CONNECTED QUANDLES AND TRANSITIVE GROUPS

ALEXANDER HULPKE, DAVID STANOVSKÝ, AND PETR VOJTĚCHOVSKÝ

Abstract. We establish a canonical correspondence between connected quandles and certain configurations in transitive groups, called quandle envelopes. This correspondence allows us to efficiently enumerate connected quandles of small orders, and present new proofs concerning connected quandles of order p and $2p$. We also present a new characterization of connected quandles that are affine.

1. Introduction

1.1. **Motivation.** Let $Q = (Q, \cdot)$ be a set with a single binary operation. Then Q is a *rack* if all *right translations*

$$R_x : Q \to Q, \quad y \mapsto yx$$

are automorphisms of Q. If the rack Q is idempotent, that is, if $xx = x$ for all $x \in Q$, then Q is a *quandle*.

Consider the *right multiplication group*

$$\mathrm{RMlt}(Q) = \langle\, R_x : x \in Q \,\rangle,$$

and note that Q is a rack if and only if $\mathrm{RMlt}(Q)$ is a subgroup of the automorphism group $\mathrm{Aut}(Q)$. A rack Q is said to be *connected* (also *algebraically connected* or *indecomposable*) if $\mathrm{RMlt}(Q)$ acts transitively on Q. The main subject of this work is connected quandles.

An important motivation for the study of quandles is the quest for computable invariants of knots and links. Connected quandles are of prime interest here because all colors used in a knot coloring fall into the same orbit of transitivity.

From a broader perspective, quandles are a special type of set-theoretical solutions to the quantum Yang-Baxter equation [10, 12] and can be used to construct Hopf algebras [1]. There are indications, such as [13], that understanding racks and quandles, particularly the connected ones, is an important step towards understanding general set-theoretical solutions of the Yang-Baxter equation.

Our main result, Theorem 5.3, is a correspondence between connected quandles and certain configurations in transitive groups. Some variants of this representation were discovered independently in [11, 15, 24, 36], but none of these works contains a complete characterization of the configurations as in Theorem 5.3, nor a discussion of the isomorphism problem as in Theorem 5.6. Using the correspondence, we reprove (and occasionally extend) several known

2000 *Mathematics Subject Classification.* Primary: 57M27. Secondary: 20N02, 20B10.

Key words and phrases. Quandle, connected quandle, homogeneous quandle, affine quandle, enumeration of quandles, quandle envelope, transitive group of degree $2p$.

Research partially supported by the Simons Foundation Collaboration Grant 244502 to Alexander Hulpke, the GAČR grant 13-01832S to David Stanovský, and the Simons Foundation Collaboration Grant 210176 to Petr Vojtěchovský.

results on connected quandles in a simpler and faster way. We focus on enumeration of "small" connected quandles, namely those of order less than 48 (see Section 8 and Algorithm 8.1) and those with p or $2p$ elements (see Section 9). Our proof of non-existence of connected quandles with $2p$ elements, for any prime $p > 5$, is based on a new group-theoretical result for transitive groups of degree $2p$, Theorem 10.1.

The modern theory of quandles originated with Joyce's paper [24] and the introduction of the knot quandle, a complete invariant of oriented knots. Subsequently, quandles have been used as the basis of various knot invariants [4, 5, 6] and in algorithms on knot recognition [6, 14].

But the roots of quandle theory are much older, going back to self-distributive quasigroups, or *Latin quandles* in today's terminology, see [38] for a comprehensive survey of results on Latin quandles and their relation to the modern theory. Another vein of results has been motivated by the abstract properties of reflections on differentiable manifolds [27, 30], resulting in what is now called *involutory quandles* [39]. Yet another source of historical examples is furnished by conjugation in groups, which eventually led to the discovery of the above-mentioned knot quandle by Joyce and Matveev [24, 31].

Quandles have also been studied as algebraic objects in their own right, and we will now briefly summarize the most relevant results. Every quandle decomposes into orbits of transitivity of the natural action of its right multiplication group. An attempt to understand the orbit decomposition was made in [11, 34], and a full description has been obtained in two special cases: for medial quandles [23] and for involutory quandles [36]. The orbits are not necessarily connected, but they share certain properties with connected quandles.

There have been several attempts to understand the structure of connected quandles, see e.g. [1]. In our opinion, the homogeneous representation reviewed in Section 3 is most useful in this regard. It was introduced by Galkin and Joyce [15, 24], and led to several structural and enumeration results, such as [13, 17, 41]. Some of them will be presented in Sections 8 and 9. A classification of simple quandles can be found in [1, 25].

1.2. **Summary of results.** The paper is written as a self-contained introduction to connected quandles. Therefore, in the next two sections, we review the theory necessary for proving the main result. Although the opening sections contain no original ideas, our presentation is substantially different from other sources. We prove the main result in Section 5, and the rest of the paper is concerned with its applications.

In Section 2 we develop basic properties of quandles in relation to the right multiplication group and its derived subgroup. In Section 3 we introduce the homogeneous representation (Construction 3.1) and characterize homogeneous quandles as precisely those obtained by this construction (Theorem 3.6). In Section 4 we discuss homogeneous representations that are minimal with respect to the underlying group (Theorem 4.1).

In Section 5 we prove the main result (Theorem 5.3), a canonical correspondence between connected quandles and quandle envelopes. We also describe all isomorphisms between two connected quandles in the canonical representation (Lemma 5.5). As a consequence, we solve the isomorphism problem (Theorem 5.6) and describe the automorphism group (Proposition 5.8).

Then we focus on two particular classes of connected quandles. In Section 6 we characterize Latin quandles in terms of their homogeneous and canonical representations (Propositions

6.2 and 6.3). Section 7 contains a characterization of connected affine quandles (Theorem 7.3): we show that a connected quandle is affine if and only if it is medial if and only if its right multiplication group is metabelian.

The rest of the paper is devoted to enumeration. In Section 8 we present an algorithm for enumeration of connected quandles, which is similar to but several orders of magnitude faster than the recent algorithm of Vendramin [41]. In addition, using combinatorial and geometric methods, we construct several families of connected quandles, relying on Theorem 5.3 for a simple verification of connectedness.

In Section 9 we investigate quandles of size p, p^2 and $2p$, where p is a prime, using again the correspondence of Theorem 5.3. First, we show that any connected quandle of prime power order has a solvable right multiplication group (Proposition 9.2). Then we give a new and conceptually simple proof that every connected quandle of order p is affine. (This has been proved already in [13] and, likewise, our proof relies on a deep result of Kazarin about conjugacy classes of prime power order.) Finally, we show in Theorem 10.1 that transitive groups of order $2p$, $p > 5$ cannot contain certain configurations that are necessary for the existence of quandle envelopes. As a consequence, we deduce that there are no connected quandles of order $2p$, $p > 5$, a result obtained already by McCarron [32] by means of Cayley-like representations.

1.3. **Terminology and notation.** Quandles have been rediscovered in several disguises and the terminology therefore varies greatly. For the most part we keep the modern quandle terminology that emerged over the last 15 years. However, in some cases we use the older and more general terminology for binary systems developed to a great extent by R. H. Bruck in his 1958 book [2]. Bruck's terminology is used fairly consistently in universal algebra, semigroup theory, loop theory and other branches of algebra. For instance, we speak of "right translations" rather than "inner mappings."

Every quandle is *right distributive*, i.e., it satisfies the identity $(yz)x = (yx)(zx)$, expressing the fact that R_x is an endomorphism. A quandle is called *medial* if it satisfies the identity $(xy)(uv) = (xu)(yv)$.

We apply all mappings to the right of their arguments, written as a superscript. Thus x^α means α evaluated at x. To save parentheses, we use $x^{\alpha\beta}$ to mean $(x^\alpha)^\beta$, while x^{α^β} stands for $x^{(\alpha^\beta)}$.

Let G be a group. For $y \in G$ we denote by ϕ_y the conjugation map by y, that is, $x^{\phi_y} = y^{-1}xy$ for all $x \in G$. As usual, we use the shorthand x^y instead of x^{ϕ_y}, and we let $[x, y] = x^{-1}x^y$. Since $(x^{-1})^y = (x^y)^{-1}$, we denote both of these elements by x^{-y}.

For $\alpha \in \mathrm{Aut}(G)$ we let $C_G(\alpha) = \{z \in G : z^\alpha = z\}$ be the centralizer of α. We write $C_G(x)$ for $C_G(\phi_x)$.

If G acts on X and $x \in X$, we let $G_x = \{g \in G : x^g = x\}$ be the stabilizer of x, and $x^G = \{x^g : g \in G\}$ the orbit of x.

Note that for any binary system $(Q, \cdot)$, $a \in Q$ and $\alpha \in \mathrm{Aut}(Q)$, the mapping R_a^α is equal to R_{a^α}, because for every $x \in Q$ we have

$$x^{R_a^\alpha} = x^{\alpha^{-1}R_a\alpha} = (x^{\alpha^{-1}} \cdot a)^\alpha = x \cdot a^\alpha = x^{R_{a^\alpha}}. \tag{1.1}$$

Consequently, if R_a is a permutation, then $R_a^{-\alpha} = (R_a^\alpha)^{-1} = R_{a^\alpha}^{-1}$. We will usually use this observation freely, without an explicit reference to (1.1).

2. The group of displacements

In this section we present basic properties of a certain subgroup of the right multiplication group, called the *group of displacements* (or the *transvection group*). Nearly all results proved in this section can be found in [24, Section 5] or [25, Section 1], often without a proof. The only fact we were not able to find elsewhere is Proposition 2.1(iv). Note that most results here apply to general racks, too.

For a rack Q, define the *group of displacements* as

$$\mathrm{Dis}(Q) = \langle\, R_a^{-1} R_b \,:\, a,\, b \in Q \,\rangle.$$

Note that

$$\mathrm{RMlt}(Q)' \le \mathrm{Dis}(Q) \le \mathrm{RMlt}(Q) \le \mathrm{Aut}(Q).$$

The first inequality follows from (1.1), as $[R_a, R_b] = R_a^{-1} R_a^{R_b} = R_a^{-1} R_{ab}$ for every $a, b \in Q$. We also have $R_a R_b^{-1} \in \mathrm{Dis}(Q)$ for every $a, b \in Q$, as $R_a R_b^{-1} = R_b^{-1} R_a^{R_b^{-1}} = R_b^{-1} R_c$, where $c = a^{R_b^{-1}}$.

Proposition 2.1. *Let Q be a rack. Then:*

(i) $\mathrm{Dis}(Q) \trianglelefteq \mathrm{Aut}(Q)$ *and* $\mathrm{RMlt}(Q) \trianglelefteq \mathrm{Aut}(Q)$.
(ii) *The group* $\mathrm{RMlt}(Q)/\mathrm{Dis}(Q)$ *is cyclic.*
(iii) $\mathrm{Dis}(Q) = \{R_{a_1}^{k_1} \dots R_{a_n}^{k_n} \,:\, n \ge 0,\, a_i \in Q \text{ and } \sum_{i=1}^n k_i = 0\}$.
(iv) *If Q is a quandle, the natural actions of* $\mathrm{RMlt}(Q)$ *and* $\mathrm{Dis}(Q)$ *on Q have the same orbits.*

Proof. Let $G = \mathrm{RMlt}(Q)$ and $D = \mathrm{Dis}(Q)$.

(i) By (1.1), conjugating a right translation by an automorphism yields another right translation. Thus the generators of both G and D are closed under conjugation in $\mathrm{Aut}(Q)$.

(ii) Fix $e \in Q$ and note that $DR_a = DR_e$ for every $a \in Q$. Given an element $\alpha = R_{a_1}^{k_1} \dots R_{a_n}^{k_n} \in G$, we then have $D\alpha = DR_e^{k_1 + \dots + k_n}$, proving that $G/D = \langle\, DR_e \,\rangle$.

(iii) Let S be the set in question. Since the defining generators of D belong to S, and since S is easily seen to be a subgroup of G, we have $D \le S$. For the other inclusion, we note that every $\alpha \in S$ can be written as $R_{a_1}^{k_1} \dots R_{a_n}^{k_n}$, where not only $\sum_i k_i = 0$ but also $k_i = \pm 1$. Assuming such a decomposition, we prove by induction on n that $\alpha \in D$.

If $n = 0$ then $\alpha = 1$, the case $n = 1$ does not occur, and if $n = 2$, we have either $\alpha = R_a R_b^{-1}$ or $\alpha = R_a^{-1} R_b$, both in D. Suppose that $n > 2$.

If $k_1 = k_n$ then there is $1 < m < n$ such that $\sum_{i<m} k_i = 0$ and $\sum_{i \ge m} k_i = 0$. Let $\beta = R_{a_1}^{k_1} \dots R_{a_{m-1}}^{k_{m-1}}$ and $\gamma = R_{a_m}^{k_m} \dots R_{a_n}^{k_n}$. Then $\beta, \gamma \in D$, and so $\alpha = \beta\gamma \in D$.

If $k_1 \ne k_n$ then $\alpha = R_a^k \beta R_b^{-k}$ for some $a, b \in Q$, $k = \pm 1$ and $\beta = R_{a_2}^{k_2} \dots R_{a_{n-1}}^{k_{n-1}}$. Note that $\sum_{2 \le i \le n-1} k_i = 0$, hence $\beta \in D$. We have $\alpha = \beta (R_a^k)^\beta R_b^{-k} = \beta R_{a^\beta}^k R_b^{-k}$, and since $R_{a^\beta}^k R_b^{-k} \in D$, we are done.

