Bonatto, M.
Osaka J. Math.
59 (2022), 145–175

CONNECTED QUANDLES OF SIZE pq AND $4p$

Marco BONATTO

(Received August 19, 2019, revised November 3, 2020)

Abstract

We classify all non-simple connected quandles of size pq and $4p$ where p, q are primes, as a special family of locally strictly simple quandles (i.e. quandles for which all proper subquandles are strictly simple). In particular, we classify all latin quandles of size pq and $4p$ and we show that latin quandles of size $8p$ are affine.

Introduction

Quandles are binary algebraic structures related to knot invariants [18, 20] and they provide a special class of solutions to the set-theoretical quantum Yang-Baxter equation [12, 13].

Quandles have been studied using both group and module theory and in a recent paper [5] we developed a universal algebraic approach, in particular towards the connection between the properties of the *displacement group* and its subgroups and properties of congruences as *abelianness* and *centrality* in the sense of commutator theory [14].

In [4] the class of finite *strictly simple quandles*, i.e. quandles with no proper subquandles has been investigated and it has been proved that it coincides with the class of simple abelian quandles (in the sense of [5, 14]). They can be described using affine representations over finite fields and their lattice of subquandles containing a given element is the two elements lattice, i.e. it has height one (the height of a lattice is the maximal length of the chains of the lattice minus one). In this paper we are studying finite quandles such that every proper subquandle is strictly simple and we call them *locally strictly simple* (LSS) quandles. Equivalently LSS quandles are quandles for which the height of the lattice of subquandles containing a given element is at most two. Strictly simple quandles are examples of LSS quandles, but there exist other examples as non-simple quandles of size 28 of the RIG database of GAP [19].

Connected quandles of size p [13], p^2 [15], and the *affine* ones of size p^3 and p^4 [16] where p is a prime have been classified. All such quandles are affine and the first class of non-affine quandles which has been classified is the class of connected quandles of size p^3 [3]. Using the results on LSS quandles, we can provide the classification of two more families of non-affine quandles, namely the classes of non-simple connected quandles of size pq and $4p$ where p, q are primes.

In Section 1 we collect some basic facts about quandles and we show some preliminary results.

In Section 2 we characterize the congruence lattice of non-simple connected LSS quan-

2020 Mathematics Subject Classification. 20N02, 20N05.

dles and we show that this class of quandles coincide with the class of *extensions* of a strictly simple quandle by a strictly simple quandle (i.e. quandles having a congruence with strictly simple factor and strictly simple blocks).
First we show that finite connected *subdirectly reducible* LSS quandles are direct products of strictly simple quandles and then we focus on the *subdirectly irreducible* case.
Finite connected abelian quandles are *polynomially equivalent* to modules over the ring of Laurent polynomial [4][Sections 3.4, 3.5], so we provide a module-theoretical description of abelian connected LSS quandles.

In Section 3 we investigate non-abelian LSS quandles employing a case-by-case discussion using the equivalence relation σ_Q (already defined in [5] in connection with central congruences, see definition (3)), defining the classes of quandles $\mathcal{LSS}(p^m, q^n, \sigma_Q)$, for p, q primes, as the classes of quandles which are extensions of a strictly simple quandle of size q^n by a strictly simple quandle of size p^m and with given σ_Q. We completely characterize the displacement groups of such quandles and we compute some constructions involving special and extraspecial p-groups. Then we focus on the case $n = 1$ and $m = 1$, with the goal to describe quandles of size pq and $4p$ and as a byproduct we obtain that latin quandles of size $8p$ are affine.

The first step in the classification of non-simple connected quandles of size pq and $4p$, is to show that they are LSS quandles, except for a few small primes (see Section 4 and Section 5 respectively).
Using the one-to-one correspondence between Bruck Loops of odd order and involutory latin quandles we can show that there is only one Bruck Loop of order pq, as already proved in [26].
The classification strategy is similar to the one adopted in [3] and it is based on the representation of connected quandles as coset quandles over their displacement groups [17]. We identify the displacement group by using the Galois connection between the congruence lattice of quandles and the lattice of certain normal subgroups of $\mathrm{Dis}(Q)$ [5, Section 3.3]. Then we characterize the automorphism of such groups providing connected quandles of the desired size. Finally, we compute the isomorphism classes which are in one-to-one correspondence with conjugacy classes of such automorphisms (see Theorem 1.3). All the group theoretical results and the technical computations useful to this end are collected in Appendix 7.
Subdirectly reducible connected affine quandles of size pq and $4p$ decompone as direct products of quandles of prime power order. We show that there exists only two non-affine non-simple connected quandles of size pq whenever $p^2 = 1 \pmod q$ (Theorem 4.4) and two non-simple non-affine connected quandles of size $4p$ whenever $p = 1 \pmod 3$ (Theorem 5.5) and the latter can not be obtained by *abelian extensions* (see Section 5). In particular such quandles provide a complete list of the non-affine latin quandles of size pq and $4p$ respectively.

Finally, in Section 6 we give a description of finite non-connected LSS quandles.

Notation and terminology

An *algebraic structure* is a set A endowed with a set of operations. We denote by $\mathrm{Aut}(A)$ the automorphisms group of A and by $\mathrm{Sg}(X)$ the subalgebra generated by $X \subseteq A$. A *congruence* of A is an equivalence relation which respects the algebraic structure. Congruences of an

algebraic structure form a lattice denoted by $\mathrm{Con}(A)$ with minimum the identity relation $0_Q = \{(a,a) \mid a \in Q\}$ and maximum $1_Q = A \times A$. By virtue of the second homomorphism theorem homomorphic images and congruences are essentially the same thing. The factor structure with respect to $\alpha \in \mathrm{Con}(A)$ is denoted by A/α. The congruence lattice of A/α is $\mathrm{Con}(A/\alpha) = \{\beta/\alpha \mid \alpha \leq \beta \in \mathrm{Con}(A)\}$ where $[a]_\alpha \, \beta/\alpha \, [b]_\alpha$ if and only if $a \, \beta \, b$.

An algebraic structure is *subdirectly irreducible* if $\bigwedge_{\alpha \in \mathrm{Con}(Q)} \alpha$ is non trivial, and *subdirectly reducible* otherwise. In particular if $\bigwedge_{i \in I} \alpha_i = 0_Q$, then A embeds into $\prod_{i \in I} A/\alpha_i$. We refer the reader to [2] for further details.
An algebraic structure is *nilpotent* (resp. *solvable*) if there exists a chain of congruences

$$\alpha_0 = 0_A \leq \alpha_1 \leq \ldots \leq \alpha_n = 1_A$$

such that α_{i+1}/α_i is *central* (resp. *abelian*) in A/α_i for every $0 \leq i \leq n-1$ in the sense of [14]. The smallest congruences of A with abelian factor is denoted by γ_A and the center of A, i.e. biggest central congruence, is denoted by ζ_A (these congruences are the analogous of the derived subgroup and the center of a group, see [5, 14] for the formal definitions).

The group operations are denoted by juxtaposition or by $+$ in the abelian case. The inner automorphism of an element g of a group G is denoted by $\widehat{g}$ and its order by $|g|$. We denote by $N_G(S)$ (resp. $C_G(S)$) the normalizer (resp. centralizer) of a subset $S \subseteq G$. The core of a subgroup H (i.e. the biggest normal subgroup of G contained in H) is denoted by $\mathrm{Core}_G(H)$. If G acts on a set Q we denote the point-wise stabilizer of a in G by G_a and the orbit of a by a^G. A group is called *semiregular* if $G_a = 1$ for every $a \in G$ and *regular* if it semiregular and transitive. If f is an automorphism of a group G we denote $\mathrm{Fix}(f)$ the set of its fixed points $\{a \in G \mid f(a) = a\}$. If H is an f-invariant subgroup of G we denote by f_H the induced mapping on G/H defined as $f_H(gH) = f(g)H$.

Recall that a p-group G is said to be *special* if $Z(G) = \Phi(G) = \gamma_1(G)$ is an elementary abelian p-group (the symbol $\Phi(G)$ denotes the Frattini subgroup of G). If $Z(G)$ is cyclic then G is *extraspecial*.

1. Preliminary results

Quandles are idempotent left-distributive left quasigroups, namely a quandle Q is a binary algebraic structure $(Q, *, \backslash)$ satisfying

$$\begin{aligned} a * (a \backslash b) &= a \backslash (a * b) = b, \\ a * (b * c) &= (a * b) * (a * c), \\ a * a &= a. \end{aligned}$$

for every $a, b \in Q$. Equivalently the left multiplication mapping $L_a : b \mapsto a * b$ is an automorphism of Q fixing a for every $a \in Q$. Clearly $a \backslash b = L_a^{-1}(b)$ for every $a, b \in Q$, so we usually specify just the $*$ operation of a quandle.

Example 1.1.

(i) A set Q with the operation $a * b = b$ for every $a, b \in Q$ is a *projection quandle*. If $|Q| = n$ we denote such quandle by $\mathcal{P}_n$.
(ii) Let G be a group and $H \subseteq G$ be a subset closed under conjugation. Then $\mathrm{Conj}(H) = (H, *)$, where $g * h = g^{-1}hg$ for every $h, g \in H$, is a quandle.

(iii) Let G be a group, $f \in \mathrm{Aut}(G)$ and $H \leq \mathrm{Fix}(f)$. Let G/H be the set of left cosets of H and the multiplication defined by

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

Then $(G/H, *)$ is a quandle denoted by $\mathcal{Q}(G, H, f)$. Such a quandle is called *principal* (over G) if $H = 1$ and it will be denoted just by $\mathcal{Q}(G, f)$, and it is *affine* (over G) if G is abelian, in this case we use the notation $\mathrm{Aff}(G, f)$.

A quandle is called *homogeneous* if $\mathrm{Aut}(Q)$ acts transitively on Q. A quandle Q is homogeneous if and only if admits a representation as in Example 1.1(iii), i.e. $Q \cong \mathcal{Q}(G, H, f)$ for some group G, $f \in \mathrm{Aut}(G)$ and $H \leq \mathrm{Fix}(f)$ [18].
The *left multiplication* group is the group generated by the left multiplications mappings and it is denoted by $\mathrm{LMlt}(Q)$ and the *displacement group* is the group generated by $\{L_a L_b^{-1} \mid a, b \in Q\}$ and we denoted it by $\mathrm{Dis}(Q)$. A quandle Q is called *connected* if $\mathrm{LMlt}(Q)$ (or equivalently $\mathrm{Dis}(Q)$) acts transitively on Q. If $Q = \mathcal{Q}(G, H, f)$, the action of $\mathrm{Dis}(Q)$ is given by the canonical left action of the group $[G, f] = \langle \{gf(g)^{-1} \mid g \in G\} \rangle$ on G/H and $\mathrm{Dis}(Q) \cong [G, f]/\mathrm{Core}_G(H)$ (see [3, Section 2]).

The blocks of congruences of quandles are subquandles. Recall that connected quandles are congruence uniform (the blocks of a congruence have all the same cardinality). If the blocks of a congruence α are all isomorphic (this is guaranteed whenever Q/α is connected [5, Proposition 2.5]) we will also say that Q is an *extension* of Q/α by $[a]_\alpha$.

According to [17, Theorem 4.1], connected quandles can be represented over their displacement group as $\mathcal{Q}(\mathrm{Dis}(Q), \mathrm{Dis}(Q)_a, \widehat{L_a})$. In particular, since $[\mathrm{Dis}(Q), \widehat{L_a}] = \mathrm{Dis}(Q)$, the order of the left multiplications of Q coincides with the order of $\widehat{L_a}$.

Lemma 1.2. *Let G be a finite group, $f \in \mathrm{Aut}(G)$ and $H \leq \mathrm{Fix}(f)$. If $G = [G, f]$ then f and f_H have the same order.*

Proof. Clearly if $f^n(g) = g$ for every $g \in G$ then also $f^n(g)H = H$ for every $g \in G$, so the order of f_H divides the order of f. On the other hand if $f^n(g)H = gH$ for every $g \in G$ then $g^{-1}f^n(g) \in H \leq \mathrm{Fix}(f)$ and so $f(g^{-1}f^n(g)) = f(g^{-1})f^{n+1}(g)) = g^{-1}f^n(g)$ for every $g \in G$. Therefore $f^n(gf(g)^{-1}) = gf(g)^{-1}$ for every $g \in G$. Then the order of f divides the order of f_H since G is generated by $\{gf(g)^{-1} \mid g \in G\}$. □

The representation of connected quandles over groups is also useful for isomorphism checking. Indeed we have the following isomorphism theorem.

Theorem 1.3 ([3, Theorem 5.12, Corollary 5.13])**.** *Let $Q_i = \mathcal{Q}(G_i, H_i, f_i)$ be connected quandles for $i = 1, 2$. If $H_i = \mathrm{Fix}(f_i)$ or $H_i = 1$ for $i = 1, 2$ then $Q_1 \cong Q_2$ if and only there exists a group isomorphism $\psi : G_1 \longrightarrow G_2$ such that $f_2 = \psi f_1 \psi^{-1}$.*

For every congruence α of a quandle Q the mapping

$$\pi_\alpha : \mathrm{Dis}(Q) \longrightarrow \mathrm{Dis}(Q/\alpha), \quad L_a L_b^{-1} \mapsto L_{[a]} L_{[b]}^{-1} \tag{1}$$

is a well-defined surjective group morphism and its kernel is

$$\mathrm{Dis}^\alpha = \{h \in \mathrm{Dis}(Q) \mid [h(a)] = [a], \text{ for every } a \in Q\}. \tag{2}$$

The *displacement group relative to the congruence* α is defined analogically to the displacement group as

$$\mathrm{Dis}_\alpha = \langle \{L_a L_b^{-1} \mid a \,\alpha\, b\} \rangle.$$

Note that the characteristic subgroups of $\mathrm{Dis}(Q)$ and both the relative displacement groups and the kernels defined in (2) belong to $\mathrm{Norm}(Q) = \{N \trianglelefteq \mathrm{LMlt}(Q) \mid N \leq \mathrm{Dis}(Q)\}$ and that $[\mathrm{Dis}(Q), \mathrm{Dis}^\alpha] \leq \mathrm{Dis}_\alpha \leq \mathrm{Dis}^\alpha$ [5, Proposition 3.3].

