hypercubes. In the following example, we illustrate the construction of a complement for a pair of orthogonal cubes to a triplet of orthogonal cubes.

Example 1. Let G and H be the given $\{1, 2\}$ -retractly orthogonal cubes. In order to complement this pair to a triplet of orthogonal cubes according to step (1) of Algorithm 1, we have to choose an arbitrary cube, each of its 3-lines is Latin, for example, cube L with its $\{1, 2\}$ -slices:

$$L: \begin{array}{|c|c|c|} \hline 0 & 0 & 2 \\ \hline 1 & 2 & 0 \\ \hline 2 & 1 & 1 \\ \hline \end{array} \quad \begin{array}{|c|c|c|} \hline 1 & 2 & 1 \\ \hline 0 & 1 & 1 \\ \hline 0 & 2 & 2 \\ \hline \end{array} \quad \begin{array}{|c|c|c|} \hline 2 & 1 & 0 \\ \hline 2 & 0 & 2 \\ \hline 1 & 0 & 0 \\ \hline \end{array}$$

Since G and H are $\{1, 2\}$ -retractly orthogonal, the first block of the corresponding partition for the algorithm is $\{1, 2\}$ and then the second one is $\{3\}$, i.e., $\pi = \{\{1, 2\}, \{3\}\}$.

Then by step (2) we have to construct cube K by cube L using the formula

$$K(x, y, z) := L(G(x, y, z), H(x, y, z), z):$$

$$K: \begin{array}{|c|c|c|} \hline 0 & 2 & 0 \\ \hline 1 & 2 & 1 \\ \hline 2 & 0 & 1 \\ \hline \end{array} \quad \begin{array}{|c|c|c|} \hline 1 & 0 & 0 \\ \hline 2 & 2 & 2 \\ \hline 1 & 1 & 1 \\ \hline \end{array} \quad \begin{array}{|c|c|c|} \hline 1 & 2 & 0 \\ \hline 2 & 1 & 0 \\ \hline 2 & 0 & 0 \\ \hline \end{array}$$

Let us superimpose cubes G, H, K :

000	022	120
101	112	211
202	010	221

001	200	100
212	222	012
121	021	111

011	002	210
122	201	020
102	220	110

In the obtained cube, every ordered triplet occurs exactly once. This means orthogonality of G, H, K . By Theorem 7, they are orthogonal as well.

4. Additional statements

Let us define the function p on pairs of positive integers:

$$p(1, s) := 1! \cdot 2! \cdot 3! \cdot \dots \cdot s!$$

We can rewrite it in the following way

$$(6) \quad p(1, s) = 2^{s-1} \cdot 3^{s-2} \cdot \dots \cdot (s-1)^2 \cdot s.$$

Thus, we have

$$1! \cdot 2! \cdot 3! \cdot \dots \cdot s! = \prod_{j=1}^s j^{s-j+1}.$$

Then

$$\begin{aligned} p(k, s) &:= k! \cdot (k+1)! \cdot \dots \cdot s! \\ &= 2^{s-k+1} \cdot \dots \cdot k^{s-k+1} \cdot (k+1)^{s-k} \cdot \dots \cdot (s-1)^2 \cdot s. \end{aligned}$$

Consequently,

$$(7) \quad k! \cdot (k+1)! \cdot \dots \cdot s! = \prod_{j=1}^k j^{s-k+1} \prod_{j=k+1}^s j^{s-j+1}.$$

Formula (6) is a partial case of (7). If $k = 1$ in (7), then

$$\prod_{j=1}^1 j^{s-1+1} = 1.$$

Lemma 8. For every $i \in \overline{1, n}$, the number of i -invertible n -ary operations on a set Q of order m is $(m!)^{m^{n-1}}$, where $m > 1$ and $n \geq 1$.

PROOF: Let Q be an arbitrary set, $m := |Q| < \infty$ and S_Q be a group of all bijective mappings of Q upon Q . Therefore $|S_Q| = m!$. If f is an i -invertible n -ary operation on Q , then the transformation α_i such that

$$\alpha_i(x) := f(a_1, \dots, a_{i-1}, x, a_{i+1}, \dots, a_n)$$

is a bijective mapping of Q upon Q , i.e., every bijection from S_Q has this form.

