Retract orthogonality and orthogonality of n-ary operations

Iryna Fryz

Khmelnitskiy National University,
Department of Programming, Computer and Telecommunication systems,
Ukraine

July 29– August 5, 2017

Definition of orthogonality

Definition

n-ary operations $f_1, \ldots, f_k$ ($n \geqslant 2, k \leqslant n$) on Q ($m := |Q|$) are called *orthogonal*, if for every $b_1, \ldots, b_k \in Q$ the system

$$\begin{cases} f_1(x_1, \ldots, x_n) = b_1, \\ \ldots\ldots\ldots\ldots\ldots\ldots \\ f_k(x_1, \ldots, x_n) = b_k \end{cases} \tag{1}$$

has m^{n-k} solutions. If $n = k$, then (1) has a unique solution. If $k = 1$, then f_1 is called *complete*, i.e., for all $b_1 \in Q$

$$f_1(x_1, \ldots, x_n) = b_1 \tag{2}$$

has m^{n-1} solutions.

CONSTRUCTION METHODS OF ORTHOGONAL OPERATIONS

[1] **A.S. Bektenov, T Yakubov**, *Systems of orthogonal n-ary operations*, Izvestiya AN MSSR, Seria fiz.-tehn. i mat. nayk, 1974, **3**, 7 – 17.

[2] **M. Trenkler**, *On orthogonal latin p-dimensional cubes*, Czechoslovak Mathematical Journal, 2005, **55 (130)**, 725 – 728.

[3] **G. Belyavskaya, G.L. Mullen**, *Orthogonal hypercubes and n-ary operations*, Quasigroups and Related Systems, 2005, **13, 1**, 73 – 86.

[4] **Fryz I.V., Sokhatsky F.M.** *Block composition algorithm for constructing orthogonal n-ary operations*, Discrete mathematics, 2017, **340**, 1957-1966.

Definition of invertibility

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

$$f(a_1, \ldots, a_{i-1}, x, a_{i+1}, \ldots, a_n) = b. \tag{3}$$

If f is i-invertible for all $i \in \overline{1, n} := \{1, 2, \ldots, n\}$, then it is called an *invertible* or *quasigroup operation*.

Problems

1. relations between orthogonal n-ary operations and their orthogonal retracts;
2. complementing of a k-tuple of orthogonal n-ary operations ($k < n$) to an n-tuple of orthogonal n-ary operations.

Problems

1. relations between orthogonal n-ary operations and their orthogonal retracts;
2. complementing of a k-tuple of orthogonal n-ary operations ($k < n$) to an n-tuple of orthogonal n-ary operations.

Definition of retract

Let f be an n-ary operation on a set Q.

An $(n-1)$-ary operation $f_{i,a}$ is called a *retract* of f by element a, if it is obtained from f by replacing variable x_i with an element $a \in Q$, i.e., if it is defined by

$$f_{i,a}(x_1, \dots, x_{i-1}, x_{i+1}, \dots, x_n) = f(x_1, \dots, x_{i-1}, a_i, x_{i+1}, \dots, x_n). \tag{4}$$

Definition of retract

Unary operation $f_{(\bar{b},\{i\})}$ defined by

$$f_{(\bar{b},\{i\})}(x_i) = f(b_1, \ldots, b_{i-1}, x_i, b_{i+1}, \ldots, b_n) \tag{5}$$

is unary $(\bar{b}, \{i\})$-retract of f, $\bar{b} := (b_1, \ldots, b_{i-1}, b_{i+1}, \ldots, b_n)$.

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

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

$$f_{(\bar{a},\delta)}(x_{i_1}, \ldots, x_{i_k}) := f(y_1, \ldots, y_n), \tag{6}$$

where $y_i := \begin{cases} x_i, & \text{if } i \in \delta, \\ a_i, & \text{if } i \notin \delta \end{cases}$ is called $(\bar{a}, \delta)$-*retract* or δ-*retract* of f.

