Distributivity in Quandles and Quasigroups

Mohamed Elhamdadi

Dedicated to the memory of Jean-Louis Loday

Abstract Distributivity in algebraic structures appeared in many contexts such as in quasigroup theory, semigroup theory and algebraic knot theory. In this paper we give a survey of distributivity in quasigroup theory and in quandle theory.

KEYWORDS: Quandles, quandle cohomology, extensions, quasigroups, Moufang loops, knot invariants

1 Introduction

Quandles are in general non-associative structures whose axioms correspond to the algebraic distillation of the three Reidemeister moves in knot theory. Quandles appeared in the literature with many different names. If one restricts himself to the most important axiom of a quandle which is the self-distributivity axiom (see definition below), then one can trace this back to 1880 in the work of Pierce [63] where one can read the following comments, *"These are other cases of the distributive principle ....These formulae, which have hitherto escaped notice, are not without interest."* Another early work fully devoted to self-distributivity appeared in 1929 by Burstin and Mayer [9] where normal subquasigroups are studied and an attempt is made to show that every minimal subquasigroup of a finite distributive quasigroup is normal. This is considered as the starting point for the investigation of normality problems in distributive quasigroups. In 1942 Mituhisa Takasaki [71] introduced the notion of kei (involutive quandle in Joyce's terminology [41]) as an abstraction of the notion of symmetric transformation. The earliest known work on racks (see

University of South Florida, e-mail: emohamed@math.usf.edu

definition below) is contained in the 1959 correspondence between John Conway and Gavin Wraith who studied racks in the context of the conjugation operation in a group. Around 1982, Joyce [41] (used the term quandle) and Matveev [45] (who call them distributive groupoids) introduced independently the notion of a quandle. Joyce and Matveev associated to each oriented knot K a quandle $Q(K)$ called the knot quandle. The knot quandle is a complete invariant up to orientation. Since then quandles and racks have been investigated by topologists in order to construct knot and link invariants and their higher analogues (see for example [22] and references therein). In 1986, Brieskorn [7] introduced the concept of automorphic sets to describe a set Δ with a binary operation $*$ such that all left multiplications $b \mapsto a*b$ are automorphisms of Δ. He considered the action of the braid group B_n on the Cartesian product Δ^n and introduced invariants of the orbit; for example, monodromy groups. In 1991, Kauffman intoduced a similar notion called crystal ([42] p. 186) as a generalization of the fundamental group of a knot in the sense that the crystal has more information than the fundamental group alone. In 1992, Fenn and Rourke [33] showed that any codimension-two link has a fundamental rack which contains more information than the fundamental group. They gave some examples of computable link invariants derived from the fundamental rack and explained the connection of the theory of racks with that of braids. In 2003, Fenn, Rourke and Sanderson [34] introduced rack homology. This (co)homology was modified in 1999 by Carter et al. [20] to give a cohomology theory for quandles. This cohomology was used to define state-sum invariant for knots in three space and knotted surfaces in four space. A nice survey paper on quandle ideas is a paper by Scott Carter [10] showing the applications of quandle cocycle invariants.

In this paper, we give a survey of distributivity in quasigroup theory and in quandle theory.

In Section 2, we review the basics of quandles and give examples. Section 3 deals with the problem of classification of quandles. In section 4 we relate quandles to quasigroups and Moufang loops. Section 5 deals with the quandle cohomology and cocycle knot invariants.

2 Basics of quandles

We start by reviewing the basics of quandles and give some examples.

Definition 1. [41] A *quandle*, X, is a set with a binary operation $(a,b) \mapsto a*b$ such that

(1) For any $a \in X$, $a*a = a$.
(2) For any $a,b \in X$, there is a unique $c \in X$ such that $a = c*b$.
(3) For any $a,b,c \in X$, we have $(a*b)*c = (a*c)*(b*c)$.

Axiom (2) states that for each $u \in X$, the map $R_u : X \to X$ with $R_u(x) := x*u$ is a bijection. The axioms for a quandle correspond respectively to the Reidemeister moves of type I, II, and III as can be seen from Figure 1.

Quandles have been used to study colorings of knots and links and to define some of their invariants, see for example [19].
Here are some examples of quandles:

- Any set X with the operation $x * y = x$ for all $x, y \in X$, is a quandle called the *trivial* quandle.
- Any group $X = G$ with conjugation $a * b = bab^{-1}$ is a quandle.
- Let n be a positive integer. For elements $i, j \in \mathbb{Z}_n$ (integers modulo n), define $i * j \equiv 2j - i \pmod{n}$. Then $*$ defines a quandle structure called the *dihedral quandle*, R_n. This set can be identified with the set of reflections of a regular n-gon with conjugation as the quandle operation. If we denote the group of symmetry of a regular n-gon by $D_n =< u, v \mid u^n = 1, v^2 = 1, vuv = u^{-1} >$, then conjugation on reflections is given by $(u^i v) * (u^j v) = u^j v u^i v (u^j v)^{-1} = u^j u^{-i} v u^{-j} = u^{2j-i} v$.
- A group $X = G$ with operation $x * y = yx^{-1}y$ is called the *core* quandle of G, denoted $Core(G)$.
- For any abelian group M and automorphism t of M define a quandle structure on M by $x * y = t(x - y) + y$. This is called an *Alexander quandle*.
- A generalization of the last example is, let G be a group and ϕ be an automorphism of G, then define a quandle structure on G by $x * y = \phi(xy^{-1})y$. Further, let H be a subgroup of G such that $\phi(h) = h$, for all $h \in H$. Then G/H is a a quandle with operation $Hx * Hy = H\phi(xy^{-1})y$. It is called the *homogeneous* quandle (G, H, ϕ).