Define a mapping $\lambda_i: Q^{n-1} \rightarrow S_Q$ in the following way:

$$\lambda_i(x_1, \dots, x_{i-1}, x_{i+1}, \dots, x_n)(x) := f(x_1, \dots, x_{i-1}, x, x_{i+1}, \dots, x_n).$$

This relationship establishes biunique correspondence between i -invertible n -ary operations on Q and mappings of $Q^{n-1} \rightarrow S_Q$. It is clear that $|Q^{n-1}| = m^{n-1}$. Therefore $|\Lambda_i| = (m!)^{m^{n-1}}$, where

$$\Lambda_i = \{\lambda_i: \lambda_i: Q^{n-1} \rightarrow S_Q\}.$$

We have shown that the number of all bijections from Λ_i and the number of i -invertible n -ary operations on Q are the same and it is $(m!)^{m^{n-1}}$. \square

Example 2. For some cases, the truth of the statement of Lemma 8 is evident. In the case when m is an arbitrary and $n = 1$, every invertible unary operation is a bijective mapping of Q upon Q , so their number is $m!$. In the case $m = 2$ and $n = 2$, there exist exactly 6 complete binary Boolean operations (complete squares of order 2). There are 4 left (right) invertible operations among them, including 2 quasigroups. In the case $m = 2$ and $n = 3$, every slice of a cube of order two is a square of order two, therefore we can find all ternary 1-invertible Boolean operations using binary 1-invertible operations. Since their number is 4, the number of all 1-invertible ternary Boolean operations is $4^2 = 16$.

Note that intersection of all sets of 1-, 2-, ..., n -invertible n -ary operations on Q is a class of all n -ary quasigroups on Q .

A k -tuple of n -ary operations f_1, \dots, f_k , $k < n$, constructed by (4) is called *prolongation* of a k -tuple of orthogonal k -ary operations h_1, \dots, h_k to a k -tuple of n -ary operations, where p_1, \dots, p_k are arbitrary 1-invertible $(n - k + 1)$ -ary operations. Besides, it is proved that each of the prolongations is a k -tuple of orthogonal n -ary operations, see [8].

Lemma 9. *For every s -tuple of orthogonal k -ary operations on a set Q of order m , $k \geq 2$, $s \leq k$, $k < n$, $m \geq 2$, there exist exactly $(m!)^{s m^{n-k}}$ different prolongations to an s -tuple of orthogonal n -ary operations.*

In the case $k = n$, we obtain orthogonal k -ary operations again.

PROOF: In order to prolong s -tuple of orthogonal k -ary operations on Q of order m by (4), we have to take an s -tuple of 1-invertible $(n - k + 1)$ -ary operations, besides some operations of this tuple can coincide. By Lemma 8, the number of 1-invertible $(n - k + 1)$ -ary operations is $(m!)^{m^{n-k}}$, therefore the number of s -tuples of 1-invertible $(n - k + 1)$ -ary operations is $(m!)^{s m^{n-k}}$. \square

If $s = k$, then there are $(m!)^{k m^{n-k}}$ different prolongations of a k -tuple of orthogonal k -ary operations to a k -tuple of orthogonal n -ary operations.

5. Estimations of the number of complements of δ -retractly orthogonal operations

The number of complements of a given tuple of orthogonal n -ary operations to an n -tuple of orthogonal n -ary operations is unknown, but we can find some of its estimations.

Two complements of the same tuple of orthogonal operations will be called *different*, if they differ in at least one operation. For arbitrary $\sigma \in S_n$, k -tuples of operations f_1, \dots, f_k and $f_{1\sigma}, \dots, f_{k\sigma}$ are assumed to be the same.

