BULETINUL ACADEMIEI DE ŞTIINŢE
A REPUBLICII MOLDOVA. MATEMATICA
Number 3(100), 2022, Pages 41–55
ISSN 1024–7696, E-ISSN 2587–4322

Construction of medial ternary self-orthogonal quasigroups

Iryna Fryz, Fedir Sokhatsky

Abstract. Algorithms for checking if a medial ternary quasigroup has a set of six triple-wise orthogonal principal parastrophes and a set of six triple-wise strongly orthogonal principal parastrophes are found. It is proved that n-ary strongly self-orthogonal linear (including medial) quasigroups do not exist when $n > 3$.

Mathematics subject classification: 05B15, 20N05, 20N15.
Keywords and phrases: medial quasigroup, orthogonal quasigroups, self-orthogonal quasigroup, strongly self-orthogonal quasigroup, central quasigroup, determinant, polynomial.

A quasigroup algebra is a universal algebra whose operations are invertible. Quasigroup algebras satisfying orthogonality problems have wide applications in algebra, combinatorics, cryptography, geometry, coding theory, etc., but the problem of their construction is still open, especially when their arities are greater than two and also for the case when the number of operations is larger than their arities.

Recall that the Cayley table of an n-ary operation of order m is a hypercube of order m, i.e. an $\underbrace{m \times m \times \cdots \times m}_{n}$ array on m distinct symbols. An operation is invertible (in other words, a quasigroup operation) if each line of the hypercube contains all symbols. An n-element set of n-ary operations are orthogonal if superimposing the corresponding hypercubes all possible n-tuples of the symbols are obtained. Another interpretation of orthogonal quasigroups as an MDS code is given, for instance, in [1].

In [2], the authors proposed an algorithm for constructing a big number of tuples of n-ary operations which generalizes the recursive algorithm introduced by G. Belyavskaya and G. Mullen [3] and improved by S. Markovsky and A. Mileva [4]. However, operations of these sets are not necessarily invertible. There are some algorithms for constructing orthogonal Latin hypercubes, for example, T. Evans [5] proposed a method for constructing using two sets of orthogonal Latin hypercubes of less dimensions, later M. Trenkler [6] suggested a method by a pair of orthogonal Latin squares.

Each n-ary quasigroup operation has $(n+1)!$ parastrophes and $n!$ of them are principal. A quasigroup is called:

- *asymmetric* if all parastrophes are different;

DOI: https://doi.org/10.56415/basm.y2022.i3.p41

- *parastrophically orthogonal* if it has n orthogonal parastrophes;
- *self-orthogonal* if it has n orthogonal principal parastrophes;
- *totally parastrophically orthogonal* (briefly, *top*) if each set of n different parastrophes is orthogonal.

Note that throughout the article we consider maximal sets of principal parastrophes, so by *self-orthogonality* we understand self-orthogonality with the additional condition that all principal parastrophes are different and triple-wise orthogonal.

There are a number of papers concerned with the parastrophic orthogonality of quasigroups. For example, V. D. Belousov [7] described all minimal identities which define varieties of parastrophically orthogonal quasigroups; G. Belyavskaya and T. Popovich [8] described conditions when a binary central asymmetric quasigroup is a top quasigroup. Consequently, they gave a method for constructing six pairwise orthogonal binary quasigroups (Latin squares).

P. Syrbu [9, 10] was the first who described series of self-orthogonal identities. Much later, in a joint paper, P. Syrbu and D. Cheban [11, 12] found a series of identities for ternary self-orthogonal quasigroups.

The main goal of this paper is to study methods for constructing orthogonal ternary quasigroups and Latin cubes. Throughout the article, we focus on medial asymmetric self-orthogonal ternary quasigroups with the restriction that all principal parastrophes are orthogonal and we found conditions under which these parastrophes are triple-wise orthogonal. Thus, having such a self-orthogonal ternary quasigroup we have 6 triple-wise orthogonal ternary quasigroups.

Here, Section 2 contains some introductory statements about medial quasigroups. The necessary and sufficient conditions for a medial ternary quasigroup to be self-orthogonal are given in Section 3, in particular these conditions are reduced to conditions of invertibility of 3 polynomials under a set of decomposition authomorphisms of the quasigroup. In Section 4, the necessary and sufficient conditions for a medial ternary quasigroup to be strongly self-orthogonal are found, these conditions are reduced to conditions of invertibility of 5 polynomials under a set of decomposition authomorphisms of the quasigroup. Also, we give some conclusions for self-orthogonal n-ary quasigroups.

1 Preliminaries

We should mention some necessary notions reformulating them for ternary case. Throughout the article, all operations are defined on a fixed set Q called a *carrier* and $|Q| =: m < \infty$.

A ternary operation f defined on Q is called *invertible* and the pair $(Q; f)$ is called a *quasigroup* of the order m if for every a, b of Q each of the terms $f(x, a, b)$, $f(a, x, b)$, $f(a, b, x)$ defines a permutation of Q.

To each ternary quasigroup $(Q; f)$ of order m there corresponds a Latin cube of order m, i.e., a 3-dimensional array on m distinct symbols from Q, each of which

occurs exactly once in any line of the array.

Orthogonality. Orthogonality of ternary operations [3] is defined as follows:

1) a triplet of ternary operations f_1, f_2, f_3 is called *orthogonal* if for all $a_1, a_2, a_3 \in Q$, the system of equations

$$\begin{cases} f_1(x_1, x_2, x_3) = a_1, \\ f_2(x_1, x_2, x_3) = a_2, \\ f_3(x_1, x_2, x_3) = a_3 \end{cases}$$

has a unique solution;

2) a pair of ternary operations f_1, f_2 is called *orthogonal* if for all $a_1, a_2 \in Q$, the system of equations

$$\begin{cases} f_1(x_1, x_2, x_3) = a_1, \\ f_2(x_1, x_2, x_3) = a_2 \end{cases}$$

has m solutions;

3) an operation f is called *complete* if the equation

$$f_1(x_1, x_2, x_3) = a_1$$

has m^2 solutions for all $a_1 \in Q$.

