УДК 512.548.7

Fedir Sokhatsky

Doctor in Physics and Mathematics, Professor of the Department of Mathematical Analysis and Differential Equations, Vasyl' Stus Donetsk National University;

ABOUT ORTHOGONALITY OF MULTIARY OPERATIONS

In this article orthogonality of multiary operations and hypercubes are under consideration. In particular, criteria of orthogonality of n-ary operations are systematized and a criterion for a operation in a set of orthogonal operations to be invertible is found. Corollaries for ternary case are given.

Key words: *n-ary quasigroup, Latin hypercubs, orthogonal quasigroups, orthogonal n-ary operations*

Introduction

Orthogonality of multiary operations and quasigroups, hypercubes and Latin hypercubes (i.e., permutation cubes) are well-known and applicable in various areas including orthogonal and projective geometries, cryptology, functional equations. In this article, we continue their investigation (see [1]–[9]).

1. Preliminaries

Let Q be an arbitrary set – finite or infinite. An *n-ary operation* f defined on the *carrier* Q is a mapping $f:\ Q^n \to Q$. An n-ary operation f is called *invertible* if there are *inverses* ${}^{[i]}f$ of f for every $i=1,\dots,n$:

$$ {}^{[i]}f(x_1,\dots,x_n) = x_{n+1} :\Leftrightarrow f(x_1,\dots,x_{i-1},x_{n+1},x_{i+1},\dots,x_n) = x_i, \tag{1}$$

$i=0,\dots,n-1$. This is a partial case of a parastrophe ${}^{\sigma}f$ of an invertible operation f:

$$ {}^{\sigma}f(x_1,\dots,x_n) = x_{n+1} :\Leftrightarrow f(x_{1\sigma},\dots,x_{(n)\sigma}) = x_{(n+1)\sigma}, \tag{2}$$

for all $\sigma\in S_{n+1}$ permutation of the set $\{0,\dots,n\}$. The algebra $(Q;f,{}^{[1]}f,\dots,{}^{[n]}f)$ is called a *quasigroup.*

2. Equivalent definitions of orthogonality

A mapping α from a set A to a set B is called *complete*, if all preimages have the same cardinality.

A k-tuple of n-ary operations defined on a finite set Q ($m:=|Q|$) is called *orthogonal*, if for all a_1, …, a_k in Q the system

$$\left\{\begin{array}{l} f_1(x_1,\dots,x_n)=a_1,\\ \dots\dots\dots\dots\dots\dots\\ f_k(x_1,\dots,x_n)=a_k \end{array}\right. \tag{3}$$

has exactly m^{n-k} solutions.

A k-tuple $(f_1,\dots,f_k)$ of operations is called *embeddable* into an m-tuple $(g_1,\dots,g_m)$ of operations, if each of the operations f_1, …, f_k is an entry in $(g_1,\dots,g_m)$, i.e., $g_{i_1}=f_1$, …, $g_{i_k}=f_k$, for some i_1, … $i_k\in\{1,\dots,m\}$.

Let Q be a set. A mapping f from Q^n in Q^k is called a *multioperation* of the *arity* n and the *rank* k or (n,k)*-multioperation.* Every (n,k)-multiopertion f uniquely defines and is uniquely defined by a k-tuple $(f_1,\dots,f_k)$ of n-ary operation:

$$f(x_1,\dots,x_n) = (f_1(x_1,\dots,x_n),\dots,f_k(x_1,\dots,x_n)).$$

For briefly, $f = (f_1,\dots,f_k)$. The tuple is called *coordinates* of the multioperation. Therefore,

$$f(x_1,\dots,x_n) = (f_1,\dots,f_k)(x_1,\dots,x_n) = (f_1(x_1,\dots,x_n),\dots,f_k(x_1,\dots,x_n)).$$

In other words, the set $\Omega_{n,k}$ of (n,k)-multioperations is a k-th power of the set of n-ary operations:

$$\Omega_{n,k} = \Omega_n^k := \underbrace{\Omega_n \times \Omega_n \times \ldots \times \Omega_n}_{k}.$$

Some multioperations are complete. For example, the multioperation

$$\iota_{1,\dots,k} := (\iota_1,\dots,\iota_k), \qquad \iota_{1,\dots,k}(x_1,\dots,x_n) := (x_1,\dots,x_k)$$

is complete because preimage of each tuple $(a_1,\dots,a_k)$ is

$$\iota_{1,\dots,k}^{-1}(a_1,\dots,a_k) = \{(a_1,\dots,a_k,x_{k+1},\dots,x_n) \mid x_{k+1},\dots,x_n \in Q\}$$

and it has m^{n-k} elements.

