BULETINUL ACADEMIEI DE ŞTIINŢE
A REPUBLICII MOLDOVA. MATEMATICA
Number 1(68), 2012, Pages 21–31
ISSN 1024–7696

Conjugate sets of loops and quasigroups. DC-quasigroups

G. B. Belyavskaya, T. V. Popovich

Abstract. It is known that the set of conjugates (the conjugate set) of a binary quasigroup can contain 1, 2, 3 or 6 elements. We investigate loops, IP-quasigroups and T-quasigroups with distinct conjugate sets described earlier. We study in more detail the quasigroups all conjugates of which are pairwise distinct (shortly, DC-quasigroups). The criterion of a DC-quasigroup (a DC-IP-quasigroup, a DC-T-quasigroup) is given, the existence of DC-T-quasigroups for any order $n \geq 5$, $n \neq 6$, is proved and some examples of DC-quasigroups are given.

Mathematics subject classification: 20N05, 05B15.
Keywords and phrases: Quasigroup, loop, IP-quasigroup, T-quasigroup, conjugate, parastrophe, identity.

1 Introduction

A quasigroup is an ordered pair (Q, A) where Q is a nonempty set and A is a binary operation defined on Q such that each of the equations $A(a, y) = b$ and $A(x, a) = b$ is uniquely solvable for any pair of elements a, b in Q was established. It is known that the multiplication table of a finite quasigroup defines a Latin square and six (not necessarily distinct) conjugates (or parastrophes) are associated with each quasigroup (Latin square) [1, 6].

In [9] a connection between five identities of two variables and the equality of a quasigroup to some of the rest five its conjugates was established. It was also proved that the number of distinct conjugates of a finite quasigroup can be 1, 2, 3 or 6 and for any $m = 1, 2, 3, 6$ and any $n \geq 4$ there exists a quasigroup of order n with m distinct conjugates (see Theorem 6 of [9]).

In [12] a connection between different pairs of conjugates of a quasigroup was established, four identities that correspond to the equality of a quasigroup to its conjugates were given. It was also proved that any two of these four identities imply the rest two identities. All six possible sets of conjugates taking into account all possible cases of the equality ("assembling") of conjugates were described. The connection between four identities and possible conjugate sets was shown.

In this article we continue the investigation of conjugates of quasigroups started in [12], in particular, we study loops, IP-quasigroups and T-quasigroups with distinct conjugate sets described in [12].

We study in more detail quasigroups and loops all conjugates of which are pairwise distinct (these quasigrops we call distinct conjugate quasigroups or, shortly,

DC-quasigroups). Such quasigroups form an important class and arise by the research of various questions of the quasigroup theory and the Latin square theory, in particular, in the research of totally conjugate-orthogonal [5] and near totally conjugate-orthogonal quasigroups [11]. They can be also used by coding and encryption of information. The criterion of a DC-quasigroup (of a DC-IP-quasigroup, a DC-T-quasigroup) is established, some examples of DC-quasigroups are given and the existence of DC-T-quasigroups of any order $n \geq 5$, $n \neq 6$, is proved.

2 Preliminaries

Remind some necessary notions and results. To any quasigroup (Q, A) the system $\Sigma(A)$ of six (not necessarily distinct) *conjugates (parastrophes)* corresponds:

$$\Sigma(A) = (A, A^{-1}, {}^{-1}A, {}^{-1}\left(A^{-1}\right), ({}^{-1}A)^{-1}, A^*),$$

where $A(x, y) = z \Leftrightarrow A^{-1}(x, z) = y \Leftrightarrow {}^{-1}A(z, y) = x \Leftrightarrow A^*(y, x) = z$.

Using the Belousov's designation of conjugates of a quasigroup (Q, A) from [2] we have the following conjugate system $\Sigma(A)$:

$$\Sigma(A) = (A,\ {}^{r}A,\ {}^{l}A,\ {}^{lr}A,\ {}^{rl}A,\ {}^{s}A),$$

where ${}^{1}A = A$, ${}^{r}A = A^{-1}$, ${}^{l}A = {}^{-1}A$, ${}^{lr}A = {}^{-1}(A^{-1})$, ${}^{rl}A = ({}^{-1}A)^{-1}$, ${}^{s}A = A^*$.

Note that $\left({}^{-1}(A^{-1})\right)^{-1} = {}^{rlr}A = {}^{-1}\left(({}^{-1}A)^{-1}\right) = {}^{lrl}A = {}^{s}A$ and ${}^{rr}A = {}^{ll}A = A$, ${}^{\sigma\tau}A = {}^{\sigma}({}^{\tau}A)$.

Let $\overline{\Sigma}(A)$ be the set of conjugates (*the conjugate set)* of a quasigroup (Q, A). It is known [9] that $|\ \overline{\Sigma}(A)\ | = 1$, 2, 3 or 6.

A quasigroup is a totally-symmetric quasigroup (a TS-quasigroup) if it satisfies the identities $x \cdot xy = y$ and $xy = yx$. For TS-quasigroups $|\ \overline{\Sigma}(A)\ | = 1$.

The following Theorem 1 of [12] describes all possible conjugate sets for quasigroups and points out the only possible variants of equality ("assembling") of conjugates in every case.

