PUBLICATIONS DE L'INSTITUT MATHÉMATIQUE
Nouvelle série, tome 101(115) (2017), 109–119 https://doi.org/10.2298/PIM1715109M

ON CONSTRUCTION OF ORTHOGONAL d-ARY OPERATIONS

Smile Markovski and Aleksandra Mileva

In Memory of Prof. G. B. Belyavskaya

ABSTRACT. A d-hypercube of order n is an $n \times \cdots \times n_d$ (d times) array with n^d elements from a set Q of cardinality n. We recall several connections between d-hypercubes of order n and d-ary operations of order n. We give constructions of orthogonal d-ary operations that generalize a result of Belyavskaya and Mullen. Our main result is a general construction of d-orthogonal d-ary operations from d-ary quasigroups.

1. Introduction

In this paper we work with positive integers and we assume that $d \geqslant 2$. A *hypercube of order n and dimension d* (or *d-hypercube of order n*, or *d-dimensional hypercube of order n*) is an $n \times \cdots \times n_d$ (d times) array with n^d elements obtained from the set of n distinct symbols. For $1 \leqslant t \leqslant d$, a *$t$-subarray* is a subset of a d-hypercube of order n which is obtained by fixing $d-t$ of the coordinates and allowing the other t coordinates to vary. Given d-hypercube of order n has *type t*, $0 \leqslant t \leqslant d-1$, if each symbol occurs exactly n^{d-t-1} times in each $(d-t)$-dimensional subarray [**12**]. It is clear that every d-hypercube of order n and type t, has also type i, for each $0 \leqslant i \leqslant t-1$. A Latin square of order n is a 2-hypercube of order n and type 1.

A *d-ary operation* f on a nonempty set Q is a mapping $f\colon Q^d \to Q$ defined by $f\colon (x_1,\dots,x_d) \mapsto x_{d+1}$, for which we write $f(x_1,\dots,x_d) = x_{d+1}$. A d-ary groupoid ($d \geqslant 1$) is an algebra (Q,f) on a nonempty set Q as its universe and with one d-ary operation f. A d-ary groupoid (Q,f) is called a *d-ary quasigroup* if any d of the elements $a_1,a_2,\dots,a_{d+1} \in Q$, satisfying $f(a_1,a_2,\dots,a_d) = a_{d+1}$, uniquely specifies the remaining one.

2010 *Mathematics Subject Classification:* 05B15; 20N05; 20N15.

Key words and phrases: Latin hypercube, orthogonal hypercubes, orthogonal functions, recursively differentiable quasigroups.

Communicated by Žarko Mijajlović.

A d-ary operation f defined on Q is said to be *i-invertible* if the equation

$$f(a_1, \dots, a_{i-1}, x, a_{i+1}, \dots, a_d) = a_{d+1}$$

has a unique solution x for each d-tuple $(a_1, \dots, a_{i-1}, a_{i+1}, \dots, a_d, a_{d+1})$ of Q^d. Equivalently, we can define a d-ary quasigroup to be a d-ary groupoid (Q, f) such that the d-ary operation f is i-invertible for each $i = 1, \dots, d$.

Given a d-ary quasigroup (Q, f), d new d-ary operations ${}^{(i)}f$, $i = 1, 2, \dots, d$, can be defined by

$${}^{(i)}f(x_1, x_2, \dots, x_d) = x_{d+1} \Leftrightarrow f(x_1, \dots, x_{i-1}, x_{d+1}, x_{i+1}, \dots, x_d) = x_i.$$

Then $(Q, {}^{(i)}f)$ are d-ary quaisgroups too. The operation ${}^{(i)}f$ is called the i-th *inverse operation* of f [**1**]. We note that the following equalities are identities in the algebra $(Q, f, {}^{(i)}f)$:

$$f\big(x_1, \dots, x_{i-1}, {}^{(i)}f(x_1, x_2, \dots, x_d), x_{i+1}, \dots, x_d\big) = x_i,$$

$${}^{(i)}f\big(x_1, \dots, x_{i-1}, f(x_1, x_2, \dots, x_d), x_{i+1}, \dots, x_d\big) = x_i.$$

A d-ary groupoid (Q, f) is of order n when $|Q| = n$. Belyavskaya and Mullen [**4**] proved that a d-ary quasigroup of order n is an algebraic equivalent of a d-hypercube of order n and type $d-1$.

In this paper we give generalizations of some results given in [**4**]. In Section 2 we survey the definitions that can be found in the literature of orthogonality and connections between d-ary hypercubes, d-ary operations and d-ary quasigroups. The main results are given in Section 3, where several new constructions of orthogonal d-tuple are presented.

2. *d*-ary hypercubes, *d*-ary operations, *d*-ary quasigroups and orthogonality

The usual definition of orthogonality states that two d-hypercubes of order n are *orthogonal* if each ordered pair occurs exactly n^{d-2} times upon superimposition. Similarly, two d-ary operations f and h defined on a set Q of cardinality n are said to be *orthogonal* if the pair of equations $f(x_1, \dots, x_d) = u$ and $h(x_1, \dots, x_d) = v$ has exactly n^{d-2} solutions for any given elements $u, v \in Q$.

