BULETINUL ACADEMIEI DE ŞTIINŢE
A REPUBLICII MOLDOVA. MATEMATICA
Number 2(81), 2016, Pages 143–154
ISSN 1024–7696

On spectrum of medial T_2-quasigroups

A. V. Scerbacova, V. A. Shcherbacov

Abstract. There exist medial T_2-quasigroups of any order of the form

$$2^{k_1}3^{k_2}5^{k_3}11^{k_4}17^{k_5}23^{k_6}53^{k_7}59^{k_8}83^{k_9}101^{k_{10}}p_1^{\alpha_1}p_2^{\alpha_2}\dots p_m^{\alpha_m},$$

where $k_1 \geq 2$, $k_2, \dots, k_{10} \geq 1$, p_i are prime numbers of the form $6t+1$, $\alpha_i \in \mathbb{N}$, $i \in \{1, \dots, m\}$. Some other results on T_2-quasigroups are given.

Mathematics subject classification: 20N05, 05B15.
Keywords and phrases: Quasigroup, medial, spectrum, T_2-quasigroup, parastrophe, orthogonal quasigroups.

1 Introduction

Definitions and elementary properties of quasigroups can be found in [1, 2, 18]. Most of presented here results are given in [20]. Quasigroups have some applications in cryptology [24]. The most usable in cryptology quasigroup property is the property of orthogonality of quasigroups [9].

V. D. Belousov [3, 4] (see also [10]) by the study of orthogonality of quasigroup parastrophes proved that there exist exactly seven parastrophically non-equivalent identities which guarantee that a quasigroup is orthogonal to at least one its parastrophe: s

$$x(x \cdot xy) = y \qquad (C_3\text{ law}) \qquad (1)$$
$$x(y \cdot yx) = y \qquad \text{of type } T_2\ [3] \qquad (2)$$
$$x \cdot xy = yx \qquad \text{(Stein's 1st law)} \qquad (3)$$
$$xy \cdot x = y \cdot xy \qquad \text{(Stein's 2nd law)} \qquad (4)$$
$$xy \cdot yx = y \qquad \text{(Stein's 3rd law)} \qquad (5)$$
$$xy \cdot y = x \cdot xy \qquad \text{(Schroder's 1st law)} \qquad (6)$$
$$yx \cdot xy = y \qquad \text{(Schroder's 2nd law).} \qquad (7)$$

The names of identities (3)–(7) originate from Sade's paper [19]. We follow [6] in the name of identity (1).

All these identities can be obtained in a unified way using criteria of orthogonality and quasigroup translations [15]. For example, identity (2), which guarantees orthogonality of a quasigroup $(Q,\cdot)$ and its $(2\,3)$-parastrophe, can be obtained from the following translation identity

$$L_y^2 x = P_y x. \tag{8}$$

Using table of translations of quasigroup parastrophes [23] we can rewrite identity (8) in the following parastrophically equivalent [4] forms:

$$\begin{aligned} &R_y^2 x = P_y^{-1} x,\\ &P_y^{-2} x = L_y^{-1} x,\\ &L_y^{-2} x = R_y x,\\ &R_y^{-2} x = L_y x,\\ &P_y^2 x = R_y^{-1} x. \end{aligned} \tag{9}$$

Passing to "standard" identities we obtain from the identities (9) the following identities that are parastrophically equivalent to the identity (2):

$$\begin{aligned} &(xy\cdot y)x = y,\\ &(y\backslash x)(y/x) = y,\\ &y(y\cdot xy) = x,\\ &(yx\cdot y)y = x,\\ &x(y/(x/y)) = y. \end{aligned} \tag{10}$$

A quasigroup $(Q,\cdot)$ with the identity $x\cdot x = x$ is called idempotent. The set $\mathfrak{Q}$ of natural numbers for which there exist quasigroups with a property T, for example, the property of idempotency, is called the spectrum of the property T in the class of quasigroups. Often the following phrase is used: spectrum of quasigroups with a property T. Therefore we can say that spectra of quasigroups with identities (3)–(7) were studied in [5, 6, 8, 12, 17, 25].

It is clear that the identity (2) and any from identities (10) have the same spectrum because order of any parastroph of a quasigroup $(Q,\cdot)$ is equal to the order of quasigroup $(Q,\cdot)$.

Idempotent models of the identity $(yx\cdot y)y = x$ can be associated with a class of resolvable Mendelsohn designs [5]. In [5] "it is shown that the spectrum of $(yx\cdot y)y = x$ contains all integers $n \geq 1$ with the exception of $n = 2, 6$ and the possible exception of $n \in \{10, 14, 18, 26, 30, 38, 42, 158\}$. It is also shown that idempotent models of $(yx\cdot y)y = x$ exist for all orders $n > 174$".

