Quasigroups and Related Systems **27** (2019), 227 − 250

On the number of autotopies of an n-ary quasigroup of order 4

Evgeny V. Gorkunov, Denis S. Krotov and Vladimir N. Potapov

Abstract. An algebraic system consisting of a finite set Σ of cardinality k and an n-ary operation f invertible in each argument is called an n-ary quasigroup of order k. An autotopy of an n-ary quasigroup (Σ, f) is a collection $(\theta_0, \theta_1, \dots, \theta_n)$ of $n+1$ permutations of Σ such that $f(\theta_1(x_1), \dots, \theta_n(x_n)) \equiv \theta_0(f(x_1, \dots, x_n))$. We show that every n-ary quasigroup of order 4 has at least $2^{[n/2]+2}$ and not more than $6 \cdot 4^n$ autotopies. We characterize the n-ary quasigroups of order 4 with $2^{(n+3)/2}$, $2 \cdot 4^n$, and $6 \cdot 4^n$ autotopies.

1. Introduction

Let Σ be the set of k elements 0, 1, ..., $k-1$. The Cartesian degree Σ^n consists of all tuples of length n formed by elements of Σ. An algebraic system with the support Σ and an n-ary operation $f\colon \Sigma^n \to \Sigma$ invertible in each argument is called an *n-ary quasigroup of order k* (sometimes, for brevity, an n-quasigroup or simply a quasigroup). The corresponding operation f is also called a quasigroup.

An *isotopy* of the set Σ^{n+1} is a tuple $\theta = (\theta_0, \theta_1, \dots, \theta_n)$ of permutations from the symmetric group S_k acting on Σ. The isotopy action on Σ^{n+1} is given by the rule

$$\theta\colon x \mapsto \theta(x) = (\theta_0(x_0), \dots, \theta_n(x_n)) \quad \text{for } x = (x_0, \dots, x_n) \in \Sigma^{n+1}.$$

To denote isotopies and permutations that constitute them, we will use the Greek alphabet, and when writing their action on elements of Σ we sometimes omit parentheses.

Two sets $M_1, M_2 \subseteq \Sigma^{n+1}$ are called *isotopic* if here exists an isotopy θ such that $\theta(M_1) = M_2$. Two quasigroups f and g are called *isotopic* if for some isotopy $\theta = (\theta_0, \theta_1, \dots, \theta_n)$ it holds

$$g(x_1, \dots, x_n) = \theta_0^{-1} f(\theta_1 x_1, \dots, \theta_n x_n). \qquad (1)$$

2010 Mathematics Subject Classification: 05B15, 20N05.
Keywords: Multiary quasigroup, latin hypercube, autotopy group
The work was supported by the RFBR grants 10-01-00616, 13-01-00463, and by the Program of Fundamental Scientific Research of the SB RAS No I.5.1., projects No 0314-2019-0016 and No 0314-2019-0017.

If $f = g$, then any isotopy θ for which (1) holds is called an *autotopy* of the quasigroup f. The *autotopy group* $\mathrm{Atp}(f)$ of a quasigroup f is the group consisting of all autotopies of f (the group operation is the composition).

A 2-quasigroup f with *neutral* element e such that $f(e,a) = f(a,e) = a$ for any $a \in \Sigma$ is called a *loop*. If a loop f satisfies the associative axiom $f(x, f(y,z)) \equiv f(f(x,y),z)$, then we have a group. It is known (see, for example, [1]), that all 2-quasigroups of order 4 are isotopic to either the group $\mathbb{Z}_2 \times \mathbb{Z}_2$ or the group $\mathbb{Z}_4$. So, quasigroups generalize groups, which illustrates their algebraic nature.

At the same time, the concept of a quasigroup admits a purely combinatorial interpretation. By *line* in Σ^{n+1}, we mean a subset of n elements that are mutually distinct exactly at one coordinate. For a quasigroup $f\colon \Sigma^n \to \Sigma$, the set $M(f) = \{(x_0, x_1, \ldots, x_n) \in \Sigma^{n+1} \mid x_0 = f(x)\}$ will be called the *code* of the quasigroup f. The term "code" is borrowed from the theory of error correcting codes, in the framework of which the set $M(f)$ is an MDS-code with distance 2 (an equivalent concept, also well known in combinatorics, is the Latin hypercube). The quasigroup code is characterized as a subset Σ^{n+1} of cardinality k^n intersecting each line in exactly one element. This view allows us to see a quasigroup from its combinatorial side. We note that the codes of isotopic quasigroups are isotopic, namely, it follows from (1) that $M(g) = \theta^{-1}(M(f))$.

In this paper, we investigate autotopies of quasigroups of order 4. We establish tight upper and lower bounds on the order of the autotopy group of such a quasigroup. In a way, it is natural that the richest group of autotopies turned out to be for the quasigroups called linear with a structure close to group. Also we characterize the quasigroups with minimum and pre-maximum (that is, next to the maximum) orders of the autotopy group.

The concept of an autotopy is a generalization of a more partial notion of "automorphism" and reflects in some sense the "regularity" or "symmetry" of a quasigroup as a combinatorial object. The study of the transformations of the space mapping the object onto itself is a classic, but at the same time a difficult task, considered in many areas of mathematics. The complexity of such problems is illustrated by Frucht's theorem [2] stating that each finite group is isomorphic to the group of automorphisms of some graph, and also a similar result concerning perfect codes in coding theory [6].

In coding theory, the group of automorphisms of a code is generated by the isometries of the metric space that sitabilize the code. There we find another example of the phenomenon that an object with group properties has the richest group of automorphisms. In papers [5, 8, 9] it is shown that the binary Hamming code, which is a linear perfect code, has the largest automorphism group among the binary 1-perfect codes, and its order at least twice exceeds the order of the automorphism group of any other binary 1-perfect code of the same length.

The paper is organized as follows. Section 2 provides basic definitions and statements. In Section 3, a representation of quasigroups necessary for further proof of the fundamental results is given. Auxiliary statements on the autotopies of quasigroups are collected in Section 4. A tight lower bound on the number of autotopies of a quasigroup of order 4 is proved in Section 5. In Section 5.2, we discuss the quasigroups with the smallest order of the autotopy group. Finally, in Section 6 an upper bound on the order of the autotopy group of a quasigroup of order 4 is derived and it is proved that this bound is attained only by the linear quasigroups. We also establish the maximum order of the autotopy group of a nonlinear quasigroup of order 4 and prove that it is attained only by isotopically transitive quasigroups, which were described in [4].

2. Notations and basic facts

For $x = (x_1, \dots, x_n) \in \Sigma^n$ and $a \in \Sigma$, we put $x_i^a = (x_1, \dots, x_{i-1}, a, x_{i+1}, \dots, x_n)$. The *inverse* of an n-quasigroup f in the i-th argument is denoted by $f^{\langle i \rangle}$; that is, for any $x \in \Sigma^n$ and $a \in \Sigma$, the equations $f^{\langle i \rangle}(x_i^a) = x_i$ and $f(x) = a$ are equivalent. Obviously, the inversion of an n-quasigroup in any argument is an n-quasigroup. By the 0-th argument of an n-quasigroup f, we mean the value of the function $f(x_1, \dots, x_n)$, which, formally not being an argument of the operation f itself, is associated with the i-th argument of the inverse $f^{\langle i \rangle}$.

In this paper, we study the autotopies of quasigroups of order 4; so, below we assume $\Sigma = \{0, 1, 2, 3\}$. A quasigroup f of order 4 is said to be *semilinear* if there are $a_j, b_j \in \Sigma$, $a_j \neq b_j$, $j = 0, 1, \dots, n$, for which

$$f(\{a_1, b_1\} \times \ldots \times \{a_n, b_n\}) = \{a_0, b_0\}. \tag{2}$$

In this case, we also say that the quasigroup f is *$\{a_j, b_j\}$-semilinear in the j-th argument*, for $j = 0, 1, \dots, n$. Note that if in the identity (2) any two of the sets $\{a_j, b_j\}$ are replaced by their complements in Σ, then the identity remains true. Thus, in every argument, a semilinear quasigroup is $\{0, 1\}$-, $\{0, 2\}$- or $\{0, 3\}$-semilinear. If f is $\{a, b\}$-semilinear in each of its arguments, then we call it simply *$\{a, b\}$-semilinear.*

A quasigroup f is *linear* if in each of its arguments it is $\{a, b\}$-semilinear for any $a, b \in \Sigma$.

Each 2-quasigroup is isotopic to one of the two quasigroups $\oplus$, $+_4$ with the value tables

$\oplus$	0	2	1	3
0	0	2	1	3
2	2	0	3	1
1	1	3	0	2
3	3	1	2	0

,

$+_4$	0	2	1	3
0	0	2	1	3
2	2	0	3	1
1	1	3	2	0
3	3	1	0	2

. (3)

The quasigroups $(\Sigma, \oplus)$ and $(\Sigma, +_4)$ are the groups $\mathbb{Z}_2 \times \mathbb{Z}_2$ and $\mathbb{Z}_4$, respectively.

