Quasigroups and Related Systems **13** (2005), 73 – 86

Orthogonal hypercubes and n-ary operations

Galina B. Belyavskaya and Gary L. Mullen

Abstract

We study connections between orthogonal hypercubes and n-ary operations and quasigroups.

1. Introduction

The notion of a Latin square is well known in combinatorial analysis. A permutation cube is a generalization of a Latin square to higher dimensions; see [5] beginning on page 181. A hypercube is an even more general object. All of these objects and their corresponding orthogonal sets have many applications in various areas including affine and projective geometries, design of experiments, error-correcting and error-detecting coding theory, and cryptology, as well as in the theory of (t, m, s)-nets; see for example [7].

It is known that a binary quasigroup is an algebraic equivalent of a Latin square. In particular, the multiplication table of a finite quasigroup containing n elements gives a Latin square of order n, and conversely, a Latin square of order n determines a quasigroup containing n elements.

The algebraic approach is useful for research on Latin squares and sets of mutually orthogonal Latin squares. In this article we consider connections between hypercubes (sets of orthogonal hypercubes) and algebraic n-ary operations (orthogonal sets of such operations). We recall some useful but little-known results with respect to orthogonal n-ary operations, and establish some of their connections with orthogonal hypercubes. We also

2000 Mathematics Subject Classification: 20N05, 20N15, 05B15

Keywords: hypercube, orthogonal hypercubes, n-ary operation, n-ary quasigroup, orthogonal n-ary operations.

The research described in this article was made possible in part by Award No. MM1-3040-CH-02 of the Moldovan Research and Development Association (MRDA) and the U.S. Civilian Research & Development Foundation for the Independent States of the Former Soviet Union (CRDF).

introduce a more general version of orthogonality for n-ary operations (hypercubes) in order to distinguish the known types of orthogonality in the combinatorial and algebraic approaches. We also establish some criterion for orthogonality of n-ary operations.

2. d-dimensional hypercubes and d-ary operations

For $d \geqslant 2$, a *d-dimensional hypercube* (briefly, a *d-hypercube*) *of order n* is an $\underbrace{n \times n \times \cdots \times n}_{d}$ array with n^d points based upon n distinct symbols. Such a d-hypercube has *type j* with $0 \leqslant j \leqslant d-1$ if, whenever any j of the d coordinates are fixed, each of the n symbols appears n^{d-j-1} times in that subarray (see [8]).

A hypercube is a generalization of a *Latin square*, which in the case of squares of *order* n, is an $n \times n$ array in which n distinct symbols are arranged so that each symbol occurs once in each row and column. A Latin square is a 2-dimensional hypercube of type 1.

Before we establish some connections between d-hypercubes and (algebraic) d-ary operations, we recall some necessary definitions and results from [3]. By x_i^j we will denote the sequence $x_i, x_{i+1}, \ldots, x_j$, $i \leqslant j$. If $j < i$, then x_i^j is the empty sequence. Let Q be a finite or infinite set, $d \geqslant 2$ a positive integer, and let Q^d denote the d-th Cartesian power of the set Q.

We begin by recalling the definition of a binary operation. *A binary operation* on a set Q is a mapping $A : Q^2 \to Q$ defined by $A(x, y) \to z$ and in this case we write $A(x, y) = z$. A set Q with a binary operation A defined on Q is called *a binary quasigroup* (Q, A) if for any two given elements $a, b \in Q$, the equations $A(a, x) = b$ and $A(y, a) = b$ each has exactly one solution.

If a set Q has order n then a binary operation A is said to be *of order n* and can be given by an $n \times n$ multiplication table with elements of Q and with a bordered row and a bordered column. In such a table the element $c \in Q$ is located at the intersection of the row a and the column b (i.e. in the position (a, b)) if $A(a, b) = c$.

Example 1. In Table 1 are given the multiplication tables of two binary operations A and B defined on the set $Q = \{1, 2, 3, 4\}$. The operation B is a quasigroup operation. The unbordered part of its multiplication table is a Latin square of order 4.

A	1	2	3	4
1	1	1	2	3
2	4	2	1	4
3	2	1	3	4
4	3	2	4	1

B	1	2	3	4
1	1	2	3	4
2	3	1	4	2
3	4	3	2	1
4	2	4	1	3

Table 1: Multiplication tables of operations A and B

A *d-ary operation* A (briefly, a *d-operation*) on a set Q is a mapping $A : Q^d \to Q$ defined by $A(x_1^d) \to x_{d+1}$, and in this case we write $A(x_1^d) = x_{d+1}$. Thus a 1-ary (unary) operation is simply a mapping from Q into Q.

A *d-groupoid* (Q, A) *of order* n is a set Q with one d-ary operation A defined on Q, where $|Q| = n$. An *i-invertible d-operation* A defined on Q is a d-operation with the property that the equation

$$A(a_1^{i-1}, x, a_{i+1}^d) = a_{d+1}$$

has a unique solution for each fixed d-tuple $(a_1^{i-1}, a_{i+1}^d, a_{d+1})$ of Q^d.