The orbit decomposition with respect to the action of $N \in \mathrm{Norm}(Q)$ denoted by $\mathcal{O}_N$ and the relation $\mathrm{con}_N = \{(a,b) \in Q \times Q \mid L_a L_b^{-1} \in N\}$ are congruences of Q [5, Lemma 2.6, Lemma 3.4].

The structure of the subgroups in $\mathrm{Norm}(Q)$ can be investigated using the following Lemma.

Lemma 1.4. *Let Q be a connected quandle, $\alpha \in \mathrm{Con}(Q)$ such that $Q/\alpha = \mathrm{Sg}([a_1], \ldots, [a_n])$ and let $N \in \mathrm{Norm}(Q)$ such that $N \leq \mathrm{Dis}^\alpha$. Then*:

(i) *the mapping*

$$\psi : \mathrm{Dis}^\alpha \longrightarrow \prod_{i=1}^{n} \mathrm{Aut}([a_i]), \quad h \mapsto (h|_{[a_1]}, \ldots, h|_{[a_n]}),$$

is an embedding of groups and $N|_{[a_i]_\alpha} \cong N|_{[a_j]_\alpha}$ for every $1 \leq i, j \leq n$.

(ii) *If N is regular on $[a]_\alpha$ and $[a]_\alpha$ is a principal connected quandle then $N|_{[a]} \cong \mathrm{Dis}([a])$ and N embeds into $\mathrm{Dis}([a])^n$.*

Proof. (i) The union of the blocks of $a_1, \ldots, a_n$ generates the quandle Q. If $\psi(h) = 1$ then h fixes a set of generators of Q and therefore $h = 1$, i.e. ψ is an embedding. Let $a_i, a_j \in Q$, $h \in \mathrm{Dis}(Q)$ such that $h([a_i]) = [a_j]$ and $\psi_i : N \longrightarrow N|_{[a_i]}$. Then $\ker(\psi_j) = h\ker(\psi_i)h^{-1}$ and so the mapping

$$N|_{[a]_i} \longrightarrow N|_{[a_j]}, \quad g|_{[a_i]} \mapsto hgh^{-1}|_{[a]_j}$$

is a well defined group isomorphism.

(ii) The group $N|_{[a]}$ is a regular automorphism group of the connected principal quandle $[a]$. According to [4, Proposition 3.1], $N|_{[a]} \cong \mathrm{Dis}([a])$. □

The set $L(Q) = \mathrm{Conj}(\{L_a \mid a \in Q\})$ is a conjugation quandle and $L_Q : Q \to L(Q)$ mapping a to L_a is a surjective quandle morphism and we denote its kernel by λ_Q. A quandle is called *faithful* if L_Q is injective, i.e. $\lambda_Q = 0_Q$. For a faithful quandle Q we have that $\mathrm{Dis}(Q)_a = \mathrm{Fix}(\widehat{L_a})$ for every $a \in Q$. A quandle is *latin* if all right multiplications $R_a : b \mapsto b * a$ are bijective and in such case we use the notation $R_a^{-1}(b) = b/a$. Latin quandles are faithful and connected.

Lemma 1.5. *Let Q be a quandle and $\alpha \in \mathrm{Con}(Q)$.*

(i) *If Q is faithful and α is a minimal congruence then Dis_α is a minimal element of $\mathrm{Norm}(Q)$. In particular, if Dis_α is solvable, then it is abelian.*

(ii) *If α is a maximal congruence then Dis^α is a maximal element of $\mathrm{Norm}(Q)$.*

Proof. (i) The quandle Q is faithful and so $\mathrm{Dis}_\alpha \neq 1$. Let $N < \mathrm{Dis}_\alpha$. Then $\mathcal{O}_N \leq \alpha$. If equality holds, $b = n(a)$ for some $n \in N$ whenever $a \,\alpha\, b$ and then

$$L_b L_a^{-1} = L_{n(a)} L_a^{-1} = n \underbrace{L_a n^{-1} L_a^{-1}}_{\in N} \in N$$

and therefore $\mathrm{Dis}_\alpha \leq N$, contradiction. Hence $\mathcal{O}_N = 0_Q$ and $N = 1$. If Dis_α is solvable, then its derived subgroup is a proper subgroup of Dis_α and it belongs to $\mathrm{Norm}(Q)$ and therefore it is trivial i.e. Dis_α is abelian.

(ii) The quandle Q/α is simple and then $\mathrm{Norm}(Q/\alpha)$ is the two element lattice. Hence, if $\mathrm{Dis}^\alpha \lneqq N \in \mathrm{Norm}(Q)$ then $\pi_\alpha(N) = \mathrm{Dis}(Q/\alpha)$ and so $N = \mathrm{Dis}(Q)$. □

Let Q be a quandle. The equivalence relation σ_Q is defined as

$$a \,\sigma_Q\, b \quad \text{if and only if} \quad \mathrm{Dis}(Q)_a = \mathrm{Dis}(Q)_b. \tag{3}$$

The classes of σ_Q are subquandles and they are blocks with respect to the action of $\mathrm{LMlt}(Q)$ [4, Proposition 2.5]. Recall that, if Q is connected, the block of a with respect to σ_Q is the orbit of a under the action of $N(\mathrm{Dis}(Q)_a)$ [4, Theorem 3.4] and so Q is principal if and only if $\sigma_Q = 1_Q$.

The properties of congruences as abeliannes and centrality in the sense of [14] are completely determined by the properties of the relative displacement groups, especially for faithful quandles.

Theorem 1.6 ([5, Sections 5.2 and 6.1])**.** *Let Q be a faithful quandle and $\alpha \in \mathrm{Con}(Q)$.*

(i) *α is abelian (resp. central) if and only if Dis_α is abelian (resp. central in $\mathrm{Dis}(Q)$).*

(ii) *Q is solvable (resp. nilpotent) if and only if $\mathrm{Dis}(Q)$ is solvable (resp. nilpotent).*

In particular, $\zeta_Q = \mathrm{con}_{Z(\mathrm{Dis}(Q))} \leq \sigma_Q$.

We refer the reader to [1, 17, 18] for further basic results on quandles.

2. Locally strictly simple quandles

Congruence lattice. *Strictly simple quandles* are quandles with no proper subquandles (proper subquandles have more than one element), i.e. quandles that are generated by any pair of distinct elements. The class of finite strictly simple quandle is well understood as it coincides with the class of simple abelian quandles, namely the class of simple affine quandles (including $\mathcal{P}_2 \cong \mathrm{Aff}(\mathbb{Z}_2, 1)$, see [4, Section 4.1]). Every strictly simple connected quandle is latin and it has an affine representation as $M = \mathrm{Aff}(\mathbb{Z}_p^m, f)$ where f acts irreducibly on $\mathbb{Z}_p^m$ and its automorphism group $\mathrm{Aut}(M) \cong \mathbb{Z}_p^n \rtimes C_{GL_n(p)}(f) \cong \mathbb{Z}_p^n \rtimes \mathbb{Z}_{p^m-1}$ is doubly transitive [4, Section 4.1]. Alternatively, such quandles arise as $\mathrm{Aff}(\mathbb{F}_q, \lambda)$ where $\mathbb{F}_q$ is the finite field with q elements and λ is the automorphism of the underlying abelian group given by the multiplication an invertible element $\lambda \in \mathbb{F}_q \setminus \{1\}$. In particular, finite strictly simple quandles are in one-to-one correspondence with irreducible polymonials over finite fields.

The lattice of subquandles containing a fixed element a strictly simple quandle is the two element lattice and so it has height one. We investigate the class of finite connected quandles for which this lattice has height at most two.

DEFINITION 2.1. A quandle A is said to be *locally strictly simple* (LSS) if all its proper subquandles are strictly simple.

Lemma 2.2. *Let Q be a connected LSS quandle. Then*:

(i) *Q/α is strictly simple for every proper congruence α.*
(ii) *$\alpha \wedge \beta = 0_Q$ for every pair of distinct proper congruences α, β.*
(iii) *The congruence lattice of Q is one of those in* Figure 1.

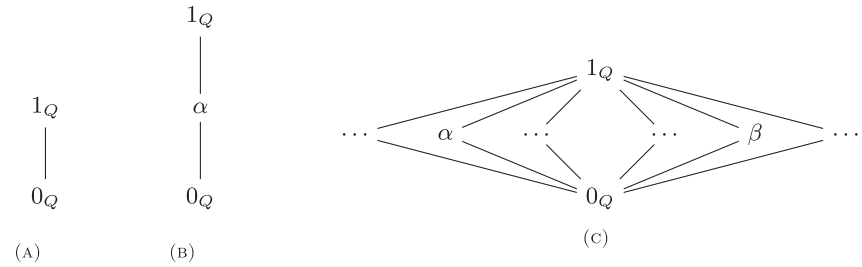


Fig. 1. (A) Simple - (B) Subdirectly Irreducible - (C) Subdirectly reducible.

Proof. (i) Let $\alpha \in \mathrm{Con}(Q)$ be a proper congruence ($\alpha \neq 0_Q, 1_Q$). Then if $[a]_\alpha \neq [b]_\alpha$ then $[a]_\alpha$ is a proper subquandle of $\mathrm{Sg}([a]_\alpha, [b]_\alpha)$ and so $Q = \mathrm{Sg}([a]_\alpha, [b]_\alpha)$. Hence $Q/\alpha = \mathrm{Sg}([a]_\alpha, [b]_\alpha)$ for every $[a]_\alpha \neq [b]_\alpha$ and then Q/α is strictly simple.

(ii) According to (i), every proper factor of Q is simple and thus every proper congruence of Q is maximal. Thus if α, β are distinct proper congruences, then $\alpha \wedge \beta = 0_Q$.

(iii) It follows by (i) and (ii). □

A characterization of (non-simple) LSS quandles is offered by the following Proposition.

REMARK 2.3. Let Q be a finite connected LSS quandle and $\alpha \in \mathrm{Con}(Q)$. Since every block and the factor Q/α is generated by any pair of its elements then Q is generated by any triple $a, b, c \in Q$ such that $[a]_\alpha = [b]_\alpha \neq [c]_\alpha$ (see also [3, Lemma 6.1]).

Proposition 2.4. *Let Q be a non-simple connected quandle. The following are equivalent*:

(i) *Q is LSS.*
(ii) *Q/α and $[a]_\alpha$ are strictly simple quandles for every proper $\alpha \in \mathrm{Con}(Q)$ and every $a \in Q$.*
(iii) *There exists $\alpha \in \mathrm{Con}(Q)$, such that Q/α and $[a]_\alpha$ are strictly simple quandles for every $a \in Q$.*

Proof. (i) $\Rightarrow$ (ii) It follows by Lemma 2.2 (iii) and since $[a]_\alpha$ is a proper subquandle of Q.

(ii) $\Rightarrow$ (iii) Clear.

(iii) $\Rightarrow$ (i) Let S be a subquandle of Q. Then either the image of S under the canonical map $a \mapsto [a]_\alpha$ is the whole Q/α or it is just a one element set.

In the first case, $|S \cap [a]_\alpha| \geq 1$ for every $[a]_\alpha$ in Q/α. If equality holds for every $a \in Q$, then $S \cong Q/\alpha$ and so S is strictly simple. Otherwise, $S = Q$ by Remark 2.3.

In the second case, $S \subseteq [a]_\alpha$ for some $a \in Q$, then either $|S| = 1$ or $S = [a]_\alpha$, and so S is strictly simple. □

The isomorphism classes of subquandles of Q are completely determined by its factors and by the block of its congruences. Indeed, by the same argument used in Proposition 2.4 to prove the implication (iii) $\Rightarrow$ (i) we have the following.

Corollary 2.5. *Let Q be a connected LSS non-simple quandle. Every subquandle of Q is isomorphic either to $[a]_\alpha$ or to Q/α for some $\alpha \in \mathrm{Con}(Q)$.*

Connected abelian LSS quandles. In this section we describe finite, abelian connected LSS quandles. Finite connected abelian quandles are latin and they are *polynomially equivalent* to modules over $\mathbb{Z}[t, t^{-1}]$ [4, Sections 3.4, 3.5]. Indeed they admit an affine representation as $\mathrm{Aff}(A, f)$ where A is an abelian group and $f \in \mathrm{Aut}(A)$. Congruences of such quandles are in one-to-one correspondence with subquandles containing 0 and with submodules i.e. with f-invariant subgroups [4, Proposition 3.18, Remark 3.19]. Moreover two connected finite affine quandles are isomorphic if and only if they are isomorphic as modules.

The first class of abelian LSS quandles is given by subdirectly reducible LSS quandles (i.e. quandle which congruence lattice is as in figure 1(C) which are just direct product of a pair of strictly simple quandles.

Lemma 2.6. *Let Q be a finite connected quandle and $\alpha, \beta \in \mathrm{Con}(Q)$ such that Q/α and Q/β are strictly simple. Then $Q/(\alpha \wedge \beta) \cong Q/\alpha \times Q/\beta$.*

Proof. Let $\gamma = \alpha \wedge \beta$. The quandle Q/γ embeds into $Q/\alpha \times Q/\beta$. The blocks of α/γ have all the same size according to [5, Proposition 2.5]. The block $[a]_{\alpha/\gamma}$ maps onto Q/β and then $|Q/\gamma| = |[a]_{\alpha/\gamma}||Q/\alpha| \geq |Q/\beta||Q/\alpha|$. Therefore $Q/\gamma \cong Q/\alpha \times Q/\beta$. □

Theorem 2.7. *Let Q be a finite connected LSS quandle. The following are equivalent*:

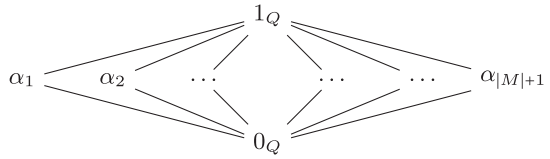
(i) *Q is subdirectly reducible.*
(ii) *$Q \cong M \times N$ where M and N are connected strictly simple quandles.*

In particular, if (ii) holds then Q is latin and abelian.

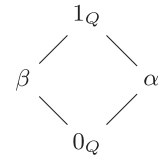
Proof. We can apply Lemma 2.6 by virtue of Lemma 2.2. The direct product of affine latin quandles is affine and latin. □

REMARK 2.8. Let $Q = M \times N$ where M, N are strictly simple quandles.