Orthogonality of three (two) operations means that under superimposition of the corresponding cubes each triplet (respectively pair) of elements from Q occurs exactly once (resp. m times). Completeness of an m-ordered ternary operation means that each element of the carrier occurs exactly m^2 times in this cube. Therefore, completeness can be considered as a partial case of orthogonality.

A set of ternary operations $\Sigma = \{f_1, f_2, \ldots, f_s\}$ is called

– *orthogonal* if each triplet of distinct operations from Σ is orthogonal, where $s \geqslant 3$;

– *pairwise orthogonal* if each pair of distinct operations from Σ is orthogonal, where $s \geqslant 2$.

A set of ternary operations f_1, f_2, f_3 on a set Q is called *strongly orthogonal* if the set of operations $\{f_1, f_2, f_3, e_1, e_2, e_3\}$ is triple-wise orthogonal, where e_1, e_2, e_3 are defined by the equalities

$$e_1(x_1, x_2, x_3) = x_1, \quad e_2(x_1, x_2, x_3) = x_2, \quad e_3(x_1, x_2, x_3) = x_3.$$

The operations e_1, e_2, e_3 are called the *1st selector*, the *2nd selector* and the *3rd selector* respectively.

Recall some definitions from [2] specifying it for ternary case.

Let f be a ternary operation defined on a set Q. Binary operations $f_{(c,\{1,2\})}$, $f_{(b,\{1,3\})}$ and $f_{(a,\{2,3\})}$ which are defined by

$$f_{(c,\{1,2\})} := f(x_1, x_2, c), \quad f_{(b,\{1,3\})} := f(x_1, b, x_3), \quad f_{(a,\{2,3\})} := f(a, x_2, x_3)$$

are called $\{1,2\}$-, $\{1,3\}$-, $\{2,3\}$-retracts of f by a, b, $c \in Q$.

Let $\delta := \{i,j\} \subset \{1,2,3\}$, operations f and g be ternary operations defined on Q and $a, b \in Q$. Binary operations $f_{(a,\delta)}$ and $g_{(b,\delta)}$ are called *similar* δ-retracts of f and g if $a = b$.

Definition 1. [2] Let $\delta \subseteq \{1,2,3\}$. A set of ternary operations is called *δ-retractly orthogonal* if all tuples of similar δ-retracts of these operations are orthogonal.

If $\delta = \{i\}$, then δ-retract orthogonality of f degenerates into its i-invertibility. If $\delta = \{1,2,3\}$, then retract orthogonality of ternary operations $f_1, \ldots, f_n$ is orthogonality.

The next statement is another form of Theorem 3 [13] for ternary quasigroups.

Theorem 1. *An orthogonal set of ternary quasigroups $f_1, f_2, \ldots, f_t$ defined on a set Q, where $t \geqslant 1$, is strongly orthogonal if and only if it is $\{i,j\}$-retractly orthogonal for each $i, j \in \{1,2,3\}$, where $i \neq j$.*

Let f_1, f_2, f_3 be ternary operations defined on Q and

$$\bar{\theta}(x_1, x_2, x_3) := (f_1(x_1, x_2, x_3);\ f_2(x_1, x_2, x_3);\ f_3(x_1, x_2, x_3)).$$

Therefore, the mapping $\bar{\theta} \mapsto (f_1, f_2, f_3)$ defines a one-to-one correspondence between the set of all transformations of the set Q^3 and the set of all triplets of ternary operations defined on Q. Since a transformation $\bar{\theta}$ is a permutation of Q^3 if and only if the corresponding triplet (f_1, f_2, f_3) of operations are orthogonal, there are $(m^3)!$ ordered triplets of orthogonal ternary operations of order m.

Let f be an operation defined on Q and γ be a permutation of Q. Then the operation αf being defined by

$$(\alpha f)(x, y, z) := \alpha\,(f(x, y, z))$$

is called a *torsion* of f.

Proposition 1. *If a set of operations is orthogonal, then their torsions are also orthogonal.*

Proof. If a triplet (a, b, c) takes each value in the set Q^3 and α, β, γ are permutations of Q, then the triplet $(\alpha^{-1}(a), \beta^{-1}(b), \gamma^{-1}(c))$ also takes each value in the set Q^3. Therefore, the statement '*for all a, b, c the triplet of operations f_1, f_2, f_3 is orthogonal*' means that '*for all a, b, c of Q the system*

$$\begin{cases} f_1(x_1, x_2, x_3) = \alpha^{-1}(a), \\ f_2(x_1, x_2, x_3) = \beta^{-1}(b), \\ f_3(x_1, x_2, x_3) = \gamma^{-1}(c) \end{cases}$$

has a unique solution'. Since this system is equivalent to the system

$$\begin{cases} (\alpha f_1)(x_1, x_2, x_3) = a, \\ (\beta f_2)(x_1, x_2, x_3) = b, \\ (\gamma f_3)(x_1, x_2, x_3) = c, \end{cases}$$

the triplet αf_1, βf_2, γf_3 is orthogonal. □

Parastrophes. For every permutation $\sigma \in S_4$, a *σ-parastrophe* ${}^{\sigma}f$ of an invertible ternary operation f is defined by

$${}^{\sigma}f(x_{1\sigma}, x_{2\sigma}, x_{3\sigma}) = x_{4\sigma} :\Longleftrightarrow f(x_1, x_2, x_3) = x_4.$$

This relationship is equivalent to

$${}^{\sigma}f(x_1, x_2, x_3) = x_4 :\Longleftrightarrow f(x_{1\sigma^{-1}}, x_{2\sigma^{-1}}, x_{3\sigma^{-1}}) = x_{4\sigma^{-1}}. \tag{1}$$

It is easy to verify that the formula

$${}^{\sigma}({}^{\tau}f) = {}^{\sigma\tau}f \tag{2}$$

holds for all permutations $\sigma, \tau \in S_4$ and for each invertible operation f.