Here we study in the main the spectrum of medial T_2-quasigroups. Such quasigroups can be easy constructed and they can be used in cryptology.

2 Medial T_2-quasigroups

The problem of the study of T_2-quasigroups is posed in [3,4]. In [26] the following proposition (Proposition 7) is proved. We formulate this proposition in a slightly changed form.

Theorem 1. *If a T_2-quasigroup $(Q,\cdot)$ is isotopic to an abelian group $(Q,\oplus)$, then for every element $b \in Q$ there exists an isomorphic copy $(Q,+) \cong (Q,\oplus)$ such that $x \cdot y = IL_b^3(x) + L_b(y) + b$, for all $x, y \in Q$, where $x + Ix = 0$ for all $x \in Q$.*

Definition 1. A quasigroup $(Q,\cdot)$ of the form $x \cdot y = \varphi x + \psi y + b$, where $(Q,+)$ is an abelian group, φ, ψ are automorphisms of the group $(Q,+)$, b is a fixed element of the set Q is called T-quasigroup. If, additionally, $\varphi\psi = \psi\varphi$, then $(Q,\cdot)$ is called medial quasigroup [1,2,16,18].

Theorem 2. *A T-quasigroup $(Q,\cdot)$ of the form*

$$x \cdot y = \varphi x + \psi y + b \tag{11}$$

satisfies T_2-identity if and only if $\varphi = I\psi^3$, $\psi^5+\psi^4+1 = (\psi^2+\psi+1)(\psi^3-\psi+1) = 0$, where 1 is identity automorphism of the group $(Q,+)$ and 0 is zero endomorphism of this group, $\psi^2 b + \psi b + b = 0$.

Proof. We rewrite T_2-identity using the right part of the form (11) as follows:

$$\varphi x + \psi(\varphi y + \psi(\varphi y + \psi x + b) + b) + b = y \tag{12}$$

or, taking into consideration that $(Q,+)$ is an abelian group, φ, ψ are its automorphisms, after simplification of equality (12) we have

$$\varphi x + \psi\varphi y + \psi^2\varphi y + \psi^3 x + \psi^2 b + \psi b + b = y. \tag{13}$$

If we put in the equality (13) $x = y = 0$, then we obtain

$$\psi^2 b + \psi b + b = 0, \tag{14}$$

where 0 is the identity (neutral) element of the group $(Q,+)$.

Therefore we can rewrite equality (13) in the following form

$$\varphi x + \psi\varphi y + \psi^2\varphi y + \psi^3 x = y. \tag{15}$$

If we put in the equality (15) $y = 0$, then we obtain that $\varphi x + \psi^3 x = 0$. Therefore $\varphi = I\psi^3$, where, as above, $x + Ix = 0$ for all $x \in Q$.

Notice in any abelian group $(Q,+)$ the map I is an automorphism of this group. Really, $I(x+y) = Iy + Ix = Ix + Iy$.

Moreover, $I\alpha = \alpha I$ for any automorphism of the group $(Q,+)$. Indeed, $\alpha x + I\alpha x = 0$. On the other hand $\alpha x + \alpha Ix = \alpha(x + Ix) = \alpha 0 = 0$. Comparing the left sides we have $\alpha x + I\alpha x = \alpha x + \alpha Ix$, $I\alpha x = \alpha Ix$, $\alpha I = I\alpha$.

It is well known that $I^2 = \varepsilon$, i.e., $-(-x) = x$. Indeed, from the equality $x + Ix = 0$ using commutativity we have $Ix + x = 0$. On the other hand $I(x + Ix) = 0$, $Ix + I^2x = 0$. Then $Ix + x = Ix + I^2x$, $x = I^2x$ for all $x \in Q$.

If we put in the equality (15) $x = 0$, then we obtain that

$$\psi\varphi y + \psi^2\varphi y = y. \tag{16}$$

If we substitute in the equality (16) the expression $I\psi^3$ for φ, then we have $I\psi^5 y + I\psi^4 y = y$, $\psi^5 y + \psi^4 y = Iy$, $\psi^5 y + \psi^4 y + y = 0$. The last condition can be written in the form $\psi^5 + \psi^4 + 1 = 0$, where 1 is identity automorphism of the group $(Q, +)$ and 0 is zero endomorphism of this group.

It is easy to check that $\psi^5 + \psi^4 + 1 = (\psi^2 + \psi + 1)(\psi^3 - \psi + 1)$.

Converse. If we take into consideration that $\psi^2 b + \psi b + b = 0$, then from equality (13) we obtain equality (15). If we substitute in equality (15) the following equality $\varphi = I\psi^3$, then we obtain $\psi I\psi^3 y + \psi^2 I\psi^3 y = y$, $\psi^4 Iy + \psi^5 Iy = y$ which is equivalent to the equality $\psi^5 y + \psi^4 y + y = 0$. Therefore T-quasigroup $(Q, \cdot)$ is T_2-quasigroup. □

Remark 1. Proposition 6 in [8] states almost the same as Theorem 2.