Definition of retract

Unary operation $f_{(\bar{b},\{i\})}$ defined by

$$f_{(\bar{b},\{i\})}(x_i) = f(b_1, \dots, b_{i-1}, x_i, b_{i+1}, \dots, b_n) \tag{5}$$

is unary $(\bar{b}, \{i\})$-retract of f, $\bar{b} := (b_1, \dots, b_{i-1}, b_{i+1}, \dots, b_n)$.

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

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

$$f_{(\bar{a},\delta)}(x_{i_1}, \dots, x_{i_k}) := f(y_1, \dots, y_n), \tag{6}$$

where $y_i := \begin{cases} x_i, & \text{if } i \in \delta, \\ a_i, & \text{if } i \notin \delta \end{cases}$ is called $(\bar{a}, \delta)$-*retract* or δ-*retract* of f.

Definition of retract orthogonality

Definition

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

Definition

If all similar δ-retracts of $f_1, \ldots, f_k$ are orthogonal, then the operations $f_1, \ldots, f_k$ are called *δ-retractly orthogonal*.

Definition of retract orthogonality

Definition

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

Definition

If all similar δ-retracts of $f_1, \dots, f_k$ are orthogonal, then the operations $f_1, \dots, f_k$ are called *δ-retractly orthogonal*.

Problem 1. Relations between orthogonality and retract orthogonality

Theorem 1 (I. Fryz, 2017)

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

Theorem 2 (I. Fryz, 2017)

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.

I.Fryz, *Orthogonality and retract orthogonality of operations* (in print).

Problem 1. Relations between orthogonality and retract orthogonality

Theorem 1 (I. Fryz, 2017)

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

Theorem 2 (I. Fryz, 2017)

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.

I.Fryz, *Orthogonality and retract orthogonality of operations* (in print).

Specification for central quasigroups

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

$$f(x_1,\dots,x_n)=\alpha_1x_1+\dots+\alpha_nx_n+a, \tag{7}$$

where $a\in Q$ and $\alpha_1,\dots,\alpha_n$ are automorphisms of $(Q;+)$. If $(Q;+)$ is abelian, then f is called a *central quasigroup* (or a T-quasigroup).

Theorem 3 (I. Fryz, 2017)

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

Specification for central quasigroups

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

$$f(x_1, \dots, x_n) = \alpha_1 x_1 + \dots + \alpha_n x_n + a, \tag{7}$$

where $a \in Q$ and $\alpha_1, \dots, \alpha_n$ are automorphisms of $(Q; +)$. If $(Q; +)$ is abelian, then f is called a *central quasigroup* (or a T-quasigroup).

Theorem 3 (I. Fryz, 2017)

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

Theorem (G. Belyavskaya, G.Mullen, 2005)

Every k-tuple of orthogonal n-ary operations ($k < n$) can be embedded in an n-tuple of orthogonal n-ary operations.

G. Belyavskaya, G.L. Mullen, *Orthogonal hypercubes and n-ary operations*, Quasigroups and Related Systems, 2005, **13, 1**, 73 – 86.

Theorem (G. Belyavskaya, G.Mullen, 2005)

Every k-tuple of orthogonal n-ary operations ($k < n$) can be embedded in an n-tuple of orthogonal n-ary operations.

This means that for every k-tuple of orthogonal n-ary operations $f_1, \ldots, f_k$, there exist an $(n-k)$-tuple of orthogonal n-ary operations $f_{k+1}, \ldots, f_n$ such that n-tuple $f_1, \ldots, f_n$ is orthogonal.

Every complete n-ary operation is complementable to an n-tuple of orthogonal n-ary operations.

G. Belyavskaya, G.L. Mullen, *Orthogonal hypercubes and n-ary operations*, Quasigroups and Related Systems, 2005, **13, 1**, 73 – 86.

