Invertibility criterion of composition of two multiary quasigroups

Fedir M. Sokhatsky, Iryna V. Fryz

Abstract. We study invertibility of operations that are composition of two operations of arbitrary arities. We find the criterion for quasigroups and specifications for T-quasigroups. For this purpose we introduce notions of perpendicularity of operations and hypercubes. They differ from the previously introduced notions of orthogonality of operations and hypercubes [Belyavskaya G., Mullen G.L., *Orthogonal hypercubes and n-ary operations*, Quasigroups Related Systems **13** (2005), no. 1, 73–86]. We establish some relationships between these notions and give illustrative examples.

Keywords: quasigroup, composition of operations, orthogonal operations, perpendicular operations, hypercube, perpendicular hypercubes, orthogonality of hypercubes, slice, linear quasigroup, T-quasigroup

Classification: 20N05, 05B15

Introduction

It is well known that every n-ary quasigroup operation (i.e., invertible function) is a composition of permutations and some fixed binary quasigroup operation [1]. Every operation is invertible if it is repetition-free composition of invertible operations [2]. But if, in the composition, at least one individual variable repeats, then operation is not always invertible.

For repetition composition the following results were obtained: invertibility criterion for binary operations which follows from [3], [4]; invertibility criterion for polyagroups, i.e., for multiary quasigroups which are (i, j)-associative for some pairs (i, j) [5].

In this article, we study invertibility of operations that are composition of two operations of arbitrary arities. For this purpose we generalize the notion of orthogonality of two binary operations (Definition 3) and call it *perpendicularity*. This generalization does not coincide with the previously introduced generalization of orthogonality ([6], here Definition 1). We find an invertibility criterion of composition of two operations (Theorem 5). We consider some specifications for quasigroup operations (Corollary 6) and for T-quasigroups (Theorem 9, Theorem 11).

Combinatorial analogue of perpendicularity of operations is perpendicularity of hypercubes (Definition 5). We illustrate the notion (Examples 1 and 2) and establish some relationships between the notions of orthogonality and perpendicularity of hypercubes (Proposition 12 and Example 3).

1. Preliminaries

Let x_i^j denote the sequence $x_i, \dots, x_j$ if $i \le j$ and the empty symbol if $i > j$. In this article, all operations have a common carrier set. We denote this set by Q.

Recall that an operation f, defined on a set Q, is called *i-invertible* if for arbitrary $a_0, \dots, a_{i-1}, b, a_{i-1}, \dots, a_n$ of Q there exists a unique element $x \in Q$ such that

$$f(a_0, \dots, a_{i-1}, x, a_{i+1}, \dots, a_n) = b. \tag{1}$$

If f is i-invertible for all $i \in \overline{0,n} := \{0, \dots, n\}$, then it is called *invertible* or *quasigroup*. The i-th division $f^{(i)}$ of an i-invertible operation f is defined by

$$f^{(i)}(x_0, \dots, x_{i-1}, x_i, x_{i+1}, \dots, x_n) = y :\Leftrightarrow f(x_0, \dots, x_{i-1}, y, x_{i+1}, \dots, x_n) = x_i$$

for all $x_0, \dots, x_n, y \in Q$.

Two binary operations g and h defined on Q are called orthogonal ($g \perp h$) if every system $\{g(x;y) = a,\ \ h(x;y) = b\}$ has a unique solution for all $a, b \in Q$. To every binary operation there corresponds some square (i.e., unbounded Cayley table) and to an invertible operation there corresponds a Latin square. Orthogonality of operations means orthogonality of the corresponding squares, i.e., their superimposition gives the square containing pairwise different pairs of elements.

To formulate a binary operations invertibility criterion which follows from [3], [4] we recall some notions.

Left and right multiplications are defined by equalities:

$$(g \underset{\ell}{\oplus} h)(x;y) := g(h(x;y);y), \quad (g \underset{r}{\oplus} h)(x;y) := g(x;h(x;y)).$$

Left and right divisions of operation h are defined by relationships:

$$h^{\ell}(z;y) = x \Leftrightarrow h(x;y) = z, \qquad h^{r}(x;z) = y \Leftrightarrow h(x;y) = z.$$

The following theorem is a slight generalization of the corresponding results from [3] and [4].

Theorem 1. *Let g, h be arbitrary binary operations and h be right invertible. Then*

$$g \underset{r}{\oplus} h \text{ is left invertible } \Leftrightarrow g \perp h^{r}.$$

The next statements are evident.

Proposition 2. *The following relationships are true:*

$$g \perp h \Leftrightarrow g^s \perp h^s,\tag{2}$$

[1]

$$(g \underset{\ell}{\oplus} h)^s = g^s \underset{r}{\oplus} h^s.\tag{3}$$

Similar results hold for multiary operations.

Proposition 3. *If multiary operations g and h are orthogonal, then g^σ and h^σ are orthogonal as well, where f^σ denotes some principal parastroph of f.*

Theorem 4. *Let g, h be arbitrary binary operations and the operation h be left invertible. Then*

$$g \underset{\ell}{\oplus} h \text{ is right invertible } \Leftrightarrow g \perp h^\ell.$$

Proof: $g \underset{\ell}{\oplus} h$ is right invertible $\Longleftrightarrow (g \underset{\ell}{\oplus} h)^s$ is left invertible $\overset{(3)}{\Longleftrightarrow} g^s \underset{r}{\oplus} h^s$ is left invertible $\overset{Th.\ 1}{\Longleftrightarrow} g^s \perp h^{sr} \overset{(2)}{\Longleftrightarrow} (g^s)^s \perp (h^{sr})^s \Longleftrightarrow g \perp h^\ell$. □

Recall the definition of orthogonality of multiary operations in [6].

Definition 1. Two n-ary operations ($n \geq 2$) g and h, given on a set Q of order m, are called orthogonal ($g \perp h$) if the system $\{g(x_0^n) = a,\ h(x_0^n) = b\}$ has exactly m^{n-1} solutions for any $a, b \in Q$.

2. Perpendicularity of operations

The study of functional equations, multiplace functions, multiary quasigroups needs solving some problems. One of them is: *under what conditions can a composition of operations be invertible*? In particular, *in what cases can a composition of invertible operations be invertible*?