A set of d hypercubes of order n and dimension d is said to be *d-orthogonal* (or *d-wise orthogonal*) if, when superimposed, each of the n^d ordered d-tuples occurs exactly once. (This is the concept of dimensional orthogonality in [**8, 9**] and of variational cube in [**10**]). The set of $m \geqslant d$ hypercubes of order n and dimension d is called *mutually d-orthogonal* (MdOH) if, given any d hypercubes from the set, they are d-orthogonal (also known as d-dimensional variational set in [**7**]).

One can define a general form of orthogonality that includes standard form of d-orthogonality. For $2 \leqslant k \leqslant d$, a set of k hypercubes of order n and dimension d is said to be *k-orthogonal* if, when superimposed, each of the n^k ordered k-tuples occurs exactly n^{d-k} times. A set of $j \geqslant k$ hypercubes of order n and dimension d is called *mutually k-orthogonal* if, given any k hypercubes from the set, they are k-orthogonal.

For d-ary operations we have the following definitions.

Definition 2.1 ([**2, 3**] for $k = d$, [**4**]). A k-tuple $\langle f_1, f_2, \ldots, f_k\rangle$, $1 \leqslant k \leqslant d$, of distinct d-ary operations defined on a set Q is *orthogonal* if the system of equations $\{f_i(x_1, \ldots, x_d) = a_i\}_{i=1}^{k}$ has exactly n^{d-k} solutions for any $a_1, \ldots, a_k \in Q^n$.

Definition 2.2. [**4**] A set $\Sigma = \{f_1, f_2, \ldots, f_s\}$ of d-ary operations is *k-orthogonal*, $1 \leqslant k \leqslant d$, $k \leqslant s$, if every k-tuple $f_{i_1}, f_{i_2}, \ldots, f_{i_k}$ of distinct d-ary operations of Σ is orthogonal.

A set of k-orthogonal d-hypercubes of order n correspond to a set of k-orthogonal d-ary operations of order n.

Let $\langle f_1, f_2, \ldots, f_d\rangle$ be a d-tuple of d-ary operations defined on a set Q. Then a unique mapping $\theta = (f_1, f_2, \ldots, f_d)\colon Q^n \to Q^n$ is defined by

$$\theta\colon (x_1, \ldots, x_d) \mapsto (f_1(x_1, \ldots, x_d), f_2(x_1, \ldots, x_d), \ldots, f_d(x_1, \ldots, x_d)).$$

The following proposition gives a connection between the orthogonal d-tuple of d-ary operations and the permutations on Q^d.

Proposition 2.1. [**3**] *A d-tuple $\langle f_1, f_2, \ldots, f_d\rangle$ of different d-ary operations on Q is orthogonal if and only if the mapping $\theta = (f_1, f_2, \ldots, f_d)$ is a permutation on Q^n.*

Further, we give another connection between d-ary hypercubes of order n and d-ary operations of order n. The d-ary operation I_j, $1 \leqslant j \leqslant d$, defined on Q by $I_j(x_1, x_2, \ldots, x_d) = x_j$, is called the *$j$-th selector* or the *$j$-th projection.*

Definition 2.3. [**3**] A set $\Sigma = \{f_1, f_2, \ldots, f_r\}$ of distinct d-ary operations defined on a set Q is *strong orthogonal* (or *strong d-wise orthogonal*) if the set $\{I_1, \ldots, I_d, f_1, f_2, \ldots, f_r\}$ is d-orthogonal, where each $I_j, 1 \leqslant j \leqslant d$, is the j-th selector.

It follows that each operation of a strong orthogonal set, which is not a selector, is a quasigroup operation. Clearly, if $r \geqslant d$, a strong d-orthogonal set is d-orthogonal, as well.

Similarly, a set of r hypercubes of order n and dimension d is called *mutually strong d-orthogonal* (MSdOH) if upon superimposition of corresponding j-subarrays of any j hypercubes in the set, $1 \leqslant j \leqslant \min(d, r)$, each ordered j-tuple appears exactly once [**8**]. Letting $j = 1$, it implies that each hypercube in the set is of type $d - 1$, and for $d = 2$ and $r \geqslant 2$, this definition is equivalent to the definition of MOLS (mutually orthogonal Latin squares). Additionally, if $r \geqslant d$, strong d-orthogonality implies d-orthogonality. There are at most $n - 1$ mutually strong d-orthogonal hypercubes of dimension d and order n.

A set of r mutually strong d-orthogonal d-hypercubes of order n corresponds to a set of r mutually strong d-orthogonal d-ary operations of order n.

3. Constructions of orthogonal d-ary operations

The main motivation for our first construction is the following theorem.

THEOREM 3.1. [4] *Let $\langle f_1, f_2, \dots, f_d\rangle$ be a d-tuple of d-ary operations defined on a set Q and let f_i, $1 \leqslant i \leqslant d$, be $(d-i+1)$-invertible d-ary operation. Then the d-tuple $\langle F_1, F_2, \dots, F_d\rangle$, defined by*

$$\begin{aligned} F_1(x_1,\dots,x_d) &= f_1(x_1,\dots,x_d),\\ F_2(x_1,\dots,x_d) &= f_2(x_1,\dots,x_{d-1},F_1(x_1,\dots,x_d)),\\ F_3(x_1,\dots,x_d) &= f_3(x_1,\dots,x_{d-2},F_1(x_1,\dots,x_d),F_2(x_1,\dots,x_d)),\\ &\vdots\\ F_d(x_1,\dots,x_d) &= f_d(x_1,F_1(x_1,\dots,x_d),F_2(x_1,\dots,x_d),\dots,F_{d-1}(x_1,\dots,x_d)), \end{aligned}$$

is orthogonal.