A σ-parastrophe is called:

- an *i-th division* if $\sigma = (i4)$ for $i = 1, 2, 3, 4$, where $(44) := \iota$ and ${}^{(44)}f := {}^{\iota}f = f$;
- an *identical division* if $\sigma = \iota$;
- a *principal parastrophe* if $4\sigma = 4$.

The formula (1) implies that any principal σ-parastrophe can be defined by

$${}^{\sigma}f(x_1, x_2, x_3) = f(x_{1\sigma^{-1}}, x_{2\sigma^{-1}}, x_{3\sigma^{-1}}). \tag{3}$$

Therefore, a ternary operation is invertible if and only if it has four divisions. Each ternary operation has at most $4! = 24$ parastrophes. If all parastrophes are pairwise different, the operation is called *asymmetric*. Four of the parastrophes are divisions, one of them is *identical*. Each operation has $3! = 6$ principal parastrophes.

Consider the subgroup $S_3 := \{\sigma \mid 4\sigma = 4\}$ of the symmetric group S_4 and the right cosets of S_3:

$$S_4 = S_3(14) \cup S_3(24) \cup S_3(34) \cup S_3(44).$$

If $\tau \in S_3(i4)$, i.e. $\tau = \sigma(i4)$ for some $\sigma \in S_3$, then

$$i = 4(i4) = 4\sigma(i4) = 4\tau$$

and

$$\begin{aligned}{}^{\tau}f(x_1,x_2,x_3) &= {}^{\sigma(i4)}f(x_1,x_2,x_3) \overset{(2)}{=} {}^{\sigma}\big({}^{(i4)}f\big)(x_1,x_2,x_3) = \\ &\overset{(3)}{=} {}^{(i4)}f(x_{1\sigma^{-1}},x_{2\sigma^{-1}},x_{3\sigma^{-1}})\end{aligned}$$

and so

$${}^{\tau}f(x_1,x_2,x_3) = {}^{(i4)}f(x_{1\sigma^{-1}},x_{2\sigma^{-1}},x_{3\sigma^{-1}}).$$

Hence,

$${}^{(i4)}f(x_1,x_2,x_3) = {}^{\tau}f(x_{1\sigma},x_{2\sigma},x_{3\sigma}).$$

Therefore, i-th division ${}^{(i4)}f$ exists, i.e. the operation f is i-invertible (note that each ternary operation is 4-invertible). Moreover, for every $\kappa \in S_3(i4)$ there exists κ-parastrophe.

Thus, the following theorem has been proved.

Theorem 2. *Let $\tau \in S_4$ and $\tau \in S_3(i4)$, where $i := 4\tau$ and $\sigma := \tau(i4) \in S_3$. Then τ-parastrophe of a ternary invertible operation is its principal σ-parastrophe of i-th division of the operation.*

2 Medial quasigroups

A pair $(Q;\Omega)$ is called a *ternary quasigroup algebra* if all elements from Ω are ternary invertible operations defined on Q.

A ternary quasigroup algebra $(Q;\Omega)$ is called:

- *medial* [14] if each pair f, g of operations from Ω satisfies the *identity of mediality*:

$$\begin{aligned}f(g(x_{11},x_{12},x_{13}),g(x_{21},x_{22},x_{23}),g(x_{31},x_{32},x_{33})) = \\ g(f(x_{11},x_{21},x_{31}),f(x_{12},x_{22},x_{32}),f(x_{13},x_{23},x_{33})).\end{aligned} \tag{4}$$

- *abelian* [14] if it is medial and has a one-element subalgebra, i.e. it has an element $0 \in Q$ such that $f(0,0,0) = 0$ for all operations from Ω. The abelian algebra is denoted by $(Q;\Omega,0)$.

The theorem given below follows from more general statement [14, Theorem 3].

Theorem 3. *A ternary quasigroup algebra $(Q;\Omega)$ is medial if and only if there exists an abelian group $(Q;+,0)$, a set E of pairwise commuting automorphisms of the group and a set $A \subseteq Q$ of elements such that for each operation $g \in \Omega$ there exist automorphisms ψ_1, ψ_2, ψ_3 from E and elements $a_g \in A$ such that*

$$g(y_1,y_2,y_3) = \psi_1 y_1 + \psi_2 y_2 + \psi_3 y_3 + a_g,$$

$$\mu_g(a_h) = \mu_h(a_g) \tag{5}$$

for all $h \in \Omega$, where $\mu_g := \psi_1 + \psi_2 + \psi_3 - \iota$.

Hence, a ternary quasigroup $(Q; f)$ is called medial if the identity (4) with $f = g$ holds. Since (5) with $f = g$ is evident, the following assertion holds.

Corollary 1 ([15])**.** *A quasigroup $(Q; f)$ is medial if and only if there exists an abelian group $(Q; +)$ such that*

$$f(x_1, x_2, x_3) = \varphi_1 x_1 + \varphi_2 x_2 + \varphi_3 x_3 + a, \tag{6}$$

where φ_1, φ_2, φ_3 are pairwise commuting automorphisms of $(Q; +)$ and $a \in Q$.