A *d-ary quasigroup* (or simply a *d-quasigroup*) is a d-groupoid (Q, A) such that the d-operation A is i-invertible for each $i = 1, 2, \ldots, d$. Thus a 1-ary quasigroup $(Q, A) = (Q, \alpha)$, where α is a permutation on Q.

Another equivalent definition of a d-quasigroup is the following. A *d-ary quasigroup* is a d-groupoid such that in the equality

$$A(x_1^d) = x_{d+1}$$

each set of d elements from x_1^{d+1} uniquely defines the $(d+1)$-th element. Sometimes a quasigroup d-operation A is itself considered as a d-quasigroup.

The d-operation E_i, $1 \leqslant i \leqslant d$, on Q with $E_i(x_1^d) = x_i$ is called the *i-th projection* (or the *i-th selector*) of arity d. Let $1 \leqslant i_1, i_2, \ldots, i_j \leqslant d$, $a_{i_1}, a_{i_2}, \ldots, a_{i_j} \in Q$, and A be a d-operation on Q. Fixing in A values of j variables $x_{i_1}, x_{i_2}, \ldots, x_{i_j}$, we obtain

$$A(x_1^{i_1-1}, a_{i_1}, x_{i_1+1}^{i_2-1}, a_{i_2}, \ldots, x_{i_j-k}^{i_j-1}, a_{i_j}, x_{i_j+1}^d) =$$
$$A_{\bar{a}}(x_1^{i_1-1}, x_{i_1+1}^{i_2-1}, \ldots, x_{i_j-k}^{i_j-1}, x_{i_j+1}^d) = B(y_1^{d-j}),$$

where $\bar{a} = (a_{i_1}, a_{i_2}, \ldots, a_{i_j})$, if we rename the remaining $d - j$ variables in the following way:

$$(x_1^{i_1-1}, x_{i_1+1}^{i_2-1}, \ldots, x_{i_j+1}^d) = (y_1^{i_1-1}, y_{i_1}^{i_2-1}, ..., y_{i_j}^d) = (y_1^{d-j}).$$

Then B is a $(d-j)$-ary operation, which is called the $(d-j)$-*ary retract* of A, defined by the positions $i_1, i_2, \ldots, i_j$ with the elements $a_{i_1}, a_{i_2}, \ldots, a_{i_j}$ in these positions.

Let H be a d-dimensional hypercube based on a set Q of order n. If we introduce a system of coordinates by d directions $x_1, x_2, ..., x_d$ with values from Q, we obtain naturally the multiplication table of a d-ary operation A_H on Q defined in the following way:

$$A_H(a_1, a_2, ..., a_d) = a_{d+1}$$

if in the position $(a_1, a_2, ..., a_d)$ of H, we place the element a_{d+1}.

Conversely, the multiplication table of a d-ary operation A is a d-dimensional cube H_A (with a system coordinates) such that the element a_{d+1} is situated in the position $(a_1, a_2, ..., a_d)$ if $A(a_1, a_2, ..., a_d) = a_{d+1}$.

Example 2. The ternary operation $A(x, y, z)$ given on the set $Q = \{1, 2, 3, 4\}$ with the multiplication table in Table 3 corresponds to the 3-dimensional hypercube in Table 2. For example, if $x = 2, y = 3, z = 2$, then $A(x, y, z) = A(2, 3, 2) = 2$.

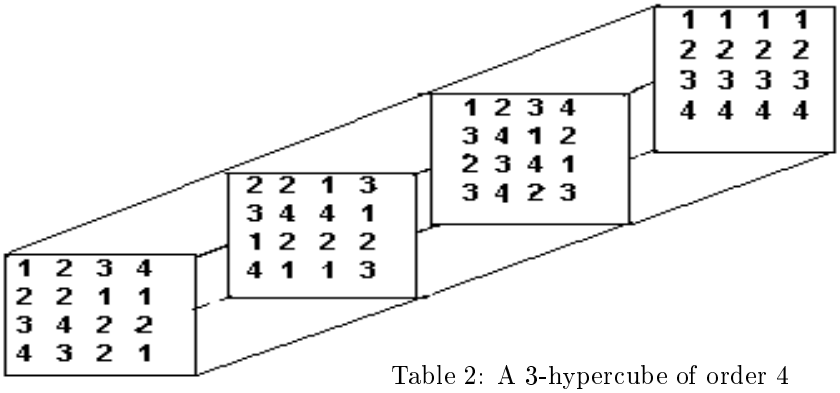

Table 2: A 3-hypercube of order 4

$x=1$	1	2	3	4
1	1	2	3	4
2	2	2	1	1
3	3	4	2	2
4	4	3	2	1

$x=2$	1	2	3	4
1	2	2	1	3
2	3	4	4	1
3	1	2	2	2
4	4	1	1	3

$x=3$	1	2	3	4
1	1	2	3	4
2	3	4	1	2
3	2	3	4	1
4	3	4	2	3

$x=4$	1	2	3	4
1	1	1	1	1
2	2	2	2	2
3	3	3	3	3
4	4	4	4	4

Table 3: A 3-operation corresponding to the 3-hypercube in Table 2

Remark 1. Below we consider a hypercube H with a fixed system of coordinates. In this case exactly one d-operation A_H corresponds to this hypercube.