(iv) Let $\alpha = R_{a_1}^{k_1} \dots R_{a_n}^{k_n} \in G$ and put $k = k_1 + \dots + k_n$. Let $x, y \in Q$ be such that $x^\alpha = y$. By (iii), we have $\beta = \alpha R_y^{-k} \in D$ and $x^\beta = x^{\alpha R_y^{-k}} = y^{R_y^{-k}} = y$, using idempotence in the last step. □

The orbits of transitivity of the group $\mathrm{RMlt}(Q)$ (or, equivalently, of the group $\mathrm{Dis}(Q)$) in its natural action on Q will be referred to simply as *the orbits of Q*. Given $e \in Q$, we denote by e^Q the orbit containing e. Orbits are subquandles, not necessarily connected.

Example 2.2. In general, the proper inclusion $\mathrm{RMlt}(Q)' < \mathrm{Dis}(Q)$ can occur in quandles. The smallest example has three elements and two orbits, and is defined by the following Cayley table:

Q	1	2	3
1	1	1	1
2	3	2	2
3	2	3	3

However, in connected racks, the equality $\mathrm{RMlt}(Q)' = \mathrm{Dis}(Q)$ always holds.

Proposition 2.3. *If Q is a connected rack then* $\mathrm{RMlt}(Q)' = \mathrm{Dis}(Q)$.

Proof. It remains to prove that every generator $R_a^{-1}R_b$ of $\mathrm{Dis}(Q)$ belongs to $\mathrm{RMlt}(Q)'$. Let $\alpha \in \mathrm{RMlt}(Q)$ be such that $b = a^\alpha$. Then $R_a^{-1}R_b = R_a^{-1}R_{a^\alpha} = R_a^{-1}R_a^\alpha = [R_a, \alpha] \in \mathrm{RMlt}(Q)'$. □

In some cases, the structure of $\mathrm{Dis}(Q)$ corresponds nicely to the algebraic properties of Q. For instance, the following characterization of mediality can be traced back to [35].

Proposition 2.4. *Let Q be a rack. Then:*

(i) $\mathrm{Dis}(Q)$ *is trivial if and only if the multiplication in Q does not depend on the second argument (in quandles, this is equivalent to the multiplication being the left projection).*

(ii) $\mathrm{Dis}(Q)$ *is abelian if and only if Q is medial.*

Proof. (i) An inspection of the generating set shows that $\mathrm{Dis}(Q)$ is trivial iff $R_a = R_b$ for every a, $b \in Q$. If Q is a quandle, we then get $ab = a^{R_b} = a^{R_a} = a$.

(ii) Note that the following identities are equivalent: Q is medial, $R_yR_{uv} = R_uR_{yv}$, $R_yR_v^{-1}R_uR_v = R_uR_v^{-1}R_yR_v$,

$$R_yR_v^{-1}R_u = R_uR_v^{-1}R_y. \tag{2.1}$$

Suppose that $\mathrm{Dis}(Q)$ is abelian. Then $(R_yR_v^{-1})(R_uR_y^{-1}) = (R_uR_y^{-1})(R_yR_v^{-1}) = R_uR_v^{-1}$, which yields (2.1) upon applying R_y to both sides. Hence Q is medial.

Conversely, if Q is medial, then (2.1) holds, and its inverse yields $R_y^{-1}R_vR_u^{-1} = R_u^{-1}R_vR_y^{-1}$, so $R_xR_y^{-1}R_vR_u^{-1} = R_xR_u^{-1}R_vR_y^{-1} = R_vR_u^{-1}R_xR_y^{-1}$, where we have again used (2.1) in the last equality. Hence $\mathrm{Dis}(Q)$ is abelian. □

A prototypical example of medial quandles is the following construction.

Example 2.5. Let $A = (A, +)$ be an abelian group and $f \in \mathrm{Aut}(A)$. Define the *affine* quandle (also called *Alexander* quandle) as

$$\mathcal{Q}_{\mathrm{Aff}}(A, f) = (A, *), \quad x * y = x^f + y^{1-f}.$$

A straightforward calculation shows that $(A, *)$ is indeed a quandle. For mediality, observe that

$$(x * y) * (u * v) = (x^f + y^{1-f}) * (u^f + v^{1-f}) = x^{f^2} + y^{(1-f)f} + u^{f(1-f)} + v^{(1-f)^2}$$

is invariant under the interchange of y and u.

Alternatively, given an R-module M and an invertible element $r \in R$, then $(M, *)$ with

$$x * y = xr + y(1 - r)$$

is an affine quandle, namely $\mathcal{Q}_{\mathrm{Aff}}(A, f)$ with $A = (M, +)$ and $x^f = xr$. The two definitions are equivalent, and without loss of generality, we can consider $R = \mathbb{Z}[t, t^{-1}]$, the ring of integral Laurent series, and $r = t$.

Most affine quandles are not connected, and most medial quandles are not affine (e.g. the one in Example 2.2). However, we prove later that all connected medial quandles are affine. See [21] for comprehensive results on affine quandles.

3. Homogeneous quandles

An algebraic structure Q is called *homogeneous* if the automorphism group $\mathrm{Aut}(Q)$ acts transitively on Q. Connected quandles are homogeneous by definition, since their right multiplication group is a transitive subgroup of the automorphism group. Not every quandle is homogeneous, as witnessed by the quandle in Example 2.2.

We will now present a well-known construction of homogeneous quandles. Despite some effort, we were not able to trace its origin. It was certainly used by Galkin [15], who recognized its importance for representing Latin quandles, and also by Joyce [24] and others in the context of connected quandles. But the construction seems to be much older, see Loos [30], for instance.

Our immediate goal is to prove Joyce's observation that a quandle Q is homogeneous if and only if it is isomorphic to a quandle obtained by Construction 3.1.

Construction 3.1. Let G be a group, $f \in \mathrm{Aut}(G)$ and $H \leq C_G(f)$. Denote by G/H the set of right cosets $\{Hx : x \in G\}$. Define

$$\mathcal{Q}_{\mathrm{Hom}}(G, H, f) = (G/H, *), \quad Hx * Hy = H(xy^{-1})^f y.$$

Lemma 3.2. *Let $Q = \mathcal{Q}_{\mathrm{Hom}}(G, H, f)$ be as in Construction 3.1. Then Q is a homogeneous quandle.*

Proof. First we note that the operation $*$ is well defined. Indeed, if $Hx = Hu$ and $Hy = Hv$ then $u = hx$, $v = ky$ for some h, $k \in H$, and

$$\begin{aligned} H(uv^{-1})^f v &= H(hxy^{-1}k^{-1})^f ky = Hh^f (xy^{-1})^f (k^{-1})^f ky \\ &= Hh(xy^{-1})^f k^{-1} ky = H(xy^{-1})^f y, \end{aligned}$$

using $H \leq C_G(f)$. Idempotence is immediate from $Hx * Hx = H(xx^{-1})^f x = Hx$. For right distributivity we calculate

$$\begin{aligned} (Hx * Hz) * (Hy * Hz) &= H(xz^{-1})^f z * H(yz^{-1})^f z = H[(xz^{-1})^f z((yz^{-1})^f z)^{-1}]^f (yz^{-1})^f z \\ &= H(xy^{-1})^{f^2} (yz^{-1})^f z = H(xy^{-1})^f y * Hz = (Hx * Hy) * Hz. \end{aligned}$$

To check that all right translations of Q are permutations of G/H, note that for x, y, $z \in G$ we have

$$Hx * Hy = Hz \;\Leftrightarrow\; H(xy^{-1})^f y = Hz \;\Leftrightarrow\; Hx^f = Hzy^{-1}y^f \;\Leftrightarrow\; Hx = H(zy^{-1})^{f^{-1}} y,$$

where in the last step we applied f^{-1} to both sides and used $H \leq C_G(f)$. Hence, given Hy, Hz, the equation $Hx * Hy = Hz$ has a unique solution Hx.

To prove homogeneity, consider for any $a \in G$ the bijection $\varphi_a : Q \to Q$, $Hx \mapsto Hxa$. Since

$$(Hx)^{\varphi_a} * (Hy)^{\varphi_a} = Hxa * Hya = H(xaa^{-1}y^{-1})^f ya = H(xy^{-1})^f ya = (Hx * Hy)^{\varphi_a},$$

φ_a is an automorphism of Q. For any Hx, Hy there is $a \in Q$ such that $(Hx)^{\varphi_a} = Hxa = Hy$, so $\mathrm{Aut}(Q)$ acts transitively on Q. □

Example 3.3. Affine quandles are homogeneous. Indeed, if $(A, +)$ is an abelian group and $f \in \mathrm{Aut}(A)$, then $\mathcal{Q}_{\mathrm{Aff}}(A, f) = \mathcal{Q}_{\mathrm{Hom}}(A, 0, f)$.

Example 3.4. Knot quandles are homogeneous. Let K be a knot, and let $G_K = \pi_1(U_K)$ be the knot group, where U_K is the complement of a tubular neighborhood of K. Let H_K be the peripheral subgroup of G_K and f_K the conjugation by the meridian. Then $\mathcal{Q}_{\mathrm{Hom}}(G_K, H_K, f_K)$ is the knot quandle of K. See [24, Corollary 16.2] or [31, Proposition 2] for details.

In the special case of $\mathcal{Q}_{\mathrm{Hom}}(G, H, f)$ where G is a permutation group on a set Q and $H = G_e$ for some $e \in Q$, we define the mapping

$$\pi_e : \mathcal{Q}_{\mathrm{Hom}}(G, G_e, f) \to e^G, \quad G_e\alpha \mapsto e^\alpha. \tag{3.1}$$

Since $G_e\alpha = G_e\beta$ holds if and only if $e^\alpha = e^\beta$, the mapping π_e is well defined and bijective.

Proposition 3.5. *Let Q be a quandle and $e \in Q$. Let G be a normal subgroup of $\mathrm{Aut}(Q)$, and let f be the restriction of the conjugation by R_e in $\mathrm{Aut}(Q)$ to G. Then $\mathcal{Q}_{\mathrm{Hom}}(G, G_e, f)$ is well defined and isomorphic to the subquandle e^G.*

Proof. Since f is a restriction of the conjugation by $R_e \in \mathrm{RMlt}(Q) \leq \mathrm{Aut}(Q)$ to a normal subgroup G of $\mathrm{Aut}(Q)$, it is indeed an automorphism of G. To check $G_e \leq C_G(f)$, consider $\alpha \in G_e$. For every $x \in Q$ we have $x^{\alpha R_e} = x^\alpha \cdot e = x^\alpha \cdot e^\alpha = (xe)^\alpha = x^{R_e\alpha}$ and so $\alpha^{R_e} = \alpha$ as required. The quandle $\mathcal{Q}_{\mathrm{Hom}}(G, G_e, f)$ is therefore well defined, with multiplication

$$G_e\alpha * G_e\beta = G_e(\alpha\beta^{-1})^f\beta = G_eR_e^{-1}\alpha\beta^{-1}R_e\beta = G_e\alpha R_e^\beta.$$

The bijective mapping π_e from (3.1) is an isomorphism $\mathcal{Q}_{\mathrm{Hom}}(G, G_e, f) \to e^G$, since

$$(G_e\alpha * G_e\beta)^{\pi_e} = e^{R_e^{-1}\alpha\beta^{-1}R_e\beta} = (e^{\alpha\beta^{-1}} \cdot e)^\beta = e^\alpha \cdot e^\beta = (G_e\alpha)^{\pi_e} \cdot (G_e\beta)^{\pi_e},$$

where we have used $\beta \in \mathrm{Aut}(Q)$. □

Consider a situation from Proposition 3.5 in which G acts transitively on Q. Then

$$e^G = Q \simeq \mathcal{Q}_{\mathrm{Hom}}(G, G_e, f),$$

and we will call the isomorphism a *homogeneous representation* of Q. The most obvious choice $G = \mathrm{Aut}(Q)$ results in the following characterization.

Theorem 3.6 ([24, Theorem 7.1])**.** *A quandle is homogeneous if and only if it is isomorphic to a quandle obtained by Construction 3.1.*

Proof. Lemma 3.2 establishes the converse implication. For the direct implication, suppose that Q is homogeneous, take $G = \mathrm{Aut}(Q)$, and apply Proposition 3.5. □

In view of Proposition 2.1(iv), connected quandles can be represented using $G = \mathrm{RMlt}(Q)$ or $G = \mathrm{Dis}(Q)$. The two cases will be studied in detail in the next two sections, resulting in the *canonical* and *minimal* representations.

4. Minimal representation for connected quandles

Suppose that Q is a connected quandle, $e \in Q$, and let $G = \mathrm{RMlt}(Q)' = \mathrm{Dis}(Q)$. The homogeneous representation $Q \simeq \mathcal{Q}_{\mathrm{Hom}}(G, G_e, f)$ of Proposition 3.5 will be called *minimal*. The following result (essentially Galkin's [15, Theorem 4.4]) gives the reason for the terminology.

Theorem 4.1. *Let Q be a connected quandle. If $Q \simeq \mathcal{Q}_{\mathrm{Hom}}(G, H, f)$ for some group G, $f \in \mathrm{Aut}(G)$ and $H \leq C_G(f)$, then $\mathrm{RMlt}(Q)'$ embeds into a quotient of G.*

Proof. Assume for simplicity that $Q = \mathcal{Q}_{\mathrm{Hom}}(G, H, f)$. Define $\varphi : G \to \mathrm{Aut}(Q)$ by $a \mapsto \varphi_a$, where $(Hx)^{\varphi_a} = Hxa$ as in the proof of Lemma 3.2. The mapping φ is obviously a homomorphism. We show that $\mathrm{RMlt}(Q)'$ is a subgroup of $\mathrm{Im}(\varphi)$, and hence that $\mathrm{RMlt}(Q)'$ embeds into $G/\mathrm{Ker}(\varphi)$.