Trivial complements. The simplest and the most studied complements of orthogonal operations are trivial complements. To construct trivial complements, it is enough to have only operations which are one-sided invertible in all different places not belonging to δ and we add exactly one operation for every step. Recall that if $\pi = \{\{n\}, \{n-1\}, \dots, \{1\}\}$ in Algorithm 1, then we have an algorithm for complementing an n -ary n -invertible operation to an n -tuple of orthogonal n -ary operations which trivially follows from the algorithm for construction of orthogonal operations from [3]. Some modifications of this algorithm were considered in [11], i.e., for all other trivial partitions of the set $\overline{1, n}$. All these algorithms are partial cases of a block-wise recursive algorithm when the partitions are trivial and they are called *trivial recursive algorithms*.

Combining Algorithm 1 with a trivial recursive algorithm, we formulate an algorithm for trivial complementing.

Algorithm 2. Let g_{i_1}, \dots, g_{i_k} be δ -retractly orthogonal n -ary operations, where $\delta = \{i_1, \dots, i_k\} \subset \overline{1, n}$.

Operations $g_{i_{k+1}}, \dots, g_{i_n}$ are constructed by the following items:

- r₀) choose arbitrary n -ary operations $f_{i_{k+1}}, \dots, f_{i_n}$ such that for all $r \in \overline{1, n-k}$ the operation $f_{i_{k+r}}$ is i_{k+r} -invertible and permutations $\tau_1 \in S_\delta$, $\tau_2 \in S_{\delta \cup \{i_{k+1}\}}, \dots, \tau_{n-k} \in S_{\delta \cup \{i_{k+1}\} \cup \dots \cup \{i_{n-k}\}}$;
- 1) the first operation $g_{i_{k+1}}$ is constructed by

$$g_{i_{k+1}}(x_1, \dots, x_n) := f_{i_{k+1}}(t_1, \dots, t_n),$$

where

$$t_s := \begin{cases} g_{s\tau_1}(x_1, \dots, x_n) & \text{if } s \in \delta, \\ x_s & \text{otherwise;} \end{cases}$$

- r) the operation $g_{i_{k+r}}, r = 2, \dots, n-k$, is constructed by

$$g_{i_{k+r}}(x_1, \dots, x_n) := f_{i_{k+r}}(t_1, \dots, t_n),$$

where

$$t_s := \begin{cases} g_{s\tau_{r-1}}(x_1, \dots, x_n) & \text{if } s \in \delta \cup \{i_{k+1}\} \cup \dots \cup \{i_{k+r-1}\}, \\ x_s & \text{otherwise.} \end{cases}$$

Corollary 10. *Every k -tuple of δ -retractly orthogonal n -ary operations, where $|\delta| = k$, is trivially complementable (i.e., by Algorithm 2) to an n -tuple of orthogonal n -ary operations.*

PROOF: If in Algorithm 1, blocks π_2, \dots, π_q are singletons, then $q = n - k + 1$. Denoting $\pi_2 := \{i_{k+1}\}, \dots, \pi_{n-k+1} := \{i_n\}$, we have a defining partition $\pi' = \{\delta, \{i_{k+1}\}, \dots, \{i_n\}\}$ of the set $\overline{1, n}$. Algorithm 2 is obtained by reformulating Algorithm 1 for π' . By virtue of Theorem 7, a tuple of operations constructed by Algorithm 2 is a complement of a given k -tuple of δ -retractly orthogonal n -ary operations to an n -tuple of orthogonal n -ary operations. Since for any integer n and for any $k \in \overline{1, n}$ there exists an $(n - k)$ -tuple of i_{k+1}, \dots, i_n -invertible operations, every tuple of δ -retractly orthogonal n -ary operations is complementable by Algorithm 2 to an n -tuple of orthogonal n -ary operations. \square

Estimation. Let $\mathfrak{C}_n(k, s; m)$ refer to the number of all different complements constructed by Algorithm 1 of a k -tuple of δ -retractly orthogonal n -ary operations on Q to an s -tuple of orthogonal n -ary operations, and $\mathfrak{c}_n(k, s; m)$ denote the number of all different trivial complements of a k -tuple of δ -retractly orthogonal n -ary operations on a set Q to an s -tuple of orthogonal n -ary operations, where $|Q| = m, |\delta| = k, k < s \leq n$.