Proposition 1. *A d-hypercube H (a d-operation A_H) defined on a set Q of order n has type j with $0 \leqslant j \leqslant d-1$ if and only if for any $(d-j)$-retract $B(y_1^{d-j})$ of the corresponding d-operation A_H, the equation $B(y_1^{d-j}) = a$ has exactly n^{d-j-1} solutions for each $a \in Q$.*

Proof. Assume H is a d-hypercube of type j and a d-operation A_H corresponds to H. Then every element of Q appears n^{d-j-1} times in a subarray whenever any j of the coordinates $i_1, i_2, \ldots, i_j$ and elements $a_{i_1}, a_{i_2}, \ldots, a_{i_j}$ on these places are fixed. This implies that in the respective $(d-j)$-retract $B(y_1^{d-j})$ of A_H defined by these positions and these elements, each element a of Q arises n^{d-j-1} times so that the equation $B(y_1^{d-j}) = a$ has exactly n^{d-j-1} solutions. The converse is evident. □

Corollary 1. *A d-hypercube H has type $j = d-1$ if and only if the d-operation A_H corresponding to H is a d-quasigroup.*

Proof. By Proposition 1 a d-hypercube H has type $j = d-1$ if and only if for any $(d-j) = (d-(d-1)) = 1$-retract the equation $A_H(a_1^{i-1}, x, a_{i+1}^d) = a_{d+1}$ has $n^{d-(d-1)-1} = 1$ solution for any $1 \leqslant i \leqslant d$ and for any fixed d-tuple $(a_1^{i-1}, a_{i+1}^d, a_{d+1}) \in Q^d$. This implies that the d-operation A_H is i-invertible for each $i = 1, 2, \ldots, d$. Thus A_H is a d-quasigroup. □

Note that in the case when a d-hypercube H has type $j = d-1$, it is a d-dimensional permutation cube of order n (see [5, p. 181]), that is a d-dimensional $n \times n \times \cdots \times n$ matrix of n elements with the property that every column (that is, every sequence of n elements parallel to an edge of the cube) contains a permutation of the elements. In particular, a two-dimensional permutation cube is simply a Latin square of order n.

We now recall some useful information from [1] (for the $d = 2$ case, see [2]). Let $< A_1, A_2, \ldots, A_d >$ (briefly, $< A_1^d >$) be a d-tuple of d-operations defined on a set Q. This d-tuple defines the unique mapping $\bar{\theta} : Q^d \to Q^d$ in the following way:

$$\bar{\theta} : (x_1^d) \to (A_1(x_1^d), A_2(x_1^d), \ldots, A_d(x_1^d)),$$

(or briefly, $\bar{\theta} : (x_1^d) \to (A_1^d)(x_1^d)$).

Conversely, any mapping Q^d into Q^d uniquely defines a d-tuple $< A_1^d >$ of d-operations on Q: if $\bar{\theta}(x_1^d) = (y_1^d)$, then we define $A_i(x_1^d) = y_i$ for all $i = 1, 2, \ldots, d$. Thus we obtain $\bar{\theta} = (A_1^d)$, where $\bar{\theta}(x_1^d) = (A_1^d)(x_1^d) = (A_1^d(x_1^d))$.

If C is a d-operation on Q and $\bar{\theta}$ is a mapping Q^d into Q^d, then the operation $C\bar{\theta}$ defined by the equality $C\bar{\theta}(x_1^d) = C(\bar{\theta}(x_1^d))$ is also a d-operation. Let $C\bar{\theta} = D$ and $\bar{\theta} = (A_1^d)$, then $D(x_1^d) = C(A_1^d(x_1^d))$ or briefly, $D = C(A_1^d)$. If $\bar{\theta} = (B_1^d)$ and $\bar{\varphi} = (A_1^d)$ are mappings Q^d into Q^d, then

$$\bar{\varphi}\bar{\theta} = (A_1^d)\bar{\theta} = (A_i\bar{\theta})_{i=1}^d = (A_1\bar{\theta}, A_2\bar{\theta}, \ldots, A_d\bar{\theta}).$$

If $\bar{\theta} = (B_1^d)$ is a permutation on Q^d, then $B_i = E_i\bar{\theta}$ and $B_i\bar{\theta}^{-1} = B_i(B_1^d)^{-1} = E_i$, $i = 1, 2, \ldots, d$.

Definition 1. (cf. [1]) A d-tuple $< A_1^d >$ of different d-operations on Q is called *orthogonal* if the system $\{A_i(x_1^d) = a_i\}_{i=1}^d$ has a unique solution for all $a_1^d \in Q^d$.

The d-tuple $< E_1^d >$ of selectors of arity d is the identity permutation on Q^d and is orthogonal.