Theorem 1 [12]. *The following conjugate sets of a quasigroup (Q, A) are only possible:* $\overline{\Sigma}_1(A) = \{A\}$; $\overline{\Sigma}_2(A) = \{A, {}^{s}A\} = \{A = {}^{lr}A = {}^{rl}A,\ {}^{l}A = {}^{r}A = {}^{s}A\}$; $\overline{\Sigma}_6(A) = \{A,\ {}^{r}A,\ {}^{l}A,\ {}^{lr}A,\ {}^{rl}A,\ {}^{s}A\}$; $\overline{\Sigma}_3(A) = \{A, {}^{lr}A, {}^{rl}A\}$ *and three cases are only possible:*

$\overline{\Sigma}^1_3(A) = \{A = {}^{r}A,\ {}^{l}A = {}^{lr}A,\ {}^{rl}A = {}^{s}A\}$;
$\overline{\Sigma}^2_3(A) = \{A = {}^{l}A,\ {}^{r}A = {}^{rl}A,\ {}^{lr}A = {}^{s}A\}$;
$\overline{\Sigma}^3_3(A) = \{A = {}^{s}A,\ {}^{r}A = {}^{lr}A,\ {}^{l}A = {}^{rl}A\}$.

For convenience we denote the classes of quasigroups (Q, A) with $\overline{\Sigma}(A) = \overline{\Sigma}_1(A), \overline{\Sigma}_2(A), \overline{\Sigma}^1_3(A), \overline{\Sigma}^2_3(A), \overline{\Sigma}^3_3(A), \overline{\Sigma}_6(A)$ by $V_1, V_2, V^1_3, V^2_3, V^3_3, V_6$, respectively.

We say that a quasigroup (Q, A) satisfies exactly one identity of the set of identities $\overline{T} = \{A(x, A(x, y)) = y, A(A(y, x), x) = y, A(x, y) = A(y, x), A(A(x, y), x) = y\}$ if it satisfies one identity and does not satisfy the rest identities of this set.

Remark 1. According to Corollary 4 [12], establishing a connection between conjugate sets described in Theorem 1 and the identities of the set $\overline{T}$ we have that V_1 is the class of quasigroups satisfying all identities of $\overline{T}$; V_2 (V_3^1, V_3^2, V_3^3) is the class of quasigroups satisfying exactly the identity $A(A(x,y),x) = y$ ($A(x,A(x,y)) = y, A(A(y,x),x) = y, A(x,y) = A(y,x)$ respectively) of $\overline{T}$ and V_6 is the class of quasigroups which satisfies none of four identities of $\overline{T}$. For a quasigroup (Q,A) of the class V_1 (of the variety of TS-quasigroups) $\mid \overline{\Sigma}(A) \mid = 1$; for a quasigroup of the class V_2 (every of the classes V_3^1, V_3^2, V_3^3) we have $\mid \overline{\Sigma}(A) \mid = 2$ ($\mid \overline{\Sigma}(A) \mid = 3$ respectively) and $\mid \overline{\Sigma}(A) \mid = 6$ for the class V_6.

Below we study loops, IP-quasigroups and T-quasigroups from the point of view of their conjugate sets.

3 Conjugate sets of loops

Let (Q,A) be a loop with the identity e, $A(I_l x, x) = A(x, I_r x) = e$, that is $I_l x = {}^{-1}x$, $I_r x = x^{-1}$. It is easy to see that if the loop (Q,A) satisfies at least one of the three identities $A(x,A(x,y)) = y$, $A(A(y,x),x) = y$, $A(A(x,y),x) = y$ of the set $\overline{T}$, then it is a loop of exponent two: $A(x,x) = e$ for any $x \in Q$. In this case $I_l = I_r = \varepsilon$.

Proposition 1. *In any of the classes $V_1, V_2, V_3^1, V_3^2, V_3^3, V_6$ of quasigroups there exists a loop of exponent two.*

Proof. Note that if a loop (Q,A) has exponent two , then all its congugates also are loops of exponent two since $L_x^r y = L_x^{-1} y$ and $R_y^l x = R_y^{-1} x$, where $L_x^r y = {}^{r}A(x,y)$, $R_y^l x = {}^{l}A(x,y)$, $L_x y = A(x,y)$, $R_y x = A(x,y)$. Any TS-loop is in V_1. The loops of exponent two given by Tables 1–5 are, respectively, in V_2, V_3^1, V_3^2, V_3^3 and V_6:

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

Tab. 1

1	2	3	4	5	6
2	1	5	6	3	4
3	6	1	5	4	2
4	3	2	1	6	5
5	4	6	2	1	3
6	5	4	3	2	1

Tab. 2

1	2	3	4	5	6
2	1	5	6	4	3
3	4	1	5	6	2
4	3	6	1	2	5
5	6	2	3	1	4
6	5	4	2	3	1

Tab. 3

1	2	3	4	5	6
2	1	6	5	3	4
3	6	1	2	4	5
4	5	2	1	6	3
5	3	4	6	1	2
6	4	5	3	2	1

Tab. 4

1	2	3	4	5	6
2	1	4	3	6	5
3	5	1	6	4	2
4	6	5	1	2	3
5	3	6	2	1	4
6	4	2	5	3	1

Tab. 5

Now consider the loops which are not loops of exponent two.