Theorem 11. *Let $m = |Q|, k = |\delta|, k \geq 1, n \geq 2, m \geq 2$ and $1 \leq r \leq n - k$. Then*

$$\frac{(m!)^{rm^{n-1}}}{r!} < \mathfrak{c}_n(k, k + r; m) < \frac{(n - k)!(m!)^{rm^{n-1}}}{(n - k - r)!} \prod_{j=1}^k j^r \prod_{j=k+1}^{k+r} j^{k+r-j}.$$

PROOF: Suppose $\delta = \{i_1, \dots, i_k\}$ and $(g_{i_1}, \dots, g_{i_k})$ is an arbitrary fixed ordered k -tuple of δ -retractly orthogonal n -ary operations on Q . By Theorem 5, this tuple of operations is orthogonal.

Let us find the lower bound of $\mathfrak{c}_n(k, k + r; m)$, where $1 \leq r \leq n - k$. Suppose for every $q \in \overline{1, r}$,

$$\Delta := \delta \cup \{i_{k+1}\} \cup \dots \cup \{i_{k+q-1}\}.$$

Note that if $q = 1$, then $i_{k+q-1} = i_k$. Therefore $i_k \in \delta$ implies $\Delta = \delta$.

For arbitrary i_{k+q} -invertible n -ary operation $f_{i_{k+q}}$, we construct n -ary operation $g_{i_{k+q}}$ by

$$(8) \quad g_{i_{k+q}}(x_1, \dots, x_n) := f_{i_{k+q}}(t_1, \dots, t_n), \quad q = 1, \dots, r,$$

where $i_{k+q} \in \overline{1, n} \setminus \delta \cup \{i_{k+1}\} \cup \dots \cup \{i_{k+q-1}\}$ and

$$t_i := \begin{cases} g_i & \text{if } i \in \Delta, \\ x_i & \text{if } i \notin \Delta. \end{cases}$$

By Algorithm 2 and Corollary 10, the tuple $(g_{i_1}, \dots, g_{i_k}, g_{i_{k+1}}, \dots, g_{i_{k+q}})$ is orthogonal. Remark that for every $q \in \overline{1, r}$, we add exactly one operation using an i_{k+q} -invertible n -ary operation.

Suppose $(g_{i_1}, \dots, g_{i_k}, g_{i_{k+1}}, \dots, g_{i_{k+q-1}}, g'_{i_{k+q}})$ is another tuple of orthogonal operations, where $g'_{i_{k+q}}$ is constructed by (8) from another i_{k+q} -invertible operation $f'_{i_{k+q}}$:

$$g'_{i_{k+q}}(x_1, \dots, x_n) := f'_{i_{k+q}}(t_1, \dots, t_n).$$

Show that

$$\begin{aligned} &(g_{i_1}, \dots, g_{i_k}, g_{i_{k+1}}, \dots, g_{i_{k+q-1}}, g_{i_{k+q}}) \\ &\neq (g_{i_1}, \dots, g_{i_k}, g_{i_{k+1}}, \dots, g_{i_{k+q-1}}, g'_{i_{k+q}}) \end{aligned}$$

if and only if $f_{i_{k+q}} \neq f'_{i_{k+q}}$.

Indeed, suppose

$$\begin{aligned} &(g_{i_1}, \dots, g_{i_k}, g_{i_{k+1}}, \dots, g_{i_{k+q-1}}, g_{i_{k+q}}) \\ &= (g_{i_1}, \dots, g_{i_k}, g_{i_{k+1}}, \dots, g_{i_{k+q-1}}, g'_{i_{k+q}}), \end{aligned}$$

so $g_{i_{k+q}} = g'_{i_{k+q}}$, i.e., $f_{i_{k+q}}(t_1, \dots, t_n) = f'_{i_{k+q}}(t_1, \dots, t_n)$. Because the tuple $(g_{i_1}, \dots, g_{i_k}, g_{i_{k+1}}, \dots, g_{i_{k+q}})$ is orthogonal, it takes all values from Q^{k+q} . This means that the tuple (t_1, \dots, t_n) takes all values from Q^n . Therefore, $f_{i_{k+q}} = f'_{i_{k+q}}$. The inverse statement is evident.