Remark 2.1. In the value tables (3), the elements 0, 2, 1, 3 are not ordered lexicographically, in the usual sense. With the given ordering, it is easier to observe the semilinear structure of the given group. In the future, similarly, the table of values of a $\{0,2\}$-semilinear n-quasigroup is convenient to be thought as an n-dimensional $4\times\ldots\times 4$ array which is divided into n-dimensional $2\times\ldots\times 2$ subarrays filled with two values 0, 2 or 1, 3.

The quasigroup $\oplus$ iterated $n-1$ times will be denoted by l_n; that is,

$$l_n(x_1,\ldots,x_n) = x_1 \oplus \ldots \oplus x_n.$$

Lemma 2.2. (cf. [7])

(*i*) *All linear n-quasigroups are isotopic to l_n.*

(*ii*) *If an n-quasigroup is simultaneously $\{0,1\}$- and $\{0,2\}$-semilinear in some argument, then it is linear.*

Lemma 2.3. *If an n-quasigroup f is $\{a,b\}$-semilinear in the i-th argument for some $i\in\{0,\ldots,n\}$ and $\theta=(\theta_0,\ldots,\theta_n)$ is an isotopy, then the n-quasigroup $\theta(f)$ is $\{\theta_i^{-1}(a),\theta_i^{-1}(b)\}$-semilinear in the i-th argument.*

An n-ary quasigroup f is said to be *reducible* if for some integer m, $2\leqslant m<n$, and permutation $\sigma\in S_n$, there exists a representation f in the form of a repetition-free composition such that

$$f(x_1,\ldots,x_n) = h(g(x_{\sigma(1)},\ldots,x_{\sigma(m)}),x_{\sigma(m+1)},\ldots,x_{\sigma(n)}) \tag{4}$$

(repetition-free means that each variable occurs only once in the right side). Without loss of generality, we can assume that the quasigroup g is irreducible.

In [3], a description of quasigroups of order 4 is obtained in terms of semilinearity and reducibility.

Theorem 2.4. *Every n-ary quasigroup of order 4 is reducible or semilinear.*

3. The representation of quasigroups

According to Theorem 2.4, a non-semilinear quasigroup can be represented as a repeatition-free composition of two or more semilinear quasigroups (some of the composed quasigroups can coincide with each other or be linear). A representation of a quasigroup f in the form of a repeatition-free composition of quasigroups of arity greater than 1 will be called a *decomposition* of f. Note that a quasigroup may have several decompositions. In the simplest case, the quasigroup represents its own trivial decomposition.

In the following, we will use a graphical representation of a decomposition of a quasigroup in the form of a labeled tree. The inner vertices of this tree (the degree of which is not less than 3) will be called *nodes* and denoted by characters u, v, w, with or without indices; and the leaves (vertices of degree 1) will be denoted by symbols of variables x_1, x_2, $\ldots$, y, z, etc. The edge incident to a leaf of the tree is called a *leaf* edge. The remaining edges are called *inner*.

Firstly, we define recursively the *root tree* $T(S)$ of a decomposition S (the notion of the root decomposition tree is introduced as an auxiliary term to define the decomposition tree and will not be used after that definition).

1) A variable x_i is associated with the tree consisting of one vertex of degree 0, being the root and labelled by the variable x_i itself.

2) Let a decomposition S be of the form $S = h(S_1, \dots, S_n)$. If the decompositions and/or variables S_1, …, S_n correspond to the root trees T_1, …, T_n, respectively, then we build the tree $T(S)$ as follows. Define a new vertex u as the root of the tree and assign the label h to it. Consistently connect vertex u with the roots of the trees T_1, …, T_n. The root of the tree T_j, $j \in \{1, \dots, n\}$, is considered as the j-th neighbor of u. On the other hand, the vertex u is considered as the 0-th neighbor of the root of the tree T_j.

By a *decomposition tree* (without "root"), we call the tree obtained by connecting the leaf x_0 as the 0-th neighbor to the root of the tree $T(S)$. The tree of the decomposition S is denoted by $T_0(S)$. The leaf x_0 corresponds to the 0-th argument, i.e., to the value of the quasigroup represented by the decomposition S.

The tree $T_0(S)$ of a decomposition S for a quasigroup f can be treated as the decomposition tree for the code $M(f)$. It is important to understand that only the enumeration of the leaves and of the neighbors of every vertex defines which arguments are independent for the quasigroup f and for every element of the decomposition. Changing this enumeration, we can get the decomposition tree for the inverse of f in any argument. Namely, to get a decomposition for $f^{<i>}$, it is sufficient to take the following. Find the path P from x_0 to x_i. Then for each inner node $u \in P$, swap the labels of its two neighbors laying in this path and replace the label of u by the corresponding inverse. Finally, swap the labels x_i and x_0. The order defined on the neighbors of every node uniquely determines the order of the arguments of the quasigroups in the decomposition and of the represented quasigroup. It is worth to note that as the autotopy groups of a quasigroup and its inverses are isomorphic, from the point of view of the questions considered in the current research, it is not necessary to remember all the time which of the arguments is the 0-th one; so, the 0-th argument will not be emphasized in the most of considerations.

For a decomposition and its tree, define the operation of *merging*. Assume that a decomposition S contains the fragment

$$f_1(S_1, \dots, S_{i-1}, f_2(S_i, \dots, S_{i+n_2-1}), S_{i+n_2}, \dots, S_{n_1+n_2-1}), \tag{5}$$

where S_1, …, $S_{n_1+n_2-1}$ are some decompositions and the n_1-quasigroup f_1 and n_2-quasigroup f_2 satisfy the identity

$$g(x_1, \dots, x_{n_1+n_2-1}) \equiv f_1(x_1, \dots, x_{i-1}, f_2(x_i, \dots, x_{i+n_2-1}), x_{i+n_2}, \dots, x_{n_1+n_2-1}) \tag{6}$$

for some $(n_1 + n_2 - 1)$-quasigroup g. The result of merging f_1 and f_2 in S is defined as the decomposition $\widetilde{S}$ obtained from S by replacing the fragment (5) by

$g(S_1, \ldots, S_n)$. Note that we consider a concrete occurrence of (5) in S (in general a fragment can occur more than one time).

Respectively, in the decomposition tree $T_0(S)$, the adjacent nodes u and v labeled by f_1 and f_2 are merged as follows. This pair of nodes is replaced by a new node w labeled by g, whose neighbors are the neighbors of the removed nodes u and v (except u and v themselves). The neighbors of w are assigned the numbers $0, \ldots, n_1+n_2-1$ consequently in the following order. At first, the neighbors of u with the numbers $0, \ldots, i-1$ are assigned (in the same order); next, the neighbors of v with the numbers $1, \ldots, n_2$ are assigned; then, the remaining neighbors of u with the numbers $i+1, \ldots, n_1$ are assigned. The result of the described merging is the decomposition tree $T_0(\widetilde{S})$. Trivially, we have the following fact.

Lemma 3.1. *Being applied to a decomposition, merging does not alter the quasigroup represented by the decomposition.*

We call a decomposition (and its tree) *semilinear* if all involved quasigroups are semilinear.

In a decomposition tree, consider two neighbor nodes u, v with labels f_1, f_2, respectively. Assume that u is the 0-th neighbor of v and v is the i-th neighbor of u. We call the nodes u and v *coherent* if for some $a, b \in \Sigma$ the quasigroup f_1 is $\{a, b\}$-semilinear in the i-th argument and f_2 is $\{a, b\}$-semilinear in the 0-th argument.

Lemma 3.2. *Merging two coherent nodes in a semilinear tree results in a semilinear tree.*

Proof. Let quasigroups f_1 and f_2 of arity n_1 and n_2, respectively, correspond to coherent nodes in a decomposition tree, and (6) holds for some (n_1+n_2-1)-ary quasigroup g. To prove the lemma, it suffices to verify that the quasigroup g is semilinear, which is straightforward from (6) and the definition of a semilinear quasigroup. □

We call a semilinear decomposition (and its tree) *proper* if there are no pairs of coherent nodes in the decomposition tree.

Lemma 3.3. *Every quasigroup of order* 4 *has a proper decomposition.*

Proof. By Theorem 2.4, every n-ary quasigroup of order 4 has a semilinear decomposition. Since there are no more than $n-1$ nodes in the decomposition tree, successively merging pairs of coherent nodes, we obtain a required decomposition in at most $n-2$ steps. □

Remark 3.4. In general, a proper decomposition is not unique and depends on the order of merging. The simplest example of a decomposition that can be merged in two ways is $f(g(h(x_1, x_2), x_3), x_4)$, where f and g are $\{0, 1\}$-semilinear quasigroups, g and h are $\{0, 2\}$-semilinear quasigroups, and f and h are not linear in contrast to g. A proper decomposition of a nonlinear quasigroup does not involve any linear quasigroups because a node labeled by a linear quasigroup is coherent with each of its neighbors.

