A GUIDE TO SELF-DISTRIBUTIVE QUASIGROUPS, OR LATIN QUANDLES

DAVID STANOVSKÝ

Abstract. We present an overview of the theory of self-distributive quasigroups, both in the two-sided and one-sided cases, and relate the older results to the modern theory of quandles, to which self-distributive quasigroups are a special case. Most attention is paid to the representation results (loop isotopy, linear representation, homogeneous representation), as the main tool to investigate self-distributive quasigroups.

1. Introduction

1.1. **The origins of self-distributivity.** *Self-distributivity* is such a natural concept: given a binary operation $*$ on a set A, fix one parameter, say the left one, and consider the mappings $L_a(x) = a * x$, called *left translations.* If all such mappings are endomorphisms of the algebraic structure $(A, *)$, the operation is called *left self-distributive* (the prefix self- is usually omitted). Equationally, the property says

$$a * (x * y) = (a * x) * (a * y)$$

for every $a, x, y \in A$, and we see that $*$ distributes over itself.

Self-distributivity was pinpointed already in the late 19th century works of logicians Peirce and Schröder [69, 76], and ever since, it keeps appearing in a natural way throughout mathematics, perhaps most notably in low dimensional topology (knot and braid invariants) [12, 15, 63], in the theory of symmetric spaces [57] and in set theory (Laver's groupoids of elementary embeddings) [15]. Recently, Moskovich expressed an interesting statement on his blog [60] that while associativity caters to the classical world of space and time, distributivity is, perhaps, the setting for the emerging world of information.

Latin squares are one of the classical topics in combinatorics. Algebraically, a latin square is represented by a binary operation, and such algebraic structures are called *quasigroups.* Formally, a binary algebraic structure $(A, *)$ is called a *quasigroup*, if the equations $a * x = b$ and $y * a = b$ have unique solutions x, y, for every $a, b \in A$.

It is no surprise that one of the very first algebraic works fully devoted to non-associative algebraic strucures was Burstin and Mayer's 1929 paper *Distributive Gruppen von endlicher Ordnung* [11] about quasigroups that are both left and right distributive. Another earliest treatise on non-associative algebraic structures was [86] by Sushkevich who observed that the proof of Lagrange's theorem (the one in elementary group theory) does not use associativity in full strength and discussed weaker conditions, some related to self-distributivity, that make the proof work. These pioneering works were quickly followed by others, with various motivations. For example, Frink [22] argued that the abstract properties of the mean value are precisely those of medial idempotent quasigroups, and self-distributivity pops up again.

Date: September 28, 2015.

2000 *Mathematics Subject Classification.* 20N05, 57M27.

Key words and phrases. Distributive quasigroups, left distributive quasigroups, latin quandles, commutative Moufang loops, Bruck loops, B-loops, affine representation.

The author was partially supported by the GAČR grant 13-01832S..

The foundations of the general theory of quasigroups were laid in the 1950s and carved in stone in Bruck's book *A survey of binary systems* [10] (despite the general title, the book leans strongly towards a particular class of *Moufang loops*). Ever since, self-distributive quasigroups and their generalizations played a prominent role in the theory of quasigroups, both in the Western and the Soviet schools [3, 30, 71]. More in the Soviet one, where the dominant driving force was Belousov's program to investigate loop isotopes of various types of quasigroups (see the list of problems at the end of the book [3]). We refer to [72] for a more detailed historical account.

Reflection in euclidean geometry (and elsewhere) is another example of a self-distributive operation: for two points a, b, consider $a*b$ to be the reflection of b over a. The equation $a*x=b$ always has a unique solution, namely, $x = a*b$, but in many cases, reflections do not yield a quasigroup operation (e.g. on a sphere). These observations, and the resulting abstraction of the notion of a reflection, can be attributed to Takasaki and his remote 1942 work [87], but the real advances have been made by Loos and others two decades later [57]. The resulting notions of *kei* (Takasaki), *symmetric spaces* (Loos), or *involutory quandles* in the modern terminology, are axiomatized by three simple algebraic properties: left distributivity, *idempotence* ($a*a=a$ for every a), and the *left involutory law* (the unique solution to $a*x=b$ is $x=a*b$; the property is also called *left symmetry*). The background is described e.g. in [54].

Group conjugation, $a*b=aba^{-1}$ on any subset of a group closed with respect to conjugation, is another prototypical self-distributive operation. This observation is often attributed to Conway and Wraithe [60], who also coined the the term *wrack of a group*, although the idea to represent self-distributive quasigroups by conjugation appeared earlier in [84] by Stein. The conjugation operation is idempotent, left distributive, but again, rarely a quasigroup: only solutions to the equation $a*x=b$ are guaranteed to exist uniquely. Algebraic structures satisfying the three conditions are called *quandles* nowadays. (The word *quandle* has no meaning in English and was entirely made up by Joyce [40]. Many other names have been introduced for quandles, such as *automorphic sets*, *pseudo-symmetric sets*, *left distributive left quasigroups*, etc.)

In early 1980s, Joyce [40] and Matveev [58], independently, picked up the idea of "wracking a group" to extract the essential part of the fundamental group of a knot complement. Unlike the fundamental group, the resulting structure, called the *fundamental quandle* of a knot, is a full invariant of (tame, oriented) knots (up to reverse mirroring) with respect to ambient isotopy. Ever since, quandles were successfully used in knot theory to design efficiently computable invariants, see e.g. [12, 21].

The works of Joyce and Matveev put the foundations for the modern theory of quandles, which covers, to some extent, many traditional aspects of self-distributivity as a special case (self-distributive quasigroups, or *latin quandles*, in particular). It is the main purpose of the present paper to overview the classical results on self-distributive quasigroups, and relate them to the results in modern quandle theory.

1.2. **Contents of the paper.** The paper is organized as a guide to the literature on self-distributive quasigroups, or latin quandles, trying to relate the results of various mathematical schools, which are often fairly hard to find and navigate (at least to me, due to a combination of writing style, terminology mess, and, to most mathematicians, language barrier).

As in most survey tasks, I had to narrow down my focus. The main subject of the paper are representation theorems, serving as the main tool to investigate self-distributive algebraic structures, such as quandles and quasigroups. To see the tools in action, my subjective choice are enumeration results. Other interesting results are cited and commented. I do not claim completeness of my survey, and apologize in advance for eventual ignorance.

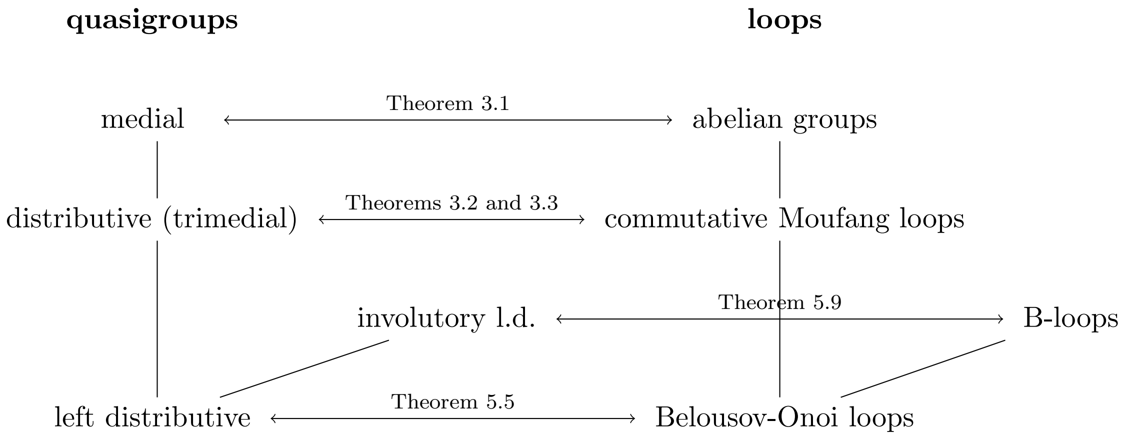

FIGURE 1. Correspondence between certain classes of quasigroups and loops.

In Section 2, we overview the background from the theory of quasigroups, loops and from universal algebra. First, we recall various equational properties of quasigroups and quandles, and define the multiplication groups. Then, various weakenings of the associative and commutative laws are introduced, with a focus towards the classes of commutative Moufang loops and Bruck loops, which are used in the representation theorems. Finally, we talk about isotopy, linear and affine representation, and polynomial equivalence between quasigroups and loops.

Section 3 addresses distributive and trimedial quasigroups. In the first part, we prove the classical affine representation of medial quasigroups (Theorem 3.1), outline Kepka's affine representation of trimedial quasigroups over commutative Moufang loops (Theorem 3.2), and comment upon some special cases and generalizations. Then, in the second part, we present a few consequences of the representation theorem, namely, a classification theorem (Theorem 3.5), enumeration results (Table 1), and we also mention the property called symmetry-by-mediality.

In a short intermezzo, Section 4, we briefly comment on the Cayley-like representation of quandles using conjugation in symmetric groups, and on the construction called the core of a loop. These were some of the first families of examples of left distributive quasigroups which are not right distributive.

In Section 5, we investigate loop isotopes of left distributive quasigroups, so called Belousov-Onoi loops. First, we prove a representation theorem (Theorem 5.5, based on more detailed Propositions 5.2 and 5.4), and then continue with the properties of Belousov-Onoi loops (among others, Propositions 5.8, 5.7, 5.10 and Theorem 5.11). We explain why, at the moment, the correspondence is of limited value for the general theory of left distributive quasigroups. Nevertheless, one special case is important: involutory left distributive quasigroups correspond to the well established class of B-loops (Theorem 5.9). The representation theorems are outlined in Figure 1.

In Section 6, we introduce the homogeneous representation of connected quandles, which is perhaps the strongest tool to study self-distributive quasigroups developed so far. We present several applications to the structure theory, with most attention paid to enumeration results.

Many proofs in our paper are only referenced. In the case of trimedial and distributive quasigroups (Theorems 3.2 and 3.3), we believe that new, shorter, and conceptually cleaner proofs are possible, using modern methods of universal algebra, but we did not succeed to make a substantial progress yet. The only minor contribution in this part is yet another proof of the Toyoda-Murdoch-Bruck theorem on medial quasigroups (Theorem 3.1). Neither we go into details in Section 6 on homogeneous representation, since it has been presented in our recent paper [35]. On the other hand, many details are given in Section 5, the Belousov-Onoi theory is presented in a substantially different way. In particular, we provide a new and cleaner proof of the representation theorem for left distributive quasigroups (Theorem 5.5), which contains as a special case the classical results of Belousov on distributive quasigroups (a part of Theorem 3.3), and the Kikkawa-Robinson theorem on involutory left distributive quasigroups (Theorem 5.9).

1.3. A remark on automated theorem proving.

Many theorems discussed in the present paper admit a short first order theory formulation, and subsequently could be attempted by automated theorem proving (ATP). Most of them are beyond the capabilites of current provers, but a few can be proved by any state-of-the art theorem prover within a few seconds. In those cases, we do not always bother to provide a reference or a proof, considering such problems "easy symbolic manipulation", although it may be rather intricate to find a proof without the aid of a computer. We refer to [73] for more information about automated theorem proving in algebra.

2. Background

2.1. Quasigroups and quandles.

Let $(A,*)$ be an algebraic structure with a single binary operation, or, shortly, a *binary algebra* (also referred to as *magma* or *groupoid* elsewhere). We say it possesses *unique left division*, if for every $a,b\in A$, there is a unique $x\in A$ such that $a*x=b$; such an x is often denoted $x=a\backslash b$. *Unique right division* is defined dually: for every $a,b\in A$, there is a unique $y\in A$ such that $y*a=b$; such a y is often denoted $y=b/a$. Binary algebras with unique left and right division are called *quasigroups.*

We list a few identities which are met frequently (all identities are assumed to be universally quantified, unless stated otherwise). A binary algebra $(A,*)$ is called

- *left distributive* if $x*(y*z)=(x*y)*(x*z)$,
- *right distributive* if $(z*y)*x=(z*x)*(y*x)$,
- *distributive* if it is both left and right distributive,
- *medial* if $(x*y)*(u*v)=(x*u)*(y*v)$,
- *trimedial* if every 3-generated subquasigroup is medial,
- *idempotent* if $x*x=x$,
- *left involutory* (or *left symmetric*) if $x*(x*y)=y$ (hence we have unique left division with $x\backslash y=x*y$).

Observe that left distributive quasigroups are idempotent: $x*(x*x)=(x*x)*(x*x)$ by left distributivity and we can cancel from the right. Non-idempotent medial quasigroups exist, indeed, abelian groups are examples. Also observe that idempotent trimedial binary algebras are distributive: given $a,b,c\in A$, the subalgebra $\langle a,b,c\rangle$ is medial, hence $(a*b)*(a*c)=(a*a)*(b*c)=a*(b*c)$, and dually for right distributivity; it requires quite an effort to prove the converse for quasigroups, see Theorem 3.3.

A binary algebra is called a (left) *quandle*, if it is idempotent, left distributive and has unique left division (remarkably, the three conditions correspond neatly to the three Reidemeister moves in knot theory, see [12, 63]). Quandles that also have unique right division are called *latin quandles.* Indeed, latin quandles and left distributive quasigroups are the very same things.

For universal algebraic considerations, it is often necessary to consider quandles as algebraic structures with two binary operations, $(A,*,\backslash)$, and quasigroups as structures with three binary operations, $(A,*,/,\backslash)$. Then, subalgebras are really quandles (quasigroups, respectively), etc. We will implicitly assume the division operations to be part of the algebraic structure whenever needed (e.g. when considering term operations in Section 2.3).

Given a binary algebra $(A,*)$, it is natural to consider *left translations* $L_a(x)=a*x$, and *right translations* $R_a(x)=x*a$, and the semigroups they generate, the *left multiplication semigroup*

$\mathrm{LMlt}(A,*) = \langle L_a : a \in A\rangle$, the *right multiplication semigroup* $\mathrm{RMlt}(A,*) = \langle R_a : a \in A\rangle$, and the *multiplication semigroup* $\mathrm{Mlt}(A,*) = \langle L_a, R_a : \ a \in A\rangle$. Unique left division turns left translations into permutations, and thus the left multiplication semigroup into a group (and dually for right translations). Observe that $L_a^{-1}(x) = a\backslash x$ and $R_a^{-1}(x) = x/a$. Also note that $(A,*)$ is left distributive if and only if L_a is an endomorphism for every $a \in A$. Hence, in quandles, $\mathrm{LMlt}(A,*)$ is a subgroup of the automorphism group.

