Comment.Math.Univ.Carolin. 51,2 (2010) 357–370

On the structure of finite paramedial quasigroups

V.A. Shcherbacov, D.I. Pushkashu

Abstract. Information on the structure of finite paramedial quasigroups, including a classification of finite simple paramedial quasigroups, is given. The problem "Classify the finite simple paramedial quasigroups" was posed by J. Ježek and T. Kepka at the conference LOOPS'03, Prague 2003.

Keywords: quasigroup, paramedial quasigroup, medial quasigroup, simple quasigroup, idempotent

Classification: 20N05

Jaroslav Ježek and Tomaš Kepka posed the problem "Classify the finite simple paramedial quasigroups" at conference LOOPS'03, Prague 2003 [34]. Paramedial quasigroups are studied in [21], [17].

1. Introduction

We shall use basic terms and concepts from the books [3], [4], [9], [22]. We shall use the following order of multiplication (composition) of maps: $(\alpha\beta)(x) = \alpha(\beta(x))$, where α, β are maps. By ε we mean the identity permutation.

As usual, $L_a : L_a x = a \cdot x$, $R_a : R_a x = x \cdot a$ are, respectively, left and right translations of a quasigroup $(Q, \cdot)$. A map h of a non-empty set Q into itself will be called a *zero map*, if $|h(Q)| = 1$.

A quasigroup $(Q, \cdot)$ satisfying the identity $x \cdot x = x$ is called an *idempotent quasigroup*. A quasigroup $(Q, \cdot)$ satisfying the identity $x \cdot x = e$, where e is a fixed element of Q, is called a *unipotent quasigroup*.

1.1 Linear quasigroups and their subclasses. A quasigroup $(Q, \cdot)$ of the form

$$x \cdot y = \varphi x + \psi y + a, \tag{1}$$

where $(Q, +)$ is a group, φ, ψ are automorphisms of $(Q, +)$, and a is a fixed element of Q, is called *linear quasigroup* (over the group $(Q, +)$) [2].

A linear quasigroup over an abelian group is called a *T-quasigroup* [21]. The theory of T-quasigroups was developed by T. Kepka and P. Němec [21], [17]. G.B. Belyavskaya [6] characterized the class of T-quasigroups by two identities. See also [8], [32].

A quasigroup $(Q, \cdot)$ satisfying the identity

$$xy \cdot uv = xu \cdot yv \tag{2}$$

is called *medial*.

Theorem 1.1 (Toyoda theorem [3], [4], [22], [33]). *Every medial quasigroup $(Q, \cdot)$ can be presented in the form:*

$$x \cdot y = \varphi x + \psi y + a, \tag{3}$$

for all $x, y \in Q$, where $(Q, +)$ is an abelian group, φ, ψ are automorphisms of $(Q, +)$ such that $\varphi\psi = \psi\varphi$ and a is some fixed element in Q.

Note that before the Toyoda theorem, D.C. Murdoch proved results about the direct decompositions of finite medial quasigroups [20] (see also Theorem 1.3).

The following identity

$$xy \cdot uv = vy \cdot ux \tag{4}$$

is called the *paramedial* identity.

Theorem 1.2 (Kepka-Němec Theorem [21]). *Every paramedial quasigroup $(Q, \cdot)$ can be presented in the form:*

$$x \cdot y = \varphi x + \psi y + g, \tag{5}$$

for all $x, y \in Q$, where $(Q, +)$ is an abelian group, φ, ψ are automorphisms of $(Q, +)$ such that $\varphi\varphi = \psi\psi$ and g is some fixed element of Q.

Remark 1.1. If we define a paramedial quasigroup $(Q, \cdot)$ using a finite ring of residues modulo n, then the automorphisms φ and ψ of the abelian group $(Q, +)$ correspond to pairs of numbers k, l such that $\gcd(k, n) = \gcd(l, n) = 1$ and $k^2 \equiv l^2 \pmod{n}$.

For a quasigroup $(Q, \cdot)$ we define the map s: $s(x) = x \cdot x$ for all $x \in Q$. As usual, $s^2(x) = s(s(x))$ and so on.

We give Murdoch's theorem [20] in a slightly modernized form [26], [27]. This modernization is based on the following easy proved fact: for any medial quasigroup $(Q, \cdot)$ the map s is an endomorphism of this quasigroup. Indeed $s(xy) = xy \cdot xy = xx \cdot yy = s(x) \cdot s(y)$.

A quasigroup $(Q, \cdot)$ is called an *unipotently-solvable quasigroup* of degree m if there exists the following finite chain of unipotent quasigroups:

$$Q/s(Q), s(Q)/s^2(Q), \ldots, s^m(Q)/s^{m+1}(Q)\,,$$

where the number m is the minimal natural number with the property $|s^m(Q)/s^{m+1}(Q)| = 1$.

Theorem 1.3. *Any finite medial quasigroup $(Q, \cdot)$ is isomorphic to the direct product of a medial unipotently-solvable quasigroup $(Q_1, \circ)$ and a quasigroup $(Q_2, *)$, where $(Q_2, *)$ is an isotope of the form $(\varepsilon, \varepsilon, \gamma)$ of a medial distributive quasigroup $(Q_2, \star)$, $\gamma \in \mathrm{Aut}(Q_2, *)$, i.e., $(Q, \cdot) \cong (Q_1, \circ) \times (Q_2, *)$* [26], [27].

Theorem 1.3 reduces the study of the structure of finite medial quasigroups to the study of the structure of finite medial unipotent and idempotent quasigroups.

1.2 Congruences and homomorphisms. A binary relation on a set Q is any subset of $Q \times Q$.

Definition 1.1. An equivalence $\theta \subset Q \times Q$ is a *normal congruence* of a quasigroup $(Q, \cdot)$ if the following implications hold:

$$a\theta b \Longrightarrow (c \cdot a)\theta(c \cdot b),\ a\theta b \Longrightarrow (a \cdot c)\theta(b \cdot c),\ (c \cdot a)\theta(c \cdot b) \Longrightarrow a\theta b,\ (a \cdot c)\theta(b \cdot c) \Longrightarrow a\theta b$$

for all $a, b, c \in Q$ [32].

In any quasigroup $(Q, \cdot)$ the binary relations $\hat{Q} = \{(x, x) \mid x \in Q\}$ and $Q \times Q$ are congruences of $(Q, \cdot)$. These congruences are called the diagonal congruence and universal congruence, respectively.

Definition 1.2. A quasigroup $(Q, \cdot)$ is *simple* if its only normal congruences are the diagonal $\hat{Q}$ and universal $Q \times Q$.