By Proposition 2.3, $\mathrm{RMlt}(Q)' = \mathrm{Dis}(Q)$. It therefore suffices to check that $R_{Hx}^{-1} R_{Hy} \in \mathrm{Im}(\varphi)$ for every x, $y \in G$. Recall that the unique solution to $Hx * Hy = Hz$ is $Hx = H(zy^{-1})^{f^{-1}} y = (Hz)^{R_{Hy}^{-1}}$. Hence for every x, y, $u \in G$ we have

$$(Hu)^{R_{Hx}^{-1} R_{Hy}} = (H(ux^{-1})^{f^{-1}} x)^{R_{Hy}} = H((ux^{-1})^{f^{-1}} xy^{-1})^f y = Hux^{-1}(xy^{-1})^f y,$$

proving $R_{Hx}^{-1} R_{Hy} = \varphi_{x^{-1}(xy^{-1})^f y}$. □

In particular, if Q is a finite connected quandle, and if G is of smallest order among all groups such that $Q \simeq \mathcal{Q}_{\mathrm{Hom}}(G, H, f)$, then $G \simeq \mathrm{RMlt}(Q)'$.

5. Canonical correspondence for connected quandles

Throughout this section, fix a set Q and an element $e \in Q$. We proceed to establish a one-to-one correspondence between connected quandles defined on Q and certain configurations in transitive groups on Q that we will call quandle envelopes. To distinguish quandles defined on Q from the underlying set Q, we will explicitly name the quandle operation on Q.

A *quandle folder* is a pair (G, ζ) such that G is a transitive group on Q and $\zeta \in Z(G_e)$, the center of the stabilizer of e. A *quandle envelope* is a quandle folder such that $\langle\, \zeta^G \,\rangle = G$, that is, the smallest normal subgroup of G containing ζ is all of G.

For a connected quandle $(Q, \cdot)$, define

$$\mathcal{E}(Q, \cdot) = (\mathrm{RMlt}(Q, \cdot), R_e).$$

Lemma 5.1. *Let $(Q, \cdot)$ be a connected quandle and $e \in Q$. Then $\mathcal{E}(Q, \cdot)$ is a quandle envelope.*

Proof. Let $(Q, \cdot)$ and $G = \mathrm{RMlt}(Q, \cdot)$. Note that $R_e \in G_e$. For any $\alpha \in G_e \leq \mathrm{Aut}(Q, \cdot)$, we calculate $x^{\alpha R_e} = x^\alpha \cdot e = x^\alpha \cdot e^\alpha = (xe)^\alpha = x^{R_e \alpha}$, so $R_e \in Z(G_e)$. Since the quandle $(Q, \cdot)$ is connected, G acts transitively on the set Q, and for every $x \in Q$ there is $\widehat{x} \in G$ such that $e^{\widehat{x}} = x$. Then $R_e^{\widehat{x}} = R_{e^{\widehat{x}}} = R_x$, proving that $\langle\, R_e^G \,\rangle = G$. □

For a quandle folder (G, ζ), define

$$\mathcal{Q}(G, \zeta) = (Q, \circ), \quad x \circ y = x^{\zeta^{\widehat{y}}},$$

where $\widehat{y}$ is any element of G satisfying $e^{\widehat{y}} = y$. We shall see that the operation does not depend on the choice of the permutations $\widehat{y}$, and that $\mathcal{Q}(G, \zeta)$ is a homogeneous quandle.

Lemma 5.2. *Let (G, ζ) be a quandle folder on a set Q with a fixed element $e \in Q$. Then:*

(i) *If α, $\beta \in G$ satisfy $e^\alpha = e^\beta$ then $\zeta^\alpha = \zeta^\beta$.*
(ii) *The definition of $\mathcal{Q}(G, \zeta)$ does not depend on the choice of the permutations $\widehat{y}$.*
(iii) *The mapping π_e of (3.1) is an isomorphism of $\mathcal{Q}_{\mathrm{Hom}}(G, G_e, \phi_\zeta)$ onto $\mathcal{Q}(G, \zeta)$.*
(iv) *$\mathcal{Q}(G, \zeta)$ is a homogeneous quandle.*
(v) $\mathrm{RMlt}(\mathcal{Q}(G, \zeta)) = \langle\, \zeta^{\widehat{y}} : y \in Q \,\rangle = \langle\, \zeta^G \,\rangle$.
(vi) *If (G, ζ) is a quandle envelope, then $\mathcal{Q}(G, \zeta)$ is a connected quandle.*

Proof. For α, $\beta \in G$, note that $\zeta^\alpha = \zeta^\beta$ iff $\beta^{-1}\alpha$ commutes with ζ. The latter condition certainly holds when $e^\alpha = e^\beta$ because $\zeta \in Z(G_e)$. This proves (i), and part (ii) follows.

Consider again the bijection π_e of (3.1). Since G is transitive, π_e is onto Q. To check that π_e is a homomorphism, note that $\zeta^\beta = \zeta^{\widehat{e^\beta}}$ by (i). Therefore, with $\mathcal{Q}_{\mathrm{Hom}}(G, G_e, \phi_\zeta) = (G/G_e, *)$, we have $G_e\alpha * G_e\beta = G_e(\alpha\beta^{-1})^\zeta\beta = G_e\zeta^{-1}\alpha\zeta^\beta = G_e\alpha\zeta^\beta$, and thus

$$(G_e\alpha * G_e\beta)^{\pi_e} = (G_e\alpha\zeta^\beta)^{\pi_e} = e^{\alpha\zeta^\beta} = (e^\alpha)^{\zeta^{\widehat{e^\beta}}} = e^\alpha \circ e^\beta = (G_e\alpha)^{\pi_e} \circ (G_e\beta)^{\pi_e}.$$

This proves (iii), and part (iv) follows from Lemma 3.2.

For (v), note that the right translation by y in $(Q, \circ)$ is the mapping $\zeta^{\widehat{y}}$ and, once again, $\zeta^\beta = \zeta^{\widehat{e^\beta}}$ for any $\beta \in G$. Part (vi) follows. □

Theorem 5.3 (Canonical correspondence)**.** *Let Q be a set with a fixed element $e \in Q$. Then the mappings*

$$\mathcal{E} : (Q, \cdot) \mapsto (\mathrm{RMlt}(Q, \cdot), R_e),$$
$$\mathcal{Q} : (G, \zeta) \mapsto (Q, \circ), \quad x \circ y = x^{\zeta^{\widehat{y}}}$$

are mutually inverse bijections between the set of connected quandles and the set of quandle envelopes on Q.

Proof. In view of Lemmas 5.1 and 5.2, it remains to show that the two mappings are mutually inverse. Let (G, ζ) be a quandle envelope, and let $(Q, \circ) = \mathcal{Q}(G, \zeta)$ be the corresponding connected quandle. Then $\mathrm{RMlt}(Q, \circ) = \langle\, \zeta^G \,\rangle = G$ by Lemma 5.2. Moreover, $x^{R_e} = x \circ e = x^{\zeta^{\widehat{e}}} = x^\zeta$ thanks to $\widehat{e} \in G_e$ and $\zeta \in Z(G_e)$. Hence ζ is the right translation by e in $(Q, \circ)$. It follows that $\mathcal{E}(\mathcal{Q}(G, \zeta)) = (G, \zeta)$.

Conversely, let $(Q, \cdot)$ be a connected quandle and let $\mathcal{E}(Q, \cdot) = (\mathrm{RMlt}(Q, \cdot), R_e)$ be the corresponding quandle envelope. Then, in $\mathcal{Q}(\mathcal{E}(Q, \cdot))$, we calculate $x \circ y = x^{R_e^{\widehat{y}}} = x^{R_y} = x \cdot y$. It follows that $\mathcal{Q}(\mathcal{E}(Q, \cdot)) = (Q, \cdot)$. □

Example 5.4. Let K be a knot, G_K its knot group, and Q_K its knot quandle. Then G_K acts transitively on the underlying set of Q_K, and the stabilizer of a fixed element $e \in Q$ is the peripheral subgroup H_K. Since $H_K \simeq \mathbb{Z} \times \mathbb{Z}$, the meridian m is central in the stabilizer, and it follows from Wirtinger's presentation of G_K that $G_K = \langle\, m^{G_K} \,\rangle$. We proved that (G_K, m) is a quandle envelope. The knot quandle Q_K is isomorphic to $\mathcal{Q}(G_K, m)$. See [24, Section 16] or [31, Section 6] for details.

We conclude this section by solving the isomorphism problem and describing the automorphism group of connected quandles under the canonical correspondence. We start with a useful characterization of isomorphisms.

Lemma 5.5. *Let (G,ζ), (K,ξ) be quandle envelopes on a set Q with a fixed element $e \in Q$, and let*

- *A be the set of all quandle isomorphisms $\varphi : \mathcal{Q}(G,\zeta) \to \mathcal{Q}(K,\xi)$ such that $e^\varphi = e$;*
- *B be the set of all permutations φ of Q such that $e^\varphi = e$, $\zeta^\varphi = \xi$ and $G^\varphi = K$;*
- *C be the set of all group isomorphisms $\psi : G \to K$ such that $\zeta^\psi = \xi$ and $G_e^\psi = K_e$.*

Then $A = B$ and $\varphi \mapsto \phi_\varphi$ is a bijection from $A = B$ to C.

Proof. Let f denote the mapping $\varphi \mapsto \phi_\varphi$ defined on B. We show that $A \subseteq B$, that f maps B into C, and we construct a mapping $g : C \to A \subseteq B$ such that fg is the identity mapping on B and gf is the identity mapping on C. This will prove the result.

Let $\mathcal{Q}(G,\zeta) = (Q,\circ)$, where $x \circ y = x^{\zeta^{\widehat{y}}}$ for some $\widehat{y} \in G$ satisfying $e^{\widehat{y}} = y$, and $\mathcal{Q}(K,\xi) = (Q,*)$, where $x * y = x^{\xi^{\overline{y}}}$ for some $\overline{y} \in K$ such that $e^{\overline{y}} = y$. For a permutation φ of Q, the following universally quantified identities are equivalent:

$$(x \circ y)^\varphi = (x^\varphi) * (y^\varphi), \qquad (x^{\zeta^{\widehat{y}}})^\varphi = (x^\varphi)^{\xi^{\overline{y^\varphi}}}, \qquad x^{\varphi^{-1}\zeta^{\widehat{y}}\varphi} = x^{\xi^{\overline{y^\varphi}}}.$$

Hence φ is an isomorphism $(Q,\circ) \to (Q,*)$ if and only if

$$(\zeta^{\widehat{y}})^\varphi = \xi^{\overline{y^\varphi}}.$$

We will use this fact freely, as well as Lemma 5.2.

($A \subseteq B$): We need to show $\zeta^\varphi = \xi$ and $G^\varphi = K$. Since $e^\varphi = e$, we have $\zeta^\varphi = (\zeta^{\widehat{e}})^\varphi = \xi^{\overline{e^\varphi}} = \xi^{\overline{e}} = \xi$. To prove $G^\varphi \subseteq K$, note that $G = \langle\, \zeta^G \,\rangle$, pick $\alpha \in G$, and calculate $(\zeta^\alpha)^\varphi = (\zeta^{\widehat{e^\alpha}})^\varphi = \xi^{\overline{e^{\alpha\varphi}}} \in K$. For the other inclusion $K \subseteq G^\varphi$, note that $K = \langle\, \xi^K \,\rangle$, pick $\beta \in K$, find $\alpha \in G$ such that $e^\beta = e^{\alpha\varphi}$ by transitivity of G, and calculate $\xi^\beta = \xi^{\overline{e^\beta}} = \xi^{\overline{e^{\alpha\varphi}}} = (\zeta^{\widehat{e^\alpha}})^\varphi \in G^\varphi$.

($f : B \to C$): For $\varphi \in B$ let $\psi = \varphi^f = \phi_\varphi$ be the conjugation by φ. Since $G^\varphi = K$, we see that ψ is an isomorphism $G \to K$. Clearly $\zeta^\psi = \zeta^\varphi = \xi$. To verify $G_e^\psi = K_e$, let $\alpha \in G_e$ and calculate $e^{\alpha^\psi} = e^{\alpha^\varphi} = e^{\varphi^{-1}\alpha\varphi} = e$, so $\alpha^\psi \in K_e$.