Proposition 2. *Let a loop (Q, A) be not of exponent two, then $(Q, A) \in V_3^3$ if (Q, A) is a commutative loop and $(Q, A) \in V_6$ if (Q, A) is a noncommutative loop.*

Proof. Indeed, in this case $(Q, A) \notin V_1, V_2, V_3^1, V_3^2$ since this loop satisfies none of identities of the set $\overline{T}$ corresponding to these classes. If the loop is commutative, then by Theorem 1 and Remark 1 it is in the class V_3^3. Otherwise it is in V_6. □

4 Conjugate sets of IP-quasigroups

At first we recall that a quasigroup (Q, A) is called a quasigroup with the property of invertibility (an IP-quasigroup) if there exist two mappings I_l and I_r of the set Q into Q such that $A(I_l x, A(x, y)) = y$ and $A(A(y, x), I_r x)) = y$ for all $x, y \in Q$.

It is known that the mappings I_l and I_r are permutations, $I_l^2 = I_r^2 = \varepsilon$ (the identity permutation) and $I_l A(x, y) = A(I_r y, I_r x)$, $I_r A(x, y) = A(I_l y, I_l x)$ [1].

The conjugates of an IP-quasigroup have the following form:
${}^{l}A(x, y) = A(x, I_r y)$, ${}^{r}A(x, y) = A(I_l x, y)$, ${}^{lr}A(x, y) = I_l A(x, I_r y)$,
${}^{rl}A(x, y) = I_r A(I_l x, y)$, ${}^{s}A(x, y) = I_r A(I_l x, I_l y) = I_l A(I_r x, I_r y)$.
By Theorem 1 of [3] all conjugates of an IP-quasigroup are isotopic. Note that in a commutative IP-quasigroup and in an IP-loop $I_r = I_l = I$.

Proposition 3. *Let a quasigroup (Q, A) be a noncommutative IP-quasigroup. Then ${}^{r}A(x, y) = {}^{l}A(x, y)$ if and only if $I_l = I_r = I$ and $IA(x, y) = A(y, x)$.*

Proof. Let ${}^{r}A =^{l} A$, then $I_l \neq \varepsilon$ ($I_r \neq \varepsilon$): by $I_l = \varepsilon$ we have $A(I_l x, y) = A(x, y) = A(x, I_r y)$, then $I_r = \varepsilon$ and (Q, A) is commutative. But in this case from ${}^{r}A(x, y) =^{l} A(x, y)$ it follows $A(I_l x, y) = A(x, I_r y)$, $A(x, y) = A(I_l x, I_r y)$, $I_l A(x, y) = I_l A(I_l x, I_r y) = A(y, I_r I_l x)$, $I_l A(I_l x, y) = A(y, I_r x)$, $I_l I_r A(I_l y, x) = A(y, I_r x)$, $I_l I_r A(I_l y, I_r x) = A(y, x) = A(I_l y, I_r x)$, since $A(x, y) = A(I_l x, I_r y)$, whence it follows that $I_l I_r = \varepsilon$ or $I_l = I_r = I$. Taking into account that $A(y, x) = A(I_l y, I_r x)$ we obtain $IA(x, y) = A(y, x)$.

Conversely, let $I_l = I_r = I$ in a noncommutative IP-quasigroup (Q, A) and $IA(x, y) = A(y, x)$, then $A(x, y) = A(Ix, Iy)$, $A(Ix, y) = A(x, Iy)$, that is ${}^{r}A(x, y) = {}^{l}A(x, y)$. □

Now we consider IP-quasigroups from the point of view of their affiliation to the classes of quasigroups $V_1, V_2, V_3^1, V_3^2, V_3^3$ and V_6.

Theorem 2. *Let a quasigroup (Q, A) be an IP-quasigroup with $I_l = I_r = I$. Then $(Q, A) \in V_1$ if and only if $I = \varepsilon$; $(Q, A) \in V_3^3$ if and only if (Q, A) is commutative and $I \neq \varepsilon$; $(Q, A) \in V_2$ if and only if (Q, A) is noncommutative and $IA(x, y) = A(y, x)$; $(Q, A) \in V_6$ if and only if (Q, A) is noncommutative and $IA(x, y) \neq A(y, x)$.*

Proof. If $I_l = I_r = I = \varepsilon$, then all conjugates coincide and $(Q, A) \in V_1$. The converse is also true. If $I \neq \varepsilon$ and (Q, A) is commutative, then $A =^{s} A$, $A \neq^{l} A$, $A \neq^{r} A$, so by Theorem 1 $(Q, A) \in V_3^3$. The converse follows from Theorem 1.

Let (Q, A) be a noncommutative IP-quasigroup. If $IA(x, y) = A(y, x)$ (in this case $I \neq \varepsilon$), then $A \neq^{s} A$, $A \neq^{l} A$, $A \neq^{r} A$ and by Proposition 3 ${}^{r}A =^{l} A$, so by

Theorem 1 $(Q,A) \in V_2$. If $(Q,A) \in V_2$, then by Theorem 1 the quasigroup (Q,A) is noncommutative and ${}^rA = {}^lA$, so by Proposition 3 $IA(x,y) = A(y,x)$.

If $IA(x,y) \neq A(y,x)$ and (Q,A) is a noncommutative quasigroup, then $A \neq^s A$, $A \neq^l A$, $A \neq^r A$ and by Proposition 3, ${}^rA \neq^l A$. It means that by Theorem 1 the quasigroup (Q,A) is contained in V_6.