Definition 1.3. If θ is a binary relation on a set Q, α is a permutation of the set Q and from $x\theta y$ it follows $\alpha x \theta \alpha y$ for all $(x, y) \in \theta$, then we shall say that the permutation α is an *admissible* permutation relative to θ and that θ is admissible relative to the permutation α [3].

Thus any quasigroup congruence is admissible relative to any left and right quasigroup translation. Any normal quasigroup congruence is admissible relative to any left, right quasigroup translation and its inverse.

Lemma 1.1. *In a quasigroup $(Q, \cdot)$ of finite order, every congruence is normal* [4], [3].

Proof: Since Q has finite order, for any left translation L_a there exists a natural number m such that $L_a^m = \varepsilon$. Thus $L_a^{-1} = L_a^{m-1}$. For right translations, the proof is similar. □

Definition 1.4. A quasigroup $(Q, \cdot)$ is *α-simple* if it does not contain a nontrivial congruence that is admissible relative to a permutation α of the set Q.

Definition 1.5. If $(Q, \cdot)$ and $(H, \circ)$ are quasigroups, $h : Q \to H$ is a mapping such that $h(x_1 \cdot x_2) = hx_1 \circ hx_2$, then h is called a (multiplicative) *homomorphism* of $(Q, \cdot)$ into $(H, \circ)$ and the set $\{hx \mid x \in Q\}$ is called the *homomorphic image* of $(Q, \cdot)$ under h ([1], [22]).

In case $(Q, \cdot) = (H, \circ)$ a homomorphism is also called an *endomorphism* and an isomorphism is referred to as an automorphism.

There exists a well known connection between quasigroup homomorphisms and congruences [4], [22].

Theorem 1.4. *If h is a homomorphism of a quasigroup $(Q, \cdot)$ onto a quasigroup $(H, \circ)$, then h determines a normal congruence θ on $(Q, \cdot)$ such that $Q/\theta \cong (H, \circ)$, and vice versa, a normal congruence θ induces a homomorphism from $(Q, \cdot)$ onto $(H, \circ) \cong Q/\theta$* ([4], [22, I.7.2 Theorem]).

A subquasigroup $(H, \cdot)$ of a quasigroup $(Q, \cdot)$ is *normal* ($(H, \cdot) \trianglelefteq (Q, \cdot)$), if $(H, \cdot)$ is an equivalence class (in other words, a coset class) of a normal congruence. Notice that any subquasigroup of a T-quasigroup is normal ([17, Theorem 43]).

Definition 1.6. A congruence θ of a quasigroup $(Q, \cdot)$ is called *regular* if it is uniquely defined by any its coset $\theta(a)$. A coset $\theta(a)$ of a congruence θ is called *regular* if it is a coset of only one congruence.

Remark 1.2. In [19] A.I. Mal'tsev has given necessary and sufficient conditions that a normal complex K of an algebraic systems A is a coset of only one congruence, i.e. K is a coset of only one congruence of a system A. From his result it follows that in a finite quasigroup $(Q, \cdot)$, any congruence is regular. See also [25].

1.2.1 Antihomomorphisms. Similarly with Definition 1.5 we give the following:

Definition 1.7. If $(Q, \cdot)$ and $(H, \circ)$ are quasigroups, $h : Q \to H$ is a mapping such that $h(x_1 \cdot x_2) = hx_2 \circ hx_1$, then h is called a (multiplicative) *antihomomorphism* of $(Q, \cdot)$ into $(H, \circ)$ and the set $\{hx \,|\, x \in Q\}$ is called the *antihomomorphic image* of $(Q, \cdot)$ under h.

Remark 1.3. It is easy to see that with any antihomomorphism h we can associate a homomorphism $\mathbf{h}$ in the following way: $h(x_1 \cdot x_2) = hx_2 \circ hx_1$ if and only if $\mathbf{h}(x_1 \cdot x_2) = \mathbf{h}x_1 * \mathbf{h}x_2$, where $(H, *)$ is (12)-parastrophe of the quasigroup $(H, \circ)$.

We have used the same letter h in various type faces because a mapping h of the set Q into the set H in both cases is the same.

In case $(Q, \cdot) = (H, \circ)$ an antihomomorphism is also called an *antiendomorphism* and an antiisomorphism is referred to as an antiautomorphism.

Lemma 1.2. *Let h be an antihomomorphism of a quasigroup $(Q, \cdot)$ onto a groupoid $(H, \circ)$. Then h induces a congruence* $\mathrm{Ker}\, h = \theta$ *(the kernel of h) in the following way: $x \,\theta\, y$ if and only if $h(x) = h(y)$.*

PROOF: It is easy to see that θ is an equivalence. We prove that the equivalence θ is a congruence. Rewrite implication $(a)\,\theta\,(b) \longrightarrow (c \cdot a)\,\theta\,(c \cdot b)$ in the following form $h(a) = h(b) \longrightarrow h(c \cdot a) = h(c \cdot b)$. The last implication is equivalent with the following $h(a) = h(b) \longrightarrow h(a) \circ h(c) = h(b) \circ h(c)$. It is clear that this last implication is true. In the similar way, we may prove the implication $(a)\,\theta\,(b) \longrightarrow (a \cdot c)\,\theta\,(b \cdot c)$. $\square$

For antiendomorphisms, the situation is more interesting.

Corollary 1.1. 1. *If h is an endomorphism of a quasigroup $(Q, \cdot)$, then $(hQ, \cdot)$ is a subquasigroup of $(Q, \cdot)$* [29], [28].

2. *If h is an antiendomorphism of a quasigroup $(Q, \cdot)$, then $(hQ, \cdot)$ is a subquasigroup of $(Q, \cdot)$.*

Proof: 1. We rewrite the proof from [4, p. 33] for more general case. We prove that $(hQ, \cdot)$ is a subquasigroup of quasigroup $(Q, \cdot)$. Let $h(a), h(b) \in h(Q)$. We demonstrate that the solution of equation $h(a) \cdot x = h(b)$ lies in $h(Q)$. Consider the equation $a \cdot y = b$. Denote solution of this equation by c, i.e. $y = c$. Then $h(c)$ is a solution of equation $h(a) \cdot x = h(b)$. Indeed, $h(a) \cdot h(c) = h(a \cdot c) = h(b)$.

It is easy to see, that this is a unique solution. Indeed, if $h(a) \cdot c_1 = h(b)$, then $h(a) \cdot h(c) = h(a) \cdot c_1$. Since $h(a), h(c), c_1$ are elements of $(Q, \cdot)$, then $h(c) = c_1$. For the equation $x \cdot h(a) = h(b)$, the proof is similar.