($g : C \to A$): For $\psi \in C$, define $\varphi = \psi^g$ by

$$x^\varphi = e^{\widehat{x}^{\,\psi}}$$

for every $x \in Q$. We show that φ is an isomorphism $(Q,\circ) \to (Q,*)$ that fixes e. The second condition follows immediately from $e^\varphi = e^{\widehat{e}^{\,\psi}} = e$, because $\widehat{e} \in G_e$ and $G_e^\psi = K_e$. Let us observe two facts. First, if α, $\beta \in G$, then

$$e^{\alpha^\psi} = e^{\beta^\psi} \;\Leftrightarrow\; e^{\beta^\psi(\alpha^\psi)^{-1}} = e \;\Leftrightarrow\; (\beta\alpha^{-1})^\psi \in K_e \;\Leftrightarrow\; \beta\alpha^{-1} \in G_e \;\Leftrightarrow\; e^\alpha = e^\beta,$$

hence φ is a bijection. Second, for any $x \in Q$ and $\alpha \in G$ we have $e^{\widehat{x^\alpha}} = x^\alpha = e^{\widehat{x}\alpha}$. Combining the two observations, we see that

$$e^{\widehat{x^\alpha}^{\,\psi}} = e^{(\widehat{x}\alpha)^\psi}. \tag{5.1}$$

For x, $y \in Q$, we then have

$$\begin{aligned}(x \circ y)^\varphi &= e^{\widehat{x\circ y}^{\,\psi}} = e^{\widehat{x\zeta^{\widehat{y}}}^{\,\psi}} = e^{(\widehat{x}\zeta^{\widehat{y}})^\psi} = e^{\widehat{x}^{\,\psi}(\zeta^{\widehat{y}})^\psi} \\ &= (x^\varphi)^{(\zeta^{\widehat{y}})^\psi} = (x^\varphi)^{(\zeta^\psi)^{(\widehat{y}^{\,\psi})}} = (x^\varphi)^{\xi^{(\widehat{y}^{\,\psi})}} = (x^\varphi)^{\xi^{\overline{y^\varphi}}} = x^\varphi * y^\varphi,\end{aligned}$$

where in the penultimate step we have used $e^{\widehat{y}^{\,\psi}} = y^\varphi$.

($fg = \mathrm{id}$): For $\varphi \in B$ and $x \in Q$ we have

$$x^{\varphi^{fg}} = x^{(\varphi^f)^g} = e^{\widehat{x}^{(\varphi^f)}} = e^{\widehat{x}^{\varphi}} = e^{\varphi^{-1}\widehat{x}\varphi} = e^{\widehat{x}\varphi} = x^{\varphi}.$$

($gf = \mathrm{id}$): For $\psi \in C$ and $\alpha \in G$, we would like to show that $\alpha^{\psi^{gf}} = \alpha^{(\psi^g)^f} = \alpha^{\psi^g}$ is equal to α^{ψ}. Let $x \in Q$, set $u = x^{(\psi^g)^{-1}}$ for brevity, and keeping (5.1) in mind, calculate

$$x^{\alpha^{\psi^g}} = x^{(\psi^g)^{-1}\alpha\psi^g} = (u^{\alpha})^{\psi^g} = e^{\widehat{u^{\alpha}}^{\psi}} = e^{(\widehat{u}\alpha)^{\psi}} = e^{\widehat{u}^{\psi}\alpha^{\psi}} = (u^{\psi^g})^{\alpha^{\psi}} = x^{\alpha^{\psi}}.$$

□

A solution to the isomorphism problem now easily follows.

Theorem 5.6. *Let (G, ζ), (K, ξ) be quandle envelopes on a set Q with a fixed element $e \in Q$. Then the following conditions are equivalent:*

(i) $\mathcal{Q}(G, \zeta) \simeq \mathcal{Q}(K, \xi)$.
(ii) *There is a permutation φ of Q such that $e^{\varphi} = e$, $\zeta^{\varphi} = \xi$ and $G^{\varphi} = K$.*
(iii) *There is an isomorphism $\psi : G \to K$ such that $\zeta^{\psi} = \xi$ and $G_e^{\psi} = K_e$.*

Proof. Let $\rho : \mathcal{Q}(G, \zeta) \to \mathcal{Q}(K, \xi)$ be an isomorphism, and let $\alpha \in K$ be such that $e^{\rho\alpha} = e$. Since $\alpha \in K = \mathrm{RMlt}(\mathcal{Q}(K, \xi)) \leq \mathrm{Aut}(\mathcal{Q}(K, \xi))$ by Theorem 5.3, the permutation $\varphi = \rho\alpha$ is also an isomorphism $\mathcal{Q}(G, \zeta) \to \mathcal{Q}(K, \xi)$ and it satisfies $e^{\varphi} = e$. The rest follows from Lemma 5.5. □

Recall that two permutation groups acting on a set Q are said to be *equivalent* if they are conjugate in the symmetric group S_Q. Theorem 5.6 shows that if the connected quandles $\mathcal{Q}(G, \zeta)$, $\mathcal{Q}(K, \xi)$ are isomorphic, then the transitive groups G, K are equivalent, and the permutations ζ, ξ have the same cycle structures. While enumerating connected quandles of order n, it therefore suffices to investigate transitive groups of degree n up to equivalence, which is the usual way transitive groups are cataloged in computational packages. The following result solves the isomorphism problem for a fixed transitive group G.

Corollary 5.7. *Let (G, ζ), (G, ξ) be quandle envelopes on a set Q with a fixed element $e \in Q$. Then $\mathcal{Q}(G, \zeta)$ is isomorphic to $\mathcal{Q}(G, \xi)$ if and only if ζ and ξ are conjugate in $N_{(S_Q)_e}(G)$, the normalizer of G in the stabilizer of e in the symmetric group S_Q.*

Another application of Lemma 5.5 reveals the structure of the automorphism group of a connected quandle in terms of its right multiplication group. For a group G, a subgroup $H \leq G$ and an element $x \in G$ we let

$$\mathrm{Aut}(G)_{x,H} = \{\psi \in \mathrm{Aut}(G) \,:\, x^{\psi} = x,\ H^{\psi} = H\} \leq \mathrm{Aut}(G).$$

Proposition 5.8. *Let $Q = (Q, \cdot)$ be a connected quandle, $e \in Q$, and let $G = \mathrm{RMlt}(Q)$. Then $\mathrm{Aut}(Q)$ is isomorphic to $(G \rtimes \mathrm{Aut}(G)_{R_e, G_e}) / \{(\alpha, \phi_{\alpha}^{-1}) \,:\, \alpha \in G_e\}$.*

Proof. By Theorem 5.3, we have $(Q, \cdot) = \mathcal{Q}(G, R_e)$. According to Lemma 5.5, $\varphi \mapsto \phi_{\varphi}$ is a bijection between $\mathrm{Aut}(Q)_e$ and $\mathrm{Aut}(G)_{R_e, G_e}$, which is easily seen to be a homomorphism. Define $f : G \rtimes \mathrm{Aut}(Q)_e \to \mathrm{Aut}(Q)$ by $(\alpha, \varphi)^f = \alpha\varphi$. This is a homomorphism, since

$$(\alpha, \varphi)^f(\beta, \psi)^f = \alpha\varphi\beta\psi = \alpha\beta^{\varphi^{-1}}\varphi\psi = ((\alpha, \varphi)(\beta, \psi))^f.$$

Since G acts transitively on Q, every $\psi \in \mathrm{Aut}(Q)$ can be decomposed as $\psi = \alpha\varphi$, where $\alpha \in G$ and $\varphi \in \mathrm{Aut}(Q)_e$. Thus f is surjective. The kernel of f consists of all tuples (α, φ) with $\alpha\varphi = 1$, hence $\varphi = \alpha^{-1} \in G \cap \mathrm{Aut}(Q)_e = G_e$. □

6. Latin quandles

A quandle Q is called *Latin*, if also the left translations

$$L_x : Q \to Q, \quad y \mapsto xy$$

are permutations of Q. Every Latin quandle is connected. Indeed, given $x, y \in Q$, let z be the unique element such that $xz = y$, and we have $x^{R_z} = y$.

In this section, we determine when a finite quandle in the homogeneous representation is Latin, and which quandle envelopes correspond to Latin quandles. For more details on Latin quandles we refer to [38].

Lemma 6.1 ([15, Theorem 4.2])**.** *Let G be a group, $f \in \mathrm{Aut}(G)$ and $H \leq C_G(f)$. Suppose that the quandle $Q = \mathcal{Q}_{\mathrm{Hom}}(G, H, f)$ is finite. Then Q is Latin if and only if, for every $a, u \in G$,*

$$(u^{-1})^f u \in H^a \text{ implies } u \in H. \tag{6.1}$$

Proof. A finite quandle is Latin if and only if every left translation is one-to-one. For $x \in G$, the following statements are then equivalent:

$$\begin{aligned}
&L_{xH} \text{ is one-to-one,}\\
&H(xy^{-1})^f y = H(xz^{-1})^f z \text{ implies } Hy = Hz,\\
&(xy^{-1})^f y z^{-1} (zx^{-1})^f \in H \text{ implies } yz^{-1} \in H,\\
&(y^{-1})^f y z^{-1} z^f \in H^{x^f} \text{ implies } yz^{-1} \in H,\\
&((u^{-1})^f u)^{z^f} \in H^{x^f} \text{ implies } u \in H,
\end{aligned}$$

where in the last equivalence we have used the substitution $u = yz^{-1}$. Now, if every L_{xH} is one-to-one, we obtain (6.1) from the last line above by taking $z = 1$ and $x^f = a$. Conversely, to prove that any L_{xH} is one-to-one, consider u, z such that $((u^{-1})^f u)^{z^f} \in H^{x^f}$. Then $(u^{-1})^f u \in H^{(xz^{-1})^f}$, and we can use (6.1) to conclude that $u \in H$. □

Proposition 6.2. *Let Q be a finite homogeneous quandle, $e \in Q$, and let G be a normal subgroup of $\mathrm{Aut}(Q)$ that is transitive on Q. Then Q is Latin if and only if for every $\alpha \in G \setminus G_e$ the commutator $[R_e, \alpha]$ has no fixed points.*

Proof. Consider the homogeneous representation $Q \simeq \mathcal{Q}_{\mathrm{Hom}}(G, G_e, f)$ from Proposition 3.5, i.e., we have $\alpha^f = \alpha^{R_e}$ for every $\alpha \in G$. Condition (6.1) says that, for every $\alpha, \beta \in G$, if $(\alpha^{-1})^{R_e}\alpha \in G_e^\beta$ then $\alpha \in G_e$. Since $G_e^\beta = G_{e^\beta}$ and G is transitive, we can reformulate the condition as follows: for every $\alpha \in G$ and $x \in Q$, if $[R_e, \alpha] \in G_x$ then $\alpha \in G_e$. In other words, if $[R_e, \alpha]$ has a fixed point then $\alpha \in G_e$. □

Proposition 6.3. *Let (G, ζ) be a quandle envelope with G finite. Then $\mathcal{Q}(G, \zeta)$ is a Latin quandle if and only if for every $\alpha \in G \setminus G_e$ the commutator $[\zeta, \alpha]$ has no fixed points.*

Proof. Using Theorem 5.3, we obtain the claim by applying Proposition 6.2 to $Q = \mathcal{Q}(G, \zeta)$ and $G = \mathrm{RMlt}(Q)$. □

7. Connected affine quandles

Let $(A,+)$ be an abelian group. Then

$$\mathrm{Aff}(A,+) = \{x \mapsto c + x^f \,:\, c \in A,\ f \in \mathrm{Aut}(A,+)\}$$

is a subgroup of the symmetric group over A, and the elements of $\mathrm{Aff}(A,+)$ are called *affine mappings* over $(A,+)$. The set of translations

$$\mathrm{Mlt}(A,+) = \{x \mapsto c + x \,:\, c \in A\}$$

is a subgroup of $\mathrm{Aff}(A,+)$.

Recall from Example 2.5 that $\mathcal{Q}_{\mathrm{Aff}}(A,f)$, where $f \in \mathrm{Aut}(A)$, denotes the affine quandle $(A,*)$ with multiplication $x * y = x^f + y^{1-f}$. In $\mathcal{Q}_{\mathrm{Aff}}(A,f)$,

$$x^{R_y} = x^f + y^{1-f}, \qquad x^{R_y^{-1}} = x^{f^{-1}} + y^{1-f^{-1}},$$

hence the right translations are affine mappings over $(A,+)$ and $\mathrm{RMlt}(\mathcal{Q}_{\mathrm{Aff}}(A,f))$ is a subgroup of $\mathrm{Aff}(A,+)$. In calculations, it is useful to remember that the group $\mathrm{Aff}(A,+)$ is isomorphic to $(A,+) \rtimes \mathrm{Aut}(A,+)$, the holomorph of $(A,+)$, where the mapping $x \mapsto c + x^f$ corresponds to the pair (c,f).

Proposition 7.1. *Let $Q = \mathcal{Q}_{\mathrm{Aff}}(A,f)$ be an affine quandle. Then*

$$\mathrm{Dis}(Q) = \{x \mapsto x + c \,:\, c \in \mathrm{Im}(1-f)\},$$

hence $\mathrm{Dis}(Q)$ *is isomorphic to* $\mathrm{Im}(1-f)$.

Proof. Let $T = \{x \mapsto x + c \,:\, c \in \mathrm{Im}(1-f)\}$. If we show that $\mathrm{Dis}(Q) = T$, then the mapping $\varphi : \mathrm{Im}(1-f) \to \mathrm{Dis}(Q)$ which maps c to the translation by c is an isomorphism. Note that T is closed with respect to composition. For the inclusion $\mathrm{Dis}(Q) \subseteq T$, we calculate

$$z^{R_x^{-1}R_y} = (z^{f^{-1}} + x^{1-f^{-1}})^f + y^{1-f} = z + x^{(1-f^{-1})f} + y^{1-f} = z + x^{f-1} + y^{1-f},$$

so $z^{R_x^{-1}R_y} = z + c$ with the constant $c = (x^{-1})^{1-f} + y^{1-f} \in \mathrm{Im}(1-f)$. The generators of $\mathrm{Dis}(Q)$ are therefore in T, and $\mathrm{Dis}(Q) \leq T$ follows.