Corollary 1. *Any T_2-T-quasigroup is medial.*

Proof. The proof follows from the equality $\varphi = I\psi^3$ (see Theorem 2). □

Corollary 2. *A T-quasigroup $(Q, \cdot)$ of the form $x \cdot y = \varphi x + \psi y$ satisfies T_2-identity if and only if $\varphi = I\psi^3$, $\psi^5 + \psi^4 + 1 = 0$.*

Proof. It is easy to see. □

Corollary 3. *A T-quasigroup $(Q, \cdot)$ of the form $x \cdot y = \varphi x + \psi y + b$ satisfies T_2-identity if $\varphi = I\psi^3$, $\psi^2 + \psi + 1 = 0$.*

Proof. The proof follows from Theorem 2 and the following fact: if $\psi^2 + \psi + 1 = 0$, then $\psi^5 + \psi^4 + 1 = 0$. In this case the following equality $\psi^2 b + \psi b + b = 0$ is also true. □

Corollary 4. *A T-quasigroup $(Q, \cdot)$ of the form $x \cdot y = \varphi x + \psi y + b$ satisfies T_2-identity if $\varphi = I\psi^3$, $\psi^3 - \psi + 1 = 0$, $\psi^2 b + \psi b + b = 0$.*

Proof. The proof follows from Theorem 2 and the following fact: if $\psi^3 - \psi + 1 = 0$, then $\psi^5 + \psi^4 + 1 = 0$. □

Lemma 1. *Any T-quasigroup of the form $x \cdot y = \varphi x + \psi y + b$ is idempotent if and only if $\varphi + \psi = \varepsilon$, $b = 0$.*

Proof. It is easy to see. See also [16]. □

Corollary 5. *Any T_2-T-quasigroup of the form $x \cdot y = \varphi x + \psi y + b$ is idempotent if and only if $\varphi = I\psi^3$, $\psi^3 - \psi + 1 = 0$, $b = 0$.*

Proof. We can use Theorem 2 and Lemma 1. Indeed, from the equality $I\psi^3 = \varepsilon - \psi$ we have that $\psi^3 = I + \psi$, $\psi^3 - \psi + 1 = 0$. □

Example 1. The following T_2-quasigroup is non-medial and therefore it is not a T-quasigroup (see Corollary 1). It is clear that this quasigroup is not idempotent.

$*$	0	1	2	3	4	5	6	7	8
0	0	1	3	4	2	5	6	7	8
1	2	0	1	6	7	3	5	8	4
2	1	4	5	8	0	6	2	3	7
3	7	3	0	5	8	1	4	2	6
4	6	2	8	0	5	7	3	4	1
5	8	7	2	3	4	0	1	6	5
6	4	8	7	1	6	2	0	5	3
7	3	5	6	7	1	4	8	0	2
8	5	6	4	2	3	8	7	1	0

3 T_2-quasigroups from the rings of residues

We use rings of residues modulo n, say $(R, +, \cdot, 1)$, and Theorem 2 to construct T_2-quasigroups. Here $(R, +)$ is cyclic group of order n, i.e., it is the group $(Z_n, +)$ with the generator element 1. It is clear that in many cases the element 1 is not a unique generator element, $(R, \cdot)$ is a commutative semigroup [13].

Multiplication of an element $b \in R$ by all elements of the group $(R, +)$ induces an endomorphism of the group $(R, +)$, i.e., $b \cdot (x + y) = b \cdot x + b \cdot y$. If $g.c.d.(b, n) = 1$, then the element b induces an automorphism of the group $(R, +)$ and it is called an invertible element of the ring $(R, +, \cdot, 1)$.

Next theorem is a specification of Theorem 2 on medial T_2-quasigroups defined using rings of residues modulo n. We denote by the symbol $\mathbb{Z}$ the set of integers, we denote by $|n|$ module of the number n.

Theorem 3. *Let $(Z_r, +, \cdot, 1)$ be a ring of residues modulo r such that $f(k) = (k^5 + k^4 + 1) \equiv 0 \pmod r$ for some $k \in \mathbb{Z}$. If $g.c.d.(|k|, r) = 1$, $k^2 \cdot b + k \cdot b + b \equiv 0 \pmod r$ for some $b \in Z_r$, then there exists T_2-quasigroup $(Z_r, \circ)$ of the form $x \circ y = -k^3 \cdot x + k \cdot y + b$ and of order r.*

Proof. We can use Theorem 2. The fact that $g.c.d.(|k|, r) = 1$ guarantees that the multiplication by the number k induces an automorphism of the group $(Z_r, +)$. In this case the map $-k^3$ is also a permutation as a product of permutations. □

Example 2. Let $k = -3$. Then $f(-3) = (-3)^5 + (-3)^4 + 1 = -161 = -(7) \cdot (23)$. Therefore $-161 \equiv 0 \pmod 7$ and $-161 \equiv 0 \pmod{23}$ and we have theoretical possibility to construct T_2 quasigroups of order $7, 23, 161$.