Theorem 1. *Let $f = (f_1,\dots,f_k)$ be an (n,k)-multioperation defined on a finite set Q ($m := |Q|$) and let $k < n$, then the following assertions are equivalent:*

1. *the multioperation f is complete;*
2. *each preimage under f has m^{n-k} elements;*
3. *the tuple $(f_1,\dots,f_k)$ of n-ary operations are orthogonal;*
4. *there exists a bijection $\theta : Q^n \to Q^n$ such that $f = \iota_{1,\dots,k}\theta$;*
5. *the tuple $(f_1,\dots,f_k)$ of n-ary operations is embeddable into an orthogonal n-tuple of n-ary operations.*

Proof. $(1)\Rightarrow(2)$. Since f is a mapping from Q^n to Q^k, then the sets Q^n/f and Q^k have the same cardinal, therefore Q^n/f has m^k elements. Completeness of f means that all members in the set Q^n/f have the same cardinal. Thus for arbitrary a_1, ..., a_k, we have

$$|f^{-1}(a_1,\dots,a_k)| = \frac{|Q^n|}{|Q^n/f|} = \frac{m^n}{m^k} = m^{n-k}.$$

$(2)\Rightarrow(3)$. The implication is true because for arbitrary a_1, ..., a_k the set of all solutions of the system (3) is equal to preimage of the tuple $(a_1,\dots,a_k)$ under f.

$(3)\Rightarrow(1)$. Orthogonality of the operations f_1, ..., f_k means that the preimage of every k-tuple $(a_1,\dots,a_k)$ has m^{n-k} elements, so, f is complete.

$(1) \Rightarrow (4)$. The multioperation $\iota_{1,\dots,k}$ is complete according to the definition and the multioperation f is complete according to the assumption. The item (2) implies that all preimages under both f and $\iota_{1,\dots,k}$ consists of m^{n-k} elements. Consequently, for every k-tuple $(a_1,\dots,a_k)\in Q^k$ there exists a bijection

$$\alpha_{a_1,\dots,a_k}:\ \iota^{-1}_{1,\dots,k}(a_1,\dots,a_k)\to f^{-1}(a_1,\dots,a_k).$$

Because all domains of the mappings form a partition of Q^n and the all codomains do, their union

$$\alpha := \bigcup_{a_1,\dots,a_k\in Q}\alpha_{a_1,\dots,a_k}$$

is a bijection of Q^n. Moreover, for each $(x_1,\dots,x_n)\in Q^n$

$$(f\alpha)(x_1,\dots,x_n)=f(\alpha(x_1,\dots,x_n))=f(\alpha_{x_1,\dots,x_k}(x_1,\dots,x_n))=(x_1,\dots,x_k).$$

As $\alpha_{x_1,\dots,x_k}(x_1,\dots,x_n)\in f^{-1}(x_1,\dots,x_k)$,

$$(f\alpha)(x_1,\dots,x_n)=(x_1,\dots,x_k)=\iota_{1,\dots,k}(x_1,\dots,x_n).$$

Hence, $f\alpha=\iota_{1,\dots,k}$. Therefrom $f=\iota_{1,\dots,k}\alpha^{-1}$.

$(4) \Rightarrow (5)$. Since the bijection θ is a mapping from Q^n to Q^n, then there is a n-tuple $(g_1,\dots,g_n)$ of n-ary operations defined on Q such that $\theta=(g_1,\dots,g_n)$. Thence,

$$(f_1,\dots,f_k)=f=\iota_{1,\dots,k}\theta=\iota_{1,\dots,k}(g_1,\dots,g_n)=(g_1,\dots,g_k),$$

so, the k-tuple $(f_1,\dots,f_k)$ is embeddable into the n-tuple $(g_1,\dots,g_n)$. Since θ is a bijection, the preimage of every n-tuple $(a_1,\dots,a_n)$ is a singleton and so the system (3) has a unique solution, i.e. the operations g_1, ..., g_n are orthogonal. Thus, the k-tuple $(f_1,\dots,f_k)$ of operations is embeddable into an orthogonal n-tuple of operations.