For the other inclusion $\mathrm{Dis}(Q) \supseteq T$, given $c \in \mathrm{Im}(1-f)$, choose $x \in A$ so that $x^{f-1} = c$, and verify that $z^{R_x^{-1}R_0} = (z^{f^{-1}} + x^{1-f^{-1}})^f = z + c$. □

Corollary 7.2. *An affine quandle $\mathcal{Q}_{\mathrm{Aff}}(A,f)$ is connected if and only if $1-f$ is onto.*

Consequently, if Q is a connected affine quandle, then the isomorphism type of the underlying abelian group $(Q,+)$ is uniquely determined by the quandle. Indeed, $(Q,+) = \mathrm{Im}(1-f) \simeq \mathrm{Dis}(Q)$. (An analogous statement does not hold for disconnected affine quandles which can be supported by non-isomorphic groups.)

Another consequence is that a finite affine quandle is connected if and only if it is Latin. A stronger result is proved in [7, Theorem 5.10]: *A finite left and right distributive quandle is connected if and only if it is Latin.* Infinite connected affine quandles need not be Latin, however. Indeed, in $\mathcal{Q}_{\mathrm{Aff}}(\mathbb{Z}_{p^\infty}, 1-p)$, the mapping $1-(1-p) = p$ is onto but not one-to-one.

We are now going to establish a characterization of connected quandles that are affine, or, equivalently, medial. Condition (iii) below provides a computationally efficient criterion for checking whether a connected quandle is affine. The crucial point is condition (iv), which is interesting in its own right and will be used in Section 9. We were not able to find the characterization of Theorem 7.3 in the literature.

Theorem 7.3. *The following conditions are equivalent for a connected quandle Q:*

(i) *Q is affine.*
(ii) *Q is medial.*
(iii) *$\mathrm{RMlt}(Q)'$ is abelian.*
(iv) *There is an abelian group $A = (Q, +)$ such that $\mathrm{Mlt}(A) \leq \mathrm{RMlt}(Q) \leq \mathrm{Aff}(A)$.*

Proof. (i) $\Rightarrow$ (ii) $\Rightarrow$ (iii): We have already seen in Example 2.5 that every affine quandle is medial. By Propositions 2.3 and 2.4, every connected medial quandle Q has $\mathrm{RMlt}(Q)' = \mathrm{Dis}(Q)$ abelian.

(iii) $\Rightarrow$ (iv): Fix $e \in Q$. Since $\mathrm{RMlt}(Q)'$ is abelian and transitive (by Propositions 2.1 and 2.3), it is sharply transitive. Thus for every $y \in Q$ there is a unique $\widehat{y} \in \mathrm{RMlt}(Q)'$ such that $e^{\widehat{y}} = y$. Define $A = (Q, +)$ by

$$x + y = x^{\widehat{y}}.$$

We claim that $\varphi : A \to \mathrm{RMlt}(Q)'$, $x \mapsto \widehat{x}$ is an isomorphism and hence that A is an abelian group. Indeed, φ is clearly a bijection, we have $e^{\widehat{x^{\widehat{y}}}} = x^{\widehat{y}} = e^{\widehat{x}\widehat{y}}$, thus $\widehat{x^{\widehat{y}}} = \widehat{x}\widehat{y}$ by sharp transitivity, and so $(x + y)^{\varphi} = (x^{\widehat{y}})^{\varphi} = \widehat{x^{\widehat{y}}} = \widehat{x}\widehat{y} = x^{\varphi} y^{\varphi}$.

Since the right translation by y in A is $\widehat{y} \in \mathrm{RMlt}(Q)'$, we have $\mathrm{Mlt}(A) = \mathrm{RMlt}(Q)' \leq \mathrm{RMlt}(Q)$. To prove that $\mathrm{RMlt}(Q) \leq \mathrm{Aff}(A)$, it suffices to show that $R_e \in \mathrm{Aut}(A)$ and $x \cdot y = x^{R_e} + y^{1-R_e}$, because then $R_y \in \mathrm{Aff}(A)$ for every $y \in Q$. We have $R_e \in \mathrm{Aut}(A)$ iff $(x + y)^{R_e} = x^{\widehat{y}R_e}$ is equal to $x^{R_e} + y^{R_e} = x^{R_e \widehat{y^{R_e}}}$ for every x, $y \in Q$, which is equivalent to $\widehat{y}^{R_e} = \widehat{y^{R_e}}$ for every $y \in Q$. Taking advantage of sharp transitivity, the last equality is verified by $e^{\widehat{y}^{R_e}} = y \cdot e = e^{\widehat{y^{R_e}}}$. We have $(Q, \cdot) = \mathcal{Q}(\mathcal{E}(Q, \cdot))$ by Theorem 5.3, and hence

$$x \cdot y = x^{R_e^{\widehat{y}}} = x^{\widehat{y}^{-1} R_e \widehat{y}} = (x - y)^{R_e} + y = y^{1-R_e} + x^{R_e}.$$

(iv) $\Rightarrow$ (i): Let 0 be the identity element of $A = (Q, +)$. Fix $y \in Q$ and denote by ρ_y the right translation by y in A. By Theorem 5.3, we have $R_y = R_0^{\widehat{y}}$ for some $\widehat{y} \in \mathrm{RMlt}(Q)$ such that $0^{\widehat{y}} = y$. Since $\mathrm{RMlt}(Q) \leq \mathrm{Aff}(A)$, there are $c \in Q$ and $g \in \mathrm{Aut}(A)$ such that $x^{\widehat{y}} = c + x^g$ for every $x \in Q$. But $c = 0^{\widehat{y}} = y$, so $x^{\widehat{y}} = y + x^g$ and $\widehat{y} = g\rho_y$. Since $\mathrm{Mlt}(A) \leq \mathrm{RMlt}(Q)$, we have $g = \widehat{y}\rho_y^{-1} \in \mathrm{RMlt}(Q)$. Hence $g \in \mathrm{RMlt}(Q)_0$, and since $R_0 \in Z(\mathrm{RMlt}(Q)_0)$, we obtain $gR_0 = R_0 g$. Since $0^{R_0} = 0$ by idempotence, we have not only $R_0 \in \mathrm{Aff}(A)$ but in fact $R_0 \in \mathrm{Aut}(A)$. Using all these facts, we calculate

$$x \cdot y = x^{R_0^{\widehat{y}}} = x^{\widehat{y}^{-1} R_0 \widehat{y}} = x^{\rho_y^{-1} g^{-1} R_0 g \rho_y} = x^{\rho_y^{-1} R_0 \rho_y} = (x - y)^{R_0} + y = x^{R_0} + y^{1-R_0}$$

for every x, $y \in Q$, proving that $(Q, \cdot) = \mathcal{Q}_{\mathrm{Aff}}(A, R_0)$ is an affine quandle. □

Corollary 7.4. *The following conditions are equivalent for a quandle envelope (G, ζ):*

(i) *$\mathcal{Q}(G, \zeta)$ is affine.*
(ii) *$\mathcal{Q}(G, \zeta)$ is medial.*
(iii) *G is metabelian.*
(iv) *There is an abelian group A such that $\mathrm{Mlt}(A) \leq G \leq \mathrm{Aff}(A)$.*

Theorem 7.3 is related to the Toyoda-Bruck theorem [2] which states that medial quasigroups are affine.

It is not hard to check that two connected affine quandles $\mathcal{Q}_{\mathrm{Aff}}(A, f)$, $\mathcal{Q}_{\mathrm{Aff}}(A, g)$ are isomorphic if and only if f and g are conjugate in $\mathrm{Aut}(A)$. (See [1, Lemma 1.33] for a proof,

and [21] for a generalization that includes disconnected quandles.) Therefore, to enumerate connected affine quandles with n elements up to isomorphism, it suffices to consider abelian groups of order n up to isomorphism, and for each group A all automorphisms $f \in \mathrm{Aut}(A)$ such that $1 - f$ is also an automorphism, up to conjugation in $\mathrm{Aut}(A)$.

Example 7.5. Let us enumerate connected affine quandles of prime size p. We can assume that $A = \mathbb{Z}_p$ and consider all $f \in \mathrm{Aut}(\mathbb{Z}_p) \simeq \mathbb{Z}_p^*$ such that $1 - f \neq 0$, that is, $f \neq 1$. Since $\mathrm{Aut}(\mathbb{Z}_p)$ is abelian, conjugacy plays no role, and we obtain $p - 2$ connected affine quandles with p elements.

An enumeration of small affine quandles has been achieved by Hou in [21]. It turns out that the function counting affine quandles of size n up to isomorphism is multiplicative (in the number-theoretic sense), hence one can focus on prime powers. Hou found explicit formulas for the number of affine quandles (and connected affine quandles) for any prime power p^k with $1 \leq k \leq 4$. See [21, equations (4.1) and (4.2)] for the formulas, [21, Table 1] for the complete list of affine quandles, and also the values $a(n)$ in our Table 1. For example, on p^2 elements, there are precisely $2p^2 - 3p - 1$ connected affine quandles, of which $p^2 - 2p$ are based on $A = \mathbb{Z}_{p^2}$ and $p^2 - p - 1$ on $A = \mathbb{Z}_p \times \mathbb{Z}_p$. As we shall see in Theorems 9.3 and 9.4, all connected quandles with p or p^2 elements are affine.

8. Enumerating small connected quandles

Suppose that we wish to enumerate all connected quandles of order n up to isomorphism. By Theorems 5.3 and 5.6, it suffices to fix a set Q of size n, an element $e \in Q$, and consider all quandle envelopes (G, ζ) on Q (with respect to e), where the transitive groups G are taken up to equivalence. The corresponding quandles $\mathcal{Q}(G, \zeta)$ then account for all connected quandles of order n up to isomorphism, possibly with repetitions.

Moreover, since $\mathcal{E}(\mathcal{Q}(G, \zeta)) = (G, \zeta)$ by Theorem 5.3, we see that $G = \mathrm{RMlt}(\mathcal{Q}(G, \zeta))$. Propositions 2.1 and 2.3 then imply that it suffices to consider transitive groups G for which G' is also transitive and G/G' is cyclic. This disqualifies many transitive groups. The conditions $\zeta \in Z(G_e)$ and $\langle \zeta^G \rangle = G$ disqualify many other transitive groups, for instance the symmetric groups in their natural actions.

Corollary 5.7 can be used to avoid isomorphic copies. But it appears to be computationally easier to allow isomorphic copies and to filter them later with a direct isomorphism check, rather than verifying whether ζ, ξ are conjugate in $N_{(S_Q)_e}(G)$.

Here is the resulting algorithm for a given size n.

Algorithm 8.1.

```
quandles ← ∅
for each G in the set of transitive groups on {1,...,n} up to equivalence do
   if G′ is transitive and G/G′ is cyclic then
      qG ← ∅
      for each ζ in Z(G_1) such that ⟨ ζ^G ⟩ = G do
         qG ← qG ∪ {Q(G, ζ)}
      qG ← qG filtered up to isomorphism
      quandles ← quandles ∪ qG
return quandles
```

We have implemented the algorithm in GAP [18]. The source code and the output of the search are available on the website of the third author. The isomorphism check is based on the methods of the LOOPS [33] package for GAP. The current version of GAP contains a library of transitive groups up to degree 30. An extension up to degree 47, except for degree 32, can be obtained from one of the authors [22]. The $2,801,324$ transitive groups of degree 32 can be obtained from Derek Holt [3]. On an Intel Core i5-2520M 2.5GHz processor, the search for all connected quandles of order $1 \leq n \leq 47$ with $n \neq 32$ takes only several minutes, and the order $n = 32$ takes about an hour.

In [41], Vendramin presented a similar algorithm, also based on a homogeneous representation, but he was not aware of Theorems 5.3 and 5.6. He therefore had to deal with many more transitive groups, filter out quandles that were not connected, and also filter more quandles up to isomorphism, resulting in a much longer computation time (on the order of weeks).

n	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
$q(n)$	1	0	1	1	3	2	5	3	8	1	9	10	11	0	7	9
$\ell(n)$	1	0	1	1	3	0	5	2	8	0	9	1	11	0	5	9
$a(n)$	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
$q(n)$	15	12	17	10	9	0	21	42	34	0	65	13	27	24	29	17
$\ell(n)$	15	0	17	3	7	0	21	2	34	0	62	7	27	0	29	8
$a(n)$	15	0	17	3	5	0	21	2	34	0	30	5	27	0	29	8

n	33	34	35	36	37	38	39	40	41	42	43	44	45	46	47
$q(n)$	11	0	15	73	35	0	13	33	39	26	41	9	45	0	45
$\ell(n)$	11	0	15	9	35	0	13	6	39	0	41	9	36	0	45
$a(n)$	9	0	15	8	35	0	11	6	39	0	41	9	24	0	45

TABLE 1. The numbers $q(n)$ of connected quandles, $\ell(n)$ of Latin quandles, and $a(n)$ of connected affine quandles of size $n \leq 47$ up to isomorphism.

Table 1 shows the numbers $q(n)$ of connected quandles, $\ell(n)$ of Latin quandles, and $a(n)$ of connected affine quandles of size $n \leq 47$ up to isomorphism. Latin quandles are recognized by a direct test whether all left translations are permutations. Affine quandles are recognized by checking whether G' is abelian, using Corollary 7.4. Note that Corollary 7.2 implies $a(n) \leq \ell(n) \leq q(n)$. As we shall see, $q(p) = a(p)$ and $q(p^2) = a(p^2)$ for every prime p (Theorems 9.3 and 9.4), and $q(2p) = 0$ for every prime $p > 5$ (Theorem 9.5). Stein's theorem [40, Theorem 9.9] forces $\ell(4k + 2) = 0$.