(i) if $M \cong N \cong \mathrm{Aff}(\mathbb{F}_q, \lambda)$ then Q is isomorphic to $\mathrm{Aff}(\mathbb{F}_{|M|}^2, \lambda I)$, its automorphism group is doubly transitive and any pair of elements generate a subquandle isomorphic to M [4, Section 4.3]. In particular $\mathrm{Con}(Q)$ has $|M| + 1$ non trivial congruences (it is the lattice of subspaces of a 2-dimensional vector space):



(ii) Let $M = Q/\alpha$ and $N = Q/\beta$ be non isomorphic and let γ be a congruence different from α, β. Then $M = [0]_\beta$ and $N = [0]_\alpha$ are both isomorphic to Q/γ since $\alpha \wedge \gamma = \beta \wedge \gamma = 0_Q$. Hence Q has just two proper congruences:



Note that if $Q = \mathrm{Aff}(A, f)$ is a subdirectly irreducible LSS connected quandle, namely the congruence lattice of Q is as in 1(B), then A has a unique proper f-invariant subgroup.

Lemma 2.9. *Subdirectly irreducible abelian LSS connected quandles are affine over p-groups of exponent less or equal to* p^2.

Proof. Let $Q = \mathrm{Aff}(A, f)$. The p-components of A provide trivially intersecting congruences as they are characteristic subgroups. So A is a p-group. Moreover, the map $p : A \to A$, $a \mapsto pa$ provides a chain of characteristic subgroups $ker(p) \leq ker(p^2)$. Therefore the exponent of A is less or equal to p^2. □

If the exponent of the group is p a complete characterization is given by module theory.

Proposition 2.10. *Let* $Q = \mathrm{Aff}(\mathbb{Z}_p^n, f)$ *be a connected quandle. The following are equivalent*:

(i) *Q is a subdirectly irreducible LSS quandle.*
(ii) $Q \cong \mathrm{Aff}(\mathbb{Z}_p[t]/(g^2), t)$ *where* $g \neq t, 1 - t$ *is an irreducible polynomial over* $\mathbb{Z}_p$ *and* $n = 2\deg(g)$.

Proof. Every affine quandle over $\mathbb{Z}_p^n$ is a module over $\mathbb{Z}_p[t, t^{-1}]$ and since Q is finite we can consider it as a module over $\mathbb{Z}_p[t]$.

The quandle Q is a connected subdirectly reducible LSS quandle if and only if Q is connected and its underlying $\mathbb{Z}[t]$-module has a unique proper submodule. According to [7, Lemma 2], this is equivalent to have that the underlying $\mathbb{Z}_p[t]$-module of Q is isomorphic to $\mathbb{Z}_p[t]/(g^2)$ where g is an irreducible polynomial and $n = 2\deg(g)$.

It is easy to check that the operation defined on $\mathbb{Z}_p[t]/(g^2)$ by $(a + (g^2)) * (b + (g^2)) = (1 - t)a + tb + (g^2)$ provides a connected quandle if and only if $g \neq t, 1 - t$, provided g be irreducible. □

Note that quandles described in Proposition 2.10 are in one-to-one correspondence with irreducible polynomials as for connected strictly simple quandles.

Proposition 2.11. *Let* $Q = \mathrm{Aff}(A, f)$ *be a finite connected abelian subdirectly irreducible LSS quandle. If* $exp(A) = p^2$, *then* $A \cong \mathbb{Z}_{p^2}^n$ *and* $Q/\alpha \cong [a]$ *for every* $a \in Q$.

Proof. The map $p : A \longrightarrow pA$ mapping a to pa is a module morphism. Since A has a unique f-invariant subroup, $\ker(p) = \mathrm{Im}(p) = pA$. Therefore $A \cong \mathbb{Z}_{p^2}^n$ and $[0]_\alpha = \ker(p)$, so $Q/\alpha \cong A/pA \cong pA = \ker(p) \cong [a]$ as modules. □

EXAMPLE 2.12. Let h be an irreducible polynomial of degree n over $\mathbb{Z}_p$ and let F be its companion matrix. Let

$$\mathcal{B} = \{e_i = (\underbrace{0, \ldots, 1}_{i}, 0, \ldots, 0) \mid 1 \leq i \leq n\}$$

be the canonical set of generators for $A = \mathbb{Z}_{p^2}^n$ and $Q = \mathrm{Aff}(A, f)$ where f is represented by F with respect to the set of generators $\mathcal{B}$. The induced matrix on the factor A/pA with respect to the basis $\{e_i + pA \mid 1 \leq i \leq n\}$ and the restriction to pA with respect to the basis $\{pe_i \mid 1 \leq i \leq n\}$ are equal to F. Therefore, A/pA and pA are isomorphic as simple modules and Q is LSS and subdirectly irreducible by Proposition 2.4. In particular for every strictly simple quandle this construction provides a quandle as in Proposition 2.11.

3. Connected non-abelian LSS quandles

The classes $\mathcal{LSS}(p^m, q^n, \sigma_Q)$. Connected non-abelian LSS quandles are subdirectly irreducible, since all quandles described in Theorem 2.7 are abelian. So their congruence lattice is as in Figure 1(B). In the following we are describing such quandles according to different properties, in particular according to the equivalence relation σ_Q (see (3)). So, we will denote by $\mathcal{LSS}(p^m, q^n, \sigma_Q)$ the class of finite non-abelian subdirectly irreducible connected quandles with given σ_Q and such that the unique congruence has factor of size q^n and blocks of size p^m.

Proposition 3.1. *Let $Q \in LSS(p^m, q^n, \sigma_Q)$ and let $G = \mathrm{Dis}(Q)$.*

(i) *The unique non-trivial congruence of Q is γ_Q.*

(ii) $Q/\gamma_Q \cong \mathrm{Aff}(G/\gamma_1(G), f_{\gamma_1(G)})$ *and* $\mathrm{Dis}(Q)_a \leq \mathrm{Dis}^{\gamma_Q} = \gamma_1(G)$ *for every* $a \in Q$.

If $p^n > 2$ then

(iii) *Q is faithful.*

(iv) $\gamma_2(G) \leq \mathrm{Dis}_{\gamma_Q} \cong \mathbb{Z}_p^{m+k}$ *where $k \leq m$ and γ_Q is abelian.*

Proof. (i) Let α be the unique non-trivial congruence of Q. The quandle Q is not abelian and Q/α is abelian. Then $\gamma_Q = \alpha$.

(ii) We can apply directly [3, Proposition 2.5].

(iii) All the strictly simple quandles of size bigger than 2 are faithful. If $L_{[a]} = L_{[b]}$ it follows that $[a] = [b]$ since Q/γ_Q is faithful (Q/γ_Q is connected and so it has not size 2). Thus $L_a|_{[a]} = L_b|_{[a]}$, and so $a = b$ since the blocks of γ_Q are faithful.

(iv) According to Lemma 1.4(i), $\gamma_1(G) = \mathrm{Dis}^{\gamma_Q}$ embeds into $\mathrm{Aut}([a]) \times \mathrm{Aut}([b]) \cong (\mathbb{Z}_p^m \rtimes \mathbb{Z}_{p^m-1})^2$. Hence $\mathrm{Dis}_{\gamma_Q} \leq \mathrm{Dis}^{\gamma_Q}$ is solvable and then it is abelian by Lemma 1.5(i). The blocks are connected, so Dis_{γ_Q} is regular on each block and $\mathrm{Dis}_{\gamma_Q}|_{[a]} \cong \mathbb{Z}_p^m$ by Lemma 1.4(ii). Hence, Dis_{γ_Q} is isomorphic to $\mathbb{Z}_p^{m+k}$ with $k \leq m$. Then γ_Q is abelian according to Theorem 1.6(i) and $\gamma_2(G) = [G, \gamma_1(G)] = [G, \mathrm{Dis}^{\gamma_1(Q)}] \leq \mathrm{Dis}_{\gamma_1(Q)}$ by [5, Proposition 3.3]. □

In the sequel we will discuss several cases according to the equivalence relation σ_Q. Such cases are described in the following Lemma.

Lemma 3.2. *Let $Q \in \mathcal{LSS}(p^m, q^n, \sigma_Q)$. Then one of the following holds*:

(i) $\sigma_Q = 1_Q$ *i.e. Q is principal.*

(ii) $\sigma_Q = \gamma_Q$.

(iii) $\sigma_Q \wedge \gamma_Q = 0_Q$.

In particular, if $p = q$ then $\gamma_Q = \zeta_Q \leq \sigma_Q$.

Proof. The blocks of σ_Q are subquandles of Q and they are blocks with respect to the action of $\mathrm{LMlt}(Q)$. Assume that $\sigma_Q \neq 1_Q$. All the subquandles of Q are strictly simple, so either $[a]_{\gamma_Q}$ and $[a]_{\sigma_Q}$ coincide or their intersection is the singleton $\{a\}$.
If $p = q$, the quandle Q is nilpotent [5, Theorem 1.4, Proposition 6.5] and then γ_Q is a central congruence, i.e. $\gamma_Q = \zeta_Q \leq \sigma_Q$. □

The classes $\mathcal{LSS}(2, q^n, \sigma_Q)$. According to Proposition 3.1(iii) the classes $\mathcal{LSS}(2, q^n, \sigma_Q)$ contain the non-faithful connected LSS quandles. We can completely characterize the elements of such classes.

Theorem 3.3. *Let $Q \in \mathcal{LSS}(2, q^n, \sigma_Q)$. Then either $|Q| = 6$ or $q = 2$ and Q is a non-faithful principal quandle over an extraspecial 2-group.*

Proof. Let $|Q/\gamma_Q| = q^n$. If Q is faithful then Q has a congruence with strictly simple factor and projection blocks. So we can apply [4, Theorem 5.8(i)] and we have $|Q| = 6$. If Q is not faithful then $\gamma_Q = \lambda_Q$ and Q/λ_Q is affine, so Q is principal over some group G by [3, Proposition 5.3]. Therefore, $|Q| = |G| = 2q^n$. If $q \geq 3$ then G has a normal q-Sylow group H of index 2. According to [4, Theorem 3.10] the coset partition with respect to a characteristic subgroups is a congruence, so H induces a congruence with non-connected factor of size 2, contradiction.
So $q = 2$ and $G = \mathrm{Dis}(Q)$ has just one characteristic subgroup, namely $\mathrm{Dis}^{\gamma_1(Q)} = \gamma_1(G) = Z(G) = \Phi(G) \cong \mathbb{Z}_2$. Thus, G is an extraspecial 2-group. □

Note that there are 2 non-isomorphic connected quandles of size 6 in the RIG library of GAP and they are both faithful and they belong to $\mathcal{LSS}(2, 3, \gamma_Q)$. Using the criterion of connectedness for quandles represented by nilpotent groups given in [3, Proposition 2.7] we can identify the automorphisms of extraspecial 2-groups giving rise to quandles $\mathcal{Q}(G, f)$ in $\mathcal{LSS}(2, 2^{2n}, 1_Q)$.

Proposition 3.4. *Let G be an extraspecial 2-group of size 2^{2n+1} and $f \in \mathrm{Aut}(G)$. The following are equivalent*:

(i) $Q = \mathcal{Q}(G, f) \in \mathcal{LSS}(2, 2^{2n}, 1_Q)$.
(ii) $f_{\gamma_1(G)}$ *acts irreducibly on* $G/\gamma_1(G)$.

Isomorphism classes of such quandles are in one-to-one correspondence with conjugacy classes of automorphisms as in (ii).

Proof. (i) ⇒ (ii) It follows since the factor $Q/\gamma_Q \cong \mathrm{Aff}(G/\gamma_1(G), f_{\gamma_1(G)})$ is strictly simple.
(ii) ⇒ (i) The group G is an extraspecial 2-group, so $\gamma_1(G) = \Phi(G) \cong \mathbb{Z}_2$ and the quandle $\mathrm{Aff}(G/\gamma_1(G), f_{\gamma_1(G)}) = \mathrm{Aff}(G/\Phi(G), f_{\Phi(G)})$ is connected. According to [3, Proposition 2.7], Q is connected and $\mathrm{Dis}(Q) \cong G$. The congruence of Q associated to $\gamma_1(G)$ has blocks of size 2 and strictly simple factor since $f_{\gamma_1(G)}$ acts irreducibly on $G/\gamma_1(G)$. Therefore Q is LSS by Proposition 2.4. By virtue of Theorem 2.7 subdirectly reducible LSS quandles are latin, then Q is subdirectly irreducible.

Isomorphism classes of connected principal quandles over a group G correspond to conjugacy classes of automorphisms (Theorem 1.3). □

EXAMPLE 3.5. A GAP computer search for quandles as in Proposition 3.4 reveals that there exist just one isomorphism class of quandles in $\mathcal{LSS}(2, 2^{2n}, 1_Q)$ for $n = 1, 2, 3$ and two of them in $\mathcal{LSS}(2, 2^8, 1_Q)$. All these examples are over the extraspecial 2-group constructed as the central product of one copy of the quaternion group and several copies of the dihedral group.

Nilpotent case. A characterization of nilpotent (non-abelian) LSS quandle is the following.

Lemma 3.6. *Let $Q \in \mathcal{LSS}(p^m, q^n, \sigma_Q)$ be a quandle and $p^m > 2$. The following are equivalent*:

(i) $p = q$.
(ii) $Z(\mathrm{Dis}(Q)) \neq 1$.
(iii) *Q is nilpotent of length* 2.

Proof. (i) $\Rightarrow$ (ii) By [5, Proposition 6.5], the displacement group of connected quandles of size a power of a prime p is a p-group and so it has non-trivial center.

(ii) $\Rightarrow$ (iii) The orbits of the center of $\mathrm{Dis}(Q)$ are contained in the center of Q. Then ζ_Q is non-trivial and so it coincides with the unique non-trivial congruence of Q. Hence $\zeta_Q = \gamma_Q$, i.e. Q is nilpotent of length 2.

(iii) $\Rightarrow$ (i) Finite connected faithful nilpotent quandles split as direct product of quandles of prime power size [5, Theorem 1.4], hence the subdirectly irreducible ones have size a power of a prime. □

According to Lemma 3.6 in this section we can assume that $p = q$. First we characterize the displacement group of quandles in $\mathcal{LSS}(p^m, p^n, \sigma_Q)$, using the following Proposition.