Here we give an answer concerning composition of two operations. Theorems 1 and 4 give an answer to the question for the binary case and imply that

$$g \underset{r}{\oplus} h^s \text{ is invertible } \Leftrightarrow g \perp h^{\ell s}, \qquad g \underset{\ell}{\oplus} h^s \text{ is invertible } \Leftrightarrow g \perp h^{rs}.$$

[2]

Let an $(n+1)$-ary operation f be an arbitrary composition of operations g and h. Then there exist partial injective transformations τ and υ of $\overline{0,n} := \{0, 1, \dots, n\}$ such that

$$\begin{aligned} &f(x_0, \dots, x_n) \\ &= g(x_{\tau 0}, \dots, x_{\tau(\tau^{-1}(m)-1)}, h(x_{\upsilon 0}, \dots, x_{\upsilon n}), x_{\tau(\tau^{-1}(m)+1)}, \dots, x_{\tau n}), \end{aligned}\tag{4}$$

---

[1] $f^s(x; y) := f(y; x)$

[2] $\ell s = r\ell$, $rs = \ell r$.

where $m \in \operatorname{Im}\tau$.[3] We denote

$$J_\tau(i) := |\{\tau(0),\dots,\tau(\tau^{-1}(i)-1)\}|, \quad i=0,\dots,n.$$

Definition 2. Let τ and υ be arbitrary partial injective transformations of the set $\overline{0,n}$ and $\overline{0,n} = \operatorname{Im}\tau \cup \operatorname{Im}\upsilon$. Then a pair of binary operations will be called (τ,υ)-*respective* $\{m;p\}$-*retracts* of g and h if they are defined by terms that are obtained from

$$g(x_{\tau 0},\dots,x_{\tau n}), \qquad h(x_{\upsilon 0},\dots,x_{\upsilon n})$$

in the following way: all the variables of the terms are replaced with some elements from Q, except x_m and x_p, where $p \neq m$; in addition, if a variable appears in both terms, then it is replaced with the same element.

Definition 3. Let τ and υ be arbitrary partial injective transformations of the set $\overline{0,n}$ and $\overline{0,n} = \operatorname{Im}\tau \cup \operatorname{Im}\upsilon$ and $m \in (\operatorname{Im}\upsilon \cap \operatorname{Im}\tau)$. Operations g and h will be called *perpendicular of the type* $(\tau,\upsilon;m)$ if for all $p \in (\operatorname{Im}\upsilon \cap \operatorname{Im}\tau)\backslash\{m\}$ every pair of (τ,υ)-respective $\{m;p\}$-retracts is orthogonal.

Let (4) be valid. If $i \notin \operatorname{Im}\tau \cup \operatorname{Im}\upsilon$, then $x_{\tau i}$ and $x_{\upsilon i}$ are empty symbols, therefore, the operation f can not be i-invertible. So, for finding a criterion of i-invertibility of f it is sufficient to consider three disjoint possibilities:

$$i \in \operatorname{Im}\tau\backslash \operatorname{Im}\upsilon, \quad i \in \operatorname{Im}\upsilon\backslash \operatorname{Im}\tau, \quad i \in (\operatorname{Im}\upsilon \cap \operatorname{Im}\tau)\backslash\{m\}.$$

Theorem 5. *Let τ and υ be arbitrary partial injective transformations of $\overline{0,n}$ and let (4) hold. The following assertions are true:*

1) *if h is $J_\upsilon(m)$-invertible and $i \in \operatorname{Im}\tau\backslash \operatorname{Im}\upsilon$, then i-invertibility of f is equivalent to $J_\tau(i)$-invertibility of g;*
2) *if g is $J_\tau(m)$-invertible and $i \in \operatorname{Im}\upsilon\backslash \operatorname{Im}\tau$, then i-invertibility of f is equivalent to $J_\upsilon(i)$-invertibility of h;*
3) *if h is $J_\upsilon(m)$-invertible and $i \in (\operatorname{Im}\upsilon \cap \operatorname{Im}\tau)\backslash\{m\}$, then i-invertibility of f is equivalent to orthogonality of (τ,υ)-respective $\{m,i\}$-retracts of g and $h^{(J_\upsilon(m))}$, where $h^{(J_\upsilon(m))}$ denotes $J_\upsilon(m)$-th division of h.*

Proof: Let assumption of p. 1) be true. Because of (4), the equation (1) is equivalent to

$$\begin{aligned} g(a_{\tau 0},\dots,a_{\tau(\tau^{-1}(i)-1)},x,a_{\tau(\tau^{-1}(i)+1)},\dots,a_{\tau(\tau^{-1}(m)-1)},\\ h(a_{\upsilon 0},\dots,a_{\upsilon n}),a_{\tau(\tau^{-1}(m)+1)},\dots,a_{\tau n}) = b. \end{aligned} \tag{5}$$

This equation has a unique solution. The operation h is surjective, since h is $J_\upsilon(m)$-invertible. That is why g is $J_\tau(i)$-invertible.

Vice versa, let g be $J_\tau(i)$-invertible for some $i \in \operatorname{Im}\tau\backslash \operatorname{Im}\upsilon$. Let us prove that (1) has a unique solution for all $a_0,\dots,a_{i-1},a_{i+1},\dots,a_n,b \in Q$. Suppose that $i < m$ (the proof is the same if $i > m$). If we combine $i \in \operatorname{Im}\tau$, $i \notin \operatorname{Im}\upsilon$, (4), (1),

[3] a_u is denoted to be empty symbol if u is empty.

we get (5). It has a unique solution for all $a_0, \dots, a_{\tau(\tau^{-1}(i)-1)}, a_{(\tau^{-1}(i)+1)}, \dots, a_n$, $b \in Q$, because g is $J_\tau(i)$-invertible. This means that (1) has a unique solution for all $a_0, \dots, a_{i-1}, a_{i+1}, \dots, a_n, b \in Q$, therefore, f is i-invertible.