Similarly, we can go one step further.

THEOREM 3.2. *Let $\langle f_1, f_2, \dots, f_d\rangle$ be d-ary operations defined on a set Q and let f_i, $1 \leqslant i \leqslant d$, be i-invertible d-ary operation. Then the d-tuple $\langle F_1, F_2, \dots, F_d\rangle$, defined by*

$$\begin{aligned} F_1(x_1,\dots,x_d) &= f_1(x_1,\dots,x_d),\\ F_2(x_1,\dots,x_d) &= f_2(F_1(x_1,\dots,x_d),x_2,\dots,x_d),\\ F_3(x_1,\dots,x_d) &= f_3(F_2(x_1,\dots,x_d),F_1(x_1,\dots,x_d),x_3,\dots,x_d),\\ &\vdots\\ F_d(x_1,\dots,x_d) &= f_d(F_{d-1}(x_1,\dots,x_d),\dots,F_1(x_1,\dots,x_d),x_d), \end{aligned}$$

is orthogonal.

PROOF. Consider the system $\{F_i(x_1,\dots,x_d)=a_i\}_{i=1}^d$ and substitute the values of $F_1,\dots,F_{d-1}$ into the last of previous equalities

$$F_d(x_1,\dots,x_d) = a_d = f_d(a_{d-1},a_{d-2},\dots,a_1,x_d).$$

We obtain a unique solution $x_d = b_d$ since the f_d is d-invertible operation, and so the F_d is d-invertible operation. Next, we substitute this value of x_d and the values of $F_1,\dots,F_{d-2}$ into the $(d-1)$-th equation

$$F_{d-1}(x_1,\dots,x_{d-1},b_d) = f_{d-1}(a_{d-2},a_{d-3},\dots,a_1,x_{d-1},b_d) = a_{d-1},$$

and we obtain a unique $x_{d-1} = b_{d-1}$ using the $(d-1)$-invertibility of f_{d-1}; F_{d-1} is $(d-1)$-invertible too. So, we do similar substitutions in all equalities till the first one, in which we would obtain

$$F_1(x_1,b_2,\dots,b_d) = f_1(x_1,b_2,\dots,b_d) = a_1,$$

and again we obtain a unique $x_1 = b_1$ from 1-invertibility of f_1.

So, the given system has a unique solution $x_1 = b_1, x_2 = b_2, \dots, x_d = b_d$ and the d-tuple $F_1,\dots,F_d$ is orthogonal. □

Now, we give the following generalization of the previous result.

THEOREM 3.3. *Let $\langle f_1, f_2, \dots, f_d\rangle$ be d-ary operations defined on a set Q and let f_i, $1 \leqslant i \leqslant d$, be p_i-invertible d-ary operations, where $p_1,\dots,p_d$ is a permutation of the positions $1,\dots,d$. Let the d-tuple $\langle F_1, F_2, \dots, F_d\rangle$ be defined by the procedure*

$$F_1(x_1,\dots,x_d) = f_1(x_1,\dots,x_d),$$

$$F_2(x_1,\dots,x_d) = f_2(x_1,\dots,x_{p_1-1},F_1(x_1,\dots,x_d),x_{p_1+1},\dots,x_d),$$
$$F_i(x_1,\dots,x_d) = f_i(y_1,\dots,y_d),\ i=3,\dots,d,$$

where $y_{p_{i-1}} = F_1(x_1,\dots,x_d)$, $y_{p_{i-2}} = F_2(x_1,\dots,x_d)$,..., $y_{p_1} = F_{i-1}(x_1,\dots,x_d)$, *and* $y_j = x_j$ *for* $j \notin \{p_1,\dots,p_{i-1}\}$. *Then, the* d*-tuple* $\langle F_1, F_2,\dots,F_d\rangle$ *is orthogonal.*

Proof. Consider the system $\{F_i(x_1,\dots,x_d) = a_i\}_{i=1}^d$ and substitute the values of $F_1,\dots,F_{d-1}$ into the last equation:

$$F_d(x_1,\dots,x_d) = f_d(y_1,\dots,y_d) = a_d$$

where $y_{p_{d-1}} = a_1$, $y_{p_{d-2}} = a_2$, $\dots, y_{p_1} = a_{d-1}$, and $y_{p_d} = x_{p_d}$. We obtain a unique $x_{p_d} = b_{p_d}$ since the f_d is p_d-invertible operation, and so the F_d is p_d-invertible operation. Next, we substitute this value of x_{p_d} and the values of $F_1,\dots,F_{d-2}$ into the $(d-1)$-th equation:

$$F_{d-1}(x_1,\dots,x_{p_d-1},b_{p_d},x_{p_d+1},\dots,x_d) = f_{d-1}(y_1,\dots,y_d) = a_{d-1},$$

where $y_{p_{d-2}} = a_1$, $y_{p_{d-3}} = a_2$, $\dots, y_{p_1} = a_{d-2}$, $y_{p_d} = b_{p_d}$, and $y_{p_{d-1}} = x_{p_{d-1}}$. We obtain a unique $x_{p_{d-1}} = b_{p_{d-1}}$ using the p_{d-1}-invertibility of f_{d-1}. So, we do similar substitutions in all equalities till the first one, in which we would obtain

$$F_1(b_1,\dots,b_{p_1-1},x_{p_1},b_{p_1+1},\dots,b_d) = f_1(b_1,\dots,b_{p_1-1},x_{p_1},b_{p_1+1},\dots,b_d) = a_1,$$

and again we obtain a unique $x_{p_1} = b_{p_1}$ from p_1-invertibility of f_1.