These automorphisms are called *coefficients*, the element a is a *free term*, and $(Q; +)$ is a *decomposition group* of f.

Corollary 2. *A ternary quasigroup algebra $(Q; \Omega, 0)$ is abelian if and only if there exists an abelian group $(Q; +, 0)$ and a set E of pairwise commuting automorphisms of $(Q; +, 0)$ such that for every operation $g \in \Omega$ there exist automorphisms ψ_1, ψ_2, ψ_3 from E such that*

$$g(y_1, y_2, y_3) = \psi_1 y_1 + \psi_2 y_2 + \psi_3 y_3.$$

Lemma 1. *Let $(Q; f)$ be a medial quasigroup with (6) and $J(x) := -x =: \varphi_4(x)$. Then for each $\tau \in S_4$*

$${}^{\tau}f(x_1, x_2, x_3) = J\varphi_{4\tau}^{-1}\varphi_{1\tau}(x_1) + J\varphi_{4\tau}^{-1}\varphi_{2\tau}(x_2) + J\varphi_{4\tau}^{-1}\varphi_{3\tau}(x_3) + b, \tag{7}$$

where $b := J\varphi_{4\tau}^{-1}(a)$.

Proof. Suppose f is a medial quasigroup and is defined by (6). By virtue of (1),

$$\varphi_1(x_{1\tau^{-1}}) + \varphi_2(x_{2\tau^{-1}}) + \varphi_3(x_{3\tau^{-1}}) + a = x_{4\tau^{-1}},$$

i.e.,

$$\varphi_1(x_{1\tau^{-1}}) + \varphi_2(x_{2\tau^{-1}}) + \varphi_3(x_{3\tau^{-1}}) + \varphi_4(x_{4\tau^{-1}}) + a = 0.$$

As the group $(Q; +)$ is commutative, the equality is equivalent to

$$\varphi_{1\tau}(x_1) + \varphi_{2\tau}(x_2) + \varphi_{3\tau}(x_3) + \varphi_{4\tau}(x_4) + a = 0.$$

Therefrom,

$$x_4 = J\varphi_{4\tau}^{-1}\varphi_{1\tau}(x_1) + J\varphi_{4\tau}^{-1}\varphi_{2\tau}(x_2) + J\varphi_{4\tau}^{-1}\varphi_{3\tau}(x_3) + J\varphi_{4\tau}^{-1}(a).$$

Thus, (7) holds. □

Corollary 3. *Any parastrophe of a medial ternary quasigroup is medial.*

Corollary 4. *Let $(Q; f, 0)$ be an abelian quasigroup with (6) and $J(x) := -x =: \varphi_4(x)$. Then for each $\tau \in S_4$,*

$${}^{\tau}f(x_1, x_2, x_3) = J\varphi_{4\tau}^{-1}\varphi_{1\tau}(x_1) + J\varphi_{4\tau}^{-1}\varphi_{2\tau}(x_2) + J\varphi_{4\tau}^{-1}\varphi_{3\tau}(x_3). \tag{8}$$

Lemma 2. *Let $(Q;f)$ be a medial ternary quasigroup $(Q;f)$ with (6) and τ_1, τ_2, $\tau_3 \in S_4$. The parastrophes ${}^{\tau_1}f$, ${}^{\tau_2}f$, ${}^{\tau_3}f$ are orthogonal if and only if the determinant*

$$\begin{vmatrix} \varphi_{1\tau_1} & \varphi_{2\tau_1} & \varphi_{3\tau_1} \\ \varphi_{1\tau_2} & \varphi_{2\tau_2} & \varphi_{3\tau_2} \\ \varphi_{1\tau_3} & \varphi_{2\tau_3} & \varphi_{3\tau_3} \end{vmatrix} \tag{9}$$

is an automorphism of the group $(Q;+)$, where $\varphi_4 := J$.

Proof. According to Proposition 1, orthogonality of the parastrophes ${}^{\tau_1}f$, ${}^{\tau_2}f$, ${}^{\tau_3}f$ is equivalent to orthogonality of their torsions

$$L_a^{-1}\varphi_{4\tau_1} J\left({}^{\tau_1}f\right), \qquad L_a^{-1}\varphi_{4\tau_2} J\left({}^{\tau_2}f\right), \qquad L_a^{-1}\varphi_{4\tau_3} J\left({}^{\tau_3}f\right).$$

By Lemma 1,

$$\begin{aligned} L_a^{-1}\varphi_{4\tau_1} J\left({}^{\tau_1}f\right)(x_1,x_2,x_3) &= \varphi_{1\tau_1}(x_1)+\varphi_{2\tau_1}(x_2)+\varphi_{3\tau_1}(x_3), \\ L_a^{-1}\varphi_{4\tau_2} J\left({}^{\tau_2}f\right)(x_1,x_2,x_3) &= \varphi_{1\tau_2}(x_1)+\varphi_{2\tau_2}(x_2)+\varphi_{3\tau_2}(x_3), \\ L_a^{-1}\varphi_{4\tau_3} J\left({}^{\tau_3}f\right)(x_1,x_2,x_3) &= \varphi_{1\tau_3}(x_1)+\varphi_{2\tau_3}(x_2)+\varphi_{3\tau_3}(x_3), \end{aligned}$$

where $L_a(x) := x+a$. Thus, the parastrophes ${}^{\tau_1}f$, ${}^{\tau_2}f$, ${}^{\tau_3}f$ are orthogonal if and only if the system of equations

$$\begin{cases} \varphi_{1\tau_1}(x_1)+\varphi_{2\tau_1}(x_2)+\varphi_{3\tau_1}(x_3)=b_1, \\ \varphi_{1\tau_2}(x_1)+\varphi_{2\tau_2}(x_2)+\varphi_{3\tau_2}(x_3)=b_2, \\ \varphi_{1\tau_3}(x_1)+\varphi_{2\tau_3}(x_2)+\varphi_{3\tau_3}(x_3)=b_3 \end{cases}$$

has a unique solution for all b_1, b_2, b_3 in Q. Since the automorphisms φ_1, φ_2, φ_3, φ_4 of the commutative group $(Q;+)$ pairwise commute, they generate a commutative ring K. Therefore, this system has a unique solution if and only if the determinant (9) is invertible, i.e. it is an automorphism of the group $(Q;+)$. □