Thus for every $q \in \overline{1, r}$, the number of all different complements of a $(k+q-1)$ -tuple of orthogonal operations constructed by (8) via i_{k+q} -invertible operation is equal to the number of all i_{k+q} -invertible n -ary operations on Q of order m and it is $(m!)^{m^{n-1}}$ according to Lemma 8. Consequently, there exist at least $(m!)^{m^{n-1}}$ different complements of a $(k+q-1)$ -tuple of orthogonal n -ary operations to a $(k+q)$ -tuple of orthogonal n -ary operations.

We iterate these steps r times until we reach a $(k+r)$ -tuple of orthogonal n -ary operations and therefore the number of tuples of the form

$$(f_{i_1}, \dots, f_{i_k}, g_{i_{k+1}}, \dots, g_{i_{k+r}})$$

is $(m!)^{rm^{n-1}}$. Suppose among constructed tuples of operations there exists one more tuple $(g'_{i_{k+1}}, \dots, g'_{i_{k+r}})$ such that

$$(g'_{i_{k+1}}, \dots, g'_{i_{k+r}}) = (g_{i_{(k+1)\sigma}}, \dots, g_{i_{(k+r)\sigma}}),$$

where $\sigma \in S_r$, i.e., we obtain the same complement twice. The maximal number of all possible repetitions is $r!$. Consequently,

$$c_n(k, k+r; m) > \frac{(m!)^{rm^{n-1}}}{r!}.$$

Now we consider the upper bound of $\mathbf{c}_n(k, k + r; m)$. Using permutations from the sets $S_\delta, S_{\delta \cup \{i_{k+1}\}}, \dots, S_{\delta \cup \{i_{k+1}\} \cup \dots \cup \{i_{k+r-1}\}}$, we also receive orthogonal operations by the block-wise recursive algorithm. Since

$$|S_\delta| = k!, \quad |S_{\delta \cup \{i_{k+1}\}}| = (k + 1)!, \quad \dots, \quad |S_{\delta \cup \{i_{k+1}\} \cup \dots \cup \{i_{k+r-1}\}}| = (k + r - 1)!,$$

we have also

$$k! \cdot (k + 1)! \cdot \dots \cdot (k + r - 1)! \stackrel{(7)}{=} \prod_{j=1}^k j^r \prod_{j=k+1}^{k+r} j^{k+r-j}$$

ways for constructing the complements.

For every $q \in \overline{1, r}, i_{k+q} \in \overline{1, n} \setminus \Delta$, therefore there exist $n - k - q + 1$ ways to choose i_{k+q} , i.e.,

$$(n - k) \cdot \dots \cdot (n - k - r + 1) = \frac{(n - k)!}{(n - k - r)!}$$

ways to choose a tuple $(i_{k+1}, \dots, i_{k+r})$ without repetitions of its elements. Since for every $i, j \in \overline{1, n}, i \neq j$, the classes of i -invertible and j -invertible n -ary operations have a nonempty intersection, we have inequality

$$\mathbf{c}_n(k, k + r; m) < \frac{(n - k)!(m!)^{rm^{n-1}}}{(n - k - r)!} \prod_{j=1}^k j^r \prod_{j=k+1}^{k+r} j^{k+r-j}.$$

□

The following corollary gives estimations for the number of complements of a k -tuple of δ -retractly orthogonal n -ary operations to a $(k + 1)$ -tuple of orthogonal n -ary operations if $k + 1 \neq n$.