Case 1. Let $r = 7$. Then $k = -3 = 4 \pmod 7$. In this case $-(k^3) = -(-3)^3 = 27 = 6 \pmod 7$. It is clear that the elements 6 and 4 are invertible elements of the ring $(Z_7, +, \cdot, 1)$. Therefore the quasigroup $(Z_7, *)$ with the form $x * y = 6 \cdot x + 4 \cdot y$ is T_2-quasigroup of order 7.

Check. We have $6x+4(6y+4(6y+4x))=y$, $70x+24y+96y=y$, $y=y$, since $70\equiv 0 \pmod 7, 120\equiv 1 \pmod 7$.

In order to construct T_2-quasigroups over the ring $(Z_7,+,\cdot,1)$ with non-zero element b we must solve congruence $(-3)^2\cdot b+(-3)\cdot b+b\equiv 0 \pmod 7$. We have $7\cdot b\equiv 0 \pmod 7$. The last equation is true for any possible value of the element b. Therefore the following quasigroups are T_2-quasigroups of order 7: $x\circ y=6\cdot x+4\cdot y+i$, for any $i\in\{1,2,\dots,5,6\}$.

Case 2. Let $r=23$. Then $k=-3=20 \pmod{23}$. In this case $-(k^3)=-(-3)^3=27=4 \pmod{23}$. It is clear that the elements 20 and 4 are invertible elements of the ring $(Z_{23},+,\cdot,1)$. Therefore quasigroup $(Z_{23},*)$ with the form $x*y=4\cdot x+20\cdot y$ is T_2-quasigroup of order 23.

Check. We have $4x+20(4y+20(4y+20x))=y$, $4x+80y+1600y+8000x=y$, $y=y$, since $8004\equiv 0 \pmod{23}, 1680\equiv 1 \pmod{23}$. This quasigroup is idempotent. Indeed, $4+20=24\equiv 1 \bmod 23$.

In order to construct T_2-quasigroups over the ring $(Z_{23},+,\cdot,1)$ with non-zero element b we must solve congruence $(-3)^2\cdot b+(-3)\cdot b+b\equiv 0 \pmod{23}$. We have $7\cdot b\equiv 0 \pmod{23}$. This congruence modulo has unique solution $b\equiv 0 \bmod 23$, since $g.c.d.(7,23)=1$.

Case 3. Let $r=161$. Then $k=-3=158 \pmod{161}$. Recall the number 161 is not prime. In this case $-(k)^3=-(-3)^3=27 \pmod{161}$, $g.c.d.(27,161)=1$, the elements 158 and 27 are invertible elements of the ring $(Z_{161},+,\cdot,1)$. Therefore quasigroup $(Z_{161},\circ)$ with the form $x\circ y=27\cdot x+158\cdot y$ is medial T_2-quasigroup of order 161.

Check. $27x+4266y+674028y+3944312x=y$, $y=y$, since $3944339\equiv 0 \pmod{161}$, $678294\equiv 1 \pmod{161}$.

In order to construct T_2-quasigroups over the ring $(Z_7,+,\cdot,1)$ with non-zero element b we must solve congruence $7\cdot b\equiv 0 \pmod{161}$. It is clear that $g.c.d.(7,161)=7$. Therefore this congruence has 6 non-zero solutions, namely, $b\in\{23,46,69,92,115,138\}=D$.

The following quasigroups are T_2-quasigroups of order 161: $x\circ y=27\cdot x+158\cdot y+i$, for any $i\in D$.

Example 3. We list some values of the polynomial f:

$$
\begin{aligned}
&f(-20)=-3039999, f(-19)=-2345777, f(-18)=-1784591,\\
&f(-17)=-1336335, f(-16)=-983039, f(-15)=-708749,\\
&f(-14)=-499407, f(-13)=-342731, f(-12)=-228095,\\
&f(-11)=-146409, f(-10)=-89999, f(-9)=-52487,\\
&f(-8)=-28671, f(-7)=-14405, f(-6)=-6479, f(-5)=-2499,\\
&f(-4)=-767, f(-3)=-161, f(-2)=-15, f(-1)=1, f(1)=3,\\
&f(2)=49, f(3)=325, f(4)=1281, f(5)=3751,\\
&f(6)=9073, f(7)=19209, f(8)=36865, f(9)=65611,\\
&f(10)=110001, f(11)=175693, f(12)=269569, f(13)=399855,
\end{aligned}
$$

$$f(14) = 576241, f(15) = 810001, f(12) = 269569, f(17) = 1503379,$$
$$f(18) = 1994545, f(19) = 2606421, f(20) = 3360001.$$

The set of prime divisors of the numbers of the set $\{f(-20), f(-19), \dots, f(-1), f(1), \dots, f(20)\}$ contains the following primes:

$$\{3, 5, 7, 13, 19, 23, 37, 43, 59, 61, 73, 101, 157, 211, 241, 307, 347,$$
$$421, 503, 719, 833, 977, 991, 1163, 1319, 2729, 3359, 5813, 6841\}.$$

It is possible to use presented numbers for the construction of T_2-quasigroups over the rings of residues.