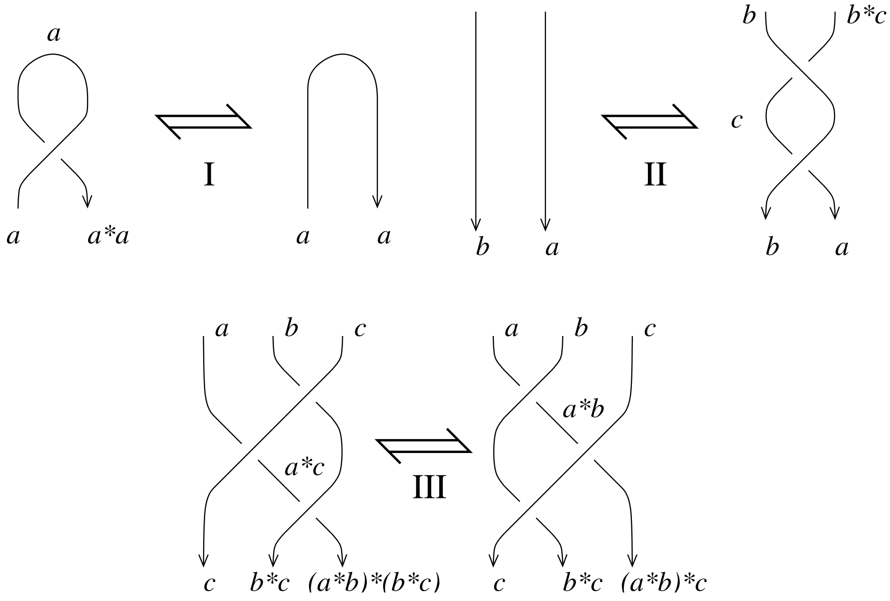

Fig. 1 Reidemeister moves and quandle axioms

- Let $<,>: \mathbb{R}^n \times \mathbb{R}^n \to \mathbb{R}$ be a symmetric bilinear form on $\mathbb{R}^n$. Let X be the subset of $\mathbb{R}^n$ consisting of vectors x such that $< x,x > \neq 0$. Then the operation
$$x * y = \frac{2 < x,y >}{< x,x >} y - x$$
defines a quandle structure on X. Note that, $x * y$ is the image of x under the reflection in y. This quandle is called a $Coxeter$ quandle.

A function $\phi : (X,*) \to (Y,\triangleright)$ is a quandle *homomorphism* if $\phi(a*b) = \phi(a) \triangleright \phi(b)$ for any $a,b \in X$. Axiom (3) of definition 1 state that for each $u \in X$, the map R_u is a quandle homomorphism. Let Aut(X) denotes the automorphism group of X. The subgroup of Aut(X) generated by the permutations R_x is called the *inner* automorphism group of X and denoted by $\text{Inn}(X)$. By axiom (3) of definition 1, the map $R : X \to \text{Inn}(X)$, sending u to R_u, satisfies the equation $R_z\, R_y = R_{y*z}\, R_z$, which can be written as $R_z\, R_y\, {R_z}^{-1} = R_{y*z}$, for all $y,z \in X$. Thus, if the group $\text{Inn}(X)$ is considered as a quandle with conjugation then the map R becomes a quandle homomorphism. The subgroup of Aut(X) generated by $R_x R_y^{-1}$, for all $x,y \in X$, is called the $transvection$ group of X denoted by $Transv(X)$. It is well known (see for example [41]) that the $transvection$ group is a normal subgroup of the inner group and the later group is normal subgroup of the automorphism group of X. The quotient group $\text{Inn(X)}/\text{Transv}(X)$ is a cyclic group (see [41]). For each $u \in X$, let us denote the left multiplication by u by the map $L_u : X \to X$ with $L_u(x) := u*x$. We list some properties and some definitions of quandles below.

- A quandle X is *involutory*, or a *kei*, if the right translations are involutions: $R_a^2 = \text{id}$, for all $a \in X$.
- A quandle is *faithful* if the mapping $a \mapsto R_a$ is an injection from X to $\text{Inn}(X)$.
- A quandle is *connected* if $\text{Inn}(X)$ acts transitively on X.
- A *Latin quandle* is a quandle such that for each $a \in X$, the left translation L_a is a bijection. That is, the multiplication table of the quandle is a Latin square.
- A quandle X is *medial* if $(a*b)*(c*d) = (a*c)*(b*d)$ for all $a,b,c,d \in X$. It is well known that a quandle is medial iff its tranvection group is abelian, that is why it is also called *abelian*. It is known and easily seen that every Alexander quandle is medial.
- A quandle X is called $simple$ if the only surjective quandle homomorphisms on X have trivial image or are bijective.

3 The problem of classification of quandles

The problem of classification of quandles and racks was attempted by many authors mainly because computable invariants of knots such as, the quandle cocycle invariant of Carter et al. [20, 22], and enhancement of counting homomorphisms from the knot quandle to a fixed quandle of Nelson et al. [52, 53] can be defined from quandles. Racks and quandles are used in the classification of pointed Hopf algebras [1] since they help in the understanding of Yetter-Drinfeld modules over groups. Below, we give a survey of the classification of finite quandles.

In 2003, Nelson gave a classification of finite Alexander quandles proving the following

Theorem 1. *[54] Two finite Alexander quandles M and N of the same cardinality are isomorphic as quandles if and only if $(1-t)M$ and $(1-t)N$ are isomorphic as $\mathbb{Z}[t,t^{-1}]$-modules.*

As a consequence of this theorem Ho and Nelson [38] computed isomorphism classes of quandles up to order 5 and their automorphim groups. Quandles of order 6, 7 and 8 were given by Henderson, Macedo and Nelson in [37] but isomorphism class representatives were not determined. In 2006, Nelson and Wong [55] obtained the orbit decomposition of finite quandles: A subset A of a quandle X is said to be X-complemented if the complement of A in X is a subquandle of X. They proved the following

Theorem 2. *[55] Up to isomorphism, every finite quandle has a unique decomposition into subquandles $A_1, A_2, \ldots, A_n$ such that every A_j is X-complemented and no proper subquandle of any A_j is X-complemented.*

Independently around the same time Yetter et al. [29] obtained a similar decomposition theorem for quandles in terms of an operation of ”semidisjoint union”, showing that all finite quandles canonically decompose via iterated semidisjoint unions into connected subquandles. Murillo and Nelson [50] proved in 2006 that there are 24 isomorphism classes of Alexander quandles of order 16. In [31] quandles up to order 9 were classified, automorphism groups of quandles (with orders up to 7) were determined and the automorphism group of the dihedral quandle R_n was proven to be isomorphic to the affine group of $\mathbb{Z}_n$. The number of isomorphism classes of quandles of order 3, 4, 5, 6, 7, 8 and 9 are respectively 3, 7, 22, 73, 298, 1581, 11079. The list of isomorphism classes can be found in https://sites.google.com/a/exactas.udea.edu.co/restrepo/quandles. Independently the same classification result was obtained in [47] by McCarron.