Corollary 12. *Let $m = |Q|, k = |\delta|, k \geq 1, n \geq 3, m \geq 2$ and $k + 1 \neq n$. Then*

$$(m!)^{m^{n-1}} < \mathbf{c}_n(k, k + 1; m) < (n - k)k!(m!)^{m^{n-1}}.$$

PROOF: By Theorem 11, if $r = 1$, then

$$\prod_{j=1}^k j^r \prod_{j=k+1}^{k+r} j^{k+r-j} = \prod_{j=1}^k j \prod_{j=k+1}^{k+1} (k + 1)^{k+1-(k+1)} = k!.$$

Therefore,

$$\frac{(m!)^{rm^{n-1}}}{r!} = (m!)^{m^{n-1}}$$

and

$$\frac{(n - k)!(m!)^{rm^{n-1}}}{(n - k - r)!} \prod_{j=1}^k j^r \prod_{j=k+1}^{k+r} j^{k+r-j} = (n - k)k!(m!)^{m^{n-1}}.$$

□

For complementing an $(n - 1)$ -tuple of δ -retractly orthogonal n -ary operations, where $|\delta| = n - 1$, to an n -tuple of orthogonal n -ary operations, we find more precise estimations in the following statement.

Corollary 13. *Let $m = |Q|$, $m \geq 2$, $n \geq 2$ and $|\delta| = n - 1$. Then*

$$(9) \quad (m!)^{m^{n-1}} \leq \mathfrak{C}_n(n - 1, n; m) \leq (n - 1)!(m!)^{m^{n-1}}.$$

PROOF: In Theorem 11, the equality $k = n - 1$ implies $r = n - (n - 1) = 1$. In this case, any possible complementing is a trivial complementing. That is why $\mathfrak{c}_n(n - 1, n; m) = \mathfrak{C}_n(n - 1, n; m)$. By Corollary 12, its lower bound is $(m!)^{m^{n-1}}$ and its upper bound is $(n - 1)!(m!)^{m^{n-1}}$.

From the proof of Theorem 11, an n -ary operation g_{i_n} is uniquely constructible by an i_n -invertible operation f_{i_n} . Consequently, an ordered tuple $(g_{i_1}, \dots, g_{i_k})$ is uniquely complementable by (8). Therefore, we have non-strict inequalities for $\mathfrak{C}_n(n - 1, n; m)$. \square

Example 3. Consider complements of binary Boolean operations. Putting $n = 2$ and $m = 2$ in (9), we have

$$4 \leq \mathfrak{C}_2(1, 2; 2) \leq 4,$$

consequently, $\mathfrak{C}_2(1, 2; 2) = 4$.

This can also be easily verified using superimposition of the corresponding squares: every left (right) invertible binary Boolean operation has 4 complements. Since there are 4 left (right) invertible Boolean operations, these complements are constructible by Algorithm 2.

Also we specify Theorem 11 for estimations of the number of complements of a k -tuple of δ -retractly orthogonal n -ary operations to an n -tuple of orthogonal operations.

Corollary 14. *Let $m = |Q|$, $k = |\delta|$, $k \geq 1$, $n \geq 3$, $m \geq 2$ and $k < n$. Then*

$$\frac{(m!)^{(n-k)m^{n-1}}}{(n - k)!} < \mathfrak{c}_n(k, n; m) < (n - k)!(m!)^{(n-k)m^{n-1}} \prod_{j=1}^k j^{n-k} \prod_{j=k+1}^n j^{n-j}.$$

PROOF: By Theorem 11, if $k + r = n$, then

$$\begin{aligned} & \frac{(n - k)!(m!)^{rm^{n-1}}}{(n - k - r)!} \prod_{j=1}^k j^r \prod_{j=k+1}^{k+r} j^{k+r-j} \\ &= \frac{(n - k)!(m!)^{(n-k)m^{n-1}}}{(n - n)!} \prod_{j=1}^k j^{n-k} \prod_{j=k+1}^n j^{n-j} \\ &= (n - k)!(m!)^{(n-k)m^{n-1}} \prod_{j=1}^k j^{n-k} \prod_{j=k+1}^n j^{n-j} \end{aligned}$$

and

$$\frac{(m!)^{rm^{n-1}}}{r!} = \frac{(m!)^{(n-k)m^{n-1}}}{(n-k)!}.$$

□

As noted in the proof of Theorem 11, we cannot even calculate the number of trivial complements directly. If we suppose that for different parameters, some complements of the same tuple of operations coincide, then this leads to series of functional equations. Remark that solutions of some functional equations are given in [1] and on arbitrary set in [12].