If a quasigroup (Q,A) is contained in V_6, then it is noncommutative and ${}^rA \neq {}^lA$, so by Proposition 3 $IA(x,y) \neq A(y,x)$ (since in this case $I_l = I_r = I$). □

Note that by Theorem 2 of [3] all conjugates of an IP-quasigroup (Q,A) are also IP-quasigroups if and only if there exists a permutation α such that $\alpha A(x,y) = A(y,x)$, so in the cases $(Q,A) \in V_1$, $(Q,A) \in V_2$ and $(Q,A) \in V_3^3$ conjugates of (Q,A) are IP-quasigroups.

Recall that a Moufang loop is defined by the identity $x(y \cdot xz) = (xy \cdot x)z$ and is a special case of IP-loops. From Theorem 2 and Proposition 2 the following corollaries easy follow.

Corollary 1. *Let (Q,A) be an IP-loop (a Moufang loop), then*
$(Q,A) \in V_1$ *if* $I = \varepsilon$;
$(Q,A) \in V_3^3$ *if (Q,A) is commutative and* $I \neq \varepsilon$;
$(Q,A) \in V_6$, *if (Q,A) is noncommutative.*

Note that the case $(Q,A) \in V_2$ of Theorem 2 for an IP-loop is impossible.

Corollary 2. *All abelian groups of exponent 2 are contained in the class V_1, the rest abelian group are contained in the class V_3^3. Non-abelian groups are in V_6.*

Theorem 3. *Let a quasigroup (Q,A) be an IP-quasigroup with $I_l \neq I_r$. Then*
$(Q,A) \in V_3^1$ *if and only if* $I_l = \varepsilon$.
$(Q,A) \in V_3^2$ *if and only if* $I_r = \varepsilon$.
$(Q,A) \in V_6$ *if and only if* $I_l, I_r \neq \varepsilon$.

Proof. In this case a quasigroup (Q,A) is noncommutative. If $I_l = \varepsilon$ ($I_r = \varepsilon$) and $I_l \neq I_r$, then $A \neq {}^sA$, $A \neq {}^{lr}A$, $A \neq {}^lA$, and $A = {}^rA$ ($A \neq {}^sA$, $A \neq {}^{rl}A$, $A \neq {}^rA$ and $A = {}^lA$), so $(Q,A) \in V_3^1$ ($(Q,A) \in V_3^2$, respectively). The converse follows from Theorem 1 since then $A = {}^rA$ ($A = {}^lA$), that is $I_l = \varepsilon$ ($I_r = \varepsilon$). If $I_l, I_r \neq \varepsilon$ and $I_l \neq I_r$ we have $A \neq^s A$, $A \neq^l A$, $A \neq^r A$ and by Proposition 3 ${}^rA \neq^l A$, so $(Q,A) \in V_6$ according to Theorem 1. If $(Q,A) \in V_6$, then $A \neq^l A$ and $A \neq^r A$, so $I_l, I_r \neq \varepsilon$. □

Example 1. In [1], p. 74, the following example of IP-quasigroup with $I_l \neq I_r$ is given. Let $(Q,\cdot)$ be a group with the identity e, θ be its automorphism of order two, (Q,A) be the quasigroup where $A(x,y) = \theta x \cdot y$. Then $(M,\circ) = (Q,\cdot) \times (Q,A)$ is an IP-quasigroup with $I_l(a,b) = (a^{-1}, b^{-1})$, $I_r(a,b) = (a^{-1}, \theta b^{-1})$, where $a \cdot a^{-1} = e$. In this quasigroup $I_l \neq I_r$ and $I_l, I_r \neq \varepsilon$ if $(Q,\cdot)$ has not exponent two, so by Theorem 3 $(M,\circ)$ is in V_6. If $(Q,\cdot)$ is a group of exponent two, then $I_l = \varepsilon$ and by Theorem 3 $M(\circ) \in V_3^1$.

Let in this example $A(x,y) = x \cdot \theta y$, $(M,\circ) = (Q,A) \times (Q,\cdot)$, $I_r(a,b) = (a^{-1}, b^{-1})$, $I_l(a,b) = (\theta a^{-1}, b^{-1})$, then

$((a,b)\circ(c,d))\circ I_r(c,d) = (a\cdot\theta c, bd)\circ(c^{-1},d^{-1}) = (a\cdot\theta c\cdot\theta c^{-1}, bd\cdot d^{-1}) = (a,b)$,
$I_l(a,b)\circ((a,b)\circ(c,d)) = (\theta a^{-1}, b^{-1})\circ(a\cdot\theta c, bd) = (\theta a^{-1}\cdot\theta a\cdot\theta^2 c, b^{-1}\cdot bd)) = (c,d)$.
Thus, $(M,\circ)$ is also an IP-quasigroup with $I_l \neq I_r$.

If the group $(Q,\cdot)$ has not exponent two, then the IP-quasigroup $(M,\circ)$ is in V_6, since $I_l, I_r \neq \varepsilon$. If the group $(Q,\cdot)$ is a group of exponent two, then $I_r = \varepsilon$, so by Theorem 3 $(M,\circ) \in V_3^2$.