A binary algebra $(A,*)$ is called *homogeneous* if $\mathrm{Aut}(A,*)$ acts transitively on A. It is called *left connected* if $\mathrm{LMlt}(A,*)$ acts transitively on A (we will omit the adjective "left" for quandles). A finite quandle is therefore connected if, for every $a,b \in A$, there exist $x_1,\dots,x_n \in A$ such that $b = x_1*(x_2*(\dots(x_n*a)))$ (compare to unique right division!). Connected quandles are arguably the most important class of quandles, both from the algebraic and topological points of view. Indeed, latin quandles are connected, and the class of connected quandles is a very natural generalization of left distributive quasigroups: many structural properties of left distributive quasigroups extend to connected quandles, as we shall see throughout Section 6.

To illustrate the power of connectedness, let us prove the following implication for quandles that are (both left and right) distributive.

Proposition 2.1 ([13, Theorem 5.10])**.** *Finite connected distributive quandles are quasigroups.*

Proof. Assume the contrary, and let $(Q,*)$ be the smallest counterexample. Right distributivity says that every right translation R_a is a homomorphism, hence, its image, $R_a(Q)$, forms a subquandle that is also connected and distributive (both properties project to homomorphic images). For every $a,b \in Q$, the subquandles $R_a(Q)$ and $R_b(Q)$ are isomorphic: connectedness of $(Q,*)$ provides an automorphism $\alpha \in \mathrm{LMlt}(Q,*)$ such that $\alpha(a) = b$, and it follows from $\alpha(x*a) = \alpha(x)*\alpha(a) = \alpha(x)*b$ that α restricts to an isomorphism between $R_a(Q)$ and $R_b(Q)$. Therefore, by minimality, all subquandles $R_a(Q)$ are proper subquasigroups. Now we prove that $R_a(Q) \subseteq R_{x*a}(Q)$ for every $x,a \in Q$. Let $y*a \in R_a(Q)$. Since $R_a(Q)$ is a quasigroup, there is $z*a \in R_a(Q)$ such that $y*a = (z*a)*(x*a)$. Hence $y*a \in R_{x*a}(Q)$. By induction, $R_a(Q) \subseteq R_{x_1*a}(Q) \subseteq R_{x_2*(x_1*a)}(Q) \subseteq \dots$, and thus, from connectedness, $R_a(Q) \subseteq R_b(Q)$ for every $a,b \in Q$. Hence all subquasigroups $R_a(Q)$ are equal, and since $x \in R_x(Q)$ for every $x \in Q$, all of them are equal to Q, a contradiction. □

2.2. **Loops.** A *loop* is a quasigroup $(Q,\cdot)$ with a *unit* element 1, i.e. $1\cdot a = a\cdot 1 = a$ for every $a \in A$. In the present paper, loops will be denoted multiplicatively. To avoid parenthesizing, we shortcut $x\cdot yz = x\cdot(y\cdot z)$ etc., and we remove parentheses whenever the elements associate, i.e. write xyz whenever we know that $x\cdot yz = xy\cdot z$. For all unproved statements, we refer to any introductory book on loops, such as [10, 71].

Let $(Q,\cdot)$ be a loop. *Inner mappings* are those elements of the multiplication group $\mathrm{Mlt}(Q,\cdot)$ that fix the unit element. For example, the conjugation mappings $T_x(z) = xz/x$ are inner and, in a way, measure the non-commutativity in the loop. The *left inner mappings* are defined by $L_{x,y}(z) = (xy)\backslash(x\cdot yz)$ and measure the non-associativity from the left.

The most common example of loops are groups (i.e. associative loops), and most classes of loops studied in literature are those satisfying a weak version of associativity or commutativity. We list a few weak associative laws (note that all the conditions hold in groups): a loop is called

- *diassociative* if all 2-generated subloops are associative;
- *left alternative* if $x\cdot xy = x^2y$;
- *power-associative* if all 1-generated subloops are associative;
- *Moufang* if $(xy\cdot x)z = x(y\cdot xz)$ (the dual law is equivalent in loops);
- *left Bol* if $(x\cdot yx)z = x(y\cdot xz)$;
- *automorphic* if all inner mappings are automorphisms.
- *left automorphic* if all left inner mappings $L_{x,y}$ are automorphisms.

Moufang's theorem [18] says that in a Moufang loop, every subloop generated by three elements that associate, is associative. In particular, Moufang loops are diassociative, since $a(ba) = (ab)a$ for every a, b, as directly follows from the Moufang law. Bol loops are power-associative.

The *nucleus* of a loop $(Q, \cdot)$ is the set of all elements $a \in Q$ that associate with all other elements, i.e.

$$N = \{a \in Q : \ a \cdot xy = ax \cdot y, \ x \cdot ay = xa \cdot y, \ x \cdot ya = xy \cdot a \text{ for all } x, y \in Q\}.$$

An element of a loop is called *nuclear* if it belongs to the nucleus. A mapping $f : Q \to Q$ is called *k-nuclear* if $x^k f(x) \in N$ for every $x \in Q$.

Commutative Moufang loops were a central topic in the Bruck's book [10], and newer results are surveyed in [7, 78]. The following characterization shows how natural the class is.

Theorem 2.2 ([10, 70])**.** *The following are equivalent for a commutative loop $(Q, \cdot)$:*

(1) *it is diassociative and automorphic;*
(2) *it is Moufang;*
(2') *the identity $xx \cdot yz = xy \cdot xz$ holds.*
(3) *the identity $f(x)x \cdot yz = f(x)y \cdot xz$ holds for some $f : Q \to Q$.*

Moreover, if $(Q, \cdot)$ is a commutative Moufang loop, than the identity of (3) holds if and only if f is a (-1)-nuclear mapping.

The equivalence of (1), (2), (2') is well-known [10]. The rest is a special case of a lesser known, but intriguing characterization of Moufang loops by Pflugfelder [70]. It is one of the crucial ingrediences in Kepka's proof of Theorem 3.2, and also in our new proof of Proposition 5.7.

Example 2.3. According to Kepka and Němec [49, Theorem 9.2], the smallest non-associative commutative Moufang loops have order 81, there are two of them (up to isomorphism), and can be constructed as follows. Consider the groups $G_1 = (\mathbb{Z}_3)^4$ and $G_2 = (\mathbb{Z}_3)^2 \times \mathbb{Z}_9$. Let $e_1, e_2, e_3(, e_4)$ be the canonical generators. Let t_1 be the triaditive mapping over G_1 satisfying

$$t_1(e_2, e_3, e_4) = e_1, \ t_1(e_3, e_2, e_4) = -e_1, \ t_1(e_i, e_j, e_k) = 0 \text{ otherwise.}$$

Let t_2 be the triaditive mapping over G_2 satisfying

$$t_2(e_1, e_2, e_3) = 3e_3, \ t_2(e_2, e_1, e_3) = -3e_3, \ t_2(e_i, e_j, e_k) = 0 \text{ otherwise.}$$

The loops $Q_i = (G_i, \cdot)$, $i = 1, 2$, with

$$x \cdot y = x + y + t_i(x, y, x - y),$$

are non-isomorphic commutative Moufang loops, and every commutative Moufang loop of order 81 is isomorphic to one of them.

In an arbitrary loop $(Q, \cdot)$, we can define the left inverse as $x^{-1} = x\backslash 1$ (in general, $x\backslash 1 \neq 1/x$). Then, the *left inverse property* (LIP) requests that $a\backslash b = a^{-1}b$ for every $a, b \in Q$, and the *left automorphic inverse property* (LAIP) requests that $(ab)^{-1} = a^{-1}b^{-1}$ for every $a, b \in Q$. The RIP and RAIP are defined dually; if left and right inverses coincide, we talk about IP and AIP.

Diassociative loops have the IP, and then, commutativity is indeed equivalent to the AIP. Bol loops have the LIP, and are power associative, hence the left and right inverses coincide. Occasionally, we will need the following technical lemma.

Lemma 2.4 ([51] or ATP)**.** *The following properties are equivalent for a left Bol loop $(Q, \cdot)$:*

(1) *the AIP;*
(2) *the identity $(xy)^2 = x \cdot y^2x$;*
(3) *$L_{ab}^2 = L_a L_b^2 L_a$ for every $a, b \in Q$.*

It seems that the AIP is the appropriate generalization of commutativity into the Bol setting (commutativity is no good, as it implies the Moufang law). We have the following “left version” of Theorem 2.2, under the additional assumption of *unique 2-divisibility*, which states that the mapping $x \mapsto x^2$ is a permutation.

Theorem 2.5 ([53] and ATP)**.** *The following are equivalent for a uniquely 2-divisible loop $(Q, \cdot)$ with the LAIP:*

(1) *it has the LIP, is left alternative and left automorphic;*
(1’) *the identities $x^2 \cdot x^{-1}y = xy$ and $L_{x,y}(z^{-1}) = L_{x,y}(z)^{-1}$ hold;*
(2) *it is left Bol;*
(2’) *the identity $(xy)^2 \cdot (x^{-1}z) = x \cdot y^2 z$ holds.*

Proof sketch. (1’) is an immediate consequence of (1), and (2’) easily follows from (2) by Lemma 2.4, but the converse implications are trickier; we could not find them anywhere in literature, but they can be verified by an automated theorem prover.

To prove that the equivalent conditions (1),(1’) are in turn equivalent to the equivalent conditions (2),(2’), we can use [53, Theorem 3], which states that, for left alternative uniquely 2-divisible loops with the LIP and LAIP, the identity (2’) is equivalent to being left automorphic. □

Left Bol loops with the AIP are called *Bruck loops* (or *K-loops* or *gyrocommutative gyrogroups*). A lot of structure theory is collected in Kiechle’s book [51]. Uniquely 2-divisible Bruck loops were called *B-loops* (we will use the shortcut, too) and studied in detail by Glauberman [31]. A finite Bruck loop is uniquely 2-divisible if and only if it has odd order [31, Proposition 1]. Every B-loop can be realized as a subset Q of a group $(G, \circ)$ such that the mapping $x \mapsto x \circ x$ is a permutation on Q and the loop operation is $a \cdot b = \sqrt{a} \circ b \circ \sqrt{a}$ [31, Theorem 2].

Example 2.6. The smallest non-associative B-loop has order 15 and can be constructed as follows. Consider the loop $(\mathbb{Z}_5 \times \mathbb{Z}_3, \cdot)$ with

$$(a, x) \cdot (b, y) = (\varphi_{x,y} a + b, x + y)$$

where $\varphi_{x,y} \in \mathbb{Z}_5^*$ are given by the following table:

	0	1	2
0	1	2	2
1	1	3	1
2	1	1	3

It is straightforward to check that this is a B-loop. It is an abelian extension of $\mathbb{Z}_5$ by $\mathbb{Z}_3$ in the sense of [82].

2.3. **Linear and affine representation.** A great portion of the present paper is about establishing that “two algebraic structures are essentially the same”. To formalize the statement, we borrow a formal definition from universal algebra. Let $(A, f_1, f_2, \dots)$ be an arbitrary algebraic structure (shortly, algebra), with basic operations $f_1, f_2, \dots$ A *term operation* is any operation that results as a composition of the basic operations. *Polynomial operations* result from term operations by substituting constants for some of the variables. Two algebras with the same underlying set are called *term equivalent* (or *polynomially equivalent*, respectively), if they have the same term operations (or polynomial operations). For example, a group can be presented in the standard way, as $(G, \cdot, ^{-1}, 1)$, or in the loop theoretical way, as an associative loop $(G, \cdot, /, \backslash, 1)$; the two algebraic structures are formally different, but they are term equivalent, since the basic operations in any one of them are term operations in the other one. Term equivalent algebras have identical subalgebras, polynomially equivalent algebras have identical congruences, and share all properties that only depend on terms or polynomials (for example, the Lagrange property, see Section 6.3). To learn more, consult [8, Section 4.8].

One of the fundamental tools to study a quasigroup is, to determine its loop isotopes, and use the properties of the loops to obtain an information about the original quasigroup. An *isotopy* between two quasigroups $(Q_1, *)$ and $(Q_2, \cdot)$ is a triple of bijective mappings $\alpha, \beta, \gamma : Q_1 \to Q_2$ such that

$$\alpha(a) \cdot \beta(b) = \gamma(a * b)$$

for every $a, b \in Q_1$. Then, $(Q_2, \cdot)$ is called an *isotope* of $(Q_1, *)$. The combinatorial interpretation is that $(Q_2, \cdot)$ is obtained from $(Q_1, *)$ by permuting rows, columns and renaming entries in the multiplication table. Up to isomorphism, we can only consider isotopes with $Q_1 = Q_2$ and $\gamma = id$, so called *principal isotopes.*

Every quasigroup admits many principal loop isotopes, often falling into more isomorphism classes, yet all of them have a particularly nice form.

Proposition 2.7 ([10, Section III])**.** *Let $(Q, *)$ be a quasigroup and α, β permutations on Q. The following are equivalent:*

- *the isotope $a \cdot b = \alpha(a) * \beta(b)$ is a loop;*
- *$\alpha = R_{e_1}$ and $\beta = L_{e_2}$ for some $e_1, e_2 \in Q$.*

Rephrased, given a quasigroup $(Q, *)$, the only loop isotopes, up to isomorphism, are $(Q, \cdot)$ with

$$a \cdot b = (a/e_1) * (e_2 \backslash b),$$

where $e_1, e_2 \in Q$ can be chosen arbitrarily. Then the unit element is $1 = e_2 * e_1$. For the division operations, we will use the symbols $\backslash^{\cdot}$ and $/^{\cdot}$, to distinguish them from the quasigroup division.

Notice that the new operation $\cdot$ is a polynomial operation over the original quasigroup, and so are the division operations. We can recover the quasigroup operation as

$$a * b = R_{e_1}(a) \cdot L_{e_2}(b),$$

but this is rarely a polynomial operation over $(Q, \cdot)$. The most satisfactory loop isotopes are those where R_{e_1} and L_{e_2} are affine mappings over $(Q, \cdot)$.