Theorem 4. *There exist medial T_2-quasigroups of any prime order p such that $p = 6m + 1$, where $m \in \mathbb{N}$.*

Proof. We use Corollary 3. Let $(Z_p, +, \cdot, 1)$ be a ring (a Galois field) of residues modulo p, where p is prime of the form $6t+1$, $t \in \mathbb{N}$. Quadratic equation $\psi^2+\psi+1 = 0$ has two roots $h_1 = (-1-\sqrt{-3})/2$ and $h_2 = (-1+\sqrt{-3})/2$. Since p is prime, then $g.c.d(h_1, p) = g.c.d(h_2, p) = 1$.

It is known [11] that the number -3 is a quadratic residue modulo any prime p such that $p = 6m + 1$. Finally, if the number $(-1 - \sqrt{-3})$ is odd, then the number $(-1 - \sqrt{-3} + p)$ is even. □

We prove the fact that the number -3 is a quadratic residue modulo any prime p such that $p = 6m + 1$ additionally in the following

Lemma 2. *The number -3 is quadratic residue modulo of odd prime p if p can be presented in the form $6t + 1$, where $t \in \mathbb{N}$.*

Proof. We use for proving this fact information from [7, p. 187-188]. We represent prime p, $p > 2$, in the following form: $p = 4qt+r$, where $1 \leq r < 4q$, $g.c.d.(r, 4q) = 1$, q or $-q$ is a prime. The number q or $-q$ is a quadratic residue modulo p if and only if

$$(-1)^{\frac{r-1}{2} \cdot \frac{q-1}{2}} \left(\frac{r}{q}\right) = 1,$$

where $\left(\frac{r}{q}\right)$ is Legendre symbol, or, speaking more formally, Legendre-Jacobi-Kronecker symbol.

If $r = 1$, then $(-1)^{\frac{1-1}{2} \cdot \frac{-3-1}{2}} \left(\frac{1}{-3}\right) = \left(\frac{1}{-3}\right) = 1$.

If $r = 5$, then $(-1)^{\frac{5-1}{2} \cdot \frac{-3-1}{2}} \left(\frac{5}{-3}\right) = \left(\frac{5}{-3}\right) = -1$.

If $r = 7$, then $(-1)^{\frac{7-1}{2} \cdot \frac{-3-1}{2}} \left(\frac{7}{-3}\right) = \left(\frac{7}{-3}\right) = 1$.

If $r = 11$, then $(-1)^{\frac{11-1}{2} \cdot \frac{-3-1}{2}} \left(\frac{11}{-3}\right) = \left(\frac{11}{-3}\right) = -1$.

Therefore prime p has the form $p = 12t + 1$ or $p = 12t + 7$. Combining the last equalities we have that $p = 6t + 1$. □

In order to construct T_2-quasigroups it is possible to use direct products of T_2-quasigroups. It is clear that direct product of T_2-quasigroups is a T_2-quasigroup.

It is possible to use also the following arguments. The class of T_2 quasigroups is defined using T_2-identity, and it forms a variety in signature with three binary operations, namely, with the operations $\cdot$, $/$, and $\backslash$ [13]. It is known that any variety is closed relative to the operator of direct product [13].

Therefore we can formulate the following

Theorem 5. *There exist medial T_2-quasigroups of any order of the form $p_1^{\alpha_1} p_2^{\alpha_2} \dots p_m^{\alpha_m}$, where p_i are prime numbers of the form $6t+1$, $\alpha_i \in \mathbb{N}$, $i \in \{1, \dots, m\}$.*

Notice that in this section and in the next section examples of medial quasigroups of prime order of the form $6 \cdot t + 5$ (for example, $5, 11, 23, 59$) are given.

