DISTRIBUTIVE AND TRIMEDIAL QUASIGROUPS OF ORDER 243

PŘEMYSL JEDLIČKA, DAVID STANOVSKÝ, AND PETR VOJTĚCHOVSKÝ

Abstract. We enumerate three classes of non-medial quasigroups of order $243 = 3^5$ up to isomorphism. There are 92 non-medial distributive quasigroups of order 243 (extending the work of Kepka and Němec), 17004 non-medial trimedial quasigroups of order 243 (extending the work of Kepka, Bénéteau and Lacaze), and 6 non-medial distributive Mendelsohn quasigroups of order 243 (extending the work of Donovan, Griggs, McCourt, Opršal and Stanovský).

The enumeration technique is based on affine representations over commutative Moufang loops, automorphism groups of commutative Moufang loops, and computer calculations with the `LOOPS` package in `GAP`.

1. Introduction

Enumeration of quasigroups (equivalently, latin squares) is one of the classical topics of combinatorics. Enumerating all quasigroups of a given order n is a difficult problem already for small values of n. Indeed, the number of latin squares is known only up to $n = 11$ [18], and the number of quasigroups up to isomorphism is known only up to $n = 10$ [17]. Consequently, enumerations of quasigroups usually deal with well-studied classes or varieties.

In this paper we focus on quasigroups that are representable over commutative Moufang loops. More precisely, we enumerate the non-medial algebras of order 243 up to isomorphism in three classes of quasigroups: distributive quasigroups, trimedial quasigroups, and distributive Mendelsohn quasigroups.

In the above classes, the enumeration is interesting only for orders that are powers of 3 (see below). The previous step, $n = 81 = 3^4$, has been completed in 1981 by Kepka and Němec for distributive quasigroups [16], in 1987 by Kepka, Bénéteau and Lacaze for trimedial quasigroups [15], and recently by Donovan, Griggs, McCourt, Opršal and Stanovský [9] for distributive Mendelsohn quasigroups. Our calculations independently verify their enumeration results.

A *quasigroup* is a set Q with a binary operation $+$ such that all left translations $L_x : Q \to Q$, $y \mapsto x + y$ and all right translations $R_x : Q \to Q$, $y \mapsto y + x$ are bijections of Q. A quasigroup $(Q, +)$ is a *loop* if it possesses a neutral element, that is, an element 0 satisfying $0 + x = x + 0 = x$ for all $x \in Q$.

A quasigroup $(Q, +)$ is called *idempotent* if it satisfies the identity

$$x + x = x,$$

2000 *Mathematics Subject Classification.* Primary: 20N05. Secondary: 05B15, 05B07.

Key words and phrases. Distributive quasigroup, trimedial quasigroup, medial quasigroup, entropic quasigroup, commutative Moufang loop, latin square, Mendelsohn triple system, classification, enumeration.

Research partially supported by the GAČR grant 13-01832S (Stanovský), and the Simons Foundation Collaboration Grant 210176 (Vojtěchovský).

medial (also *entropic*) if it satisfies the identity

$$(x+y)+(u+v)=(x+u)+(y+v),$$

and *distributive* if it satisfies the two identities

$$x+(y+z)=(x+y)+(x+z),$$
$$(x+y)+z=(x+z)+(y+z).$$

A quasigroup $(Q,+)$ is *trimedial* (also *terentropic* or *triabelian*) if every three elements of Q generate a medial subquasigroup.

Belousov established the following connection between these three types of quasigroups:

Theorem 1.1 ([1]). *A quasigroup is distributive if and only if it is trimedial and idempotent.*

Historically, distributive and medial quasigroups were one of the first nonassociative algebras studied [8]. Their structure theory has been developed mostly in the 1960s and 1970s: see [3] or [25, Section 3] for an overview. Quasigroups satisfying various forms of self-distributivity were one of the favorite topics of Belousov's school of quasigroup theory [2], and they have connections to other branches of mathematics as well [25, Section 1].

The classification of medial quasigroups is to a large extent a matter of understanding conjugation in the automorphism groups of abelian groups. This is explained in detail in [26], for instance, where one can also find the complete classification of medial quasigroups up to order 63 (up to order 127 with a few gaps). Hou [12] has strong results on the enumeration of idempotent medial quasigroups.

In the present paper, we will focus on *non-medial* trimedial quasigroups, which will require computational tools that are rather different from those of the medial case.

One of the fundamental tools in quasigroup theory is loop isotopy. Affine representations of quasigroups over various classes of loops are particularly useful in the study of quasigroups.

Kepka Theorem 2.9 [14] represents trimedial quasigroups over commutative Moufang loops. It is a generalization of both the Toyoda-Bruck Theorem 2.10 [5, 20, 27] that represents medial quasigroups over abelian groups, and the Belousov-Soublin Theorem 2.11 [1, 24] that represents distributive quasigroups over commutative Moufang loops. Theorem 2.13 [15] solves the isomorphism problem for representations of trimedial quasigroups and forms the basis for our enumeration algorithm.

The class of commutative Moufang loops has attracted attention from the very onset of abstract loop theory. It is only a slight hyperbole to say that the fundamental text of loop theory, Bruck's "A survey of binary systems" [7], has been written largely to develop tools for dealing with commutative Moufang loops.

Every finite commutative Moufang loop decomposes as a direct product of an abelian group of order coprime to 3 and of a commutative Moufang loop of order a power of 3 [6, Theorem 7C].

It was known to Bruck that there are no nonassociative commutative Moufang loops of order less than 3^4. Kepka and Němec [16] classified nonassociative commutative Moufang loops of order 3^4 and 3^5 up to isomorphism: there are two of order 3^4 and six of order 3^5. See [16] for explicit constructions of these commutative Moufang loops, and [4, Theorem IV.3.44] for more results on commutative Moufang loops with a prescribed nilpotence class.

Every automorphism of a commutative Moufang loop decomposes as a direct product of automorphisms of the two coprime components. Therefore, thanks to Kepka Theorem, every finite trimedial quasigroup is a direct product of a medial quasigroup of order coprime to 3 and of a non-medial trimedial quasigroup of order a power of 3. In particular, there are no non-medial trimedial quasigroups of order less than 3^4.

The classification of non-medial distributive quasigroups of order 3^4 was also carried out in [16]; there are 6 such quasigroups up to isomorphism. Non-medial trimedial quasigroups of order 3^4 were enumerated by Kepka, Bénétau and Lacaze in [15]; there are 35 of them up to isomorphism. Both [16] and [15] use affine representations and a careful analysis of the automorphism groups of the two nonassociative commutative Moufang loops of order 3^4, without using computers.

The main result of this paper is a computer enumeration of non-medial distributive quasigroups and non-medial trimedial quasigroups of order 3^5 up to isomorphism; see Table 3. The paper is organized as follows.

In Section 2 we summarize the theoretical results of [16] and [15] that we use in the enumeration. After introducing the notions of 1-central automorphisms and orthomorphisms, we state the representation theorems 2.9–2.11. Theorem 2.13 is an isomorphism theorem for affine representations that covers the situations of Theorems 2.9–2.11. We finish the section with notes on general affine representations and on Steiner and Mendelsohn quasigroups.

In Section 3 we describe in detail our main contribution, the classification algorithm (Theorem 3.3).

In Section 4 we present the results of our calculations; see Tables 2 and 3. We also give a sample of explicit constructions of non-medial distributive quasigroups of order 3^5, covering all non-medial distributive Mendelsohn triple systems of order 3^5.