In [39] it was shown first that the isomorphism class of an Alexander quandle $(M,*)$ is determined by the isomorphism type of the Λ-module $(1-t)M$ and the cardinality of the quotient A/K, where A is the annihilator of $(1-t)$ in M, $K = A \cap (1-t)M$ and $\Lambda = \mathbb{Z}[t,t^{-1}]$. This recovers a result of Sam Nelson [54]. The structure of the automorphism group of a general Alexander quandle $(M,*)$ is completely determined (see [39] for more details). Enumeration of Alexander quandles has been much improved. Edwin Clark computed the number of Alexander quandles of orders up to 255 (see http://oeis.org/A193024, for more details) based on results from [40] which contains other interesting enumeration results concerning Alexander quandles. More sequences related to quandles can be found on http://oeis.org.

Example 1. One way of describing a finite quandle is by the Cayley table. Since by the second axiom of a quandle right multiplication by a fixed i, $R_i : j \mapsto j*i$ is is a permutation. We then can describe each quandle by writing each column R_i of the

Cayley table as a product of disjoint cycles. Here we include the list of quandles of order 4. The notation (1) in the table means that the permutation is the identity permutation. For example the quandle Q_5 is the set $\{1,2,3,4\}$ where R_1 is the identity permutation, R_2 is the transposition sending 3 to 4, R_3 is the transposition sending 2 to 4 and R_4 is the transposition sending 2 to 3.

Table 1 Quandles of order 4 in terms of disjoint cycles of columns

Quandle	Disjoint Cycle Notation for the Columns of the Quandle
Q_1	$(1),(1),(1),(1)$
Q_2	$(1),(1),(1),(23)$
Q_3	$(1),(1),(1),(123)$
Q_4	$(1),(1),(12),(12)$
Q_5	$(1),(34),(24),(23)$
Q_6	$(34),(34),(12),(12)$
Q_7	$(234),(143),(124),(132)$

Using computers the search space in general becomes too large to obtain the computation of all quandles up to isomorphism for higher cardinality. Clearly, this depends on the algorithm used to find quandles. However if one restricts himself to the subclass of connected quandles then classification becomes more accessible to calculation in a somehow comparable way to the classification of finite groups. In [28], Clauwens studied connected quandles and proved the following

Proposition 1. [28] If $f : Q \to P$ is a surjective quandle homomorphism and P is connected then for all $x, y \in P$, there is a bijection between $f^{-1}(x)$ and $f^{-1}(y)$. In particular the cardinality of P divides the cardinality of Q.

This allowed him to obtain isomorphism classes of connected quandles up to order 14, in particular he showed that there is no connected quandle of order 14. In [73], Vendramin extended Clauwens results to the list of all connected quandles of orders less than 36. He used the classification of transitive groups and the program described in [29] based mainly on the following

Theorem 3. *[73] Let X be a connected quandle of cardinality n. Let $x_0 \in X$ and $z = R_{x_0}$ be the right multiplication by x_0, $G = \mathrm{Inn}(X)$ and $H = Stab_G(x_0) = \{g \in G, gx_0 = x_0\}$. Then (1) G is a transitive group of order n, (2) z is central element of H and (3) X is isomorphic to the homogeneous quandle (G, H, I_z), where I_z is the conjugation by z.*

A complete list of isomorphism classes of quandles with up to 6 elements appeared in the appendix [22] .

4 Quandles and quasigroups

In this section we will discuss the relation between left and right distributive quasigroups and the following types of quandles: Alexander, Latin and medial quandles. Two connections between quasigroups and quandles were established in [67].
Self-distributivity appeared in 1929 by Burstin and Mayer [9] where they studied quasigroups which are left- and right-distributive. They stated that there are none of orders 2 and 6, observed that the group of automorphisms is transitive, and showed that such a quasigroup is idempotent.

Definition 2. [8] (1) A quasigroup is a set Q with a binary operation $*$ such for all $u \in Q$ the right translation R_u and left translation L_u by u are both permutations.
(2) If the operation $*$ has an identity element e in Q then the quasigroup is called a *loop* and denoted $(Q,*,e)$.

Quasigroups differ from groups in the sense that they satisfy identities which usually conflict with associativity. Distributive quasigroups have transitive groups of automorphisms but the only group with this property is the trivial group. In [70] it is shown that there are no right-distributive quasigroups whose order is twice an odd number. Right-distributive quasigroups are intimately connected with the binary operation of a conjugation in a group since in a right-distributive quasigroup it holds that $R_{y*z} = R_z R_y R_z^{-1}$ and the mapping $x \mapsto R_x$ is injective. We will see below that distributive quasigroups relate to Moufang loops.

Definition 3. [8] Let $(M,*)$ be a set with a binary operation. It is called a *Moufang loop* if it is a loop such that the binary operation satisfies one of the following equivalent identities:

$$x*(y*(x*z)) = ((x*y)*x)*z, \tag{1}$$

$$z*(x*(y*x)) = ((z*x)*y)*x, \tag{2}$$

$$(x*y)*(z*x) = (x*(y*z))*x. \tag{3}$$

As the name suggests, the Moufang identity is named for Ruth Moufang who discovered it in some geometrical investigations in the first half of this century [49]. Moufang loops differ from groups in that they need not be associative. A Moufang loop that is associative is a group. The Moufang identities may be viewed as weaker forms of associativity. The typical examples include groups and the set of nonzero octonions which gives a nonassociative Moufang loop.

Theorem 4. *(Moufang's Theorem) Let a,b,c be three elements in a commutative Moufang loop (abbreviated CML) M for which the relation $(a*b)*c = a*(b*c)$ holds. Then the subloop generated by them is associative and hence is an Abelian group.*

A consequence of this theorem is that every two elements in CML generate an Abelian subgroup. Let $(X,*)$ be a right-distributive quasigroup. Then $(x*x)*x = (x*x)*(x*x)$ which implies that each element is idempotent and $(X,*)$ is then a

Latin quandle. Fix $a \in X$ and define the following operation, denoted $+$, on X by $x+y := {R_a}^{-1}(x) * {L_a}^{-1}(y)$. Then $a+y=y$ and $y+a=y$. Thus $(X,+,a)$ is a loop. Therefore any right-distributive quasigroup satisfying one of the Moufang identities (1), (2) and (3) is a Moufang loop. Note that $R_a(x)+L_a(y)=x*y$. The Moufang loop is commutative if and only if

$$(u*v)*(w*z)=(u*w)*(v*z) \tag{4}$$

A magma $(X,*)$ that satisfies equation (4) is said to be *medial* (Belousov [5]) or *abelian* (Joyce [41]). The Bruck-Toyoda theorem gives the following characterization of medial quasigroup. Given an Abelian group M, two commuting automorphisms f and g of M and a fixed element a of M, define an operation $*$ on M by $x*y=f(x)+g(y)+a$. This quasigroup is called *affine* quasigroup. It's clear that $(M,*)$ is a medial qasigroup. The Bruck-Toyoda theorem states that every medial quasigroup is of this form, i.e. is isomorphic to a quasigroup defined from an abelian group in this way. Belousov gave the connection between distributive quasigroups and Moufang loops in the following

Theorem 5. *[5] If $(X,*)$ be a distributive quasigroup then for all $a \in X$, $(X,+,a)$ is a commutative Moufang loop.*

Now let $(X,*)$ be a Latin quandle (that is right-distributive quasigroup), then the automorphism $\phi = R_a$ satisfies $2\phi(a)=a$. If the order of a is odd then one can write $\phi(a)=\frac{1}{2}a$. The map $x \mapsto 2x$ being a homomorphism is equivalent to $(x+y)+(x+y)=(x+x)+(y+y)$, (mediality property).