A permutation φ of Q is called *affine* over $(Q, \cdot)$, if

$$\varphi(x) = \tilde{\varphi}(x) \cdot u \quad \text{or} \quad \varphi(x) = u \cdot \tilde{\varphi}(x)$$

where $\tilde{\varphi}$ is an automorphism of $(Q, \cdot)$ and $u \in Q$. In other terms, if $\varphi = R_u\tilde{\varphi}$ or $\varphi = L_u\tilde{\varphi}$. A quasigroup $(Q, *)$ is called *affine* over a loop $(Q, \cdot)$ if, for every $a, b \in Q$,

$$a * b = \varphi(a) \cdot \psi(b),$$

where φ, ψ are affine mappings over $(Q, \cdot)$ such that $\tilde{\varphi}\tilde{\psi} = \tilde{\psi}\tilde{\varphi}$. If both φ, ψ are automorphisms, we call $(Q, *)$ *linear* over $(Q, \cdot)$. (Note that the affine mappings φ, ψ do not necessarily commute.)

Example 2.8. To illustrate the concept of affine representation, consider a quasigroup $(Q, *)$ affine over an abelian group $(Q, \cdot)$. We prove that it is medial. With $\varphi = R_u\tilde{\varphi}$, $\psi = R_v\tilde{\psi}$ (left or right makes no difference here), we have

$$\begin{aligned}(a * b) * (c * d) &= \varphi\left(\varphi(a) \cdot \psi(b)\right) \cdot \psi\left(\varphi(c) \cdot \psi(d)\right)\\ &= \tilde{\varphi}\left(\tilde{\varphi}(a)u \cdot \tilde{\psi}(b)v\right) u \cdot \tilde{\psi}\left(\tilde{\varphi}(c)u \cdot \tilde{\psi}(d)v\right) v\\ &= \tilde{\varphi}^2(a) \cdot \tilde{\varphi}\tilde{\psi}(b) \cdot \tilde{\psi}\tilde{\varphi}(c) \cdot \tilde{\psi}^2(d) \cdot \tilde{\varphi}(uv) \cdot \tilde{\psi}(uv) \cdot uv.\end{aligned}$$

Since $\tilde{\varphi}\tilde{\psi} = \tilde{\psi}\tilde{\varphi}$, the expression is invariant with respect to interchange of b and c. As we shall see, Theorem 3.1 states also the converse: every medial quasigroup is affine over an abelian group.

Any adjective to the words "affine" or "linear" will refer to the properties of the mappings φ and ψ. In Section 3, we will consider 1-nuclear affine representations over commutative Moufang loops, i.e. we will assume that φ, ψ are 1-nuclear affine mappings. Notice that if $\varphi = F_u\tilde{\varphi}$, with $F \in \{L, R\}$, is 1-nuclear, then u is nuclear (substitute 1), and if the nucleus is a normal subloop, then $\tilde{\varphi}$ is also 1-nuclear.

How to turn an affine representation into a polynomial equivalence? Consider affine mappings $\varphi = F_u\tilde{\varphi}$, $\psi = G_v\tilde{\psi}$ where $F, G \in \{L, R\}$ and $\tilde{\varphi}, \tilde{\psi}$ are automorphisms of $(Q, \cdot)$. Then $x * y = \varphi(x) \cdot \psi(y)$ is a polynomial operation over the algebra $(Q, \cdot, \tilde{\varphi}, \tilde{\psi})$, and a similar statement applies to the division operations, too (one also needs to use the inverse automorphisms $\tilde{\varphi}^{-1}, \tilde{\psi}^{-1}$). Conversely, if $(Q, \cdot)$ is a loop isotope of a quasigroup $(Q, *)$, then $x \cdot y = (x/e_1) * (e_2 \backslash y)$, $x \backslash^{\cdot} y = e_2 * ((x/e_1) \backslash y)$, and $x /^{\cdot} y = (x/(e_2 \backslash y)) * e_1$ are all polynomial operations over the quasigroup. If the translations R_{e_1}, L_{e_2} are affine over $(Q, \cdot)$, then $\tilde{R}_{e_1}(x) = (x * e_1) /^{\cdot} (1 * e_1)$, $\tilde{L}_{e_2}(x) = (e_2 * x) /^{\cdot} (e_2 * 1)$ are polynomial operations, too, hence the quasigroup $(Q, *, \backslash, /)$ and the algebra $(Q, \cdot, \backslash^{\cdot}, /^{\cdot}, \tilde{R}_{e_1}, \tilde{R}_{e_1}^{-1}, \tilde{L}_{e_2}, \tilde{L}_{e_2}^{-1})$ are polynomially equivalent, i.e. essentially the same object. It is convenient to perceive the loop expanded by two automorphisms in a module-theoretic way, as we shall explain now.

The classical case first: assume the loop is an abelian group and let us denote it additively, $(Q, +)$. Let φ, ψ be two commuting automorphisms of $(Q, +)$. Then the algebra $(Q, +, -, 0, \varphi, \varphi^{-1}, \psi, \psi^{-1})$ is term equivalent to the module over the ring of Laurent polynomials $\mathbb{Z}[s, s^{-1}, t, t^{-1}]$ whose underlying additive structure is $(Q, +)$ and the action of s, t is that of φ, ψ, respectively. The corresponding quasigroup operation can be written as the affine form

$$x * y = sx + ty + c,$$

where $c \in Q$ is a constant.

For general loops, one can consider "generalized modules" over commutative "generalized rings", where the underlying additive structures are not necessarily associative. No general theory has been developed yet, but there are indications that this approach could provide a powerful tool. For example, commutative diassociative loops share a lot of module-theoretic properties of abelian groups, such as the primary decomposition [56]. The idea of "generalized modules" and the corresponding homological methods have been exploited several times to prove interesting theorems about quasigroups [33, 34, 48].

Finally, let us note that our definition of affine quasigroup is too strong in one sense, and possibly weak in another sense.

The condition that the two automorphisms $\tilde{\varphi}, \tilde{\psi}$ commute is strongly tied to mediality and its weaker forms, and we included it only for brevity. Omitting the condition makes a very good sense from the universal algebra point of view. Quasigroups that admit a "non-commuting" affine representation over an abelian group (and thus polynomially equivalent to a module over the ring of Laurent polynomials of two non-commuting variables) have been studied since the 1970s, see [79, Chapter 3] or [17] for recent developments (the original name *T-quasigroups* is slowly fading away, being replaced by the adjective *central*; in universal algebra, they would be called *abelian* or *affine*, as the two concepts are equivalent for quasigroups).

In Section 3, all affine representations will be 1-nuclear. However, we resist to enforce nuclearity in the definition of affineness, since we do not understand its role properly (in particular, we do not know whether the representation of Theorem 5.5 admits any sort of nuclearity). We are not yet certain what is the appropriate generalization of the notion of an affine form into the non-associative setting.

3. Distributive quasigroups

3.1. **Affine representation.**

The first ever affine representation theorem was the one for medial quasigroups, proved independently by Toyoda [88], Murdoch [61] and Bruck [9] in the 1940s.

Theorem 3.1 ([9, 61, 88])**.** *The following are equivalent for a quasigroup $(Q,*)$:*

(1) *it is medial;*
(2) *it is affine over an abelian group.*

Proof. (2) $\Rightarrow$ (1) was calculated in Example 2.8.

(1) $\Rightarrow$ (2). Pick arbitrary $e_1, e_2 \in Q$ and define a loop operation on Q by $a \cdot b = (a/e_1) * (e_2\backslash b)$. We can recover the quasigroup operation as $a * b = R_{e_1}(a) \cdot L_{e_2}(b)$, where R_{e_1}, L_{e_2} are translations in $(Q,*)$. We show that $(Q,\cdot)$ is an abelian group, and that R_{e_1}, L_{e_2} are affine mappings over $(Q,\cdot)$.

First, consider the quasigroup $(Q,\circ)$ with $a \circ b = (a/e_1) * b$. We prove that it is also medial. Observe that, for every $x, y, u, v \in Q$,

$$(x/y) * (u/v) = (x * u)/(y * v), \tag{†}$$

since $((x/y) * (u/v)) * (y * v) = ((x/y) * y) * ((u/v) * v) = x * u$, and we obtain the identity by division from the right. Now we expand

$$\begin{aligned}(a \circ b) \circ (c \circ d) &= (((a/e_1) * b)/e_1) * ((c/e_1) * d)\\ &= (((a/e_1) * b)/((e_1/e_1) * e_1)) * ((c/e_1) * d)\\ &= (((a/e_1)/(e_1/e_1)) * (b/e_1)) * ((c/e_1) * d),\end{aligned}$$

and using mediality, we can interchange b/e_1 and c/e_1, and by an analogous calculation obtain $(a \circ b) \circ (c \circ d) = (a \circ c) \circ (b \circ d)$. Now notice that $a \cdot b = a \circ (e_2\backslash b) = a \circ ((e_2 * e_1)\backslash^{\circ} b)$, hence a dual argument, with $*$ replaced for $\circ$ and e_1 replaced for $e_2 * e_1$, shows that the loop $(Q,\cdot)$ is also medial. But medial loops are abelian groups.

It remains to prove that the mappings R_{e_1}, L_{e_2} are affine over $(Q,\cdot)$ and that the corresponding automorphisms $\tilde{R}_{e_1}, \tilde{L}_{e_2}$ commute. Let 1 denote the unit and $^{-1}$ the inverse element in the group $(Q,\cdot)$. Consider $a, b \in Q$. By mediality,

$$(R_{e_1}^{-1}(a) * L_{e_2}^{-1}(b)) * (L_{e_2}^{-1}(1) * L_{e_2}^{-1}(1)) = (R_{e_1}^{-1}(a) * L_{e_2}^{-1}(1)) * (L_{e_2}^{-1}(b) * L_{e_2}^{-1}(1)).$$

Rewriting $x * y = R_{e_1}(x) \cdot L_{e_2}(y)$, we obtain

$$R_{e_1}(a \cdot b) \cdot L_{e_2} R_{e_1} L_{e_2}^{-1}(1) = R_{e_1}(a) \cdot L_{e_2} R_{e_1} L_{e_2}^{-1}(b).$$

With $a = 1$, we obtain $L_{e_2} R_{e_1} L_{e_2}^{-1}(b) = R_{e_1}(b) \cdot L_{e_2} R_{e_1} L_{e_2}^{-1}(1) \cdot R_{e_1}(1)^{-1}$, and after replacement of the last term in the previous identity, and after cancelling the term $L_{e_2} R_{e_1} L_{e_2}^{-1}(1)$, we obtain

$$R_{e_1}(a \cdot b) = R_{e_1}(a) \cdot R_{e_1}(b) \cdot R_{e_1}(1)^{-1}.$$

This shows that R_{e_1} is an affine mapping, with the underlying automorphism $\tilde{R}_{e_1}(x) = R_{e_1}(x) R_{e_1}(1)^{-1}$. Dually, we obtain that L_{e_2} is an affine mapping, with the underlying automorphism $\tilde{L}_{e_2}(x) = L_{e_2}(x) L_{e_2}(1)^{-1}$.

Finally we show that the two automorphisms commute. With $\varphi = R_{e_1}$, $\psi = L_{e_2}$, $u = R_{e_1}(1)^{-1}$ and $v = L_{e_2}(1)^{-1}$, we can calculate as in Example 2.8 that, for every $x \in Q$,

$$\tilde{\varphi}\tilde{\psi}(x) \cdot \tilde{\varphi}(uv) \cdot \tilde{\psi}(uv) \cdot uv = (1 * x) * (1 * 1) = (1 * 1) * (x * 1) = \tilde{\psi}\tilde{\varphi}(x) \cdot \tilde{\varphi}(uv) \cdot \tilde{\psi}(uv) \cdot uv.$$

After cancellation, we see that $\tilde{\varphi}\tilde{\psi} = \tilde{\psi}\tilde{\varphi}$. $\square$

Note that we proved a stronger statement: *any* loop isotope of a medial quasigroup is an abelian group that provides an affine representation. For other classes, in order to obtain an affine representation over a nice class of loops, one often has to choose the parameters e_1, e_2 in a special way. For instance, for trimedial quasigroups, one has to take $e_1 = e_2$ which is a square, as we shall see.

Perhaps the best way to perceive distributive quasigroups is through *trimediality*. As we shall see, a quasigroup is distributive if and only if it is idempotent and trimedial. This was first realized by Belousov in [2], and his proof was based on finding an isotopy of a distributive quasigroup to a commutative Moufang loop, and subsequently using Moufang's theorem (see also his book [3, Theorems 8.1 and 8.6]). Belousov's method actually provides a linear representation, but this fact was recognized and explicitly formulated only later by Soublin [80, Section II.7, Theorem 1]. An analogous theorem for general (not necessarily idempotent) trimedial quasigroups was proved by Kepka [43] a few years later (Theorem 3.2). We will now outline Kepka's proof, and show how the Belousov-Soublin theorem follows as a special case (Theorem 3.3).

Many equivalent conditions charecterizing trimediality are formulated in [43], we only pick the most important ones here: (1) trimediality, (2) a stronger fact stating that mediating elements generate a medial subquasigroup, (3) a finite equational base for trimediality, and (4) the affine representation. In fact, Kepka lists several finite bases, but not the one we state here: our condition (3) is a *minimal* base, found in [55], and subsumes most of Kepka's bases.

Theorem 3.2 ([43])**.** *The following are equivalent for a quasigroup $(Q,*)$:*

1. *it is trimedial;*
2. *for every $a, b, c, d \in Q$, if $(a*b)*(c*d) = (a*c)*(b*d)$ then the subquasigroup $\langle a, b, c, d\rangle$ is medial;*
3. *it satisfies, for every $a, b, c \in Q$, the identities*

$$(c*b)*(a*a) = (c*a)*(b*a),$$
$$(a*(a*a))*(b*c) = (a*b)*((a*a)*c);$$

4. *it is 1-nuclear affine over a commutative Moufang loop.*

Proof sketch. (2) ⇒ (1). For any $a, b, c \in Q$, we have $(b*a)*(a*c) = (b*a)*(a*c)$. Hence, by (2), $\langle a, b, c\rangle$ is medial.

(1) ⇒ (3). Given $a, b, c \in Q$, consider the subquasigroup $\langle a, b, c\rangle$. It is medial, hence the two identities hold for a, b, c.