The numbers $q(n)$ agree with those calculated by Vendramin in [41], and the numbers $a(n)$ agree with the enumeration results of Hou [21], as discussed at the end of Section 7.

We conclude this section by providing examples of infinite sequences of connected quandles. The first source of examples is combinatorial, resulting from multi-transitivity of the symmetric and alternating groups.

Example 8.2. For $n \geq 2$ let $G = S_n$ act on 2-element subsets of $\{1, \ldots, n\}$, let $e = \{1, 2\}$ and $\zeta = (1, 2)$. Then $\zeta \in Z(G_e)$ and $\langle \zeta^G \rangle = G$, since all transpositions are conjugate to ζ in S_n. Thus $\mathcal{Q}(G, \zeta)$ is a connected quandle of order $\binom{n}{2}$.

Example 8.3. For $n \geq 2$ let $G = S_n$ act on n-cycles by conjugation, let $e = (1, \ldots, n)$ and $\zeta = (1, \ldots, n)$. Since the orbit of e consists of all n-cycles, we see that $|G_e| = n$ and $G_e = Z(G_e) = \langle \zeta \rangle$, so certainly $\zeta \in Z(G_e)$. Furthermore, $\langle \zeta^G \rangle$ generates S_n if n is even (and A_n if n is odd). Therefore, if n is even then $\mathcal{Q}(G, \zeta)$ is a connected quandle of order $(n-1)!$.

Example 8.4. For $n \geq 3$ let $G = S_n$ act on $(n-2)$-tuples of distinct elements pointwise, let e be the $(n-2)$-tuple $(1, \ldots, n-2)$, and let $\zeta = (n-1, n)$. Then we obviously have $G_e = Z(G_e) = \langle \zeta \rangle$, so $\zeta \in Z(G_e)$, and $\langle \zeta^G \rangle = G$. Thus $\mathcal{Q}(G, \zeta)$ is a connected quandle of order $n!/2$.

Example 8.5. For $n \geq 4$ let $G = A_n$ act on $(n-3)$-tuples of distinct elements pointwise, let e be the $(n-3)$-tuple $(1, \ldots, n-3)$, and let $\zeta = (n-2, n-1, n)$. Since $|G_e| = 6/2 = 3$ (because $G = A_n$, rather than $G = S_n$), we have $G_e = Z(G_e) = \langle \zeta \rangle$, so $\zeta \in Z(G_e)$. As A_n is generated by 3-cycles, we also have $\langle \zeta^G \rangle = G$. Thus $\mathcal{Q}(G, \zeta)$ is a connected quandle of order $n!/6$.

There are also geometric constructions, as illustrated by the following examples:

Example 8.6. For a prime power q, let $G = \mathrm{SL}_2(q)$ act (on the right) on Q, the set of all non-zero vectors in the plane $(\mathbb{F}_q)^2$. Let $e = (1, 0)$. A quick calculation shows that $G_e = \{M_a : a \in \mathbb{F}_q\}$, where $M_a = \left(\begin{smallmatrix} 1 & 0 \\ a & 1 \end{smallmatrix}\right)$. Let $\zeta = M_1$. Since $M_a M_b = M_{a+b}$, we have $G_e \simeq (\mathbb{F}_q, +)$, so $\zeta \in Z(G_e) = G_e$. We claim that $\langle \zeta^G \rangle = G$.

First, it is easy to check that M_a is conjugate to ζ in G if and only if a is a square in $\mathbb{F}_q$. If q is even then $\mathbb{F}_q^*$ has odd order and thus every element of $\mathbb{F}_q$ is a square, so $G_e \leq \langle \zeta^G \rangle$. When $q = p^k$ is odd then $\mathbb{F}_q^*$ contains $|\mathbb{F}_q^*|/2 = (q-1)/2$ squares, so $|G_e \cap \langle \zeta^G \rangle| \geq (q-1)/2 + 1 > q/2$, and Lagrange's Theorem then implies that $G_e \leq \langle \zeta^G \rangle$ again.

Since $G_e \leq \langle \zeta^G \rangle$, we establish $\langle \zeta^G \rangle = G$ by proving that $\langle \zeta^G \rangle$ acts transitively on Q. Given $(x, y) \in Q$ with $y \neq 0$, we have $(x, y) = eDM_{-y}D^{-1}$ with $D = \left(\begin{smallmatrix} 0 & 1 \\ -1 & d \end{smallmatrix}\right)$, $d = (1-x)y^{-1}$. In particular, $(0, 1) \in e^{\langle \zeta^G \rangle}$, and given $(x, 0) \in Q$, we obtain $(x, 0) = (0, 1)EM_xE^{-1}$ with $E = \left(\begin{smallmatrix} 1 & x^{-1} \\ 0 & 1 \end{smallmatrix}\right)$. Hence $\langle \zeta^G \rangle = G$, and thus $\mathcal{Q}(G, \zeta)$ is a connected quandle of order $q^2 - 1$.

Example 8.7. For a prime power q, let $G = \mathrm{PSL}_3(q)$ act on Q, the set of all two-element subsets of the projective plane $\mathbb{P}^2(\mathbb{F}_q)$. This is a transitive action, because the natural action of G on $\mathbb{P}^2(\mathbb{F}_q)$ is 2-transitive. Pick a two-element subset $e = \{e_1, e_2\}$ arbitrarily, and consider matrices with respect to the basis (e_1, e_2, e_3), with an arbitrary completion by e_3. Clearly, $G_e = \{M_{a,b}, N_{a,b} : a, b \in \mathbb{F}_q\}$, where

$$M_{a,b} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ a & b & 1 \end{pmatrix}, \qquad N_{a,b} = \begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ a & b & -1 \end{pmatrix}.$$

A quick calculation shows that $\zeta = M_{a,-a} \in Z(G_e)$ for every $a \in \mathbb{F}_q$. Since G is a simple group, we obtain for free that the normal subgroup $\langle \zeta^G \rangle$ is equal to G (unless $a = 0$). Thus $\mathcal{Q}(G, \zeta)$ is a connected quandle of order $|Q| = (q^2 + q + 1)(q^2 + q)/2$.

Example 8.8. The group G of rotations of a Platonic solid (see [9, p.136]) acts on faces. Let e be a face.

- Tetrahedron: We have $G = A_4$ acting on 4 points (faces), and with ζ a generator of $G_e \simeq \mathbb{Z}_3$ we get $\langle \zeta^G \rangle = G$. Thus $\mathcal{Q}(G, \zeta)$ is a connected quandle of order 4. Since A_4 is metabelian, Theorem 7.3 implies that $\mathcal{Q}(G, \zeta)$ is affine.
- Cube: We have $G = S_4$ acting on 6 points, and with ζ a generator of $G_e \simeq \mathbb{Z}_4$ we get $\langle \zeta^G \rangle = G$. Thus $\mathcal{Q}(G, \zeta)$ is a connected quandle of order 6.
- Octahedron: We have $G = S_4$ acting on 8 points, and $G_e \simeq \mathbb{Z}_3$. Since 3-cycles do not generate S_4, no choice of $\zeta \in G_e$ yields a connected quandle $\mathcal{Q}(G, \zeta)$.
- Dodecahedron: We have $G = A_5$ acting on 12 points, and with ζ a generator of $G_e \simeq \mathbb{Z}_5$ we get $\langle \zeta^G \rangle = G$. Thus $\mathcal{Q}(G, \zeta)$ is a connected quandle of order 12.
- Icosahedron: We obtain $G = A_5$ acting on 20 points, and with ζ a generator of $G_e \simeq \mathbb{Z}_3$ we get $\langle \zeta^G \rangle = G$. Thus $\mathcal{Q}(G, \zeta)$ is a connected quandle of order 20.

There are algebraic constructions where the quandle envelope is not obvious. For example, the following construction of connected quandles of size $3n$, extending an affine quandle $\mathcal{Q}_{\mathrm{Aff}}(A, -1)$ by $\mathcal{Q}_{\mathrm{Aff}}(\mathbb{Z}_3, -1)$, presented by Clark et al. [7], inspired by Galkin [16].

Example 8.9. Let A be an abelian group and $u \in A$. We define $\mu, \tau : \mathbb{Z}_3 \to A$ by $0^\mu = 2$, $1^\mu = 2^\mu = -1$ and $0^\tau = 1^\tau = 0$, $2^\tau = u$, and we define a binary operation on $\mathbb{Z}_3 \times A$ by

$$(x, a) \circ (y, b) = (-x - y, -a + (x - y)^\mu b + (x - y)^\tau).$$

Then $\mathcal{Q}_{\mathrm{Gal}}(A, u) = (\mathbb{Z}_3 \times A, \circ)$ is a connected quandle, called the *Galkin quandle corresponding to the pointed group* (A, u). It is affine iff $3A = 0$. It is Latin iff $|A|$ is odd. Two Galkin quandles are isomorphic iff the corresponding pointed groups are isomorphic. See [7] for details.

Table 2 lists all connected non-affine quandles of orders $n \leq 15$ and $n \in \{21, 33\}$. In the column labeled "construction" we either give a reference to a numbered example which uniquely determines the quandle, or we specify how the quandle can be constructed as $\mathcal{Q}_{\mathrm{Hom}}(G, H, f)$ of Construction 3.1, or we specify how the quandle can be constructed as $\mathcal{Q}_{\mathrm{Gal}}(A, u)$ of Example 8.9.

Problem 8.10. *Let $p \geq 11$ be a prime. Is it true that the only non-affine connected quandles of order $3p$ are the Galkin quandles $\mathcal{Q}_{\mathrm{Gal}}(\mathbb{Z}_p, 0)$ and $\mathcal{Q}_{\mathrm{Gal}}(\mathbb{Z}_p, 1)$?*

9. Connected quandles of order p, p^2 and $2p$

First, we will show that connected quandles of prime power order have a solvable right multiplication group, using a deep result on conjugacy classes of prime power size by Kazarin [26]. Based on that, we give two new, conceptually simple proofs that connected quandles of prime order are affine: the first argument uses an observation about $\mathrm{RMlt}(Q)$ of simple quandles, the second one requires Galois' result on solvable primitive groups. The original proof of Etingof, Soloviev and Guralnick [13] relies on a group-theoretical result equivalent to the one of Kazarin, too.

Then we mention the result of Graña [19] that connected quandles of prime square order are affine, and conclude with a new, shorter and purely group-theoretical proof (modulo Theorem 5.3) of the recent result of McCarron [32] that there are no connected quandles of order $2p$ with $p > 5$ prime.

size	RMlt(Q)	construction	properties
6	S_4	8.2 or $\mathcal{Q}_{\mathrm{Gal}}(\mathbb{Z}_2, 0)$	
6	S_4	8.3 or 8.8 or $\mathcal{Q}_{\mathrm{Gal}}(\mathbb{Z}_2, 1)$	
8	$\mathrm{SL}_2(3)$	8.6	
10	S_5	8.2	simple
12	S_4	8.4	
12	A_5	8.8	simple
12	$A_4 \rtimes \mathbb{Z}_4$	$\mathcal{Q}_{\mathrm{Hom}}(A_4, 1, (1,2,3,4))$	
12	$(\mathbb{Z}_3^2 \rtimes Q_8) \rtimes \mathbb{Z}_3$		
12	$(\mathbb{Z}_4^2 \rtimes \mathbb{Z}_3) \rtimes \mathbb{Z}_2$	$\mathcal{Q}_{\mathrm{Gal}}(\mathbb{Z}_4, 0)$	
12	$(\mathbb{Z}_4^2 \rtimes \mathbb{Z}_3) \rtimes \mathbb{Z}_2$	$\mathcal{Q}_{\mathrm{Gal}}(\mathbb{Z}_4, 1)$	
12	$(\mathbb{Z}_4^2 \rtimes \mathbb{Z}_3) \rtimes \mathbb{Z}_2$	$\mathcal{Q}_{\mathrm{Gal}}(\mathbb{Z}_4, 2)$	
12	$(\mathbb{Z}_2^4 \rtimes \mathbb{Z}_3) \rtimes \mathbb{Z}_2$	$\mathcal{Q}_{\mathrm{Gal}}(\mathbb{Z}_2^2, (0,0))$	
12	$(\mathbb{Z}_2^4 \rtimes \mathbb{Z}_3) \rtimes \mathbb{Z}_2$	$\mathcal{Q}_{\mathrm{Gal}}(\mathbb{Z}_2^2, (1,1))$	
15	$(\mathbb{Z}_5^2 \rtimes \mathbb{Z}_3) \rtimes \mathbb{Z}_2$	$\mathcal{Q}_{\mathrm{Gal}}(\mathbb{Z}_5, 0)$	Latin
15	$(\mathbb{Z}_5^2 \rtimes \mathbb{Z}_3) \rtimes \mathbb{Z}_2$	$\mathcal{Q}_{\mathrm{Gal}}(\mathbb{Z}_5, 1)$	Latin
15	S_6	8.2	simple
15	$\mathrm{SL}_2(4)$	8.6	simple
⋮			
21	$(\mathbb{Z}_7^2 \rtimes \mathbb{Z}_3) \rtimes \mathbb{Z}_2$	$\mathcal{Q}_{\mathrm{Gal}}(\mathbb{Z}_7, 0)$	Latin
21	$(\mathbb{Z}_7^2 \rtimes \mathbb{Z}_3) \rtimes \mathbb{Z}_2$	$\mathcal{Q}_{\mathrm{Gal}}(\mathbb{Z}_7, 1)$	Latin
21	S_7	8.2	simple
21	$\mathrm{PSL}_3(2)$	8.7	simple
⋮			
33	$(\mathbb{Z}_{11}^2 \rtimes \mathbb{Z}_3) \rtimes \mathbb{Z}_2$	$\mathcal{Q}_{\mathrm{Gal}}(\mathbb{Z}_{11}, 0)$	Latin
33	$(\mathbb{Z}_{11}^2 \rtimes \mathbb{Z}_3) \rtimes \mathbb{Z}_2$	$\mathcal{Q}_{\mathrm{Gal}}(\mathbb{Z}_{11}, 1)$	Latin

TABLE 2. All connected non-affine quandles of certain orders.