Proposition 3.7. [24, Proposition 9.2.5] *Let G be a group and let $X \subseteq G$ such that $G/\gamma_1(G) = \langle \{x\gamma_1(G) \mid x \in X\} \rangle$. Then $\gamma_1(G)/\gamma_2(G) = \langle \{[x, y]\gamma_2(G) \mid x, y \in X\} \rangle$. In particular if $G/\gamma_1(G)$ is cyclic, then $\gamma_1(G) = \gamma_2(G)$.*

Theorem 3.8. *Let $Q \in \mathcal{LSS}(p^m, p^n, \sigma_Q)$, $G = \mathrm{Dis}(Q)$ and $a \in Q$. Then*:

(i) *Q is latin.*
(ii) *$Z(G) = \mathrm{Dis}_{\zeta_Q} \cong \mathbb{Z}_p^m$ and $\Phi(G) = \gamma_1(G) \cong Z(G) \times G_a \cong \mathbb{Z}_p^{m+k}$ for some $k \leq m$.*
(iii) *$n \geq 2$.*

Proof. The quandle Q is a finite connected faithful quandle of nilpotency length 2 by Lemma 3.6 and G is a p-group.

(i) According to [3, Proposition 3.5], Q is latin.

(ii) The center of Q is $\zeta_Q = \mathrm{con}_{Z(\mathrm{Dis}(Q))}$ and so according to [3, Proposition 3.1] we have $\mathrm{Dis}_{\zeta_Q} = Z(G) \cong \mathrm{Dis}([a]) \cong \mathbb{Z}_p^m$. By [3, Proposition 3.5], the kernel $\gamma_1(G)$ decomposes as the direct product of the center of G and the stabilizer G_a. The subgroup $\gamma_1(G)$ is regular on every block of γ_Q since $\gamma_Q = \zeta_Q \leq \sigma_Q$. According to Lemma 1.4(ii) it embeds into $\mathrm{Dis}([a])^2 \cong \mathbb{Z}_p^{2m}$, therefore $\gamma_1(G)$ is an elementary abelian p-group. The factor $\mathrm{Dis}(Q/\gamma_Q) = G/\gamma_1(G)$ is elementary abelian, so $\gamma_1(G) = \Phi(G)$.

(iii) The group G is nilpotent. According to Proposition 3.7, $G/\gamma_1(G)$ can not be cyclic, therefore $n \geq 2$. □

The classes $\mathcal{LSS}(p^m, p^n, 1_Q)$ are given by principal quandles over special p-groups.

Proposition 3.9. *Let Q be a finite quandle. The following are equivalent*:

(i) $Q \in \mathcal{LSS}(p^m, p^n, \sigma_Q)$ *and* $\gamma_2(\mathrm{Dis}(Q)) = 1$.
(ii) $Q \in \mathcal{LSS}(p^m, p^n, 1_Q)$ *and* $m \leq \frac{n(n-1)}{2}$.
(iii) $Q \cong \mathcal{Q}(G, f)$ *where G is a special p-group, f acts irreducibly on $Z(G) \cong \mathbb{Z}_p^m$ and $f_{Z(G)}$ acts irreducibly on $G/Z(G) \cong \mathbb{Z}_p^n$.*

Isomorphism classes of such quandles are in one-to-one correspondence with conjugacy classes of automorphisms as in (iii).

Proof. (i) $\Leftrightarrow$ (ii) According to Theorem 3.8(ii), we have that $\gamma_2(G) = 1$ if and only if $\gamma_1(G) = Z(G)$, that is equivalent to $G_a = 1$. Moreover, if (i) holds $\gamma_1(G) \cong \mathbb{Z}_p^m$ and by Proposition 3.7 $\gamma_1(G)$ has at most $\binom{n}{2}$ generators. Therefore we have $m \leq \binom{n}{2} = \frac{n(n-1)}{2}$.

(ii) $\Rightarrow$ (iii) The quandle Q is isomorphic to $\mathcal{Q}(G, f)$ where G is a special p-group. Since Q is LSS then the action of f over $Z(G) = [1]_{\zeta_Q}$ and the action of $f_{Z(G)}$ over $\mathrm{Dis}(Q/\zeta_Q) \cong G/Z(G)$ are irreducible.

(iii) $\Rightarrow$ (ii) The coset partition with respect to $Z(G) = \Phi(G)$ is a congruence of the quandle $Q = \mathcal{Q}(G, f)$ with strictly simple factor and strictly simple blocks. According to [3, Proposition 2.7], Q is connected since $\mathrm{Aff}(G/\Phi(G), f_{\Phi(G)})$ is connected and $G \cong \mathrm{Dis}(Q)$. Then Q is LSS according to Proposition 2.4. □

EXAMPLE 3.10. Let $Q \in \mathcal{LSS}(p^m, p^2, 1_Q)$. By Proposition 3.9 we have $m = 1$ and so $|Q| = p^3$. According to the results of [3], there are $\frac{(p-1)^2}{2}$ non-isomorphic quandles in $\mathcal{LSS}(p, p^2, 1_Q)$ and $\mathcal{LSS}(p, p^2, \gamma_Q)$ is empty.

Non-nilpotent case. According to Lemma 3.6, in this subsection we assume that p and q are different primes and $p^m > 2$. Let $Q \in \mathcal{LSS}(p^m, q^n, \sigma_Q)$ and $G = \mathrm{Dis}(Q)$. According to Lemma 1.5(ii) then $\gamma_1(G)$ is maximal in $\mathrm{Norm}(Q)$ and so in particular it is a maximal characteristic subgroup of G. Moreover, $\gamma_2(G)$ is an elementary p-abelian group and $G/\gamma_1(G)$ is an elementary q-abelian group (see Lemma 3.1). Hence G satisfies the hyphothesis of the following Proposition. The result below was stated improperly in [4, Proposition 5.7], so we include the correct statement for reader's convenience.

Proposition 3.11 ([4, Proposition 5.7])**.** *Let p, q be different primes, $m, n \in \mathbb{N}$ and let G be a group such that $\gamma_2(G) \cong \mathbb{Z}_p^m$, $G/\gamma_1(G) \cong \mathbb{Z}_q^n$ and $\gamma_1(G)$ be a maximal characteristic subgroup. If $\gamma_1(G) = \gamma_2(G)$ then $G \cong \mathbb{Z}_p^m \rtimes_\rho \mathbb{Z}_q^m$, otherwise $G \cong \mathbb{Z}_p^m \rtimes_\rho K$ where K is a special q-group with $Z(K) \cong \gamma_1(G)/\gamma_2(G)$.*

Lemma 3.12. *Let $Q \in \mathcal{LSS}(p^m, q^n, \sigma_Q)$ and $G = \mathrm{Dis}(Q)$. The following are equivalent*:

(i) $\gamma_Q \leq \sigma_Q$.
(ii) $\mathrm{Dis}_{\gamma_Q} = \gamma_1(G) = \gamma_2(G) \cong \mathbb{Z}_p^{m+k}$ *with* $k \leq m$.
(iii) $Z(\gamma_1(G)) \neq 1$.

Proof. (i) $\Rightarrow$ (ii) Since $\mathcal{O}_{\gamma_1(G)} = \gamma_Q \leq \sigma_Q$ the group $\gamma_1(G)$ is regular on each block of γ_Q. The factor Q/γ_Q is generated by two elements, thus by Lemma 1.4(ii) $\gamma_1(G)$ embeds into $\mathbb{Z}_p^{2m}$ and has at least size p^m. Then we can apply Proposition 3.11 to G. So, $\gamma_1(G)$ is contained in the p-Sylow of G that is $\gamma_2(Q)$ by Proposition 3.11. Thus, $\gamma_2(G) \leq \mathrm{Dis}_{\gamma_Q} \leq$

$\mathrm{Dis}^{\gamma_Q} = \gamma_1(G) = \gamma_2(G)$ and so equality holds.

(ii) $\Rightarrow$ (iii) Clear.

(iii) $\Rightarrow$ (i) Let $Z = Z(\gamma_1(G))$. The orbits of Z are non-trivial and they are contained in the blocks of σ_Q: indeed $\mathrm{Dis}(Q)_a \leq \gamma_1(G)$ and then Z centralizes $\mathrm{Dis}(Q)_a$. Then $a \neq a^Z \subseteq [a]_{\sigma_Q} \cap [a]_{\gamma_Q}$ and so $[a]_{\gamma_Q} \leq [a]_{\sigma_Q}$, since $[a]_{\gamma_Q}$ is strictly simple for every $a \in Q$. Hence $\gamma_Q \leq \sigma_Q$. □

We can characterize the structure of the displacement group of quandles in the classes $\mathcal{LSS}(p^m, q^n, \sigma_Q)$ using again Proposition 3.11.

Theorem 3.13. *Let $Q \in \mathcal{LSS}(p^m, q^n, \sigma_Q)$ and $\gamma_Q \leq \sigma_Q$. Then*

$$\mathrm{Dis}(Q) \cong \mathbb{Z}_p^{m+k} \rtimes_\rho \mathbb{Z}_q^n \tag{4}$$

where $k \leq m$, ρ is a faithful action and $\gamma_1(\mathrm{Dis}(Q)) = \gamma_2(\mathrm{Dis}(Q)) = \mathrm{Dis}_{\gamma_Q}$.

Proof. Let $G = \mathrm{Dis}(Q)$. By virtue of Lemma 3.12 we have that $\gamma_1(G) = \gamma_2(G) = \mathrm{Dis}_{\gamma_Q} \cong \mathbb{Z}_p^{m+k}$ and $G/\gamma_1(Q)$ is elementary q-abelian. According to Proposition 3.11, $G \cong \mathbb{Z}_p^{m+k} \rtimes_\rho \mathbb{Z}_q^n$. According to Lemma 3.6, $Z(G) = 1$, so $\ker(\rho) \leq Z(G) = 1$ and then the action ρ is faithful. □

Let us consider the case $\sigma_Q \wedge \gamma_Q = 0_Q$.

Theorem 3.14. *Let $Q \in \mathcal{LSS}(p^m, q^n, \sigma_Q)$ and $\sigma_Q \wedge \gamma_Q = 0_Q$.*

(i) *There exists an extraspecial q-group K and a faithful action $\rho : K \longrightarrow GL_{m+k}(p)$ such that*

$$\mathrm{Dis}(Q) \cong \mathbb{Z}_p^{m+k} \rtimes_\rho K \tag{5}$$

for some $k \leq m$ and if $h \in \gamma_1(\mathrm{Dis}(Q))$ has order q then there exists $c_a \in [a]$ such that $h \in \mathrm{Dis}(Q)_{c_a}$ for every $[a] \in Q/\gamma_Q$.

(ii) *$p^m = 1 \pmod q$ and n is even.*

(iii) *If q is odd then $\exp(K) = q$.*

Proof. (i) Let $G = \mathrm{Dis}(Q)$. As in Theorem 3.13 we have that $\gamma_2(G)$ is elementary p-abelian, $G/\gamma_1(Q)$ is elementary q-abelian and $\gamma_1(G)$ is a maximal characteristic subgroup of G. According to Lemma 3.12, $\gamma_2(G) \lneqq \gamma_1(G)$. So we can apply Proposition 3.11 to G: then $G \cong \gamma_2(G) \rtimes_\rho K$ where K is a special q-group and $Z(K) \cong \gamma_1(G)/\gamma_2(G)$. Moreover $\ker(\rho) \cap Z(K) \leq Z(G) = 1$. The group K is nilpotent, so $\ker(\rho) = 1$, i.e. ρ is faithful.

The automorphism group of a block is $\mathrm{Aut}([a]) = \mathbb{Z}_p^m \rtimes \mathbb{Z}_{p^m-1}$ and the only fixed-point-free automorphisms have order p. So, every element of order q of $\gamma_1(G)$ fixes an element for every block of γ_Q. The element $h \in Z(K)$ has order q and so $h \in \mathrm{Dis}(Q)_{c_a}$ for some $c_a \in [a]$ for every $[a] \in Q/\gamma_Q$. Consider the map

$$\phi : Z(K) \longrightarrow \mathrm{Aut}([b])_{c_b} \cong \mathbb{Z}_{p^m-1}, \quad h \mapsto h|_{[b]}.$$

If $\phi(h) = h|_{[b]} = 1$ then h fixes $[b]$ and c_a for some $[a] \neq [b]$. By Remark 2.3 $Q = \mathrm{Sg}(c_a, [b])$, then $h = 1$ and so ϕ is an embedding. Therefore $Z(K)$ is cyclic and so K is a extraspecial q-group.

The inequality $k \leq m$ follows by Lemma 3.1(iv).

(ii) Since $Z(K)$ embeds into $\mathbb{Z}_{p^m-1}$ then q divides $p^m - 1$ and since K is an extraspecial q-group, n is even.

(iii) Using the coset representation over the diplacement group we have that $Q = \mathcal{Q}(G, \mathrm{Fix}(f), f)$ and the induced automorphism $f_{\gamma_1(G)}$ acts irreducibly on $G/\gamma_1(G) \cong K/Z(K)$. Let q be odd and let the exponent of K be q^2. According to [27, Corollary 1], then $\mathrm{Fix}(f_{\gamma_1(G)}) \neq 1$, contradiction. □

The equivalence σ_Q is controlled by the properties of the action of Dis_{γ_Q}.

Lemma 3.15. *Let $Q \in \mathcal{LSS}(p^m, q^n, \sigma_Q)$ and $\gamma_Q \wedge \sigma_Q = 0_Q$. The following are equivalent*:

(i) $\sigma_Q \neq 0_Q$.

(ii) $\left(\mathrm{Dis}_{\gamma_Q}\right)_a = 1$ *for every* $a \in Q$.

Proof. (i) $\Rightarrow$ (ii) Let $\sigma_Q \neq 0_Q$ and $b \,\sigma_Q\, a$ such that $b \notin [a]_{\gamma_Q}$. Therefore, $\left(\mathrm{Dis}_{\gamma_Q}\right)_a = \left(\mathrm{Dis}_{\gamma_Q}\right)_b$ and $\left(\mathrm{Dis}_{\gamma_Q}\right)_a$ fixes $[a]$ and b which generate Q by Remark 2.3. Hence $\left(\mathrm{Dis}_{\gamma_Q}\right)_a = 1$.