$(5) \Rightarrow (3)$. Let a k-tuple $(f_1,\dots,f_k)$ of n-ary operations is embeddable into an orthogonal n-tuple $(f_1,\dots,f_n)$ of orthogonal n-ary operations. It means that for every n-tuple $(a_1,\dots,a_n)$ of elements of the set Q the system

$$\begin{cases} f_1(x_1,\dots,x_n)=a_1,\\ \dots\dots\dots\dots\dots\dots\dots\dots\\ f_k(x_1,\dots,x_n)=a_k,\\ f_{k+1}(x_1,\dots,x_n)=a_{k+1},\\ \dots\dots\dots\dots\dots\dots\dots\dots\\ f_n(x_1,\dots,x_n)=a_n. \end{cases} \tag{4}$$

has a unique solution. Let $(a_1,\dots,a_k)$ be an arbitrary fixed k-tuple of elements in Q and X be the set of all solutions of the system (3). Let define a mapping

$$\lambda:\ \ Q^{n-k}\to X$$

as follows: $\lambda(a_{k+1},\dots,a_n)=(x_1,\dots,x_n)$ means that $(x_1,\dots,x_n)$ is a solution of the system (4). Since λ is a bijection and Q^{n-k} has m^{n-k} elements, the set X also has m^{n-k} elements. Inasmuch as a_1, ..., a_k are arbitrary elements, the k-tuple $(f_1,\dots,f_k)$ of n-ary operations is orthogonal. □

Let $k>n$, then the set of n-ary operations $\mathbf{f}:=\{f_1,\dots,f_k\}$ is called *orthogonal* if each n operations from the set is orthogonal.

3. About orthogonality of hypercubes

A *table* of the *dimension* m^n is a set containing m^n cells. The number n is called an *arity* and the number m is an *order* of the table. Let Q be an m-element set. Since Q^n has m^n elements, we can bijectively label all cells of the table by elements of Q^n. If a cell is labelled by $\bar{a} := (a_1, \ldots, a_n)$ then the tuple $\bar{a}$ is called *coordinates* of the cell. In this case, we will say that *the table is defined over the set* Q. The following set of cells

$$L_{i,\bar{a}} := \{(a_1, \ldots, a_{i-1}, x, a_{i+1}, \ldots, a_n) \mid x \in \overline{0, m-1}\},$$

is called an i*-th line* defined by $\bar{a}$ and the number i is a *direction* of the line.

A *hypercube* or *cube* of *dimension* m^n over a set Q ($|Q| = m$) is a table of the dimension m^n whose each cell contains an element from Q called an *entry.*

A table of results (i.e., Cayley table) of an n-ary operation f defined on Q is a cube of the dimension m^n with entries from the set Q. The cube is called *Latin* if all entries in each line are pairwise different. Cayley table of a function is Latin if and only if the function is invertible.

Let C_1, …, C_n be n-ary cubs defined over the same set Q. Let us superimpose all of them. As a result, we obtain a cube $C_{1,\ldots,n}$ such that each its cell contains one n-tuple of elements from Q. If all the tuples are pairwise different, the cubs C_1, …, C_n are called *orthogonal.* It is easy to verify that cubes are orthogonal iff the corresponding functions are orthogonal.

The following question is natural: *When one of orthogonal cubes is Latin?*

The set of all cells taken exactly one from each line of an n-ary table is called its $(n-1)$*-ary diagonal.*

Lemma 1. *A set d of cells of an n-ary table is its diagonal if and only if there exist an $(n-1)$-ary invertible operation g such that*

$$d = \{(x_1, \ldots, x_{n-1}, g(x_1, \ldots, x_{n-1})) \mid x_1, \ldots, x_{n-1} \in Q\}. \tag{5}$$

Proof. Let d be a set of cells and let $\bar{x} := (x_1, \ldots, x_n)$, where x_1, …, x_n are variables. d is an $(n-1)$-ary diagonal means that d has exactly one cell in each of the following lines

$$L_{1,\bar{x}}, \quad L_{2,\bar{x}}, \quad \ldots, \quad L_{n,\bar{x}}.$$

It is equivalent to "in the belonging

$$(x_1, \ldots, x_n) \in d$$

arbitrary values of arbitrary $n-1$ variables uniquely define the value of n-th variable". It the same that "the relationship

$$g(x_1, \ldots, x_{n-1}) = x_n :\Leftrightarrow \; (x_1, \ldots, x_n) \in d$$

defines an invertible $(n-1)$-ary operation g on Q". This relationship can be rewritten as (5). $\square$

Let d be an $(n-1)$-ary diagonal of the table of the dimension m^n and let i be an arbitrary direction. Each i-line has $n-1$ parameters which takes their values in Q. Therefore, there are m^{n-1} different i-lines. d has exactly one cell in each line and so d has m^{n-1} different cells. Thus, d is a sub-table of the dimension m^{n-1}.