So, the given system has a unique solution $x_1 = b_1, x_2 = b_2,\dots,x_d = b_d$ and the d-tuple $F_1,\dots,F_d$ is orthogonal. □

The systems from Theorem 3.1 and Theorem 3.2 are special cases of Theorem 3.3, where we use the permutation $d, d-1,\dots,1$ in the first case, and $1,2,\dots,d$ in the second case.

Another special case of Theorem 3.3 is when $f_1 = \dots = f_d = f$, where f is d-ary quasigroup operation.

Corollary 3.1. *Let* f *be a* d*-ary quasigroup operation, and let* $p_1,\dots,p_d$ *be a permutation of the positions* $1,\dots,d$. *Then the system of operations* $\langle F_1,\dots,F_d\rangle$*:*

$$F_1(x_1,\dots,x_d) = f(x_1,\dots,x_d),$$
$$F_2(x_1,\dots,x_d) = f(x_1,\dots,x_{p_1-1},F_1(x_1,\dots,x_d),x_{p_1+1},\dots,x_d),$$
$$F_i(x_1,\dots,x_d) = f(y_1,\dots,y_d),\ i=3,\dots,d,$$

where $y_{p_{i-1}} = F_1(x_1,\dots,x_d)$, $y_{p_{i-2}} = F_2(x_1,\dots,x_d)$,..., $y_{p_1} = F_{i-1}(x_1,\dots,x_d)$, *and* $y_j = x_j$ *for* $j \notin \{p_1,\dots,p_{i-1}\}$ *is orthogonal.*

Example 3.1. Let (Q,f) be the 4-ary quasigroup on $Q = \{0,1,2,3\}$ defined by $f(x_1,x_2,x_3,x_4) = x_1+x_2+x_3+x_4 \mod 4$. Take in Corollary 3.1 the permutation $3,1,2,4$ of the positions $1,2,3,4$. Then the following 4-tuple $\langle F_1,F_2,F_3,F_4\rangle$ of orthogonal 4-ary operations is obtained, where F_2, F_3, and F_4 are not 4-ary quasigroup operations:

$$F_1(x_1,x_2,x_3,x_4) = f(x_1,x_2,x_3,x_4) = x_1+x_2+x_3+x_4 \mod 4,$$
$$F_2(x_1,x_2,x_3,x_4) = f(x_1,x_2,F_1(x_1,x_2,x_3,x_4),x_4) = 2x_1+2x_2+x_3+2x_4 \mod 4,$$

$$\begin{aligned}F_3(x_1,x_2,x_3,x_4) &= f(F_1(x_1,x_2,x_3,x_4),x_2,F_2(x_1,x_2,x_3,x_4),x_4)\\ &= 3x_1+2x_3 \mod 4,\\ F_4(x_1,x_2,x_3,x_4) &= f(F_2(x_1,x_2,x_3,x_4),F_1(x_1,x_2,x_3,x_4),F_3(x_1,x_2,x_3,x_4),x_4)\\ &= 2x_1+3x_2 \mod 4.\end{aligned}$$

One can see that F_2 is 3-invertible, F_3 is 1-invertible and F_4 is 2-invertible 4-ary operation.

We will prove that this system of functions can not be obtained from some other set of linear 4-ary operations by using Belyavskaya and Mullen method from Theorem 3.1. Let suppose the opposite - that the system F_1, F_2, F_3, F_4 can be obtained by a set $\langle g_1, g_2, g_3, g_4\rangle$ of linear 4-ary operations using Theorem 3.1, where g_1 is 4-invertible, g_2 is 3-invertible, g_3 is 2-invertible, and g_4 is 1-invertible operation. In other words, we suppose that $\langle G_1, G_2, G_3, G_4\rangle = \langle F_1, F_2, F_3, F_4\rangle$, where G_i are got from g_i as in Theorem 3.1. It is clear from Theorem 3.1 that if g_i is k-invertible, then G_i is k-invertible too. Then, the following system with unknown linear functions g_i on $(\mathbb{Z}_4,+)$ should be satisfied:

$$\begin{aligned}G_1(x_1,x_2,x_3,x_4) &= g_1(x_1,x_2,x_3,x_4) = F_1(x_1,x_2,x_3,x_4)\\ &= x_1+x_2+x_3+x_4 \mod 4,\\ G_2(x_1,x_2,x_3,x_4) &= g_2(x_1,x_2,x_3,G_1(x_1,x_2,x_3,x_4)) = F_2(x_1,x_2,x_3,x_4)\\ &= 2x_1+2x_2+x_3+2x_4 \mod 4,\\ G_3(x_1,x_2,x_3,x_4) &= g_3(x_1,x_2,G_1(x_1,\dots,x_4),G_2(x_1,\dots,x_4))\\ &= F_3(x_1,\dots,x_4) = 3x_1+2x_3 \mod 4,\\ G_4(x_1,x_2,x_3,x_4) &= g_4(x_1,G_1(x_1,\dots,x_4),G_2(x_1,\dots,x_4),G_3(x_1,\dots,x_4))\\ &= F_4(x_1,\dots,x_4) = 2x_1+3x_2 \mod 4.\end{aligned}$$

It can be easily seen that this system has no 4-ary linear function solutions g_1, g_2, g_3, g_4. Hence, we conclude that our generalization of Theorems 1 and 2 is sound.