2. We prove that $(hQ, \cdot)$ is a subquasigroup of $(Q, \cdot)$. Let $h(a), h(b) \in h(Q)$. We demonstrate that the solution of equation $h(a) \cdot x = h(b)$ lies in $h(Q)$. Consider the equation $y \cdot a = b$. Denote solution of this equation by c, i.e. $y = c$. Then we have $h(c \cdot a) = h(a) \cdot h(c) = h(b)$. Then the element $h(c)$ is a solution of equation $h(a) \cdot x = h(b)$.

We prove that this is a unique solution. Indeed, if $h(a) \cdot c_1 = h(b)$, then $h(a) \cdot h(c) = h(a) \cdot c_1$. Since $h(a), h(c), c_1$ are elements of $(Q, \cdot)$, then $h(c) = c_1$.

For the equation $x \cdot h(a) = h(b)$, the proof is similar. □

Notice that Case 1 of Corollary 1.1 follows from Theorem 1.4.

2. Paramedial quasigroups

2.1 Antiendomorphisms of paramedial quasigroups. Note that the fact that a quasigroup has an endomorphism often plays a determining role in the study of the structure of the quasigroup [20], [26], [29], [28]. In this article we apply the endomorphic (or, more precisely, antiendomorphic) approach to the study of finite paramedial quasigroups.

Lemma 2.1. *For any paramedial quasigroup $(Q, \cdot)$, the map s is an antiendomorphism* [21], [17].

Proof: Indeed, $s(xy) = xy \cdot xy = yy \cdot xx = s(y) \cdot s(x)$. □

Corollary 2.1. *For any paramedial quasigroup $(Q, \cdot)$ the map s^2 is an endomorphism of this quasigroup.*

Proof: Indeed, $s^2(xy) = s(s(xy)) = s(s(y) \cdot s(x)) = s^2(x) \cdot s^2(y)$. □

Corollary 2.2. *For any paramedial quasigroup $(Q, \cdot)$ the map s^{2n+1}, $n \in \mathbb{N}$, is an antiendomorphism and the map s^{2n}, $n \in \mathbb{N}$, is an endomorphism.*

Proof: This follows from Lemma 2.1 and Corollary 2.1. □

Theorem 2.1. *The antiendomorphism s of a paramedial quasigroup $(Q, \cdot)$ is a zero map if and only if $(Q, \cdot)$ is a unipotent quasigroup given by $x \cdot y = \varphi x - \varphi y + g$ for all $x, y \in Q$, where $(Q, +)$ is an abelian group, $\varphi \in \mathrm{Aut}(Q, +)$ and $g \in Q$.*

Proof: ($\Rightarrow$) By Theorem 1.2, there exist an abelian group $(Q,+)$ and automorphisms φ, ψ such that $x\cdot y = \varphi x + \psi y + g$. From the conditions of the theorem, $s(0) = g$. Since the map s is a zero antiendomorphism of $(Q,\cdot)$ we have $s(x) = g$ for all $x \in Q$. Thus $s(x) = \varphi x + \psi x + g = g$, and so $\varphi x + \psi x = 0$ for all $x \in Q$, whence $\psi = -\varphi$.

($\Leftarrow$) In the quasigroup $(Q,\cdot)$ of the form $x\cdot y = \varphi x - \varphi y + g$ we have $s(x) = x\cdot x = \varphi x - \varphi x + g = g$ for all $x \in Q$. Then the map s is a zero antiendomorphism of $(Q,\cdot)$. $\square$

Corollary 2.3. *If a paramedial quasigroup $(Q,\cdot)$ of the form $x\cdot y = \varphi x - \varphi y + g$ has zero antiendomorphism s, then $(Q,\cdot)$ is isomorphic to a quasigroup $(Q,\circ)$ of the form $x\circ y = \varphi x - \varphi y$.*

Proof: Let $x\circ y = L_{-g}(L_g x \cdot L_g y)$, $x, y \in Q$. It is clear that $(Q,\circ) \cong (Q,\cdot)$. Quasigroup $(Q,\circ)$ has the following form

$$x\circ y = -g + \varphi(g+x) - \varphi(g+y) + g = \varphi g + \varphi x - \varphi g - \varphi y = \varphi x - \varphi y.$$

$\square$

Theorem 2.2. *The antiendomorphism s of a paramedial quasigroup $(Q,\cdot)$ is the identity permutation of the set Q if and only if $(Q,\cdot)$ is a medial distributive commutative quasigroup of the form $x\cdot y = \varphi x + \varphi y$ for all $x, y \in Q$, where $(Q,+)$ is an abelian group, $\varphi \in \operatorname{Aut}(Q,+)$.*

Proof: ($\Rightarrow$) By Theorem 1.2, there exist an abelian group $(Q,+)$ and automorphisms φ, ψ such that $x\cdot y = \varphi x + \psi y + g$. Since $s = \varepsilon$, we have $s(0) = \varphi 0 + \psi 0 + g = 0$, so that $g = 0$.

Therefore $s^{\cdot}(x) = \varphi x + \psi x = x$ for all $x \in Q$, $\psi = \varepsilon - \varphi$. Then $\varphi^2 = (\varepsilon - \varphi)^2$, $\varphi^2 = \varepsilon - \varphi - \varphi + \varphi^2$, $\varphi + \varphi = \varepsilon$. But $\varphi + \psi = \varepsilon$. Therefore $\varphi = \psi$, $x\cdot y = \varphi x + \varphi y$ and the quasigroup $(Q,\cdot)$ is a medial distributive commutative quasigroup.

($\Leftarrow$) In a medial distributive commutative quasigroup $(Q,\cdot)$, the map s is the identity (anti)endomorphism. $\square$

Lemma 2.2. *Let $(Q,\circ)$ be a distributive medial quasigroup with the form $x\circ y = \varphi x + \psi y$, $\alpha \in \operatorname{Aut}(Q,+)$. A quasigroup $(Q,\cdot)$ of the form $x\cdot y = L_a^+\alpha(x\circ y) = \alpha\varphi x + \alpha\psi y + a$ is a paramedial quasigroup if and only if $\psi = \alpha^{-1}\varphi\alpha$.*

Proof: If quasigroup $(Q,\cdot)$ is a paramedial quasigroup, we have $\alpha\varphi\alpha\varphi = \alpha\psi\alpha\psi$, and so $\varphi\alpha\varphi = \psi\alpha\psi$. But $\psi = \varepsilon - \varphi$, since $(Q,\circ)$ is a medial distributive quasigroup. Then $\varphi\alpha\varphi = (\varepsilon-\varphi)\alpha(\varepsilon-\varphi) = \alpha - \alpha\varphi - \varphi\alpha + \varphi\alpha\varphi$, so that $\alpha = \alpha\varphi + \varphi\alpha$, and thus $\varepsilon = \varphi + \alpha^{-1}\varphi\alpha$. But $\varepsilon = \varphi + \psi$. Therefore $\psi = \alpha^{-1}\varphi\alpha$, that is, $\alpha\psi = \varphi\alpha$.