(3) ⇒ (4). First of all, we need to prove the following two additional identities: $(a*a)*(b*c) = (a*b)*(a*c)$ and $(a*b)*(c*a) = (a*c)*(b*a)$ (in Kepka's terminology, to prove that $(Q,*)$ is a WAD-quasigroup). A proof can be found quickly by an automated theorem prover, or read in [55]. Now we can follow Kepka's proof from [43], whose structure is similar to our proof of Theorem 3.1.

Pick an arbitrary square $e \in Q$ (i.e. $e = e'*e'$ for some e') and define the loop operation on Q by $a \cdot b = (a/e)*(e\backslash b)$. We can recover the quasigroup operation as $a*b = R_e(a) \cdot L_e(b)$, where L_e, R_e are translations in $(Q,*)$. To show that $(Q,\cdot)$ is a commutative Moufang loop, it is sufficient to verify condition (3) of Theorem 2.2 with $f = R_e L_e^{-1}$. The proof is rather technical, see [42, Proposition 4.8(iii)]. It also follows that the mapping f is (-1)-nuclear, and another technical calculation, as in [43, Lemma 3(iii)], shows that the mappings L_e, R_e are 1-nuclear. Finally, we can reuse the second part of our proof of Theorem 3.1 to show that the two mappings are affine and that the underlying automorphisms commute, since we only used the identity $(a*a)*(b*c) = (a*b)*(a*c)$ and its dual in the proof. We have to be careful about non-associativity of the multiplication, but fortunately, all calculations are correct thanks to the fact that the mappings L_e, R_e are 1-nuclear, hence preserve the nucleus (in particular, all elements resulting by application of L_e, R_e on 1 are nuclear).

(4) ⇒ (2). The idea is, find a subloop Q' of $(Q,\cdot)$ that contains all four elements a,b,c,d and is generated by three elements u,v,w that associate. Then, by Moufang's theorem [18], Q' is an abelian group, and thus the subquasigroup $\langle a,b,c,d\rangle$ is medial by Theorem 3.1. The construction is described in [43, Theorem 2 (vi)⇒(vii)]. □

As a corollary to Theorem 3.2, we settle the case of distributive quasigroups.

Theorem 3.3 ([80]). *The following are equivalent for an idempotent quasigroup $(Q,*)$:*

(1) *it is trimedial;*
(2) *for every $a,b,c,d\in Q$, if $(a*b)*(c*d)=(a*c)*(b*d)$ then the subquasigroup $\langle a,b,c,d\rangle$ is medial;*
(3) *it is distributive;*
(4) *it is 1-nuclear linear over a commutative Moufang loop.*

Proof. Look at Theorem 3.2. Conditions (1) and (2) are identical. Under the assumption of idempotence, condition (3) of Theorem 3.2 is equivalent to distributivity. To obtain the equivalence of the fourth conditions, we observe that an idempotent quasigroup which is 1-nuclear affine over a commutative Moufang loop $(Q,\cdot)$ is actually linear over $(Q,\cdot)$: with $\varphi=R_u\tilde\varphi$ and $\psi=R_v\tilde\psi$, thanks to nuclearity and commutativity, we have $a*b=\tilde\varphi(a)\tilde\psi(a)uv$, and since $1=1*1=\tilde\varphi(1)\tilde\psi(1)uv=uv$ we see that $a*b=\tilde\varphi(a)\tilde\psi(a)$ is a linear representation. □

For idempotent quasigroups, the linear representation $a*b=\varphi(a)\cdot\psi(b)$ is determined by either one of the automorphisms φ or ψ, since $a=a*a=\varphi(a)\cdot\psi(a)$, hence $\varphi(a)=a/^{\cdot}\psi(a)$ or $\psi(a)=\varphi(a)\backslash^{\cdot}a$. Mappings φ,ψ satisfying $\varphi(a)\cdot\psi(a)=a$ will be called *companions.* Note that the companion of an automorphism is not necessarily a permutation or an endomorphism! However, if it is an endomorphism, then the two mappings commute.

Example 3.4. Combining Theorem 3.3 and Example 2.3, one can determine the smallest non-medial distributive quasigroups. They have order 81 and there are six of them (up to isomorphism) [49, Theorem 12.4]. A careful analysis of the automorphisms of the loops $(G_1,\cdot)$ and $(G_2,\cdot)$ of Example 2.3 (see [49, Sections 5 and 6], respectively) leads to the following classification:

(1) $(G_1,*)$ with $x*y=x^{-1}\cdot y^{-1}$.
(2) $(G_1,*)$ with $x*y=\varphi(x)\cdot\psi(y)$ where $\varphi(x)=(x_2-x_1)e_1-x_2e_2-x_3e_3-x_4e_4$ and ψ is its companion.
(3) $(G_2,*)$ with $x*y=\sqrt{x}\cdot\sqrt{y}$. In $(G_2,\cdot)$, the mapping $x\mapsto x^2$ is a 1-nuclear automorphism, and so is its inverse $x\mapsto\sqrt{x}$.
(4) $(G_2,*)$ with $x*y=x^{-1}\cdot y^2$.
(5) $(G_2,*)$ with $x*y=x^2\cdot y^{-1}$.
(6) $(G_2,*)$ with $x*y=\varphi(x)\cdot\psi(y)$ where $\varphi(x)=-x_1e_1-x_2e_2-(3x_1+x_3)e_3$ and ψ is its companion.

Theorem 3.3 has an interesting connection to design theory. It is well known that *Steiner triple systems* correspond to a certain class of (finite) idempotent quasigroups, called *Steiner quasigroups.* Affine Steiner triple systems, constructed over the affine spaces $(\mathbb{F}_3)^k$, correspond to medial Steiner quasigroups, $((\mathbb{F}_3)^k,*)$ with $a*b=-a-b$. *Hall triple systems* can be defined by the property that every subsystem generated by three points is affine. Theorem 3.3 implies that the corresponding quasigroups are precisely the distributive Steiner quasigroups. As a consequence, one can obtain, for instance, the enumeration of Hall triple systems, see the numbers $DQ(n)$ in Table 1 (the one of order 81 is item (1) of Example 3.4). We refer to [6, 16] for details and other relations between distributive quasigroups, finite geometries and combinatorial designs.

Theorems 3.2 and 3.3 can be further generalized in several directions. For example, it was proved by Kepka, Kinyon and Phillips [47, Theorem 1.2] that the class of *F-quasigroups*, properly containing the trimedial quasigroups, admits a 1-nuclear (-1)-Moufang-central affine representation over *NK-loops*, a class of Moufang loops that are sums of their nucleus and Moufang center. Another direction is weakening the unique divisibility condition, see the comprehensive studies by Ježek, Kepka and Němec [36, 38, 39, 45, 49]. In all of these papers, a self-dual condition (such as trimediality or both-sided distributivity) is essential for linearization. The one-sided case is quite different and will be studied in Section 5. Nevertheless, we will be able to obtain the representation from Theorem 3.3 as a consequence of the one-sided theory.

3.2. **Structure and enumeration.** Theorem 3.3 allows to use the well developed theory of commutative Moufang loops to build the structure theory of distributive quasigroups. We will describe a few examples. Further results can be found in the comprehensive survey [7].

We start with Galkin's interpretation of the Fischer-Smith theorem [23, 77].

Theorem 3.5 ([23]). *Let Q be a finite distributive quasigroup of order $p_1^{n_1}\cdot\ldots\cdot p_k^{n_k}$ where $p_1,\ldots,p_k$ are pairwise different primes. Then*

$$Q \simeq Q_1 \times \ldots \times Q_k$$

where $|Q_i| = p_i^{n_i}$. Moreover, if Q_i is not medial, then $p_i = 3$ and $n_i \geq 4$.

The story of the proof goes as follows. Let Q be a finite distributive quasigroup. The first step was Fischer's proof [20] that $\mathrm{LMlt}(Q)$ is solvable, using substantial results from group theory, including the Feit-Thompson theorem and the Brauer-Suzuki theorem. Then Smith [77] was able to strengthen Fischer's theorem, while avoiding the heavy finite group machinery, by combining Theorem 3.3 and the Bruck-Slaby theorem [10, Chapter VIII] stating that finite commutative Moufang loops are centrally nilpotent. Smith's result says that the derived subgroup $\mathrm{LMlt}(Q)'$ is the direct product of a 3-group and an abelian group of order coprime to 3 (hence $\mathrm{LMlt}(Q)'$ is nilpotent and $\mathrm{LMlt}(Q)$ is solvable, as proved by Fischer). Finally, Galkin [23] observed that his idea of minimal representation (explained in our Section 6) implies that the quasigroup Q decomposes in a way analogous to the decomposition of $\mathrm{LMlt}(Q)'$. Using the fact that every 3-generated subquasigroup is medial (see Theorem 3.3), one concludes that a non-medial distributive quasigroup has at least $3^4 = 81$ elements.

A somewhat different approach to the Fischer-Smith theorem, based on the homogeneous representation of Section 6, is presented in [29].

An interesting story is the *enumeration* of distributive quasigroups. Again, Theorem 3.3 is crucial here, as it allows to focus on the enumeration of commutative Moufang loops and their automorphism groups. It is not difficult to prove (see e.g. [49, Lemma 12.3]) that two commutative Moufang loops, Q_1 and Q_2, and their nuclear automorphisms, ψ_1 and ψ_2, respectively, provide isomorphic distributive quasigroups if and only if there is a loop isomorphism $\varphi : Q_1 \to Q_2$ such that $\psi_2 = \varphi\psi_1\varphi^{-1}$.

In particular, the lemma applies to abelian groups, hence the number $MI(n)$ of medial idempotent quasigroups of order n up to isomorphism can be determined using the classification of finite abelian groups and the corresponding linear algebra. The function $MI(n)$ is indeed multiplicative (i.e. $MI(mn) = MI(m)MI(n)$ for every m, n coprime) and explicit formulas for $MI(p^k)$, p prime and $k \leq 4$, were found by Hou [34] (in his paper, (finite) medial idempotent quasigroups are referred to as connected Alexander quandles; the formulas are given in [34, equation (4.2)] and the complete list of quasigroups is displayed in [34, Table 1]). See our Table 3 for the first 47 values of $MI(n)$.

Theorem 3.5 says that the interesting (i.e. directly indecomposable) non-medial distributive quasigroups have orders $n = 3^k$, $k \geq 4$. Table 1 summarizes some of the enumeration results found in literature. $CML(n)$ denotes the number of non-associative commutative Moufang loops of order n up to isomorphism, as calculated in [49]; the next four rows describe the numbers of non-medial quasigroups of order n up to isomorphism in the following classes: $3M(n)$ refers to trimedial quasigroups [46], $D(n)$ to distributive quasigroups [49], $DM(n)$ to distributive Mendelsohn quasigroups [16], and $DS(n)$ to distributive Steiner quasigroups [6, 44]; the last row displays the medial case.

n	3	3^2	3^3	3^4	3^5	3^6
$CML(n)$	0	0	0	2	6	≥ 8
$3M(n)$	0	0	0	35		
$D(n)$	0	0	0	6		
$DM(n)$	0	0	0	2	≥ 3	
$DS(n)$	0	0	0	1	1	3
$MI(n)$	1	8	30	166		

Table 1. Enumeration of commutative Moufang loops and of various classes of distributive quasigroups.

Another interesting enumeration result says that the smallest non-medial *hamiltonian* distributive quasigroup has order 3^6, and that there are two of them [33]. This is perhaps the deepest application of the module-theoretical approach to distributive quasigroups.

Finally, let us mention the property called *symmetry-by-mediality.* An idempotent binary algebra is called symmetric-by-medial, if it has a congruence α such that its blocks are *symmetric* (i.e. both left and right involutory), and the factor over α is medial. (In idempotent algebras, congruence blocks are always subalgebras.) Symmetric distributive quasigroups are commutative, and they are precisely the distributive Steiner quasigroups. Using Bruck's associator calculus for Moufang loops, Belousov proved that distributive quasigroups are symmetric-by-medial [3, Theorem 8.7]. Again, the theorem generalizes to a non-quasigroup setting [37, 81].

4. Conjugation and cores

Let $(G,\cdot)$ be a group and Q a subset of G closed with respect to conjugation. Then the binary algebra $(Q,*)$ with
$$a*b = aba^{-1}$$
is a quandle, called a *conjugation quandle* over the group $(G,\cdot)$. It is easy to verify that every quandle admits a *Cayley-like representation* over a conjugation quandle.

Proposition 4.1. *Let $(Q,*)$ be a quandle. Then $a\mapsto L_a$ is a quandle homomorphism of $(Q,*)$ onto a conjugation quandle over the group* $\mathrm{LMlt}(Q,*)$.

Proof. Left distributivity implies $a*(b*(a\backslash x)) = (a*b)*x$, hence $L_a * L_b = L_aL_bL_a^{-1} = L_{a*b}$. □

This homomorphism is rarely an embedding, even for connected quandles. However, it is an embedding for every latin quandle, because, in a latin quandle, $L_a(x) = a*x \neq b*x = L_b(x)$ for every $a\neq b$ and every x. Hence, every latin quandle *is* a conjugation quandle, up to isomorphism. This observation can probably be attributed to Stein [84]. He also found the following criterion.

Proposition 4.2 ([84])**.** *Let $(G,\cdot)$ be a group, Q a subset of G closed with respect to conjugation, and assume that for every $a,b,c\in Q$, $aN_G(c) = bN_G(c)$ iff $a=b$. Then the conjugation quandle $(Q,*)$ is latin.*

A few structural results on quandles have been proved using the Cayley representation. For instance, Kano, Nagao and Nobusawa [41] used it for involutory quandles (in this case, the quandle is represented by involutions), and proved the following characterization of involutory quandles that are latin.

Theorem 4.3 ([41])**.** *A finite involutory quandle $(Q,*)$ is a quasigroup if and only if the derived subgroup* $\mathrm{LMlt}(Q,*)'$ *has odd order.*

The proof is not easy and uses Glauberman's Z^*-theorem. They conclude that involutory left distributive quasigroups are solvable, and possess the Lagrange and Sylow properties (see Section 6.3 for a more comprehensive discussion).

The Cayley representation is fundamental in Pierce's work on involutory quandles [74], and McCarron [59] used conjugation to represent simple quandles and to argue that there were no connected quandles with $2p$ elements, for any prime $p > 5$ (see also Section 6.2).