Recall that a *magma* is a set with a binary operation. We have the following question: do the following three properties imply associativity for a finite magma $(X,+)$?

1. $(X,+)$ is a commutative loop with identity element 0.
2. For all x,y in X we have the identity $(x+y)+(z+z)=(x+z)+(y+z)$.
3. There is an automorphism f of $(X,+)$ satisfying $f(x)+f(x)=x$ for all x. (in other words, the map $x \mapsto 2x$ is onto and $(x+x)+(y+y)=(x+y)+(x+y)$.

In fact, if $(X,+)$ is a loop satisfying condition 2, then $(X,+)$ is a commutative Moufang loop, necessarily satisfying the other conditions. There exist nonassociative commutative Moufang loops. The smallest order at which such loops occur is 81, and there are, in fact, two such loops of that order. The easier to describe of the two commutative Moufang loops of order 81 is the one of exponent 3. Special thanks to Michael Kinyon and David Stanovsky for telling us about the following example and some other results about quasigroups. Let $F=\mathbb{Z}_3$ and on F^4, define

$$(x_0,x_1,x_2,x_3)+(y_0,y_1,y_2,y_3)= \\ (x_0+y_0+(x_1-y_1)(x_2y_3-x_3y_2),x_1+y_1,x_2+y_2,x_3+y_3),$$

This is very first known example, published by Bol, who attributed it to Zassenhaus [6].

The construction from loops to quandles requires the maps $x \mapsto 2x$ to be bijections as well as a homomorphisms. Is this guaranteed for commutative Moufang loops? Every abelian group is a commutative Moufang loop, so squaring is not always a bijection, of course. For the two examples we mentioned above (loops of order 81), the answer is yes. Any commutative Moufang loop modulo its center will have exponent 3. If you have a commutative Moufang loop which is indecomposable in the sense that it is not a direct product of smaller loops, then it will have order a power of 3. Nonassociativity starts showing up at order 81. Classification of commutative Moufang loops of higher order has not been worked out in detail because of the computational difficulties. Much literature has been about free commutative Moufang loops of exponent 3, because they turn out to be finite and of order 3^n. Quandles which are also quasigroups correspond to a class of loops known as Bruck loops. Commutative Moufang loops have been investigated in detail by Bruck and Salby

Theorem 6. *[8] If $(X,+)$ is a commutative Moufang loop then $X = A \times B$ is a direct product of an abelian group A with order prime to* 3 *and a commutative Moufang loop of order* 3^k.

Latin quandles are right distributive quasigroups and left-distributive Latin quandles are distributive quasigroups. Belousov's theorem tells us that if $(X,*)$ is left-distributive Latin quandle then $(X,+)$ is a commutative Moufang loop and then Bruck-Slaby theorem tells us that $(X,*)$ is affine over a commutative Moufang loop, and then medial. The smallest Latin quandle that is not left distributive is of order 15 and was found by David Stanovsky (see [69], p 29) using an automatic model builder SEM for all quasigroups satisfying left distributivity, but not mediality. This motivated Jan Vlachy [74] to look for a more theoretical argument that would explain the nonexistence of any smaller quasigroups of this kind and proved that there are exactly two non-isomorphic types of these smallest non-right-distributive left-distributive quasigroups with 15 elements. He constructed them explicitly using the Galkin's representation [36]. In the survey paper [35], page 950, Galkin states that nonmedial quasigroups of order less than 27 appear only in orders 15 and 21 and are given by the following construction: Define a binary operation on $\mathbb{Z}_3 \times \mathbb{Z}_p$ by

$$(x,a)*(y,b) = (2y-x, -a+\mu(x-y)b+\tau(x-y)) \quad x,y \in \mathbb{Z}_3,\ a,b \in \mathbb{Z}_p,$$

where $\mu(0) = 2$, $\mu(1) = \mu(2) = -1$, and $\tau : \mathbb{Z}_3 \to \mathbb{Z}_p$ is such that $\tau(0) = 0$. This construction was generalized by replacing $\mathbb{Z}_p$ by any abelian group A in [26]. Let A be an abelian group, also regarded naturally as a $\mathbb{Z}$-module. Let $\mu : \mathbb{Z}_3 \to \mathbb{Z}$, $\tau : \mathbb{Z}_3 \to A$ be functions. These functions μ and τ need not be homomorphisms. Define a binary operation on $\mathbb{Z}_3 \times A$ by

$$(x,a)*(y,b) = (2y-x, -a+\mu(x-y)b+\tau(x-y)) \quad x,y \in \mathbb{Z}_3,\ a,b \in A.$$

Proposition 2. *[26] For any abelian group A, the above operation $*$ defines a quandle structure on $\mathbb{Z}_3 \times A$ if $\mu(0) = 2$, $\mu(1) = \mu(2) = -1$, and $\tau(0) = 0$.*

This quandle $(\mathbb{Z}_3 \times A, *)$ is called the *Galkin quandle* and denoted by $G(A,\tau)$.

Lemma 1. *[26] For any abelian group A and $c_1, c_2 \in A$, $G(A, c_1, c_2)$ and $G(A, 0, c_2 - c_1)$ are isomorphic.*

Various properties of Galkin quandles were studied in [26] and their classification in terms of pointed abelian groups was given. We mention a few properties. Each $G(A, c)$ is connected but not Latin unless A has odd order, $G(A, c)$ is non-medial unless $3A = 0$
We conclude with the folowing properties relating distributivity and mediality to quandles [26]: Alexander quandles are left-distributive and medial. It is easy to check that for a finite Alexander quandle (M, T) with $T \in \mathrm{Aut}(M)$, the following are equivalent: (1) (M, T) is connected, (2) $(1 - T)$ is an automorphism of M, and (3) (M, T) is Latin. It was also proved by Toyoda [72] that a Latin quandle is Alexander if and only if it is medial. As noted by Galkin, $G(\mathbb{Z}_5, 0)$ and $G(\mathbb{Z}_5, 1)$ are the smallest non-medial Latin quandles and hence the smallest non-Alexander Latin quandles.
We note that medial quandles are left-distributive (by idempotency). It is proved in [26] that any left-distributive connected quandle is Latin. This implies, by Toyoda's theorem, that every medial connected quandle is Alexander and Latin. The smallest Latin quandles that are not left-distributive are the Galkin quandles of order 15. It is known that the smallest left-distributive Latin quandle that is not Alexander is of order 81. This is due to V. D. Belousov.