A *diagonal partition* of a table is its partition whose blocks are diagonals of the table. A *natural partition* of a cube is its partition whose blocks are sets of cells containing the same element. It is easy to see the validity of the following proposition.

Proposition 1. *A natural partition of a cube is diagonal iff the cube is Latin.*

An $(n-1)$-ary diagonal d of n-ary cubes $C_1, \dots, C_{n-1}$ is said to be their *transversal*, if sub-cubes of these cubes defined by d are orthogonal. A *transversal partition* of $n-1$ n-ary cubes of the same order is their diagonal partition, if each block is a transversal of the cubes.

Theorem 2. *n-ary cubes $C_1, \dots, C_{n-1}$ of the same dimension have a Latin compliment iff they have a transversal partition.*

Proof. Let $C_1, \dots, C_n$ be orthogonal cubes of the dimension m^n and let C_n be Latin. All tuples in cells of the cube $C_{1,\dots,n}$ obtained by superimposition of the given cubes are different. Since C_n is Latin, then its natural partition is diagonal, i.e., all its blocks are diagonals of the m^n-dimension table. Since the partition is natural in the cube C_n, then an arbitrary block B_a in the cube $C_{1,\dots,n}$ consists of cells which contains n-tuples $(x_1, \dots, x_{n-1}, a)$ for some fixed element a. Because the cubes $C_1, \dots, C_n$ are orthogonal, all tuples in cells of the cube $C_{1,\dots,n}$ are pairwise different. Therefore, all tuples in B_a are also different. The n-th coordinate in all tuple from B_a are the same element a, so the sequences of other $n-1$ coordinates are pairwise different. Therefore, the $(n-1)$-ary sub-cubes (which are diagonals) of the cubes C_1, $\dots$, C_{n-1} defined by the B_a are orthogonal.

Vise versa, let n-ary cubes $C_1, \dots, C_{n-1}$ of the dimension m^n have a transversal partition. It means that there is a partition of the table of dimension m^n such that each block B is a $(n-1)$-ary diagonal and so it is sub-table of the arity $n-1$ but the same order m. Therefore, the block B has m^{n-1} cells. In each cubes $C_1, \dots, C_{n-1}$ the block B defines a sub-cube: $B_1, \dots, B_{n-1}$. According to assumption, the sub-cubes are orthogonal, i.e., the cube $B_{1,\dots,n-1}$ has a $(n-1)$-tuple of elements from Q. All the tuples are pairwise different because the sub-cubes are orthogonal. Note, that there are m blocks of the partition, so, we can bijectively label all the blocks with the elements of the set Q. We define a cube C_n by the following way: we put an element a in a cell, if the cell belong to the block labeled by a. Since each block is a diagonal, then the same element appears in pairwise differen lines. That is why the constructed cube is Latin. Consider the cube $C_{1,\dots,n}$. If two its cells belong to the different blocks, the they are different because they labeled by different elements from Q and so the tuple in the cells differ the n-th coordinates. If the celles belong to the same block, then they are different because the sequences of fist $n-1$ coordinates are different which follows from orthogonality of sub-cubes. □

4. Ternary case

This subsection contains corollaries from the obtained results for the ternary case.

Corollary 1. *Let $f = (f_1, f_2)$ be an $(3,2)$-multioperation defined on a finite set Q ($m := |Q|$), then the following assertions are equivalent:*

1. *the multioperation f is complete;*
2. *each preimage under f has m elements;*
3. *the tuple (f_1, f_2) of ternary operations is orthogonal;*
4. *there exists a bijection $\theta : Q^3 \to Q^3$ such that $f = \iota_{1,2}\theta$;*
5. *the tuple (f_1, f_2) of ternary operations is embeddable into an orthogonal triplet of ternary operations.*

Corollary 2. *Let $f = (f_1, f_2, f_3)$ be an $(3,3)$-multioperation defined on a finite set Q ($m := |Q|$), then the following assertions are equivalent:*