Let $(G,\cdot)$ be a group, or, more generally, a Bol loop. The binary algebra $(G,*)$ with

$$a * b = a \cdot b^{-1}a$$

is an involutory quandle, called the *core* of $(G,\cdot)$. The core is a quasigroup if and only if the loop is uniquely 2-divisible [3, Theorem 9.4]. The core operation was introduced by Bruck who proved that isotopic Moufang loops have isomorphic cores [10]. It was later picked up by Belousov and others to construct some of the first examples of involutory left distributive quasigroups, see e.g. [3, Chapter IX] or [89].

Example 4.4. The smallest non-medial involutory left distributive quasigroup has order 15 and it is the core of the B-loop constructed in Example 2.6. Explicitly, it is the quasigroup $(\mathbb{Z}_5 \times \mathbb{Z}_3, *)$ with

$$(a,x) * (b,y) = (\mu_{x,y}a - b, -x-y)$$

where $\mu_{x,y} \in \mathbb{Z}_5^*$ are given by the following table:

	0	1	2
0	2	-1	-1
1	-1	2	-1
2	-1	-1	2

5. Left distributive quasigroups: Isotopy

5.1. **Right linear representation.** Restricting self-distributivity to only one side, it is natural to expect that the loop counterpart will admit one of the weaker one-sided loop conditions mentioned in Section 2.2. There are good news and bad news. Left distributive quasigroups are polynomially equivalent to a certain class of "non-associative modules", satisfying a (very) weak associative law. However, the connection is non-linear (only one of the defining mappings is an automorphism), and the corresponding class of loops, called *Belousov-Onoi loops* here, extends beyond the well-established theories (except for some special cases). The correspondence is therefore of limited utility at the moment. Nevertheless, it is interesting to look at details. Most of the ideas of the present section were discovered by Belousov and Onoi [5], but our presentation is substantially different.

Let $(Q,\cdot)$ be a loop and ψ its automorphism. We will call $(Q,\cdot,\psi)$ a *Belousov-Onoi module* (shortly, *BO-module*) if

(BO) $$\varphi(ab)\cdot\psi(ac) = a\cdot\varphi(b)\psi(c)$$

holds for every $a,b,c \in Q$, where $\varphi(x) = x/^{\cdot}\psi(x)$ is the *companion mapping* for ψ. (The explanation why is it reasonable to consider such structures as "non-associative modules" has been explained at the end of Section 2.3.) To match the identity (BO) to the Bol identity, substitute $\psi^{-1}(ac)$ for c and obtain an equivalent identity

(BO') $$\varphi(ab)\cdot(\psi(a)\cdot ac) = a\cdot(\varphi(b)\cdot ac).$$

Example 5.1. We state a few examples of Belousov-Onoi modules.

(1) Every loop $(Q,\cdot)$ turns into the BO-module $(Q,\cdot,id)$. If $\psi(x)=x$, then $\varphi(x)=1$ and thus the identity (BO) holds.
(2) Every group $(Q,\cdot)$ with any automorphism ψ turns into the BO-module $(Q,\cdot,\psi)$. Condition (BO) is easily verified.
(3) Every Bruck loop $(Q,\cdot)$ turns into the BO-module $(Q,\cdot,^{-1})$. If $\psi(x)=x^{-1}$, then $\varphi(x)=x^2$ by power-associativity, and we verify (BO') by $(ab)^2\cdot(a^{-1}\cdot ac)=(ab)^2\cdot c=a\cdot(b^2\cdot ac)$ using Lemma 2.4 in the second step.

Call a BO-module *non-trivial* if $\psi\neq id$. There are relatively few loops that turn into a non-trivial BO-module, see the values of $BOM(n)$ in Table 2. Nevertheless, nearly all groups and all Bruck loops (except possibly those where $x^{-1}=x$) have the property.

A BO-module turns naturally into a quandle. The proof illustrates very well the conditions imposed by the definition.

Proposition 5.2. *Let $(Q,\cdot,\psi)$ be a Belousov-Onoi module, φ the companion mapping, and define for every $a,b\in Q$*

$$a*b=\varphi(a)\cdot\psi(b).$$

Then $(Q,*)$ is a quandle. The quandle is a quasigroup if and only if φ is a permutation.

Proof. Idempotence explains the definition of the companion mapping: we have $a*a=a$ iff $\varphi(a)\cdot\psi(a)=a$ iff $\varphi(a)=a/^{\cdot}\psi(a)$.

Unique left division follows from the fact that ψ is a permutation: we have $a*x=\varphi(a)\cdot\psi(x)=b$ iff $\psi(x)=\varphi(a)\backslash^{\cdot}b$ iff $x=\psi^{-1}(\varphi(a)\backslash^{\cdot}b)$.

Left distributivity is verified as follows: expanding the definition of $*$ and using the identity (BO), we obtain

$$(a*b)*(a*c)=\varphi(\varphi(a)\psi(b))\cdot\psi(\varphi(a)\psi(c))=\varphi(a)\cdot(\varphi\psi(b)\cdot\psi^2(c)),$$

and since ψ is an automorphism and φ a term operation, we have $\varphi\psi=\psi\varphi$, and thus the right hand side equals

$$\varphi(a)\cdot(\psi\varphi(b)\cdot\psi^2(c))=\varphi(a)\cdot\psi(\varphi(b)\psi(c))=a*(b*c).$$

Unique right division is dual to the left case: it happens if and only if φ is a permutation. □

Example 5.3. Consider the three items from Example 5.1.

(1) Any trivial BO-module $(Q,\cdot,id)$ results in a projection quandle $(Q,*)$ with $a*b=b$.
(2) The BO-module $(Q,\cdot,\psi)$, constructed over a group with an automorphism, results in a homogeneous quandle $(Q,*)$ with

$$a*b=a\psi(a^{-1}b).$$

If Q is finite, then $(Q,*)$ is a quasigroup if and only if ψ is a regular automorphism (i.e. the unit is the only fixed point of ψ). Belousov [3, Theorem 9.2] proves that all left distributive quasigroups isotopic to a group result in this particular way, and Galkin [24, Section 5] shows a number of interesting properties of such quasigroups. See Construction 6.1 for a generalization of this idea which covers all left distributive quasigroups.
(3) The BO-module $(Q,\cdot,^{-1})$, constructed over a Bruck loop, results in an involutory quandle $(Q,*)$ with $a*b=a^2b^{-1}$. It follows from Lemma 2.4(2) that $x\mapsto x^2$ is a homomorphism from $(Q,*)$ to the core of $(Q,\cdot)$; hence, if $(Q,\cdot)$ is a B-loop, then the two constructions result in isomorphic quasigroups. In Theorem 5.9, we shall see that all involutory left distributive quasigroups result this way.

Relatively few quandles admit a *Belousov-Onoi representation* as in Proposition 5.2, see the values of $BOQ(n)$ in Table 2. Even connected quandles do not always result from a BO-module:

for example, a quick computer search reveals that none of the quandles constructed over a BO-module of order 6 is connected (compare to [35, Table 2]). In the latin case, however, the situation is different. The setting of BO-modules was designed by Belousov and Onoi in order to prove that all left distributive quasigroups (latin quandles) admit a representation as in Proposition 5.2.

A loop $(Q,\cdot)$ possesing an automorphism ψ such that $(B,\cdot,\psi)$ is a BO-module and the companion mapping for ψ is a permutation, will be called a *Belousov-Onoi loop* (shortly, *BO-loop*) with respect to ψ. (The original name was *S-loops*, for no apparent reason. Our definition uses the characterizing condition of [5, Theorem 4].)

Proposition 5.4 ([5])**.** *Let $(Q,*)$ be a left distributive quasigroup, $e\in Q$ and let*

$$a\cdot b=(a/e)*(e\backslash b).$$

Then $(Q,\cdot)$ is a Belousov-Onoi loop with respect to $\psi=L_e$, the companion mapping is $\varphi=R_e$ and

$$a*b=\varphi(a)\cdot\psi(b).$$

Moreover, different choices of e result in isomorphic loops.

Proof. First notice that $a*b=(a*e)\cdot(e*b)=\varphi(a)\cdot\psi(b)$. Indeed, both φ,ψ are permutations and φ is the companion for ψ, since $\varphi(a)\cdot\psi(a)=a$. To prove that ψ is an automorphism of $(Q,\cdot)$, we calculate for every $a,b\in Q$

$$\begin{aligned}\psi(ab)=e*ab&=e*((a/e)*(e\backslash b))\\&=(e*(a/e))*(e*(e\backslash b))\\&=((e*a)/e)*(e\backslash(e*b)=(e*a)\cdot(e*b)=\psi(a)\psi(b).\end{aligned}$$

In the third and fourth steps, we used left distributivity: in the latter case, since L_e is an automorphism of $(Q,*)$, we also have $L_e(x/y)=L_e(x)/L_e(y)$ for every x,y. To prove the condition (BO), we calculate for every $a,b\in Q$

$$\begin{aligned}\varphi(ab)\cdot\psi(ac)&=(ab*e)\cdot(e*ac)=ab*ac\\&=((a/e)*(e\backslash b))*((a/e)*(e\backslash c))\\&=(a/e)*((e\backslash b)*(e\backslash c))\\&=(a/e)*(e\backslash(b*c))=a\cdot(b*c)=a\cdot\varphi(b)\psi(c).\end{aligned}$$

In the fourth and fifth steps, we used left distributivity: in the latter case, using the fact that L_e^{-1} is also an automorphism of $(Q,*)$.

Let $e_1,e_2\in Q$ and consider an automorphism ρ of $(Q,*)$ such that $\rho(e_1)=e_2$ (for example, we can take $\rho=L_{e_2/e_1}$). Then ρ is an isomorphism of the corresponding loops $(Q,\cdot_1)$ and $(Q,\cdot_2)$, since

$$\rho(a\cdot_1 b)=\rho((a/e_1)*(e_1\backslash b))=(\rho(a)/\rho(e_1))*(\rho(e_1)\backslash\rho(b))=\rho(a)\cdot_2\rho(b)$$

for every $a,b\in Q$. □

If $(Q,\cdot)$ is a Belousov-Onoi loop with respect to ψ, the companion mapping φ is usually not an automorphism. In such a case, the representation of $(Q,*)$ over $(Q,\cdot)$ will be called *right linear*. In Proposition 5.7, we shall prove that φ is an automorphism if and only if the loop is commutative Moufang. Therefore, according to Theorem 3.3, we do not have a linear representation, unless we handle a (both-side) distributive quasigroup.

Still, the left distributive quasigroup $(Q,*)$ (formally, the algebra $(Q,*,\backslash,/)$) is *polynomially equivalent* to the Belousov-Onoi module $(Q,\cdot,\psi)$ (formally, the algebra $(Q,\cdot,\backslash^{\cdot},/^{\cdot},\psi,\psi^{-1})$): all operations in Proposition 5.4 were defined polynomially, the same can be shown about the division operations, and $\varphi(x)=x/^{\cdot}\psi(x)$ is a polynomial, too. In fact, we can think of the mapping φ as *quadratic* over the BO-module $(Q,\cdot,\psi)$, as the variable x appears only twice in its definition.

Combining Propositions 5.2 and 5.4, we can formulate the following representation theorem.

Theorem 5.5 ([5])**.** *The following are equivalent for a quasigroup* $(Q, *)$*:*

1. *it is left distributive;*
2. *it is right linear over a Belousov-Onoi loop (with respect to the automorphism used in the right linear representation).*

Example 5.6. The smallest non-associative Belousov-Onoi loops have order 15, and there are two of them (up to isomorphism). One is a B-loop, see Example 2.6. The other one can be constructed by a modification of the previous construction. Consider the loop $(\mathbb{Z}_5 \times \mathbb{Z}_3, \cdot)$ with

$$(a,x)\cdot(b,y) = (\varphi_{x,y}a + b + \theta_{x,y}, x+y)$$

where $\varphi_{x,y} \in \mathbb{Z}_5^*$ are as before, and $\theta_{x,y} \in \mathbb{Z}_5$ are given by the following table:

	0	1	2
0	0	0	0
1	0	-1	1
2	0	-2	2

It is straightforward to check that this is a BO-loop with respect to the automorphism $(a,x) \mapsto (-a+\delta_{x,2}, -x)$ where $\delta_{x,y} = 1$ if $x = y$ and $\delta_{x,y} = 0$ otherwise. It is not a B-loop, it does not even have the LIP. It is also an abelian extension of $\mathbb{Z}_5$ by $\mathbb{Z}_3$. If we set $\theta_{x,y} = 0$ for every x, y, we would have obtained the B-loop of Example 2.6.

Correspondingly, the smallest non-medial left distributive quasigroups have order 15, and there are two of them (up to isomorphism). One is involutory, see Example 4.4. The other one can be constructed as $(\mathbb{Z}_5 \times \mathbb{Z}_3, *)$ with

$$(a,x) * (b,y) = (\mu_{x,y}a - b + \tau_{x,y}, -x-y)$$

where $\mu_{x,y} \in \mathbb{Z}_5^*$ is as before, and $\tau_{x,y} = \delta_{x-y,1}$ for every x, y. (See [13, 14] for a generalization of this construction, originally suggested by Galkin [26].)

5.2. **Belousov-Onoi loops.** Given the correspondence of Theorem 5.5, a natural question arises. What are these Belousov-Onoi loops? Can we use an established part of loop theory to investigate left distributive quasigroups? The current state of knowledge is unsatisfactory in this respect. In the rest of the section, we summarize most of the known results on BO-loops.

First of all, it is not even clear how to construct Belousov-Onoi loops which are not B-loops. All BO-loops of order less than 15 are abelian groups, and there are two non-associative BO-loops of order 15, see Example 5.6. Nowadays, these facts are easy to check on a computer, but back in the 1970s, this was realized only indirectly, via Theorem 5.5, using the theory of left distributive quasigroups. The first example of a left distributive quasigroup not isotopic to any Bol loop was constructed by Onoi in [67]. The construction is quite intricate, and occupies a major part of the paper: Onoi starts with 2×2 matrices over a certain non-associative ring with four elements, takes a quadratic operation on pairs of the matrices, and then creates a left distributive isotope; thus, the quasigroup has order 2^{16}. The smallest example, of order 15, was found later by Galkin in [26]. We see the situation twisted: it is not the loops that reveal properties of the quasigroups, it is the other way around!