Lemma 9.1 ([1, Lemma 1.29])**.** *Let Q be a connected rack. For $a, b \in Q$ let $a \sim b$ iff $R_a = R_b$. Then $\sim$ is an equivalence relation on Q, and all equivalence classes of $\sim$ have the same size.*

Proof. It is clear that $\sim$ is an equivalence relation. Let $[a]$, $[c]$ be two equivalence classes of $\sim$. Since Q is connected, there is $\theta \in \mathrm{RMlt}(Q)$ such that $a^\theta = c$. If $a \sim b$ then $R_c = R_{a^\theta} = R_a^\theta = R_b^\theta = R_{b^\theta}$, thus $c \sim b^\theta$, showing that $[a]^\theta \subseteq [c]$. Since θ is one-to-one, we deduce $|[a]| \leq |[c]|$. The mapping $\theta^{-1} \in \mathrm{RMlt}(Q)$ gives the other inequality. □

Proposition 9.2. *Let Q be a connected quandle of prime power order. Then* RMlt(Q) *is a solvable group.*

Proof. Kazarin proved in [26] that in a group G, if $x \in G$ is such that $|x^G|$ is a prime power, then the subgroup $\langle\, x^G \,\rangle$ is solvable.

Let Q be a connected quandle of prime power order, let $G = \mathrm{RMlt}(Q)$ and $\zeta = R_e$ for any $e \in Q$. Note that $\zeta^G = \{R_x : x \in Q\}$. By Lemma 9.1, $|\zeta^G|$ is a divisor of $|Q|$, hence a prime power. Kazarin's result then implies that $\langle\, \zeta^G \,\rangle = G$ is solvable. □

Recall that a quandle Q is *simple* if all its congruences are trivial.

Theorem 9.3 ([13])**.** *Every connected quandle of prime order is affine.*

Proof. Let Q be the quandle in question. By Proposition 9.2, $G = \mathrm{RMlt}(Q)$ is solvable. Moreover, since G acts transitively on a set of prime size, it must act primitively.

Proof 1. Consequently, the quandle Q is simple, because every congruence of Q is invariant under the action of G. An observation by Joyce [25, Proposition 3] says that if Q is simple then G' is the smallest nontrivial normal subgroup in G. Since G is solvable, we then must have $G'' = 1$, hence G' is abelian, and so Q is affine by Theorem 7.3.

Proof 2. A theorem of Galois says that a solvable primitive group acts as a subgroup of the affine group over a finite field. Theorem 7.3 now concludes the proof. □

An analogous statement holds for prime square orders, but the reason seems to be more complicated. Graña's proof relies on an examination of several cases of the right multiplication group of a potential counterexample.

Theorem 9.4 ([19])**.** *Every connected quandle of prime square order is affine.*

We now turn our attention to order $2p$. For every integer $n \geq 2$, Example 8.2 yields a connected quandle of order $\binom{n}{2}$. With $n = 4$ and $n = 5$ we obtain connected quandles of order $6 = 2 \cdot 3$ and $10 = 2 \cdot 5$, respectively. These examples are sporadic in the sense that $\binom{n}{2}$ is equal to $2p$ for a prime p if and only if $n \in \{4, 5\}$.

Theorem 9.5 ([32])**.** *There is no connected quandle of order $2p$ for a prime $p > 5$.*

We conclude the paper with a new proof of Theorem 9.5. Suppose that Q is a connected quandle of order $2p$. Then $G = \mathrm{RMlt}(Q) \leq S_{2p}$, G' acts transitively on Q by Proposition 2.3, and $\langle\, \zeta^G \,\rangle = G$ for some $\zeta \in Z(G_e)$ by Theorem 5.3, so, in particular, $\langle\, Z(G_e)^G \,\rangle = G$. Theorem 9.5 therefore follows from the group-theoretical Theorem 10.1 below that we prove separately.

10. A result on transitive groups of degree $2p$

Theorem 10.1. *Let $p > 5$ be a prime. There is no transitive group $G \leq S_{2p}$ satisfying both of the following conditions:*

(A) *G' is transitive on $\{1, \ldots, 2p\}$.*
(B) *$\langle\, Z(G_1)^G \,\rangle = G$.*

We start with two general results on the center of the stabilizer of almost simple primitive groups of degree p and $2p$. Both proofs are based on the explicit classification of almost simple primitive groups of degree p and $2p$ [37] (which are essentially results from [20, 29]). In the next subsection, we prove Theorem 10.1.

We will use repeatedly the easy fact that a nontrivial normal subgroup of a transitive group does not have fixed points.

10.1. Almost simple primitive groups of degree p, $2p$.

Theorem 10.2. *Let $p \geq 5$ be a prime, $G \leq S_p$ an almost simple primitive group, $U = G_1$ and $V \leq U$ with $[U : V] \leq 2$. Then $Z(V) = \langle\, 1 \,\rangle$.*

An explicit classification of these groups is given in [37, Lemma 3.1]:

Lemma 10.3. *Let p be a prime and $G \leq S_p$ be an almost simple primitive group. Then $K = \mathrm{Soc}(G)$ is one of the following groups:*

(i) $K = A_p$,
(ii) $K = \mathrm{PSL}_d(q)$ *acting on 1-spaces or hyperplanes of its natural projective space, d is a prime and $p = (q^d - 1)/(q - 1)$,*
(iii) $K = \mathrm{PSL}_2(11)$ *acting on cosets of A_5,*
(iv) $K = M_{23}$ *or* $K = M_{11}$.

For case (ii) we note the following fact:

Lemma 10.4. *Let $d \geq 2$ and q be a prime power such that $(d, q) \neq (2, 2)$. Let $G = \mathrm{Aut}(\mathrm{PSL}_d(q))$, U be the stabilizer in G of a 1-dimensional subspace, $W = U \cap \mathrm{PSL}_d(q)$ and $V \leq W$ with $[W : V] \leq 2$. Then $C_U(V) = \langle 1 \rangle$.*

Proof. Since the graph automorphism of $\mathrm{PSL}_d(q)$ swaps the stabilizers of 1-dimensional subspaces with those of hyperspaces it cannot be induced by U. Thus $U \leq \mathrm{P\Gamma L}_d(q)$ and elements of U can be represented by pairs [field automorphism, matrix] of the form

$$\left[\tau, \begin{pmatrix} a & 0 \\ B & A \end{pmatrix}\right]$$

with $a \in \mathbb{F}_q^*$, $B \in \mathbb{F}_q^{d-1}$ and $A \in \mathrm{GL}_{d-1}(q)$ and $\tau \in \langle \sigma \rangle$. Two such elements multiply as

$$\left[\tau_1, \begin{pmatrix} a_1 & 0 \\ B_1 & A_1 \end{pmatrix}\right] \cdot \left[\tau_2, \begin{pmatrix} a_2 & 0 \\ B_2 & A_2 \end{pmatrix}\right] = \left[\tau_1\tau_2, \begin{pmatrix} a_1a_2 & 0 \\ B_1^{\tau_2} + A_1^{\tau_2}B_2 & A_1^{\tau_2}A_2 \end{pmatrix}\right]$$

Elements of W will have a trivial field automorphism part and $a \cdot \det(A) = 1$, thus the A-part includes all of $\mathrm{SL}_{d-1}(q)$. If $V \neq W$ we have $V \lhd W$ of index 2, so it has a smaller A-part. (If it had a smaller B-part, this would have to be a submodule for the natural $\mathrm{SL}_{d-1}(q)$-module which is irreducible.) The A-part cannot be smaller if $d - 1 \geq 3$, or if $d - 1 = 2$ and $q \geq 4$.

In the remaining cases ($d - 1 = 2$ and $q \in \{2, 3\}$; respectively $d - 1 = 1$) the A-part can be smaller by index 2. However we note by inspection that there is no B-part that is fixed by all A-parts by multiplication.

We now consider a pair of elements, the second being in V and the first being in $C_U(V)$. By the multiplication formula the elements commute only if $B_1^{\tau_2} + A_1^{\tau_2}B_2 = B_2^{\tau_1} + A_2^{\tau_1}B_1$. We will select elements of V suitably to impose restrictions on $C_U(V)$.

If A_1 is not the identity we can set A_2 as identity, B_2 a vector defined over the prime field moved by A_1, and $\tau_2 = 1$ violating the equality. Similarly, if B_1 is nonzero (with trivial A_1) we can chose B_2 to be zero, $\tau_2 = 1$ and A_2 a matrix defined over the prime field that moves B_1 (we noted above such matrices always exist in V) to violate the equality. Finally, if B_1 is zero and A_1 the identity but τ_1 nontrivial we can chose τ_2 to be trivial and B_2 a vector moved by τ_1 and violate the equation. This shows that the only element of U commuting with all of V is the identity. □

Corollary 10.5. *Let $\mathrm{PSL}_d(q) \leq G \leq \mathrm{Aut}(\mathrm{PSL}_d(q))$, U be the stabilizer in G of a 1-dimensional subspace, and $W \leq U$ with $[U : W] \leq 2$. Then $Z(W) = \langle 1 \rangle$.*

Proof. As subgroups of index 2 are normal we know that there exists a subgroup $V \leq W$ as specified in Lemma 10.4. But then by this lemma

$$Z(W) \leq C_W(V) \leq C_{\mathrm{Aut}(PSL_d(q))_{\mathrm{subspace}}}(V) = \langle 1 \rangle.$$

□

Proof of Theorem 10.2. For case (i) of Lemma 10.3, we have that $U \in \{S_{p-1},\ A_{p-1}\}$ and so also $V \in \{S_{p-1},\ A_{p-1}\}$, thus (as $p \geq 5$) clearly $Z(V) = \langle 1 \rangle$. For case (ii) we get from Corollary 10.5 that $Z(V) = \langle 1 \rangle$. Finally for the groups in cases (iii) and (iv) an explicit calculation in GAP (as U/V is abelian we can find all candidates for V by calculating in U/U') establishes the result. □

Now we turn to the case $2p$.

Theorem 10.6. *Let $p > 5$ be a prime and $G \leq S_{2p}$ a primitive group. Then $Z(G_1) = \langle 1 \rangle$.*

By the O'Nan-Scott theorem [28], G must be almost simple. An explicit classification of these groups is given in [37, Theorem 4.6].

Lemma 10.7. *Let p be a prime and $G \leq S_{2p}$ be a primitive group. Then $K = \mathrm{Soc}(G)$ is one of the following groups:*

(i) $K = A_{2p}$,
(ii) $p = 5$, $K = A_5$ *acting on 2-sets,*
(iii) $2p = q + 1$, $q = r^{2^a}$ *for an odd prime r,* $K = \mathrm{PSL}_2(q)$ *acting on 1-spaces,*
(iv) $p = 11$, $K = M_{22}$.

Proof of Theorem 10.6. In case (i) of Lemma 10.7 we have that $G \in \{S_{2p}, A_{2p}\}$ and thus $G_1 \in \{S_{2p-1}, A_{2p-1}\}$ for which the statement is clearly true. Case (ii) is irrelevant here as $p = 5$. Case (iii) follows from Corollary 10.5. Case (iv) is again done with an explicit calculation in GAP. □

10.2. **Proof of Theorem 10.1.** We start by discussion what block systems are afforded by G.

Lemma 10.8. *If G is primitive, then condition* (B) *is violated.*

Proof. This is a direct consequence of Theorem 10.6. □

Lemma 10.9. *If G affords a block system with blocks of size p, then condition* (A) *is violated.*

Proof. Consider a block system with two blocks of size p and $\varphi\colon G \to S_2$ the action on these blocks. Then $[G : \mathrm{Ker}(\varphi)] = 2$, and thus $G' \leq \mathrm{Ker}(\varphi)$ is clearly intransitive. □

So it remains to check the case when G has p blocks of size 2. Denote the set of blocks by $\mathcal{B}$, let $1 \in B \in \mathcal{B}$. Labeling points suitably, we can assume that $B = \{1, 2\}$. Let $S = G_1$ be a point stabilizer and $T = G_B$ a (setwise) block stabilizer.

Let $\varphi\colon G \to S_p$ be the action on the blocks. We set $H = \mathrm{Im}(\varphi) \leq S_p$ and $M = \mathrm{Ker}(\varphi)$ and note that $M \leq C_2^p$ is either trivial or has exactly p orbits of length 2.