PROPOSITION 3.1. *Every d-ary quasigroup (Q,f) of order n can rise at most $d!$ different d-tuples $\langle F_1, F_2, \dots, F_d\rangle$ of orthogonal d-ary operations generated by the procedure given in Corollary 3.1, where $f_1 = \dots = f_d = f$.*

The following proposition is a generalization of Proposition 7 in [**4**].

PROPOSITION 3.2. *Let (Q,f) be a d-ary quasigroup of order n. Then the $(d+1)$-tuple $\langle F_1, F_2, \dots, F_{d+1}\rangle$, defined by*

$$\begin{aligned}F_1(x_1,\dots,x_d) &= f(x_1,\dots,x_d),\\ F_2(x_1,\dots,x_d) &= f(x_1,\dots,x_{d-1},F_1(x_1,\dots,x_d)),\\ F_3(x_1,\dots,x_d) &= f(x_1,\dots,x_{d-2},F_1(x_1,\dots,x_d),F_2(x_1,\dots,x_d)),\\ &\vdots\\ F_d(x_1,\dots,x_d) &= f(x_1,F_1(x_1,\dots,x_d),F_2(x_1,\dots,x_d),\dots,F_{d-1}(x_1,\dots,x_d)),\\ F_{d+1}(x_1,\dots,x_d) &= f(F_1(x_1,\dots,x_d),F_2(x_1,\dots,x_d),\dots,F_d(x_1,\dots,x_d)),\end{aligned}$$

is d-orthogonal.

PROOF. Orthogonality of the d-tuple $\langle F_1, F_2, \dots, F_d\rangle$ follows from Theorem 3.1.

Consider the system $\{F_i(x_1,\dots,x_d) = a_i\}_{i=2}^{d+1}$. From the last equation $a_{d+1} = F_{d+1}(x_1,\dots,x_d)$, we have $f(f(x_1,\dots,x_d), a_2,\dots,a_d) = a_{d+1}$ and it follows that

$$F_1(x_1,\dots,x_d) = f(x_1,\dots,x_d) = {}^{(1)}f(a_{d+1}, a_2,\dots,a_d) = a_1$$

for some $a_1 \in Q$, where $(Q, {}^{(1)}f)$ is the 1-th inverse d-ary quasigroup for (Q,f).

Now, as before, the system $\{F_i(x_1,\dots,x_d) = a_i\}_{i=1}^{d}$ has a unique solution $x_1 = b_1, x_2 = b_2, \dots, x_d = b_d$ over Q. Since

$$\begin{aligned} F_{d+1}(b_1,\dots,b_d) &= f(F_1(b_1,\dots,b_d), F_2(b_1,\dots,b_d),\dots,F_d(b_1,\dots,b_d)) \\ &= f({}^{(1)}f(a_{d+1}, a_2,\dots,a_d), a_2,\dots,a_d) = a_{d+1}, \end{aligned}$$

we have that $x_1 = b_1$, $x_2 = b_2,\dots,x_d = b_d$ is the unique solution of the system $\{F_i(x_1,\dots,x_d) = a_i\}_{i=2}^{d+1}$ as well, meaning the system is orthogonal.

Finally, for $2 \leqslant j \leqslant d$, consider the system

$$\{F_i(x_1,\dots,x_d) = a_i \mid i \in \{1,\dots,j-1, j+1,\dots,d+1\}\}.$$

We have $F_j(x_1,\dots,x_d) = f(x_1,\dots,x_{d-j+1}, a_1,\dots,a_{j-1})$. By replacing the values for F_t, $1 \leqslant t \leqslant d$, in the equation $F_{d+1}(x_1,\dots,x_d) = a_{d+1}$, we obtain

$$a_{d+1} = f(a_1,\dots,a_{j-1}, f(x_1,\dots,x_{d-j+1}, a_1,\dots,a_{j-1}), a_{j+1},\dots,a_d),$$

which implies

$$f(x_1,\dots,x_{d-j+1}, a_1,\dots,a_{j-1}) = {}^{(j)}f(a_1,\dots,a_{j-1}, a_{d+1}, a_{j+1},\dots,a_d) = a_j,$$

for some $a_j \in Q$. As before, the system $\{F_i(x_1,\dots,x_d) = a_i\}_{i=1}^{d}$ has a unique solution $x_1 = b_1, x_2 = b_2,\dots,x_d = b_d$ over Q. Now we compute

$$\begin{aligned} &F_{d+1}(b_1,\dots,b_d) = f(F_1(b_1,\dots,b_d), F_2(b_1,\dots,b_d),\dots,F_d(b_1,\dots,b_d)) \\ &\quad = f(a_1,\dots,a_{j-1}, {}^{(j)}f(a_1,\dots,a_{j-1}, a_{d+1}, a_{j+1},\dots,a_d), a_{j+1},\dots,a_d) = a_{d+1}. \end{aligned}$$

We conclude that the system

$$\{F_i(x_1,\dots,x_d) = a_i \mid i \in \{1,\dots,j-1, j+1,\dots,d+1\}\}$$

has the unique solution $x_1 = b_1, x_2 = b_2,\dots,x_d = b_d$ over Q. This completes the proof of the theorem. □

Now we can give the second main construction, which is a generalization of Proposition 3.2.