Let S be some decomposition, and let its tree $T_0(S)$ have the edge set E. An *isotopy* of the decomposition is a collection $\theta = (\theta_e)_{e\in E}$ of permutations of Σ, acting on S as follows. If a node of $T_0(S)$ has a label f_i and e_j, $j = 0, 1, \ldots, n_i$, is the j-th edge incident to this node, then f_i is replaced by f'_i, where f'_i is the quasigroup defined by

$$f'_i(x_1, \ldots, x_{n_i}) = \theta_{e_0}^{-1} f_i(\theta_{e_1} x_1, \ldots, \theta_{e_{n_i}} x_{n_i}). \tag{7}$$

As a result, we get the tree of some decomposition, denoted by $\theta(S)$ and called isotopic to S. The following is straightforward.

Lemma 3.5. *Isotopic decompositions represent isotopic quasigroups. More precisely, if θ is an isotopy connecting decompositions of quasigroups f and f', then*

$$x_0 = f'(x_1, \ldots, x_n) = \theta_{e_0}^{-1} f(\theta_{e_1}(x_1), \ldots, \theta_{e_n}(x_n)),$$

where e_j is the edge incident to the leaf x_j, $j = 0, 1, \ldots, n$.

An *autotopy* of the decomposition S is an isotopy θ such that $\theta(S) = S$. The *support* of an autotopy is the set of edges corresponding to non-identity permutations. We call a proper decomposition (and its tree) *reduced* if every involved quasigroup is $\{0, 1\}$- or $\{0, 2\}$-semilinear.

Lemma 3.6. *For every quasigroup of order 4, there is an isotopic quasigroup with a reduced decomposition.*

Proof. Consider an n-quasigroup f and construct an isotopic quasigroup with a reduced decomposition. We start with a proper decomposition S of f, which exists by Lemma 3.3. Since the decomposition tree $T_0(S)$ is a bipartite graph, its vertices are divided into two independent parts; the vertices of one part are called even, those of the other part are odd.

Let us find an isotopy θ such that the odd nodes of $\theta(S)$ are $\{0, 1\}$-semilinear, while the even nodes are $\{0, 2\}$-semilinear. To do this, we define the permutation θ_e for every edge e in the tree $T_0(S)$.

Consider two cases. Firstly, let e connect two nodes, an odd one with a label g and an even one labeled by h. Suppose that g is the i-th neighbor of h, which in turn is the 0-th neighbor of g. Note that if g is $\{0, a\}$-semilinear in the 0-th argument and h is $\{0, b\}$-semilinear in the i-th one, then $a \neq b$ because the decomposition S is proper. In this case, we put $\theta_e(0) = 0$, $\theta_e(1) = a$, $\theta_e(2) = b$, $\theta_e(3) \in \{1, 2, 3\} \setminus \{a, b\}$.

Now we turn to the other case, where e connects a node labeled by g and its i-th neighbor, a variable x. Suppose g is $\{0, a\}$-semilinear in the i-th argument. Then we set $\theta_e = (1a)$ if the node is in the odd part of $T_0(S)$, and $\theta_e = (2a)$ if the node is in the even part.

Consider the action of the constructed isotopy on the decomposition S. A node of the decomposition tree $T_0(S)$ labeled by f_i will get the label f_i' (see (7)) in the tree $T_0(\theta(S))$. Suppose f_i is $\{0,a\}$-semilinear in the j-th argument. Then, by Lemma 2.3, the quasigroup f_i' is $\{0,1\}$-semilinear in the j-th argument if f_i is an odd node, or $\{0,2\}$-semilinear in the j-th argument if f_i is an even node.

Thus, the decomposition $\theta(S)$ is proper by the definition. By Lemma 3.5, the quasigroup represented by $\theta(S)$ is isotopic to the original quasigroup f. □

4. Autotopies of quasigroups

Let $\pi = (\pi_0, \dots, \pi_m)$ and $\tau = (\tau_0, \dots, \tau_{n-m+1})$ be isotopies. If $\pi_0 = \tau_1$, then we define

$$\pi \dot{\otimes} \tau = (\tau_0, \pi_1, \dots, \pi_m, \tau_2, \dots, \tau_{n-m+1}).$$

Let us consider the n-ary quasigroup f obtained as the composition of an m-quasigroup g and an $(n-m+1)$-quasigroup h:

$$f(x_1, \dots, x_n) = h(g(x_1, \dots, x_m), x_{m+1}, \dots, x_n).$$

We define the action of the operation $\dot{\otimes}$ on the autotopy groups of g and h as follows:

$$\mathrm{Atp}(g) \dot{\otimes} \mathrm{Atp}(h) = \{\pi \dot{\otimes} \tau \mid \pi = (\pi_0, \dots, \pi_m) \in \mathrm{Atp}(g),$$
$$\tau = (\tau_0, \dots, \tau_{n-m+1}) \in \mathrm{Atp}(h), \pi_0 = \tau_1\}.$$

We restrict ourselves by considering quasigroups of order 4 only; however, the next lemma holds for any other order as well.

Lemma 4.1. *If f is an n-quasigroup represented as the composition*

$$f(x_1, \dots, x_n) = h(g(x_1, \dots, x_m), x_{m+1}, \dots, x_n),$$

then

$$\mathrm{Atp}(f) = \mathrm{Atp}(g) \dot{\otimes} \mathrm{Atp}(h).$$

Proof. Obviously, $\mathrm{Atp}(g) \dot{\otimes} \mathrm{Atp}(h) \leqslant \mathrm{Atp}(f)$. To prove the reverse, consider an autotopy $\theta = (\tau_0, \pi_1, \dots, \pi_m, \tau_2, \dots, \tau_{n-m+1}) \in \mathrm{Atp}(f)$. Let us show that there exists a permutation $\pi_0 = \tau_1 \in S_4$ such that $\pi = (\pi_0, \dots, \pi_m) \in \mathrm{Atp}(g)$, $\tau = (\tau_0, \dots, \tau_{n-m+1}) \in \mathrm{Atp}(h)$, and $\theta = \pi \dot{\otimes} \tau$.

Note that if such a permutation π_0 exists, then it is uniquely defined by the permutations $\pi_1, \dots, \pi_m$, because for every tuple in Σ^n the quasigroup g possesses only one value. Moreover, if we put $\pi_0 = \tau_1$, then $\pi \in \mathrm{Atp}(g)$ if and only if $\tau \in \mathrm{Atp}(h)$. Indeed, the relation $\pi \in \mathrm{Atp}(g)$, by the definition, means that the equations

$$x_0 = h(g(x_1, \dots, x_m), x_{m+1}, \dots, x_n) \text{ and}$$
$$x_0 = h(\pi_0 g(\pi_1^{-1} x_1, \dots, \pi_m^{-1} x_m), x_{m+1}, \dots, x_n)$$

are equivalent. Applying the autotopy $\theta \in \mathrm{Atp}(f)$, for any tuple $(x_1, \dots, x_n)$ in Σ^n we get

$$x_0 = h(g(x_1, \dots, x_m), x_{m+1}, \dots, x_n) = \\ = \tau_0^{-1} h(\pi_0 g(x_1, \dots, x_m), \tau_2 x_{m+1}, \dots, \tau_{n-m+1} x_n).$$

The last equality implies that for any $(t, x_{m+1}, \dots, x_n) \in \Sigma^{n-m+1}$ it holds

$$h(t, x_{m+1}, \dots, x_n) = \tau_0^{-1} h(\pi_0 t, \tau_2 x_{m+1}, \dots, \tau_{n-m+1} x_n).$$

That is, for $\tau_1 = \pi_0$ we have $\tau \in \mathrm{Atp}(h)$.

So, it remains to show that there exists a permutation $\pi_0 \in S_4$ such that $\pi \in \mathrm{Atp}(g)$. Taking into account that $\theta \in \mathrm{Atp}(f)$, we can write that for every $(x_1, \dots, x_m) \in \Sigma^m$ it holds

$$x_0 = h(g(x), 0, \dots, 0) = \tau_0^{-1} h(g(\pi_1 x_1, \dots, \pi_m x_m), \tau_2(0), \dots, \tau_{n-m+1}(0)). \quad (8)$$

Trivially, the 1-quasigroups

$$q_1(s) = h(s, 0, \dots, 0), \quad q_2(t) = \tau_0^{-1} h(t, \tau_2(0), \dots, \tau_{n-m+1}(0))$$

are permutations of Σ. So, (8) can be rewritten as follows:

$$g(x) = q_1^{-1}(q_2(g(\pi_1 x_1, \dots, \pi_m x_m))).$$

Defining $\pi_0(\cdot) = q_2^{-1}(q_1(\cdot))$, we have $(\pi_0, \dots, \pi_m) \in \mathrm{Atp}(g)$. □

Lemma 4.1 and the results of the previous section allows us to make the following observation. Studying the autotopy group of a quasigroup of order 4, we can assume it to be represented as a repetition-free composition of quasigroups, where each of the quasigroups is $\{0, a\}$-semilinear for some $a \in \Sigma$, but not linear.