1.1. **Basic definitions and results.** Loops will be denoted additively. The *center* $Z(Q)$ of a loop Q is the set of all elements of Q that commute and associate with all elements of Q. The *associator subloop* $A(Q)$ of a loop Q is the smallest normal subloop of Q generated by all associators $L^{-1}_{x+(y+z)}((x+y)+z)$. The *automorphism group* of Q will be denoted by $\mathrm{Aut}(Q)$.

A loop Q is *power associative* if any element of Q generates an associative subloop. Every element x of a power associative loop $(Q,+)$ has a two-sided inverse $-x$ satisfying $(-x)+x = 0 = x+(-x)$. We write $x-y$ as a shorthand for $x+(-y)$.

A loop Q is *diassociative* if any two elements of Q generate an associative subloop. Certainly, diassociative loops are power associative. Commutative diassociative loops satisfy the *automorphic inverse property* $-(x+y) = -x-y$.

A loop Q is *Moufang* it it satisfies the identity $x+(y+(x+z)) = ((x+y)+x)+z$. By Moufang's theorem [19], Moufang loops are diassociative. In a commutative Moufang loop $(Q,+)$, $3x \in Z(Q,+)$ for every $x \in Q$ [6].

See [2, 4, 6, 7] for more results on commutative Moufang loops.

2. Affine representation of trimedial quasigroups

2.1. **1-central automorphisms and orthomorphisms.** Let $Q = (Q,+)$ be a loop and $\alpha : Q \to Q$ a mapping. Throughout the paper, denote by $\hat{\alpha}$ the mapping $id + \alpha$, i.e.,

$$\hat{\alpha} : Q \to Q, \quad x \mapsto x + \alpha(x).$$

As in [16, p. 636], we say that α is 1-*central* if $\hat{\alpha}(x) \in Z(Q)$ for every $x \in Q$.

Note that when Q is a loop with two-sided inverses and $\alpha : Q \to Q$ is 1-central, then $x + (-x + \hat{\alpha}(x)) = (x - x) + \hat{\alpha}(x) = \hat{\alpha}(x) = x + \alpha(x)$ implies

$$\alpha(x) = -x + \hat{\alpha}(x),$$

an identity we will use freely.

For a loop Q, let

$$\mathrm{Aut}_C(Q) = \{\alpha \in \mathrm{Aut}(Q) : \alpha \text{ is 1-central}\}$$

be the set of all 1-central automorphisms of Q. Note that $\mathrm{Aut}_C(Q)$ need not be a subgroup of $\mathrm{Aut}(Q)$. When Q is an abelian group then $\mathrm{Aut}_C(Q) = \mathrm{Aut}(Q)$, of course.

Lemma 2.1. *Let $Q = (Q, +, 0)$ be a loop with the automorphic inverse property and let $\alpha : Q \to Q$ be a mapping. Then α is a 1-central endomorphism if and only if $\hat{\alpha}$ is an endomorphism into $Z(Q)$. Moreover,*

$$\mathrm{Ker}(\alpha) = \{x \in Q : \alpha(x) = 0\} = \{x \in Q : \hat{\alpha}(x) = x\} = \mathrm{Fix}(\hat{\alpha}).$$

In particular, if Q is a finite loop with the automorphic inverse property and $\alpha : Q \to Q$ is a mapping, then $\alpha \in \mathrm{Aut}_C(Q)$ if and only if $\hat{\alpha}$ is an endomorphism into $Z(Q)$ with a unique fixed point.

Proof. Suppose that α is a 1-central endomorphism. Then $\hat{\alpha}(x + y) = (x + y) + \alpha(x + y) = (x + y) + (\alpha(x) + \alpha(y)) = (x + y) + ((-x + \hat{\alpha}(x)) + (-y + \hat{\alpha}(y)) = ((x + y) + (-x - y)) + (\hat{\alpha}(x) + \hat{\alpha}(y)) = ((x + y) - (x + y)) + (\hat{\alpha}(x) + \hat{\alpha}(y)) = \hat{\alpha}(x) + \hat{\alpha}(y)$, where we have used the automorphic inverse property.

Conversely, suppose that $\hat{\alpha}$ is an endomorphism into $Z(Q)$. Then $\alpha(x + y) = -(x + y) + \hat{\alpha}(x + y) = (-x - y) + (\hat{\alpha}(x) + \hat{\alpha}(y)) = (-x + \hat{\alpha}(x)) + (-y + \hat{\alpha}(y)) = \alpha(x) + \alpha(y)$, where we have again used the automorphic inverse property.

Note that $\alpha(x) = 0$ if and only if $\hat{\alpha}(x) = x$. The rest is clear. $\square$

As in [13], we say that a bijection α of a loop $(Q, +, 0)$ with two-sided inverses is a (*left*) *orthomorphism* if the mapping $id - \alpha$ is also a bijection of Q.

Remark 2.2. Strictly speaking, orthomorphisms were defined only for finite groups in [13]. Nowadays, researchers routinely work with orthomorphisms in arbitrary groups, but usually use the dual notion of a right orthomorphism ($-id + \alpha$ is a bijection). In loops with the automorphic inverse property, $id - \alpha$ is a bijection if and only if $-id + \alpha$ is a bijection.

An orthomorphism need not be an automorphism. For brevity, we call orthomorphisms that are also automorphisms *orthoautomorphisms*.

For a loop Q with two-sided inverses, let

$$\mathrm{Aut}_{CO}(Q) = \{\alpha \in \mathrm{Aut}_C(Q) : \alpha \text{ is an orthomorphism}\}$$

be the set of all 1-central orthoautomorphisms of Q.

Lemma 2.3. *Let Q be a commutative Moufang loop and let $\alpha : Q \to Q$ be a mapping. Then $\alpha \in \mathrm{Aut}_{CO}(Q)$ if and only if $id - \alpha \in \mathrm{Aut}_{CO}(Q)$.*

Proof. In any diassociative loop we have $id - (id - \alpha) = \alpha$ because $x - (x - \alpha(x)) = \alpha(x)$. It therefore suffices to show that if $\alpha \in \mathrm{Aut}_{CO}(Q)$ then $\beta = id - \alpha \in \mathrm{Aut}_{CO}(Q)$. Suppose that $\alpha \in \mathrm{Aut}_{CO}(Q)$. By Lemma 2.1, $\hat{\alpha}$ is an endomorphism into $Z(Q)$.

For every $x \in Q$ we have $\beta(x) = x - \alpha(x) = x - (-x + \hat{\alpha}(x)) = 2x - \hat{\alpha}(x)$. Hence $\beta(x)+\beta(y) = (2x-\hat{\alpha}(x))+(2y-\hat{\alpha}(y)) = (2x+2y)-(\hat{\alpha}(x)+\hat{\alpha}(y)) = 2(x+y)-\hat{\alpha}(x+y) = \beta(x+y)$, proving that $\beta \in \mathrm{Aut}(Q)$. We also have $\hat{\beta}(x) = x + \beta(x) = 3x - \hat{\alpha}(x) \in Z(Q)$ because $3x \in Z(Q)$, so β is 1-central. Finally, $id - \beta = id - (id - \alpha) = \alpha$ shows that β is an orthomorphism. □

Lemma 2.4. *Let Q be a loop with two-sided inverses. Then the subsets $\mathrm{Aut}_C(Q)$ and $\mathrm{Aut}_{CO}(Q)$ of $\mathrm{Aut}(Q)$ are closed under conjugation by elements of $\mathrm{Aut}(Q)$.*

Proof. Let $\alpha \in \mathrm{Aut}_C(Q)$ and $\xi \in \mathrm{Aut}(Q)$. Certainly, $\alpha^\xi \in \mathrm{Aut}(Q)$. For every $x \in Q$ we have $\widehat{\alpha^\xi}(x) = (id + \alpha^\xi)(x) = (id + \alpha)^\xi(x) = \hat{\alpha}^\xi(x) = \xi^{-1}\hat{\alpha}\xi(x) \in Z(Q)$ since α is 1-central. Therefore α^ξ is 1-central.