THEOREM 3.4. *Let (Q,f) be a d-ary quasigroup of order n. Let $p_1,\dots,p_d$ be a permutation of the positions $1,\dots,d$. Then the $(d+1)$-tuple $\langle F_1, F_2,\dots,F_{d+1}\rangle$, defined by*

$$\begin{aligned} F_1(x_1,\dots,x_d) &= f(x_1,\dots,x_d), \\ F_2(x_1,\dots,x_d) &= f(x_1,\dots,x_{p_1-1}, F_1(x_1,\dots,x_d), x_{p_1+1},\dots,x_d), \\ F_i(x_1,\dots,x_d) &= f(y_1,\dots,y_d),\ i = 3,\dots,d+1, \end{aligned}$$

where $y_{p_{i-1}} = F_1(x_1,\dots,x_d)$, $y_{p_{i-2}} = F_2(x_1,\dots,x_d)$,..., $y_{p_1} = F_{i-1}(x_1,\dots,x_d)$, and $y_j = x_j$ for $j \notin \{p_1,\dots,p_{i-1}\}$, is d-wise orthogonal.

PROOF. Orthogonality of the d-tuple $\langle F_1, F_2, \dots, F_d\rangle$ follows from Proposition 3.2.

Consider the system $\{F_i(x_1,\dots,x_d) = a_i\}_{i=2}^{d+1}$. From the last equation, we have $F_{d+1}(x_1,\dots,x_d) = f(y_1,\dots,y_d) = a_{d+1}$, where $y_{p_k} = a_{d+1-k}$ for $k = 1,\dots,d-1$ and $y_{p_d} = F_1(x_1,\dots,x_d) = f(x_1,\dots,x_d)$.

It follows that $a_{d+1} = f(y_1,\dots,y_{p_d-1}, f(x_1,\dots,x_d), y_{p_d+1},\dots,y_d)$, and that implies $f(x_1,\dots,x_d) =^{(p_d)} f(y_1,\dots,y_{p_d-1}, a_{d+1}, y_{p_d+1},\dots,y_d) \in Q$, since $y_t \in Q$. So, $F_1(x_1,\dots,x_d) = f(x_1,\dots,x_d) = a_1$ for some $a_1 \in Q$.

Next we replace the value a_1 of $F_1(x_1,\dots,x_d)$ in the equation for F_d, obtaining $F_d(x_1,\dots,x_d) = f(y_1,\dots,y_d) = a_d$, where $y_{p_d} = x_{p_d}, y_{p_{d-1}} = a_1$ and $y_{p_k} = a_{d-k}$ for $k = 1,\dots,d-2$. Because f is p_d-invertible operation, we obtain a unique $x_{p_d} = b_{p_d} \in Q$.

For $i = d-1,\dots,2$, we substitute the value a_1 of $F_1(x_1,\dots,x_d)$ and the already obtained unique new values $b_{p_d},\dots,b_{p_{i+1}}$ of $F_d,\dots,F_{i+1}$, respectively, and we obtain $F_i(x_1,\dots,x_d) = f(y_1,\dots,y_d) = a_i$, where $y_{p_i} = x_{p_i}$, $y_{p_{i-1}} = a_1$, $y_{p_k} = b_{p_k}$ for $k = d,\dots,i+1$, and $y_{p_k} = a_{i-k}$ for $k = 1,\dots,i-1$. Because f is p_i-invertible operation, this leads to a unique $x_{p_i} = b_{p_i}$.

Finally, in the equation $F_1(x_1,\dots,x_d) = f(x_1,\dots,x_d) = a_1$, we replace x_{p_k} with b_{p_k} for $k = 2,\dots,d$, and because f is p_1-invertible operation, we obtain a unique $x_{p_1} = b_{p_1}$. So, the system $\{F_i(x_1,\dots,x_d) = a_i\}_{i=2}^{d+1}$ is orthogonal.

To complete the proof, we have to show that the d-tuples $\langle F_i \mid i \neq j,\ i = 1, \dots, d+1\rangle$ for each j, $2 \leqslant j \leqslant d$, are orthogonal. For that aim, consider the systems of equations $\{F_i(x_1,\dots,x_d) = a_i\}_{i=1,i\neq j}^{d+1}$ for each j, $2 \leqslant j \leqslant d$. We have

$$F_{d+1}(x_1,\dots,x_d) = f(y_1,\dots,y_d) = a_{d+1},$$

where $y_{p_{d+1-k}} = a_k$ for $k \neq j$ and $k = 1,\dots,d$, and $y_{p_{d+1-j}} = F_j(x_1,\dots,x_d)$.

From the equality $f(y_1,\dots,y_{p_{d+1-j}-1}, F_j(x_1,\dots,x_d), y_{p_{d+1-j}+1},\dots,y_d) = a_{d+1}$, since $y_t \in Q$, it follows that

$$F_j(x_1,\dots,x_d) =^{(p_{d+1-j})} f(y_1,\dots,y_{p_{d+1-j}-1}, a_{d+1}, y_{p_{d+1-j}+1},\dots,y_d) \in Q,$$

hence we have $F_j(x_1,\dots,x_d) = a_j$ for some $a_j \in Q$.

There are two cases to consider.