5 Quandle cohomology and cocycle invariant of knots

In the classical theory of knots and links in 3-space, one utilizes projections of knots and links and applies to them the Reidemeister moves, a sequence of which will take one from any one projection of a given knot or link to any other projection of that knot or link. The Reidemeister moves have played an essential role in the development of a wide variety of invariants for knots and links, since any quantity that remains unchanged by the three moves is an invariant for knots and links. In 1999, Carter et al. [20] used quandle cohomology to define combinatorial "state-sum" invariants for classical knots and knotted surfaces called quandle cocycle invariant (see definition below). Here we mention some interesting results on surfaces in 4-space they obtained: (1) constructing an example of a sphere that is knotted in 4-dimensional space [20], (2) giving obstructions to ribbon concordance for knotted surfaces [24], and (3) detecting non-invertibility of knotted surfaces [20]. This was extended to some other examples [19] and [16].
In order to define quandle homology and the cocycle knot invariant we need to define coloring of knots by a quandle. A *coloring* of an oriented classical knot K is a function $\mathscr{C} : R \to X$, where X is a fixed quandle and R is the set of over-arcs in a fixed diagram of K, satisfying the condition depicted in the top of Figure 2. This definition of colorings on knot diagrams has been known, see [33] for example. In the bottom of Figure 2, the relation between Redemeister type III move and a quandle axiom (self-distributivity) is indicated. In particular, the colors of the bottom right segments before and after the move correspond to the self-distributivity. By

assigning a weight $\phi(x,y)$ at each crossing of a knot diagram (as in the top Figure 2) we obtain a 2-cocycle condition which can be generalized to a homology of cohomology theory which we describe now.

Let $C_n(X)$ be the free abelian group generated by n-tuples $(x_1,\dots,x_n)$ of elements of a quandle X. Define a homomorphism $\partial_n : C_n(X) \to C_{n-1}(X)$ by

$$\begin{aligned}&\partial_n(x_1,x_2,\dots,x_n)\\ &\quad=\sum_{i=2}^{n}(-1)^i\,[(x_1,x_2,\dots,x_{i-1},x_{i+1},\dots,x_n)\\ &\qquad-(x_1*x_i,x_2*x_i,\dots,x_{i-1}*x_i,x_{i+1},\dots,x_n)]\end{aligned} \tag{5}$$

for $n \geq 2$ and $\partial_n = 0$ for $n \leq 1$. Then $C_*(X) = \{C_n(X), \partial_n\}$ is a chain complex. The nth *quandle homology group* and the nth *quandle cohomology group* [20] of a quandle X with coefficient in a group A can be defined. One can consider cohomology also and for example:

A *2-cocycle* is a function $\phi : X \times X \to A$ such that $\phi(x,y) + \phi(x*y,z) = \phi(x,z) + \phi(x*z,y*z)$, and for all x, $\phi(x,x) = 0$.

A *3-cocycle* is a function $\psi : X \times X \times X \to A$ such that

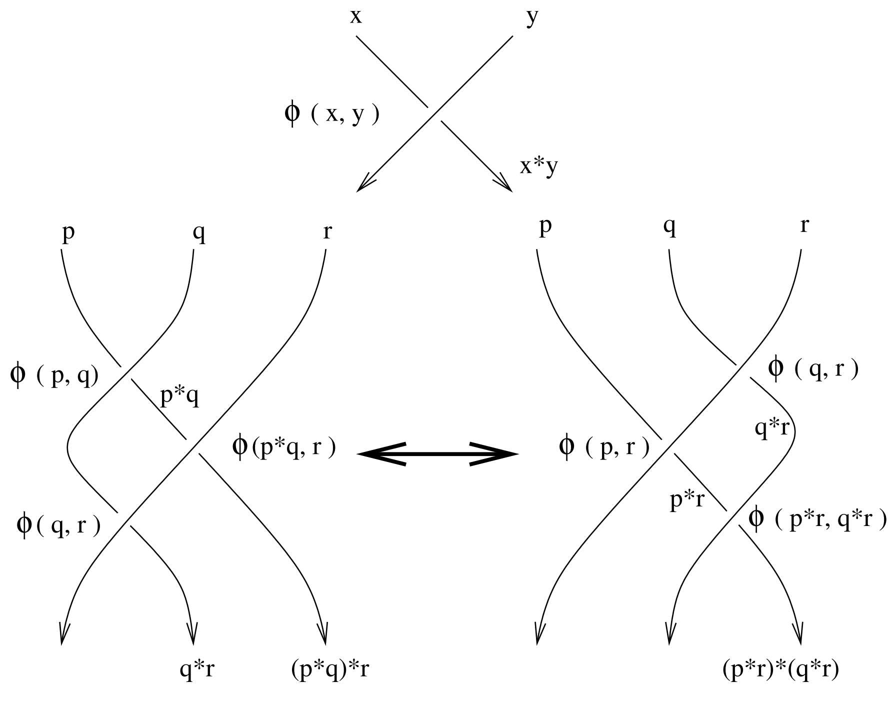

Fig. 2 2-cocycle condition and Reidemeister move III

$$\psi(x,y,z)+\psi(x,z,w)+\psi(x*z,y*z,w)=\psi(x*y,z,w)+\psi(x*w,y*w,z*w)+\psi(x,y,w),$$

and and for all x,y, $\psi(x,x,y)=\psi(x,y,y)=0$.
Let $\mathscr{C}$ denote a coloring of a knot K by a quandle X and choose a quandle 2-cocycle ϕ, Then define a *(Boltzmann) weight*, $B(\tau,\mathscr{C})$, at a crossing τ, by $B(\tau,\mathscr{C})=\phi(x,y)^{\varepsilon(\tau)}$, where $\varepsilon(\tau)=1$ or -1, if the sign of τ is positive or negative, respectively. The *partition function* (called also *state-sum*) is the expression

$$\Phi_\phi(K):=\sum_{\mathscr{C}}\prod_{\tau}B(\tau,\mathscr{C}).$$

The product is taken over all crossings of the given diagram, and the sum is taken over all possible colorings. The values of the partition function are taken to be in the group ring $\mathbb{Z}[A]$ where A is the coefficient group written multiplicatively.