In order to find the number of all complements of a k -tuple of δ -retractly orthogonal n -ary operations to an n -tuple of orthogonal n -ary operations, we have to calculate the number of complements for all possible partitions of $\overline{1, n}$, where the first block is δ , and then to omit all repetitions.

Since Algorithm 1 is a partial case of Algorithm 2, Theorem 11 and its corollaries give also the lower bound of the number $\mathfrak{C}(k, k + r; m)$ of all complements.

6. Complements of orthogonal operations to greater arity and their estimation

In view of the composition algorithm, an algorithm for complementing a k -tuple of orthogonal k -ary operations to an n -tuple of orthogonal n -ary operations can be formulated. Note that additional restrictions on a given k -tuple are not imposed.

If $\delta = \{i_1, \dots, i_k\} \subset \overline{1, n}$ and $\sigma \in S_n$, then

$$\sigma\delta := \{(i_1)\sigma^{-1}, \dots, (i_k)\sigma^{-1}\}.$$

Algorithm 3. Let $\delta \subseteq \overline{1, n}$ and h_1, \dots, h_k be k -ary orthogonal operations, where $k \geq 2$.

Operations $g_{i_{k+1}}, \dots, g_{i_n}$ are constructed by the following items:

- 1) choose 1-invertible $(n - k + 1)$ -ary operations p_1, \dots, p_k and a permutation $\sigma \in S_n$ such that $\sigma^{-1}\delta = \overline{1, k}$;
- 2) operations f_1, \dots, f_k are constructed by (4);
- 3) operations g_{i_1}, \dots, g_{i_k} are obtained from f_1, \dots, f_k in the following way:

$$g_{i_1} := \sigma f_1, \quad \dots, \quad g_{i_k} := \sigma f_k;$$

- 4) implementation of Algorithm 1.

Theorem 15. Algorithm 2 constructs a complement for a k -tuple of orthogonal k -ary operations to an n -tuple of orthogonal n -ary operations. Besides, every k -tuple of orthogonal k -ary operations is complementable by Algorithm 3 to an n -tuple of orthogonal n -ary operations.

PROOF: Steps 1)–3) of the Algorithm 3 construct a tuple of δ -retractly orthogonal operations. By virtue of Algorithm 1 and Theorem 7, we can find a complement of this tuple to an n -tuple of orthogonal n -ary operations.

The second part of the theorem follows from the existence of a k -tuple of $(n - k + 1)$ -ary 1-invertible operations and Theorem 10. \square

Lemma 9 and Corollary 14 of Theorem 11 imply the following statement.

Theorem 16. *Let $k < n$, $k \geq 2$, $n \geq 3$ and $m \geq 2$. The number of all complements constructed by Algorithm 3 of a given k -tuple of orthogonal k -ary operations to an n -tuple of orthogonal n -ary operations is greater than*

$$\frac{(m!)^{(n-k)m^{n-1} + km^{n-k}}}{(n-k)!}.$$

PROOF: In order to obtain δ -retractly orthogonal operations from $\overline{1, k}$ -retractly orthogonal operations by step 3) of Algorithm 3, we have to apply $\sigma \in S_n$ such that $\sigma \overline{1, k} = \delta$. Suppose f_1, \dots, f_k are $\overline{1, k}$ -retractly orthogonal n -ary operations and g_1, \dots, g_k are δ -retractly orthogonal n -ary operations. The equality

$$\{f_1, \dots, f_k\} = \{\sigma g_1, \dots, \sigma g_k\}$$

establishes biunique correspondence between the class of $\overline{1, k}$ -retractly orthogonal n -ary operations and the class of δ -retractly orthogonal n -ary operations. Consequently, the number of $\overline{1, k}$ -retractly orthogonal n -ary operations and the number of δ -retractly orthogonal n -ary operations are the same.