It is easy to check that the converse also holds. $\square$

Theorem 2.3. *If the antiendomorphism s of a paramedial quasigroup $(Q,\cdot)$ of the form $x\cdot y = \varphi x + \psi y + g$ is a permutation of the set Q, then*

(i) *the map $\varphi + \psi$ is an automorphism of $(Q,+)$;*
(ii) *the quasigroup $(Q,\circ)$ of the form $x\circ y = s^{-1}(x\cdot y) = (\varphi+\psi)^{-1}\varphi x + (\varphi+\psi)^{-1}\psi y$ is a distributive medial quasigroup;*

(iii) *the map s is an antiautomorphism of* $(Q, \circ)$.

PROOF: (i) By Kepka-Nemec Theorem $x \cdot y = \varphi x + \psi y + g$. Then $s(x) = \varphi x + \psi x + g$, that is, $s = L_g(\varphi + \psi)$. Since the maps s and L_g are permutations of Q, the map $\varphi+\psi$ is an automorphism of the group $(Q, +)$, and $s^{-1} = (\varphi+\psi)^{-1}L_{-g}$.

(ii) Thus

$$x \circ y = s^{-1}(\varphi x+\psi y+g) = (\varphi+\psi)^{-1}(\varphi x+\psi y+g-g) = (\varphi+\psi)^{-1}\varphi\, x+(\varphi+\psi)^{-1}\psi y.$$

Notice $x \circ x = (\varphi + \psi)^{-1}\varphi\, x + (\varphi + \psi)^{-1}\psi x = (\varphi + \psi)^{-1}(\varphi + \psi)x = \varepsilon x = x$. Thus $(Q, \circ)$ is an idempotent T-quasigroup. It is well known that any idempotent T-quasigroup is a medial distributive quasigroup [21], [17]. Indeed, it is clear that $(\varphi + \psi)^{-1}\varphi + (\varphi + \psi)^{-1}\psi = \varepsilon$. Denote the expression $(\varphi + \psi)^{-1}\varphi$ by α and the expression $(\varphi + \psi)^{-1}\psi$ by β. If $\alpha = \varepsilon - \beta$, then $\alpha\beta = (\varepsilon - \beta)\beta = \beta - \beta^2 = \beta(\varepsilon - \beta) = \beta\alpha$. Therefore by Theorem 1.1 $(Q, \circ)$ is a medial quasigroup. Further we have $xx \cdot yz = x \cdot yz = xy \cdot xz$ and $xy \cdot zz = xy \cdot z = xz \cdot yz$.

(iii) We prove that the map s is an antiautomorphism of $(Q, \circ)$, i.e., $s(y \circ x) = s(x) \circ s(y)$. We have

$$s(y \circ x) = s(s^{-1}(y \cdot x)) = \varphi y + \psi x + g; \tag{6}$$

$$\begin{aligned} s(x) \circ s(y) &= (L_g(\varphi + \psi)x) \circ (L_g(\varphi + \psi)y) \\ &= (\varphi + \psi)^{-1}\varphi(L_g(\varphi + \psi)x) + (\varphi + \psi)^{-1}\psi(L_g(\varphi + \psi)y) \\ &= (\varphi + \psi)^{-1}\varphi(g + \varphi x + \psi x) + (\varphi + \psi)^{-1}\psi(g + \varphi y + \psi y) \\ &= (\varphi + \psi)^{-1}(\varphi g + \varphi^2 x + \varphi\psi x) + (\varphi + \psi)^{-1}(\psi g + \psi\varphi y + \psi^2 y) \\ &= (\varphi + \psi)^{-1}(\varphi g + \varphi^2 x + \varphi\psi x + \psi g + \psi\varphi y + \psi^2 y) \\ &\overset{(\varphi^2=\psi^2)}{=} (\varphi + \psi)^{-1}(\varphi g + \psi^2 x + \varphi\psi x + \psi g + \psi\varphi y + \varphi^2 y) \\ &= (\varphi + \psi)^{-1}((\varphi + \psi)g + (\varphi + \psi)\psi x + (\varphi + \psi)\varphi y) \\ &= (\varphi + \psi)^{-1}(\varphi + \psi)(\psi x + \varphi y + g) \\ &= \varphi y + \psi x + g. \end{aligned} \tag{7}$$

Since the right sides of equalities (6) and (7) are equal, we obtain that $s(y \circ x) = s(x) \circ s(y)$. □

Remark 2.1. For detailed information on the structure of medial paramedial quasigroups in which the map s is a permutation see [17, Lemma 22, Theorem 23].

Corollary 2.4. *The quasigroup* $(Q, \circ)$ *from Theorem* 2.3 *is paramedial if and only if* $\varphi(\varphi + \psi)^{-1}\varphi = \psi(\varphi + \psi)^{-1}\psi$.

PROOF: $(Q, \circ)$ is paramedial if and only if $(\varphi+\psi)^{-1}\varphi(\varphi+\psi)^{-1}\varphi = (\varphi+\psi)^{-1}\psi(\varphi+\psi)^{-1}\psi$. The last equality is equivalent with the following $(\varphi+\psi)(\varphi+\psi)^{-1}\varphi(\varphi+\psi)^{-1}\varphi = (\varphi+\psi)(\varphi+\psi)^{-1}\psi(\varphi+\psi)^{-1}\psi$, that is, $\varphi(\varphi+\psi)^{-1}\varphi = \psi(\varphi+\psi)^{-1}\psi$. □

2.2 Finite simple paramedial quasigroups. We recall that any antiautomorphism of a quasigroup defines a congruence (Lemma 1.2) which is normal in the finite case (Lemma 1.1).

Then a necessary condition for the simplicity of a finite paramedial quasigroup $(Q, \cdot)$ is that the antiendomorphism s is either a permutation of the set Q (i.e. an antiendomorphism with trivial kernel) or is a zero antiendomorphism.