Theorem 7. *[20] The state sum $\Phi_\phi(K)$ does not depend on the choice of a diagram of a knot K, so that it is a knot invariant.*

This knot invariant is also called quandle cocycle invariant associated with the quandle 2-cocycle ϕ.

Example 2. see [21] p 52, Let $X=\mathbb{Z}_2[T,T^{-1}]/(T^2+T+1)$, $A=\mathbb{Z}_2$, and cocycle $\Phi=\prod\chi_{(a,b)}$ where $a,\ b\in\{0,1,T+1\}$ and $a\neq b$.
For knots K (up to nine crossings, see [25] for diagrams and other information) the Invariants $\Phi(K)$ are:

- $4(1+3T)$ for $3_1,4_1,7_2,7_3,8_1,8_4,8_{11},8_{13},9_1,9_6,9_{12},9_{13},9_{14},9_{21},9_{23},9_{35},9_{37}$,
- $16(1+3T)$ for 8_{18}, and 9_{40}
- 16 for $8_5,8_{10},8_{15},8_{19}-8_{21},9_{16},9_{22},9_{24},9_{25},9_{28}-9_{30},9_{36},9_{38},9_{39},9_{41}-9_{45},9_{49}$
- 4 otherwise.

Generalizations of the cocycle knot invariants have been discovered; for example, see [19] and [16].

5.1 Extensions of quandles

Quandle extension theory was developed in [18] by analogy with group extensions defined for low dimensional group cocycles. Let X be a quandle, A be an abelian group and given a 2-cocycle $\phi\in Z^2_{\mathrm{Q}}(X;A)$, the quandle operation in extension is defined on $E=A\times X$ by $(a_1,x_1)*(a_2,x_2)=(a_1+\phi(x_1,x_2),\ x_1*x_2)$. The following lemma is the converse of the fact proved in [23] that $E(X,A,\phi)$ is a quandle.

Lemma 2. *[18] Let X, E be finite quandles, and A be a finite abelian group written multiplicatively. Suppose there exists a bijection $f:E\to A\times X$ with the following* *property. There exists a function* $\phi : X \times X \to A$ *such that for any* $e_i \in E$ $(i = 1,2)$*, if* $f(e_i) = (a_i, x_i)$*, then* $f(e_1 * e_2) = (a_1\phi(x_1,x_2), x_1 * x_2)$*. Then* $\phi \in Z^2_{\mathrm{Q}}(X;A)$*.*

The following two theorems produce examples of extensions of quandles.

Theorem 8. *[18] For any positive integers* q *and* m*,* $E = \mathbb{Z}_{q^{m+1}}[T,T^{-1}]/(T-1+q)$ *is an abelian extension* $E = E(\mathbb{Z}_{q^m}[T,T^{-1}]/(T-1+q), \mathbb{Z}_q, \phi)$ *of* $X = \mathbb{Z}_{q^m}[T,T^{-1}]/(T-1+q)$ *for some cocycle* $\phi \in Z^2_{\mathrm{Q}}(X;\mathbb{Z}_q)$*.*

Theorem 9. *[18] For any positive integer* q *and* m*, the quandle* $E = \mathbb{Z}_q[T,T^{-1}]/(1-T)^{m+1}$ *is an abelian extension of* $X = \mathbb{Z}_q[T,T^{-1}]/(1-T)^m$ *over* $\mathbb{Z}_q$*:* $E = E(X, \mathbb{Z}_q, \phi)$*, for some* $\phi \in Z^2_{\mathrm{Q}}(X;\mathbb{Z}_q)$*.*

Below are some explicit examples of extensions.

Example 3. [18] For any positive integer q and m, the quandle $E = \mathbb{Z}_q[T,T^{-1}]/(1-T)^{m+1}$ is an abelian extension of $X = \mathbb{Z}_q[T,T^{-1}]/(1-T)^m$ over $\mathbb{Z}_q$: $E = E(X, \mathbb{Z}_q, \phi)$, for some $\phi \in Z^2_{\mathrm{Q}}(X;\mathbb{Z}_q)$.

Example 4. [18] Consider the case $q = 2$, $m = 2$ in Example 3. In this case

$$\mathbb{Z}_4[T,T^{-1}]/(T+1) = R_4, \quad \text{and}$$

$$\mathbb{Z}_8[T,T^{-1}]/(T+1) = R_8 = E(R_4, \mathbb{Z}_2, \phi)$$

for some $\phi \in Z^2_{\mathrm{Q}}(R_4;\mathbb{Z}_2)$. We obtain an explicit formula for this cocycle ϕ by computation:

$$\phi = \chi_{0,2} + \chi_{0,3} + \chi_{1,0} + \chi_{1,3} + \chi_{2,0} + \chi_{2,3} + \chi_{3,0} + \chi_{3,1},$$

where

$$\chi_{a,b}(x,y) = \begin{cases} 1 \text{ if } (x,y) = (a,b), \\ 0 \text{ if } (x,y) \neq (a,b) \end{cases}$$

denotes the characteristic function.

Other extensions of quandles have been considered by some authors; see, for example, in [1] where a more general homology theory is developed and in [30] where algebraic covering theory of quandle is established.

Dynamical cocycles [1] Let X be a quandle and S be a non-empty set. Let $\alpha : X \times X \to \mathrm{Fun}(S \times S, S) = S^{S \times S}$ be a function, so that for $x, y \in X$ and $a, b \in S$ we have $\alpha_{x,y}(a,b) \in S$.

Then it is checked by computations that $S \times X$ is a quandle by the operation $(a,x) * (b,y) = (\alpha_{x,y}(a,b), x * y)$, where $x * y$ denotes the quandle product in X, if and only if α satisfies the following conditions:

1. $\alpha_{x,x}(a,a) = a$ for all $x \in X$ and $a \in S$;
2. $\alpha_{x,y}(-,b) : S \to S$ is a bijection for all $x, y \in X$ and for all $b \in S$;
3. $\alpha_{x*y,z}(\alpha_{x,y}(a,b),c) = \alpha_{x*z,y*z}(\alpha_{x,z}(a,c), \alpha_{y,z}(b,c))$, $\forall x,y,z \in X$ and $\forall a,b,c \in S$.