In the remaining part of this section, we prove three lemmas on minimum autotopy groups of semilinear quasigroups. In the description of autotopies, it is convenient to use the following notation.

For a nonlinear $\{0, a\}$-semilinear quasigroup f (and the corresponding nodes of decomposition trees), $a \in \Sigma \setminus \{0\}$, the permutation $(0a)(bc)$, where $\{b, c\} = \Sigma \setminus \{0, a\}$, is called the *native involution*, and the permutations $(0b)(ca)$ and $(0c)(ab)$ are called the *foreign involutions*. Each of the transpositions $(0a)$ and (bc) forming the native involution $(0a)(bc)$ is called a *native transposition* of the semilinear quasigroup (node). The two cyclic permutations $(0bac)$ and $(0cab)$ whose square is the native involution $(0a)(bc)$ are called the *native cycles* of the semilinear quasigroup (node).

Lemma 4.2. *The following isotopies belong to the autotopy group of a $\{0, a\}$-semilinear n-ary quasigroup f, $a \in \Sigma \setminus \{0\}$.*

(i) *An isotopy consisting of two native involutions and* $n-1$ *identity permutations, in an arbitrary order.*

(ii) *An isotopy consisting of* $n+1$ *native transpositions all of which differ from* $(0a)$ *in the case* $f(\{0,a\}^n) = \{0,a\}$*, and exactly one of which equals* $(0a)$ *in the case* $f(\{0,a\}^n) = \Sigma\backslash\{0,a\}$*.*

Proof. Without loss of generality we assume $a = 1$. The identity (2) holds for any $\{a_i, b_i\}$ from $\{\{0,1\},\{2,3\}\}$, $i = 1,\dots,n$ (the pair $\{a_0, b_0\}$ is uniquely defined from the other pairs and also coincides with $\{0,1\}$ or $\{2,3\}$).

(i) Applying the native involution $(01)(23)$ in one of the arguments changes the values of the quasigroup in all points, but at the same time leaves the sets $\{a_1, b_1\}\times\ldots\times\{a_n, b_n\}$ with the above restrictions in place. It follows from (2) that the values of the quasigroup also change in accordance with the native involution. When applying the native involution in some other argument, we again obtain the original quasigroup.

(ii) Let $f(\{0,1\}^n) = \{0,1\}$. Consider an arbitrary tuple $(x_1,\dots,x_n)$ of values of the arguments and the value x_0 of the quasigroup on this tuple. Among x_0, x_1, $\dots$, x_n, an even number of values belong to $\{2,3\}$. Thus, applying successively the transposition (23) to each of the arguments, we change the value of the quasigroup an even number of times, and the changes do not take the value in a partial point beyond the pair $\{0,1\}$ or the pair $\{2,3\}$. As a result, we get that after applying all transpositions, the value of the quasigroup has not changed. The case $f(\{0,1\}^n) = \{2,3\}$ is treated similarly. □

Lemma 4.3. *Assume that an* $\{a,b\}$*-semilinear binary quasigroup* q *of order* 4 *is not linear. Let* ξ *be the corresponding native involution. The autotopy group of* q *consists of the following transformations.*

(i) *The autotopies* (Id,ξ,ξ), (ξ,Id,ξ), (ξ,ξ,Id), *and the identity autotopy.*

(ii) *The autotopies* (τ_0,τ_1,τ_1), (τ_1,τ_0,τ_1), (τ_1,τ_1,τ_0), (τ_0,τ_0,τ_0), *where* τ_0, τ_1 *are the two distinct native transpositions; the choice of* τ_0 *is unique for* q*.*

(iii) *The autotopies* $(\xi',\varphi_1,\varphi_2)$, $(\varphi_1,\xi'',\varphi_2)$, $(\varphi_1,\varphi_2,\xi''')$, *where the pair* φ_1, φ_2 *is an arbitrary pair of native cycles, for which the permutations* $\xi',\xi'',\xi''' \in \{\mathrm{Id},\xi\}$ *are uniquely defined.r*

(iv) *The autotopies* (τ',ψ_1,ψ_2), (ψ_1,τ'',ψ_2), (ψ_1,ψ_2,τ'''), *where the pair* ψ_1, ψ_2 *is an arbitrary pair of foreign involutions, for which the native transpositions* τ', τ'', τ''' *are uniquely defined.*

Proof. It can be directly checked that each of the presented isotopies is an autotopy of q. To do this, it is sufficient to consider the $\{0,2\}$-semilinear quasigroup $+_4$ (see Example 4.4 below) because all quasigroups satisfying the hypothesis of the lemma are isotopic to $+_4$. It is easy to see that the set of presented autotopies is closed under the composition; that is, this set forms a group.

The completeness is checked numerically. There are 4 autotopies of each of the types (i), (ii) and 12 autotopies of each of the types (iii), (iv); totally we have 32 autotopies. On the other hand, we can bound the number of autotopies from the upper side. It follows from the nonlinearity of $+_4$ and Lemma 2.3 that for an arbitrary autotopy (ψ_0, ψ_1, ψ_2) each of the permutations ψ_0, ψ_1, ψ_2 maps $\{0, 2\}$ to $\{0, 2\}$ or $\{1, 3\}$. There are 8 ways to choose ψ_1 meeting this condition, and 8 ways for ψ_2; by the definition of a quasigroup, ψ_0 is determined uniquely from ψ_1 and ψ_2. Moreover, it is easy to check that there is no autotopy with $\psi_1 = \mathrm{Id}$ and $\psi_2 = (01)$. It follows that the order of the autotopy group is less than 64. Hence, this group coincides with the group from the autotopies (i)–(iv). □

Example 4.4. Consider the binary quasigroup $+_4$ defined in (3). The permutation (02)(13) is the native involution for q; the permutations (02) and (13) are the native transpositions for q, and (0123), (0321) are the native cycles. The autotopy group of q is generated by the following (strictly speaking, redundant) set of autotopies:

(i) $((02)(13), (02)(13), \mathrm{Id})$, $((02)(13), \mathrm{Id}, (02)(13))$, $(\mathrm{Id}, (02)(13), (02)(13))$;
(ii) $((13), (13), (13))$;
(iii) $(\mathrm{Id}, (0123), (0321))$;
(iv) $((13), (03)(12), (01)(23))$, $((02), (01)(23), (01)(23))$, $((02), (03)(12), (03)(12))$.

Thus, we know the group of autotopies of the unique, up to isotopy, nonlinear binary quasigroup. In addition, we need examples of semilinear 3- and 4-ary quasigroups with the minimal group of autotopies. We define the n-ary quasigroup $l_n^\bullet$ by the identity

$$l_n^\bullet(x) = \begin{cases} l_n(x) \oplus 2, & \text{if } x \in \{0, 2\}^n, \\ l_n(x), & \text{if } x \notin \{0, 2\}^n. \end{cases}$$

Lemma 4.5. *If $n \geqslant 3$ then the autotopy group of $l_n^\bullet$ is generated by the autotopies enumerated in Lemma 4.2 and has the order 2^{n+1}.*

We prove Lemma 4.5 for any n. However, we note that only the cases $n = 3$ and $n = 4$ are used in the further discussion. For these cases, the statement of Lemma 4.5 can be checked directly.

Proof. Obviously, the autotopies in Lemma 4.2 have order 2, commute and are linearly independent; whence the order of the group generated by them follows.

The code $M(l_n)$ of the quasigroup l_n is a $2n$-dimensional affine subspace of the vector space over the field GF(2) of two elements with the addition $\oplus$ and trivial multiplication by 0 and 1.

The code $M(l_n^\bullet)$ of $l_n^\bullet$ differs from the affine subspace $M(l_n)$ in the 2^n vertices of the set B_n, where $B_n = M(l_n^\bullet) \backslash M(l_n) = \{(l_n^\bullet(x), x) \mid x \in \{0, 2\}^n\}$. Moreover,

$M(l_n)$ is a unique closest (in the sense above) to $M(l_n^\bullet)$ affine subspace, because any other affine subspace of the same dimension differs from $M(l_n)$ in at least $2^{2n-1} \geqslant 4 \cdot 2^n$ vertices. Under the action of an autotopy of $l_n^\bullet$, the code $M(l_n^\bullet)$ is mapped to itself (by the definition), while $M(l_n)$ is mapped to an affine subspace (indeed, it is easy to see that any permutation of Σ is an affine transformation over GF(2)), which is also closest to $M(l_n^\bullet)$. It follows that an autotopy of $l_n^\bullet$ is necessarily an autotopy of l_n. Moreover, it also follows that under the action of such an autotopy the set B_n (the difference between the codes of $l_n^\bullet$ and l_n) is mapped to itself. In particular, every permutation of that autotopy stabilizes the set $\{0, 2\}$, i.e. is one of Id, (02), (13), (02)(23). As it follows from the description of the autotopy group of l_n in Section 6, all such autotopies are combinations of the autotopies listed in Lemma 4.2. □

5. A lower bound and quasigroups attaining it

5.1. The estimation

In this section, we consider an arbitrary quasigroup of order 4 and prove a sharp lower bound for the order of its autotopy group. In particular, the autotopy group of a semilinear quasigroup is rather large. For a reducible quasigroup f, we show that the nodes of its decomposition tree $T_0(f)$ can be grouped into subsets, which we call bunches. Each bunch in $T_0(f)$ consists of nodes of the same parity, i.e. it does not contain any adjacent nodes of the tree $T_0(f)$. A current subgroup of the autotopy group $\mathrm{Atp}(f)$ corresponds to each bunch, and the subgroups corresponding to different bunches are independent.