This condition is not sufficient. For example, in any distributive quasigroup the map s is a permutation [29], [28], but it is easy to construct non-simple distributive quasigroups. Simple medial quasigroups are described in [15]. Finite simple T-quasigroups are researched in [23], [24].

A loop $(Q, +)$ satisfying the identity $(x+x)+(y+z) = (x+y)+(x+z)$ is called a commutative Moufang loop. It is clear that any abelian group is a commutative Moufang loop.

We recall some definitions [18]. Let $V(k, p)$ be a k-dimensional vector space over a field $GF(p)$. We denote by $\mathrm{GL}(k, p)$ the group of all invertible linear operators on $V(k, p)$, i.e., the automorphism group of the vector space $V(k, p)$.

Let G be a group. Any homomorphism $\Phi : G \longrightarrow \mathrm{GL}(k, p)$ is called a *linear representation of the group G in the vector space $V(k, p)$*. This representation of the group G is denoted by $(\Phi, V(k, p))$.

Let $(\Phi, V(k, p))$ be a linear representation of a group G. A subspace U of $V(k, p)$ is called an invariant subspace relative to G if $\Phi(g)u \in U$ for all $u \in U$ and all $g \in G$. The zero subspace and the entire space $V(k, p)$ are called trivial invariant subspaces.

A representation $(\Phi, V(k, p))$ of a group G that has only trivial invariant subspaces is called an *irreducible representation*.

We shall use the following theorem ([24], [23, Theorem 2]).

Theorem 2.4. *Let $(Q, \cdot)$ be a linear quasigroup of the form $x \cdot y = (\varphi x + \psi y) + a$, where $(Q, +)$ is n-generated commutative Moufang loop. Then the quasigroup $(Q, \cdot)$ is simple if and only if $(Q, +) \cong \bigoplus_{i=1}^{n} (Z_p)_i$ for some prime p; the group $\langle \varphi, \psi \rangle$ is an irreducible two-generated subgroup of the group $\mathrm{GL}(n, p)$.*

Theorem 2.5. *A finite paramedial quasigroup $(Q, \cdot)$ of the form $x \cdot y = \varphi x + \psi y + c$ over an abelian group $(Q, +)$ is simple if and only if*

1. *$(Q, +) \cong \bigoplus_{i=1}^{n} (Z_p)_i$;*
2. *the group $\langle \varphi, \psi \rangle$ is an irreducible subgroup of the group $\mathrm{GL}(n, p)$;*
3. *if $|Q| > 1$, the quasigroup $(Q, \cdot)$ lies in one of the following disjoint quasigroup classes:*
   - (a) *the map s is a zero antiendomorphism; in this case, $\psi = -\varphi$, $(Q, \cdot)$ is a medial unipotent quasigroup, and $(Q, \cdot)$ is isomorphic to a quasigroup $(Q, \circ)$ of the form $x \circ y = \varphi x - \varphi y$ over the group $(Q, +)$;*
   - (b) *the map s is the identity permutation; in this case, $c = 0$, $\varphi = \psi, \varphi + \varphi = \varepsilon$, $(Q, \cdot)$ is a paramedial medial commutative distributive quasigroup;*

(c) *the map s is a non-identity permutation;* $(Q, \circ)$, $x \circ y = (\varphi+\psi)^{-1}\varphi x + (\varphi+\psi)^{-1}\psi y$, *is an* $(\varphi+\psi)$*-simple medial distributive quasigroup,* $(\varphi+\psi) \in \mathrm{Aut}(Q, +)$.

Proof: $(\Rightarrow)$ Cases 1 and 2 follow from Theorem 2.4.

From Lemma 1.2 we have that if a paramedial quasigroup $(Q, \cdot)$ is simple, then in this case the map s is a permutation of the set Q, or it is a zero antiendomorphism.

Case 3(a) follows from Theorem 2.1.

Case 3(b) follows from Theorem 2.2.

Case 3(c) follows from Theorem 2.3.

$(\Leftarrow)$ Any quasigroup mentioned in Case 3 with the properties mentioned in Cases 1 and 2 is simple and paramedial. □

2.3 Direct decomposition of finite paramedial quasigroups. In this section we prove an analog of Murdoch's Theorem [20] on the structure of finite medial quasigroups. See also [26], [29]. Direct decompositions of some paramedial quasigroups and abelian groups, which are connected with these quasigroups, are studied in [17].

Definition 2.1. If $(Q_1, \cdot)$, $(Q_2, \circ)$ are quasigroups, then their (*external*) *direct product* $(Q, *) = (Q_1, \cdot) \times (Q_2, \circ)$ is the set of all ordered pairs (a', a'') where $a' \in Q_1$, $a'' \in Q_2$, and where the operation in $(Q, *)$ is defined component-wise, that is, $(a_1 * a_2) = (a'_1 \cdot a'_2, a''_1 \circ a''_2)$.

Direct products of quasigroups are studied in many articles and books, see, for example, [11], [30], [21], [14], [5], [7]. The concept of direct product of quasigroups was used already in [20]. In the group case it is possible to find these definitions, for example, in [13].

In [10], [30], [31], there is a definition of the (internal) direct product of Ω-algebras. We recall that any quasigroup is an Ω-algebra.

Definition 2.2. If U and W are congruences on the algebra A which commute and for which $U \cap W = \hat{A} = \{(a, a) | \forall\, a \in A\}$, then the join $U \circ W = U \vee W$ of U and W is called the *direct product* $U \sqcap W$ of U and W [30], [31].

The following theorem establishes the connection between concepts of internal and external direct product of Ω-algebras.

Theorem 2.6. *An Ω-algebra A is isomorphic to a direct product of Ω-algebras B and C with isomorphism φ, i.e. $\varphi : A \to B \times C$, if and only if there exist such congruences U and W of A that $A^2 = U \sqcap W$* ([30, p. 16], [31]).

Lemma 2.3. *If a paramedial quasigroup Q is isomorphic to the direct product of quasigroups A and B, then the quasigroups A and B also are paramedial quasigroup.*

Proof: If we suppose that A or B is not paramedial, then Q is paramedial neither. □

We need the following well known fact.

Lemma 2.4. *Normal quasigroup congruences commute in pairs* [19], [30], [10], [29].

Define in a finite paramedial quasigroup $(Q, \cdot)$ the following chain

$$Q \supset s^1(Q) \supset s^2(Q) \supset \dots \supset s^m(Q) \supset \dots \tag{8}$$

The chain (8) becomes *stable* if there exists a natural number m such that $s^m(Q) = s^{m+1}(Q) = s^{m+2}(Q) \dots$. In this case we shall say that the antiendomorphism s has the order m.