3 Self-orthogonal medial ternary quasigroups

A self-orthogonal ternary operation f has 6 triple-wise orthogonal operations, i.e. 20 triplets of orthogonal principal parastrophes of f. Therefore according to Lemma 2, to check self-orthogonality of an invertible medial operation f, we have to examine invertibility of 20 determinants, which can be described by polynomials with some conditions.

Definition 2. A polynomial p over a commutative ring K will be called *invertible-valued* over a subset $H \subseteq K$ if $p(a,b,c)$ is invertible in K whenever a, b, c are in H.

Lemma 3. *A ternary medial quasigroup (Q, f), where f is defined by* (6)*, is self-orthogonal if and only if the polynomials*

$$\begin{gathered}\gamma_1 - \gamma_2, \qquad \gamma_1 + \gamma_2 + \gamma_3, \\ \gamma_1^2 + \gamma_2^2 + \gamma_3^2 - \gamma_1\gamma_2 - \gamma_1\gamma_3 - \gamma_2\gamma_3\end{gathered} \tag{10}$$

are invertible-valued over the set of automorphisms $\{\varphi_1, \varphi_2, \varphi_3\}$ of the group $(Q, +)$.

Proof. Suppose that $(Q; f)$ is a medial ternary quasigroup and (6) is its decomposition which exists by Corollary 1. Since the automorphisms φ_1, φ_2, φ_3 of the group $(Q; +)$ pairwise commute, they generate a subring K in the ring of all endomorphisms of the commutative group $(Q; +)$. According to Lemma 2, orthogonality of principal parastrophes ${}^{\tau_1}f$, ${}^{\tau_2}f$, ${}^{\tau_3}f$ of the operation f is equivalent to invertibility of the determinant (9) in the ring K, i.e. the determinant should be an automorphism of the group $(Q; +)$. Self-orthogonality means that all 20 determinants of the form (9) with conditions τ_1, τ_2, $\tau_3 \in S_3$ should be invertible. In other words, the polynomial

$$d := d_{\vec{\tau}}(\gamma_1, \gamma_2, \gamma_3) := \begin{vmatrix} \gamma_{1\tau_1} & \gamma_{2\tau_1} & \gamma_{3\tau_1} \\ \gamma_{1\tau_2} & \gamma_{2\tau_2} & \gamma_{3\tau_2} \\ \gamma_{1\tau_3} & \gamma_{2\tau_3} & \gamma_{3\tau_3} \end{vmatrix} \tag{11}$$

is invertible-valued over the set $\{\varphi_1, \varphi_2, \varphi_3\}$ in the ring K, where γ_1, γ_2, γ_3 are variables, $\vec{\tau} := (\tau_1, \tau_2, \tau_3)$.

Two polynomials are supposed to be equivalent if they are invertible simultaneously and we will denote this fact by $\sim$.

Now permute columns in (11) to get sequence γ_1, γ_2, γ_3 in the first row and permute the second and third rows to get the determinant

$$d \sim \begin{vmatrix} \gamma_1 & \gamma_2 & \gamma_3 \\ \gamma_{1\nu} & \gamma_{2\nu} & \gamma_{3\nu} \\ \gamma_{1\tau} & \gamma_{2\tau} & \gamma_{3\tau} \end{vmatrix}$$

with $1 \leqslant 1\nu \leqslant 1\tau$, where $\nu, \tau \in S_3$. Add the first and second columns to the third one:

$$d \sim (\gamma_1 + \gamma_2 + \gamma_3) \begin{vmatrix} \gamma_1 & \gamma_2 & \iota \\ \gamma_{1\nu} & \gamma_{2\nu} & \iota \\ \gamma_{1\tau} & \gamma_{2\tau} & \iota \end{vmatrix}$$

Therefore,

$$d \sim \begin{vmatrix} \gamma_1 & \gamma_2 & \iota \\ \gamma_{1\nu} & \gamma_{2\nu} & \iota \\ \gamma_{1\tau} & \gamma_{2\tau} & \iota \end{vmatrix} \tag{12}$$

under the condition that the polynomial $\gamma_1 + \gamma_2 + \gamma_3$ is invertible.

No column has three repetitions of a variable, otherwise d has two equal rows and consequently $d = 0$. If d has two repetitions of a variable, then rename it by γ_1. Permuting rows and columns, we obtain (12) with $1\nu = 1$. In the second row

of this determinant, $2\nu = 3$, otherwise the first and second rows coincide. Multiply the first row by $-\iota$ and add it to the second row:

$$d \sim \begin{vmatrix} \gamma_1 & \gamma_2 & \iota \\ 0 & \gamma_3 - \gamma_2 & 0 \\ \gamma_{1\tau} & \gamma_{2\tau} & \iota \end{vmatrix} = (\gamma_3 - \gamma_2)(\gamma_1 - \gamma_{1\tau}).$$

Thus, invertibility of d is equivalent to the fact that both polynomials of the form $\gamma_1 + \gamma_2 + \gamma_3$ and $\gamma_1 - \gamma_2$ are invertible-valued over the set $\{\varphi_1, \varphi_2, \varphi_3\}$.