If α is also an orthomorphism then $id - \alpha$ is a bijection of Q, hence $id - \alpha^\xi = (id - \alpha)^\xi$ is a bijection of Q, and α^ξ is an orthomorphism. □

2.2. **Affine representations and isomorphism theorems.** For the purposes of this paper, we define quasigroups affine over loops as follows:

Definition 2.5. *Let $(Q,+)$ be a loop, let φ, ψ be automorphisms of $(Q,+)$, and let $c \in Z(Q,+)$. Define a binary operation $*$ on Q by*

$$x * y = \varphi(x) + \psi(y) + c. \tag{2.1}$$

The resulting quasigroup $(Q,*)$ is said to be affine over the loop $(Q,+)$*, it will be denoted by $\mathcal{Q}(Q,+,\varphi,\psi,c)$, and the quintuple $(Q,+,\varphi,\psi,c)$ will be called an* arithmetic form *of $(Q,*)$.*

Remark 2.6. Definition 2.5 can be further generalized by not assuming that c is a central element or, even more generally, that $x * y = (\varphi(x) + c) + (\psi(y) + d)$ for automorphisms φ, ψ and arbitrary elements c, d. On the other hand, it can be specialized by assuming that $c = 0$ (linear case), that $\varphi\psi = \psi\varphi$, or that φ, ψ are 1-central, for instance.

Lemma 2.7. *An affine quasigroup $(Q,*) = \mathcal{Q}(Q,+,\varphi,\psi,c)$ is idempotent if and only if $c = 0$ and $\varphi + \psi = id$.*

Proof. If $(Q,*)$ is idempotent then $x = x * x = \varphi(x) + \psi(x) + c$ for every $x \in Q$. With $x = 0$ we deduce $c = 0$. Then $\varphi(x) + \psi(x) = x$ for every $x \in Q$, so $\varphi + \psi = id$.

Conversely, if $\varphi + \psi = id$ and $c = 0$ then $x * x = \varphi(x) + \psi(x) + c = x$. □

Lemma 2.8. *Let $(Q,*) = \mathcal{Q}(Q,+,\varphi,\psi,c)$ be an affine quasigroup. Then $(Q,*)$ is medial if and only if $(Q,+)$ is an abelian group and $\varphi\psi = \psi\varphi$.*

Proof. Note that $(x * u) * (v * y)$ is equal to

$$(\varphi\varphi(x) + \varphi\psi(u) + \varphi(c)) + (\psi\varphi(v) + \psi\psi(y) + \psi(c)) + c.$$

Since $\varphi(c)$, $\psi(c)$, c are central, we see that $(Q,*)$ is medial if and only if

$$(\varphi\varphi(x) + \varphi\psi(u)) + (\psi\varphi(v) + \psi\psi(y)) = (\varphi\varphi(x) + \varphi\psi(v)) + (\psi\varphi(u) + \psi\psi(y)). \tag{2.2}$$

If $(Q,+)$ is an abelian group and $\varphi\psi = \psi\varphi$ then (2.2) holds.

Conversely, suppose that (2.2) holds. With $x = y = v = 0$ we deduce $\varphi\psi = \psi\varphi$ from (2.2). Then with $x = y = 0$ we deduce $\varphi\psi(u) + \varphi\psi(v) = \varphi\psi(v) + \varphi\psi(u)$, so $(Q,+)$ is commutative. Finally, with $x = 0$ we deduce the identity $r + (s + t) = s + (r + t)$, which, combined with commutativity, yields associativity of $(Q,+)$. □

Theorem 2.9 (Kepka Theorem [14])**.** *A quasigroup is trimedial if and only if it admits an arithmetic form* $(Q,+,\varphi,\psi,c)$*, where* $(Q,+)$ *is a commutative Moufang loop,* φ*,* ψ *are* 1*-central automorphisms, and* $\varphi\psi=\psi\varphi$*.*

Lemmas 2.7, 2.8 and Theorem 1.1 show that Kepka Theorem generalizes both the Toyoda-Bruck Theorem and the Belousov-Soublin Theorem. (Set $(Q,+)$ to be an abelian group to deduce the Toyoda-Bruck Theorem, and set $c=0$ and $\varphi+\psi=id$ to deduce the Belousov-Soublin Theorem.)

Theorem 2.10 (Toyoda-Bruck Theorem [5, 20, 27])**.** *A quasigroup is medial if and only if it admits an arithmetic form* $(Q,+,\varphi,\psi,c)$*, where* $(Q,+)$ *is an abelian group and* $\varphi\psi=\psi\varphi$*.*

Theorem 2.11 (Belousov-Soublin Theorem [1, 24])**.** *A quasigroup is distributive if and only if it admits an arithmetic form* $(Q,+,\varphi,\psi,0)$*, where* $(Q,+)$ *is a commutative Moufang loop,* φ*,* ψ *are* 1*-central automorphisms, and* $\varphi=id-\psi$*.*

Note that in the Belousov-Soublin Theorem the condition $\varphi=id-\psi$ implies that ψ is an orthomorphism. We then of course have $\varphi\psi=(id-\psi)\psi=\psi-\psi^2=\psi(id-\psi)=\psi\varphi$ for free.

We offer a variation of the Belousov-Soublin Theorem which will be used in Section 4:

Proposition 2.12. *A quasigroup is distributive if and only if it is isomorphic to* $(Q,\circ)$*, where* $(Q,+)$ *is a commutative Moufang loop,* ψ *is a* 1*-central orthoautomorphism of* $(Q,+)$*, and* $x\circ y=(2x-y)+\hat{\psi}(y-x)$*.*

Proof. By Lemma 2.3, if $(Q,+)$ is a commutative Moufang loop and $\psi\in\mathrm{Aut}_{CO}(Q,+)$ then $id-\psi\in\mathrm{Aut}_{CO}(Q,+)\subseteq\mathrm{Aut}_{C}(Q,+)$.

It therefore suffices to show that $(x-\psi(x))+\psi(y)=(2x-y)+\hat{\psi}(y-x)$ when $(Q,+)$ is a commutative Moufang loop and $\psi\in\mathrm{Aut}_{CO}(Q,+)$. By Lemma 2.1, $\hat{\psi}$ is an endomorphism into $Z(Q,+)$. Therefore, $(x-\psi(x))+\psi(y)=(2x-\hat{\psi}(x))+(-y+\hat{\psi}(y))=(2x-y)+\hat{\psi}(y)-\hat{\psi}(x)=(2x-y)+\hat{\psi}(y-x)$. □

Let us now state a solution to the isomorphism problem for certain affine representations that cover the representations in Theorems 2.9, 2.10, 2.11.