Example 4. Using Corollary 5 and ideas of Example 2 we construct medial idempotent T_2-quasigroups over some cyclic groups Z_r ($r < 174$). Notice that such quasigroups are distributive [1, 16]. We have:

$x \cdot y = -2x + 3y \bmod 5;$	$x \cdot y = -x + 2y \bmod 7;$
$x \cdot y = -4x + 5y \bmod 11;$	$x \cdot y = -11x + 12y \bmod 17;$
$x \cdot y = -12x + 13y \bmod 19;$	$x \cdot y = -19x + 20y \bmod 23;$
$x \cdot y = -2x + 3y \bmod 25;$	$x \cdot y = -22x + 23y \bmod 35;$
$x \cdot y = -23x + 24y \bmod 37;$	$x \cdot y = -32x + 33y \bmod 43;$
$x \cdot y = -36x + 37y \bmod 49;$	$x \cdot y = -15x + 16y \bmod 53;$
$x \cdot y = -37x + 38y \bmod 55;$	$x \cdot y = -16x + 17y \bmod 59;$
$x \cdot y = -45x + 46y \bmod 59;$	$x \cdot y = -3x + 4y \bmod 61;$
$x \cdot y = -59x + 60y \bmod 67;$	$x \cdot y = -15x + 16y \bmod 77;$
$x \cdot y = -58x + 59y \bmod 79;$	$x \cdot y = -16x + 17y \bmod 83;$
$x \cdot y = -62x + 63y \bmod 85;$	$x \cdot y = -71x + 72y \bmod 89;$
$x \cdot y = -12x + 13y \bmod 95;$	$x \cdot y = -45x + 46y \bmod 97;$
$x \cdot y = -7x + 8y \bmod 101;$	$x \cdot y = -11x + 12y \bmod 101;$
$x \cdot y = -8x + 9y \bmod 103;$	$x \cdot y = -72x + 73y \bmod 107;$
$x \cdot y = -82x + 83y \bmod 109;$	$x \cdot y = -58x + 59y \bmod 113;$
$x \cdot y = -12x + 13y \bmod 115;$	$x \cdot y = -113x + 114y \bmod 119;$
$x \cdot y = -4x + 5y \bmod 121;$	$x \cdot y = -102x + 103y \bmod 125;$
$x \cdot y = -50x + 51y \bmod 133;$	$x \cdot y = -63x + 64y \bmod 137;$
$x \cdot y = -118x + 119y \bmod 149;$	$x \cdot y = -46x + 47y \bmod 157;$
$x \cdot y = -127x + 128y \bmod 161;$	$x \cdot y = -32x + 33y \bmod 167;$
$x \cdot y = -33x + 34y \bmod 173;$	$x \cdot y = -75x + 76y \bmod 173.$

Using Mace 4 [14] we construct the following examples of medial T_2-quasigroups.

$*$	0	1	2
0	0	1	2
1	2	0	1
2	1	2	0

$\boxtimes$	0	1	2	3
0	0	2	3	1
1	1	3	2	0
2	2	0	1	3
3	3	1	0	2

$\circ$	0	1	2	3	4
0	0	2	4	1	3
1	2	1	3	4	0
2	4	3	2	0	1
3	1	4	0	3	2
4	3	0	1	2	4

$\diamond$	0	1	2	3	4	5	6	7
0	0	2	4	1	6	3	7	5
1	6	1	5	2	0	7	3	4
2	7	4	2	5	3	6	0	1
3	4	7	0	3	5	1	2	6
4	5	3	6	7	4	2	1	0
5	2	0	7	6	1	5	4	3
6	3	5	1	4	7	0	6	2
7	1	6	3	0	2	4	5	7

We recall (see Section 1) that in [5] it is proved that idempotent models of identity $(yx \cdot y)y = x$ (therefore also idempotent models of T_2-quasigroups) exist for all orders $n > 174$.

Remark 2. From Example 4 and the example of medial idempotent T_2-quasigroup of order 8 we obtain partial spectrum of idempotent medial T_2-quasigroups of order less than 174.

Lemma 3. *There exist medial T_2-quasigroups of order 2^k for any $k \geq 2$.*

Proof. It follows since T_2-quasigroup with the operation $\boxtimes$ is medial quasigroup of order 2^2 and T_2-quasigroup with the operation $\diamond$ is medial quasigroup of order 2^3 and $g.c.d.(2,3) = 1$. $\square$

Example 5. There exists medial T_2-quasigroup of order 2^{11} since $11 = 2 \cdot 1 + 3 \cdot 3$.

Example 6. Quasigroup $(Z_{341}, \circ)$, $x \circ y = -125x + 5y$, is an example of medial non-idempotent T_2-quasigroup. Notice, in this example $5^2 + 5 + 1 = 31$, $5^3 - 5 + 1 = 121$, but $31 \cdot 121 \equiv 0 \bmod 341$, i.e. $5^5 + 5^4 + 1 \equiv 0 \bmod 341$.

It is possible to check that quasigroup $(Z_{341}, \circ)$ is isomorphic to the direct product of quasigroup $(Z_{31}, *)$, where $x * y = -x + 5y$, and quasigroup $(Z_{11}, \star)$, where $x \star y = -4x + 5y$.