We now introduce additional notation and definitions concerning the representation of quasigroups in a form of a decomposition tree. Let f be an n-ary quasigroup of order 4 with a reduced decomposition S and the decomposition tree $T = T_0(S)$.

• Let $N = n + 1$ denote the number of leaves in the tree T, and let V be the number of nodes in T.

• A *bald* node is an inner vertex u of the tree T without leaves among the neighbors of u. Let E equal the number of bald nodes in T.

• A *bridge* node, or simply *bridge*, is a vertex u of degree 3 in the tree T that is adjacent to exactly one leaf. The leaf adjacent to the bridge u is called a *bridge* leaf. Let B equal the number of bridges in T.

• A *fork* is a vertex u of degree 3 in the tree T that is adjacent to exactly two leaves. Let F equal the number of forks in T.

• By $G(T)$, we denote the graph with the set of nodes of the tree T taken as the vertex set. Two vertices are adjacent in the graph $G(T)$ if the corresponding nodes are adjacent to the same bridge in T. It is easy to see that $G(T)$ is a forest.

• A *bunch* is a connected component of $G(T)$. Let Γ equal the number of bunches in T.

• For a bunch G in $G(T)$, a leaf x of the tree T belongs to the *leaf set* of G if x is adjacent to some node of T included in G. A bunch of the graph $G(T)$ is called *bald* if its leaf set is empty. Let L equal the number of bald bunches in T.

It is worth to note that a bridge providing a corresponding edge in a bunch G does not belong to G as its vertex. The bridge being a node is contained in another bunch which differs from G. In addition, all bridges providing the edges of the bunch G belong to one of two parts of the bipartite graph T while the nodes of G pertain to the other part of T.

For example, consider the decomposition tree designed in Figure 1. There are one bald node ι, five bridges γ, δ, ζ, η, θ, and one fork β. The nodes form seven bunches, namely $\{\alpha,\beta,\varepsilon,\eta,\iota\}$, $\{\gamma\}$, $\{\delta\}$, $\{\zeta,\theta\}$, $\{\kappa\}$, $\{\lambda\}$, $\{\mu\}$.

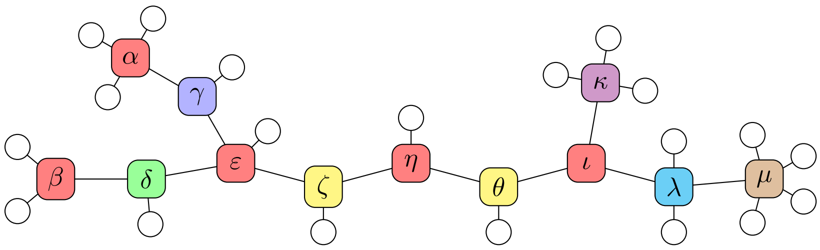


Figure 1: A decomposition tree

Since the number V of nodes in a tree T equals the number of vertices in the forest $G(T)$, the number B of bridges in T equals the number of edges in $G(T)$, and the number Γ of bunches in T equals the number of connected components of $G(T)$, it follows that

$$\Gamma = V - B. \tag{9}$$

It is evident that the number $\Gamma - L$ of non-bald bunches is less than or equal to the number $V - E$ of non-bald nodes. Therefore, the relations $\Gamma - L = V - B - L \leqslant V - E$ hold and from that we get a bound for the number of bald bunches

$$L \geqslant E - B. \tag{10}$$

For two different leaves x and y in the leaf set of a bunch G in the graph $G(T)$, we define an isotopy $\psi^{x,y}$ of the decomposition S in the following way. For any edge of the chain P connecting leaves x and y in the tree T we take the involution $\xi = \xi(G)$ native to the nodes of the bunch G. Each bridge node in the chain P does not belong to G, but is adjacent to two nodes of the bunch G and one leaf z of the tree T. If a bridge v is labeled by f, then for the leaf edge of v we take a native transposition $\tau = \tau(z)$ of the bridge v such that the three permutations ξ, ξ, τ in an appropriate order form an autotopy of the binary quasigroup f. Such a transposition exists by Lemma 4.3(iv). Finally, we take the identity permutation for the remaining edges of the tree T.

Lemma 5.1. *For any two leaves x and y from the leaf set of a bunch in $G(T)$, the isotopy $\psi^{x,y}$ is an autotopy of the decomposition S.*

Proof. Consider a bunch G and any two leaves x and y from the leaf set of G. The nodes of the chain P connecting x and y in the tree T can be partitioned into two parts. The first part consists of the nodes of the bunch G. If $u \in P$ is a node of G, then by construction the isotopy $\psi^{x,y}$ contains the involution $\xi = \xi(G)$ native to u for each of the two edges incident to u in the chain P and identity permutations for all other edges incident to u in the tree T. By Lemma 4.2, such a collection of permutations forms an autotopy of the quasigroup prescribed to the vertex u.

The second part of nodes in the chain P consists of bridges, which do not belong to the bunch G, but provide the edges of G. Let v be such a bridge in the tree T and z be the only leaf of v. By construction, the isotopy $\psi^{x,y}$ contains two foreign to v involutions $\xi(G)$ and a native to v transposition $\tau(z)$ that form an autotopy of the quasigroup prescribed to the vertex v.

For each of the nodes not in the chain P, the isotopy $\psi^{x,y}$ induces the identity autotopy. From these arguments, we conclude that for each node in the tree T, the isotopy $\psi^{x,y}$ yields an autotopy of the quasigroup prescribed to this node. Consistently, $\psi^{x,y}$ is an autotopy of the decomposition S. □

Let us note that a bald bunch, as well as a bunch with only one leaf, do not grant any autotopies of the kind $\psi^{x,y}$.

Lemma 5.2. *If a bunch G contains $k \geqslant 1$ leaves in its leaf set, then there exist at least 2^{k-1} autotopies of the decomposition S acting in the following way: on the edges incident to leaves of G, they act with identity permutations or involutions native to the nodes of G; on the edges that are incident to the leaves of the bridges connecting the nodes of G, they act with identity permutations or transpositions native to the bridges.*

Proof. Let $\{x, y_1, \ldots, y_{k-1}\}$ be the leaf set of the bunch G. Autotopies ψ^{x,y_i}, $i = 1, \ldots, k-1$, of order 2 each commute with each other and are independent from each other since for each i only one of them, namely ψ^{x,y_i} obtains a non-identity permutation for the edge incident to the leaf y_i. Therefore, these $k-1$ autotopies yield 2^{k-1} autotopies corresponding to the bunch G. □

In further, the autotopies of the decomposition S described in Lemma 5.2 are called the *autotopies induced by the bunch G*. All them are of order 2.

If a bunch contains a fork, we can point out autotopies of order 4, which contribute additionally to the size of the autotopy group of the corresponding quasigroup.

Lemma 5.3. *For each fork in a decomposition tree, one can find two autotopies of the decomposition acting on the leaf edges of the fork with its native cycles and on all other edges with identity permutations.*

Proof. Consider a fork u in a decomposition S and let ξ be the native involution of u. Without loss of generality, we assume that the node adjacent to the fork u is its 0-th neighbor, while the leaves x and y of u are the 1-st and 2-nd neighbors respectively. For each pair φ_1, φ_2 of cycles native to u, by Lemma 4.3 there exists exactly one permutation $\xi' \in \{\mathrm{Id}, \xi\}$ such that the triple $\varphi = (\xi', \varphi_1, \varphi_2)$ forms an autotopy of the quasigroup f prescribed to the fork u.

If $\xi' = \mathrm{Id}$ then φ and φ^{-1} are required autotopies of f, which can be finished up to autotopies of the decomposition S by use of identity permutations. If $\xi' = \xi$, then one can take the isotopy $(\xi', \varphi_1, \varphi_2)(\xi, \xi, \mathrm{Id}) = (\mathrm{Id}, \varphi_1\xi, \varphi_2)$ instead of φ. By Lemma 4.3, the former is also an autotopy of the quasigroup f with its native cycles $\varphi_1\xi$ and φ_2. □

Lemma 5.4. *For any decomposition, its non-identity autotopies induced by different bunches of the decomposition tree are independent and commute with each other.*

Proof. Consider a decomposition S with the tree T and two autotopies of S. If the supports of the autotopies intersect in the empty set, then they are trivially independent and commute with each other. At the same time, the supports of autotopies induced by different bunches of $G(T)$ can intersect only in edges of bridge nodes. Indeed, according to Lemma 5.3, the support of the autotopy corresponding to a fork does not exceed the set of leaf edges of the fork. As while as the support of an autotopy $\psi^{x,y}$ induced by a bunch G can contain only edges incident to the nodes of G. If there are more than one node in G, then some of the edges in the support of $\psi^{x,y}$ are also inner edges of bridges connecting nodes of G.