5 Conjugate sets of T-quasigroups

A quasigroup (Q,A) is *a T-quasigroup* if there exist an abelian group $(Q,+)$, its automorphisms φ,ψ and an element $c\in Q$ such that $A(x,y) = \varphi x + \psi y + c$ for any $x,y\in Q$ [8].

The conjugates of a T-quasigroup $A(x,y) = \varphi x + \psi y + c$ (which are also T-quasigroups) have the following form:
${}^{s}A(x,y) = \psi x + \varphi y + c$, ${}^{r}A(x,y) = \psi^{-1}(y - \varphi x - c)$,
${}^{l}A(x,y) = \varphi^{-1}(x - \psi y - c)$, ${}^{rl}A(x,y) = \psi^{-1}(x - \varphi y - c)$,
${}^{lr}A(x,y) = \varphi^{-1}(y - \psi x - c)$ (see, for example, [10]).

Let $Ix = -x$, then $I^2 = \varepsilon$ where ε is the identity transformation, and $I\varphi = \varphi I$ for any automorphism φ of a group $(Q,+)$.

By Proposition 1 of [12] all pairs of conjugates of the conjugate system $\Sigma(A)$ of a quasigroup (Q,A) can be divided into four disjoint classes:
I. $(A,{}^{r}A)$, $({}^{l}A,{}^{lr}A)$, $({}^{rl}A,{}^{s}A)$;
II. $(A,{}^{l}A)$, $({}^{r}A,{}^{rl}A)$, $({}^{s}A,{}^{lr}A)$;
III. $(A,{}^{s}A)$, $({}^{r}A,{}^{lr}A)$, $({}^{l}A,{}^{rl}A)$;
IV. $({}^{l}A,{}^{r}A)$, $(A,{}^{lr}A)$, $({}^{r}A,{}^{s}A)$, $({}^{lr}A,{}^{rl}A)$, $(A,{}^{rl}A)$, $({}^{l}A,{}^{s}A)$
such that the equality (inequality) of components of one pair in a class implies the equality (inequality) of components of any pair in this class.

For T-quasigroups the following (Theorem 2 of [12]) was proved:

Theorem 4 [12]. *The components of any pair of a class I, II, III or IV for a T-quasigroup (Q,A): $A(x,y) = \varphi x + \psi y$ coincide if and only if $\psi = I$ for the pairs of class I; $\varphi = I$ for the pairs of class II; $\varphi = \psi$ for the pairs of class III; $\varphi^2 = I\psi$ and $\psi^2 = I\varphi$ (or $\varphi = \psi^{-1}$ and $\varphi^3 = I$) for the pairs of class IV.*

Note that in [12] the equivalence of the pair of equalities $\varphi^2 = I\psi$ and $\psi^2 = I\varphi$ to the pair of equalities $\varphi = \psi^{-1}$ and $\varphi^3 = I$ was proved.

Now we shall describe T-quasigroups with distinct conjugate sets.

Theorem 5. *Let (Q,A) be a T-quasigroup: $A(x,y) = \varphi x + \psi y$. Then*
$(Q,A) \in V_1$ if and only if $\varphi = \psi = I$;
$(Q,A) \in V_2$ if and only if $\varphi^3 = I, \varphi = \psi^{-1}, \varphi \neq I, \psi$;
$(Q,A) \in V_3^1$ if and only if $\psi = I, \varphi \neq I$;
$(Q,A) \in V_3^2$ if and only if $\varphi = I, \psi \neq I$;

$(Q, A) \in V_3^3$ if and only if $\varphi = \psi, \varphi \neq I$, and at least one of two inequalities $\varphi \neq \psi^{-1}$, $\varphi^3 \neq I$ is fulfilled;

$(Q, A) \in V_6$ if and only if $\varphi, \psi \neq I$, $\varphi \neq \psi$ and at least one of two inequalities $\varphi \neq \psi^{-1}$, $\varphi^3 \neq I$ and at least one of two inequalities $\varphi^2 \neq I\psi$ or $\psi^2 \neq I\varphi$ is fulfilled.

Proof. The first statement is easy checked if to take into account the definition of a TS-quasigroup.

Let $\varphi^3 = I, \varphi = \psi^{-1}$ and $\varphi \neq I, \psi$. In this case we have $\psi \neq I$ and $\varphi \neq \psi$, so by Proposition 1 of [12] and Theorem 4 $A = {}^{lr}A = {}^{rl}A$, ${}^{l}A = {}^{r}A = {}^{s}A$ (these equalities correspond to the pairs of class IV), $A \neq {}^{r}A$, $A \neq {}^{l}A$ and $A \neq {}^{s}A$. Thus, in the set $\overline{\Sigma}(A)$ there are exactly two conjugates and $(Q, A) \in V_2$. The converse follows from the form of $\overline{\Sigma}_2(A)$ for V_2 in Theorem 1 and from Theorem 4 since in this case $A = {}^{lr}A = {}^{rl}A$, ${}^{l}A = {}^{r}A = {}^{s}A$, moreover, $A \neq {}^{r}A$, $A \neq {}^{l}A$, $A \neq {}^{s}A$, since $\overline{\Sigma}_2(A)$ contains two elements.