(ii) $\Rightarrow$ (i) If $\left(\mathrm{Dis}_{\gamma_Q}\right)_a = 1$ then, according to Theorem 3.14(i) $\mathrm{Dis}(Q)_a \cong \mathbb{Z}_q$ and it fixes some $c_b \in [b]$ for every block of γ_Q. So $\mathrm{Dis}(Q)_a = \mathrm{Dis}(Q)_{c_b}$, i.e. $\sigma_Q \neq 0_Q$. □

Note that if $\sigma_Q \neq 0_Q$ then $\mathrm{Dis}_{\gamma_Q} \cong \mathbb{Z}_p^m$ and so it has the minimal admitted size. On the other extreme, i.e. when the size of Dis_{γ_Q} is maximal, we have the following.

Proposition 3.16. *Let $Q \in \mathcal{LSS}(p^m, q^n, 0_Q)$. If $\mathrm{Dis}_{\gamma_Q} \cong \mathbb{Z}_p^{2m}$ then $\mathrm{Sg}(a, b) \cong Q/\gamma_Q$ whenever $[a] \neq [b]$ and Q is latin.*

Proof. Let $[a] \neq [b]$. The subgroup $\left(\mathrm{Dis}_{\gamma_Q}\right)_{a,b}$ fixes $[a]$ and b that form a set of generators of Q (see Remark 2.3). Therefore $\left(\mathrm{Dis}_{\gamma_Q}\right)_{a,b} = 1$ and the action of $\left(\mathrm{Dis}_{\gamma_Q}\right)_a \cong \mathbb{Z}_p^m$ restricted to $[b]$ is regular. In particular, for every $c \in [a]$ and $d \in [b]$ there exist $g \in \left(\mathrm{Dis}_{\gamma_Q}\right)_a$, $g' \in \left(\mathrm{Dis}_{\gamma_Q}\right)_b$ such that $c = g'(a_1)$ and $d = g(a_2)$ and so $\mathrm{Sg}(a, b) \cong gg'\mathrm{Sg}(a, b) = \mathrm{Sg}(c, d)$.

According to Theorem 3.14(i), if $h \in \gamma_1(\mathrm{Dis}(Q))$ has order q there exists $c_a \in [a]$ such that $h(c_a) = c_a$ for every block of γ_Q. If $Q = \mathrm{Sg}(a, b)$ then $\mathrm{Sg}(c_a, c_b) = Q$. Therefore h fixes a set of generators of Q and so $h = 1$, contradiction. Then according to Corollary 2.5, $\mathrm{Sg}(a, b) \cong Q/\gamma_Q$ whenever $[a] \neq [b]$. A finite quandle in which every pair of elements generates a latin subquandle is latin, so Q is latin. □

The classes $\mathcal{LSS}(p, q^n, \sigma_Q)$. In this section we turn our attention to the case $m = 1$.

Lemma 3.17. *Let $Q \in \mathcal{LSS}(p^m, q^n, \sigma_Q)$.*

(i) *If $n = 1$ then $\gamma_Q \leq \sigma_Q$.*

(ii) *If $m = 1$ then $\mathrm{Dis}_{\gamma_Q} \cong \mathbb{Z}_p^2$ and $\sigma_Q \neq 1_Q$.*

Proof. (i) Let $G = \mathrm{Dis}(Q)$. According to Proposition 3.7, $\gamma_1(G) = \gamma_2(G)$ since $\mathrm{Dis}(Q/\gamma_Q) \cong G/\gamma_1(G)$ is cyclic [13]. So by Lemma 3.12, $\gamma_Q \leq \sigma_Q$.

(ii) The congruence γ_Q is not central and so according to [4, Lemma 5.4] Dis_{γ_Q} is not cyclic. The subgroup Dis_{γ_Q} embeds into $\mathbb{Z}_p^2$ and then Dis_{γ_Q} has size p^2. In particular Q is not principal, since $\mathrm{Dis}(Q)_a$ is non-trivial. □

By virtue of Lemma 3.17(ii), if $Q \in \mathcal{LSS}(p, q^n, \sigma_Q)$, then either $\sigma_Q = \gamma_Q$ or $\sigma_Q \wedge \gamma_Q = 0_Q$. In both cases, we can give some further conditions on σ_Q, q and n (we are using the results collected in Appendix 7).

Proposition 3.18. *Let $Q \in \mathcal{LSS}(p, q^n, \sigma_Q)$ and $p > 2$.*

(i) *If $\sigma_Q = \gamma_Q$ then $q > 2$ and $n = 1$.*
(ii) *If $\sigma_Q \wedge \gamma_Q = 0_Q$ then $\sigma_Q = 0_Q$ and $q = 2$.*

Proof. (i) By virtue of Theorem 3.13 and Lemma 3.17(ii), $\mathrm{Dis}(Q) = G \cong \mathbb{Z}_p^2 \rtimes_\rho \mathbb{Z}_q^n$ where ρ is a faithful action. Then q divides $p^2 - 1$. Since $\sigma_Q = \gamma_Q$ then $N(\mathrm{Dis}(Q)_a) = \gamma_1(\mathrm{Dis}(Q))$ for every $a \in Q$.
If q divides $p - 1$ or $q = 2$ then the action of $\mathbb{Z}_q^n$ is diagonalizable (see Lemma 7.1) and then $\mathbb{Z}_q^n$ embeds into the subgroup of diagonal matrices of order q (see Lemma 7.1(i)). The subgroup of diagonal matrices of order q has size q^2, then $n \leq 2$. If $n = 2$ then there exists $h \in \mathbb{Z}_q^2$ such that $\rho(h) = kI$ and so $h \in N(\mathrm{Dis}(Q)_a)$, contradiction. Hence $n = 1$ and $q > 2$ since the two elements quandle is not connected.
If $q > 2$ divides $p+1$ then by Lemma 7.1(ii) $\rho(\mathbb{Z}_q^n) \cong \mathbb{Z}_q^n$ is abelian and then cyclic, i.e. $n = 1$.
(ii) The equivalence σ_Q is trivial by virtue of Lemma 3.17(ii) and Lemma 3.15. According to Theorem 3.14 then $\mathrm{Dis}(Q) \cong \mathbb{Z}_p^2 \rtimes_\rho K$ where K is an extraspecial q-group and ρ is faithful. According to Lemma 7.2 we have $q = 2$. □

According to Lemma 3.17 and Proposition 3.18, the smallest examples of faithful LSS subdirectly irreducible quandles are in the classes $\mathcal{LSS}(p, q, \gamma_Q)$ and $\mathcal{LSS}(p, 4, 0_Q)$.

EXAMPLE 3.19. Let p be a prime. According to Lemma 3.17(ii) and Proposition 3.18, if $Q \in \mathcal{LSS}(p, 2^n, \sigma_Q)$ then $\sigma_Q = 0_Q$ and according to Theorem 3.14, n is even. So the class $\mathcal{LSS}(p, 8, \sigma_Q)$ is empty.
If $Q \in \mathcal{LSS}(8, p, \sigma_Q)$ then $\gamma_Q \leq \sigma_Q$ by Lemma 3.17(i). So we can apply Theorem 3.13 and we have that $\mathrm{Dis}(Q) \cong \mathbb{Z}_2^{3+k} \rtimes_\rho \mathbb{Z}_p$ for $k \leq 3$. Then p divides $|GL_{3+k}(2)|$ and so $p \in \{7, 31\}$. An exhaustive GAP computer search on the groups of the form $\mathbb{Z}_2^{3+k} \rtimes \mathbb{Z}_p$ and their automorphisms for $0 \leq k \leq 3$ and $p \in \{7, 31\}$ shows that there are no such quandles.

Using the results of this section and that simple latin quandles are affine of prime power size, we can prove that latin quandles of size $8p$ where p is a prime are affine.

Theorem 3.20. *Let p be a prime. Latin quandles of size $8p$ are affine.*

Proof. A computer search on the RIG library of GAP reveals that the claim is true for $p \leq 5$ and that latin quandles of size 8 are strictly simple and so affine.
Let $p > 5$. There are no connected quandles of size 2 and of size $2p$ for $p > 5$ [21]. So the quandle Q has no factor or subquandle of size 2 and $2p$. In particular the blocks of the congruences of Q can not be 2 or $2p$ and so Q has no factor of size $4p$ or 4. Simple factors of Q have prime power size, so they have either size 8 or p.
Assume that α and β are maximal congruences of Q and $\gamma = \alpha \wedge \beta$. According to Lemma 2.6, $Q/\gamma \cong Q/\alpha \times Q/\beta$. The size of Q/γ divides $8p$ and so necessarily $|Q/\alpha \times Q/\beta| = 8p$ and so Q is the direct product of affine quandles and then affine.
Assume that Q has a unique maximal congruence α. The blocks of α have size either

8 or p, so α is also minimal. Thus Q has a unique proper congruence with strictly simple blocks and strictly simple factor. Hence Q is an LSS subdirectly irreducible quandle, i.e. $Q \in \mathcal{LSS}(8, p, \sigma_Q)$ or $Q \in \mathcal{LSS}(p, 8, \sigma_Q)$. According to Example 3.19 such classes are empty. □

For the quandles in $\mathcal{LSS}(p, 2^{2n}, 0_Q)$ we can also compute the order of the left multiplications. Recall that strictly simple quandles have an affine representation over finite fields given by $\mathrm{Aff}(\mathbb{F}_q, \lambda)$ where $\lambda \in \mathbb{F}^* \setminus \{1\}$. In particular the cycles of the bijection $x \mapsto \lambda x$ have all length equal to the multiplicative order of λ.

Proposition 3.21. *Let $Q \in \mathcal{LSS}(p, 2^{2n}, 0_Q)$ and let k be the order of the left multiplications of Q/γ_Q. Then $|L_a| = k$ for every $a \in Q$ and $p = 1 \pmod{k}$.*

Proof. Let $Q = Q(G, H, f)$ where $G = \mathrm{Dis}(Q)$, $f = \widehat{L_a}$ and $H = \mathrm{Fix}(f)$. Let $b \notin [a]$. According to Theorem 3.14 $G \cong \gamma_2(G) \rtimes K \cong \mathbb{Z}_p^2 \rtimes K$ where K is an extraspecial q-group. By Proposition 3.16, $\mathrm{Sg}(a, b) \cong Q/\gamma_Q$ and then $|b^{L_a}| = |[b]^{L_{[a]}}| = k$, since all the cycles of $L_{[a]}$ have equal length. The block $[a]$ is isomorphic to $\mathrm{Aff}(\gamma_2(G)/\gamma_2(G)_a, f|_{\gamma_2(G)}) \cong \mathrm{Aff}(\mathbb{Z}_p, t)$ for some $t \in \mathbb{Z}_p^* \setminus \{1\}$. So the restriction of f to $\gamma_2(G)$ is diagonalizable with eigenvalues 1 and $t \neq 1$. We denote by F the matrix with respect to a basis of eigenvectors. The center of K is fixed by $f_{\gamma_2(G)}$ and its induced mapping over $K/Z(K) \cong G/\gamma_1(G)$ is $f_{\gamma_1(G)}$. Then according to Lemma 1.2 the order of $f_{\gamma_2(G)}$ and the order of $f_{\gamma_1(G)}$ coincide and so $f^k_{\gamma_2(G)}(x) = x$ for every $x \in K$ and we have

$$\rho_{f^k_{\gamma_2(G)}(x)} = F^k \rho_x F^{-k} = \rho_x. \tag{6}$$

Thus, $\rho(K)$ centralizes the diagonal matrix F^k with entries 1 and t^k. If $t^k \neq 1$, according to Lemma 7.1(i), $K \cong \rho(K)$ is a subgroup of the diagonal matrices and so abelian, contradiction. Thus $t^k = 1$.

Accordingly, $p - 1 = 0 \pmod{k}$ and $|b^{L_a}|$ divides k whenever $b \in [a]_\alpha$. Therefore $|L_a| = \text{l.c.m.}\{|b^{L_a}| \mid b \in Q\} = k$ for every $a \in Q$. □

4. Connected quandles of size *pq*

A complete description of connected quandles of size p^2 is provided in [15]. In this section we give a complete classification of non-simple connected quandles of size pq where p and q are different primes. As we shall see, they are LSS and so we can apply the results of the previous section.

First of all note that all connected quandles of size pq are faithful.

Lemma 4.1. *Connected quandles of size pq are faithful.*

Proof. According to [6, Theorem 1.1] if Q is connected, then Q/λ_Q has not prime size. If $|Q| = pq$ every factor of Q has prime size, so λ_Q is trivial. □

Using that every factor and the blocks of every proper congruence have prime size, it is easy to show that the congruence lattice of connected quandles of size pq is one of the lattices in Figure 1. In particular, every factor is strictly simple and connected, and so we can characterize subdirectly reducible quandles of size pq using Lemma 2.6.

Proposition 4.2. *Let p, q be different primes and let Q be a connected quandle Q of size pq. The following are equivalent*:

(i) *Q is subdirectly reducible.*
(ii) *$Q \cong \mathrm{Aff}(\mathbb{Z}_p, f) \times \mathrm{Aff}(\mathbb{Z}_q, g)$ for some $f \in \mathbb{Z}_p^* \setminus \{1\}$ and $g \in \mathbb{Z}_q^* \setminus \{1\}$.*

In particular, there are $(p-2)(q-2)$ isomorphism classes of such quandles.

Note that quandles in Proposition 4.2 are connected subdirectly reducible LSS quandles as described in Theorem 2.7.

Let us consider the subdirectly irreducible case. Arguing as in Proposition 3.1(i), we see that the unique proper congruence is γ_Q and the blocks have prime size. According to [13] the blocks are either connected or projection.

Proposition 4.3. *Let Q be a non-simple subdirectly irreducible connected quandle of size pq.*

(i) *If the blocks of γ_Q are projection then $Q \in \mathcal{LSS}(2, 3, \gamma_Q)$.*
(ii) *If the blocks of γ_Q are connected then $Q \in \mathcal{LSS}(p, q, \gamma_Q)$ and $p^2 = 1 \pmod q$.*

Proof. (i) The quandle Q is a faithful connected extension of a strictly simple quandle of prime size by a projection quandle of prime size. Then [4, Theorem 5.8(i)] applies and so $|Q| = 6$ and $Q \in \mathcal{LSS}(2, 3, \gamma_Q)$.