There is a close connection between orthogonal d-tuples of d-operations on Q and permutations on Q^d by virtue of the following:

Proposition 2. (cf. [1]) *A d-tuple $< A_1^d >$ of d-operations is orthogonal if and only if the mapping $\bar{\theta} = (A_1^d)$ is a permutation on Q^d.*

Some properties of d-operations can be expressed by means of orthogonality. For example

Proposition 3. (cf. [1]) *A d-operation A is i-invertible $(1 \leqslant i \leqslant d)$ if and only if the d-tuple $< E_1^{i-1}, A, E_{i+1}^d >$ is orthogonal (or equivalently, the mapping $(E_1^{i-1}, A, E_{i+1}^d)$ is a permutation).*

Proposition 4. (cf. [1]) *A d-operation A is a d-quasigroup if and only if the d-tuple $< E^{i-1}, A, E_{i+1}^d >$ is orthogonal for all $i = 1, 2, \ldots, d$.*

Definition 2. (cf. [9]). Two d-operations A and B on a set Q are said to be of *one-type* if there exists a permutation $\bar{\varphi}$ on Q^d such that $A = B\bar{\varphi}$.

It is easy to check that this relation is an equivalence relation.

Definition 3. (cf. [9]) A d-operation A defined on a set Q is called *complete* if it is one-type with the selector E_1 (or with the selector E_i for some $i = 1, 2, \ldots, d$), that is $A = E_1\bar{\varphi}$ for some permutation $\bar{\varphi}$ on Q^d.

For $d = 2$ these definitions were given in [2]. A complete d-operation is always a component of a permutation $\bar{\varphi}$: if $\bar{\varphi} = (B_1, B_2, \ldots, B_d)$ and $A = E_1\bar{\varphi}$, then $A = B_1$. The converse is also true: if a d-operation A is a component of some permutation, then it is complete (see [9]). So, we have

Proposition 5. *A d-operation A can be embedded in an orthogonal d-tuple if and only if it is complete.*

From Definition 3 it follows that the completeness of a d-operation A of order n defined on Q implies that each of the n elements appears as a value of A exactly n^{d-1} times, that is the equation $A(x_1^d) = a$ has n^{d-1} solutions for any $a \in Q$. Now we can reformulate Proposition 1 as follows.

Proposition 6. *A d-hypercube H of order n has type j with $0 \leqslant j \leqslant d-1$ if and only if any $(d-j)$-retract of the respective d-operation A_H is complete.*

Indeed, in this case each of the n elements appears $n^{(d-j)-1}$ times.

Corollary 2. *A d-hypercube H has type $j = 0$ if and only if the respective d-operation A_H is complete.*

3. Orthogonal d-hypercubes and orthogonal d-operations

Two d-hypercubes H_1 and H_2 of order n are *orthogonal* if when superimposed, each of the n^2 ordered pairs appears n^{d-2} times, and a set of $s \geqslant 2$, d-hypercubes is *orthogonal* if every pair of distinct d-hypercubes is orthogonal (see [6], [8]). This notion of orthogonality for d-hypercubes leads naturally to the notion of orthogonality for d-operations.

Definition 4. Two d-operations A and B of order n defined on a set Q are said to be *orthogonal* if the pair of equations $A(x_1^d) = a$ and $B(x_1^d) = b$ has exactly n^{d-2} solutions for any elements $a, b \in Q$.

Definition 5. A set $\Sigma = \{A_1, A_2, \ldots, A_s\}$ of d-operations, with $s \geqslant 2$, is called orthogonal if every pair of distinct d-operations from Σ is orthogonal.

It is easy to see that two d-hypercubes H_1 and H_2 are orthogonal if and only if the respective d-operations A_{H_1} and A_{H_2} are orthogonal. A set of (pairwise) orthogonal d-operations corresponds to a set of (pairwise) orthogonal d-hypercubes.

In [1] another concept of an orthogonal set of d-ary operations was given.

Definition 6. (cf. [1]) A set $\{A_1, A_2, \ldots, A_s\}$, $s \geqslant d$, of d-operations is called orthogonal if every d-tuple of these d-operations is orthogonal (see Definition 1).

We point out that a similar notion for sets of d-hypercubes to be d-orthogonal was considered in [8]. In order to distinguish distinct notions of orthogonality of d-operations and of d-hypercubes we give the following

Definition 7. A *k-tuple* $< A_1, A_2, \ldots, A_k >$, $1 \leqslant k \leqslant d$, of distinct d-operations defined on a set Q is called *orthogonal* if the system

$$\{A_i(x_1^d) = a_i\}_{i=1}^k$$

has exactly n^{d-k} solutions for any $a_1^k \in Q^k$.

For $k = 1$ we say that a d-operation A is itself orthogonal (the same A is complete).

Definition 8. A set $\Sigma = \{A_1, A_2, \ldots, A_s\}$ of d-operations is called *k-wise orthogonal*, $1 \leqslant k \leqslant d$, $s \geqslant k$, if every k-tuple $A_{i_1}, A_{i_2}, \ldots, A_{i_k}$ of distinct d-operations of Σ is orthogonal.