Theorem (Belyavskaya and Mullen's algorithm, 2005)

Let $f_1, \ldots, f_n$ be n-ary $(n-i+1)$-invertible operations for all $i \in \overline{1,n}$. Operations $g_1, \ldots, g_n$ defined by

$$\begin{cases} g_1(x_1,\ldots,x_n) = f_1(x_1,\ldots,x_n), \\ g_2(x_1,\ldots,x_n) = f_2(x_1,\ldots,x_{n-1}, g_1(x_1,\ldots,x_n)), \\ g_3(x_1,\ldots,x_n) = f_3(x_1,\ldots,x_{n-2}, g_1(x_1,\ldots,x_n), g_2(x_1,\ldots,x_n)), \\ \quad \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ g_n(x_1,\ldots,x_n) = f_n(x_1, g_1(x_1,\ldots,x_n),\ldots, g_{n-1}(x_1,\ldots,x_n)) \end{cases}$$

are orthogonal.

Let $\delta=\{i_1,\dots,i_k\}\subset\overline{1,n}$ *and* $g_{i_1},\dots,g_{i_k}$ *are* δ*-retractly orthogonal*

Operations $g_{i_{k+1}},\dots,g_{i_n}$ *are constructed by*

1) *choose a partition* $\pi := \{\delta,\pi_2,\dots,\pi_q\}$ *of* $\overline{1,n}$, $f_{i_{k+1}},\dots,f_{i_n}$ *such that for every* $r\in\overline{2,q}$ *a tuple* $\{f_j|j\in\pi_r\}$ *is* π_r*-retractly orthogonal;*

2) *for every* $j\in\pi_2$, *operation* g_j *is constructed by*

$$g_j(x_1,\dots,x_n) := f_j(t_1,\dots,t_n), \tag{8}$$

where

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

r) *for every* $j\in\pi_r$, $r=3,\dots,q$, *operation* g_j *is constructed by* (8), *where*

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

Let $\delta = \{i_1, \dots, i_k\} \subset \overline{1,n}$ *and* $g_{i_1}, \dots, g_{i_k}$ *are* δ*-retractly orthogonal*
Operations $g_{i_{k+1}}, \dots, g_{i_n}$ *are constructed by*

1) *choose a partition* $\pi := \{\delta, \pi_2, \dots, \pi_q\}$ *of* $\overline{1,n}$, $f_{i_{k+1}}, \dots, f_{i_n}$ *such that for every* $r \in \overline{2,q}$ *a tuple* $\{f_j | j \in \pi_r\}$ *is* π_r*-retractly orthogonal;*
2) *for every* $j \in \pi_2$, *operation* g_j *is constructed by*

$$g_j(x_1, \dots, x_n) := f_j(t_1, \dots, t_n), \tag{8}$$

where

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

r) *for every* $j \in \pi_r$, $r = 3, \dots, q$, *operation* g_j *is constructed by* (8), *where*

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

Let $\delta=\{i_1,\ldots,i_k\}\subset\overline{1,n}$ *and* $g_{i_1},\ldots,g_{i_k}$ *are* δ*-retractly orthogonal Operations* $g_{i_{k+1}},\ldots,g_{i_n}$ *are constructed by*

1) *choose a partition* $\pi := \{\delta,\pi_2,\ldots,\pi_q\}$ *of* $\overline{1,n}$, $f_{i_{k+1}},\ldots,f_{i_n}$ *such that for every* $r\in\overline{2,q}$ *a tuple* $\{f_j | j\in\pi_r\}$ *is* π_r*-retractly orthogonal;*
2) *for every* $j\in\pi_2$*, operation* g_j *is constructed by*

$$g_j(x_1,\ldots,x_n) := f_j(t_1,\ldots,t_n), \tag{8}$$

where

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

r) *for every* $j\in\pi_r$*,* $r=3,\ldots,q$*, operation* g_j *is constructed by* (8)*, where*

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

Complementing orthogonal n-ary operations

Theorem 4 (I. Fryz, 2017)

A $(n-k)$-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.

If partition $\pi := \{\delta, \pi_1, \dots, \pi_q\}$ of $\overline{1, n}$, where $\pi_r =: \{i_{k+r}\}$ for all $r \in \overline{1, n-k}$, then constructed complements are trivial. Thus, we have to take i_{k+1}-,…, i_n-invertible n-ary operations.