Such a function α is called a *dynamical quandle cocycle* [1]. The quandle constructed above is denoted by $S \times_{\alpha} X$, and is called the *extension* of X by a dynamical cocycle α. The construction is general, as Andruskiewitsch and Graña show:

Lemma 3. *[1] Let $p : Y \rightarrow X$ be a surjective quandle homomorphism between finite quandles such that the cardinality of $p^{-1}(x)$ is a constant for all $x \in X$. Then Y is isomorphic to an extension $S \times_{\alpha} X$ of X by some dynamical cocycle on the set S such that $|S| = |p^{-1}(x)|$.*

Acknowledgments I would like to thank Scott Carter, Edwin Clark and Masahico Saito for commenting on an early version and for fruitful suggestions. Thanks also to the referee for all comments.

References

1. Andruskiewitsch N. , and Graña M., *From racks to pointed Hopf algebras,* Adv. Math. 178, no. 2, 2003, 177–243.
2. Ameur K.; Elhamdadi M.; Rose T.; Saito M.; Smudde C., *Tangle embeddings and quandle cocycle invariants,* Experiment. Math. 17 (2008), no. 4, 487–497.
3. Belousov, V. D., *Fundamentals of the theory of quasigroups and loops,* (in Russian), Nauka Moskva, 1967.
4. Belousov, V. D., *Les quasi-groupes transitifs et distributifs.,* Ukrain.Mat. Z. 10 1958 no. 1, pp13–22.
5. Belousov, V. D., *The structure of distributive quasigroups,* (in Russian) Mat. Sb. (N.S.) 50 (92) 1960, pp 267–298.
6. Bol G., *Gewebe und gruppen,* Math. Ann. 114 (1937), no. 1, 414-431.
7. Brieskorn, E., *Automorphic sets and singularities,* Contemporary math., 78 (1988), 45–115.
8. Bruck, H., *A survey of binary systems,* Ergeb. Math. Grenzgeb. Neue Folge, Heft 20. Reihe: Gruppentheorie, Springer-Verlag, Berlin, 1958.
9. Burstin, C. and Mayer, W., *Distributive Gruppen,* J. Reine Angew. Math. 160 (1929) 111-130.
10. Carter, J.S. *A survey of quandle ideas,* Introductory lectures on knot theory, 22-53, Ser. Knots Everything, 46, World Sci. Publ., Hackensack, NJ, 2012.
11. Carter S., Elhamdadi M., Saito M., Silver D., and Williams S., *Virtual knot invariants from group biquandles and their cocycles,* J. Knot Theory Ramifications 18, no.7, 2009, 957-972.
12. Carter S., Crans A., Elhamdadi M., Karadayi E., and Saito M., *Cohomology of Frobenius algebras and the Yang-Baxter equation,* Commun. Contemp. Math. 10 (2008), suppl. 1, 791-814.
13. Carter S., Crans A., Elhamdadi M., and Saito M., *Cohomology of categorical self-distributivity,* J. Homotopy Relat. Struct. 3 (2008), no. 1, 13-63.
14. Carter S., Crans A., Elhamdadi M., and Saito M., *Cohomology of the adjoint of Hopf algebras,* J. Gen. Lie Theory Appl. 2 (2008), no. 1, 19-34.
15. Carter S., Elhamdadi M., Saito M., and Satoh S., *A lower bound for the number of Reidemeister moves of type III,* Topology Appl. 153 (2006), no. 15, 2788-2794.
16. Carter J.S.; Elhamdadi M.; Graña M.; Saito M., *Cocycle knot invariants from quandle modules and generalized quandle homology,* Osaka J. Math., 42, (2005), 499-541.
17. Carter J.S.; Elhamdadi M.; and Saito M., *Homology theory for the set-theoretic Yang-Baxter equation and knot invariants from generalizations of quandles,* Fund. Math. 184 (2004), 31-54.
18. Carter S., Elhamdadi M., Nikifourou M., and Saito M., *Extensions of quandles and cocycle knot invariants,* J. Knot Theory Ramifications 12, no.6, 2003, 725-738.

19. Carter S.; Elhamdadi M.; and Saito M., *Twisted quandles homology and cocycle knot invariants,* Algebr. Geom. Topol. 2, 2002, 95-135.
20. Carter, J.S.; Jelsovsky, D.; Kamada, S.; Langford, L.; Saito, M., *Quandle cohomology and state-sum invariants of knotted curves and surfaces,* Trans. Amer. Math. Soc. 355 (2003), 3947-3989.
21. Carter, J.S.; Jelsovsky, D.; Kamada, S.; Saito, M., *Computations of quandle cocycle invariants of knotted curves and surfaces,* Adv. Math. 157 (2001), no. 1, 36-94.
22. Carter S., Kamada S., and Saito M., *Surfaces in 4-space,* Encyclopaedia of Mathematical Sciences, 142, 2004. Low-Dimensional Topology, III. Springer-Verlag, Berlin.
23. Carter S., Kamada S., and Saito M., *Diagrammatic computations for quandles and cocycle knot invariants,* Diagrammatic morphisms and applications (San Francisco, CA, 2000), 5174, Contemp. Math., 318, Amer. Math. Soc., Providence, RI, 2003,
24. Carter S., Saito M., and Satoh S., *Ribbon concordance of surface-knots via quandle cocycle invariants,* J. Aust. Math. Soc. 80 (2006), no. 1, 131-147.
25. Cha J. C. and Livingston., *KnotInfo: Table of Knot Invariants,* http://www.indiana.edu/ knotinfo.
26. Clark W.; Elhamdadi M.; Hou X.; Saito M.; and Yetman T., *Connected Quandles Associated with Pointed Abelian Groups ,* Pacific J. Math. 264 (2013), no. 1, 31-60.
27. Clauwens F. J. B. J., *The algebra of rack and quandle cohomology,* J. Knot Theory Ramifications 20 (2011), no. 11, 1487-1535.
28. Clauwens F. J. B. J., *Small connected quandles,* preprint (2010), arXiv:1011.2456.
29. Ehrman, G.; Gurpinar, A.; Thibault, M.; Yetter, D. N. , *Toward a classification of finite quandles,* J. Knot Theory Ramifications 17 (2008), no. 4, 511-520.
30. Eisermann M., *Quandle coverings and their Galois correspondence,* arXiv:math/0612459.
31. Elhamdadi M.; MacQuarrie J.; and Restrepo R., *Automorphism groups of quandles,* J. Algebra Appl., vol. 11, no 1, 2012, 1250008 (9 pages).
32. Elhamdadi M.; and Makhlouf A., *Cohomology and formal deformations of alternative algebras,* J. Gen. Lie Theory Appl. 5 (2011), Art. ID G110105, 10 pp.
33. Fenn R., and Rourke C., 1992. *Racks and links in codimension two,* J. Knot Theory Ramifications, 1, 343-406.
34. Fenn R., Rourke C. and Sanderson B., 1992. *The rack space,* Trans. Amer. Math. Soc. 359 (2007), no. 2, 701-740.
35. Galkin, V. M., *Quasigroups*, Itogi Nauki i Tekhniki, Algebra. Topology. Geometry, Vol. 26 (Russian), 344, 162, Akad. Nauk SSSR, Vsesoyuz. Inst. Nauchn. i Tekhn. Inform., Moscow (1988), Translated in J. Soviet Math. 49 (1990), no. 3, 941967.
36. Galkin, V. M., *Left distributive finite order quasigroups,* (Russian) Quasigroups and loops. Mat. Issled. No. 51 (1979), 43-54, 163.
37. Henderson, R.; Macedo T.;and Nelson S. *Symbolic computation with finite quandles,* J. Symbolic Comput. 41 (2006), no. 7, 811-817.
38. Ho, B.; Nelson S. *Matrices and finite quandles,* Homology Homotopy Appl. 7 (2005), no. 1, 197–208.
39. Hou X., *Automorphism groups of Alexander quandles,* J. Algebra 344 (2011), 373-385.
40. Hou X., *Finite modules over* $\mathbb{Z}[t,t^{-1}]$, arXiv:1107.2076, 2012.
41. Joyce, D., *A classifying invariant of knots, the knot quandle,* J. Pure Appl. Alg., 23, (1982), 37–65.
42. Kauffman, L. H., *Knots and Physics*, World Scientific, Series on knots and everything, vol. 1, 1991.
43. Keunen, K., *Moufang Quasigroups,* J. Algebra 183, (1996), no 1, 231-234.
44. Lopes P. and Roseman D., *On finite racks and quandles,* Comm. Algebra 34 (2006), no. 1, 371-406.
45. Matveev, S., *Distributive groupoids in knot theory,* (Russian) Mat. Sb. (N.S.) 119(161) (1982), no. 1, 78–88, 160.
46. McCarron J., *The On-Line Encyclopedia of integer sequences,* http://oeis.org/A181769.
47. McCarron J., *Connected Quandles with Order Equal to Twice an Odd Prime,* arXiv:1210.2150, 2012.