Let assumption of p. 2) be true. Taking into account (4), the equation (1) is equivalent to

$$g(a_{\tau 0}, \dots, a_{\tau(\tau^{-1}(m)-1)}, h(a_{\upsilon 0}, \dots, a_{\upsilon(\upsilon^{-1}(i)-1)}, x, a_{\upsilon(\upsilon^{-1}(i)+1)}, \dots, a_{\upsilon n}), a_{\tau(\tau^{-1}(m)+1)}, \dots, a_{\tau n}) = b. \tag{6}$$

We denote

$$\beta_i(x) := f(a_0, \dots, a_{i-1}, x, a_{i+1}, \dots, a_n), \quad i = 0, \dots, n,$$

$$\gamma_m(x) := g(a_{\tau 0}, \dots, a_{\tau(\tau^{-1}(m)-1)}, x, a_{\tau(\tau^{-1}(m)+1)}, \dots, a_{\tau n}), \quad m = 0, \dots, n,$$

$$\delta_i(x) := h(a_{\upsilon 0}, \dots, a_{\upsilon(\upsilon^{-1}(i)-1)}, x, a_{\upsilon(\upsilon^{-1}(i)+1)}, \dots, a_{\upsilon n}), \quad i = 0, \dots, n.$$

Then (6) can be written as $\beta_i = \gamma_m \delta_i$. The transformations β_i and δ_i are permutations simultaneously, since γ_m is a permutation. So, i-invertibility of f is equivalent to $J_\upsilon(i)$-invertibility of h.

Let assumption of p. 3) be true. Then

$$g(a_{\tau 0}, \dots, a_{\tau(\tau^{-1}(i)-1)}, x, a_{\tau(\tau^{-1}(i)+1)}, \dots, a_{\tau(\tau^{-1}(m)-1)}, h(a_{\upsilon 0}, \dots, a_{\upsilon(\upsilon^{-1}(i)-1)}, x, a_{\upsilon(\upsilon^{-1}(i)+1)}, \dots, a_{\upsilon n}), a_{\tau(\tau^{-1}(m)+1)}, \dots, a_{\tau n}) = b. \tag{7}$$

We denote

$$h(a_{\upsilon 0}, \dots, a_{\upsilon(\upsilon^{-1}(i)-1)}, x, a_{\upsilon(\upsilon^{-1}(i)+1)}, \dots, a_{\upsilon n}) =: y. \tag{8}$$

Without loss of generality, we suppose that $i < m$. The $J_\upsilon(m)$-th division $h^{(J_\upsilon(m))}$ exists, because h is $J_\upsilon(m)$-invertible, therefore, (8) is equivalent to

$$h^{(J_\upsilon(m))}(a_{\upsilon 0}, \dots, a_{\upsilon(\upsilon^{-1}(i)-1)}, x, a_{\upsilon(\upsilon^{-1}(i)+1)}, \dots, a_{\upsilon(\upsilon^{-1}(m)-1)}, y, a_{\upsilon(\upsilon^{-1}(m)+1)}, \dots, a_{\upsilon n}) = a_m.$$

Therefore, uniqueness of solution of (7) is equivalent to uniqueness of solution of the system

$$\begin{cases} h^{(J_\upsilon(m))}(a_{\upsilon 0}, \dots, a_{\upsilon(\upsilon^{-1}(i)-1)}, x, a_{\upsilon(\upsilon^{-1}(i)+1)}, \dots, \\ \qquad a_{\upsilon(\upsilon^{-1}(m)-1)}, y, a_{\upsilon(\upsilon^{-1}(m)+1)}, \dots, a_{\upsilon n}) = a_m, \\ g(a_{\tau 0}, \dots, a_{\tau(\tau^{-1}(i)-1)}, x, a_{\tau(\tau^{-1}(i)+1)}, \dots, \\ \qquad a_{\tau(\tau^{-1}(m)-1)}, y, a_{\tau(\tau^{-1}(m)+1)}, \dots, a_{\tau n}) = b \end{cases}$$

which, in turn, means orthogonality of (τ, υ)-respective $\{m, i\}$-retracts of g and $h^{(J_\upsilon(m))}$. $\square$

Corollary 6. *Let τ, υ be an arbitrary partial injective transformations of $\overline{0,n}$; g, h be invertible operations;* (4) *be fulfilled. Then the invertibility of operation f is equivalent to the perpendicularity of the type $(\tau,\upsilon;m)$ of g and $h^{(J_\upsilon(m))}$.*

PROOF: By p. 1) and p. 2) of Theorem 5, the operation f is i-invertible for all $i \in (\operatorname{Im}\tau \setminus \operatorname{Im}\upsilon) \cup (\operatorname{Im}\upsilon \setminus \operatorname{Im}\tau)$, since g and h are invertible operations. Thus, invertibility of operation f is equivalent to the perpendicularity of the type $(\tau,\upsilon;m)$ of g and $h^{(J_\upsilon(m))}$. □

The notions of orthogonality and perpendicularity of the types $(\varepsilon,\varepsilon;0)$ and $(\varepsilon,\varepsilon;1)$ coincide in binary case. So, Theorem 5 implies Theorem 1, Theorem 4, Theorem 2 [3], and Corollary 1 [4].

3. Perpendicularity of T-quasigroups

Linear transformation of a group is defined as a composition of its translations and automorphisms. A multiary quasigroup (Q,f) is called an isotope of a binary group $(Q;+)$ if $(Q;f)$ is isotopic to $(Q;d)$, where $d(x_0,\dots,x_n) := x_0+\dots+x_n$. If, in addition, all components of the isotopism are linear over $(Q;+)$, then $(Q;f)$ is called *linear on* $(Q;+)$.

Let τ be an arbitrary partial injective transformation of the set $\overline{0,n}$. If a $|\{\tau 0,\dots,\tau n\}|$-ary quasigroup f is linear on a group $(Q;+)$, then it has decomposition:

$$g(x_{\tau 0},\dots,x_{\tau n}) = \alpha_{\tau 0}x_{\tau 0}+\dots+\alpha_{\tau n}x_{\tau n}+a, \tag{9}$$

where $a \in Q$ and $\alpha_{\tau 0},\dots,\alpha_{\tau n}$ are automorphisms of $(Q;+)$ but if τi does not exist, then $\alpha_{\tau i}x_{\tau i}$ is assumed to be the empty symbol. The decomposition (9) is called *τ-canonical* and $\alpha_{\tau 0},\dots,\alpha_{\tau n}$ are called *decomposition automorphisms* [7]. A linear isotope of an abelian group is called a *T-quasigroup*.