Theorem 2.13 ([15])**.** *For* $i=1,\,2$*, let* $(Q_i,+_i)$ *be a commutative Moufang loop,* φ_i*,* ψ_i 1*-central automorphisms of* $(Q_i,+_i)$*, and* c_i *a central element of* $(Q_i,+_i)$*. Then the two affine quasigroups* $\mathcal{Q}(Q_1,+_1,\varphi_1,\psi_1,c_1)$*,* $\mathcal{Q}(Q_2,+_2,\varphi_2,\psi_2,c_2)$ *are isomorphic if and only if there is a loop isomorphism* $f:(Q_1,+_1)\to(Q_2,+_2)$ *and* $u\in\mathrm{Im}(id-_1(\varphi_1+_1\psi_1))$ *such that* $\varphi_2=f\varphi_1f^{-1}$*,* $\psi_2=f\psi_1f^{-1}$*, and* $c_2=f(c_1+_1u)$*.*

Remark 2.14. The original formulation of the isomorphism test in Theorem 2.13 is somewhat different in [15]. Namely, the condition is replaced with: *There is a loop isomorphism* $f:(Q_1,+_1)\to(Q_2,+_2)$ *and* $w\in Q_2$ *such that*

$$\varphi_2f=f\varphi_1,\quad \psi_2f=f\psi_1,\quad f(c_1)-_2c_2=w-_2(\varphi_2(w)+_2\psi_2(w)).$$

We claim that this condition is equivalent to the condition of Theorem 2.13. First, because "to be isomorphic" is a symmetric relation, we can replace the above condition with: *There is a loop isomorphism* $f:(Q_2,+_2)\to(Q_1,+_1)$ *and* $w\in Q_1$ *such that*

$$\varphi_1f=f\varphi_2,\quad \psi_1f=f\psi_2,\quad f(c_2)-_1c_1=w-_1(\varphi_1(w)+_1\psi_1(w)).$$

Upon considering f^{-1}, we can further replace it with the statement: *There is a loop isomorphism $f:(Q_1,+_1)\to(Q_2,+_2)$ and $w\in Q_1$ such that*

$$\varphi_1 f^{-1}=f^{-1}\varphi_2,\quad \psi_1 f^{-1}=f^{-1}\psi_2,\quad f^{-1}(c_2)-_1 c_1=w-_1(\varphi_1(w)+_1\psi_1(w)).$$

The condition on c_2 is then equivalent to $c_2=f(c_1+_1 w-_1(\varphi_1(w)+\psi_1(w)))$, which says that $c_2=f(c_1+_1 u)$ for some $u\in\mathrm{Im}(id-_1(\varphi_1+_1\psi_1))$.

Note that in the distributive case ($c=0$ and $\varphi+\psi=id$), the isomorphism test of Theorem 2.13 reduces to: *There is a loop isomorphism $f:(Q_1,+_1)\to(Q_2,+_2)$ such that $\psi_2=f\psi_1 f^{-1}$.*

2.3. **Commuting 1-central automorphisms.** Our computational results show that, surprisingly, for some small nonassociative commutative Moufang loops Q, any two 1-central automorphisms of Q commute. This is partly explained by Proposition 2.16.

Lemma 2.15. *Let $(Q,+)$ be a commutative Moufang loop and let φ, ψ be 1-central automorphisms of $(Q,+)$. Then $\varphi\psi=\psi\varphi$ if and only if $\hat{\varphi}\hat{\psi}=\hat{\psi}\hat{\varphi}$.*

Proof. We must proceed carefully since the addition of mappings on $(Q,+)$ is not necessarily an associative operation. However, for any $\alpha\in\mathrm{Aut}_C(Q,+)$ and β, $\gamma\in\mathrm{Aut}(Q,+)$ we have $\hat{\alpha}+(\beta+\gamma)=(\hat{\alpha}+\beta)+\gamma$ because $\mathrm{Im}(\hat{\alpha})\subseteq Z(Q,+)$. In particular, we have

$$\hat{\psi}+\varphi=\hat{\psi}+\hat{\varphi}-id=\hat{\varphi}+\hat{\psi}-id=\hat{\varphi}+\psi. \tag{2.3}$$

Now, $\hat{\varphi}\hat{\psi}=(id+\varphi)\hat{\psi}=\hat{\psi}+\varphi\hat{\psi}=\hat{\psi}+\varphi+\varphi\psi$ and, by symmetry, $\hat{\psi}\hat{\varphi}=\hat{\varphi}+\psi+\psi\varphi$. Thanks to (2.3), we see that φ and ψ commute if and only if $\hat{\varphi}$ and $\hat{\psi}$ commute. □

Proposition 2.16. *Let Q be a nonassociative commutative Moufang loop of order a power of 3 such that $Z(Q)$ is cyclic and $Q/Z(Q)$ is associative. Then any two 1-central automorphisms of Q commute.*

Proof. Let φ, ψ be 1-central automorphisms of $Q=(Q,+)$. By Lemma 2.15, it suffices to show that $\hat{\varphi}\hat{\psi}=\hat{\psi}\hat{\varphi}$.

By Lemma 2.1, $\hat{\varphi}$ and $\hat{\psi}$ are endomorphism into $Z(Q)$. Any endomorphism into $Z(Q)$ has all associators $(x+(y+z))-((x+y)+z)$ in its kernel, and thus vanishes on the associator subloop $A(Q)$. Since $Z(Q)$ is cyclic, there are integers a, b such that $\hat{\varphi}(z)=az$, $\hat{\psi}(z)=bz$ for every $z\in Z(Q)$.

By our assumption, $Q/Z(Q)$ is associative and $0<A(Q)$. Thus $0<A(Q)<Z(Q)$ and the restriction of each of $\hat{\varphi}$, $\hat{\psi}$ onto $Z(Q)$ has nontrivial kernel. Since $|Z(Q)|$ is a power of 3, it follows that 3 divides a and b. Then ax, $bx\in Z(Q)$ for every $x\in Q$, and we calculate

$$\hat{\varphi}\hat{\psi}(x)=a\hat{\psi}(x)=\hat{\psi}(ax)=bax=abx=\hat{\varphi}(bx)=b\hat{\varphi}(x)=\hat{\psi}\hat{\varphi}(x)$$

for every $x\in Q$. □

Every commutative Moufang loop of order $\leq 3^5$ is centrally nilpotent of class at most two [16, Lemma 1.6]. Both of the nonassociative commutative Moufang loops of order 3^4 have cyclic centers, and so do two of the six nonassociative Moufang loops of order 3^5 (see Table 1). Proposition 2.16 therefore applies to these loops. However, Proposition 2.16 does not tell the whole story, as there is a commutative Moufang loop of order 3^5 that has a non-cyclic center yet any two of its 1-central automorphisms commute.

2.4. **Quasigroups corresponding to triple systems.** Certain distributive quasigroups correspond to interesting combinatorial designs, such as Hall triple systems (these are the *distributive Steiner quasigroups*), or distributive Mendelsohn triple systems (the *distributive Mendelsohn quasigroups*); see [9] for details. The classification of the respective quasigroups directly translates into the classification of the corresponding triple systems.

Non-medial distributive Mendelsohn quasigroups were enumerated up to order 3^4 in [9], and non-medial distributive Steiner triple systems were enumerated up to order 3^6 in [3]. In the present paper, we extend the classification in the Mendelsohn case to order 3^5. The following simple criterion identifies the relevant quasigroups in our classification results.

Proposition 2.17 ([9, Proposition 2.1]). *Let $(Q,+)$ be a commutative Moufang loop and let $\psi \in \mathrm{Aut}_{CO}(Q,+)$. The corresponding distributive quasigroup $\mathcal{Q}(Q,+,id-\psi,\psi,0)$ is:*

(i) *Steiner if and only if $(Q,+)$ has exponent 3 and $\psi(x)=-x$ for every $x\in Q$;*
(ii) *Mendelsohn if and only if $\psi^2(x)-\psi(x)+x=0$ for every $x\in Q$.*

Remark 2.18. In a commutative Moufang loop we have $(x+y)+z=0$ if and only if $x+(y+z)=0$, so it is not necessary to specify the order of addition in the expression $\psi^2(x)-\psi(x)+x$ above.