Quasigroup with operation $x \cdot y = 13x + 18y \bmod 35$ is isomorphic to the direct product of quasigroup of order five with the operation $x * y = -2x + 3y \bmod 5$ and quasigroup of order seven with the operation $x \star y = -x + 4y \bmod 7$.

See [21, 22] about direct products of medial quasigroups.

Combining Lemma 3, Theorem 5, and constructed examples we formulate the following

Theorem 6. *There exist medial T_2-quasigroups of any order of the form*

$$2^{k_1}3^{k_2}5^{k_3}11^{k_4}17^{k_5}23^{k_6}53^{k_7}59^{k_8}83^{k_9}101^{k_{10}}p_1^{\alpha_1}p_2^{\alpha_2}\dots p_m^{\alpha_m},$$

where $k_1 \geq 2$, $k_2, \dots, k_{10} \geq 1$, p_i are prime numbers of the form $6t+1$, $\alpha_i \in \mathbb{N}$, $i \in \{1, \dots, m\}$.

Notice that direct calculation demonstrates that no solution of the equations $x^2+x+1=0$, $x^3-x+1=0$, $x^5+x^4+1=0$ exists in the field $GF(29)$.

4 Annex

Computer calculations show that there exist the following medial idempotent T_2-quasigroups of order r of the form $r = 6t+5$. Such quasigroups of orders less than 174 are given in Example 4 and we omit them here. We give such quasigroups up to $r = 1155$. We present triplets in which the permutations φ, ψ and the order r of quasigroup $(Z_r, \varphi, \psi, 0)$ are given:

$(-97, 98, 185)$;	$(-153, 154, 191)$;	$(-202, 203, 209)$;	$(-32, 33, 215)$;
$(-33, 34, 227)$;	$(-232, 233, 245)$;	$(-208, 209, 251)$;	$(-118, 119, 263)$;
$(-202, 203, 275)$;	$(-151, 152, 281)$;	$(-59, 60, 293)$;	$(-247, 248, 305)$;
$(-170, 171, 317)$;	$(-164, 165, 323)$;	$(-327, 328, 335)$;	$(-22, 23, 347)$;
$(-312, 313, 359)$;	$(-15, 16, 371)$;	$(-39, 40, 383)$;	$(-66, 67, 389)$;
$(-137, 138, 395)$;	$(-309, 310, 401)$;	$(-356, 357, 407)$;	$(-113, 114, 413)$;
$(-55, 56, 419)$;	$(-402, 403, 425)$;	$(-310, 311, 431)$;	$(-12, 13, 437)$;
$(-249, 250, 449)$;	$(-313, 314, 467)$;	$(-290, 291, 473)$;	$(-197, 198, 479)$;
$(-142, 143, 485)$;	$(-494, 495, 503)$;	$(-317, 318, 515)$;	$(-127, 128, 521)$;
$(-477, 478, 539)$;	$(-82, 83, 545)$;	$(-233, 234, 557)$;	$(-237, 238, 563)$;
$(-109, 110, 569)$;	$(-127, 128, 575)$;	$(-99, 100, 581)$;	$(-111, 112, 593)$;
$(-71, 72, 599)$;	$(-367, 368, 605)$;	$(-538, 539, 617)$;	$(-71, 72, 623)$;
$(-504, 505, 629)$;	$(-552, 553, 641)$;	$(-266, 267, 659)$;	$(-582, 583, 665)$;
$(-125, 126, 671)$;	$(-591, 592, 677)$;	$(-354, 355, 701)$;	$(-484, 485, 707)$;
$(-117, 118, 719)$;	$(-419, 420, 731)$;	$(-59, 60, 737)$;	$(-436, 437, 743)$;
$(-393, 394, 749)$;	$(-66, 67, 773)$;	$(-517, 518, 785)$;	$(-736, 737, 791)$;
$(-225, 226, 797)$;	$(-424, 425, 809)$;	$(-322, 323, 821)$;	$(-150, 151, 827)$;
$(-232, 233, 833)$;	$(-541, 542, 839)$;	$(-134, 135, 851)$;	$(-532, 533, 869)$;
$(-477, 478, 875)$;	$(-389, 390, 881)$;	$(-512, 513, 905)$;	$(-165, 166, 911)$;
$(-147, 148, 935)$;	$(-709, 710, 941)$;	$(-210, 211, 953)$;	$(-337, 338, 959)$;
$(-706, 707, 971)$;	$(-957, 958, 977)$;	$(-208, 209, 983)$;	$(-548, 549, 989)$;
$(-542, 543, 995)$;	$(-810, 811, 1007)$;	$(-180, 181, 1019)$;	$(-637, 638, 1031)$;

$$
\begin{array}{llll}
(-674, 675, 1037); & (-267, 268, 1043); & (-82, 83, 1049); & (-427, 428, 1055); \\
(-433, 434, 1067); & (-269, 270, 1091); & (-536, 537, 1097); & (-889, 890, 1103); \\
(-761, 762, 1109); & (-382, 383, 1115); & (-753, 754, 1121); & (-134, 135, 1127); \\
(-1038, 1039, 1133); & (-997, 998, 1139); & (-872, 873, 1145); & (-561, 562, 1151).
\end{array}
$$

References

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

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

[3] Belousov V. D. *Parastrophic-orthogonal quasigroups.* Preprint, Kishinev, Shtiinta, 1983 (in Russian).