Theorem 7. *Let $(Q;+)$ be a group and $\alpha,\beta,\gamma,\delta$ be its automorphisms. Then the system*

$$\begin{cases} \alpha x+\beta y = a, \\ \gamma x+\delta y = b \end{cases} \tag{10}$$

has a unique solution for all $a,b \in Q$ if and only if $-\gamma^{-1}\delta+\alpha^{-1}\beta$ (or $\beta^{-1}\alpha-\delta^{-1}\gamma$) is a permutation of Q.

PROOF: The system (10) is equivalent to

$$\begin{cases} x+\alpha^{-1}\beta y = \alpha^{-1}a, \\ x+\gamma^{-1}\delta y = \gamma^{-1}b. \end{cases}$$

Apply I^4 to the second equation:

$$\begin{cases} x + \alpha^{-1}\beta y = \alpha^{-1} a, \\ I\gamma^{-1}\delta y + Ix = I\gamma^{-1} b. \end{cases}$$

Add the first equation to the second one from the right side:

$$\begin{cases} x + \alpha^{-1}\beta y = \alpha^{-1} a, \\ I\gamma^{-1}\delta y + Ix + x + \alpha^{-1}\beta y = I\gamma^{-1} b + \alpha^{-1} a. \end{cases}$$

Thus, (10) is equivalent to

$$\begin{cases} x + \alpha^{-1}\beta y = \alpha^{-1} a, \\ (I\gamma^{-1}\delta + \alpha^{-1}\beta) y = I\gamma^{-1} b + \alpha^{-1} a. \end{cases}$$

It is easy to see that the system has a unique solution for all $a, b \in Q$ if and only if $-\gamma^{-1}\delta + \alpha^{-1}\beta$ is a permutation of Q.

The theorem is true for $\beta^{-1}\alpha - \delta^{-1}\gamma$, since $-\delta^{-1}\gamma(-\gamma^{-1}\delta + \alpha^{-1}\beta)\beta^{-1}\alpha = \beta^{-1}\alpha - \delta^{-1}\gamma$. $\square$

Theorem 7 immediately implies the following theorem.

Theorem 8 ([8, Theorem 16])**.** *Let $(Q;+)$ be an abelian group and $\alpha, \beta, \gamma, \delta$ be its automorphisms. Then the system (10) has a unique solution if and only if $\alpha^{-1}\beta - \gamma^{-1}\delta$ is an automorphism of $(Q;+)$.*

It is natural that the following question arises: under what conditions can a composition of linear quasigroups be a *quasigroup*?

An answer is given in the following theorem for T-quasigroups.

Theorem 9. *Let f, g, h be linear quasigroups over an abelian group $(Q;+)$ defined by (4), (9) and*

$$h(x_{\upsilon 0}, \dots, x_{\upsilon n}) := \beta_{\upsilon 0} x_{\upsilon 0} + \dots + \beta_{\upsilon n} x_{\upsilon n} + c. \tag{11}$$

The operation f is invertible if and only if for every $p \in (\operatorname{Im}\upsilon \cap \operatorname{Im}\tau)\backslash\{m\}$ the transformation $\alpha_p + \alpha_m\beta_p$ is an automorphism of $(Q;+)$.

Proof: By Corollary 6, invertibility of f is equivalent to perpendicularity of the type $(\tau, \upsilon; m)$ of g and $h^{(J_\upsilon(m))}$, since g and h are linear quasigroups. This perpendicularity is equivalent to orthogonality of their (τ, υ)-respective $\{m, p\}$-retracts for every $p \in (\operatorname{Im}\upsilon \cap \operatorname{Im}\tau)\backslash\{m\}$ and for all $a_0, \dots, a_n, b \in Q$. By Definition 3, orthogonality of (τ, υ)-respective $\{m, p\}$-retracts means uniqueness of solution of

[4] $Ix := -x$.

the corresponding system:

$$
(12) \qquad \begin{cases} g(a_{\tau 0}, \dots, a_{\tau(\tau^{-1}(p)-1)}, x, a_{\tau(\tau^{-1}(p)+1)}, \dots, \\ \qquad\qquad a_{\tau(\tau^{-1}(m)-1)}, y, a_{\tau(\tau^{-1}(m)+1)}, \dots, a_{\tau n}) = b, \\ h^{(J_\upsilon(m))}(a_{\upsilon 0}, \dots, a_{\upsilon(\upsilon^{-1}(p)-1)}, x, a_{\upsilon(\upsilon^{-1}(p)+1)}, \dots, \\ \qquad\qquad a_{\upsilon(\upsilon^{-1}(m)-1)}, y, a_{\upsilon(\upsilon^{-1}(m)+1)}, \dots, a_{\upsilon n}) = a_m. \end{cases}
$$

By (11), $J_\upsilon(m)$-th division of operation h has the following expression:

$$
\begin{aligned}
&h^{(J_\upsilon(m))}(x_{\upsilon 0}, \dots, x_{\upsilon(\upsilon^{-1}(m)-1)}, y, x_{\upsilon(\upsilon^{-1}(m)+1)}, \dots, x_{\upsilon n}) \\
&= -\beta_m^{-1}\beta_{\upsilon 0}x_{\upsilon 0} - \dots - \beta_m^{-1}\beta_{\upsilon(\upsilon^{-1}(m)-1)}x_{\upsilon(\upsilon^{-1}(m)-1)} + \beta_m^{-1}y \\
&\quad -\beta_m^{-1}\beta_{\upsilon(\upsilon^{-1}(m)+1)}x_{\upsilon(\upsilon^{-1}(m)+1)} - \dots - \beta_m^{-1}\beta_{\upsilon n}x_{\upsilon n} - \beta_m^{-1}c.
\end{aligned}
$$