Corollary 2.19. *Let $(Q,+)$ be a commutative Moufang loop and let $\psi\in\mathrm{Aut}_{CO}(Q,+)$. The corresponding distributive quasigroup $\mathcal{Q}(Q,+,id-\psi,\psi,0)$ is:*

(i) *Steiner if and only if $(Q,+)$ has exponent 3 and $\hat{\psi}=0$;*
(ii) *Mendelsohn if and only if $\hat{\psi}^2(x)-3\hat{\psi}(x)+3x=0$ for every $x\in Q$.*

Proof. Part (i) is obvious. For (ii), we calculate $\psi^2-\psi+id=(-id+\hat{\psi})^2-(-id+\hat{\psi})+id=\hat{\psi}^2-3\hat{\psi}+3id$. □

In particular, if a commutative Moufang loop $(Q,+)$ has exponent 3 then the corresponding distributive quasigroup is Steiner if and only if $\hat{\psi}=0$, and it is Mendelsohn if and only if $\hat{\psi}^2=0$.

3. The classification algorithm

3.1. **Outline of the algorithm.** For the purposes of this classification, let us call an affine quasigroup $\mathcal{Q}(Q,+,\varphi,\psi,c)$ of Definition 2.5 *1-central* if the automorphisms φ, ψ are 1-central. (In particular, quasigroups that are 1-central over abelian groups are precisely the central quasigroups [26].)

Theorem 2.13 suggests the following algorithm for the classification of 1-central quasigroups $\mathcal{Q}(Q,+,\varphi,\psi,c)$ over commutative Moufang loops.

Let $Q=(Q,+)$. We calculate the set $\mathrm{Aut}_C(Q)\times\mathrm{Aut}_C(Q)\times Z(Q)$ and filter it subject to the equivalence induced by the condition in Theorem 2.13. To obtain trimedial quasigroups, we consider only triples (φ,ψ,c) satisfying $\varphi\psi=\psi\varphi$. To obtain distributive quasigroups, we consider only triples (φ,ψ,c) satisfying $c=0$ and $\varphi+\psi=id$.

To complete the classification for a fixed order n, it suffices to consider the disjoint union of the classifications obtained for each of the commutative Moufang loops of order n because isomorphic 1-central quasigroups have isomorphic underlying loops, cf. Theorem 2.13. To obtain non-medial quasigroups, we consider only nonassociative loops, cf. Lemma 2.8.

Essentially the same idea was used in [15, 16] to classify trimedial and distributive quasigroups of order $3^4 = 81$ by hand. Manual classification is out of the question for order 3^5, and even straightforward computer calculation is insufficient since the size of the set $\mathrm{Aut}_C(Q) \times \mathrm{Aut}_C(Q) \times Z(Q)$ is of the magnitude 10^8 for some of the loops under consideration.

In the rest of this section we describe how to speed up the algorithm. We start with general ideas that can be used for any order.

3.2. **Calculating 1-central automorphisms.** We do not calculate the set $\mathrm{Aut}_C(Q)$ directly by filtering $\mathrm{Aut}(Q)$ because $\mathrm{Aut}(Q)$ can be large. Instead, we use an incremental approach. Let

$$H(Q) = \{\alpha \in \mathrm{Aut}(Q) : \ \alpha(x) + x \in Z(Q) \text{ or } \alpha(x) - x \in Z(Q) \text{ for every } x \in Q\}.$$

We clearly have $\mathrm{Aut}_C(Q) \subseteq H(Q)$ and it is not hard to check that $H(Q)$ is a subgroup of $\mathrm{Aut}(Q)$ (unlike $\mathrm{Aut}_C(Q)$).

The standard algorithm for calculating automorphisms of a given algebraic structure attempts to extend a partial map defined on a fixed generating set into an automorphism, while employing various isomorphism invariants to restrict possible images of the generators. Modifying this algorithm, we can calculate a (small) subgroup of $\mathrm{Aut}(Q)$ containing $H(Q)$ as follows. Let X be a set of generators of Q used in the search. Whenever a choice is being made for the image of $x \in X$, restrict the choice to the cosets $\pm x + Z(Q)$. Since we enforce this condition only for generators, the algorithm can yield a subgroup G of $\mathrm{Aut}(Q)$ properly containing $H(Q)$. We can then filter the elements of G to obtain $H(Q)$ and, in turn, $\mathrm{Aut}_C(Q)$ and $\mathrm{Aut}_{CO}(Q)$.

To finish the classification of *distributive* quasigroups, various subgroups U of $\mathrm{Aut}(Q)$ can be used to filter $\mathrm{Aut}_{CO}(Q)$ up to conjugacy in U (which makes sense thanks to Lemma 2.4). This is not necessarily as powerful as the conjugacy in the entire group $\mathrm{Aut}(Q)$, but it reduces the number of elements of $\mathrm{Aut}_{CO}(Q)$ to be considered in the final stage, where we employ the entire $\mathrm{Aut}(Q)$ to finish the classification. In our implementation, we used for U the pointwise stabilizer of $Z(Q)$ in $\mathrm{Aut}(Q)$.

3.3. **Calculating the action on $\mathrm{Aut}_C(Q) \times \mathrm{Aut}_C(Q) \times Z(Q)$.** For trimedial quasigroups, we must find a way to handle the equivalence on $\mathrm{Aut}_C(Q) \times \mathrm{Aut}_C(Q)$ and the relation between c_1 and c_2 in the isomorphism test of Theorem 2.13.

Consider any group G and a subset $X \subseteq A$ closed under conjugation in A. (Later we will take $G = \mathrm{Aut(Q)}$ and $X = \mathrm{Aut}_C(Q)$, cf. Lemma 2.4.) Then G acts on $X \times X$ by simultaneous conjugation in both coordinates, i.e., $(\alpha, \beta)^\gamma = (\alpha^\gamma, \beta^\gamma)$. To calculate orbits on $X \times X$, we take advantage of the following well-known result.

Lemma 3.1. *Let G be a group acting on a set X. Let O be the set of orbit representatives of the action, and for every $x \in O$ let O_x be the set of orbit representatives of the action of the stabilizer G_x of x on X. Then*

$$\{(a, b) : a \in O,\, b \in O_a\}$$

is a complete set of orbit representatives of the action of G on $X \times X$ given by $(x, y)^g = (x^g, y^g)$.

Proof. For every $(x, y) \in X \times X$ there is a unique $a \in O$ and some $z \in X$ such that (x, y) and (a, z) are in the same orbit. For a fixed $a \in O$ and some u, $v \in X$, we have (a, u) in the same orbit as (a, v) if and only if u, v belong to the same orbit of G_a. $\square$

Lemma 3.2. *Let $Q = (Q, +)$ be a commutative Moufang loop, let $A = \mathrm{Aut}(Q)$, and let α, $\beta \in \mathrm{Aut}_C(Q)$. Then $C_A(\alpha) \cap C_A(\beta)$ acts naturally on $Z(Q)/\mathrm{Im}(id - (\alpha + \beta))$.*

Proof. Let $I = \mathrm{Im}(id - (\alpha + \beta))$. First, we note that $I \leq Z(Q)$. Indeed, for every $x \in Q$, we have

$$x - (\alpha(x) + \beta(x)) = x - ((-x + \hat{\alpha}(x)) + (-x + \hat{\beta}(x))) = 3x - (\hat{\alpha}(x) + \hat{\beta}(x)) \in Z(Q),$$

because $3x \in Z(Q)$ and α, β are 1-central.