Table 2 shows some enumeration results related to Belousov-Onoi loops. The upper part compares the numbers $L(n)$ of all loops, $BOM(n)$ of loops that turn into a non-trivial BO-module, and $BOL(n)$ of BO-loops, of order n up to isomorphism. The lower part compares the numbers $Q(n)$ of all quandles, $BOQ(n)$ of quandles that admit a Belousov-Onoi representation as in Proposition 5.2, and $LQ(n)$ of latin quandles (left distributive quasigroups), of order n up to isomorphism. The sequences $L(n)$, $Q(n)$ are well known [66], the other numbers were calculated using an exhaustive computer search.

n	1	2	3	4	5	6	7	8
$L(n)$	1	1	1	2	6	109	23746	106228849
$BOM(n)$	0	0	1	1	1	3	1	144
$BOL(n)$	1	0	1	1	1	0	1	3
$Q(n)$	1	1	3	7	22	73	298	1581
$BOQ(n)$	1	1	2	3	4	3	6	9
$LQ(n)$	1	0	1	1	3	0	5	2

Table 2. Enumeration of small loops and quandles related to the Belousov-Onoi representation.

In the rest of the section, we present a few results that relate the Belousov-Onoi loops to more established classes of loops, and specialize the correspondence between left distributive quasigroups and Belousov-Onoi loops, proved in Theorem 5.5, on two important subclasses: the distributive quasigroups, and the involutory left distributive quasigroups.

We start with a variation on [68, Theorem 2]. Our proof, based on Theorem 2.2 (the Pflugfelder's part), is much simpler.

Proposition 5.7. *Let $(Q,\cdot)$ be a loop, ψ an automorphism of $(Q,\cdot)$ and assume its companion mapping φ is a permutation. Then any two of the following properties imply the third:*

- *$(Q,\cdot)$ is a Belousov-Onoi loop with respect to ψ;*
- *$(Q,\cdot)$ is a commutative Moufang loop;*
- *φ is an automorphism.*

Proof. According to Theorem 2.2, $(Q,\cdot)$ is a commutative Moufang loop if and only if, for some mapping f on Q, the identity $f(x)y\cdot xz = f(x)x\cdot yz$ holds. Let $f=\varphi\psi^{-1}$ and substitute $x=\psi(a)$, $y=\varphi(b)$, $z=\psi(c)$. We obtain that $(Q,\cdot)$ is a commutative Moufang loop if and only if $\varphi(a)\varphi(b)\cdot\psi(a)\psi(c)=\varphi(a)\psi(a)\cdot\varphi(b)\psi(c)=a\cdot\varphi(b)\psi(c)$ for every $a,b,c\in Q$. Consider the following three expressions:

$$X=\varphi(a)\varphi(b)\cdot\psi(a)\psi(c)$$
$$Y=a\cdot\varphi(b)\psi(c)$$
$$Z=\varphi(ab)\cdot\psi(a)\psi(c)$$

We just proved that $X=Y$ for every $a,b,c\in Q$ iff $(Q,\cdot)$ is commutative Moufang. According to condition (BO), $Y=Z$ for every $a,b,c\in Q$ iff $(Q,\cdot)$ is a BO-loop with respect to ψ. And, obviously, $X=Z$ for every $a,b,c\in Q$ iff φ is an automorphism of $(Q,\cdot)$. □

Now we can reprove Belousov's result that every distributive quasigroup is linear over a commutative Moufang loop (a similar argument is presented in [68, Theorem 3]).

Proof of Theorem 3.3, (3) ⇒ (4). Let $(Q,*)$ be a distributive quasigroup, pick $e\in Q$ a let $a\cdot b=(a/e)*(e\backslash b)$. Since $(Q,*)$ is left distributive, $(Q,\cdot)$ is a BO-loop with respect to L_e, which in turn is an automorphism of $(Q,\cdot)$. Since $(Q,*)$ is right distributive, $(Q,\cdot)$ is also a right(!) BO-loop (this is irrelevant for us) with respect to R_e, which in turn is an automorphism of $(Q,\cdot)$. We showed that the companion of L_e is an automorphism, hence $(Q,\cdot)$ is a commutative Moufang loop by Proposition 5.7. □

Next we show that B-loops are precisely the BO-loops with respect to the left inverse mapping.

Proposition 5.8 ([5, Theorem 8])**.** *Let $(Q,\cdot)$ be a loop and $\psi(x)=x\dot{\backslash}1$. Then $(Q,\cdot)$ is a Belousov-Onoi loop with respect to ψ if and only if it is a B-loop.*

Proof. The backward implication was proved in Example 5.1(3). In the forward direction, condition (BO) with $b = 1$ and $c = a$ says that $\varphi(a)\psi(a^2) = a\psi(a) = 1$, and thus

$$\varphi(a) = 1/^{\cdot}\psi(a^2) = 1/^{\cdot}(a^2\backslash^{\cdot}1) = a^2$$

for every $a \in Q$. Hence, $(Q, \cdot)$ is a uniquely 2-divisible loop with the LAIP. Now, condition (BO), upon substitution of $\psi^{-1}(c)$ for c, says that $(ab)^2 \cdot ((a\backslash^{\cdot}1) \cdot c) = a \cdot b^2c$, and we can use Theorem 2.5 to conclude that $(Q, \cdot)$ is a Bol loop. □

With the aid of Proposition 5.8, we establish the correspondence between involutory left distributive quasigroups and B-loops. This connection has a rich history: it was first realized by Robinson in his 1964 PhD thesis, but published only 15 years later in [75]. Independently, Belousov and Florya [4, Theorem 3] noticed that involutory left distributive quasigroups are isotopic to Bol loops, but they did not formulate the full correspondence. Independently, the theorem was formulated by Kikkawa [52] (at the first glance, it is not obvious that his loop axioms are equivalent to those of B-loops, as he uses condition (2') of Theorem 2.5 instead of the Bol identity). The theorem was rediscovered once more in [62, Theorems 2.5 and 2.7]. Unlike all of the other representation theorems in the present paper, Theorem 5.9 has a fairly straightforward direct proof, and contemporary ATP systems can prove it within a second.

Theorem 5.9 ([52, 62, 75])**.** *The following are equivalent for a quasigroup $(Q, *)$:*

(1) *it is involutory left distributive;*
(2) *there is a B-loop $(Q, \cdot)$ such that $a * b = a^2 \cdot b^{-1}$.*

Proof. (1) ⇒ (2) Consider the quasigroup operation $a \cdot b = (a/e) * (e\backslash b)$. According to Theorem 5.5, $(Q, \cdot)$ is a BO-loop with respect to L_e. If we prove that $L_e(x) = x\backslash^{\cdot}1$, Proposition 5.8 applies and $(Q, \cdot)$ is a B-loop. Then, clearly, the companion mapping is $\varphi(x) = x^2$, and thus $a * b = a^2 \cdot b^{-1}$.

We need to check that $L_e(a) = e * a$ equals $a\backslash^{\cdot}1 = a\backslash^{\cdot}e$ for every $a \in Q$. We have $e * a = a\backslash^{\cdot}e$ iff $a \cdot (e * a) = e$ iff $(a/e) * a = e$ (we expanded the definition of $\cdot$). Now multiply the last identity by a/e from the left, and obtain $(a/e) * ((a/e) * a) = (a/e) * e = a$, which is always true thanks to the involutory law.

(2) ⇒ (1) Left distributivity was verified in Proposition 5.2 through Example 5.1(3). It is involutory, as $a * (a * b) = a^2(a^2b^{-1})^{-1} = a^2(a^{-2}b) = b$ thanks to the AIP and LIP in Bruck loops. □

As far as we know, only two papers, [5, 68], are devoted to Belousov-Onoi loops. We state two more results here. The first one identifies some important subclasses of BO-loops, see [5, Theorem 2], [68, Theorem 1] and [5, Theorem 3], respectively.

Proposition 5.10 ([5, 68])**.** *Let $(Q, \cdot)$ be a Belousov-Onoi loop.*

(1) *It is Bol if and only if it is left alternative.*
(2) *It is Moufang iff it is right alternative, iff it has the RIP, iff the identity $(xy)^{-1} = y^{-1}x^{-1}$ holds, iff the identity $x \cdot yx = xy \cdot x$ holds.*
(3) *It is a group if and only if it is left alternative and every square is nuclear.*

The second is a characterization of Belousov-Onoi loops that matches well with Theorem 2.5 on B-loops.

Theorem 5.11 ([5])**.** *The following are equivalent for a loop $(Q, \cdot)$ with an automorphism ψ such that its companion mapping φ is a permutation:*

(1) *it satisfies the identity $\varphi(x) \cdot \psi(x)y = xy$ and it is left automorphic as a BO-module (i.e. the left inner mappings are automorphisms of $(Q, \cdot, \psi)$);*
(1') *the identities $\varphi(x) \cdot \psi(x)y = xy$ and $L_{x,y}\psi = \psi L_{x,y}$ hold;*

(2) *it satisfies condition (BO).*

Proof sketch. The equivalence of (1') and (2) is proved in [5, Theorem 4]. Condition (1') is a special case of (1). It remains to prove that in any BO-loop $(Q,\cdot)$, every inner mapping $L_{x,y}$ is an automorphism of $(Q,\cdot,\psi)$. It respects ψ as postulated in (1'). According to Theorem 5.5, $(Q,\cdot)$ is isotopic to a left distributive quasigroup, and Belousov and Florya prove in [4, Theorem 2] that every loop isotope of a left distributive quasigroup (actually, more generally, of any F-quasigroup) is left automorphic. □

We are not aware of any general structural results on left distributive quasigroups proved using the correspondence of Theorem 5.5. Actually, with the efficient methods we will describe in Section 6, the correspondence could be used in the other direction, to investigate properties of Belousov-Onoi loops via left distributive quasigroups.

Nevertheless, in the involutory case, loop theory helps considerably, as the theory of Bruck loops is well developed. One example for all: Glauberman proved that finite B-loops are solvable, and that analogies of the Lagrange and Sylow theorems hold (see [31, Section 8] for precise statements). Since a B-loop $(Q,\cdot)$ and its corresponding involutory left distributive quasigroup $(Q,*)$ are polynomially equivalent, they share all the properties defined by polynomial operations. For instance, congruences and solvability. The polynomial correspondence uses a single constant, e, therefore, the subloops of $(Q,\cdot)$ are exactly the subquasigroups of $(Q,*)$ containing e. Since e can be chosen arbitrarily, the Lagrange and Sylow properties are shared by $(Q,*)$ as well. In Section 6.3, we put these results into a broader context.

6. Left distributive quasigroups: Homogeneous representation

6.1. **Homogeneous representation.**

Our exposition in this section follows our recent paper [35] where many older ideas are collected and adjusted to the modern quandle setting. A reader interested in more details (proofs in particular), is recommended to consult [35]. Here we try to reference the original sources.

Recall that a quandle Q is *homogeneous*, if $\mathrm{Aut}(Q)$ acts transitively on Q. Since $\mathrm{LMlt}(Q)$ is a subgroup of $\mathrm{Aut}(Q)$, all connected quandles (and thus all left distributive quasigroups) are homogeneous.

It is not clear who came up with Construction 6.1. But it was certainly Galkin [24] who recognized its importance for representing self-distributive algebraic structures, followed independently by Joyce and others (perhaps a partial credit could be paid to Loos [57], too).

Construction 6.1 ([24, 40])**.** Let $(G,\cdot)$ be a group, H its subgroup, and ψ an automorphism of $(G,\cdot)$ such that $\psi(a)=a$ for every $a\in H$. Such a triple (G,H,ψ) will be called *admissible.* Denote G/H the set of left cosets $\{aH : a\in G\}$, and consider the binary algebra $\mathcal{Q}(G,H,\psi)=(G/H,*)$ with

$$aH*bH=a\psi(a^{-1}b)H.$$

It is straightforward to verify that $\mathcal{Q}(G,H,\psi)$ is a homogeneous quandle. If G is finite, then $\mathcal{Q}(G,H,\psi)$ is a quasigroup if and only if, for every $a,u\in G$, $a\psi(a^{-1})\in H^u$ implies $a\in H$.

Note that the operation can be written as $aH*bH=\varphi(a)\psi(b)H$, where φ is the companion mapping to ψ, so this really is, in a way, a variation on the isotopy method. Also note that the special case $\mathcal{Q}(G,1,\psi)$, with the trivial subgroup $H=1$, is the same construction as in Example 5.3(2).

Example 6.2. According to Theorem 3.1, medial idempotent quasigroups are precisely the quasigroups $\mathcal{Q}(G,1,\psi)$ where G is an abelian group and ψ is an automorphism such that its companion is a permutation (and therefore an automorphism, too).

In the present section, we will denote conjugation as $a^b = bab^{-1}$ (unlike most texts on group theory, we use the right-left composition of mappings, hence it is natural to use the dual notation for conjugation). Similarly, we will denote $a^G = \{a^g : g \in G\}$ the conjugacy class of a in G, $H^b = \{h^b : h \in H\}$, and $-^b$ the mapping $x \mapsto x^b$. If G is a group acting on a set X and $e \in X$, we will denote e^G the orbit containing e, and G_e the stabilizer of e.

The following observation appeared in many sources in various forms, its complete proof can be found e.g. in [35, Section 3].

Proposition 6.3. *Let $(Q,*)$ be a quandle and $e \in Q$. Let G be a normal subgroup of* $\mathrm{Aut}(Q,*)$. *Then $(G, G_e, -^{L_e})$ is an admissible triple and the orbit subquandle $(e^G,*)$ is isomorphic to the quandle $\mathcal{Q}(G, G_e, -^{L_e})$.*

Proof sketch. Since $-^{L_e}$ is a restriction of an inner automorphism to a normal subgroup, it is an automorphism of G. It is straightforward to check that it fixes the stabilizer pointwise. Consider the bijective mapping $f : G/G_e \to e^G$, $\alpha G_e \mapsto \alpha(e)$. Again, it is straightforward to check that this is a quandle isomorphism $\mathcal{Q}(G, G_e, -^{L_e}) \simeq (e^G,*)$. □

Consider three particular choices of the normal subgroup: $G = \mathrm{Aut}(Q,*)$, $G = \mathrm{LMlt}(Q,*)$ and $G = \mathrm{LMlt}(Q,*)'$, respectively. If G acts transitively on Q, Proposition 6.3 claims the following:

- Every homogeneous quandle $(Q,*)$ is isomorphic to $\mathcal{Q}(G, G_e, -^{L_e})$ with $G = \mathrm{Aut}(Q,*)$.
- Every connected quandle $(Q,*)$ is isomorphic to $\mathcal{Q}(G, G_e, -^{L_e})$ with $G = \mathrm{LMlt}(Q,*)$. This will be called the *canonical representation* of $(Q,*)$.
- Every connected quandle $(Q,*)$ is isomorphic to $\mathcal{Q}(G, G_e, -^{L_e})$ with $G = \mathrm{LMlt}(Q,*)'$. This will be called the *minimal representation* of $(Q,*)$. (To make it work, one has to show that the actions of $\mathrm{LMlt}(Q,*)$ and $\mathrm{LMlt}(Q,*)'$ have identical orbits [24, 40].)