So, (12) can be written as follows

$$
\begin{cases}
\underbrace{\alpha_{\tau 0}a_{\tau 0} + \dots + \alpha_{\tau(\tau^{-1}(p)-1)}a_{\tau(\tau^{-1}(p)-1)}}_{q_1} + \alpha_p x \\
\quad + \underbrace{\alpha_{\tau(\tau^{-1}(p)+1)}a_{\tau(\tau^{-1}(p)+1)} + \dots + \alpha_{\tau(\tau^{-1}(m)-1)}a_{\tau(\tau^{-1}(m)-1)}}_{q_2} \\
\qquad + \alpha_m y + \underbrace{\alpha_{\tau(\tau^{-1}(m)+1)}a_{\tau(\tau^{-1}(m)+1)} + \dots + \alpha_{\tau n}a_{\tau n} + a}_{q_3} = b, \\
\underbrace{\beta_{\upsilon 0}a_{\upsilon 0} + \dots + \beta_{\upsilon(\upsilon^{-1}(p)-1)}a_{\upsilon(\upsilon^{-1}(p)-1)}}_{d_1} + \beta_p x \\
\quad + \underbrace{\beta_{\upsilon(\upsilon^{-1}(p)+1)}a_{\upsilon(\upsilon^{-1}(p)+1)} + \dots + \beta_{\upsilon(\upsilon^{-1}(m)-1)}a_{\upsilon(\upsilon^{-1}(m)-1)}}_{d_2} \\
\qquad - y + \underbrace{\beta_{\upsilon(\upsilon^{-1}(m)+1)}a_{\upsilon(\upsilon^{-1}(m)+1)} + \dots + \beta_{\upsilon n}a_{\upsilon n} + c}_{d_3} = -\beta_m a_m,
\end{cases}
$$

i.e., we have

$$
\begin{cases} \alpha_p x + \alpha_m y = b - q_1 - q_2 - q_3, \\ \beta_p x - y = -\beta_m a_m - d_1 - d_2 - d_3. \end{cases}
$$

According to Theorem 8, existence and uniqueness of the system solution is equivalent to invertibility of the transformation $\beta_p^{-1} + \alpha_p^{-1}\alpha_m$. This transformation is invertible if and only if $\alpha_p + \alpha_m\beta_p$ is invertible, since

$$
\alpha_p + \alpha_m\beta_p = \alpha_p(\beta_p^{-1} + \alpha_p^{-1}\alpha_m)\beta_p.
$$

□

Corollary 10. *Let, in the condition of Theorem 9, $(Q;+)$ be an additive group of residues modulo s. Then the operation f is invertible if and only if the number $\alpha_p+\alpha_m\beta_p$ is relatively prime to s for all $p\in(\operatorname{Im}\upsilon\cap\operatorname{Im}\tau)\backslash\{m\}$.*

The question arises: under what conditions can the linear quasigroup be perpendicular to a component of its decomposition?

Theorem 11. *Let $(Q;+)$ be an abelian group, an operation f and linear quasigroups g and h be defined by (4), (9), and (11) respectively. The operation f is perpendicular of the type $(\tau,\upsilon;m)$ to g if and only if the following two conditions are true:*

1) *the mappings $\alpha_p+\alpha_m(\varepsilon-\beta_m)^{-1}\beta_p$ and $\alpha_p+\alpha_m\beta_p$ are automorphisms of $(Q;+)$ for all $p\in(\operatorname{Im}\upsilon\cap\operatorname{Im}\tau)\backslash\{m\}$;*
2) *the mapping $\varepsilon-\beta_m$ is an automorphism of $(Q;+)$ for all $p\in\operatorname{Im}\tau\backslash\operatorname{Im}\upsilon$.*

Proof: The operation f is linear over $(Q;+)$:

$$f(x_0,\dots,x_n)\overset{(4),(9),(11)}{=}\alpha_{\tau 0}x_{\tau 0}+\dots+\alpha_{\tau(\tau^{-1}(m)-1)}x_{\tau(\tau^{-1}(m)-1)}$$
$$+\alpha_m(\beta_{\upsilon 0}x_{\upsilon 0}+\dots+\beta_{\upsilon n}x_{\upsilon n}+c)$$
$$+\alpha_{\tau(\tau^{-1}(m)+1)}x_{\tau(\tau^{-1}(m)+1)}+\dots+\alpha_{\tau n}x_{\tau n}+a.$$

By Theorem 9, the transformation $\alpha_p+\alpha_m\beta_p$ is an automorphism of $(Q;+)$ for all $p\in(\operatorname{Im}\upsilon\cap\operatorname{Im}\tau)\backslash\{m\}$.

The perpendicularity condition of operations f and g means uniqueness of solution of the system

$$\begin{cases}\alpha_m\beta_m y+(\alpha_m\beta_p+\alpha_p)x=c_0,\\ \alpha_m y+\alpha_p x=d_0\end{cases}$$

for some elements c_0 and d_0 in Q. According to Theorem 8, the system has a unique solution if and only if the transformation $-\alpha_m^{-1}\alpha_p+(\alpha_m\beta_m)^{-1}(\alpha_m\beta_p+\alpha_p)$ is an automorphism of $(Q;+)$. The transformation $\alpha_p+\alpha_m(\varepsilon-\beta_m)^{-1}\beta_p$ is an automorphism of $(Q;+)$ for all $p\in(\operatorname{Im}\upsilon\cap\operatorname{Im}\tau)\backslash\{m\}$, since

$$-\alpha_m^{-1}\alpha_p+(\alpha_m\beta_m)^{-1}(\alpha_m\beta_p+\alpha_p)=-\alpha_m^{-1}\alpha_p+\beta_m^{-1}\alpha_m^{-1}\alpha_m\beta_p+\beta_m^{-1}\alpha_m^{-1}\alpha_p$$
$$=-\alpha_m^{-1}\alpha_p+\beta_m^{-1}\beta_p+\beta_m^{-1}\alpha_m^{-1}\alpha_p=(\beta_m^{-1}-\varepsilon)\alpha_m^{-1}\alpha_p+\beta_m^{-1}\beta_p$$
$$=\beta_m^{-1}\beta_m\big((\beta_m^{-1}-\varepsilon)\alpha_m^{-1}\alpha_p+\beta_m^{-1}\beta_p\big)=\beta_m^{-1}\big((\varepsilon-\beta_m)\alpha_m^{-1}\alpha_p+\beta_p\big)$$

and

$$(\varepsilon-\beta_m)\alpha_m^{-1}\alpha_p+\beta_p=(\varepsilon-\beta_m)\alpha_m^{-1}\big(\alpha_p+\alpha_m(\varepsilon-\beta_m)^{-1}\beta_p\big).$$

Thus, the operation f is perpendicular of the type $(\tau,\upsilon;m)$ to g if and only if the transformations $\alpha_p+\alpha_m(\varepsilon-\beta_m)^{-1}\beta_p$ and $\alpha_p+\alpha_m\beta_p$ are automorphisms of the group $(Q;+)$ simultaneously for all $p\in(\operatorname{Im}\upsilon\cap\operatorname{Im}\tau)\backslash\{m\}$.