Case $j = d$. We have $F_d(x_1,\dots,x_d) = a_d$, and the system $\{F_i(x_1,\dots,x_d) = a_i\}_{i=1}^{d}$ has a unique solution $b_1, b_2,\dots,b_d$ according to Theorem 4. We compute

$$F_{d+1}(b_1,\dots,b_d) = f(y_1,\dots,y_d),$$

where $y_{p_{d+1-k}} = F_k(b_1,\dots,b_d) = a_k$ for $k = 1,\dots,d-1$ and

$$y_{p_1} = F_d(b_1,\dots,b_d) =^{(p_1)} f(y_1,\dots,y_{p_1-1}, a_{d+1}, y_{p_1+1},\dots,y_d).$$

The last equation implies $f(y_1,\dots,y_d) = a_{d+1}$, i.e., $F_{d+1}(b_1,\dots,b_d) = a_{d+1}$, hence $b_1,\dots,b_d$ is the unique solution of the system $\{F_i(x_1,\dots,x_d) = a_i\}_{i\neq d, i=1}^{d+1}$. So, the d-tuple $\langle F_i \mid i = 1,\dots,d-1,d+1\rangle$ is orthogonal.

Case $j < d$. We replace the value a_j of $F_j(x_1,\dots,x_d)$ in the equation for F_d, obtaining $F_d(x_1,\dots,x_d) = f(y_1,\dots,y_d) = a_d$, where $y_{p_d} = x_{p_d}$, $y_{p_{d-j}} = a_j$ and

$y_{p_{d-k}} = a_k$ for $k \neq j$ and $k = 1, \dots, d-1$. Because f is p_d-invertible operation, we obtain a unique $x_{p_d} = b_{p_d}$.

In the same way, from $F_{d-1}(x_1, \dots, x_d) = f(y_1, \dots, y_d) = a_{d-1}$, where $y_{p_d} = x_{p_d} = b_{p_d}$, $y_{p_{d-1}} = x_{p_{d-1}}$, $y_{p_{d-1-j}} = a_j$ and $y_{p_{d-1-k}} = a_k$ for $k \neq j$ and $k = 1, \dots, d-2$, we can compute the value $x_{p_{d-1}} = b_{p_{d-1}}$, since f is p_{d-1}-invertible. Continuing, we can compute the values $x_{p_d} = b_{p_d}, x_{p_{d-1}} = b_{p_{d-1}}, \dots, x_{p_{j+1}} = b_{p_{j+1}}$.

For $i = j-1, \dots, 1$, we substitute obtained new values in the equation for F_i and we obtain $F_i(x_1, \dots, x_d) = f(y_1, \dots, y_d) = a_i$, where $y_{p_i} = x_{p_i}$, $y_{p_{i-k}} = b_{p_k}$ for $k = d, \dots, i+1$, and $y_{p_k} = a_k$ for $k = 1, \dots, i-1$. Because f is p_i-invertible operation, this leads to a unique $x_{p_i} = b_{p_i}$.

Finally, in the equation $F_j(x_1, \dots, x_d) = a_j$, we replace x_{p_k} with b_{p_k} for $k \neq j$ and $k = 1, \dots, d$, and because f is p_j-invertible operation, we obtain a unique $x_{p_j} = b_{p_j}$.

We compute $F_{d+1}(b_1, \dots, b_d) = f(y_1, \dots, y_d)$, where $y_{p_{d+1-k}} = F_k(b_1, \dots, b_d) = a_k$ for $k = 1, \dots, d$, $k \neq j$, and

$$y_{p_{d+1-j}} = F_j(b_1, \dots, b_d) =^{(p_{d+1-j})} f(y_1, \dots, y_{p_{d+1-j}-1}, a_{d+1}, y_{p_{d+1-j}+1}, \dots, y_d).$$

The last equation implies $f(y_1, \dots, y_d) = a_{d+1}$, i.e., $F_{d+1}(b_1, \dots, b_d) = a_{d+1}$, hence $b_1, \dots, b_d$ is the unique solution of the system $\{F_i(x_1, \dots, x_d) = a_i\}_{i \neq d, i=1}^{d+1}$. So, the d-tuple $\langle F_i \mid i = 1, \dots, j-1, j+1, \dots, d+1\rangle$ is orthogonal. □

At the end, we give one more construction.

THEOREM 3.5. *Let $\langle f_1, f_2, \dots, f_d\rangle$ be d-ary operations defined on a set Q and let f_i, $1 \leqslant i \leqslant d$, be 1-invertible d-ary operation. Then the d-tuple $\langle F_1, F_2, \dots, \dots, F_d\rangle$, defined by*

$$\begin{aligned}
F_1(x_1, \dots, x_d) &= f_1(x_1, \dots, x_d),\\
F_2(x_1, \dots, x_d) &= f_2(x_2, \dots, x_d, F_1(x_1, \dots, x_d)),\\
F_3(x_1, \dots, x_d) &= f_3(x_3, \dots, x_d, F_1(x_1, \dots, x_d), F_2(x_1, \dots, x_d)),\\
&\vdots\\
F_d(x_1, \dots, x_d) &= f_d(x_d, F_1(x_1, \dots, x_d), F_2(x_1, \dots, x_d), \dots, F_{d-1}(x_1, \dots, x_d)),
\end{aligned}$$

is orthogonal.