A k-wise orthogonal set of d-hypercubes corresponds to a k-wise orthogonal set of d-operations. A 1-wise orthogonal set of d-operations is any set of complete operations. Taking into account Definition 8 we conclude that an orthogonal set of d-operations (or d-hypercubes) from Definition 5 (Definition 6) is a 2-wise orthogonal set (a d-wise orthogonal set).

Theorem 1. *If a set $\Sigma = \{A_1, A_2, \ldots, A_s\}$, $s \geqslant k$, of d-operations of order n defined on a set Q is k-wise orthogonal with $1 \leqslant k \leqslant d$, then the set Σ is l-wise orthogonal for any l with $1 \leqslant l < k$.*

Proof. Let Σ be a k-wise orthogonal set of d-operations. Consider any k, d-operations from Σ. Let these be denoted by $A_1, A_2, \ldots, A_k$. Then the system

$$\{A_1(x_1^d) = a_1, \ldots, A_k(x_1^d) = a_k\} \tag{1}$$

has n^{d-k} solutions; that is every k-tuple $a_1^k \in Q^k$ appears n^{d-k} times, since Σ is k-wise orthogonal. Fix l, d-operations $A_{i_1}, A_{i_2}, \ldots, A_{i_l}$ from A_1^k. Then the system

$$\{A_{i_1}(x_1^d) = a_{i_1},\ A_{i_2}(x_1^d) = a_{i_2},\ \ldots,\ A_{i_l}(x_1^d) = a_{i_l}\} \tag{2}$$

must have n^{d-k} solutions for every fixed $(k-l)$-tuple from the n^{k-l}, $(k-l)$-tuples of elements $a_{j_1}, a_{j_2}, \ldots, a_{j_{k-l}}$ which correspond to the remaining d-operations of A_1^k in (1). Thus the system (2) has $n^{d-k} \cdot n^{k-l} = n^{d-l}$ solutions. It follows that any l-tuple $(a_{i_1} a_{i_1}, \ldots, a_{i_l}) \in Q^l$ appears n^{d-l} times and the set Σ is l-wise orthogonal since we can take any k-tuple of d-operations in (1). □

A combinatorial interpretation of this proof may be made along the following lines. If d-hypercubes $H_1, H_2, \ldots, H_k$ of order n defined on a set Q are k-orthogonal (that is by their superimposing every k-tuple of elements appears exactly n^{d-k} times), then by superimposing any l, $1 \leqslant l \leqslant k$, of them, each l-tuple of elements must appear n^{d-k} times for each of the n^{k-l} distinct $(k-l)$-tuples of Q^{k-l}.

Theorem 2. *A d-operation A has type j with $0 \leqslant j \leqslant d-1$ if and only if the set $\Sigma = \{A, E_1^d\}$ is $(j+1)$-wise orthogonal.*

Proof. Let A be a d-operation of type j. By Theorem 1 any $(j+1)$-tuple of distinct selectors is orthogonal since the d-tuple $< E_1^d >$ is orthogonal. Consider a $(j+1)$-tuple of d-operations from Σ, which contains the d-operation A, and the respective of equations

$$\{A(x_1^d) = a_1,\ E_{i_1}(x_1^d) = a_2,\ \ldots,\ E_{i_j}(x_1^d) = a_{j+1}\}. \tag{3}$$

This system corresponds to the $(d-j)$-retract of A defined by the places $i_1, i_2, \ldots, i_j$ and elements $a_2, \ldots, a_{j+1}$ on these places and has $n^{d-j-1} = n^{d-(j+1)}$ solutions for any $a_1 \in Q$ by Proposition 1. Thus, the set Σ is $(j+1)$-wise orthogonal.

Conversely, if a set Σ is $(j+1)$-wise orthogonal, then system (3) has $n^{d-(j+1)}$ solutions for any distinct $i_1, i_2, \ldots, i_j \in \{1, 2, \ldots, d\}$ and any $a_2, \ldots, a_{j+1} \in Q$. This implies that every element a_1 appears in each $(d-j)$-retract of A exactly n^{d-j-1} times, that is, A has type j by Proposition 1. □

We note that if $j = d-1$, this result reduces to Proposition 4. From Theorems 1 and 2 we have

Corollary 3. *A d-operation of type j with $0 \leqslant j \leqslant d-1$ has type j_1 for all j_1 with $0 \leqslant j_1 < j$.*

We now provide a method to construct orthogonal d-tuples of d-operations (and by Theorem 1, a k-wise orthogonal set with d, d-operations, $2 \leqslant k < d$), using properties of d-operations.