If $p \in \operatorname{Im}\tau \setminus \operatorname{Im}\upsilon$, then perpendicularity of f and g of the type $(\tau,\upsilon;m)$ is equivalent to uniqueness of the system solution

$$\begin{cases} \alpha_m\beta_m y + \alpha_p x = c_0, \\ \alpha_m y + \alpha_p x = d_0. \end{cases}$$

The system has a unique solution if and only if the transformation $-\alpha_m^{-1}\alpha_p + (\alpha_m\beta_m)^{-1}\alpha_p$ is an automorphism of $(Q;+)$, i.e. $\varepsilon - \beta_m$ is an automorphism of $(Q;+)$. Really,

$$-\alpha_m^{-1}\alpha_p + (\alpha_m\beta_m)^{-1}\alpha_p = -\alpha_m^{-1}\alpha_p + \beta_m^{-1}\alpha_m^{-1}\alpha_p = \beta_m^{-1}(\varepsilon - \beta_m)\alpha_m^{-1}\alpha_p.$$

If $p \in \operatorname{Im}\upsilon \setminus \operatorname{Im}\tau$, then $\{m;p\}$-retract of g does not exist. $\square$

4. Perpendicularity of hypercubes

It is well known [6] that to every invertible n-ary operation there corresponds an n-dimensional Latin hypercube and to k-tuple of orthogonal n-ary quasigroup operations there corresponds a k-tuple of Latin hypercubes of dimension n.

Let ρ be an arbitrary partial injective transformation of $\overline{0,n}$. If ρi is empty symbol, then in the corresponding hypercube in the direction ρi all slices are empty.

Naturally, the following question appears: what relationship is there between the hypercubes corresponding to the perpendicular operations of the type $(\tau,\upsilon;m)$?

To give an answer, we introduce the following notions.

Definition 4. If all coordinates in a hypercube are fixed, except m and p, then the obtained square will be called *$\{m,p\}$-slice*.

The combinatorial equivalent of Definition 3 is

Definition 5. Two hypercubes H_1 and H_2 are called *perpendicular of the type* $(\tau,\upsilon;m)$ if for all $p \in \operatorname{Im}\upsilon \cap \operatorname{Im}\tau$ the pair of $\{m,p\}$-slices of H_1 and of H_2 are orthogonal.

It is easy to see that every pair of perpendicular operations corresponds to the pair of respective perpendicular hypercubes of the same type.

Example 1. The following operations f and f_1, which are defined on $Q := Z_5$ by

$$f(x_0,x_1,x_2) := x_0 + x_1 + x_2 \quad \text{and} \quad f_1(x_0,x_1,x_2) := 2x_0 + 3x_1 + x_2,$$

are perpendicular of the type $(\varepsilon,\varepsilon;0)$.

Indeed, according to Corollary 10, the numbers $1+3=4$, $1+1\cdot 1=2$ are relatively prime to 5. So, the operations are perpendicular of the type $(\varepsilon,\varepsilon;0)$.

To illustrate perpendicularity of the corresponding cubes, we present their $\{0,1\}$-slices and $\{0,2\}$-slices, since the type of the perpendicularity is equal to $(\varepsilon, \varepsilon; 0)$.

The cube H is presented by $\{0,1\}$-slices:

0	1	2	3	4
1	2	3	4	0
2	3	4	0	1
3	4	0	1	2
4	0	1	2	3

1	2	3	4	0
2	3	4	0	1
3	4	0	1	2
4	0	1	2	3
0	1	2	3	4

2	3	4	0	1
3	4	0	1	2
4	0	1	2	3
0	1	2	3	4
1	2	3	4	0

3	4	0	1	2
4	0	1	2	3
0	1	2	3	4
1	2	3	4	0
2	3	4	0	1

4	0	1	2	3
0	1	2	3	4
1	2	3	4	0
2	3	4	0	1
3	4	0	1	2

The cube H_1 is presented by $\{0,1\}$-slices:

0	3	1	4	2
2	0	3	1	4
4	2	0	3	1
1	4	2	0	3
3	1	4	2	0

1	4	2	0	3
3	1	4	2	0
0	3	1	4	2
2	0	3	1	4
4	2	0	3	1

2	0	3	1	4
4	2	0	3	1
1	4	2	0	3
3	1	4	2	0
0	3	1	4	2

3	1	4	2	0
0	3	1	4	2
2	0	3	1	4
4	2	0	3	1
1	4	2	0	3

4	2	0	3	1
1	4	2	0	3
3	1	4	2	0
0	3	1	4	2
2	0	3	1	4

Superimposition of the corresponding $\{0,1\}$-slices of the cubes H and H_1:

00	13	21	34	42
12	20	33	41	04
24	32	40	03	11
31	44	02	10	23
43	01	14	22	30

11	24	32	40	03
23	31	44	02	10
30	43	01	14	22
42	00	13	21	34
04	12	20	33	41

22	30	43	01	14
34	42	00	13	21
41	04	12	20	33
03	11	24	32	40
10	23	31	44	02

33	41	04	12	20
40	03	11	24	32
02	10	23	31	44
14	22	30	43	01
21	34	42	00	13

44	02	10	23	31
01	14	22	30	43
13	21	34	42	00
20	33	41	04	12
32	40	03	11	24

So, the corresponding $\{0,1\}$-slices of H and H_1 are orthogonal.