(ii) The quandle Q is a LSS quandle and $Q \in \mathcal{LSS}(p, q, \gamma_Q)$ according to Lemma 3.17. By Theorem 3.13, $\mathrm{Dis}(Q) \cong \mathbb{Z}_p^2 \rtimes_\rho \mathbb{Z}_q$ and so q divides $|GL_2(p)| = p(p^2 - 1)$. □

From now on we focus on the classes $\mathcal{LSS}(p, q, \gamma_Q)$ with $p \geq 3$. In particular, using the results in Appendix 7, we have that the isomorphism classes of the displacement groups of quandles in $\mathcal{LSS}(p, q, \gamma_Q)$ are the following:

- if $p = 1 \pmod q$

$$\mathcal{G}_+ = \langle \sigma, \tau, \epsilon,\ \sigma^p = \tau^p = \epsilon^p = [\tau, \sigma] = 1,\ \epsilon\sigma\epsilon^{-1} = \sigma^g, \epsilon\tau\epsilon^{-1} = \tau^{g^{-1}} \rangle,$$

  where g is a fixed element of order q of $\mathbb{Z}_p^*$.
- If $p = -1 \pmod q$

$$\mathcal{G}_- = \langle \sigma, \tau, \epsilon,\ \sigma^p = \tau^p = \epsilon^p = [\tau, \sigma] = 1,\ \epsilon\sigma\epsilon^{-1} = \tau, \epsilon\tau\epsilon^{-1} = \sigma^{-1}\tau^{-\xi} \rangle,$$

  where $x^2 + \xi x + 1$ is an irreducible polynomial over $\mathbb{Z}_p$.

We show that there exists just two subdirectly irreducible connected quandles of size pq up to isomorphism using the isomorphism Theorem 1.3 and the description of the relevant automorphisms provided in Propositions 7.3 and 7.4.

Theorem 4.4. *Let $p, q \geq 3$ be primes such that $p = \pm 1 \pmod q$. The quandles $\mathfrak{Q}_a = \mathcal{Q}(\mathcal{G}_\pm, \mathrm{Fix}(f_a), f_a)$ where*

$$f_a = \begin{cases} f_a|_{\langle \sigma, \tau \rangle} = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}, \\ \epsilon \mapsto a\epsilon^{-1}, \end{cases}$$

for $a = 1, \sigma$ are the unique quandles in $\mathcal{LSS}(p, q, \gamma_Q)$ up to isomorphism. In particular, they are the unique non-affine latin quandles of size pq.

Proof. We need to prove that the $\{f_a \mid a = 1, \sigma\}$ is a set of representatives of conjugacy classes of automorphisms providing connected quandles over the groups $\mathcal{G}_\pm$ as described in Propositions 7.3 and 7.4.

Let $p = 1 \pmod q$. There are $p^2(p-1)$ automorphisms satisfying the conditions of Proposition 7.3. A direct computation in $\mathrm{Aut}(\mathcal{G}_+)$ shows that the centralizer of f_1 has size $2p(p-1)$ and the centralizer of f_σ has size $2(p-1)$. Therefore, f_1 and f_σ are not conjugate and

$$\begin{aligned}[\mathrm{Aut}(\mathcal{G}_+) : C_{\mathrm{Aut}(\mathcal{G}_+)}(f_1)] + [\mathrm{Aut}(\mathcal{G}_+) : C_{\mathrm{Aut}(\mathcal{G}_+)}(f_\sigma)] &= \frac{2p^2(p-1)^2}{2p(p-1)} + \frac{2p^2(p-1)^2}{2p} \\ &= p^2(p-1).\end{aligned}$$

Therefore f_1 and f_σ are the representatives of conjugacy classes of the desired automorphisms.

If $p = -1 \pmod q$ we can argue similarly, using Proposition 7.4.

It is easy to check that the right multiplication map

$$R_{\mathrm{Fix}(f_a)} : \mathcal{G}_\pm/\mathrm{Fix}(f_a) \longrightarrow \mathcal{G}_\pm/\mathrm{Fix}(f_a), \quad x\mathrm{Fix}(f_a) \mapsto x f_a(x)^{-1}\mathrm{Fix}(f_a)$$

is bijective and therefore the quandles $\mathfrak{Q}_a$ are latin. Simple latin quandle have size a power of a prime [4, 25], therefore $\mathfrak{Q}_1$ and $\mathfrak{Q}_\sigma$ are the unique non-affine latin quandles of size pq. □

According to the enumeration above, the (non-simple) connected subdirectly irreducible quandle of size $3p$ with $p > 2$ are the *Galkin quandles* defined in [9, 10].

As a byproduct we obtain the classification of non-associative Bruck loops of order pq already shown in [26], by virtue of the one-to-one correspondence between involutory latin quandles and Bruck loops of odd order [25]. Indeed $\mathfrak{Q}_1$ is the unique non-affine involutory latin quandle of size pq (note that the only involutory strictly simple quandles are $\mathrm{Aff}(\mathbb{Z}_p, -1)$ and so the unique subdirectly irreducible LSS involutory quandle is $\mathfrak{Q}_1$ as defined in Theorem 4.4).

Corollary 4.5. *Let $p, q \geq 3$ be primes such that $p^2 = 1 \pmod q$. There exists a unique non-associative Bruck loop of size pq up to isomorphism.*

5. Connected quandles of size $4p$

In this section we classify all non-simple connected quandles of size $4p$ and we show that all but a few small exceptions are examples of LSS connected quandles.

If $p > 5$ there are no connected quandles of size $2p$ [17, 21], so every factor of a connected quandle of size $4p$ has size either 4 or p and consequently also the blocks of congruences have size either 4 or p. Recall that there exists a unique connected quandle of size 4, i.e. the strictly simple quandle $\mathrm{Aff}(\mathbb{Z}_2^2, C)$ where

$$C = \begin{bmatrix} 0 & 1 \\ 1 & 1 \end{bmatrix}$$

and the order of C is 3. Therefore the congruence lattice of such quandles is one of the lattices in Figure 1.

Lemma 5.1. *Connected quandles of size* $4p$ *with* $p > 5$ *are faithful.*

Proof. Assume that Q is not faithful. Then Q/λ_Q has not prime size (see [6, Theorem 1.1]) and so Q/λ_Q is the unique connected quandle of size 4. According to [6, Example 8.3] the orbit with respect to $\mathrm{LMlt}(Q)$ of every element of Q has size 8, therefore Q has size 8 and $p = 2$. □

If Q is subdirectly reducible then it is a direct product (the same argument of Proposition 4.2 applies).

Proposition 5.2. *Let* Q *be a connected quandle of size* $4p$ *with* $p > 5$*. The following are equivalent*:

(i) Q *is subdirectly reducible.*
(ii) $Q \cong \mathrm{Aff}(\mathbb{Z}_2^2, C) \times \mathrm{Aff}(\mathbb{Z}_p, f)$ *for some* $f \in \mathbb{Z}_p^* \setminus \{1\}$.

In particular there are $p - 2$ *such quandles.*

We turn now out attention to the subdirectly irreducible case. In particular, if Q is a subdirectly irreducible connected quandle of size $4p$ with $p > 5$ then γ_Q is the unique congruence of Q (Q is not abelian and the unique factor of Q is affine and then abelian).

Proposition 5.3. *Let* Q *be a subdirectly irreducible connected quandle of size* $4p$*. If* $|Q/\gamma_Q| = p > 5$ *then* $p = 7$.

Proof. Let $G = \mathrm{Dis}(Q)$. Since $\mathrm{Dis}(Q/\gamma_Q)$ is cyclic and $\gamma_2(G) \leq \mathrm{Dis}_{\gamma_1(Q)} \leq \mathrm{Dis}^{\gamma_1(Q)} = \gamma_1(G)$, according to Proposition 3.7 we have $\gamma_2(G) = \mathrm{Dis}_{\gamma_Q} = \gamma_1(G)$.

The blocks of γ_Q are isomorphic to one of the homogeneous quandles of size 4: $\mathrm{Aff}(\mathbb{Z}_2^2, C)$, $\mathcal{P}_4$ or $\mathrm{Aff}(\mathbb{Z}_4, -1)$. Let us discuss all the possible cases according to the isomorphism class of the blocks of γ_Q:

(i) if they are are connected, then Q is LSS and we can apply Lemma 3.1(iv) and so the group $\gamma_1(G)$ embeds into $\mathbb{Z}_2^{2+k}$ for $k \leq 2$.
(ii) If the blocks of γ_Q are isomorphic to $\mathrm{Aff}(\mathbb{Z}_4, -1)$. Then $\gamma_1(G)|_{[a]}$ embeds into $\mathrm{Aut}([a]) \cong \mathbb{Z}_4 \rtimes \mathbb{Z}_2$, see [11, Theorem 2.1]. Therefore, $\gamma_1(G) = \mathrm{Dis}_{\gamma_Q}$ is solvable and so it is abelian by Lemma 1.5(i). Hence $\gamma_1(G)$ is regular on each block, so $|\gamma_1(G)|_{[a]}| = 4$ and then $\gamma_1(G)$ embeds into $\mathbb{Z}_4^2$ or into $\mathbb{Z}_2^{2+k}$ for $k \leq 2$.
(iii) If the blocks of γ_Q are projection subquandles, then by Lemma [4, Lemma 5.1] γ_Q is abelian and so also $\mathrm{Dis}_{\gamma_Q} = \gamma_1(G)$ is abelian and thus regular on each block of γ_Q. Therefore $|\gamma_1(G)|_{[a]}| = 4$, so $\gamma_1(G)$ embeds into $\mathbb{Z}_4^2$ or into $\mathbb{Z}_2^4$.

Hence, $\mathrm{Dis}(Q) \cong A \rtimes \mathbb{Z}_p$, and p divides the size of $\mathrm{Aut}(A)$ where $A = \mathbb{Z}_2^{2+k}$ or $A = \mathbb{Z}_4^k$ and $k \leq 2$. In the first case $p \in \{2, 3, 5, 7\}$ and in the second case $p \in \{2, 3\}$. □

A complete list of the subdirectly irreducible connected quandles of size 28 described in Proposition 5.3 is given in the following table (none of them is latin):

RIG	Dis(Q)	Class
(28,3)	$\mathbb{Z}_2^3 \rtimes \mathbb{Z}_7$	$\mathcal{LSS}(4, 7, \gamma_Q)$
(28,4)	$\mathbb{Z}_2^3 \rtimes \mathbb{Z}_7$	$\mathcal{LSS}(4, 7, \gamma_Q)$
(28,5)	$\mathbb{Z}_2^3 \rtimes \mathbb{Z}_7$	$\mathcal{LSS}(4, 7, \gamma_Q)$
(28,6)	$\mathbb{Z}_2^3 \rtimes \mathbb{Z}_7$	$\mathcal{LSS}(4, 7, \gamma_Q)$

Let us consider the case in which Q/γ_Q is the unique connected quandle of size 4, i.e. Aff$(\mathbb{Z}_2^2, C)$.

Proposition 5.4. *Let $p > 5$ be a prime and Q be a connected subdirectly irreducible quandle of size $4p$ such that $|Q/\gamma_Q| = 4$. Then*:

(i) $Q \in \mathcal{LSS}(p, 4, 0_Q)$.
(ii) $\mathrm{Dis}(Q) \cong \mathbb{Z}_p^2 \rtimes_\rho \mathcal{Q}_8$ *where ρ is a faithful action.*
(iii) Q *is latin, $L_a^3 = 1$ for every $a \in Q$ and $p = 1 \pmod 3$.*

Proof. (i) The blocks of γ_Q are homogeneous quandles of prime size. So they are either projection or connected. In the first case the quandle Q is a connected faithful extension of a strictly simple factor by a prime size projection quandle. So the size of Q is either 6 or 12 according to [4, Theorem 5.8]. Therefore the blocks are connected strictly simple quandle and then $Q \in \mathcal{LSS}(p, 4, \sigma_Q)$. According to Lemma 3.17(ii) and to Proposition 3.18 then $\sigma_Q = 0_Q$.

(ii)-(iii) By Theorem 3.14 and Lemma 3.17(ii), $\mathrm{Dis}(Q) \cong G = \mathbb{Z}_p^2 \rtimes_\rho K$ where K is an extraspecial 2-group of size 8 and ρ is a faithful action.

Let $f = \widehat{L_a}$. According to Lemma 1.2 and Lemma 3.21 $|f| = |L_a| = |L_{[a]}| = 3$ for every $a \in Q$ and $p = 1 \pmod 3$. So, the automorphism $f_{\gamma_2(G)} \in \mathrm{Aut}(K)$ has also order 3. The automorphisms group of $\mathcal{D}_8$ has size 8, then it has no element of order 3, so $K \cong \mathcal{Q}_8$.

Finally, Q is latin by Proposition 3.16. □

According to [22] there exists a unique faithful representation of degree 2 of the quaternion group

$$\mathcal{Q}_8 = \langle x, y, z \,|\, x^2 = y^2 = [x, y] = z,\ z^2 = [z, y] = [z, x] = 1 \rangle.$$

Let p be a prime such that $p = 1 \pmod 3$ and let $k \in \mathbb{Z}_p^*$ be an element of order 3. We define the action ρ by setting

$$\rho_x = \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix}, \quad \rho_y = \begin{bmatrix} k^2 & k \\ k & -k^2 \end{bmatrix}, \quad \rho_z = \begin{bmatrix} -1 & 0 \\ 0 & -1 \end{bmatrix}.$$

and we denote by $\mathcal{G}_k = \mathbb{Z}_p^2 \rtimes_\rho \mathcal{Q}_8$ the correspondent semidirect product.

According to the isomorphism Theorem 1.3, in order to classify subdirectly irreducible connected quandles of size $4p$, or equivalently the quandles in the classes $\mathcal{LSS}(p, 4, 0_Q)$, we need to compute conjugacy classes of automorphisms of $\mathcal{G}_k$ providing connected quandles. A complete description of the automorphisms of such group is given in Appendix 7 and the suitable automorphisms are described in Proposition 7.6.