Corollary 6.4 ([40, Theorem 7.1])**.** *A quandle is isomorphic to $\mathcal{Q}(G,H,\psi)$ for some admissible triple (G,H,ψ) if and only if it is homogeneous.*

Why minimal representation? Galkin [24, Theorem 4.4] proved the following fact: if a connected quandle $(Q,*)$ is isomorphic to $\mathcal{Q}(G,H,\psi)$ for some admissible triple (G,H,ψ), then $\mathrm{LMlt}(Q)'$ embeds into a quotient of G. Hence, if Q is finite, the minimal representation is the one with the smallest group G.

Why canonical representation? Fix a set Q and an element e. We have a 1-1 correspondence between connected quandles $(Q,*)$ on one side, and certain configurations in transitive groups acting on Q on the other side. A *quandle envelope* is a pair (G,ζ) where G is a transitive group on Q and $\zeta \in Z(G_e)$ (here Z denotes the center) such that $\langle \zeta^G \rangle = G$. The correspondence is given by the following two mutually inverse mappings:

$$\begin{array}{rcl} \text{connected quandle} & \leftrightarrow & \text{quandle envelope} \\ (Q,*) & \to & (\mathrm{LMlt}(Q,*), L_e) \\ \mathcal{Q}(G, G_e, -^{\zeta}) & \leftarrow & (G,\zeta) \end{array}$$

If Q is finite, then an envelope (G,ζ) corresponds to a latin quandle if and only if $\zeta^{-1}\zeta^{\alpha}$ has no fixed point for every $\alpha \in G \smallsetminus G_e$. Moreover, two envelopes (G_1,ζ_1) and (G_2,ζ_2) yield isomorphic quandles if and only if there is a permutation f of Q such that $f(e) = e$, $\zeta_1^f = \zeta_2$ and $G_1^f = G_2$ (in particular, the two groups are isomorphic). See [35, Section 5] for details, and [35, Section 7] for a plenty of illustrative examples (the correspondence seems to be an original contribution of the paper).

Canonical representation is arguably the most powerful tool currently available to study connected quandles, and left distributive quasigroups in particular, as we shall see in the remaining part of the section.

6.2. **Enumeration.** Canonical representation allows to enumerate connected quandles (left distributive quasigroups in particular) with n elements, provided a classification of transitive groups of degree n. Currently, such a library is available for $n \leq 47$. The enumeration of small connected quandles was carried out in [35, 90]. Here, in Table 3, we present the numbers of quasigroups, where $LD(n)$ refers to non-medial left distributive ones, and $ILD(n)$ to non-medial involutory left distributive ones, of order n up to isomorphism. We recall from Section 3.2 that $MI(n)$ denotes the number of medial idempotent quasigroups and can be determined by Hou's formulas [34].

n	1	2	3	4	5	6	7	8	9	10	11	12	13	14	**15**	16
$LD(n)$	0	0	0	0	0	0	0	0	0	0	0	0	0	0	**2**	0
$ILD(n)$	0	0	0	0	0	0	0	0	0	0	0	0	0	0	**1**	0
$MI(n)$	1	0	1	1	3	0	5	2	8	0	9	1	11	0	3	9

n	17	18	19	20	**21**	22	23	24	25	26	**27**	**28**	29	30	31	32
$LD(n)$	0	0	0	0	**2**	0	0	0	0	0	**32**	**2**	0	0	0	0
$ILD(n)$	0	0	0	0	**1**	0	0	0	0	0	**4**	**0**	0	0	0	0
$MI(n)$	15	0	17	3	5	0	21	2	34	0	30	5	27	0	29	8

	33	34	35	**36**	37	38	**39**	40	41	42	43	44	**45**	46	47
$LD(n)$	**2**	0	0	**1**	0	0	**2**	0	0	0	0	0	**12**	0	0
$ILD(n)$	**1**	0	0	**0**	0	0	**1**	0	0	0	0	0	**3**	0	0
$MI(n)$	9	0	15	8	35	0	11	6	39	0	41	9	24	0	45

Table 3. Enumeration of small left distributive quasigroups.

From the historical perspective, the first serious attempt on enumeration was carried out by Galkin [26] who calculated (without a computer!) the numbers $LD(n)$ for $n < 27$, and found that $LD(27) \geq 3$. A few results in the involutory case can be found in an earlier paper by Nobusawa [64]. In [90], Vendramin enumerated connected quandles of size $n \leq 35$, which was the state-of-the-art in the classification of transitive groups at the time, but his algorithm works for larger orders as well.

One can make a few observations about Table 3. Most obviously, we do not see any left distributive quasigroups (medial or not) with $4k + 2$ elements. This is true for every k, as proved by Stein already in the 1950s [83, Theorem 9.9].

Theorem 6.5 ([83])**.** *There are no left distributive quasigroups of order $4k + 2$, for any $k \geq 0$.*

The fact is easy to observe in the medial case: any medial idempotent quasigroup of order $4k+2$ is linear over an abelian group which is the direct product of $\mathbb{Z}_2$ and a group of odd order; however, there is no idempotent quasigroup of order 2. Stein's remarkable argument uses a topological reasoning, constructing a triangulated polyhedron from the graph of the quasigroup and discussing parity of its Euler characteristic (for details, see [83] or [30, Section 6]). In [85], Stein observed that the result extends to all homogeneous quasigroups, since each of them is isotopic to an idempotent quasigroup and the same method as in the self-distributive case proves non-existence. In [24, Theorem 6.1], Galkin proved Stein's theorem using a short group theoretical argument about the minimal representation.

Let us note that connected quandles of order $4k + 2$ do exist, although there are no connected quandles with $2p$ elements for any prime $p > 5$ [35, 59].

Our second observation about Table 3 is that there are severe restrictions on the admissible orders of non-medial left distributive quasigroups. Many gaps are justified by the following theorem.

Theorem 6.6 ([19, 32])**.** *Every connected quandle with p or p^2 elements, p prime, is medial.*

The prime case was proved by Galkin [24] for quasigroups, and by Etingof, Soloviev and Guralnick [19] for connected quandles. A conceptually simpler proof using canonical representation can be found in [35, Section 8], here is an outline. First, use a group-theoretical result by Kazarin: in a finite group G, if $|a^G|$ is a prime power, then $\langle a^G \rangle$ is solvable; with little work, it follows that if Q is a connected quandle of prime power size, then $\mathrm{LMlt}(Q)$ is solvable. Now recall that a transitive group (here: $\mathrm{LMlt}(Q)$) acting on a set of prime size (here: Q) is primitive, and apply a theorem of Galois stating that any finite solvable primitive group acts as a subgroup of the affine group over a finite field.

The prime square case for quasigroups is claimed by Galkin in [30] but never appeared in print; for connected quandles, it was solved by Graña [32]. For involutory left distributive quasigroups, the proof is substantially easier, see [64]. The prime cubed case is discussed in [1], but the classification is not easy to state.

We can also observe that there are no non-medial left distributive quasigroups of order 2^k for $k = 1, 2, 3, 4, 5$. However, this is not a general property: in fact, the first ever example of a left distributive quasigroup not isotopic to a Bol loop, constructed by Onoi [67], has 2^{16} elements. The smallest non-medial connected quandle with 2^k elements exists for $k = 5$, but we do not know the smallest k in the quasigroup case.

Our final observation is that there are precisely two non-medial left distributive quasigroups of order $3p$ for $p = 5, 7, 11, 13$. Two such examples were constructed for every prime $p \geq 5$ by Galkin in [26] (the construction was studied recently in a great detail in [13, 14], see also Example 5.6). It is an open problem whether there exist any other connected quandles with $3p$ elements.

6.3. **Structural properties.** We will mention a few subalgebra and congruence properties here. A finite quasigroup of order n has the *Lagrange property*, if the order of every subquasigroup divides n. It has the *Sylow property*, if, for every maximal prime power divisor p^k of n, there is a subquasigroup of order p^k (stronger versions of the Sylow property exist, and we refer to each particular paper for its own precise definition). Informally, a left distributive quasigroup is called *solvable*, if it can be constructed by a chain of extensions by medial quasigroups; formal definitions differ [25, 41, 65], but they seem to share the following property: a left distributive quasigroup is solvable if and only if its left multiplication group is solvable. (We note that it is not at all clear what is the "correct" notion of solvability for quasigroups and loops, see [82] for a thorough discussion; the particular choice made by Glauberman, following Bruck, is only one of the reasonable options.)

Finite involutory left distributive quasigroups are solvable and have the Lagrange and Sylow properties. This has been proved independently several times, using each of the three methods we have discussed: through the conjugation representation in [41], through the isotopy to B-loops (combining Theorem 5.9 and the results of Glauberman on B-loops [31]), and through the homogeneous representation in [28]. In each case, the underlying group theoretical result is Glauberman's Z*-theorem, which is used to show that the left multiplication group is solvable. An infinite counterexample to solvability is presented in [28].

Later, Galkin generalized the results into the non-involutory setting. In [25], he proves that every finite solvable left distributive quasigroup has the Lagrange property, but not necessarily the Sylow property (a counterexample of order 15 exists). In [27], he proves the Sylow property under the additional assumption that the order of the quasigroup, and the order of its translations, are coprime (this is always true in the involutory case).

Recall that all left distributive quasigroups isotopic to a group admit a homogeneous representation of the form $\mathcal{Q}(G, 1, \psi)$, cf. Example 5.3(2). They also satisfy the Lagrange and Sylow properties [24, Theorem 5.3]. This fact is used to show an important structural feature: a finite left distributive quasigroup with no non-trivial subquasigroups is medial [24, Theorems 5.5 and 7.2].

More information about Galkin's results on left distributive quasigroups can be found in his survey paper [30, Section 6]. A part of Galkin's theory was translated to English and clarified in [91].

7. Open problems

Several interesting problems appeared to us while writing the paper.

7.1. **Commutator theory over "non-associative modules".** Universal algebra develops a commutator theory based on the notion of *abelianess*, related to affine representation over classical modules (see [82] for the commutator theory adapted to loops, and the references thereof). For instance, Theorem 3.1 can be explained in this manner. Is there a meaningful weakening of the principle of abelianess, related to affine representation over some sort of "non-associative modules"? A one that would, for instance, explain Theorem 3.2? To what extent the module theoretic methods can be adapted to the non-associative setting?

7.2. **Non-idempotent generalization of left distributive quasigroups.** Find a "non-idempotent generalization" of Theorem 5.5: describe the class of quasigroups (whose idempotent members are precisely the left distributive quasigroups) that are right affine over Belousov-Onoi loops; perhaps, impose an additional condition on the representation in order to obtain an elegant description of the class. Theorem 3.2 shall follow as an easy consequence of this generalization, just as it happens in the idempotent case (see Section 5.2). We are not aware of any results even in the involutory case (generalizing Theorem 5.9).

7.3. **Enumeration.** The generic problem is, to extend all enumeration results presented in this paper. Perhaps the most interesting questions are:

1. distributive and trimedial quasigroups of order 3^5;
2. commutative Moufang loops of order 3^6 and the corresponding enumeration of distributive and trimedial quasigroups of order 3^6;
3. connected quandles and left distributive quasigroups of order $3p$, p prime, or more generally, pq, p, q primes;
4. left distributive quasigroups of order 2^k, $k > 5$.

Acknowledgement

I am indebted to my former student Jan Vlachý for a thorough research on Galkin's papers and for explaining me their contents and significance. His remarkable student project [91] on enumeration of small left distributive quasigroups convinced me that this is the right approach to left distributive quasigroups in particular, and connected quandles in general.

References

[1] G. Bianco, PhD Thesis, University of Ferrara (2015).

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

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

[4] V. D. Belousov, I. A. Florya, *On left-distributive quasigroups.* Bul. Akad. Ştiinţe RSS Moldoven. 1965/7, 3–13 (Russian).

[5] V. D. Belousov, V. I. Onoi, *On loops isotopic to left distributive quasigroups.* Mat. Issled. 25/3 (1972), 135–152 (Russian).

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

[7] 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.

[8] C. Bergman, *Universal algebra: Fundamentals and selected topics.* Chapman & Hall/CRC Press (2011).

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

[10] R. H. Bruck, *A Survey of Binary Systems.* Ergebnisse der Mathematik und ihrer Grenzgebiete, Springer Verlag, Berlin-Göttingen-Heidelberg, 1958.

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

[12] J. S. Carter, *A survey of quandle ideas.* in: Kauffman, Louis H. (ed.) et al., *Introductory lectures on knot theory,* Series on Knots and Everything 46, World Scientific (2012), 22–53.

[13] W. E. Clark, M. Elhamdadi, X. Hou, M. Saito, T. Yeatman, *Connected quandles associated with pointed abelian groups.* Pac. J. Math. 264/1 (2013), 31–60.

[14] W. E. Clark, X. Hou, *Galkin quandles, pointed abelian groups, and sequence A000712.* Electron. J. Comb. 20/1 (2013), P45, 8 pp.

[15] P. Dehornoy, *Braids and self-distributivity.* Progress in Math. 192, Birkhäuser, Basel (2000).

[16] D. Donovan, T. Griggs, T. McCourt, J. Opršal, D. Stanovský, *Distributive and anti-distributive Mendelsohn triple systems.* Submitted. `http://arxiv.org/abs/1411.5194`.

[17] A. Drápal, *Group isotopes and a holomorphic action.* Results in Math. 54 (2009), 253–272.

[18] A. Drápal, *A simplified proof of Moufang's theorem.* Proc. Amer. Math. Soc. 139 (2011), 93–98.