It remains to show that for every $\gamma \in C_A(\alpha) \cap C_A(\beta)$ the mapping $u + I \mapsto \gamma(u) + I$ is well-defined. Suppose that $u + I = v + I$ for some u, $v \in Z(Q)$. Then $u = v + (x - (\alpha(x) + \beta(x)))$ for some $x \in Q$, and we have

$$\begin{aligned} \gamma(u) &= \gamma(v) + (\gamma(x) - (\gamma\alpha(x) + \gamma\beta(x))) \\ &= \gamma(v) + (\gamma(x) - (\alpha\gamma(x) + \beta\gamma(x))) \\ &= \gamma(v) + (id - (\alpha + \beta))(\gamma(x)) \in \gamma(v) + I, \end{aligned}$$

finishing the proof. $\square$

We can now reformulate Theorem 2.13 so that it can be used directly in the enumeration of quasigroups that are 1-central over a given commutative Moufang loop. (A similar theorem for abelian groups was obtained by Drápal [10, Theorem 3.2] and used as an enumeration tool in [26].)

Theorem 3.3. *Let $Q = (Q, +)$ be a commutative Moufang loop and let $A = \mathrm{Aut}(Q)$. The isomorphism classes of 1-central quasigroups over Q (resp. trimedial quasigroups over Q) are in one-to-one correspondence with the elements of the set*

$$\{(\varphi, \psi, c) : \varphi \in X,\ \psi \in Y_\varphi,\ c \in Z_{\varphi,\psi}\},$$

where

- *X is a complete set of orbit representatives of the conjugation action of A on $\mathrm{Aut}_C(Q)$;*
- *Y_φ is a complete set of orbit representatives of the conjugation action of $C_A(\varphi)$ on $\mathrm{Aut}_C(Q)$ (resp. on $\mathrm{Aut}_C(Q) \cap C_A(\varphi)$), for every $\varphi \in X$;*
- *$Z_{\varphi,\psi}$ is a complete set of orbit representatives of the natural action of $C_A(\varphi) \cap C_A(\psi)$ on $Z(Q)/\mathrm{Im}(id - (\varphi + \psi))$.*

Proof. Consider the equivalence relation of $\mathrm{Aut}_C(Q) \times \mathrm{Aut}_C(Q) \times Z(Q)$ implicitly defined by Theorem 2.13. By Lemma 3.1, it remains to describe when two triples (φ, ψ, c_1) and (φ, ψ, c_2) are equivalent, where $\varphi \in X$, $\psi \in Y_\varphi$ and c_1, $c_2 \in Z(Q)$.

Let $I = \mathrm{Im}(id - (\varphi + \psi))$. Using Lemma 3.2, for any $\gamma \in \mathrm{Aut}(Q)$ we have $c_2 = \gamma(c_1 + u)$ for some $u \in I$ if and only if $c_2 \in \gamma(c_1 + I) = \gamma(c_1) + I$, which is equivalent to $c_2 + I = \gamma(c_1) + I = \gamma(c_1 + I)$. $\square$

3.4. **Calculating with loops of order 243.** Recall that all six commutative Moufang loops of order 243 were constructed by Kepka and Němec [16]. Moufang loops of order 81 were classified by Nagy and Vojtěchovský in [22], and Moufang loops of order 243 were classified by Slattery and Zenisek in [23].

The 71 nonassociative Moufang loops of order 243 can be found in the `LOOPS` [21] package for `GAP` [11] and can be obtained by calling `MoufangLoop(243,i)`. The six nonassociative commutative Moufang loops correspond to the indices $i \in \{1, 2, 5, 56, 57, 67\}$.

The default method in `LOOPS` for calculating automorphism groups of loops is powerful enough to calculate automorphism groups of Moufang loops of order 81 and even of some Moufang loops of order 243. We adopted the default algorithm, made a better use of global variables and ran it with different choices of generators (to which the algorithm is highly sensitive). We succeeded in calculating the automorphism groups for the six commutative Moufang loops of order 243. The longest calculation, for `MoufangLoop(243,5)`, took several hours.

The calculation of the sets $\mathrm{Aut}_C(Q)$ and $\mathrm{Aut}_{CO}(Q)$ and of the respective actions of the automorphism group was described in the previous two subsections.

To get a feel for the complexity of the calculations, the sizes of the various sets of automorphisms encountered during the enumeration can be found in Table 1. Here X/G denotes the number of orbits of the action of a group G on a set X (where the action is as described above). The loop notation n/k refers to `MoufangLoop(n,k)`.

Q	243/1	243/2	243/5	243/56	243/57	243/67
exponent of Q	9	27	9	3	9	9
$Z(Q)$	C_3^2	C_9	C_3^2	C_3^2	C_3^2	C_9
size of $A = \mathrm{Aut}(Q)$	629856	34992	78732	49128768	1889568	909792
$\lvert\mathrm{Aut}_C(Q)\rvert$	729	81	729	4374	4374	81
$\lvert\mathrm{Aut}_C(Q)/A\rvert$	16	12	38	8	18	6
$\lvert\mathrm{Aut}_C(Q)^2/A\rvert$	1827	207	11061	283	2146	54
$\lvert(\mathrm{Aut}_C(Q)^2 \times Z(Q))/A\rvert$	2310	288	13056	375	2537	114
$\lvert\mathrm{Aut}_{CO}(Q)\rvert$	729	81	729	2187	2187	81
$\lvert\mathrm{Aut}_{CO}(Q)/A\rvert$	16	12	38	6	14	6

TABLE 1. Sizes of various subsets of automorphisms that appear in the classification.

4. Results

4.1. **Enumeration.** Let $c(Q)$ denote the number of 1-central quasigroups, $t(Q)$ the number of trimedial quasigroups, $d(Q)$ the number of distributive quasigroups, $dM(Q)$ the number of distributive Mendelsohn quasigroups, and $dS(Q)$ the number of distributive Steiner quasigroups over a loop Q, up to isomorphism.

Table 2 displays these numbers for every nonassociative commutative Moufang loop of order 81 and 243. The entries for order 81 can be found already in [9, 15, 16] and have been independently verified by our calculations. The entries in the last row can be found in [3] and have also been independently verified. The remaining entries for order 243 are new.

Since all the commutative Moufang loops in the table are nonassociative, the corresponding quasigroups are non-medial by Lemma 2.8.

Q	81/1	81/2	243/1	243/2	243/5	243/56	243/57	243/67
$c(Q)$	8	27	2310	288	13056	375	2537	114
$t(Q)$	8	27	2310	288	13056	165	1071	114
$d(Q)$	2	4	16	12	38	6	14	6
$dM(Q)$	2	0	0	0	0	5	1	0
$dS(Q)$	1	0	0	0	0	1	0	0

TABLE 2. Enumeration of various classes of affine quasigroups over a given commutative Moufang loop.