Thereby, it is sufficient to prove the lemma for autotopies induced by different bunches with supports intersecting in edges incident to bridge nodes. An arbitrary autotopy induced by a bunch G acts on edges in its support in the following way:

- on edges incident to nodes of G, it acts with involutions native to nodes of the bunch G;
- on leaf edges incident to bridges connecting nodes of G, it acts with transpositions native to the bridges.

Assume that a bridge v with a leaf z connects two nodes of the bunch G; and let v be contained in another bunch G'. By Lemma 4.3(iv), all autotopies induced by G contain exactly one of the two transpositions native to v, namely $\tau = \tau(z)$. The transposition τ cannot generate the involution native to the bridge v. Thus, the autotopies induced by the bunch G and the autotopies induced by the bunch G' are independent.

Consider autotopies $\theta = \psi^{x,y}$ and $\theta' = \psi^{x',y'}$ induced by the bunches G and G' respectively. Let the supports of these two autotopies contain edges incident to a bridge v in their intersection. Autotopies θ and θ' act on inner edges of v with involutions $\xi = \xi(G)$ and $\xi' = \xi'(G')$ native to G and G' respectively. Since involutions (01)(23), (02)(31) and (03)(12) commute with each other, we have $\xi\xi' = \xi'\xi$.

The autotopy θ acts on the leaf edge of the bridge v with the transposition τ, while the autotopy θ' acts on this edge with some involution η' (or the identity permutation, which is considered trivially). Both τ and η' are native to v. It is obvious that, for example, the involution (01)(23) and the transpositions (01) and (23) forming it commute. The same is true for the involutions (02)(31) and (03)(12). Therefore, we get $\tau\eta' = \eta'\tau$.

From the reasoning above it is follows that the autotopies θ and θ' commute on every edge that is contained in the intersection of their supports. This proves commutativity of autotopies of the decomposition S induced by different bunches in its tree. □

Theorem 5.5. *For an arbitrary n-ary quasigroup f of order 4, the following inequality holds:*

$$|\mathrm{Atp}(f)| \geqslant 2^{[n/2]+2}. \tag{11}$$

If $n \geqslant 5$, then this bound is sharp.

Proof. Let the quasigroup f have a reduced decomposition S with the tree T. For each bunch G with $k \geqslant 1$ leaves, by Lemma 5.2 one can construct 2^{k-1} autotopies of f which act on variables corresponding to leaves of the bunch G with permutations of order 2. Taking into account all bunches of the graph $G(T)$ except the bald ones, by use of Lemma 5.4 we get $2^{N-(\Gamma-L)}$ autotopies of f.

In addition, for any fork v in the tree T, by Lemma 5.3 there are 2 autotopies of f which act on variables corresponding to the leaves adjacent to v with cycles native to the fork v. This contributes the factor 2^F to the number of constructed here autotopies of f. In this way, using (9) we obtain

$$|\mathrm{Atp}(f)| \geqslant 2^{N-(\Gamma-L)+F} = 2^{N-V+B+L+F}. \tag{12}$$

Suppose that in the decomposition tree T there are t edges and V_s vertices of degree s, $s = 0, 1, 2, \ldots$. By definition of a quasigroup decomposition and accordingly to notation stabilized above, it can be written $V_1 = N$, $V_2 = 0$. Thus,

$$N + \sum_{s\geqslant 3} sV_s = 2t = 2(N + V - 1).$$

It follows that

$$N + 2V - 2 = \sum_{s\geqslant 3} sV_s = 4\sum_{s\geqslant 3} V_s + \sum_{s\geqslant 5} (s-4)V_i - V_3 \geqslant 4V - V_3. \tag{13}$$

Consequently, the inequality $N \geqslant 2V - V_3 + 2$ holds.

In accordance with the number of adjacent leaves, the nodes of degree 3 in the tree T are partitioned into forks, bridge nodes, and bald nodes (there are no vertices of degree 3 with three adjacent leaves since $n > 2$). Trivially, the number of bald nodes of degree 3 is not greater than the total number of bald nodes in T. Taking into account (10), we get

$$V_3 \leqslant F + B + E \leqslant F + 2B + L, \tag{14}$$

which allows to rewrite the estimate for N in more detail:

$$N \geqslant 2V - V_3 + 2 \geqslant 2V - F - 2B - L + 2.$$

Hence,

$$-V + B \geqslant -\frac{1}{2}(N + F + L) + 1.$$

Applying this inequality to (12), we derive

$$|\mathrm{Atp}(f)| \geqslant 2^{(N+F+L)/2+1} \geqslant 2^{N/2+1} = 2^{(n+3)/2} \tag{15}$$

Let us note that the second inequality in (15) is strict if and only if the decomposition tree contains a fork or bald node. Since $|\mathrm{Atp}(f)|$ is an integer and the number of autotopies generated by those described in Lemmas 5.2 and 5.3 is a power of 2, we have

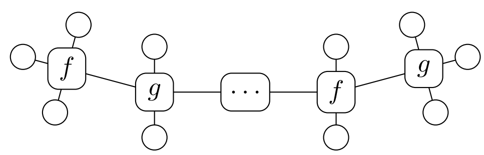
$$|\mathrm{Atp}(f)| \geqslant 2^{\lfloor n/2 \rfloor + 2}. \tag{16}$$

Further, let us show that the bound (16) is attainable. Consider the quasigroups $l_3^\bullet$ and $l_4^\bullet$ in Lemma 4.5, which we denote here by f and h correspondingly, and the quasigroup $x_0 = g(x_1, x_2, x_3) = \tau f(\tau x_1, \tau x_2, \tau x_3)$ with $\tau = (12)$, which is isotopic to the ternary quasigroup f.

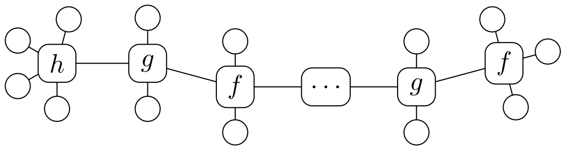
The quasigroups f and g are $\{0,2\}$- and $\{0,1\}$-semilinear, respectively. Their autotopy groups are isomorphic to each other, namely one of them is conjugate with the other by the transposition τ. The permutation $(01)(23)$ is a native involution for g, as (01) and (23) are native transpositions of g.

Note that only the identity permutation Id can be met in autotopies of both f and g. The same is true for h and g. Therefore, if f and g (or h and g, respectively) are adjacent in a decomposition tree of some quasigroup q, then by Lemma 4.1 their autotopies can concatenate to an autotopy of the decomposition of q only by the identity permutation.

Reasoning in this way, it is easy to see that for odd $n \geqslant 5$ the quasigroup q_n of arity n with a decomposition tree of kind



has the autotopy group of order $2^{(n-1)/2+2}$. For even $n \geqslant 6$, the quasigroup q_n of arity n with a decomposition tree of kind



has the autotopy group of order $2^{n/2+2}$. In both cases, the equality is attained in (16) for the quasigroups designed. □

Remark 5.6. For $n = 3$ and $n = 4$, the bound pointed out in Theorem 5.5 is not sharp. The quasigroup q_n described in the proof degenerates into a semilinear quasigroup, which has autotopies consisting of its native transpositions (see Lemma 4.5(ii)). Such autotopies are not taken into account in the estimation of Theorem 5.5.

The quasigroup q_n also delivers the minimum for order of autotopy group in the case $n \in \{3, 4\}$. However, in this case the minimum is two times greater than the minimum number in Theorem 5.5. At the same time, any decomposition tree of a reducible quasigroup of arity $n \in \{3, 4\}$ contains a fork. If there are two forks, then the difference can be seen from inequalities in (15). If there is one fork, then by Lemma 4.3(iv) the quasigroup q_n has autotopies with non-identity involution acting on the inner edge of the fork, which are not considered in the proof of Theorem 5.5.

5.2. Quasigroups with autotopy groups of minimum order

Besides the examples of quasigroups described in the proof of Theorem 5.5, there are many other such quasigroups for which the equality is attained in the lower bound given by the theorem. In this section, we characterize quasigroups with this property for n odd. In our reasoning we examine the cases in which all non-strict inequalities occurring in the proof of the theorem turn into equalities. In case of even n, we have not got such an opportunity since we explicitly use the ceil function.