Let $\psi = I, \varphi \neq I$, then $\varphi \neq \psi, \psi^{-1}$, so by Theorem 4 and Theorem 1 we have the set $\overline{\Sigma}_3^1(A)$, as $A = {}^{r}A$, $A \neq {}^{l}A$, $A \neq {}^{s}A$ and ${}^{l}A \neq {}^{r}A$. The converse follows from the form of $\overline{\Sigma}_3^1(A)$ in Theorem 1 as in this case $A = {}^{r}A$, $A \neq {}^{l}A$, $A \neq {}^{s}A$ and so by Theorem 4 $\psi = I, \varphi \neq I$ and $\varphi \neq \psi$ whence $\varphi \neq \psi^{-1}$.

The case of $\overline{\Sigma}_3^2(A)$ is proved analogously. Let $\varphi = \psi, \varphi \neq I$ and at least one of two inequalities $\varphi \neq \psi^{-1}$, $\varphi^3 \neq I$ be fulfilled, then $\psi \neq I$, so by Theorem 4 and Theorem 1 we have the set $\overline{\Sigma}_3^3(A)$, as $A = {}^{s}A$, $A \neq {}^{l}A$, $A \neq {}^{r}A$ and ${}^{l}A \neq {}^{r}A$. The converse follows from the form of $\overline{\Sigma}_3^3(A)$ in Theorem 1 and from Theorem 4.

Let $\varphi, \psi \neq I$, $\varphi \neq \psi$ and at least one of two equalities $\varphi = \psi^{-1}$, $\varphi^3 = I$ be not fulfilled. Then the quasigroup (Q, A) satisfies none of conditions of Theorem 4, so all conjugates of this quasigroup are distinct and $\overline{\Sigma}(A) = \overline{\Sigma}_6(A)$. Conversely, if all conjugates of a quasigroup (Q, A) are different, then by Theorem 4 in (Q, A) $\varphi, \psi \neq I$, $\varphi \neq \psi$ and at least one of two equalities of $\varphi = \psi^{-1}$, $\varphi^3 = I$ is not fulfilled. □

6 *DC*-quasigroups

Consider in more detail the class of quasigroups all six conjugates of which are distinct.

Definition 1. *A quasigroup is called a distinct conjugate quasigroup or, shortly, a DC-quasigroup if all its conjugates are distinct, that is $\mid \overline{\Sigma} \mid = 6$.*

All DC-quasigroups form the class V_6.

Theorem 6. *A quasigroup (Q, A) is a DC-quasigroup if and only if $A \neq {}^{r}A, {}^{l}A, {}^{s}A, {}^{lr}A$. A quasigroup (Q, A) is a DC-quasigroup if and only if it satisfies none of four identities of the set $\overline{T}$.*

Proof. Indeed, by Proposition 1 of [12]
if $A \neq^r A$, then ${}^lA \neq^{lr} A$ and ${}^{rl}A \neq^s A$;
if $A \neq^l A$, then ${}^rA \neq^{rl} A$ and ${}^sA \neq^{lr} A$;
if $A \neq^s A$, then ${}^rA \neq^{lr} A$ and ${}^lA \neq^{rl} A$;
if $A \neq^{lr} A$, then ${}^lA \neq^r A$, ${}^rA \neq^s A$, ${}^{lr}A \neq^{rl} A$, $A \neq^{rl} A$ and ${}^lA \neq^s A$
since the corresponding pairs of conjugates coincide simultaneously. □

Let (Q, A) be a DC-quasigroup, $A = {}^\varepsilon A$ where ε is the identity transformation, $C = \{\varepsilon, r, l, rl, lr, s\}$ be the set of six conjugations, as transformations of a quasigroup (Q, A). On the set C we shall define the operation $(\cdot)$, corresponding to the passage from one conjugate of a quasigroup to another one, taking into account that the multiplication is realized from the right to the left.

We obtain the group $C(\cdot)$ which is isomorphic to the symmetric group S_3 (see [1]). The multiplication table of the group $C(\cdot)$ is the following:

$\cdot$	ε	r	l	rl	lr	s
ε	ε	r	l	rl	lr	s
r	r	ε	rl	l	s	lr
l	l	lr	ε	s	r	rl
rl	rl	s	r	lr	ε	l
lr	lr	l	s	ε	rl	r
s	s	rl	lr	r	l	ε

Tab. 6

In this table rs means that at first s then r are applied, so $rs = rrlr = lr$, and $sr = rlrr = rl$.

The following statement gives some properties of DC-quasigroups.

Proposition 4. *For a DC-quasigroup the group $C(\cdot)$ is isomorphic to the symmetric group S_3.*

Any DC-quasigroup is noncommutative and nontrivial.

Any conjugate of a DC-quasigroup is a DC-quasigroup.

Any quasigroup containing a DC-subquasigroup is a DC-quasigroup.

The direct product of DC-quasigroups is a DC-quasigroup.

The direct product of a TS-quasigroup and a DC-quasigroup is a DC-quasigroup.

The direct product of two quasigroups from distinct classes of $V_2, V_3^1, V_3^2, V_3^3, V_6$ is a DC-quasigroup.

A nontrivial quasigroup which is a homomorphic image of a DC-quasigroup is not necessarily a DC-quasigroup.