Let $A_1, A_2, ..., A_d$ be d-operations defined on a set Q and assume that the operation A_i, $1 \leqslant i \leqslant d$, is $(d-i+1)$-invertible. Recursively define the following d-operations:

$$\left.\begin{aligned}
B_1(x_1^d) &= A_1(x_1^d),\\
B_2(x_1^d) &= A_2(x_1^{d-1}, B_1(x_1^d)),\\
B_3(x_1^d) &= A_3(x_1^{d-2}, B_1(x_1^d), B_2(x_1^d)),\\
&\cdots\cdots\cdots\cdots\cdots\cdots\\
B_i(x_1^d) &= A_i(x_1^{d-(i-1)}, B_1(x_1^d), B_2(x_1^d), ..., B_{i-1}(x_1^d)),\\
&\cdots\cdots\cdots\cdots\cdots\cdots\\
B_d(x_1^d) &= A_d(x_1^{d-(d-1)}, B_1(x_1^d), B_2(x_1^d), ..., B_{d-1}(x_1^d)).
\end{aligned}\right\} \qquad (4)$$

Theorem 3. *The d-tuple $< B_1, B_2, ..., B_d >$ defined by (4) is orthogonal.*

Proof. Consider the system of equations $\{B_i(x_1^d) = a_i\}_{i=1}^d$ and substitute the values of $B_1, B_2, ..., B_{d-1}$ into the last equation:

$$B_d(x_1^d) = A_d(x_1, a_1, a_2, ..., a_{d-1}) = a_d.$$

From this equation we obtain a unique $x_1 = b_1$ since the d-operation B_d is $d - d + 1$=1-invertible. Now substitute this value of x_1 and the values of $B_1, B_2, ..., B_{d-2}$ into the $(d-1)$-th equation:

$$B_{d-1}(b_1, x_2^d) = A_{d-1}(b_1, x_2, a_1, a_2, ..., a_{d-2})$$

from which we obtain a unique $x_2 = b_2$ by virtue of the $d-(d-1)+1 = 2$-invertibility of A_{d-1}. In the same way at the last step we would obtain

$$B_1(b_1, b_2, ..., b_{d-1}, x_d) = A_1(b_1, b_2, ..., b_{d-1}, x_d) = a_1$$

whence we obtain a unique $x_d = b_d$ using the d-invertibility of A_1.

Thus, the given system has a unique solution $x_1 = b_1, x_2 = b_2, ..., x_d = b_d$ and the d-tuple $< B_1, B_2, ..., B_d >$ is orthogonal. □

The above theorem generalizes Theorem 2 of [4], in which all d-operations A_i, $1 \leqslant i \leqslant d$, are parastrophes [3] of one d-quasigroup.

As a particular case we can take $A_1 = A_2 = \cdots = A_d = A$ where A is an arbitrary d-quasigroup (it is, by definition, i-invertible for any i, $1 \leqslant i \leqslant d$). Then all of the d-operations B_i,$i \leqslant d$, are expressed by means of the d-quasigroup A:

$$
\begin{aligned}
B_1(x_1^d) &= A(x_1^d),\\
B_2(x_1^d) &= A(x_1^{d-1}, A(x_1^d)),\\
B_3(x_1^d) &= A(x_1^{d-2}, A(x_1^d), A(x_1^{d-1}, A(x_1^d))),\\
&\cdots\cdots\cdots\cdots\cdots\cdots\\
B_d(x_1^d) &= A(x_1, B_1(x_1^d), B_2(x_1^d), ..., B_{d-1}(x_1^d)),
\end{aligned}
$$

where each B_i is determined by A.

We shall illustrate this situation when

$$B_1(x,y,z) = A(x,y,z) = x + y + z (\text{mod } n), \quad n > 4.$$

In this case

$$
\begin{aligned}
B_2(x,y,z) &= A(x,y,A(x,y,z))\\
&= x + y + (x + y + z) = 2x + 2y + z \ (\text{mod } n),\\
B_3(x,y,z) &= A(x, A(x,y,z), A(x,y,A(x,y,z)))\\
&= x + (x + y + z) + (2x + 2y + z) = 4x + 3y + 2z \ (\text{mod } n).
\end{aligned}
$$

By Theorem 1 the 3-tuple $< B_1, B_2, B_3 >$ of 3-operations is orthogonal. In this example all of these 3-operations are 3-quasigroups if n is not divisible by 2 or 3; otherwise B_2 or B_3 is not a 3-quasigroup.

For the ternary case we can prove the stronger statement than in the above theorem.

Proposition 7. *Let A be a 3-quasigroup and $\Sigma = \{B_1, B_2, B_3, B_4\}$ be a set of 3-operations where*

$$
\begin{aligned}
B_1(x,y,z) &= A(x,y,z),\\
B_2(x,y,z) &= A(x,y,B_1(x,y,z)),\\
B_3(x,y,z) &= A(x,B_1(x,y,z),B_2(x,y,z)),\\
B_4(x,y,z) &= A(B_1(x,y,z),B_2(x,y,z),B_3(x,y,z)).
\end{aligned}
$$

Then Σ is a 3-wise orthogonal set.

Proof. Orthogonality of the 3-tuple $< B_1, B_2, B_3 >$ follows from the above theorem.