At last, suppose the variables are different in each row and in each column. Then we obtain

$$d \sim \begin{vmatrix} \gamma_1 & \gamma_2 & \iota \\ \gamma_2 & \gamma_3 & \iota \\ \gamma_3 & \gamma_1 & \iota \end{vmatrix} = \gamma_1^2 + \gamma_2^2 + \gamma_3^2 - \gamma_1\gamma_2 - \gamma_1\gamma_3 - \gamma_2\gamma_3.$$

Consequently, the lemma has been proved. □

Theorem 4. *A ternary medial quasigroup (Q, f), where f is defined by* (6)*, is self-orthogonal if and only if the mappings*

$$\begin{gathered} \varphi_1 - \varphi_2, \qquad \varphi_1 - \varphi_3, \qquad \varphi_2 - \varphi_3, \qquad \varphi_1 + \varphi_2 + \varphi_3, \\ (\varphi_1 + \varphi_2 + \varphi_3)^2 - 3(\varphi_1\varphi_2 + \varphi_1\varphi_3 + \varphi_2\varphi_3) \end{gathered} \tag{13}$$

are automorphisms of the group $(Q, +)$.

Proof. The polynomial $\gamma_1 - \gamma_2$ is invertible-valued over the automorphisms φ_1, φ_2, φ_3 if and only if the endomorphisms

$$\varphi_1 - \varphi_2, \qquad \varphi_1 - \varphi_3, \qquad \varphi_2 - \varphi_3$$

are automorphisms. The polynomials

$$\gamma_1 + \gamma_2 + \gamma_3, \qquad \gamma_1^2 + \gamma_2^2 + \gamma_3^2 - \gamma_1\gamma_2 - \gamma_1\gamma_3 - \gamma_2\gamma_3$$

are symmetric and contain three variables, then they are invertible-valued if and only if the endomorphisms $\varphi_1 + \varphi_2 + \varphi_3$ and

$$\varphi_1^2 + \varphi_2^2 + \varphi_3^2 - (\varphi_1\varphi_2 + \varphi_1\varphi_3 + \varphi_2\varphi_3) = (\varphi_1 + \varphi_2 + \varphi_3)^2 - 3(\varphi_1\varphi_2 + \varphi_1\varphi_3 + \varphi_2\varphi_3)$$

are automorphisms of the group $(Q; +)$. □

Corollary 5. *If at least two coefficients of a central quasigroup coincide, then the quasigroup can not be self-orthogonal.*

4 Strongly self-orthogonal medial quasigroups

The concept of strong orthogonality of the given ternary quasigroups which follows from Theorem 1 with the restriction of mediality is: a triplet of ternary medial quasigroups is strongly orthogonal if for all $s \in \{1, 2, 3\}$, all minors of order s of the corresponding determinant are invertible.

Lemma 4. *A ternary medial quasigroup (Q, f), where f is defined by* (6)*, is strongly self-orthogonal if and only if the polynomials* (10) *and the polynomials*

$$\gamma_1\gamma_2 - \gamma_3^2, \qquad \gamma_1 + \gamma_2 \tag{14}$$

are invertible-valued over the set of automorphisms $\{\varphi_1, \varphi_2, \varphi_3\}$ of the group $(Q, +)$.

Proof. According to Theorem 1, the necessary and sufficient condition for a set of quasigroups to be strongly orthogonal is that each its subset is retractly orthogonal. For the ternary quasigroups it means that

1. Each operation has to be a quasigroup;
2. Each pair of quasigroups has to be $\{1, 2\}$-, $\{1, 3\}$-, $\{2, 3\}$-retractly orthogonal;
3. Each triplet of quasigroups has to be orthogonal.

Conditions for satisfying item 3 are found in Lemma 3. Consequently, it remains to consider item 2, i.e. invertibility conditions for minors of order 2 of determinant (11).

If every column contains each of the variables γ_1, γ_2, γ_3, then the determinant is a Latin square of order 3. Therefore permuting rows and columns, we obtain the determinant

$$\begin{vmatrix} \gamma_1 & \gamma_2 & \gamma_3 \\ \gamma_2 & \gamma_3 & \gamma_1 \\ \gamma_3 & \gamma_1 & \gamma_2 \end{vmatrix}$$

which is invertible simultaneously with (11). It is obvious that this determinant contains only one form of minors of order 2 up to sign J and relabeling of the variables: namely, it is $\gamma_1\gamma_2 - \gamma_3^2$.

Suppose that not every column contains each of the variables γ_1, γ_2, γ_3. Therefore, one of the variables repeats. Let us label it by means of γ_1. Then permuting rows and columns, we obtain the determinant

$$d = \begin{vmatrix} \gamma_1 & \gamma_2 & \gamma_3 \\ \gamma_1 & \gamma_i & \gamma_j \\ \gamma_{1\nu} & \gamma_{2\nu} & \gamma_{3\nu} \end{vmatrix}$$

each row of which contains different variables. If $i = 2$, then $j = 3$ and thence the first and second rows are equal and so $d = 0$. It means that $i = 3$ and $j = 2$. If $1\nu = 1$, then two rows coincide and so the determinant is 0. Therefore, $1\nu \neq 1$.