The cube H is presented by $\{0,2\}$-slices:

0	1	2	3	4
1	2	3	4	0
2	3	4	0	1
3	4	0	1	2
4	0	1	2	3

1	2	3	4	0
2	3	4	0	1
3	4	0	1	2
4	0	1	2	3
0	1	2	3	4

2	3	4	0	1
3	4	0	1	2
4	0	1	2	3
0	1	2	3	4
1	2	3	4	0

3	4	0	1	2
4	0	1	2	3
0	1	2	3	4
1	2	3	4	0
2	3	4	0	1

4	0	1	2	3
0	1	2	3	4
1	2	3	4	0
2	3	4	0	1
3	4	0	1	2

The cube H_1 is presented by $\{0,2\}$-slices:

0	1	2	3	4
2	3	4	0	1
4	0	1	2	3
1	2	3	4	0
3	4	0	1	2

3	4	0	1	2
0	1	2	3	4
2	3	4	0	1
4	0	1	2	3
1	2	3	4	0

1	2	3	4	0
3	4	0	1	2
0	1	2	3	4
2	3	4	0	1
4	0	1	2	3

4	0	1	2	3
1	2	3	4	0
3	4	0	1	2
0	1	2	3	4
2	3	4	0	1

2	3	4	0	1
4	0	1	2	3
1	2	3	4	0
3	4	0	1	2
0	1	2	3	4

Superimposition of the corresponding $\{0,2\}$-slices of the cubes H and H_1:

00	11	22	33	44
12	23	34	40	01
24	30	41	02	13
31	42	03	14	20
43	04	10	21	32

13	24	30	41	02
20	31	42	03	14
32	43	04	10	21
40	00	11	22	33
01	12	23	34	40

21	32	43	04	10
33	44	00	11	22
40	01	12	23	34
02	13	24	30	41
14	20	31	42	03

34	40	01	12	23
41	02	13	24	30
03	14	20	31	42
10	21	32	43	04
22	33	44	00	11

42	03	14	20	31
04	10	21	32	43
11	22	33	44	00
23	34	40	01	12
30	41	02	13	24

So, the corresponding $\{0,2\}$-slices of H and H_1 are orthogonal.
Thus, the cubes H and H_1 are perpendicular of the type $(\varepsilon;\varepsilon;0)$.

Example 2. Operations f and f_2, which are defined on $Q := Z_5$ by

$$f(x_0,x_1,x_2) := x_0 + x_1 + x_2, \qquad f_2(x_0,x_2) := 2x_0 + x_2,$$

are perpendicular of the type $(\varepsilon,\upsilon;0)$, where $\upsilon 1$ is empty, $\upsilon 0 = 0$, $\upsilon 2 = 2$.

Really, according to Corollary 10, the number $1 + 1 \cdot 1 = 2$ is relatively prime to 5. So, the operations are perpendicular of the type $(\varepsilon,\upsilon;0)$.

To illustrate perpendicularity of the respective hypercubes, we present them by their $\{0,2\}$-slices, since the type of the perpendicularity is equal to $(\varepsilon,\upsilon;0)$.

The square H_2

0	1	2	3	4
2	3	4	0	1
4	0	1	2	3
1	2	3	4	0
3	4	0	1	2

corresponds to the operation f_2 and the following cube H corresponds to the operation f and is represented by $\{0,2\}$-slices:

0	1	2	3	4
1	2	3	4	0
2	3	4	0	1
3	4	0	1	2
4	0	1	2	3

1	2	3	4	0
2	3	4	0	1
3	4	0	1	2
4	0	1	2	3
0	1	2	3	4

2	3	4	0	1
3	4	0	1	2
4	0	1	2	3
0	1	2	3	4
1	2	3	4	0

3	4	0	1	2
4	0	1	2	3
0	1	2	3	4
1	2	3	4	0
2	3	4	0	1

4	0	1	2	3
0	1	2	3	4
1	2	3	4	0
2	3	4	0	1
3	4	0	1	2

Superimposition of the square H_2 on every of the $\{0,2\}$-slices of H:

00	11	22	33	44
12	23	34	40	01
24	30	41	02	13
31	42	03	14	20
43	04	10	21	32

10	21	32	43	04
22	33	44	00	11
34	40	01	12	23
41	02	13	24	30
03	14	20	31	42

20	31	42	03	14
32	43	04	10	21
44	00	11	22	33
01	12	23	34	40
13	24	30	41	02

30	41	02	13	24
42	03	14	20	31
04	10	21	32	43
11	22	33	44	00
23	34	40	01	12

40	01	12	23	34
02	13	24	30	41
14	20	31	42	03
21	32	43	04	10
33	44	00	11	22

Thus, the corresponding $\{0,2\}$-slices of H and H_2 are orthogonal, therefore, f and f_2 are perpendicular of the type $(\varepsilon, \upsilon; 0)$.

5. A relationship between the notions of orthogonality and perpendicularity

Let us show relationship between the notions of orthogonality and perpendicularity. For this purpose, suppose that τ and υ are permutations of $\overline{0,n}$. If g is perpendicular to h of some type, then g is perpendicular to h^σ, where h^σ is a principal parastroph of h. So, it is sufficient to consider the case $\tau = \upsilon = \varepsilon$.

Let $(n+1)$-ary operations f and g be defined on a finite set Q, $k := |Q|$ and let f and g be perpendicular of the type $(\varepsilon, \varepsilon; m)$, i.e., the system

$$\begin{cases} f(a_0, \ldots, a_{m-1}, x, a_{m+1}, \ldots, a_{p-1}, y, a_{p+1}, \ldots, a_n) = a, \\ g(a_0, \ldots, a_{m-1}, x, a_{m+1}, \ldots, a_{p-1}, y, a_{p+1}, \ldots, a_n) = b \end{cases}$$

has a unique solution for every pair $(a;b)\in Q^2$ and for every sequence $(a_0,\dots,a_{m-1},a_{m+1},\dots,a_{p-1},a_{p+1},\dots,a_n)\in Q^{n-1}$. The system

$$\begin{cases} f(x_0,\dots,x_n)=a,\\ g(x_0,\dots,x_n)=b\end{cases}$$

has k^{n-1} solutions, since for every pair $(a;b)$ there exist exactly $|Q^{n-1}|=k^{n-1}$ sequences. This means that operations f and g are orthogonal according to Definition 1.