Proof. The results follow from the definitions, Theorem 6, the characterization of the classes $V_1, V_2, V_3^1, V_3^2, V_3^3, V_6$ using the identities of the set $\overline{T}$ (see Remark 1) and taking into account that if a quasigroup satisfies an identity, then this identity holds in any its subquasigroup. The last statement is true since, for example, the non-abelian group S_3 which by Corollary 2 is a DC-group has a homomorphic group of order two, which is contained in the class V_1. □

By Theorem 6 of [9] for any $m = 1, 2, 3, 6$ and any $n \geq 4$ there exists a quasigroup of order n with m distinct conjugates. The proof of this theorem for a quasigroup (Q, A) with $| \overline{\Sigma}(A) | = 6$ is based on the existence of a quasigroup of order 3 satisfying none of the identities in the set T. But it is easy to check that such quasigroups do not exist, since six of 12 quasigroups of order 3 are commutative and every of the remaining six quasigroups coincide with the left or the right inverse quasigroup. So below we shall bring in small correction in the proof for the case of quasigroups with $| \overline{\Sigma}(A) | = 6$ using the idea of embedding used in the proof of Theorem 6 [9].

Theorem 7. *For every $n \geq 4$ there exists a DC-quasigroup of order n.*

Proof. It is easy to check that, for example, the quasigroup (Q, A) of order 4 with the following multiplication table:

A	1	2	3	4
1	1	2	3	4
2	2	4	1	3
3	4	3	2	1
4	3	1	4	2

Tab. 7

is a DC-quasigroup. In [7] Trevor Evans has shown that a quasigroup of order n can be embedded in a quasigroup of order t for every $t \geq 2n$. Using the quasigroup of order 4, given above, for embedding we obtain a DC-quasigroup of any order $n \geq 8$ by Proposition 4. The existence of DC-quasigroups of order $n = 5, 7$ follows, for example, from Theorem 8 below (for $n = 5$ see also Example 2 in the end). By Corollary 2 the noncommutative group S_3 of order $n = 6$ is a DC-group. □

Summarizing the above results we have the following DC-loops and DC-quasigroups.

Proposition 5. *A noncommutative loop (Q, A) which is not of exponent two is a DC-loop.*

A noncommutative IP-quasigroup (Q, A) with $I_l = I_r = I$ and $IA(x, y) \neq A(y, x)$ is a DC-quasigroup.

A noncommutative IP-loop (a noncommutative Moufang loop, a non-abelian group) is a DC-loop.

A noncommutative IP-quasigroup with $I_l \neq I_r$ and $I_l, I_r \neq \varepsilon$ is a DC-quasigroup.

A T-quasigroup (Q, A): $A(x, y) = \varphi x + \psi y$ such that $\varphi \neq I, \psi$; $\psi \neq I$ and $\varphi^2 \neq I\psi$ or $\psi^2 \neq I\varphi$ (and $\varphi \neq \psi^{-1}$ or $\varphi^3 \neq I$) is a DC-quasigroup.

Denote by s_n the number of DC-groups of order n, then using Fig. 4.3.4 of [6] with the number of all non-abelian groups of order $n < 32$ we get that $s_6 = s_{10} = s_{14} = s_{21} = s_{22} = s_{26} = s_{27} = 1$; $s_8 = s_{20} = s_{24} = s_{28} = 2$; $s_{12} = s_{18} = s_{30} = 3$; $s_{16} = 9$.

The criterion of Theorem 5 for a DC-T-quasigroup can be reformulated in the following way.

Corollary 3. *A T-quasigroup (Q, A): $A(x, y) = \varphi x + \psi y$ is a DC-quasigroup if and only if $\varphi + \varepsilon \neq \overline{0}$, $\psi + \varepsilon \neq \overline{0}$, $\varphi - \psi \neq \overline{0}$ and $\varphi^2 + \psi \neq \overline{0}$ or $\psi^2 + \varphi \neq \overline{0}$, where $\overline{0}$ is the endomorphism zero of the abelian group $(Q, +)$.*

Indeed, for example, the inequality $\varphi \neq I$ means that $\varphi x_0 \neq I x_0$ for some $x_0 \in Q$, $x_0 \neq 0$, that is $(\varphi x_0 + x_0) \neq 0$, $(\varphi + \varepsilon)x_0 \neq 0$ and $\varphi + \varepsilon \neq \overline{0}$.

An operation A of the form $A(x, y) = ax + by \pmod n$, $n \geq 3$, $a, b \neq 0$, is a T-quasigroup if and only if the numbers a, b modulo n are relatively prime to n. In this case $\varphi = L_a$, $\psi = L_b$, where $L_a x = ax \pmod n$, $x \in Q = \{0, 1, 2, ..., n-1\}$, are permutations (automorphisms of the additive group modulo n). Note that since the elements a, b modulo n are relatively prime to n, then they are invertible and belong to the multiplicative group of the residue-class ring (mod n). This multiplicative group consists of all numbers from 1 to $n-1$ relatively prime to n. In this case $L_a^{-1} x = L_{a^{-1}} x \pmod n$. Taking into account that $I = L_{n-1}$ for such quasigroups we have

Corollary 4. *A T-quasigroup (Q, A): $A(x, y) = ax + by \pmod n$ is a DC-quasigroup if and only if $a, b \neq n-1$, $a \neq b$ and $a \neq b^{-1}$ or $a^3 \neq n-1$ (mod n).*

The following theorem gives some information about the spectrum of DC-T-quasigroups.