In Table 3 we summarize the results of Table 2 by order, and we use notation analogous to that of Table 2. For instance, $t(n)$ denotes the number of *non-medial* trimedial quasigroups of order n up to isomorphism. Note that we have *not* enumerated non-medial 1-central quasigroups of order 243, since this would require also the enumeration of all quasigroups $\mathcal{Q}(Q,+,\varphi,\psi,c)$, where $(Q,+)$ is an abelian group of order 243 and φ, ψ are non-commuting automorphisms of $(Q,+)$; a difficult task. Finally, see [26] for an enumeration of medial quasigroups up to order 63.

n	3^3	3^4	3^5	3^6
$t(n)$	0	35	17004	?
$d(n)$	0	6	92	?
$dM(n)$	0	2	6	?
$dS(n)$	0	1	1	3

TABLE 3. Enumeration of various classes of non-medial quasigroups for a given order.

4.2. **Explicit constructions.** Detailed results of the enumeration, including arithmetical forms for all the quasigroups, can be obtained from the third author upon request.

To present a sample of the detailed results, we now give explicit formulas for all elements of $\mathrm{Aut}_{CO}(Q)$ up to conjugacy in $\mathrm{Aut}(Q)$, where Q is `MoufangLoop(243,`i`)` with $i = 56$ or $i = 57$. As a consequence, we obtain an explicit description of all non-medial distributive Mendelsohn triple systems of order 243 (cf. Table 3).

Example 4.1. According to [16], the loop `MoufangLoop(81,1)` is isomorphic to $(\mathbb{Z}_3^4,+)$, where

$$(a_1,b_1,c_1,d_1)+(a_2,b_2,c_2,d_2)=(a_1+a_2+(d_1-d_2)(b_1c_2-c_1b_2),b_1+b_2,c_1+c_2,d_1+d_2).$$

Then $Q =$ `MoufangLoop(243,56)` is the direct product `MoufangLoop(81,1)` $\times\,\mathbb{Z}_3$. The associator subloop is $A(Q)=\mathbb{Z}_3\times 0\times 0\times 0\times 0$ and the center is $Z(Q)=\mathbb{Z}_3\times 0\times 0\times 0\times \mathbb{Z}_3$.

The elements of $\mathrm{Aut}_{CO}(Q)$ up to conjugacy by $\mathrm{Aut}(Q)$ are given by the following six endomorphisms into the center:

$$\hat{\psi}_1 : (a,b,c,d,e) \mapsto (0,0,0,0,0), \qquad \hat{\psi}_2 : (a,b,c,d,e) \mapsto (b,0,0,0,0),$$
$$\hat{\psi}_3 : (a,b,c,d,e) \mapsto (e,0,0,0,0), \qquad \hat{\psi}_4 : (a,b,c,d,e) \mapsto (0,0,0,0,b),$$
$$\hat{\psi}_5 : (a,b,c,d,e) \mapsto (b,0,0,0,c), \qquad \hat{\psi}_6 : (a,b,c,d,e) \mapsto (e,0,0,0,b).$$

It is straightforward to check that each of these mappings is an endomorphism into the center with a unique fixed point, and that all $id - \psi_i = 2id - \hat{\psi}_i$ are permutations. By Lemma 2.1, $\psi_i \in \mathrm{Aut}_{CO}(Q)$ for every i.

To check that the six mappings are pairwise non-conjugate, we use the following criterion: *Let $\alpha \in \mathrm{End}(Q)$ and $\xi \in \mathrm{Aut}(Q)$. If H is characteristic subloop of Q, we have $\alpha^\xi(H) = \xi\alpha(H)$. If both H and $\alpha(H)$ are characteristic subloops of Q then $\alpha(H) = \alpha^\xi(H)$.* Now observe that:

- $\mathrm{Im}(\hat{\psi}_1) = 0$,
- $\mathrm{Im}(\hat{\psi}_2) = A(Q)$ and $\hat{\psi}_2(Z(Q)) = 0$,
- $\mathrm{Im}(\hat{\psi}_3) = A(Q)$ and $\hat{\psi}_3(Z(Q)) \neq 0$,
- $\mathrm{Im}(\hat{\psi}_4)$ is neither $A(Q)$, nor $\neq Z(Q)$,
- $\mathrm{Im}(\hat{\psi}_5) = Z(Q)$ and $\hat{\psi}_5(Z(Q)) = 0$,
- $\mathrm{Im}(\hat{\psi}_6) = Z(Q)$ and $\hat{\psi}_6(Z(Q)) \neq 0$.

Example 4.2. According to [16], the loop `MoufangLoop(81,2)` is isomorphic to $(\mathbb{Z}_3^2 \times \mathbb{Z}_9, +)$, where

$$(a_1, b_1, c_1) + (a_2, b_2, c_2) = (a_1 + a_2, b_1 + b_2, c_1 + c_2 + 3(c_1 - c_2)(a_1 b_2 - b_1 a_2)).$$

Then $Q =$ `MoufangLoop(243,57)` is the direct product `MoufangLoop(81,2)` $\times \mathbb{Z}_3$. The associator subloop is $A(Q) = 0 \times 0 \times 3\mathbb{Z}_9 \times 0$ and the center is $Z(Q) = 0 \times 0 \times 3\mathbb{Z}_9 \times \mathbb{Z}_3$.

The elements of $\mathrm{Aut}_{CO}(Q)$ up to conjugacy by $\mathrm{Aut}(Q)$ are given by the following endomorphisms into the center:

$$\hat{\psi}_1 : (a,b,c,d) \mapsto (0,0,0,0), \qquad \hat{\psi}_2 : (a,b,c,d) \mapsto (0,0,3c,0),$$
$$\hat{\psi}_3 : (a,b,c,d) \mapsto (0,0,6c,0), \qquad \hat{\psi}_4 : (a,b,c,d) \mapsto (0,0,3d,0),$$
$$\hat{\psi}_5 : (a,b,c,d) \mapsto (0,0,3a,0), \qquad \hat{\psi}_6 : (a,b,c,d) \mapsto (0,0,0,a),$$
$$\hat{\psi}_7 : (a,b,c,d) \mapsto (0,0,0,c \bmod 3), \qquad \hat{\psi}_8 : (a,b,c,d) \mapsto (0,0,3a,b),$$
$$\hat{\psi}_9 : (a,b,c,d) \mapsto (0,0,3c,a), \qquad \hat{\psi}_{10} : (a,b,c,d) \mapsto (0,0,6c,a),$$
$$\hat{\psi}_{11} : (a,b,c,d) \mapsto (0,0,3a,c \bmod 3), \qquad \hat{\psi}_{12} : (a,b,c,d) \mapsto (0,0,3d,a),$$
$$\hat{\psi}_{13} : (a,b,c,d) \mapsto (0,0,3d,c \bmod 3), \qquad \hat{\psi}_{14} : (a,b,c,d) \mapsto (0,0,3d,2c \bmod 3).$$

Again, it is straightforward to check that the corresponding mappings ψ_i belong to $\mathrm{Aut}_{CO}(Q)$. To show that they are pairwise non-conjugate, first notice that $\hat{\psi}_1 = 0$, $\hat{\psi}_2 = 3id$ and $\hat{\psi}_3 = 6id$, so they commute with any automorphism. To distinguish the remaining mappings, consider also the characteristic subloop $B = \{x \in Q : x^3 = 1\} = \mathbb{Z}_3 \times \mathbb{Z}_3 \times 3\mathbb{Z}_9 \times \mathbb{Z}_3$ and observe that

- $\mathrm{Im}(\hat{\psi}_i) = A(Q)$ iff $i = 4, 5$; here $\hat{\psi}_5(Z(Q)) = 0$ but $\hat{\psi}_4(Z(Q)) \neq 0$;