Theorem 5.5. *Let $p > 5$ be a prime such that $p = 1 \pmod 3$. The quandles $\mathfrak{Q}_j = \mathcal{Q}(\mathcal{G}_k, \mathrm{Fix}(f_j), f_j)$ where*

$$f_j = \begin{cases} x \mapsto y, \quad y \mapsto xy, \quad z \mapsto z, \quad f_j|_{\gamma_1(\mathcal{G}_k)} = \begin{bmatrix} 1+k^j & -k(1+k^j) \\ k^2(1+k^j) & 0 \end{bmatrix} \end{cases}$$

and $j = 1, 2$ are the unique quandles in $\mathcal{LSS}(p, 4, 0_Q)$ up to isomorphism. In particular, they are the unique non-affine latin quandles of size $4p$.

Proof. According to Theorem 1.3 we need to compute the conjugacy classes of automorphisms as in Proposition 7.6. The number of such automorphisms is $16p$ according to Lemma 7.7. The automorphisms f_1 and f_2 are not conjugate, since their restriction to $\gamma_2(\mathcal{G}_k)$ have different trace. Then using Lemma 7.8 we have

$$\frac{|\mathrm{Aut}(\mathcal{G}_k)|}{|C_{\mathrm{Aut}(\mathcal{G}_k)}(f_1)|} + \frac{|\mathrm{Aut}(\mathcal{G}_k)|}{|C_{\mathrm{Aut}(\mathcal{G}_k)}(f_2)|} = 2\frac{24p^2(p-1)}{3p(p-1)} = 16p.$$

Hence f_1, f_2 are the representative of the conjugacy classes of the desired automorphisms.

Since simple latin quandles have prime power size, $\mathfrak{Q}_j$ with $j = 1, 2$ are the unique non-affine latin quandles of size $4p$ (a GAP computer search reveals that for $p \leq 5$ latin quandles of size $4p$ are affine). □

Abelian extensions of the four-elements latin quandle. Let Q be a connected quandle, $a \in Q$ and $\alpha \in \mathrm{Con}(Q)$. Then Q is isomorphic to $Q/\alpha \times_\beta [a] = (Q/\alpha \times [a], *)$ where $(b, s) * (c, t) = (b * c, \beta(b, c, s)(t))$ and $\beta : Q \times Q \times [a] \to \mathrm{Sym}([a])$ is called *dynamical cocycle* (the permutations $\beta(b, c, s)$ satisfy suitable conditions, see [1, Section 2]). Moreover for every $\gamma : Q \to \mathrm{Sym}(S)$, the mapping

$$\sigma : Q/\alpha \times Q/\alpha \times [a] \longrightarrow \mathrm{Sym}_{[a]}, \quad (b, c, s) \mapsto \gamma(b * c)\beta(b, c, \gamma(b)^{-1}(s))\gamma(c)^{-1}$$

is a dynamical cocycle and $Q \times_\beta S \cong Q \times_\sigma S$.

We turn our attention to a particular family of cocycles. An *abelian cocycle* of Q with coefficients in an abelian group A is a triple $\beta = (\psi, \phi, \theta)$ where $\psi : Q \times Q \to \mathrm{Aut}(A)$, $\phi : Q \times Q \to \mathrm{End}(A)$ and $\theta : Q \times Q \to A$ satisfy the following conditions:

$$\begin{aligned} \psi_{a,b*c}(\theta_{b,c}) + \theta_{a,b*c} &= \psi_{a*b,a*c}(\theta_{a,c}) + \phi_{a*b,a*c}(\theta_{a,b}) + \theta_{a*b,a*c}, \\ \phi_{a,b*c} &= \phi_{a*b,a*c}\phi_{a,b} + \psi_{a*b,a*c}\phi_{a,c}, \\ \psi_{a,b*c}\psi_{b,c} &= \psi_{a*b,a*c}\psi_{a,c}, \\ \psi_{a,b*c}\phi_{b,c} &= \phi_{a*b,a*c}\psi_{a,b}, \\ \phi_{a,a} + \psi_{a,a} &= 1, \\ \theta_{a,a} &= 0. \end{aligned} \tag{CC}$$

We call such conditions *cocycle conditions* and the quandle $Q \times_\beta A$ where $\beta(a, b, s)(t) = \phi_{a,b}(s) + \psi_{a,b}(t) + \theta_{a,b}$ for every $a, b \in Q/\alpha$ and $s, t \in A$ is called *abelian extension of Q* (in the literature this construction is also known as *quandle modules* [1]).

If Q is latin, $u \in Q$ and $\beta = (\phi, \psi, \theta)$ is an abelian cocycle we can define $\gamma(a) = \psi^{-1}_{a/u,u}$ for every $a \in Q$ in order to construct an abelian cocycle as follows:

$$\begin{aligned} \sigma(u)(a, b, s)(t) &= \gamma(a * b)\left(\phi_{a,b}\gamma(a)^{-1}(s) + \psi_{a,b}\gamma(b)^{-1}(t) + \theta_{a,b}\right) = \\ &= \underbrace{\phi^{-1}_{(a*b)/u),u}\phi_{a,b}\psi_{a/u,u}(s)}_{\phi(u)_{a,b}(s)} + \underbrace{\psi^{-1}_{(a*b)/u,u}\psi_{a,b}\psi_{b/u,u}(t)}_{\psi(u)_{a,b}(t)} + \underbrace{\psi^{-1}_{(a*b)/u,u}(\theta_{a,b})}_{\theta(u)_{a,b}}. \end{aligned}$$

In particular, $Q \times_{\sigma(u)} A$ is isomorphic to $Q \times_\beta A$. We call $\sigma(u) = (\psi(u), \phi(u), \theta(u))$ a *u-normalized cocycle*.

Using the same techniques developed in [6] it can be shown that normalized cocycles with coefficients in $\mathbb{Z}_p$ have some special properties, taking also advantage from the fact that the automorphism group of $\mathbb{Z}_p$ is abelian (all the computations are straightforward manipulation of the cocycle conditions and then omitted). We define $g, f, h : Q \times Q \longrightarrow Q \times Q$ as:

$$g : (a,b) \to (u * a, u * b), \quad f : (a,b) \to (a * (b/u), a * u), \quad h : (a,b) \to ((b/(u\backslash a)) * a, b).$$

These mappings are permutations of $Q \times Q$ [6, Section 4].

Proposition 5.6. *Let Q be a latin quandle and $\beta = (\psi, \phi, \theta)$ a u-normalized abelian cocycle with coefficients in $\mathbb{Z}_p$. Then*:

(i) $\psi_{a,u} = \psi_{u,a} = \psi_{u,u} = \psi_{a,a}$;
(ii) $\psi_{k(a,b)} = \psi_{a,b}$,

for every $a, b \in Q$ and every $k \in \langle f, g, h\rangle$.

Applying Proposition 5.6 to the unique connected quandle of size 4, $Q = \mathrm{Aff}(\mathbb{Z}_2^2, C)$ we have that 0-normalized cocycles of Q have the following form

$$\psi = \begin{bmatrix} \lambda & \lambda & \lambda & \lambda \\ \lambda & \lambda & \mu & \mu \\ \lambda & \mu & \lambda & \mu \\ \lambda & \mu & \mu & \lambda \end{bmatrix}, \quad \phi = \begin{bmatrix} 1-\lambda & \phi_0 & \phi_0 & \phi_0 \\ \phi_1 & 1-\lambda & \phi_2 & \phi_3 \\ \phi_1 & \phi_3 & 1-\lambda & \phi_2 \\ \phi_1 & \phi_2 & \phi_3 & 1-\lambda \end{bmatrix}, \tag{7}$$

where $\lambda, \mu \in \mathbb{Z}_p^*$ and $\phi_i \in \mathbb{Z}_p$ for $0 \le i \le 3$. Starting from (7) and using the cocycle conditions (CC) we have the following.

Proposition 5.7. *Let $\beta = (\phi, \psi, \theta)$ be an abelian 0-normalized cocycle of $Q = \mathrm{Aff}(\mathbb{Z}_2^2, C)$ with coefficients in $\mathbb{Z}_p$. Then $\psi_{a,b} = \lambda$ and $\phi_{a,b} = 1 - \lambda$ for every $a, b \in Q$ for some $\lambda \in \mathbb{Z}_p^*$.*

If an abelian cocycle β is as in Proposition 5.7, then the kernel of the canonical projection $Q \times_\beta A \longrightarrow Q$ is a central congruence [5, Proposition 7.5]. Therefore subdirectly irreducible latin quandles of size $4p$ are not abelian extensions of $\mathrm{Aff}(\mathbb{Z}_2^2, C)$.

6. Non connected LSS quandles

In this section we study non connected LSS quandles. Every subset of a projection subquandle is a subquandle, so LSS projection quandle have size 2 or 3. From now on we consider just non-projection quandles.

Lemma 6.1. *Let Q be a finite non-connected non-projection LSS quandle. Then* $\mathrm{Dis}(Q)$ *has* 2 *orbits.*

Proof. If $\mathrm{Dis}(Q)$ has at least 3 orbits, then the union of any pair of them is a non-connected subquandle of Q and so it has size 2. Then the union of the three orbits is a projection subquandle of size 3, and so $Q = \mathcal{P}_3$. □

Let us denote the orbits of $\mathrm{Dis}(Q)$ by Q_1, Q_2 and their mutual actions by

$$\rho_1 : Q_1 \to \mathrm{Conj}(\mathrm{Aut}(Q_2)), \quad \rho_2 : Q_2 \to \mathrm{Conj}(\mathrm{Aut}(Q_1)),$$

where ρ_i are morphisms of quandles and

$$x * a = \rho_1(x)(a), \quad a * x = \rho_2(a)(x),$$

for every $x \in Q_1$ and $a \in Q_2$. In particular the action need to satisfy

$$\rho_1(\rho_2(a)(x)) = L_a \rho_1(x) L_a^{-1}, \quad \rho_2(\rho_1(x)(a)) = L_x \rho_2(a) L_x^{-1}, \tag{8}$$

for every $x \in Q_1$ and $a \in Q_2$, see [1, Lemma 1.18]. The orbits are subquandles, and so we have that either $|Q_i|$ is 1 or 2 or Q_i is a connected strictly simple quandle. We need to discuss all the possible cases. In the following we are using the affine representation of $\mathcal{P}_2$ as $\mathrm{Aff}(\mathbb{Z}_2, 1)$.

Proposition 6.2. *Let $Q = Q_1 \cup Q_2$ be a finite non-connected non-projection LSS quandle. If Q_1 and Q_2 are projection subquandles, then Q is one of the following*:

$$R = \begin{bmatrix} 1 & 3 & 2 \\ 1 & 2 & 3 \\ 1 & 2 & 3 \end{bmatrix}, \qquad S = \begin{bmatrix} 1 & 2 & 4 & 3 \\ 1 & 2 & 4 & 3 \\ 2 & 1 & 3 & 4 \\ 2 & 1 & 3 & 4 \end{bmatrix}.$$

Proof. Let $x \in Q_1$ and $a \in Q_2$. If both the orbits are projection, then Q_1 is the orbit of x under the action of $\langle L_b,\ b \in Q_2 \rangle$ and so Q_1 is the orbit of x under the action of $\langle \rho_2(b),\ b \in Q_2 \rangle$ (dually Q_2 is the orbit of a under the action of $\langle \rho_1(y),\ y \in Q_1 \rangle$. According to (8) we have

$$\rho_1(\rho_2(a)(x)) = \rho_1(x), \quad \rho_2(\rho_1(x)(a)) = \rho_2(x),$$

for every $x \in Q_1$ and every $a \in Q_2$. So we have that ρ_1 and ρ_2 are constant mapping. If $|Q_1| = 1$ then we obtain R, if $|Q_1| = |Q_2| = 2$ we obtain S. □

Lemma 6.3. *Let $Q = Q_1 \cup Q_2$ be a finite non-connected non-projection LSS quandle.*

(i) *If $\rho_2(a) = 1$, for every $a \in Q_2$, then $|Q_1| = 1$.*
(ii) *If Q_1 is connected and $\rho_2(a) = f$ for every $a \in Q_2$ then $f = 1$.*

Proof. (i) Let $x \in Q_1$. If the action ρ_2 is trivial, then $\{x\} \cup Q_2$ is a subquandle of Q which contains Q_2 as a proper subquandle. Then $Q = \{x\} \cup Q_2$ and so $|Q_1| = 1$.

(ii) According to (8) we have that

$$f = \rho_2(\rho_1(x)(a)) = L_x \rho_2(a) L_x^{-1} = L_x f L_x^{-1}$$

i.e. f centralizes L_x for every $x \in Q_1$. Then $L_{f(x)} = f L_x f^{-1} = L_x$ for every $x \in Q_1$ and since Q_1 is faithful we have $f = 1$. □

Proposition 6.4. *Let $Q = Q_1 \cup Q_2$ be a finite non-connected non-projection LSS quandle. If Q_1 is a strictly simple connected quandle and Q_2 is projection, then Q is one of the following*:

(i) *$|Q_2| = 1$ and Q_2 acts trivially on Q_1.*
(ii) *$Q_1 = \mathrm{Aff}(\mathbb{Z}_p, -1)$, $Q_2 = \mathrm{Aff}(\mathbb{Z}_2, 1)$ and*

$$a * x = x + (-1)^a, \quad x * a = a + 1$$

for every $x \in Q_1$ and every $a \in Q_2$.

Proof. (i) Assume that $|Q_2| = 1$. Let $Q_1 = R$ and $Q_2 = \{a\}$ where R is a connected strictly simple quandle. So $L_a|_R = f \in \mathrm{Aut}(R)$ and so according to Lemma 6.3(ii) $f = 1$.

(ii) Assume that $|Q_2| = 2$ and that $Q_1 = \mathrm{Aff}(\mathbb{Z}_p^n, f)$ is a connected strictly simple quandle. So the image of ρ_1 has size 1 (Q_1 is simple and $\mathrm{Aut}(Q_2) \cong \mathbb{Z}_2$). By virtue of Lemma 6.3(i), $\rho_1(x)(a) = a + 1$ for every $x \in Q_1$ and every $a \in Q_2$. Let $\rho_2(a) = (\lambda_a, g_a) \in \mathrm{Aut}(Q_1) = \mathbb{Z}_p^n \rtimes C_{GL_n(p)}(f)$. Since

$$\rho_2(1) = \rho_2(\rho_1(x)(0)) = L_x \rho_2(0) L_x^{-1}$$
$$\rho_2(0) = \rho_2(\rho_1(x)(1)) = L_x \rho_2(1) L_x^{-1}$$

for all $x \in Q_1$, it follows that $g_0 = g_1 = 1$, $\lambda_1 = f(\lambda_0) = f^2(\lambda_1)$ and so $\lambda_0, \lambda_1 \neq 0$ by Lemma 6.3(i). Hence f has order 2, i.e. $f = -1$ and accordingly $n = 1$.