1. *the multioperation f is a permutation of Q^3;*
2. *each preimage under f has one element;*
3. *the tuple (f_1, f_2, f_3) of ternary operations is orthogonal;*
4. *there exists a bijection $\theta : Q^3 \to Q^3$ such that $f\theta = \iota_{1,2,3}$.*

The set of all cells taken exactly one from each line of a ternary table will be called its *binary diagonal* or *spacial square.*

Lemma 2. *A set d of cells of a ternary table is its diagonal if and only if there exists a binary invertible operation g such that $d = \{(x, y, g(x, y)) \mid x, y \in Q\}$.*

Let d be a binary diagonal of the table of the dimension m^3 and let i be an arbitrary direction. Each i-line has two parameters which take their values in Q. Therefore, there are m^2 different i-lines. d has exactly one cell in each line and so d has m^2 different cells. Thus, d is a sub-table of the dimension m^2.

A *diagonal partition* of a table is the partition whose blocks are diagonals of the table. A *natural partition* of a cube is its partition whose blocks are sets of cells containing the same element. It is easy to see the validity of the following proposition.

Proposition 2. *A natural partition of a cube is diagonal iff the cube is Latin.*

An binary diagonal d of ternary cubes C_1, C_2 will be their *transversal*, if sub-cubes of these cubes defined by d are orthogonal. A *transversal partition* of two binary cubes of the same order is their diagonal partition, if each block is a transversal of the cubes.

Theorem 3. *Ternary cubes C_1, C_2 of the same dimension have a Latin compliment iff they have a transversal partition.*

Conclusion

The obtained results permits to defined all diagonals of an n-ary table: diagonal of a diagonal also is a diagonal of the given n-ary table. Consequently, it is possible to establish their connection with orthogonality of multi-ary cubes.

References

[1] Belyavskaya G. *Pairwise ortogonality of n-ary operations* // Bul. Acad. Ştiinţe Repub. Mold. Mat. – 2005. – №3(49). – P. 5-18.

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

[3] Belyavskaya G. *S-systems of n-ary quasigroups* // Quasigroups Related Systems. – 2007. – Vol. 15, №2. – P. 251-260.

[4] Belyavskaya G. *Power sets of n-ary quasigroups* // Bul. Acad. Ştiinţe Repub. Mold. Mat. – 2007. – №1(53). – P. 37-45.

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

[6] Shcherbacov V. *Elements of Quasigroup Theory and Applications.* – Chapman and Hall/CRC, 2017. – xxi+576 p.
[7] Belousov V.D. *Foundations of the theory of quasigroups and loops.* Nauka (1967), 222 (Russian).
[8] Sokhatsky F.M. *Parastrophic symmetry in quasigroup theory. Visnyk DonNU, A: natural Sciences.* 2016. Vol.1-2. P. 70–83.
[9] Markovski S., Mileva A. *On construction of orthogonal d-ary operations.* Publication de l'institute mathematique, Nouvelle serie, tom 101(115) (2017), 109–119 https://doi.org/10.2298/PIM1715109M

Федір Сохацький

Доктор фізико-математичних наук, професор кафедри математичного аналізу та диференціальних рівнянь
Донецький національний університет імені Василя Стуса

ПРО ОРТОГОНАЛЬНІСТЬ БАГАТОМІСНИХ ОПЕРАЦІЙ

РЕЗЮМЕ
В цій статті розглядається ортогональність багатоміних операцій та гіперкубів. Зокрема, систематизовано критерії ортогональності багатомісних операцій та знайдено умови за яких куб із ортогональної системи кубів є латинським. Наведено наслідки для тернарного випадку.

Key words: *n-арна квазігрупа, латинський гіперкуб, ортогональні квазігрупи, ортогональні n-арні операції.*

Федор Сохацкий

Доктор физико-математических наук, професор кафедры математического анализа и дифференциальных уравнений,
Донецкий национальный университет имени Василя Стуса

ОБ ОРТОГОНАЛЬНОСТИ МНОГОМЕСТНЫХ ОПЕРАЦИЙ

РЕЗЮМЕ
В этой статье изучется ортогональность многоместных операций. В частности, систематизированы критерии ортогональности многоместных операций и найдено условие при котором операция из системы ортогональных кубов якляется латинским. Приведено следствия для тернарного случая.

Ключевые слова: *n-арная квазигруппа, латинский гиперкуб, ортогональные квазигруппы, ортогональные n-арные операции.*