For the triple $< B_1, B_3, B_4 >$ we have the system

$$\{B_1(x,y,z) = a, \quad B_3(x,y,z) = b, \quad B_4(x,y,z) = c\}.$$

From the third equation taking into account the first one and the form of B_2 we obtain $A(a, A(x,y,a), b) = c$, whence it follows that

$$A(x,y,a) = {}^{(2)}A(a,c,b) = d_0, \tag{5}$$

where ${}^{(2)}A$ is the 2-th inverse 3-quasigroup for A (by the definition

$$A(x_1^d) = x_{d+1} \iff {}^{(i)}A(x_1^{i-1}, x_{d+1}, x_{i+1}^d) = x_i, \quad 1 \leqslant i \leqslant d \ \ [3]).$$

Using (5) and the first equation of the system in the second one we obtain $A(x, a, A(x, y, a)) = A(x, a, d_0) = b$ and so we obtain a unique $x = x_0$. Substituting x_0 in (5) we obtain a unique $y = y_0$. Finally from the first equation we have $A(x_0, y_0, z) = a$ and $z = z_0$.

Consider the 3-tuple $< B_2, B_3, B_4 >$ and the corresponding system

$$\{B_2(x, y, z) = a, \quad B_3(x, y, z) = b, \quad B_4(x, y, z) = c\}.$$

Using the first and the second equations in the third: $A(A(x, y, z), a, b) = c$ whence it follows that

$$A(x, y, z) = {}^{(1)}A(c, a, b) = d_1. \tag{6}$$

Then from the second with the first equation we have $A(x, d_1, a) = b$ and $x = x_0$. Now use the first equation: $A(x_0, y, d_1) = a$, whence we obtain $y = y_0$. Finally from (6), using x_0 and y_0, we obtain a unique $z = z_0$. □

4. Complete k-tuples of d-operations and embeddings

From Proposition 5 it follows that a complete d-operation (Definition 3) can always be extended, or completed, to an orthogonal d-tuple of d-operations. We shall show that any orthogonal k-tuple ($1 \leqslant k < d$) of d-operations can be embedded in an orthogonal d-tuple of d-operations.

We first generalize the concept of a complete d-operation in the following way. As was indicated above, any mapping Q^d into Q^d uniquely defines a d-tuple $< B_1, B_2, \ldots, B_d >$ such that $\bar{\varphi}(x_1^d) = (B_1(x_1^d), B_2(x_1^d), \ldots, B_d(x_1^d))$, or briefly, $\bar{\varphi} = (B_1, B_2, \ldots, B_d)$. Moreover, by Proposition 2 $\bar{\varphi}$ is permutation on Q^d if and only if the d-tuple $< B_1, B_2, \ldots, B_d >$ is orthogonal.

Definition 9. A k-tuple $< A_1, A_2, \ldots, A_k >$, $1 \leqslant k \leqslant d$, of distinct d-operations given on a set Q is called *complete* if there exists a permutation $\bar{\varphi} = (B_1, B_2, \ldots, B_d)$ on Q^d such that

$$(A_1, A_2, \ldots, A_k)(x_1^d) = (E_1, E_2, \ldots, E_k)\bar{\varphi}(x_1^d) \tag{7}$$

where E_i, $i = 1, 2, ..., k$, is the $i - th$ selector of arity d on Q.

For $k = 1$ we obtain the definition of a complete d-operation.

Theorem 4. *A k-tuple of d-operations ($1 \leqslant k \leqslant d$) is orthogonal if and only if it is complete.*

Proof. Let $< A_1^k >$ be an orthogonal k-tuple of d-operations. We will show that it is complete. Define a mapping $\bar{\varphi}$ on Q^d in the following way

$$\bar{\varphi}(x_1, x_2, \ldots, x_d)_{(a_1^k)} = (a_1^k, y_{k+1}^d),$$

where $(x_1, \ldots, x_d)_{(a_1^k)}$ denotes all n^{d-k} collections of coordinates such that

$$(A_1, A_2, \ldots, A_k)(x_1, x_2, \ldots, x_d)_{(a_1^k)} = (a_1, a_2, \ldots, a_k), \tag{8}$$

and where y_{k+1}^d runs through all different n^{d-k}, $(d-k)$-tuples from Q^{d-k} (arbitrarily associated to the distinct collections $(x_1, x_2, \ldots, x_d)_{(a_1^k)}$ for a fixed (a_1^k)), when (8) holds.