48. Mochizuki T., *Some calculations of cohomology groups of finite Alexander quandles,* J. Pure Appl. Algebra 179, (2003), no. 3, 287–330.
49. Moufang R., *Alternativkrper und der Satz vom vollstŁndigen Vierseit (D9),* Abh. Math. Sem. Univ. Hamburg 9, (1933), 207-222.
50. Murillo G., and Nelson S. *Erratum: Alexander quandles of order 16,* J. Knot Theory Ramifications 18 (2009), no. 5, 727.
51. Murillo G., and Nelson S. *Alexander quandles of order 16,* J. Knot Theory Ramifications 17 (2008), no. 3, 273-278.
52. Navas E. A.; and Nelson S. *On symplectic quandles,* Osaka J. Math. 45 (2008), no. 4, 973-985
53. Nelson S. *A polynomial invariant of finite quandles,* J. Algebra Appl. 7 (2008), no. 2, 263-273.
54. Nelson S. *Classification of finite Alexander quandles,* Proceedings of the Spring Topology and Dynamical Systems Conference. Topology Proc. 27 (2003), no. 1, 245-258.
55. Nelson S.; Wong C., *On the orbit decomposition of finite quandles,* J. Knot Theory Ramifications 15 (2006), no. 6, 761-772.
56. Niebrzydowski, M., *On colored quandle longitudes and its applications to tangle embeddings and virtual knots,* J. Knot Theory Ramifications 15 (2006), no. 8, 1049–1059.
57. Niebrzydowski, M; Przytycki, J. H., *The quandle of the trefoil knot as the Dehn quandle of the torus,* Osaka J. Math. 46 (2009), no. 3, 645-659.
58. Niebrzydowski, M; Przytycki, J. H., *The second quandle homology of the Takasaki quandle of an odd abelian group is an exterior square of the group,* J. Knot Theory Ramifications 20 (2011), no. 1, 171-177.
59. Niebrzydowski, M; Przytycki, J. H., *Burnside Kei,* Fund. Math. 190 (2006), 211–229.
60. Niebrzydowski, M; Przytycki, Jozef H., *Homology of Dihedral quandles,* J. Pure Appl. Algebra 213 (2009), no. 5, 742–755.
61. Niebrzydowski, M; Przytycki, Jozef H., *Homology operations on homology of quandles.,* J. Algebra 324 (2010), no. 7, 1529-1548.
62. Orrin F., *Symmetric and self-distributive systems,* Amer. Math. Monthly vol. 62 (1955) pp. 697-707.
63. Pierce, C. S., *On the algebra of logic,* Amer. J. Math. 3 (1880) 15-57.
64. Przytycki J. H., *Distributivity versus associativity in the homology theory of algebraic structures ,* Demonstratio Mathematica, Vol. 44, no. 4, (2011), 823-869.
65. Przytycki, J. H.; Silver, Daniel S.; Williams, Susan G. *3-manifolds, tangles and persistent invariants,* Math. Proc. Cambridge Philos. Soc. 139 (2005), no. 2, 291–306.
66. Przytycki, J.H., 3*-colorings and other elementary invariants of knots,* Banach Center publications vol. 42, knot theory (1998), 275–295.
67. Smith, J. D. H., *Quasigroups and quandles,* Discrete Math. 109 (1992), no. 1-3, 277282.
68. Smith, J. D. H., *Finite distributive quasigroups,* Math. Proc. Cambridge Philos. Soc. 80 (1976), no. 1, 37-41.
69. Stanovsky, D., *Left distributive left quasigroups,* PhD thesis, Charles University in Prague, 2004.
70. Stein S., *On the foundations of quasigroups,* Trans. Amer. Math. Soc. 85, 1957, 228-256.
71. Takasaki, M., *Abstraction of symmetric transformation,* Tohoku Math. J. 49 (1942/3) 145-207, (in Japanese).
72. Toyoda, K., *On axioms of linear functions*, Proceedings of the Imperial Academy, 17(7) (1941), 221–227.
73. Vendramin, L., *On the classification of quandles of low order,* J. Knot Theory Ramifications 21 (2012), no. 9, 1250088 (10 pages).
74. Vlach‘y, J., *Small left distributive quasigroups,* Thesis, 2010