Theorem 8. *For any $n \geq 5$, $n \neq 6$, there exists a DC-T-quasigroup of order n.*

Proof. Consider a T-quasigroup (Q, A) with $A(x, y) = x + ky \pmod n$ of order n, $n \geq 5$, $n \neq 6$, such that the greatest common divisor (n, k) is equal to 1 (that is $(n, k) = 1$), $k \neq 1, n-1$, where $1 \cdot x = x \pmod n$. It is easy to see that for any finite $n \geq 5$, $n \neq 6$ the required number k exists. For this quasigroup $a = 1$, $b = k (\mathrm{mod}\ n)$. Check the conditions of Corollary 4: $1, k \neq n-1 \pmod n$, $k \neq 1$ and $1 \neq k^{-1} \pmod n$. Thus, by Corollary 4 all conjugates of the quasigroup (Q, A) are different and it is a DC-T-quasigroup. □

Note that among T-quasigroups (Q, A): $A(x, y) = ax + by \pmod 4$ or $A(x, y) = ax + by \pmod 6$ there are not DC-quasigroups. That follows if we take into account Corollary 4 and that the numbers a, b modulo n are relatively prime to n.

Example 2. Find the conjugates of the DC-T-quasigroup (Q, A) with $A(x, y) = x + 2y \pmod 5$ of order 5, taking into account the form of conjugates of a T-quasigroup:

${}^{s}A(x, y) = \psi x + \varphi y = 2x + y \pmod 5$,

${}^{r}A(x, y) = \psi^{-1}(y - \varphi x) = L_{2^{-1}}(y - x) = 3y - 3x \pmod 5 = 2x + 3y \pmod 5$,

${}^{l}A(x, y) = \varphi^{-1}(x - \psi y) = x - 2y \pmod 5 = x + 3y \pmod 5$,

${}^{rl}A(x, y) = \psi^{-1}(x - \varphi y) = L_{2^{-1}} x - L_{2^{-1}} y = 3x - 3y \pmod 5 = 3x + 2y \pmod 5$,

${}^{lr}A(x, y) = \varphi^{-1}(y - \psi x) = -2x + y \pmod 5 = 3x + y \pmod 5$.

Recall that a quasigroup (Q, A) is called *totally conjugate orthogonal (near totally conjugate orthogonal), shortly, a totCO-quasigroup* [5] *(near totCO-quasigroup,*

respectively [11]) if all six its conjugates (five of its conjugates) are pairwise orthogonal. It is evident that these quasigroups are DC-quasigroups if to take into account that in an orthogonal system all quasigroups are different. In [5] it was proved that for any number n which is relatively prime to 2, 3, 5 and 7 there exists a $totCO$-quasigroup (moreover, a T-quasigroup) of order n.

Note that loops (moreover, quasigroups with right or left identity) and IP-quasigroups can not be $totCO$-quasigroups. That follows, for example, from Proposition 3 of [4] where impossibility of orthogonality of some conjugates for these quasigroups is proved.

References

[1] Belousov V. D. *Foundations of the quasigroup and loop theory,* Moscow, Nauka, 1967 (in Russian).

[2] Belousov V. D. *Parastrophic-orthogonal quasigroups*, Quasigroups and related systems, 2005, **13**, No. 1, 25–72.

[3] Belousov V. D., Florea I. A. *Quasigroups with the property of invertibility*, Izvestiya of Academy of Sciences, Mold. SSR, Ser.fiz.-tehn., 1966, No. 1, 3–17 (in Russian).

[4] Belyavskaya G., Diordiev A. *Conjugate-orthogonality and the complete multiplication group of a quasigroup*, Buletinul Academiei de Ştiinţe a Republicii Moldova, Matematica, 2009, No. 1(59), 22–30.

[5] Belyavskaya G. B., Popovich T. V. *Totally conjugate orthogonal quasigroups and complete graphs*, Fundamental and Applied Mathematics, Moscow, 2010, vol. 16, 35–45 (in Russian).

[6] Dénеš J., Keedwell A. D. *Latin squares and their applications*, Académiai Kiado, Budapest and Academic Press, New York, 1974.

[7] Trevor Evans. *Embedding incomplete latin squares*, Amer. Math. Monthly, 1960, **67**, 958–961.

[8] Kepka T., Nemec P. *T-quasigroups. I* , Acta Universitatis. Carolinae. Math. et Phys., 1971, **12**, No. 1, 39–49.

[9] Lindner C. C., Steedly D. *On the number of conjugates of a quasigroup*, Algebra Univ., 1975, **5**, 191–196.

[10] Mullen G., Shcherbacov V. *On orthogonality of binary operations and squares*, Buletinul Academiei de Ştiinţe a Republicii Moldova, Matematica, 2005, No. 2(48), 3–42.

[11] Popovich T. V. *On parastrophical-orthogonal quasigroups and graphs*, Proceedings of the 10-th Conference "Discrete Mathematics and its Applications", Moscow, 2010, 258–260 (in Russian).

[12] Popovich T. V. *On conjugate sets of quasigroups*, Buletinul Academiei de Ştiinţe a Republicii Moldova, Matematica, 2011, No. 3(67), 69–76.

G. B. Belyavskaya, T. V. Popovich
Institute of Mathematics and Computer Science
Academy of Sciences of Moldova
Academiei str. 5, MD-2028 Chişinău
Moldova

E-mail: *gbel1@rambler.ru, tanea-popovici@mail.ru*

Received June 24, 2011