- $\mathrm{Im}(\hat{\psi}_i)$ is of order 3 but not $A(Q)$ iff $i = 6, 7$; here $\hat{\psi}_7(B) = 0$ but $\hat{\psi}_6(B) \neq 0$,
- $\mathrm{Im}(\hat{\psi}_i) = Z(Q)$ for $i = 8, \ldots, 14$;
  - $\hat{\psi}_i(Z(Q)) = 0$ for $i = 8, 9, 10, 11$, but
    * $\hat{\psi}_8(B) = Z(Q)$,
    * $\hat{\psi}_{11}(B) = A(Q)$,
    * both $\hat{\psi}_9(B), \hat{\psi}_{10}(B)$ have order 3, $\neq A(Q)$; we have $\hat{\psi}_9 = \hat{\psi}_2 + \hat{\psi}_6$ and if there existed ξ such that $\hat{\psi}_9^{\xi} = \hat{\psi}_{10}$ then $\hat{\psi}_6^{\xi} = \hat{\psi}_{10} - \hat{\psi}_2 = \hat{\psi}_9$ which is impossible;
  - $\hat{\psi}_i(Z(Q)) = A(Q)$ for $i = 12, 13, 14$, but
    * $\hat{\psi}_{12}(B) = Z(Q)$,
    * $\hat{\psi}_{13}(B) = \hat{\psi}_{14}(B) = A(Q)$; they cannot be conjugate, because their squares, $\hat{\psi}_{13}^2 = \hat{\psi}_2$ and $\hat{\psi}_{14}^2 = \hat{\psi}_3$, are not.

Which of these quasigroups give rise to distributive Mendelsohn triple systems? According to Corollary 2.19:

- for $Q =$ `MoufangLoop(243,56)` whose exponent is 3, these are precisely the mappings $\hat{\psi}_i$ with $\hat{\psi}_i^2 = 0$, which is the case for $i = 1, 2, 3, 4, 5$.
- for $Q =$ `MoufangLoop(243,57)`, since $3Z(Q) = 0$, the equation is equivalent to $\hat{\psi}_i^2 = -3id$, which is satisfied only for $i = 14$.

Recall that (see Proposition 2.12) the triple systems are defined on Q by

$$\{(x,\, y,\, 2x - y + \hat{\psi}(y - x)) :\; x,\, y \in Q\},$$

from which explicit formulas for the triples can be derived.

Acknowledgement

We thank Prof. Anthony Evans for historical comments on orthomorphisms.

References

[1] V. D. Belousov, *On structure of distributive quasigroups.* Mat. Sb. (N.S.) **50**(**92**) (1960), 267–298 (Russian).

[2] V. D. Belousov, *Fundametals of the theory of quasigroups and loops.* Nauka, Moskva (1967) (Russian).

[3] L. Bénéteau, *The geometry of distributive quasigroups.* Rend. Semin. Math. Brescia **7** (1984), 57–65.

[4] L. Bénéteau, *Commutative Moufang loops and related groupoids.* in: O. Chein, H. O. Pflugfelder, J. D. H. Smith (eds.), *Quasigroups and Loops: Theory and Applications.* Sigma Series in Pure Math. **9**, Heldermann Verlag (1990), 115–142.

[5] R.H. Bruck, *Some results in the theory of quasigroups.* Trans. Amer. Math. Soc. **55** (1944), 19–52.

[6] R.H. Bruck, *Contributions to the Theory of Loops.* Trans. Amer. Math. Soc. **60** (1946), no. **2**, 245–354.

[7] R. H. Bruck, *A Survey of Binary Systems.* Third printing, corrected, Ergebnisse der Mathematik und ihrer Grenzgebiete, Springer Verlag, New York-Heidelberg-Berlin, 1971.

[8] C. Burstin, W. Mayer, *Distributive Gruppen von endlicher Ordnung.* J. reine und angew. Math. **160** (1929), 111–130 (German).

[9] D. Donovan, T. Griggs, T. McCourt, J. Opršal, D. Stanovský, *Distributive and anti-distributive Mendelsohn triple systems.* To appear in Canad. Math. Bulletin.

[10] A. Drápal, *Group isotopes and a holomorphic action.* Result. Math. **54** (2009), no. **3**–**4**, 253–272.

[11] The GAP Group, GAP – Groups, Algorithms, and Programming, Version 4.5.5; 2012. `http://www.gap-system.org`

[12] X. Hou, *Finite modules over* $\mathbb{Z}[t, t^{-1}]$. J. Knot Theory Ramifications **21/8** (2012), 1250079, 28 pp.
[13] D.M. Johnson, A.L. Dulmage, and N.S. Mendelsohn, *Orthomorphisms of groups and orthogonal latin squares I.* Canad. J. Math. **13** (1961), 356–372.
[14] T. Kepka, *Structure of triabelian quasigroups.* Comment. Math. Univ. Carolin. **17/2** (1976), 229–240.
[15] T. Kepka, L. Bénéteau, J. Lacaze, *Small finite trimedial quasigroups.* Commun. Algebra **14** (1986), 1067–1090.
[16] T. Kepka, P. Němec, *Commutative Moufang loops and distributive groupoids of small orders.* Czech. Math. J. **31/106** (1981), 633–669.
[17] B. D. McKay, A. Meynert and W. Myrvold, *Small Latin squares, quasigroups and loops.* J. Combinatorial Designs **15** (2007), 98–119.
[18] B. D. McKay and I. M. Wanless, *On the number of Latin squares.* Ann. Comb. **9** (2005), 335–344.
[19] R. Moufang, *Zur Struktur von Alternativkörpern* (German). Math. Ann. **110** (1935), no. **1**, 416–430.
[20] D.C. Murdoch, *Structure of abelian quasi-groups.* Trans. Amer. Math. Soc. **49** (1941), 392–409.
[21] G.P. Nagy, P. Vojtěchovský, `LOOPS`: Computing with quasigroups and loops in GAP, version 2.2.0, `http://www.math.du.edu/loops`.
[22] G.P. Nagy, P. Vojtěchovský, *The Moufang loops of order 64 and 81.* J. Symbolic Comput. **42** (2007), no. **9**, 871–883.
[23] M.C. Slattery and A.L. Zenisek, *Moufang loops of order 243.* Comment. Math. Univ. Carolin. **53** (2012), no. **3**, 423–428.
[24] J.-P. Soublin, *Étude algébrique de la notion de moyenne* (French). J. Math. Pures Appl. **50** (1971), 53–264.
[25] D. Stanovský, *A guide to self-distributive quasigroups, or latin quandles.* Quasigroups Related Systems **23/1** (2015), 91–128.
[26] D. Stanovský, P. Vojtěchovský, *Central and medial quasigroups of small order.* Submitted.
[27] K. Toyoda, *On axioms of linear functions.* Proc. Imp. Acad. Tokyo **17** (1941), 221–227.

(Jedlička) Department of Mathematics, Faculty of Technology, Czech University of Life Sceinces, Prague, Czech Republic

(Stanovský) Department of Algebra, Faculty of Mathematics and Physics, Charles University, Prague, Czech Republic

(Stanovský) Department of Electrotechnics and Computer Science, Kazakh-British Technical University, Almaty, Kazakhstan

(Vojtěchovský) Department of Mathematics, University of Denver, 2280 S Vine St, Denver, Colorado 80208, U.S.A.

E-mail address, Jedlička: `jedlickap@tf.czu.cz`
E-mail address, Stanovský: `stanovsk@karlin.mff.cuni.cz`
E-mail address, Vojtěchovský: `petr@math.du.edu`