For odd n, the number in the right part of (11) equals $2^{\lfloor n/2 \rfloor+2} = 2^{\frac{n-1}{2}+2} = 2^{\frac{n+3}{2}}$. Based on the proof of Theorem 5.5, for odd n one can derive properties of reduced decompositions with exactly $2^{\frac{n+3}{2}}$ autotopies. The tree of such a decomposition does not contain:

(I) any vertices of degree greater than 4 (this follows from the equality in (13)),

(II) any forks (the equality in (15)),

(III) any bald bunches (the equality in (15)),

(IV) greater than one non-bald vertex in each bunch (the equality in (10)),

(V) any bald vertices of degree greater than 3 (the equality in (14)).

Conditions (III)–(V) imply that in a decomposition with exactly $2^{\frac{n+3}{2}}$ autotopies

(III–V) each bunch contains exactly one non-bald node, which can be a bridge or node of degree 4, and possibly some bald nodes of degree 3 as well.

Let us take a reduced decomposition that satisfies the conditions (I)–(V) and label each of its nodes of degree 4 with a ternary quasigroup isotopic to $l_3^{\bullet}$. This decomposition has only the autotopies considered in the proof of Theorem 5.5, and the corresponding quasigroup meets the bound $2^{\frac{n+3}{2}}$ for the order of the autotopy group. On the other side, the following statement takes place.

Lemma 5.7. *Let S be a reduced decomposition of an n-quasigroup f of order 4 with $|\mathrm{Atp}(f)| = 2^{\frac{n+3}{2}}$. Each node of degree 4 in the decomposition S has a ternary quasigroup isotopic to the quasigroup $l_3^{\bullet}$ as its label.*

Proof. There exist exactly five ternary quasigroups up to isotopy, variable permutation, and inversion [10]. One of them is linear and another one is non-semilinear. The remaining three quasigroups are semilinear, but not linear. These three are the quasigroups $l_3^{\bullet}$,

$$g(x_1, x_2, x_3) = x_1 \oplus (x_2 +_4 x_3), \quad \text{and} \quad h(x_1, x_2, x_3) = x_1 +_4 x_2 +_4 x_3.$$

The quasigroup g admits the autotopy $\varphi = ((01)(23), (01)(23), \mathrm{Id}, \mathrm{Id})$ with two involutions foreign to g. The quasigroup h has got the autotopy

$$((01)(23), (01)(23), (01)(23), (01)(23)),$$

consisting of four foreign involutions.

Suppose that the tree T of a decomposition S has a node α labeled with g (the case of h can be handled similarly). We will show that under the assumptions made one can obtain $|\mathrm{Atp}(f)| > 2^{\frac{n+3}{2}}$. With this aim, for the decomposition S we construct a special autotopy consisting of permutations in the transformation φ. It helps us to get the inequality.

Consider the 0-th neighbor of the node α. If it is a leaf, then we prescribe the permutation $(01)(23)$ to the leaf edge. If the neighbor is a node, it belongs to some bunch G. According to (III), the bunch G is not bald and contains at least one leaf x. Assume that a chain P connects the leaf x with the node α in the tree T. Prescribe the permutation $(01)(23)$ to each edge of P. If there is any bridge node in the chain P, which connects two nodes of the bunch G, we prescribe a native transposition to the leaf edge of the bridge accordingly to Lemma 4.3(iv). Next, we do the same construction for the 1-st neighbor of the node α and prescribe the identity permutation to the remaining edges in the tree T.

Finally, we obtain an autotopy θ of the decomposition S because for each node v in T the permutations acting on the edges incident to v form an autotopy of the quasigroup corresponding to v. In addition, the autotopy θ does not contribute to the number given as a lower bound in Theorem 5.5. Indeed, in the proof of the theorem we consider only those autotopies of the decomposition which act on every edge incident to a node of degree 4 with an involution native to the node. In contrast, the autotopy θ acts on two edges incident to α with the involution (01)(23), which is not native to g. Consequently, θ increases the order of the autotopy group of f; so, $|\mathrm{Atp}(f)| > 2^{\frac{n+3}{2}}$.

If the quasigroups h is prescribed to the node α, then one can construct an additional autotopy of f in the same way. The only difference is that in this case all neighbors of the node α should be considered. □

A decomposition tree satisfying conditions (I)–(V) can be constructed using the following procedure.

Construction T.

Step 1. Take an arbitrary tree T_1 with exactly $(n-1)/2$ vertices, which we call *nodes*. The degree of each node should not exceed 3.

Step 2. Connect $4-i$ new *leaves* to each node of degree $i \in \{1,2,3\}$ in the tree T_1. Degree of each node in the resulting tree T_2 equals 4.

Step 3. Select some (maybe none, maybe all) nodes adjacent to exactly one leaf. Replace each selected node s by two new nodes u_s and v_s of degree 3 adjacent to each other. Four neighbors of v can be distributed among the neighborhoods of u_s and v_s in any of three possible ways. Denote the tree obtained at this step by T_3.

Step 4. Divide the nodes of T_3 into two independent parts V_1 and V_2, which is possible because any tree is a bipartite graph.

Step 5. To each node in the part V_i, $i = 1, 2$, assign a $\{0, i\}$-semilinear quasigroup isotopic to $+_4$ or $l_3^\bullet$

Step 6. Finally, choose a leaf to represent the value of the quasigroup, index the neighbors of each node in an appropriate way and get a decomposition tree T of some quasigroup f.

Moreover, it turns out that, for every quasigroup f which meets the bound on the order of its autotopy group, one can build a quasigroup isotopic to f using Construction T.

Theorem 5.8. *Every n-ary quasigroup f with the autotopy group of order $2^{\frac{n+3}{2}}$ is isotopic to some quasigroup with a decomposition tree obtained with Construction T.*

Proof. Let T be a decomposition tree built using the construction. Nodes of degree 3 are combined in pairs "bald node – bridge node" input at Step 3. In each pair, the bald node is included into some bunch, while the bridge node corresponds to an edge of that bunch. Since a bunch is a tree and the number of vertices in a tree is one more than the number of edges, every bunch contains exactly one non-bald node. By construction, it is a bridge node or node of degree 4. Therefore, the tree T satisfies conditions (I)–(V).

On the other hand, consider a quasigroups f that meets the bound $2^{\frac{n+3}{2}}$ on the order of the autotopy group. Let T be the tree of a decomposition of f. From condition (III–V), it follows that in any bunch the numbers of bald nodes and edges coincide. Consequently, there is a one-to-one correspondence between the bridges and the bald nodes, all of which have degree 3. In addition, we can require that a bridge is adjacent to its corresponding bald node. Shrinking the pairs of corresponding nodes of degree 3 (an operation reverse to Step 3), we get a tree whose all nodes are non-bald and of degree 4. Any such a tree can be obtained at Step 2. By Lemmas 3.5 and 5.7, the node labeling of the decomposition tree T conforms to the labeling at Step 5. □

6. An upper bound

In this section, we prove that the maximum order of the autotopy group of an n-ary quasigroup of order 4 equals $6 \cdot 2^n$, and only the linear quasigroup, which is unique up to isotopy, reaches the upper bound. We also determine the quasigroups that have the maximum order of autotopy groups among the nonlinear quasigroups and point out this order as well.

Here we use Orbit–Stabilizer Theorem. In our case, this theorem says that the order of the autotopy group of a code M equals the size of the stabilizer of any element $x \in M$ multiplied by size of the orbit of x under the action of the autotopy group. Let us start with several auxiliary statements concerning autotopies of a n-ary quasigroups that stabilize a certain element in the quasigroup code. For simplicity, that element is usually considered to be the all-zero tuple $(0, \dots, 0)$. The next lemma takes place for a quasigroup of any order k.

Lemma 6.1. *Let f be an n-quasigroup and $f(0, \dots, 0) = 0$. Then an arbitrary autotopy $(\theta_0, \dots, \theta_n) \in \mathrm{Atp}(f)$ stabilizing the all-zero tuple is uniquely determined by any single of its permutations θ_i, $i \in \{0, \dots, n\}$. In particular, if for some $i \in \{0, \dots, n\}$ the permutation θ_i is identity, then all the others are also identity.*

Proof. Without loss of generality, given the permutation θ_0, we express the permutations $\theta_1, \dots, \theta_n$ in terms of it.

Assume that $(\theta_0, \dots, \theta_n)$ is an autotopy of f such that $\theta_i 0 = 0$, $i = 0, 1, \dots, n$. By the

By the autotopy definition, we get

$$\theta_0^{-1} f(\theta_1 x_1, 0, \dots, 0) = f(x_1, 0, \dots, 0) \quad \text{for any } x_1 \in \Sigma,$$

which is equivalent to

$$\theta_1 x_1 = f^{<1>}(\theta_0 f(x_1, 0, \dots, 0), 0, \dots, 0) \quad \text{for any } x_1 \in \Sigma.$$

One can see that the permutation θ_1 is entirely determined by the quasigroup f and permutation θ_0. In the same manner, we can express any of $\theta_0, \ldots, \theta_n$ through any other one.