Let $1\nu = 3$. Now relabel variable γ_2 by γ_3, γ_3 by γ_2 and then permute the second and third columns. As a result, we obtain determinants with $1\nu = 2$. There are two such determinants:

$$d_1 = \begin{vmatrix} \gamma_1 & \gamma_2 & \gamma_3 \\ \gamma_1 & \gamma_3 & \gamma_2 \\ \gamma_2 & \gamma_1 & \gamma_3 \end{vmatrix}, \qquad d_2 = \begin{vmatrix} \gamma_1 & \gamma_2 & \gamma_3 \\ \gamma_1 & \gamma_3 & \gamma_2 \\ \gamma_2 & \gamma_3 & \gamma_1 \end{vmatrix}.$$

They are equivalent. Indeed, relabel variable γ_1 by γ_3, γ_3 by γ_1 in d_2 and then permute the rows and the columns:

$$d_2 \sim \begin{vmatrix} \gamma_3 & \gamma_2 & \gamma_1 \\ \gamma_3 & \gamma_1 & \gamma_2 \\ \gamma_2 & \gamma_1 & \gamma_3 \end{vmatrix} \sim \begin{vmatrix} \gamma_3 & \gamma_1 & \gamma_2 \\ \gamma_2 & \gamma_1 & \gamma_3 \\ \gamma_3 & \gamma_2 & \gamma_1 \end{vmatrix} \sim \begin{vmatrix} \gamma_1 & \gamma_2 & \gamma_3 \\ \gamma_1 & \gamma_3 & \gamma_2 \\ \gamma_2 & \gamma_1 & \gamma_3 \end{vmatrix} = d_1.$$

Thus, it is enough to consider all minors of the determinant d_1.

The minors of the first and second rows are

$$\begin{vmatrix} \gamma_1 & \gamma_2 \\ \gamma_1 & \gamma_3 \end{vmatrix} = \gamma_1(\gamma_3 - \gamma_2), \qquad \begin{vmatrix} \gamma_1 & \gamma_3 \\ \gamma_1 & \gamma_2 \end{vmatrix} = \gamma_1(\gamma_2 - \gamma_3),$$

$$\begin{vmatrix} \gamma_2 & \gamma_3 \\ \gamma_3 & \gamma_2 \end{vmatrix} = \gamma_2^2 - \gamma_3^2 = (\gamma_2 + \gamma_3)(\gamma_2 - \gamma_3).$$

The minors of the first and third rows are

$$\begin{vmatrix} \gamma_1 & \gamma_2 \\ \gamma_2 & \gamma_1 \end{vmatrix} = \gamma_1^2 - \gamma_2^2 = (\gamma_1 + \gamma_2)(\gamma_1 - \gamma_2), \qquad \begin{vmatrix} \gamma_1 & \gamma_3 \\ \gamma_2 & \gamma_3 \end{vmatrix} = \gamma_3(\gamma_1 - \gamma_2),$$

$$\begin{vmatrix} \gamma_2 & \gamma_3 \\ \gamma_1 & \gamma_3 \end{vmatrix} = \gamma_3(\gamma_2 - \gamma_1).$$

The minors of the second and third rows are

$$\begin{vmatrix} \gamma_1 & \gamma_3 \\ \gamma_2 & \gamma_1 \end{vmatrix} = \gamma_1^2 - \gamma_2\gamma_3, \qquad \begin{vmatrix} \gamma_1 & \gamma_2 \\ \gamma_2 & \gamma_3 \end{vmatrix} = \gamma_1\gamma_3 - \gamma_2^2,$$

$$\begin{vmatrix} \gamma_3 & \gamma_2 \\ \gamma_1 & \gamma_3 \end{vmatrix} = \gamma_3^2 - \gamma_1\gamma_2.$$

Consequently, strong self-orthogonality of f is equivalent to the fact that polynomials (10) and (14) are invertible-valued over $\{\varphi_1, \varphi_2, \varphi_3\}$. □

Theorem 5. *A ternary medial quasigroup (Q, f), where f is defined by* (6)*, is strongly self-orthogonal if and only if the mappings* (13) *and*

$$\begin{array}{lll} \varphi_2\varphi_3 - \varphi_1^2, & \varphi_1\varphi_3 - \varphi_2^2, & \varphi_1\varphi_2 - \varphi_3^2, \\ \varphi_1 + \varphi_2, & \varphi_1 + \varphi_3, & \varphi_2 + \varphi_3 \end{array} \tag{15}$$

are automorphisms of the group $(Q, +)$.

Proof. The first part of the theorem follows from Theorem 4.

The polynomial $\gamma_1 + \gamma_2$ is invertible-valued over the automorphisms φ_1, φ_2, φ_3 if and only if the endomorphisms

$$\varphi_1 + \varphi_2, \qquad \varphi_1 + \varphi_3, \qquad \varphi_2 + \varphi_3$$

are automorphisms. The polynomial $\gamma_1\gamma_2 - \gamma_3^2$ is invertible-valued if and only if the endomorphisms

$$\varphi_1\varphi_2 - \varphi_3^2, \qquad \varphi_1\varphi_3 - \varphi_2^2, \qquad \varphi_2\varphi_3 - \varphi_1^2$$

are automorphisms of the group $(Q;+)$. □

Conclusion

Let $\mathbb{Z}_m$ be a ring of integers modulo m. Consider a ternary operation f with decomposition

$$f(x,y,z) := x + 2y + 3z.$$

If m is relatively prime to 6, then $(\mathbb{Z}_m; f)$ is a quasigroup.

Let us now consider conditions (13) and (15) for f. Conditions (13) are

$$2-1=1, \quad 3-1=2, \quad 3-2=1, \quad 1+2+3=6,$$
$$6^2 - 3\cdot(1\cdot 2 + 1\cdot 3 + 2\cdot 3) = 36 - 33 = 3.$$

Conditions (15) are

$$1\cdot 2 - 3^2 = -7, \quad 1\cdot 3 - 2^2 = -1, \quad 2\cdot 3 - 1^2 = 5,$$
$$1+2=3, \quad 1+3=4, \quad 2+3=5.$$

According to Theorem 4 and Theorem 5, we have three conclusions:

1. $(\mathbb{Z}_m; f)$ is a self-orthogonal ternary quasigroup if m is not divisible by 6;
2. $(\mathbb{Z}_m; f)$ is a self-orthogonal ternary quasigroup, but it is not strongly self-orthogonal if m is not divisible by 6 and m is divisible by 5 or 7;
3. $(\mathbb{Z}_m; f)$ is a strongly self-orthogonal ternary quasigroup if m is not divisible by 2, 3, 5 and 7.