Estimation of complements

Theorem 6 (I. Fryz, 2017)

The number of all complements constructed by Algorithm 1 of a k-tuple of δ-retractly orthogonal n-ary operations ($|\delta| = k$, $k < n$) on Q of order m to an n-tuple of orthogonal n-ary operations is greater than

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

Let $\delta \subset \overline{1,n}$ and $h_1, \ldots, h_k$ be orthogonal k-ary operations.

1) choose $(n-k+1)$-ary 1-invertible operations $p_1, \ldots, p_k$ and a permutation $\sigma \in S_n$ such that ${}^{\sigma^{-1}}\delta = \overline{1,k}$;
2) operations $f_1, \ldots, f_k$ are constructed by

$$\begin{cases} f_1(x_1, \ldots, x_n) := p_1(h_1(x_1, \ldots, x_k), x_{k+1}, \ldots, x_n), \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ f_k(x_1, \ldots, x_n) := p_k(h_k(x_1, \ldots, x_k), x_{k+1}, \ldots, x_n); \end{cases} \quad (9)$$

3) operations $g_{i_1}, \ldots, g_{i_k}$ are obtained from $f_1, \ldots, f_k$ in the following way:

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

4) implementation of Algorithm 1.

Let $\delta \subset \overline{1,n}$ and $h_1, \ldots, h_k$ be orthogonal k-ary operations.

1) choose $(n-k+1)$-ary 1-invertible operations $p_1, \ldots, p_k$ and a permutation $\sigma \in S_n$ such that ${}^{\sigma^{-1}}\delta = \overline{1,k}$;
2) operations $f_1, \ldots, f_k$ are constructed by

$$\begin{cases} f_1(x_1,\ldots,x_n) := p_1(h_1(x_1,\ldots,x_k), x_{k+1},\ldots,x_n), \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ f_k(x_1,\ldots,x_n) := p_k(h_k(x_1,\ldots,x_k), x_{k+1},\ldots,x_n); \end{cases} \tag{9}$$

3) operations $g_{i_1}, \ldots, g_{i_k}$ are obtained from $f_1, \ldots, f_k$ in the following way:

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

4) implementation of Algorithm 1.

Let $\delta \subset \overline{1,n}$ and $h_1, \dots, h_k$ be orthogonal k-ary operations.

1) choose $(n-k+1)$-ary 1-invertible 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, ..., f_k are constructed by

$$\begin{cases} f_1(x_1, \dots, x_n) := p_1(h_1(x_1, \dots, x_k), x_{k+1}, \dots, x_n), \\ \dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots \\ f_k(x_1, \dots, x_n) := p_k(h_k(x_1, \dots, x_k), x_{k+1}, \dots, x_n); \end{cases} \quad (9)$$

3) operations g_{i_1}, ..., g_{i_k} are obtained from f_1, ..., 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.

Let $\delta \subset \overline{1,n}$ and $h_1, \ldots, h_k$ be orthogonal k-ary operations.

1) choose $(n-k+1)$-ary 1-invertible operations $p_1, \ldots, p_k$ and a permutation $\sigma \in S_n$ such that ${}^{\sigma^{-1}}\delta = \overline{1,k}$;
2) operations $f_1, \ldots, f_k$ are constructed by

$$\begin{cases} f_1(x_1, \ldots, x_n) := p_1(h_1(x_1, \ldots, x_k), x_{k+1}, \ldots, x_n), \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ f_k(x_1, \ldots, x_n) := p_k(h_k(x_1, \ldots, x_k), x_{k+1}, \ldots, x_n); \end{cases} \quad (9)$$

3) operations $g_{i_1}, \ldots, g_{i_k}$ are obtained from $f_1, \ldots, f_k$ in the following way:

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

4) implementation of Algorithm 1.

Complementing orthogonal k-ary operations

Theorem 5 (I. Fryz, 2017)

Algorithm 2 complements a k-tuple of orthogonal k-ary operations to an n-tuple of orthogonal n-ary operations.

Estimation of complements

Theorem (I. Fryz, 2017)

The number of all complements constructed by Algorithm 2 of a k-tuple of orthogonal k-ary operations on a set Q of order m to an n-tuple of orthogonal n-ary operations is greater than

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

Thank you for your attention