It is easy to see that $\bar{\varphi}(x_1^d)$ is a permutation on Q^d since $(a_1^k, y_{k+1}^d) \neq (b_1^k, y_{k+1}^d)$ if $a_1^k \neq b_1^k$ (there is an i such that $a_i \neq b_i$) and $(a_1^k, y_{k+1}^d) \neq (a_1^k, z_{k+1}^d)$ if $y_{k+1}^d \neq z_{k+1}^d$ by the definition of $\bar{\varphi}$. In this case

$$(A_1, A_2, \ldots, A_k)(x_1^d) = (E_1, E_2, \ldots, E_k)\bar{\varphi}(x_1^d).$$

Conversely, assume that a k-tuple $< A_1^k >$ of d-operations is complete so that equality (7) holds. Then $(A_1, A_2, \ldots, A_k)(x_1^d) = (E_1, E_2, \ldots, E_k)$ $(B_1, B_2, \ldots, B_d)(x_1^d) = (B_1 B_2, \ldots, B_k)(x_1^d)$. Hence, $A_i = B_i,\ i = 1, 2, \ldots, k$, and the permutation $\bar{\varphi}$ has the form

$$\bar{\varphi} = (A_1, \ldots, A_k, B_{k+1}, \ldots, B_d).$$

By Proposition 2 the d-tuple $< A_1^k, B_{k+1}^d >$ of d-operations is orthogonal and because of Theorem 1, the k-tuple $< A_1^k >$ is also orthogonal. □

Remark 2. Let $< A_1^k >$ be a k-tuple of d-operations on Q. This k-tuple defines a mapping $\bar{\theta}_k$: Q^d in Q^k in the following way:

$$\bar{\theta}_k(x_1^d) = (A_1, A_2, ..., A_k)(x_1^d).$$

Conversely, any mapping $\bar{\theta}_k$: Q^d into Q^k defines a k-tuple $< A_1^k >$ of d-operations on Q: if $\bar{\theta}_k(x_1^d) = (y_1^k)$, then we define $A_i(x_1^d) = y_i$ for all $i = 1, 2, ..., k$.

Consider the following notion: $\bar{\varepsilon}_k(x_1^d) = (E_1, E_2, ..., E_k)(x_1^d)$, where E_i is the i-th selector on Q. Then Definition 9 and Theorem 4 imply that a k-tuple $< A_1^k >$ is orthogonal if and only if for the mapping $\bar{\theta}_k$ there exists a permutation $\bar{\varphi}$ on Q^d such that

$$\bar{\theta}_k(x_1^d) = \bar{\varepsilon}_k \bar{\varphi}(x_1^d). \tag{9}$$

Thus, any k-tuple of orthogonal d-operations given on a set Q is defined by some permutation on Q^d by (9) and conversely, any permutation on Q^d gives a k-tuple of orthogonal d-operations given on Q for each k, $2 \leqslant k \leqslant d$.

Corollary 4. *Any orthogonal k-tuple $< A_1^k >$, $1 \leqslant k \leqslant d$, of d-operations can be embedded in an orthogonal d-tuple $< A_1^k, B_{k+1}^d >$ of d-operations.*

Proof. An orthogonal k-tuple $< A_1^k >$ is complete by Theorem 4 and so it follows from the proof of that theorem that the d-operations $A_1, A_2, \ldots, A_k$ are components of a permutation $\bar{\varphi} = (A_1^k, B_{k+1}^d)$. Taking into account Proposition 2 it follows that the k-tuple $< A_1^k >$ is embedded in the orthogonal d-tuple $< A_1^k, B_{k+1}^d >$. □

References

[1] **A. S. Bektenov and T. Yakubov**: *Systems of orthogonal n-ary operations*, (Russian). Bol. (Izv.) AN Moldavskoi SSR, Ser. fiz.-teh. i mat. nauk, no. 3, 1974, 7 – 14.

[2] **V. D. Belousov**: *On properties of binary operations*, (Russian), Uchenye zapiski Bel'tskogo pedinstituta No.5, 1960, 9 – 28.

[3] **V. D. Belousov**: *n-ary quasigroups*, (Russian), Shtiintsa, Kishinev 1972.

[4] **V. D. Belousov and T. Yakubov**: *On n-ary operations*, (Russian), Collection "Combinatornaya matematica", Moscow 1974, 3 – 17.

[5] **J. Dénes and A. D. Keedwell**: *Latin Squares and Their Applications*, Academian Kiado, Budapest 1974.

[6] **K. Kishen**: *On the construction of Latin and hyper-graceo-Latin cubes and hypercubes*, J. Ind. Soc. Agric. Statist. **2** (1950), 20 – 48.

[7] **C. F. Laywine and G. L. Mullen**: *Discrete Mathematics Using Latin Squares*, Wiley, New York 1998.

[8] **C. F. Laywine, G. L. Mullen and G. Whittle**, *D-Dimensional hypercubes and the Euler and MacNeish conjectures*, Monatsh. Math. **111** (1995), 223 – 238.

[9] **T. Yakubov**: *On $(2, n)$-semigroup of n-ary operations*, (Russian), Bol. (Izv.) AN Mold. SSR, Ser. fiz.-teh. i mat. nauk, no. 1, 1974, 29 – 46.

Received February 17, 2005

G. B. Belyavskaya
Institute of Mathematics and Computer Science, Academy of Sciences,
Academiei str. 5 MD-2028, Chisinau, Moldova
e-mail: gbel@math.md

Gary L. Mullen
Department of Mathematics, The Pennsylvania State University, University Park, PA 16802, USA
e-mail: mullen@math.psu.edu