[19] P. Etingof, A. Soloviev, R. Guralnick, *Indecomposable set-theoretical solutions to the quantum Yang-Baxter equation on a set with a prime number of elements.* J. Algebra **242/2** (2001), 709–719.

[20] B. Fischer, *Distributive Quasigruppen endlicher Ordnung*, Math. Z. 83 (1964), 267–303 (German).

[21] A. Fish, A. Lisitsa, D. Stanovský, *Combinatorial approach to knot recognition.* To appear in: R. Horn (ed.), *Embracing Global Computing in Emerging Economies*, Communications in Computer and Information Science, Springer.

[22] O. Frink, *Symmetric and self-distributive systems*, Am. Math. Monthly 62/10 (1955), 697–707.

[23] V. M. Galkin, *Finite distributive quasigroups.* Mat. Zametki **24** (1978), 39–41 (Russian).

[24] V. M. Galkin, *Left distributive finite order quasigroups.* Mat. Issled. **51** (1979), 43–54 (Russian).

[25] V. M. Galkin, *φ-groups and left distributive quasigroups.* Preprint VINITI No. 4406-81, Gor'kovskiy politechnicheskiy tekhnicheskiy institut, Gorkiy (1981) (Russian).

[26] V. M. Galkin, *Left distributive quasigroups of small orders.* Preprint VINITI No. 6510-84, Gor'kovskiy politechnicheskiy tekhnicheskiy institut, Gorkiy (1984) (Russian).

[27] V. M. Galkin, *Sylow properties in a class of quasigroups.* Mat. Zametki **36/4** (1984), 617–620 (Russian).

[28] V. M. Galkin, *On symmetric quasigroups.* Uspekhi mat. nauk 39/6 (1984), 191–192 (Russian).

[29] V. M. Galkin, *On the Fischer-Smith theorem.* J. Soviet Math. 32/11 (1988), 23–30 (English, Russian original).

[30] V. M. Galkin, *Quasigroups.* Itogi nauki i tekhniki 26 (1988), 3–44 (1988) (Russian). Translated in J. Soviet Math. **49**/3 (1990), 941–967.

[31] G. Glauberman, *On loops of odd order.* J. Alg. 1 (1964), 374–396.

[32] M. Graña, *Indecomposable racks of order p^2.* Beiträge Algebra Geom. **45/2** (2004), 665–676.

[33] D. Herbera, T. Kepka, P. Němec, *Hamiltonian selfdistributive quasigroups.* J. Algebra 289/1 (2005), 70–104.

[34] X. Hou, *Finite modules over $\mathbb{Z}[t,t^{-1}]$.* J. Knot Theory Ramifications **21/8** (2012), 1250079, 28 pp.

[35] A. Hulpke, D. Stanovský, P. Vojtěchovský, *Connected quandles and transitive groups.* To appear in J. Pure Appl. Algebra. `http://arxiv.org/abs/1409.2249`.

[36] J. Ježek, T. Kepka, *Notes on distributive groupoids.* Comment. Math. Univ. Carolinae 24 (1983), 237–249.

[37] J. Ježek, T. Kepka, *Distributive groupoids and symmetry-by-mediality.* Algebra Universalis 19 (1984), 208–216.

[38] J. Ježek, T. Kepka, *Selfdistributive groupoids of small orders,* Czech. Math. J. 47 (1997), 463–468.

[39] J. Ježek, T. Kepka, P. Němec, *Distributive groupoids.* Rozpravy ČSAV 91 (1981).

[40] D. Joyce, *Classifying invariant of knots, the knot quandle.* J. Pure Applied Algebra, 23 (1982), 37–65.

[41] M. Kano, H. Nagao, N. Nobusawa, *On finite homogeneous symmetric sets*, Osaka J. Math. 13 (1976), 399–406.

[42] T. Kepka, *Quasigroups which satisfy certain generalized forms of the Abelian identity.* Čas. pěst. mat. 100/1 (1975), 46–60.

[43] T. Kepka, *Structure of triabelian quasigroups.* Comment. Math. Univ. Carolinae 17/2 (1976), 229–240.

[44] T. Kepka, *Distributive Steiner quasigroups of order 3^5.* Comment. Math. Univ. Carolin. 19 (1978) 389–401.

[45] T. Kepka, *Distributive division groupoids.* Math. Nachr. 87 (1979), 103–107.

[46] T. Kepka, L. Bénéteau, J. Lacaze, *Small finite trimedial quasigroups.* Commun. Algebra 14 (1986), 1067–1090.

[47] T. Kepka, M. Kinyon, J. D. Phillips, *The structure of F-quasigroups.* J. Algebra 317/2 (2007), 435–461.

[48] T. Kepka, M. Kinyon, J. D. Phillips, *F-quasigroups and generalized modules.* Comment. Math. Univ. Carolin. 49/2 (2008), 249–257.

[49] T. Kepka, P. Němec, *Commutative Moufang loops and distributive groupoids of small orders.* Czech. Math. J. 31/106 (1981), 633–669.

[50] T. Kepka, P. Němec, *T-quasigroups. I, II.* Acta Univ. Carolin. Math. Phys., 12/1 (1972), 39–49; 12/2 (1972), 31–49.

[51] H. Kiechle, *Theory of K-loops.* Lecture Notes in Math. 1778, Springer (2002).

[52] M. Kikkawa, *On some quasigroups of algebraic models of symmetric spaces.* Mem. Fac. Lit. Sci., Shimane Univ. (Natur. Sci.) 6 (1973), 9–13.

[53] M. Kikkawa, *On some quasigroups of algebraic models of symmetric spaces II.* Mem. Fac. Lit. Sci., Shimane Univ. (Natur. Sci.) 7 (1974), 29–35.

[54] M. Kikkawa, *Kikkawa loops and homogeneous loops.* Commentat. Math. Univ. Carol. 45/2 (2004), 279–285.

[55] M. Kinyon, J. D. Phillips, *A note on trimedial quasigroups.* Quasigroups and Related Systems, 9 (2002), 65–66.

[56] M. Kinyon, P. Vojtěchovský, *Primary decompositions in varieties of commutative diassociative loops.* Communications in Algebra 37/4 (2009), 1428–1444.

[57] O. Loos, *Symmetric spaces.* J. Benjamin, New York (1969).

[58] S. V. Matveev, *Distributive groupoids in knot theory.* Math. USSR - Sbornik **47/1** (1984), 73–83.

[59] J. McCarron, *Connected quandles with order equal to twice an odd prime.* `http://arxiv.org/abs/1210.2150`.

[60] D. Moskovich, *Associativity vs. Distributivity.* Low Dimensional Topology Blog, July 21, 2014, `https://ldtopology.wordpress.com/2014/07/21/associativity-vs-distributivity`.

[61] D. C. Murdoch, *Structure of abelian quasi-groups.* Trans. Amer. Math. Soc. 49 (1941), 392–409.

[62] P. Nagy, K. Strambach, *Loops, their cores and symmetric spaces*, Israel J. Math. 105 (1998), 285–322.

[63] S. Nelson, *The combinatorial revolution in knot theory.* Notices Amer. Math. Soc. 58/11 (2011), 1553–1561.

[64] N. Nobusawa, *On symmetric structures of a finite set*, Osaka J. Math. 11 (1974), 569–575.

[65] N. Nobusawa, *Some structure theorems on pseudo-symmetric sets*, Osaka J. Math. 20 (1983), 727–734.

[66] OEIS Foundation Inc., *The On-Line Encyclopedia of Integer Sequences.* `http://oeis.org`.

[67] V. I. Onoi, *Left distributive quasigroups that are left homogeneous over a quasigroup.* Bul. Akad. Ştiinţe RSS Moldoven. 1970/2, 24–31 (Russian).

[68] V. I. Onoi, *A connection between S-loops and Moufang loops.* Mat. issledovaniya 7, Izdat. Ştiinţa, Kishinev (1972), 197–212 (Russian).

[69] C. S. Peirce, *On the algebra of logic.* Amer. J. Math. 3 (1880), 15–57.

[70] H. O. Pflugfelder, A special class of Moufang loops. Proc. Amer. Math. Soc. 26 (1970), 583–586.

[71] H. O. Pflugfelder, *Quasigroups and loops: introduction.* Sigma Series in Pure Mathematics 7, Heldermann Verlag, Berlin (1990).

[72] H. O. Pflugfelder, *Historical notes on loop theory.* Comment. Math. Univ. Carolinae 41/2 (2000), 359–370.

[73] J. D. Phillips, D. Stanovský, *Automated theorem proving in quasigroup and loop theory.* Artificial Intelligence Commun. 23/2-3 (2010), 267–283.

[74] R. S. Pierce, *Symmetric groupoids.* Osaka J. Math. 15 (1978), 51–76.

[75] D. A. Robinson, *A loop-theoretic study of right-sided quasigroups.* Ann. Soc. Sci. Bruxelles, 93/1 (1979), 7–16.

[76] E. Schröder, *Über algorithmen und Calculi.* Arch. der Math. und Phys. 5 (1887), 225–278 (German).

[77] J. D. H. Smith, *Finite distributive quasigroups.* Math. Proc. Cambridge Philos. Soc. **80** (1976), 37–41.

[78] J. D. H. Smith, *Commutative Moufang loops: the first 50 years.* Algebras Groups Geom. 2 (1985), 209–234.

[79] J. D. H. Smith. *An introduction to quasigroups and their representations.* Studies in Advanced Mathematics, Chapman & Hall/CRC, Boca Raton (2007).

[80] J.-P. Soublin, *Étude algébrique de la notion de moyenne.* J. Math. Pures Appl. **50** (1971), 53–264 (French).

[81] D. Stanovský, *Distributive groupoids are symmetric-by-medial: An elementary proof.* Comment. Math. Univ. Carolinae 49/4 (2008), 541–546.

[82] D. Stanovský, P. Vojtěchovský, *Abelian extensions and solvable loops*, Results in Math. 66/3-4 (2014), 367–384.

[83] S. K. Stein, *On the foundations of quasigroups.* Trans. Amer. Math. Soc. 85 (1957), 228–256.

[84] S. K. Stein, *Left-distributive quasigroups.* Proc. Amer. Math. Soc. 10 (1959), 577–578.

[85] S. K. Stein, *Homogeneous quasigroups.* Pacific J. Math. 14 (1964), 1091–1102.

[86] A. K. Suschkewitsch, *On a generalization of the associative law.* Trans. Amer. Math. Soc. 31 (1929), 204–214.

[87] M. Takasaki, *Abstractions of symmetric transformations.* Tôhoku Math. J. 49 (1943), 143–207. (Japanese)

[88] K. Toyoda, *On axioms of linear functions.* Proc. Imp. Acad. Tokyo 17 (1941), 221–227.

[89] N. Umaya, *On symmetric structure of a group*, Proc. Japan Acad. 52 (1976), 174–176.

[90] L. Vendramin, *On the classification of quandles of low order*, J. Knot Theory Ramifications 21/9 (2012), 1250088.

[91] J. Vlachý, *Small left distributive quasigroups.* Bachelor's Thesis, Charles University in Prague (2010). Available at `https://is.cuni.cz/webapps/zzp`.

Addendum: Finite left distributive quasigroup have solvable multiplication groups

It is an outrageous ignorance that I missed the 2001 paper of Alexander Stein [S] in my survey (many thanks to Giuliano Bianco for pointing this out). Stein proves the following group-theoretical result, generalizing Glauberman's Z*-theorem: Let G be a finite group and $g \in G$ such that the conjugacy class g^G is a transversal to some subgroup H of G. Then the subgroup $\langle g^G \rangle$ is solvable. The proof is complicated and uses the classification of finite simple groups. The following is an easy consequence.

Theorem 7.1 ([S, Theorem 1.4]). *Let Q be a finite left distributive quasigroup. Then* $\mathrm{LMlt}(Q)$ *is solvable.*

Proof. Let $G = \mathrm{LMlt}(Q)$, $g = L_e$ for some $e \in Q$ and $H = \mathrm{LMlt}(Q)_e$, the stabilizer. Then $g^G = \{L_a : a \in Q\}$ is a transversal to H: indeed, $L_aH \cap g^G = \{L_a\}$, since $L_x \in L_aH$ iff $L_a^{-1}L_x \in H$ iff $ae = xe$ iff $a = x$ (here we need unique right division). Hence $G = \langle g^G \rangle$ is solvable. □

From the proof, we see that a quandle envelope (G, ζ) corresponds to a latin quandle if and only if ζ^G is a transversal to G_e. This seems to be an even more convenient characterization than the one presented on p. 22. A related argument also shows an interesting alternative to Proposition 4.2.

Proposition 7.2 ([S, Lemma 1.6]). *Let G be a finite group and $g \in G$ such that g^G is a transversal to $C_G(g)$. Then the conjugation quandle over g^G is latin.*

Theorem 7.1 subsumes previous results in the involutory case [28,31,41] (based on the Z*-theorem, see Section 6.3) and in the both-sided case [20] (Fischer's theorem, see Section 3.2). As a corollary, using Galkin's results [25], we obtain that all finite left distributive quasigroups have the Lagrange property.

Another short argument shows that all finite simple left distributive quasigroups are medial, hence affine over abelian groups.

Corollary 7.3. *Finite simple left distributive quasigroups are medial.*

Proof. An observation by Joyce [J, Proposition 3] says that if a quandle Q is simple then $\mathrm{LMlt}(Q)'$ is the smallest normal subgroup of $\mathrm{LMlt}(Q)$. Since $\mathrm{LMlt}(Q)$ is solvable, we then must have $\mathrm{LMlt}(Q)'' = 1$, hence $\mathrm{LMlt}(Q)'$ is abelian, and so Q is medial by [J, Remark on p. 308]. □

The classification of finite simple medial quandles can be found in [J, Theorem 7], or [AG, Corollary 3.13].

[AG] N. Andruskiewitsch, M. Graña, *From racks to pointed Hopf algebras*, Adv. Math. 178/2 (2003), 177–243.

[J] D. Joyce, *Simple quandles*, Journal of Algebra 79 (1982), 307–318.

[S] A. Stein, *A conjugacy class as a transversal in a finite group*, Journal of Algebra 239 (2001), 365–390.

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

Department of Information Systems and Mathematical Modeling, International IT University, Almaty, Kazakhstan

E-mail address: stanovsk@karlin.mff.cuni.cz