PROOF. Consider the system $\{F_i(x_1, \dots, x_d) = a_i\}_{i=1}^{d}$ and substitute the values of $F_1, \dots, F_{d-1}$ into the last equation:

$$F_d(x_1, \dots, x_d) = f_d(x_d, a_1, a_2, \dots, a_{d-1}) = a_d.$$

We obtain a unique $x_d = b_d$ since the f_d is 1-invertible operation, and so the F_d is d-invertible operation. Next, we substitute this value of x_d and the values of $F_1, \dots, F_{d-2}$ into the $(d-1)$-th equation:

$$F_{d-1}(x_1, \dots, x_{d-1}, b_d) = f_{d-1}(x_{d-1}, b_d, a_1, a_2, \dots, a_{d-2}) = a_{d-1},$$

and we obtain a unique $x_{d-1} = b_{d-1}$ using the 1-invertibility of f_{d-1}; again, we have that F_{d-1} is a $(d-1)$-invertible operation. Proceeding in the same way, we do similar substitution in all equations till the first one,

$$F_1(x_1, b_2, \dots, b_d) = f_1(x_1, b_2, \dots, b_d) = a_1.$$

We obtain a unique $x_1 = b_1$ from 1-invertibility of f_1.

So, the given system has a unique solution $x_1 = b_1, x_2 = b_2, \dots, x_d = b_d$ and the d-tuple $\langle F_1, \dots, F_d \rangle$ is orthogonal. □

A special case of Theorem 3.5 is when $f_1 = \cdots = f_d = f$, where (Q, f) is an arbitrary d-ary quasigroup (this special case of Theorem 3.5 is firstly proved in [**11**]). The operations $F_1, F_2, \dots, F_d$ are known as *recursive derivatives* of f [**5, 6**]. Recursive derivatives are also the functions defined by $F_{i+d}(x_1, \dots, x_d) = f(F_i(x_1, \dots, x_d), \dots, F_{i+d-1}(x_1, \dots, x_d))$, $i \geqslant 1$. A d-ary quasigroup (Q, f) is called *recursively r-differentiable* if all recursive derivatives $F_2, \dots, F_{r+1}$ are quasigroup operations.

Example 3.2. Let (Q, f) be the 4-ary quasigroup on $Q = \{0, 1, 2, 3, 4\}$ with the operation

$$f(x_1, x_2, x_3, x_4) = x_1 + x_2 + x_3 + x_4 \mod 5.$$

We compute by Theorem 3.5 the 4-ary operations

$$\begin{aligned} F_2(x_1, x_2, x_3, x_4) &= x_1 + 2x_2 + 2x_3 + 2x_4 \mod 5, \\ F_3(x_1, x_2, x_3, x_4) &= 2x_1 + 3x_2 + 4x_3 + 4x_4 \mod 5, \\ F_4(x_1, x_2, x_3, x_4) &= 4x_1 + x_2 + 2x_3 + 3x_4 \mod 5. \end{aligned}$$

All of the operations F_2, F_3, F_4 are quasigroup operations, so (Q, f) is an example of a recursively 3-differentiable quasigroup.

References

1. V. D. Belousov, M. D. Sandik, *n-ary Quasi-groups and Loops*, Sib. Math. J. **7**(1) (1966), 24–42.
2. V. D. Belousov, T. Yakubov, *On orthogonal n-ary operations*, Vopr. Kibern., Mosk. **16** (1975), 3–17. (in Russian)
3. A. S. Bektenov, T. Yakubov, *Systems of orthogonal n-ary operations*, Izv. Akad. Nauk Mold. SSR, Ser. Fiz.-Tekh. Mat. Nauk **3** (1974), 7–14. (in Russian)
4. G. B. Belyavskaya, G. L. Mullen, *Orthogonal hypercubes and n-ary operations*, Quasigroups Relat. Syst. **13** (2005), 73–86.
5. E. Couselo, S. Gonsales, V. Markov, A. Nechaev, *Recursive MDS-codes and recursively differentiable quasigroup*, Discrete Math. **10**(2) (1998), 3–29.
6. ______, *The parameters of recursive MDS-codes*, Discrete Math. **12**(4) (2000), 3–24.
7. J. Dénes, A. D. Keedwell, *Latin Squares and Their Applications*, Academic Press, New York, 1974.
8. J. T. Ethier, *Strong Forms of Orthogonality for Sets of Hypercubes*, PhD thesis, Pennsylvania State University, 2008.
9. J. T. Ethier, G. L. Mullen, *Strong forms of orthogonality for sets of hypercubes*, Discrete Math. **312**(12–13) (2012), 2050–2061.
10. A. Heppes, P. Révész, *A new generalization of the method of latin squares and orthogonal latin squares and its application to the design of experiments*, Magyar Tud. Akad. Mat. Int. Közl. **1** (1956), 379–390.
11. V. I. Izbash, P. Syrbu, *Recursively differentiable quasigroups and complete recursive codes*, Comment. Math. Univ. Carolinae **45** (2004), 257–263.

12. C. F. Laywine, G. L. Mullen, G. Whittle, *D-dimensional hypecubes and the Euler and MacNeish conjectures*, Monatsh. Math. **111** (1995), 223–238.

Faculty for Computer Science and Engineering
Ss Cyril and Methodius University
Skopje, Macedonia
smile.markovski@gmail.com

(Received 04 03 2016)

Faculty for Infromatics
Goce Delcev University
Stip, Macedonia
aleksandra.mileva@ugd.edu.mk