Lemma 10.10. *If $M \neq \langle 1 \rangle$ then $T = MS$.*

Proof. If $M \neq \langle 1 \rangle$, then M has orbits of length 2. Consider $t \in T$. If $1^t \neq 1$ then $1^t = 2$ is in the same M-orbit. Thus there exists $m \in M$ such that $1^t = 1^m$, thus $tm^{-1} \in S$. □

As p is a prime, H is a primitive group. By the O'Nan-Scott theorem [28], we know that H is either of affine type or almost simple.

Lemma 10.11. *If H is almost simple, then condition* (B) *is violated.*

Proof. If $M \neq \langle 1 \rangle$ then by Lemma 10.10 $S^\varphi = T^\varphi = H_1$. But then $Z(S)^\varphi \leq Z(H_1) = \langle 1 \rangle$ by Theorem 10.6. Thus $Z(S) \leq \mathrm{Ker}(\varphi) \lhd G$ and $\langle Z(S)^G \rangle \neq G$.

If $M = \langle 1 \rangle$ then φ is faithful and $G \simeq H$. The point stabilizer $S \leq G$ is (isomorphic to) a subgroup of the point stabilizer of H of index 2. But then by Theorem 10.2 we have that $Z(S) = \langle 1 \rangle$ and thus $\langle Z(S)^G \rangle \neq G$. □

It remains to consider the affine case, i.e. $H \leq \mathbb{F}_p \rtimes \mathbb{F}_p^*$. We can label the p points on which H acts as $0, \ldots, p-1$, then the action of the $\mathbb{F}_p$-part is by addition, and that of the $\mathbb{F}_p^*$-part by multiplication modulo p. Without loss of generality assume that $T^\varphi = H_1$. We may also assume that H is not cyclic as otherwise $H' = \langle 1 \rangle$ and thus $G' \leq M$ and condition (A) would be violated.

For $p = 7$ an inspection of the list of transitive groups of degree 14 [8] shows that there is no group of degree 14 which fulfills (A) and (B). Thus it remains to consider $p > 7$.

Let $L = S \cap M = M_1$.

Lemma 10.12. *If $|L| \leq 2$ and $p > 7$ then condition* (A) *is violated.*

Proof. If $|L| \leq 2$ then $|M| \leq 4$ and $|G|$ divides $4p(p-1)$. Consider the number n of p-Sylow subgroups of G. Then $n \equiv 1 \pmod p$ and n divides $4(p-1)$. Thus $n = ap + 1$ with $a \in \{0, 1, 2, 3\}$ and $b(ap+1) = 4(p-1)$. If $a \neq 0$ this implies that $b \in \{1, 2, 3, 4\}$. Trying out all combinations (a, b) we see that there is no solution for $a > 0$, $p > 7$.

So $n = 1$. But a normal p-Sylow subgroup must have two orbits of length p, which as orbits of a normal subgroup form a block system for G. The result follows by Lemma 10.9. □

This in particular implies that we can assume that $M \neq \langle 1 \rangle$, thus by Lemma 10.10 we have that $S^\varphi = H_1 \leq \mathbb{F}_p^*$. Thus there exists $b \in S$ such that $H_1 = \langle b^\varphi \rangle$.

Lemma 10.13. $S = \langle b \rangle \cdot L$.

Proof. Clearly $S \geq \langle b \rangle \cdot L$. Consider $s \in S$. Then $s^\varphi \in H_1$, thus $s^\varphi = (b^\varphi)^x$ for a suitable x and thus $sb^{-x} \in \mathrm{Ker}(\varphi) \cap S = L$. □

We shall need a technical lemma about finite fields. For $\beta \in \mathbb{F}_p^*$, a subset $I \subset \mathbb{F}_p$ is called *β-closed* if $I\beta = I$, that is $x \in I$ iff $x\beta \in I$.

Lemma 10.14. *Let $\alpha, \beta \in \mathbb{F}_p^*$, $\beta \neq 1$ and assume that $\emptyset \neq I \subset \mathbb{F}_p^*$ is β-closed. Then $I - \alpha = \{i - \alpha \mid i \in I\}$ is not β-closed.*

Proof. Assume that $I - \alpha$ is β-closed and consider an arbitrary $x \in I$. Then (as β has a finite multiplicative order) $x\beta^{-1} \in I$ and thus $x\beta^{-1} - \alpha \in I - \alpha$. But by the assumption $(x\beta^{-1} - \alpha)\beta \in I - \alpha$ and thus $(x\beta^{-1} - \alpha)\beta + \alpha = x + \alpha(1 - \beta) \in I$. Thus I would be closed under addition of $\alpha(1-\beta) \neq 0$. But the additive order of a nonzero element in $\mathbb{F}_p$ is p, implying that $I = \mathbb{F}_p$, contradicting that $0 \notin I$. □

Lemma 10.15. *If condition* (A) *holds, then $Z(S) \leq L \leq M$.*

Proof. Assume the condition holds. We show the stronger statement that $C_S(L) \leq L$. For this assume to the contrary that $b^x \cdot l \in C_S(L)$ with $l \in L$ and x a suitable exponent such that $b^x \notin L$. As $L \leq M$ is abelian this implies that $b^x \in C_S(L)$. Let $\beta \in \mathbb{F}_p^* \leq H$ be such that $(b^x)^\varphi = \beta$. As $b^x \notin L$ we know that $\beta \neq 1$.

When we consider the conjugation action of G on $M \leq C_2^p$, note that an element of M is determined uniquely by its support (that is the blocks in $\mathcal{B}$ whose points are moved by the

element), which we consider as a subset of $\mathbb{F}_p$, which is the domain on which H acts. An element $g \in G$ acts by conjugation on M with the effect of moving the support of elements in the same way as g^φ moves the points $\mathbb{F}_p$. For b^x to centralize an element $a \in L$, the support I of a thus must be β-closed for $\beta = (b^x)^\varphi$.

By Lemma 10.12 we can assume that $|L| > 2$. Thus there exists an element $a \in L$ whose support I is a proper nonempty subset of $\mathbb{F}_p^*$. Thus there exists $\alpha \in \mathbb{F}_p^*$, $\alpha \notin I$.

That means that if we conjugate a with $-\alpha \in \mathbb{F}_p$, the resulting element $\tilde{a}$ has support $I - \alpha$. By assumption $0 \notin I - \alpha$, so $\tilde{a} \in L$. But by Lemma 10.14 we know that $I - \alpha$ is not β-closed, that is $\tilde{a} \in L$ is not centralized by b^x. □

Corollary 10.16. *If H is of affine type, then at least one of conditions* (A), (B) *is violated.*

Proof. If (A) holds, then $\langle\, Z(G_1)^G \,\rangle \leq M \neq G$. □

This concludes the proof of Theorem 10.1.

ACKNOWLEDGMENT

We thank Derek Holt for the library of transitive groups of degree 32. We also thank an anonymous referee for a number of useful comments, particularly regarding the presentation of older results.

References

[1] N. Andruskiewitsch and M. Graña, *From racks to pointed Hopf algebras*, Adv. Math. **178** (2003), no. **2**, 177–243.

[2] R.H. Bruck, *A survey of binary systems*, Ergebnisse der Mathematik und ihrer Grenzgebiete, Springer Verlag, Berlin-Göttingen-Heidelberg, 1958.

[3] J.J. Cannon and D.F. Holt, *The transitive permutation groups of degree 32*, Experiment. Math. **17** (2008), no. **3**, 307–314.

[4] 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.

[5] J.S. Carter, D. Jelsovsky, S. Kamada, L. Langford, and M. Saito, *Quandle cohomology and state-sum invariants of knotted curves and surfaces*, Trans. Amer. Math. Soc. **355** (2003), no. **10**, 3947-3989.

[6] W.E. Clark, M. Elhamdadi, M. Saito and T. Yeatman, *Quandle colorings of knots and applications.* J. Knot Theory Ramifications **23** (2014), no. **6**, 1450035.

[7] W.E. Clark, M. Elhamdadi, X. Hou, M. Saito and T. Yeatman, *Connected quandles associated with pointed abelian groups*, Pacific J. Math. **264** (2013), no. **1**, 31–60.

[8] J.H. Conway, A. Hulpke, and J. McKay, *On transitive permutation groups*, LMS J. Comput. Math. **1** (1998), 1–8.

[9] H.S.M. Coxeter, *Regular Polytopes*, Courier Dover Publications, New York, 1973

[10] V.G. Drinfeld, *On some unsolved problems in quantum group theory*, in Quantum Groups (Leningrad, 1990), Lecture Notes in Math. **1510**, Springer-Verlag, Berlin, 1992, 1–8.

[11] G. Ehrman, A. Gurpinar, M. Thibault and D.N. Yetter, *Toward a classification of finite quandles*, J. Knot Theory Ramifications **17** (2008), no. **4**, 511–520.

[12] M. Eisermann, *Yang-Baxter deformations of quandles and racks*, Algebr. Geom. Topol. **5** (2005), 537–562.

[13] P. Etingof, A. Soloviev and R. Guralnick, *Indecomposable set-theoretical solutions to the quantum Yang-Baxter equation on a set with a prime number of elements*, J. Algebra **242** (2001), no. **2**, 709–719.

[14] 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.

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

[16] V.M. Galkin, *Left distributive quasigroups of small orders*, preprint VINITI No. 6510-84, Gor'kovskiy politechnicheskiy tekhnicheskiy institut, Gorkiy (1984) (Russian).
[17] V.M. Galkin, *Quasigroups*, Itogi nauki i tekhniki **26** (1988), 3–44 (Russian). Translated in J. Soviet Math. **49** (1990), no. **3**, 941–967.
[18] The GAP Group, GAP – Groups, Algorithms, and Programming, Version 4.6.3; 2013. `http://www.gap-system.org`.
[19] M. Graña, *Indecomposable racks of order p^2*, Beiträge Algebra Geom. **45** (2004), no. **2**, 665–676.
[20] R.M. Guralnick, *Subgroups of prime power index in a simple group*, J. Algebra **81** (1983), no. **2**, 304–311.
[21] X. Hou, *Finite modules over $\mathbb{Z}[t, t^{-1}]$*, J. Knot Theory Ramifications **21** (2012), no. **8**, 1250079, 28 pp.
[22] A. Hulpke, *Constructing transitive permutation groups*, J. Symbolic Comput. **39** (2005), no. **1** (2001), 1–30.
[23] P. Jedlička, A. Pilitowska, D. Stanovský and A. Zamojska-Dzienio, *The structure of medial quandles*, to appear in J. Algebra.
[24] D. Joyce, *A classifying invariant of knots, the knot quandle*, J. Pure Appl. Alg. **23** (1982), 37–66.
[25] D. Joyce, *Simple quandles*, J. Algebra **79** (1982), 307–318.
[26] L.S. Kazarin, *Burnside's p^α-lemma*, Mat. Zametki **48** (1990), 45–48, 158 [in Russian]; translation in Math. Notes **48** (1990), 749–751.
[27] M. Kikkawa, *Kikkawa loops and homogeneous loops*, Commentat. Math. Univ. Carol. **45** (2004), no. **2**, 279–285.
[28] M.W. Liebeck, C.E. Praeger, and J. Saxl, *On the O'Nan-Scott theorem for finite primitive permutation groups*, J. Austral. Math. Soc. Ser. A **44** (1988), 389–396.
[29] M.W. Liebeck and J.Saxl, *Primitive permutation groups containing an element of large prime order*, J. London Math. Soc. (2) **31** (1985), no. **2**, 237–249.
[30] O. Loos, *Symmetric spaces*, J. Benjamin New York, 1969.
[31] S.V. Matveev, *Distributive groupoids in knot theory*, Math. USSR - Sbornik **47/1** (1984), 73–83.
[32] J. McCarron, *Connected quandles with order equal to twice an odd prime*, `http://arxiv.org/abs/1210.2150`.
[33] G.P. Nagy and P. Vojtěchovský, *Loops: Computing with quasigroups and loops in GAP*, version 2.2.0, available at `http://www.math.du.edu/loops`
[34] S. Nelson, C.-Y. Wong, *On the orbit decomposition of finite quandles*, J. Knot Theory Ramifications **15** (2006), no. **6**, 761–772.
[35] N. Nobusawa, *On symmetric structures of a finite set*, Osaka J. Math. **11** (1974), 569–575.
[36] R.S. Pierce, *Symmetric groupoids*, Osaka J. Math. **15/1** (1978), 51–76.
[37] J. Shareshian, *On the Möbius number of the subgroup lattice of the symmetric group*, J. Combin. Theory Ser. A **78** (1997), no. **2**, 236–267.
[38] D. Stanovský, *A guide to self-distributive quasigroups, or latin quandles*, Quasigroups and Related Systems **23/1** (2015), 91–128.
[39] D. Stanovský, *The origins of involutory quandles*, arxiv, 2015.
[40] S.K. Stein, *On the foundations of quasigroups*. Trans. Amer. Math. Soc. **85** (1957), 228–256.
[41] L. Vendramin, *On the classification of quandles of low order*, J. Knot Theory Ramifications **21** (2012), no. **9**, 1250088, 10 pp.

(Hulpke) Department of Mathematics, Colorado State University, 1874 Campus Delivery, Ft. Collins, Colorado 80523, U.S.A.

(Stanovský) Department of Algebra, Faculty of Mathematics and Physics, Charles University, Sokolovská 83, Praha 8, 18675, Czech Republic

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

E-mail address, Hulpke: `hulpke@math.colostate.edu`
E-mail address, Stanovský: `stanovsk@karlin.mff.cuni.cz`
E-mail address, Vojtěchovský: `petr@math.du.edu`