Finally, by the argumentation above it is evident that, for example, $\theta_0 = \mathrm{Id}$ imply $\theta_i = \mathrm{Id}$ for any $i \in \{1, \ldots, n\}$. □

Corollary 6.2. *If an autotopy $\theta = (\theta_0, \ldots, \theta_n)$ of an n-quasigroup f stabilizes a tuple $(a_0, \ldots, a_n)$ from $M(f)$, then all of the permutations θ_i, $i = 0, \ldots, n$, have the same order.*

Proof. By the hypothesis, $(a_0, \ldots, a_n) \in M(f)$; that is $a_0 = f(a_1, \ldots, a_n)$. Consider the quasigroup g defined as

$$g(x_1, \ldots, x_n) = \tau_0 f(\tau_1 x_1, \ldots, \tau_1 x_n),$$

where $\tau = (\tau_0, \ldots, \tau_n)$ is an isotopy consisting of the transpositions $\tau_i = (0\, a_i)$, $i = 0, \ldots, n$. It is easy to verify that $g(0, \ldots, 0) = 0$ and the isotopy

$$\delta = \tau\theta\tau = (\tau_0\theta_0\tau_0, \ldots, \tau_n\theta_n\tau_n),$$

conjugate to θ, is an autotopy of g stabilizing the all-zero tuple.

By Lemma 6.1, for any integer r, all permutations from the autotopy δ^r are identity if there is at least one identity permutation among them. Consequently, all permutations δ_i, $i = 0, \ldots, n$, have the same order.

It remains to note that the permutations δ_i, θ_i are of the same order because $\delta_i^r = \tau\theta_i^r\tau$, $i = 0, \ldots, n$. □

Lemma 6.3. *Let f be an n-quasigroup of order 4 such that $f(0, \ldots, 0) = 0$. If f has an autotopy θ of order 2 that stabilizes the all-zero tuple, then f is semilinear.*

Proof. By Corollary 6.2, each of the permutations θ_i, $i = 0, \ldots, n$, has order 2. Since $\theta_i(0) = 0$ for each $i = 0, \ldots, n$, we have $\theta_i \in \{(12), (13), (23)\}$. Without loss of generality, assume that $\theta_0 = \ldots = \theta_n = (23)$ (otherwise, consider a quasigroup isotopic to f that has the autotopy consisting of permutations (23)).

For every $(x_1, \ldots, x_n)$ from $\{0, 1\}^n$ and for $x_0 = f(x_1, \ldots, x_n)$, we have

$$x_0 = f(x_1, \ldots, x_n) = \theta_0^{-1} f(\theta_1 x_1, \ldots, \theta_n x_n) = \theta_0 f(x_1, \ldots, x_n) = \theta_0 x_0.$$

Since $\theta_0 = (23)$, the value of x_0 can only be 0 or 1. Therefore, the quasigroup f maps $\{0, 1\}^n$ to $\{0, 1\}$. So, f is semilinear by the definition. □

Lemma 6.4. *Let f be an n-quasigroup of order 4 such that $f(0, \ldots, 0) = 0$. If f has an autotopy θ of order 3 that stabilizes some tuple $(a_0, \ldots, a_n) \in M(f)$, then f is linear.*

Proof. By Corollary 6.2, each of the permutations θ_i, $i = 0, \dots, n$, has order 3.

(i) If f is $\{0,1\}$-, $\{0,2\}$-, or $\{0,3\}$-semilinear in every variable, then it is $\{a,b\}$-semilinear for any $a \neq b \in \Sigma$ and, consequently, linear. Hence, the lemma is true for semilinear quasigroups.

(ii) Assume f is not semilinear. Consider a proper decomposition S of f and the corresponding tree T. The autotopy δ of S induced by θ has the same order 3. Therefore, δ consists of 3-cycles or identity permutations. Each of those permutations stabilizes some element in Σ.

Consider an arbitrary non-bald node v labeled by a quasigroup g. The autotopy of g induced by δ satisfies the hypothesis of Corollary 6.2; so, each of its permutations has order 3. Since S is a proper decomposition, g is semilinear, and from item (i) of this proof we conclude that it is linear. This contradicts the definition of a proper decomposition. □

Theorem 6.5. *(i) The maximum order for an autotopy group of an n-ary quasigroup of order 4 equals $6 \cdot 4^n$; only the linear quasigroups reach this maximum. (ii) The maximum order for an autotopy group of a nonlinear n-ary quasigroup of order 4 equals $2 \cdot 4^n$; only the semilinear quasigroups whose autotopy group acts transitively on their codes reach this maximum.*

Proof. Consider an arbitrary n-ary quasigroup f of order 4. Without loss of generality, we assume that $f(0, \dots, 0) = 0$.

By Orbit–Stabilizer Theorem, the order of $\mathrm{Atp}(M(f))$ equals the size of its stabilizer subgroup with respect to $(0, \dots, 0) \in M(f)$ multiplied by the size of the orbit of $(0, \dots, 0)$ under the action of $\mathrm{Atp}(M(f))$.

For the all-zero tuple, the size of its orbit does not exceed the cardinality of $M(f)$, i.e., 4^n (the equality takes place if and only if the orbit coincides with the code; in other words if the action of the autotopy group is transitive on the code.)

Next, consider the size of the stabilizer with respect to the all-zero tuple. For a non-semilinear quasigroup, it equals 1 by Lemmas 6.3 and 6.4. As for a semilinear quasigroup that is not linear, the size of the stabilizer is 2 (at least 2 by Lemma 4.5; at most 2 by Lemmas 6.1 and 6.4). So, (ii) is proved.

Since any linear quasigroup is isotopic to the quasigroup $l_n(x_1, \dots, x_n) = x_1 \oplus \dots \oplus x_n$, it remains to find $|\mathrm{Atp}(l_n)|$. For an arbitrary tuple $(a_0, \dots, a_n) \in M(l_n)$, the mapping $(x_0, \dots, x_n) \mapsto (x_0 \oplus a_0, \dots, x_n \oplus a_n)$ maps $(0, \dots, 0)$ to $(a_0, \dots, a_n)$ and induces an autotopy of l_n. Hence, the size of the orbit of $(0, \dots, 0)$ equals 4^n.

The size of the stabilizer with respect to $(0, \dots, 0)$ is at most 3! by Lemma 6.1. On the other hand, for each of 3! permutations θ_* of Σ such that $\theta_*(0) = 0$, we have ab autotopy $\theta = (\theta_*, \dots, \theta_*)$ (this can be checked by induction on the arity n). Therefore, the size of the stabilizer equals 6, and the order of the autotopy group of any linear n-ary quasigroup of order 4 is $6 \cdot 4^n$. □

In conclusion, we should note that the semilinear n-ary quasigroups with transitive autotopy groups were characterized in [4], where a correspondence between such quasigroups and Boolean polynomials of degree at most 2 was established.

References

[1] **V.D. Belousov**, *n-Ary Quasigroups*, (Russian), Shtiintsa, Kishinev, 1972.

[2] **R. Frucht**, *Herstellung von graphen mit vorgegebener abstrakter gruppe*, Compos. Math. **6** (1938), 239 – 250.

[3] **D.S. Krotov, V.N. Potapov**, *n-Ary quasigroups of order* 4, SIAM J. Discrete Math. **23** (2009), no. 2, 561 – 570.

[4] **D.S. Krotov, V.N. Potapov**, *Constructions of transitive latin hypercubes*, Eur. J. Comb. **54** (2016), 51 – 64.

[5] **S.A. Malyugin**, *On the order of the automorphism group of perfect binary codes*, (Russian), Diskretn. Anal. Issled. Oper., Ser. 1 **7** (2000), no. 4, 91 – 100.

[6] **K.T. Phelps**, *Every finite group is the automorphism group of some perfect code*, J. Comb. Theory, Ser. A **43** (1986), 45 – 51.

[7] **V.N. Potapov, D.S. Krotov**, *Asymptotics for the number of n-quasigroups of order* 4, Sib. Math. J. **47** (2006), no. 4, 720 – 731.

[8] **F.I. Solov'eva, S.T. Topalova**, *On automorphism groups of perfect binary codes and Steiner triple systems*, Probl. Inf. Transm. **36** (2000), no. 4, 331 – 335.

[9] **F.I. Solov'eva, S.T. Topalova**, *Perfect binary codes and Steiner triple systems with maximum orders of automorphism groups*, (Russian) Diskretn. Anal. Issled. Oper., Ser. 1 **7** (2000), no. 4, 101 – 110.

[10] **V.A. Zinoviev, D.V. Zinoviev**, *Binary extended perfect codes of length* 16 *by the generalized concatenated construction*, Probl. Inf. Transm. **38** (2001), no. 4, 296 – 322.

Received March 03, 2019

Sobolev Institute of Mathematics, pr. Akademika Koptyuga 4, Novosibirsk 630090, Russia
and
Novosibirsk State University, Pirogova 2, Novosibirsk 630090, Russia
E-mails: gorkunov@math.nsc.ru, krotov@math.nsc.ru, vpotapov@math.nsc.ru