Taking into consideration Corollary 1.1 we can say that such a chain exists in any paramedial quasigroup. It is clear that the chain (8) becomes stable in any finite paramedial quasigroup.

Theorem 2.7. *Any finite paramedial quasigroup $(Q, \cdot)$ has the following structure*

$$(Q, \cdot) \cong (A, \circ) \times (B, \cdot),$$

where $(A, \circ)$ is a quasigroup with a unique idempotent element; $(B, \cdot)$ is isotope of a distributive medial quasigroup $(B, \star)$, $x \cdot y = s(x \star y)$, $x \star y = \varphi x + \psi y$, $s = L_a^+ \alpha$, $a \in B$, $\alpha \in \mathrm{Aut}(B, +)$, $\varphi \alpha \varphi = \psi \alpha \psi$.

Proof: The proof of this theorem mainly repeats the proof of Theorem 6 from [26].

If the map s is a permutation of Q, then by Theorem 2.3, $(Q, \cdot)$ is an isotope of a distributive quasigroup.

If $s(Q) = k$, where k is a fixed element of the set Q, then $(Q, \cdot)$ is a unipotent quasigroup, $(Q, \cdot) \cong (Q, \circ)$, where $x \circ y = \varphi x - \varphi y$, $(Q, +)$ is an abelian group, $\varphi \in \mathrm{Aut}(Q, +)$ (Theorem 2.1).

We suppose that $s^m = s^{m+1}$, where $m \geq 1$. From Corollary 1.1 it follows that $s^m(Q, \cdot) = (B, \cdot)$ is a subquasigroup of $(Q, \cdot)$. It is clear that $(B, \cdot)$ is a paramedial quasigroup in which the map $\overline{s} = s|_{s^m(Q)}$ is a permutation of $B \subset Q$. In other words, $s(B) = B$.

Define a binary relation δ on $(Q, \cdot)$ by the following rule: $x \delta y$ if and only if $s^m(x) = s^m(y)$.

By Lemma 1.2 (if s^m is an antiendomorphism) or by Theorem 1.4 (if s^m is an endomorphism), the relation δ is a congruence of $(Q, \cdot)$. By Lemma 1.1, δ is a normal congruence.

It is known that any subquasigroup of a T-quasigroup is normal ([17, Theorem 43]). Thus the subquasigroup $(B, \cdot)$ of $(Q, \cdot)$ is normal. By Remark 1.2, this subquasigroup defines exactly one normal congruence. Denote this congruence by the letter ρ.

It is known ([3, pp. 56–57], [4], [22]) that any coset $\rho(a)$ of a normal congruence ρ of a quasigroup $(Q, \cdot)$ can be presented in the form $a \cdot B$, where B is a normal subquasigroup of $(Q, \cdot)$ and $B = \rho(b)$ for some $b \in Q$. Indeed, we can take into consideration the following equalities $a \cdot \rho(b) = \rho(a \cdot b) = \rho(a) \cdot b$ that are true for any normal congruence ρ of a quasigroup $(Q, \cdot)$.

Taking into consideration Remark 1.2, we can say that any normal subquasigroup B of a quasigroup Q defines in a unique way a normal congruence ρ by the rule: $x\rho y$ if and only if $B \cdot x = B \cdot y$, i.e. for any $b_1 \in B$ there exists exactly one element $b_2 \in B$ such that $b_1 \cdot x = b_2 \cdot y$ and vice versa, for any $b_2 \in B$ there exists exactly one element $b_1 \in B$ such that $b_1 \cdot x = b_2 \cdot y$.

We prove that $\delta \cap \rho = \hat{Q} = \{(x, x) | \forall x \in Q\}$. From the reflexivity of δ and ρ, we have that $\delta \cap \rho \supseteq \hat{Q}$. On the other hand, let $(x, y) \in \delta \cap \rho$, i.e. let $x\delta y$ and $x\rho y$ where $x, y \in Q$. Using the definitions of δ, ρ we have $s^m(x) = s^m(y)$ and $(B, \cdot) \cdot x = (B, \cdot) \cdot y$. Then there exist $a, b \in B$ such that $a \cdot x = b \cdot y$. Applying to both sides of last equality the map s^m we obtain $s^m(a) \cdot s^m(x) = s^m(b) \cdot s^m(y)$, $s^m(a) = s^m(b)$, $a = b$, since the map $s^m|_B$ is a permutation of the set B. If $a = b$, then from $a \cdot x = b \cdot y$ we obtain $x = y$.

From Definition 2.2, it follows that in order to prove the existence of the congruence direct decomposition of $(Q, \cdot)$, we should prove that $\delta \circ \rho = Q \times Q$.

Let a, c be fixed elements of Q. We will have proven the equality if we can shown that there exists $y \in Q$ such that $a\delta y$ and $y\rho c$. Now, from the definition of δ we have that condition $a\delta y$ is equivalent to equality $s^m(a) = s^m(y)$. From the definition of congruence ρ it follows that condition $y\rho c$ is equivalent to the following condition: $y \in \rho(c) = B \cdot c$. Thus we will have proven the equality $\delta \circ \rho = Q \times Q$ if we demonstrate that there exists $y \in B \cdot c$ such that $s^m(a) = s^m(y)$. Such an element y exists since $s^m(B \cdot c) = s^m(B) \cdot s^m(c) = B = s^m(Q)$, if the map s^m is an endomorphism of $(Q, \cdot)$, while if s^m is an antiendomorphism of $(Q, \cdot)$, then $s^m(B \cdot c) = s^m(c) \cdot s^m(B) = B = s^m(Q)$.

Therefore $\rho \circ \delta = Q \times Q = \delta \circ \rho$, $\delta \cap \rho = \hat{Q}$ and we can use Theorem 2.6. Now we can say that $(Q, \cdot)$ is isomorphic to the direct product of $(Q, \cdot)/\delta \cong (B, \cdot)$ (Theorem 1.4) and $(Q, \cdot)/\rho \cong (A, \circ)$ [9].

The paramedial identity holds in $(B, \cdot)$ since $(B, \cdot) \subseteq (Q, \cdot)$. If the quasigroups $(Q, \cdot)$ and $(B, \cdot)$ are paramedial quasigroups, $(Q, \cdot) \cong (A, \circ) \times (B, \cdot)$, then $(A, \circ)$ is a paramedial quasigroup as well (Lemma 2.3).

Now we prove that the quasigroup $(A, \circ) \cong (Q, \cdot)/(B, \cdot)$, where $s^m(Q, \cdot) = (B, \cdot)$, has a unique idempotent element.