Corollary 6. *n-ary strongly self-orthogonal linear quasigroups do not exist if $n > 3$.*

Proof. Suppose that $(G;h)$ is an n-ary strongly self-orthogonal linear quasigroup, where $n > 3$, i.e. there exists a group $(G;+)$, its automorphisms $\varphi_1, \ldots, \varphi_n$ and an element $a \in G$ such that

$$h(x_1, x_2, \ldots, x_n) = \varphi_1 x_1 + \varphi_2 x_2 + \ldots + \varphi_n x_n + a.$$

A decomposition of its principal σ-parastrophe ${}^{\sigma}h$ with the conditions $1\sigma = 1$, $2\sigma = 2$ is

$$ {}^{\sigma}h(x_1, x_2, x_3, \ldots, x_n) = \varphi_1 x_1 + \varphi_2 x_2 + \varphi_3 x_{3\sigma^{-1}} + \ldots + \varphi_n x_{n\sigma^{-1}} + a. $$

Strong self-orthogonality of h implies that, in particular, any $\{1, 2\}$-retracts of h and ${}^{\sigma}h$ are orthogonal, i.e. for every b_1, b_2 and for all a_3, $\ldots$, a_n, the system

$$ \begin{cases} \varphi_1 x_1 + \varphi_2 x_2 + \varphi_3 a_3 + \ldots + \varphi_n a_n + a = b_1, \\ \varphi_1 x_1 + \varphi_2 x_2 + \varphi_3 a_{3\sigma^{-1}} + \ldots + \varphi_n a_{n\sigma^{-1}} + a = b_2 \end{cases} $$

has a unique solution. Therefore, the system

$$ \begin{cases} \varphi_1 x_1 + \varphi_2 x_2 = c_1, \\ \varphi_1 x_1 + \varphi_2 x_2 = c_2 \end{cases} $$

has a unique solution for all c_1 and c_2 from G, in particular, when $c_1 \neq c_2$, which is a contradiction. This contradiction shows that an n-ary ($n > 3$) linear quasigroup $(G; h)$ with the property of strong self-orthogonality does not exist. □

References

[1] Ethier J. T., Mullen G. L. *Strong forms of orthogonality for sets of hypercubes*, Discrete Math., **312** (2012), No. 12-13, 2050–2061. DOI: https://doi.org/10.1016/j.disc.2012.03.008

[2] Fryz I. V., Sokhatsky F. M. *Block composition algorithm for constructing orthogonal n-ary operations*, Discrete Math., **340** (2017), No. 8, 1957–1966. DOI: https://doi.org/10.1016/j.disc.2016.11.012

[3] Belyavskaya G. B., Mullen G. L. *Orthogonal hypercubes and n-ary operations*, Quasigroups Related System, **13** (2005), No. 1, 73–86.

[4] Markovsky S., Mileva A. *On construction of orthogonal d-ary operations*, Publications de L'institut Mathématique, Nouvelle série, **101 (115)** (2017), 109–119. DOI: https://doi.org/10.2298/PIM1715109M

[5] Evans T. *The construction of orthogonal k-skeins and latin k-cubes*, Aequationes Math., **14** (1976), No. 3, 485–491. DOI: https://doi.org/10.1007/BF01835999

[6] Trenkler M. *On orthogonal latin p-dimensional cubes*, Czech. Math. J., **55** (2005), No. 3, 725–728. DOI: https://doi.org/10.1007/s10587-005-0060-7

[7] Belousov V. D. *Parastrophic-orthogonal quasigroups*, Quasigroups Related Systems, **13** (2005), No. 1, 25–72.

[8] Belyavskaya G. B., Popovich T. V. *Totally conjugate orthogonal quasigroups and complete graphs*, J. Math. Sci., **185** (2012), No. 2, 184-191. DOI: https://doi.org/10.1007/s10958-012-0907-z

[9] Syrbu P. N. *Orthogonality and self-orthogonality n-ary operations*, Mat. Issled., **95** (1987), 121–129 (Russian).

[10] Syrbu P. N. *On self-orthogonality of n-ary operations*, Mat. Issled., **102** (1988), 92–96 (Russian).

[11] Syrbu P., Ceban D. *On paratopies of orthogonal systems of ternary quasigroups. I*, Bul. Acad. Ştiinţe Repub. Mold. Mat., **1** (80) (2016), 91–117

[12] Syrbu P., Ceban D. *On orthogonal systems of ternary quasigroups admitting nontrivial paratopies*, Quasigroups Related Systems, **25** (2017), No. 1, 133–150.

[13] Belyavskaya G., Mullen G. L. *Strongly orthogonal and uniformly orthogonal many-place operations*, Algebra Discrete Math., **5** (2006), No. 1, 1–17.

[14] Sokhatsky F. *Factorization of operations of medial and abelian algebras*, Visnyk DonNY. Ser. A: Pyrodnychi nauky, **1-2** (2017), 84–96. DOI: https://doi.org/10.31558/1817-2237.2017.1-2.7

[15] Belousov V. D. *n-ary quasigroups*. Chisinau: Stiintsa, (1972), 228 pp. (Russian)

Iryna Fryz
Vasyl' Stus Donetsk National University
E-mail: *iryna.fryz@ukr.net*

Fedir Sokhatsky
Vasyl' Stus Donetsk National University
E-mail: *fmsokha@ukr.net*

Received November 12, 2022