[4] Belousov V. D. *Parastrophic-orthogonal quasigroups.* Translated from the 1983 Russian original. Quasigroups Relat. Syst., 2005, **13**, No. 1, 25–72.

[5] Bennett F. E. *Quasigroup identities and Mendelsohn designs.* Canad. J. Math., 1989, **41**, No. 2, 341–368.

[6] Bennett F. E. *The spectra of a variety of quasigroups and related combinatorial designs.* Discrete Math., 1989, **77**, 29–50.

[7] Buchstab A. A. *Number Theory.* Prosveshchenie, 1966 (in Russian).

[8] Ceban D., Syrbu P. *On qusigroups with some minimal idetities.* Studia Universitatis Moldaviae. Stiinte Exacte si Economice, 2015, **82**, No. 2, 47–52.

[9] Dénes J., Keedwell A. D. *Latin Squares and their Applications.* Académiai Kiadó, Budapest, 1974.

[10] Evans T. *Algebraic structures associated with latin squares and orthogonal arrays.* Congr. Numer., 1975, **13**, 31–52.

[11] Keedwell A. D., Shcherbacov V. A. *Construction and properties of (r,s,t)-inverse quasigroups, I.* Discrete Math., 2003, **266**, No. 1–3, 275–291.

[12] Lindner C. C., Mendelsohn N. S., Sun S. R. *On the construction of Schroeder quasigroups.* Discrete Math., 1980, **32**, No. 3, 271–280.

[13] Mal'tsev A. I. *Algebraic Systems.* Moscow, Nauka, 1976 (in Russian).

[14] McCune W. *Mace 4.* University of New Mexico, www.cs.unm.edu/mccune/prover9/, 2007.

[15] Mullen G. L., Shcherbacov V. A. *On orthogonality of binary operations and squares.* Bul. Acad. Ştiinţe Repub. Moldova, Mat., 2005, No. 2(48), 3–42.

[16] Němec P., Kepka T. *T-quasigroups, I.* Acta Univ. Carolin. Math. Phys., 1971, **12**, No. 1, 39–49.

[17] Pelling M. J., Rogers D. G. *Stein quasigroups. I: Combinatorial aspects.* Bull. Aust. Math. Soc., 1978, **18**, 221–236.

[18] Pflugfelder H. O. *Quasigroups and Loops: Introduction.* Heldermann Verlag, Berlin, 1990.

[19] Sade A. *Quasigroupes obéissant á certaines lois.* Rev. Fac. Sci. Univ. Istambul, 1957, **22**, 151–184.

[20] Scerbacova A. V., Shcherbacov V. A. *About spectrum of T_2-quasigroups.* Technical report, arXiv:1509.00796, 2015.

[21] Shcherbacov V. A. *On simple n-ary medial quasigroups.* In Proceedings of Conference Computational Commutative and Non-Commutative Algebraic Geometry, vol. 196 of NATO Sci. Ser. F Comput. Syst. Sci., pages 305–324. IOS Press, 2005.

[22] Shcherbacov V. A. *On structure of finite n-ary medial quasigroups and automorphism groups of these quasigroups.* Quasigroups Relat. Syst., 2005, **13**, No. 1, 125–156.

[23] Shcherbacov V. A. *On definitions of groupoids closely connected with quasigroups.* Bul. Acad. Ştiinţe Repub. Moldova, Mat., 2007, No. 2(54), 43–54.

[24] Shcherbacov V. A. *Quasigroups in cryptology.* Comput. Sci. J. Moldova, 2009, **17**, No. 2, 193–228.

[25] Syrbu P., Ceban D. *On π-quasigroups of type T_1.* Bul. Acad. Ştiinţe Repub. Moldova, Mat., 2014, No. 2(75), 36–43.

[26] Syrbu P. N. *On π-quasigroups isotopic to abelian groups.* Bul. Acad. Ştiinţe Repub. Moldova, Mat., 2009, No. 3(61), 109–117.

A. V. Scerbacova
Gubkin Russian State Oil and Gas University
Leninsky Prospect, 65, Moscow 119991
Russia
E-mail: *scerbik33@yandex.ru*

Received May 26, 2016

V.A. Shcherbacov
Institute of Mathematics and Computer Science
Academy of Sciences of Moldova
Academiei str. 5, MD−2028 Chişinău
Moldova
E-mail: *scerb@math.md*