We can identify elements of $(Q, \cdot)/(B, \cdot)$ with cosets of the form $B \cdot c$, where $c \in Q$. From properties of $(A, \circ)$, we have that $s^m(A) = a$, where the element a is a fixed element of A that corresponds to the coset class B.

Further, taking into consideration the properties of endomorphism s of the quasigroup $(A, \circ)$, we obtain $s^{m+1}A = s(s^m A) = s(a) = a$. Therefore $s(a) = a$, i.e. the element a is an idempotent element of $(A, \circ)$. To prove the uniqueness of the idempotent element, suppose there exists $c \in A$ such that $c \circ c = c$, i.e. such that $s(c) = c$. Then $s^m(c) = c = a$, since $s^m(A) = a$.

The fact that $(B, \cdot)$ is an isotope of a distributive quasigroup $(B, \star)$ follows from Theorem 2.3. $\square$

Taking into consideration Theorem 2.7 we can formulate an analog of Theorem 1.3 for finite paramedial quasigroups.

Theorem 2.8. *Any finite paramedial quasigroup $(Q,\cdot)$ is isomorphic to the direct product of a paramedial unipotently-solvable quasigroup $(Q_1,\circ)$ with a unique idempotent element and a quasigroup $(Q_2,*)$, where $(Q_2,*)$ is an isotope of the form $(\varepsilon,\varepsilon,\gamma)$ of a medial distributive quasigroup $(Q_2,\star)$, $x*y=\gamma(x\star y)$, $x\star y=\varphi x+\psi y$, $(Q_2,+)$ is the abelian group corresponding to $(Q_2,\star)$, $\gamma=L_a^+\alpha$, $a\in Q_2$, $\alpha\in \operatorname{Aut}(Q_2,+)$, $\varphi\alpha\varphi=\psi\alpha\psi$.*

2.4 Paramedial quasigroups of order 4. We shall use the following

Remark 2.2. If a map f of a quasigroup $(Q,\cdot)$ has the form $L_a\xi$, where ξ is an antiendomorphism of $(Q,\cdot)$, then $\xi L_a x=\xi(a\cdot x)=\xi x\cdot\xi a=R_{\xi a}\xi x$. Thus $f^2=L_aR_{\xi a}\xi^2$ and so on. Therefore, f^k is a zero map if and only if ξ^k is a zero map.

There are two abelian groups of order 4: the additive group Z_4 of residues modulo 4 and the elementary abelian 2-group $Z_2\oplus Z_2$.

Let $Z_4=\{0,1,2,3\}$. Then $\operatorname{Aut} Z_4=\{\varepsilon,I\}$, where $I=(13)$. Notice that the automorphism I is often denoted by the sign "–".

The following triplets define paramedial quasigroups of order 4 over the group Z_4:

1) Case $\varphi=\psi$. We have such triplets $(\varepsilon,\varepsilon,\overline{0,3})$, $(I,I,\overline{0,3})$. Here the expression $\overline{0,3}$ denotes the set of integers $\{0,1,2,3\}$.

It is clear that any triplet from the first series defines the group Z_4.

Any quasigroup from the second series is a medial paramedial quasigroup in which the antiendomorphism s has the form $L_i^+\xi$, where $i\in\{0,1,2,3\}$, the map ξ is multiplication of any quasigroup element x element by the number $-2\equiv 2 \pmod 4$.

Using Remark 2.2 we obtain that any quasigroup from the second series is a unipotently-solvable quasigroup of degree 2.

2) Case $\varphi^2=\psi^2$ and $\varphi\neq\psi$. We have the following subcases: $(\varepsilon,I,\overline{0,3})$, $(I,\varepsilon,\overline{0,3})$. Any quasigroup from the last triplets has zero antiendomorphism s since $I\equiv -$. Therefore in this case we can use Corollary 2.3.

We denote elements of the group $Z_2\oplus Z_2$ as follows: $\{(0;0),(1;0),(0;1),(1;1)\}$. Then $\operatorname{Aut}(Z_2\oplus Z_2)$ has the form

$$\operatorname{Aut}(Z_2\oplus Z_2)=\left\{\begin{pmatrix}1&0\\0&1\end{pmatrix},\begin{pmatrix}1&0\\1&1\end{pmatrix},\begin{pmatrix}1&1\\0&1\end{pmatrix},\begin{pmatrix}0&1\\1&0\end{pmatrix},\begin{pmatrix}1&1\\1&0\end{pmatrix},\begin{pmatrix}0&1\\1&1\end{pmatrix}\right\}.$$

Denote automorphisms φ_i as follows $\varepsilon=\left(\begin{smallmatrix}1&0\\0&1\end{smallmatrix}\right)$, $\varphi_2=\left(\begin{smallmatrix}1&0\\1&1\end{smallmatrix}\right)$, $\varphi_3=\left(\begin{smallmatrix}1&1\\0&1\end{smallmatrix}\right)$, $\varphi_4=\left(\begin{smallmatrix}0&1\\1&0\end{smallmatrix}\right)$, $\varphi_5=\left(\begin{smallmatrix}1&1\\1&0\end{smallmatrix}\right)$, $\varphi_6=\left(\begin{smallmatrix}0&1\\1&1\end{smallmatrix}\right)$.

It is known that $\operatorname{Aut}(Z_2\oplus Z_2)\cong S_3$ [12], [16].

1) Case $\varphi=\psi$ is obvious and we omit it.

2) Case $\varphi^2=\psi^2$ and $\varphi\neq\psi$.

We notice $\varepsilon^2 = \varphi_2^2 = \varphi_3^2 = \varphi_4^2 = \varepsilon, \varphi_5^2 = \varphi_6, \varphi_6^2 = \varphi_5$. Then the condition $\varphi^2 = \psi^2$ and $\varphi \neq \psi$ is fulfilled for the following automorphisms: $\varepsilon, \varphi_2, \varphi_3$ and φ_4.

The following triplets define paramedial quasigroups of order 4 with the property $\varphi \neq \psi$ over the group $Z_2 \oplus Z_2$:

$(\varepsilon, \varphi_2, \overline{0,3}), (\varphi_2, \varepsilon, \overline{0,3})$, $(\varepsilon, \varphi_3, \overline{0,3})$, $(\varphi_3, \varepsilon, \overline{0,3})$, $(\varepsilon, \varphi_4, \overline{0,3})$, $(\varphi_4, \varepsilon, \overline{0,3})$,
$(\varphi_2, \varphi_3, \overline{0,3})$, $(\varphi_2, \varphi_4, \overline{0,3})$, $(\varphi_4, \varphi_2, \overline{0,3})$, $(\varphi_3, \varphi_2, \overline{0,3})$, $(\varphi_3, \varphi_4, \overline{0,3})$, $(\varphi_4, \varphi_3, \overline{0,3})$.