Proposition 12. *If finite operations are perpendicular of the type* $(\varepsilon,\varepsilon;m)$, *then they are orthogonal.*

A converse proposition is not true. The following example confirms this.

Example 3. The operations f and g, which are defined by

$$f(x_0,x_1,x_2)=3x_0+x_1+2x_2,\quad g(x_0,x_1,x_2)=x_0+x_1+x_2$$

on the set $Q=Z_6$, are orthogonal and are not perpendicular of the type $(\varepsilon,\varepsilon;0)$.

PROOF: The operation g is invertible but f is not invertible, since 2 (and 3) is not relatively prime to 6. Consider the corresponding hypercubes H_f and H_g.

The cube H_f is presented by $\{0,1\}$-slices:

0	1	2	3	4	5
3	4	5	0	1	2
0	1	2	3	4	5
3	4	5	0	1	2
0	1	2	3	4	5
3	4	5	0	1	2

2	3	4	5	0	1
5	0	1	2	3	4
2	3	4	5	0	1
5	0	1	2	3	4
2	3	4	5	0	1
5	0	1	2	3	4

4	5	0	1	2	3
1	2	3	4	5	0
4	5	0	1	2	3
1	2	3	4	5	0
4	5	0	1	2	3
1	2	3	4	5	0

0	1	2	3	4	5
3	4	5	0	1	2
0	1	2	3	4	5
3	4	5	0	1	2
0	1	2	3	4	5
3	4	5	0	1	2

2	3	4	5	0	1
5	0	1	2	3	4
2	3	4	5	0	1
5	0	1	2	3	4
2	3	4	5	0	1
5	0	1	2	3	4

4	5	0	1	2	3
1	2	3	4	5	0
4	5	0	1	2	3
1	2	3	4	5	0
4	5	0	1	2	3
1	2	3	4	5	0

The cube H_g is presented by $\{0,1\}$-slices:

0	1	2	3	4	5
1	2	3	4	5	0
2	3	4	5	0	1
3	4	5	0	1	2
4	5	0	1	2	3
5	0	1	2	3	4

1	2	3	4	5	0
2	3	4	5	0	1
3	4	5	0	1	2
4	5	0	1	2	3
5	0	1	2	3	4
0	1	2	3	4	5

2	3	4	5	0	1
3	4	5	0	1	2
4	5	0	1	2	3
5	0	1	2	3	4
0	1	2	3	4	5
1	2	3	4	5	0

3	4	5	0	1	2
4	5	0	1	2	3
5	0	1	2	3	4
0	1	2	3	4	5
1	2	3	4	5	0
2	3	4	5	0	1

4	5	0	1	2	3
5	0	1	2	3	4
0	1	2	3	4	5
1	2	3	4	5	0
2	3	4	5	0	1
3	4	5	0	1	2

5	0	1	2	3	4
0	1	2	3	4	5
1	2	3	4	5	0
2	3	4	5	0	1
3	4	5	0	1	2
4	5	0	1	2	3

Superimposition of the corresponding $\{0,1\}$-slices H_f and H_g:

00	11	22	33	44	55
31	42	53	04	15	20
02	13	24	35	40	51
33	44	55	00	11	22
04	15	20	31	42	53
35	40	51	02	13	24

21	32	43	54	05	10
52	03	14	25	30	41
23	34	45	50	01	12
54	05	10	21	32	43
25	30	41	52	03	14
50	01	12	23	34	45

42	53	04	15	20	31
13	24	35	40	51	02
44	55	00	11	22	33
15	20	31	42	53	04
40	51	02	13	24	35
11	22	33	44	55	00

03	14	25	30	41	52
34	45	50	01	12	23
05	10	21	32	43	54
30	41	52	03	14	25
01	12	23	34	45	50
32	43	54	05	10	21

24	35	40	51	02	13
55	00	11	22	33	44
20	31	42	53	04	15
51	02	13	24	35	40
22	33	44	55	00	11
53	04	15	20	31	42

45	50	01	12	23	34
10	21	32	43	54	05
41	52	03	14	25	30
12	23	34	45	50	01
43	54	05	10	21	32
14	25	30	41	52	03

The operations f and g are not perpendicular of the type $(\varepsilon, \varepsilon; 0)$, because the squares have repeated pairs. However, hypercubes H_f and H_g are orthogonal according to Definition 1, since every pair has six appearances. $\square$

References

[1] Gluhov M.M., *About α-closed classes and α-complete systems of functions of k-valued logics*, Discrete Math. **1** (1989), no. 1, 16–21.

[2] Sokhatsky F.M., *The deepest repetition-free decompositions of non-singular functions of finite valued logics*, Proceedings of The Twenty-Sixth International symposium on Multiple-Valued Logic (Santiago de Compostela, Spain, May 29-31, 1996), pp. 279–282.

[3] Belousov V.D., *Crossed isotopies of quasigroup*, Quasigroups and their Systems, Stiintsa, Chishinau, 1990, 14–20 (in Russian).

[4] Belyavskaya G., *Pairwise orthogonality of n-ary operations*, Bul. Acad. Stiinte Repub. Mold. Mat. **3** (2005), 5–18.

[5] Yurevych O., *About cross isotopy of poliagroup*, Pratsi Instytutu prykladnoi matematyky i mechaniky NAN Ukraina **11** (2005), 34–39 (in Ukrainian).

[6] Belyavskaya G., Mullen G.L., *Orthogonal hypercubes and n-ary operations*, Quasigroups Related Systems **13** (2005), no. 1, 73–86.

[7] Sokhatskyj F., Syvakivskyj P., *On linear isotopes of cyclic groups*, Quasigroups Related Systems **1** (1994), no. 1, 66–76.

[8] Mullen G.L., Shcherbacov V.A., *On orthogonality of binary operations and squares*, Bul. Acad. Stiinte Repub. Mold. Mat. **2** (2005), 3–42.

University "Ukraina", Vinnytsia Institute of Economics and Social Sciences, Ukraine

E-mail: fmsokha@ukr.net
friz_irina@ukr.net

(*Received* October 14, 2011, *revised* January 25, 2012)