By Lemma 9, the number of different k -tuples of n -ary operations constructed by step 2) of Algorithm 3 is $(m!)^{km^{n-k}}$. According to Corollary 14 of Theorem 11, the lower bound of the number of complements of retractly orthogonal operations is $\frac{(m!)^{(n-k)m^{n-1}}}{(n-k)!}$. These imply the truth of the theorem. \square

Conclusion. The found estimations can be improved in further research. Note that if $n - k = 1$, then more precise estimations are found in Corollary 13. For arbitrary $k < n - 1$, the problems of finding the upper bound of the number of all complements of

- a given k -tuple of δ -retractly orthogonal n -ary operations to an n -tuple of orthogonal n -ary operations,
- a given k -tuple of orthogonal k -ary operations to an n -tuple of orthogonal n -ary operations

remain open.

Acknowledgment. The author wishes to express her gratitude to Doctor of Mathematics Fedir Sokhatsky for his helpful suggestions during the preparation of the paper and to the English language reviewer Vira Obshanska for her help and advice.

REFERENCES

- [1] Aczél J., Dhombres J., *Functional Equations in Several Variables*, With applications to Mathematics, Information Theory and to the Natural and Social Sciences. Encyclopedia of Mathematics and Its Applications, 31, Cambridge University Press, Cambridge, 1989.
- [2] Bektenov A. S., Jakubov T., *Systems of orthogonal n -ary operations*, Bul. Akad. Štiinca RSS Moldoven. (1974), no. 3, 7–14, 93 (Russian).
- [3] Belyavskaya G. B., Mullen G. L., *Orthogonal hypercubes and n -ary operations*, Quasigroups Related Systems **13** (2005), no. 1, 73–86.
- [4] Couselo E., Gonzalez S., Markov V., Nechaev A., *Recursive MDS-codes and recursively differentiable quasigroups*, Discrete Math. Appl. **8** (1998), no. 3, 217–245; doi: 10.1515/dma.1998.8.3.217.
- [5] Dougherty S. T., Szczepanski T. A., *Latin k -hypercubes*, Australas. J. Combin. **40** (2008), 145–160.
- [6] Ethier J. T., Mullen G. L., *Strong forms of orthogonality for sets of hypercubes*, Discrete Math. **312** (2012), no. 12–13, 2050–2061; doi: 10.1016/j.disc.2012.03.008.
- [7] Evans T., *The construction of orthogonal k -skeins and latin k -cubes*, Aequationes Math. **14** (1976), no. 3, 485–491.
- [8] Fryz I. V., *Orthogonality and retract orthogonality of operations*, to appear in Bul. Akad. Štiinca RSS Moldoven.
- [9] Fryz I. V., Sokhatsky F. M., *Block composition algorithm for constructing orthogonal n -ary operations*, Discrete Math. **340** (2017), no. 8, 1957–1966; doi: 10.1016/j.disc.2016.11.012.
- [10] Keedwell A. D., Dénes J., *Latin Squares and Their Applications*, Elsevier/North Holland, Amsterdam, 2015.
- [11] Markovski S., Mileva A., *On construction of orthogonal d -ary operations*, Publ. Inst. Math. (Beograd) (N.S.) **101(115)** (2017), 109–119; doi: 10.2298/PIM1715109M.
- [12] Sokhatsky F. M., Krainichuk H. V., *Solution of distributive-like quasigroup functional equations*, Comment. Math. Univ. Carolin. **53** (2012), no. 3, 447–459.
- [13] Trenkler M., *On orthogonal latin p -dimensional cubes*, Czechoslovak Math. J. **55(130)** (2005), no. 3, 725–728; doi: 10.1007/s10587-005-0060-7.

I. V. Fryz:

VASYL' STUS DONETSK NATIONAL UNIVERSITY, 600-RICHIA STR. 21, 21021 VINNYTSIA, UKRAINE

E-mail: iryna.fryz@ukr.net

(Received October 15, 2017, revised February 6, 2018)