Any quasigroup from the first row is a medial paramedial quasigroup. Each of these quasigroups is unipotently-solvable quasigroup of degree 2.

Quasigroups from the second row are simple paramedial quasigroups since any pair of elements of the set $\{\varphi_2, \varphi_3, \varphi_4\}$ generates the group $\mathrm{Aut}(Z_2 \oplus Z_2) \cong S_3$ [12], [16].

Moreover all these quasigroups are not medial, since automorphisms $\varphi_2, \varphi_3, \varphi_4$ are not permutable in pairs relative to the operation of multiplication. Therefore all these quasigroups are from Case 3(c) of Theorem 2.5.

Acknowledgment. The authors thank Consiliul Suprem pentru Ştiinţă şi Dezvoltare Tehnologică al Republicii Moldova (grant 08.820.08.08 RF) for financial support. V. Shcherbacov also thanks the organizers of the 2nd Mile High Conference on Nonassociative Mathematics for financial support.

References

[1] Bates G.E., Kiokemeister F., *A note on homomorphic mappings of quasigroups into multiplicative systems*, Bull. Amer. Math. Soc. **54** (1948), 1180–1185.

[2] Belousov V.D., *Balanced identities on quasigroups*, Mat. Sb. **70** (1966), 55–97 (in Russian).

[3] Belousov V.D., *Foundations of the Theory of Quasigroups and Loops*, Nauka, Moscow, 1967 (in Russian).

[4] Belousov V.D., *Elements of Quasigroup Theory: A Special Course*, Kishinev State University Printing House, Kishinev, 1981 (in Russian).

[5] Belyavskaya G.B., *Direct decompositions of quasigroups*, Mat. Issled. **95** (1987), 23–38 (in Russian).

[6] Belyavskaya G.B., *T-quasigroups and the center of a quasigroup*, Mat. Issled. **111** (1989), 24–43 (in Russian).

[7] Belyavskaya G.B., *Full direct decompositions of quasigroups with an idempotent element*, Mat. Issled. **113** (1990), 21–36 (in Russian).

[8] Belyavskaya G.B., Tabarov A.Kh., *One-sided T-quasigroups and irreducible balanced identities*, Quasigroups Related Systems **1** (1994), 8–21.

[9] Bruck R.H., *A Survey of Binary Systems*, third printing, corrected edition, Springer, New York, 1971.

[10] Burris S., Sankappanavar H.P., *A Course in Universal Algebra*, Springer, New York-Berlin, 1981.

[11] Cohn P.M., *Universal Algebra*, Harper & Row, New York, 1965.

[12] Hall M., *The Theory of Groups*, The Macmillan Co., New York, 1959.

[13] Herstein I.N., *Abstract Algebra*, second edition, Macmillan Publishing Company, New York, 1990.

[14] Ježek J., *Normal subsets of quasigroups*, Comment. Math. Univ. Carolin. **16** (1975), no. 1, 77–85.

[15] Ježek J., Kepka T., *Varieties of abelian quasigroups*, Czechoslovak Math. J. **27** (1977), 473–503.

[16] Kargapolov M.I., Merzlyakov M.Yu., *Foundations of Group Theory*, Nauka, Moscow, 1977 (in Russian).
[17] Kepka T., Němec P., *T-quasigroups, II*, Acta Univ. Carolin. Math. Phys. **12** (1971), no. 2, 31–49.
[18] Kostrikin A.I., *Introduction in Algebra*, Nauka, Moscow, 1977 (in Russian).
[19] Mal'tsev A.I., *On the general theory of algebraic systems*, Mat. Sb. **35** (77) (1954), no. 1, 3–20 (in Russian).
[20] Murdoch D.C., *Structure of abelian quasigroups*, Trans. Amer. Math. Soc. **49** (1941), 392–409.
[21] Němec P., Kepka T., *T-quasigroups, I*, Acta Univ. Carolin. Math. Phys. **12** (1971), no. 1, 39–49.
[22] Pflugfelder H.O., *Quasigroups and Loops: Introduction*, Heldermann, Berlin, 1990.
[23] Shcherbacov V.A., *On automorphism groups and congruences of quasigroups*, PhD Thesis, Institute of Mathematics, Academy of Sciences of Republic Moldova, 1991 (in Russian).
[24] Shcherbacov V.A., *On linear quasigroups and their automorphism groups*, Mat. Issled. **120** (1991), 104–113 (in Russian).
[25] Shcherbacov V.A., *On Bruck-Belousov problem*, Bul. Acad. Stiinte Repub. Mold. Mat. 2005, no. 3, 123–140.
[26] Shcherbacov V.A., *On structure of finite n-ary medial quasigroups and automorphism groups of these quasigroups*, Quasigroups Related Systems **13** (2005), no. 1, 125–156.
[27] Shcherbacov V.A., *On the structure of finite medial quasigroups*, Bul. Acad. Stiinte Repub. Mold. Mat. 2005, no. 1, 11–18.
[28] Shcherbacov V.A., *On the structure of left and right F-, SM- and E-quasigroups*, `http://arxiv.org/`, arXiv:0811.1725:67 pages, 2008.
[29] Shcherbacov V.A., *On the structure of left and right F-, SM- and E-quasigroups*, J. Gen. Lie Theory Appl. **3** (2009), no. 3, 197–259.
[30] Smith J.D.H., *Mal'cev Varieties*, Lecture Notes in Mathematics, 554, Springer, New York, 1976.
[31] Smith J.D.H., *An Introduction to Quasigroups and Their Representation*, Studies in Advanced Mathematics, Chapman and Hall/CRC, London, 2007.
[32] Syrbu P.N., *On congruences on n-ary T-quasigroups*, Quasigroups Related Systems **6** (1999), 71–80.
[33] Toyoda K., *On axioms of linear functions*, Proc. Imp. Acad. Tokyo **17** (1941), 221–227.
[34] Wikipedia. Problems in loop theory and quasigroup theory, 2004, `http://en.wikipedia.org/wiki`.

Institute of Mathematics and Computer Science, Academy of Sciences of Moldova, 5 Academiei str., Chişinău MD–2028, Moldova

E-mail: scerb@math.md
dmitry.pushkashu@gmail.com

(*Received* September 28, 2009, *revised* February 8, 2010)