Let $Q(\lambda_0)$ be the quandle described above. The map:

$$\phi : Q(\lambda_0) \longrightarrow Q(1), \quad \begin{cases} 0 \mapsto 0, \\ 1 \mapsto 1, \\ x \mapsto x\lambda_0^{-1}, \text{ for every } x \in Q_1, \end{cases}$$

is an isomorphism. □

Proposition 6.5. *Let $Q = Q_1 \cup Q_2$ be a finite non-connected non-projection LSS quandle. If Q_1 and Q_2 are non-trivial strictly simple connected quandles then $|Q_1| = |Q_2|$.*

Proof. Assume that both Q_1 and Q_2 are connected strictly simple quandles. Then the size of the image of ρ_i is either 1 or equal to $|Q_i|$ for $i = 1, 2$. In the first case, according to Lemma 6.3 we have that $|Q_i| = 1$, contradiction. So we can assume that the mappings ρ_i are injective for $i = 1, 2$. According to [4, Proposition 4.5] the connected subquandles of $\mathrm{Aut}(Q_i)$ are of the form $\mathrm{Dis}(Q_i) \times \{h\}$ for $h \in \mathrm{Aut}(Q_i)_0$. So, $|Q_1| = |\mathrm{Dis}(Q_1)| = |\rho_1(Q_2)| = |Q_2|$. □

Example 6.6. Let $Q_1 = \mathrm{Aff}(\mathbb{Z}_p^n, f)$ and $Q_2 = \mathrm{Aff}(\mathbb{Z}_p^n, g)$ be strictly simple quandles. The actions defined by

$$\begin{aligned} \rho_1(y)(a) &= (1 - f)(y) + f(a), \\ \rho_2(b)(y) &= (1 - g)(b) + g(y), \end{aligned}$$

for every $x, y \in Q_1$ and every $a, b \in Q_2$ satisfy (8). Then for every pair of strictly simple quandles of the same size we can construct a quandle $Q = Q_1 \cup Q_2$ as in Proposition 6.5.

7. Appendix

Matrices and representations. We collect some basic results about matrices of rank 2 and faithful representations.

Lemma 7.1. *Let p, q be primes such that $p^2 = 1 \pmod q$ and let $A \in GL_2(p)$. If $|A| = q^n$ and $q > 2$ then*:

(i) *A is diagonalizable if and only if q divides $p - 1$. If A is not scalar then $C_{GL_2(p)}(A)$ is the subgroups of diagonal matrices.*

(ii) *A has no eigenvalues if and only if q divides $p + 1$. Moreover, $C_{GL_2(p)}(A)$ is cyclic.*

If $|A| = 2$ and $p > 2$ then A is diagonalizable.

Proof. The order of A divides the order of $GL_2(p)$ and so either q divides $p-1$ or q divides $p+1$. Consider the action of A on the set of 1-dimensional subspaces of $\mathbb{Z}_p^2$. Then

$$p + 1 = e + nq,$$

where e is the number of eigenspaces of A. So e can not be 1, and since $q > 2$, $e = 0$ if and only if q divides $p + 1$ and $e = 2$ if and only if q divides $p - 1$. If A is diagonalizable but not scalar a direct computation using a basis of eigenvectors of A shows that its centralizer is given by the diagonal matrices, and if A acts irreducibly the centralizer of A is cyclic according to [23, Theorem 2.3.5].

If the order of A is 2 then either A is diagonal or it has trace zero and determinant -1. So the eigenvalues of A are 1 and -1 and then A is diagonalizable. □

Lemma 7.2. *Let p, q be dinstinct primes, G be a an extraspecial q-group and $\rho : G \longrightarrow GL_2(p)$ be a faithful representation. Then $q = 2$.*

Proof. Assume that $q > 2$ and $z \in Z(G)$. Since $\rho(G) \leq C_{GL_2(p)}(\rho(z))$, if $\rho(z)$ is not scalar or $p = -1 \pmod q$, then according to Lemma 7.1 we have that $G \cong \rho(G)$ is abelian, contradiction. Hence $\rho_z = kI$ for $k \neq 1$ and $p = 1 \pmod q$ and ρ_x is diagonalizable for every $x \in G$. Let $x, y \in G$ such that $[x, y] = z$. Then, working out the condition $[\rho_x, \rho_y] = \rho_z = kI$ in a basis of eigenvectors of ρ_x it follows that $k = -1$ and so $q = |\rho_z| = 2$, contradiction. □

The non-abelian groups of size p^2q. A classification of the groups of order p^2q and their automorphisms is given in [8]. We focus on the non-abelian groups with $q > 2$, since we need such groups in order to construct connected quandles of size pq, so we assume that $p = \pm 1 \pmod q$ and $p \geq 2$.

Note that if G is a group, then every automorphism $f \in \mathrm{Aut}(G)$ induces an automorphism on the factor $G/\gamma_1(G)$. According to Lemma 3.1(ii), if $Q = Q(G, \mathrm{Fix}(f), f)$ is a connected quandle of size pq, then the factor $Q/\gamma_Q = \mathrm{Aff}(G/\gamma_1(G), f_{\gamma_1(G)})$ is also connected. In particular the induced automorphism $f_{\gamma_1(G)}$ is not trivial. According to the description given in [8] it is easy to identify the groups of size p^2q admitting such automorphism.

- If $p = 1 \pmod q$, then

  $$G \cong \mathcal{G}_+ = \langle \sigma, \tau, \epsilon,\ \sigma^p = \tau^p = \epsilon^p = [\tau, \sigma] = 1,\ \epsilon\sigma\epsilon^{-1} = \sigma^g, \epsilon\tau\epsilon^{-1} = \tau^{g^{-1}} \rangle,$$

  where g is a fixed element of order q of $\mathbb{Z}_p^*$.
- If $p = -1 \pmod q$, then

  $$G \cong \mathcal{G}_- = \langle \sigma, \tau, \epsilon,\ \sigma^p = \tau^p = \epsilon^p = [\tau, \sigma] = 1,\ \epsilon\sigma\epsilon^{-1} = \tau, \epsilon\tau\epsilon^{-1} = \sigma^{-1}\tau^{-\xi} \rangle,$$

  where $x^2 + \xi x + 1$ is an irreducible polynomial over $\mathbb{Z}_p$.

The next step is to identify the automorphisms of the groups listed above that provide connected quandles of size pq.

According to [8, Section 4.1 and 4.3],

$$\mathrm{Aut}(\mathcal{G}_+) \cong (\mathbb{Z}_p^2 \rtimes_\sigma (\mathbb{Z}_p^* \times \mathbb{Z}_p^*)) \rtimes_\rho \mathbb{Z}_2,$$

where $\sigma(a,b)(n,m) = (an, bm)$ and $\rho(1)((n,m),(a,b)) = ((-gm, -g^{-1}n),(b,a))$. In particular, the mapping

$$(\mathbb{Z}_p^2 \rtimes_\sigma (\mathbb{Z}_p^* \times \mathbb{Z}_p^*)) \rtimes_\rho \mathbb{Z}_2 \longrightarrow \mathrm{Aut}(\mathrm{Aut}(\mathcal{G})_+), \quad ((n,m),(a,b),i) \mapsto f_i = \begin{cases} f_i|_{\langle\sigma,\tau\rangle} = F_i \\ \epsilon \mapsto \sigma^n\tau^m\epsilon^{(-1)^i} \end{cases},$$

where

$$F_0 = \begin{bmatrix} a & 0 \\ 0 & b \end{bmatrix}, \quad F_1 = \begin{bmatrix} 0 & b \\ a & 0 \end{bmatrix},$$

is an isomorphism.

Proposition 7.3. *Let $p = 1 \pmod q$. The following are equivalent:*

(i) *$Q = \mathcal{Q}(\mathcal{G}_+, \mathrm{Fix}(f), f)$ is a connected quandle of size pq and $\mathrm{Dis}(Q) \cong \mathcal{G}_+$.*
(ii) *$f = ((n,m),(a,a^{-1}),1)$ for some $0 \le n, m \le p-1$ and $a \in \mathbb{Z}_p^*$.*

Proof. (i) $\Rightarrow$ (ii) Let $f = ((n,m),(a,b),i)$. The factor $Q/\gamma_Q = \mathrm{Aff}(\mathcal{G}_+/\gamma_1(\mathcal{G}_+), f_{\gamma_1(\mathcal{G}_+)})$ is connected, and so $f_{\gamma_1(\mathcal{G}_+)} = -1$, i.e. $i = 1$. Moreover $|\mathrm{Fix}(f)| = p$ and so $b = a^{-1}$.

(ii) $\Rightarrow$ (i) The size of $\mathrm{Fix}(f)$ is p and so $Q = \mathcal{Q}(\mathcal{G}_+, \mathrm{Fix}(f), f)$ has size pq. Since $\mathrm{Fix}(f) = \{\sigma^x\tau^y \mid y - ax = 0\}$ then $\mathrm{Core}_{\mathcal{G}_+}(\mathrm{Fix}(f)) = 1$. The subgroup $[\mathcal{G}_+, f]$ is generated by the set $T = \{gf(g)^{-1} \mid g \in \mathcal{G}_+\}$ of size pq. Since T is not a subgroup then $\langle T\rangle = [\mathcal{G}_+, f] = \mathcal{G}_+$. Therefore $\mathrm{Dis}(Q) = [\mathcal{G}_+, f] = \mathcal{G}_+$ and then Q is connected. □

Let M be the companion matrix of the irreducible polynomial $h(x) = x^2 + \xi x + 1$. The elements of $N_{GL_2(p)}(M)$ are of the form

$$F_+ = \begin{bmatrix} a & -b \\ b & a - \xi b \end{bmatrix}, \quad F_- = \begin{bmatrix} a & b \\ b + \xi a & -a \end{bmatrix},$$

for $a, b \in \mathbb{Z}_p$. According to [8, Section 4.1 and 4.4], the mapping

$$\mathbb{Z}_p^2 \rtimes N_{GL_2(p)}(M) \longrightarrow \mathrm{Aut}(\mathrm{Aut}(\mathcal{G})), \quad ((n,m), F_\pm) \mapsto f_\pm = \begin{cases} f_\pm|_{\langle\sigma,\tau\rangle} = F_\pm \\ \epsilon \mapsto \sigma^n\tau^m\epsilon^{\pm 1} \end{cases}$$

is an isomorphism.

Proposition 7.4. *Let $p = -1 \pmod q$. The following are equivalent*:

(i) *$Q = \mathcal{Q}(\mathcal{G}_-, \mathrm{Fix}(f), f)$ is a connected quandle of size pq and $\mathrm{Dis}(Q) \cong \mathcal{G}_-$.*
(ii) *$f = ((n,m), F_-)$ and $\det(F_-) = -1$.*

Proof. (i) $\Rightarrow$ (ii) As in Proposition 7.3, from the condition that the factor Q/γ_Q is connected and $|\mathrm{Fix}(f)| = p$ the conditions over f follows.

(ii) $\Rightarrow$ (i) The induced automorphism $f_{\gamma_1(\mathcal{G}_-)}$ has no fixed points. So $\mathrm{Fix}(f) \le \gamma_1(\mathcal{G}_-)$. Since $\det(F_-) = -1$ and $\mathrm{Tr}(F_-) = 0$ then the characteristic polynomial of F_- is $x^2 - 1 = (x-1)(x+1)$ and so $|\mathrm{Fix}(f)| = p$. Using the same argument as in Proposition 7.3 we have $\mathcal{G}_- = [\mathcal{G}_-, f]$ and $\mathrm{Core}_{\mathcal{G}_-}(\mathrm{Fix}(f)) = 1$ since $\langle\sigma,\tau\rangle$ contains no proper normal subgroups. Then $\mathrm{Dis}(Q) = [\mathcal{G}_-, f] = \mathcal{G}_-$ and Q is connected. □

The group $\mathcal{G}_k$. The group $\mathcal{Q}_8$ has the following presentation

$$\mathcal{Q}_8 = \langle x, y, z \,|\, x^2 = y^2 = [x, y] = z,\ z^2 = [z, y] = [z, x] = 1 \rangle.$$

In this section we investigate the group $\mathcal{G}_k = \mathbb{Z}_p^2 \rtimes_\rho \mathcal{Q}_8$, where $p = 1 \pmod 3$ and $k \in \mathbb{Z}_p$ such that $k^3 = 1$. The action ρ is the irreducible action of $\mathcal{Q}_8$ defined by setting

$$\rho_x = \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix}, \quad \rho_y = \begin{bmatrix} k^2 & k \\ k & -k^2 \end{bmatrix}, \quad \rho_z = \begin{bmatrix} -1 & 0 \\ 0 & -1 \end{bmatrix}.$$

Faitfhul representation of degree 2 of non-abelian groups are irreducible. According to [22], ρ is the unique irreducible action of $\mathcal{Q}_8$ of degree 2, and moreover it is a fixed-point-free action, i.e. $\mathrm{Fix}(\rho_h) = \left\{ v \in \mathbb{Z}_p^2 \,|\, \rho_h(v) = v \right\} = 0$ for every $h \in \mathcal{Q}_8$. Equivalently $1 - \rho_h \in GL_2(p)$ for every $h \in \mathcal{Q}_8$. In particular, $\gamma_1(\mathcal{G}_k) = \mathbb{Z}_p^2 \rtimes Z(\mathcal{Q}_8)$ and $\gamma_2(\mathcal{G}_k) = \mathbb{Z}_p^2 \times \{1\}$ is the p-Sylow subgroup of $\mathcal{G}_k$. The action ρ has no invariant subspaces, so $\gamma_2(\mathcal{G}_k)$ is a minimal normal subgroup of $\mathcal{G}_k$.

Proposition 7.5. *The automorphisms of $\mathcal{G}_k$ are given by the mappings*

$$f = \left\{ x \mapsto hv_1, \quad y \mapsto gv_2, \quad z \mapsto zw, \quad F = f|_{\gamma_2(\mathcal{G}_k)} \in GL_2(p) \right. \tag{9}$$

where $g, h \in \mathcal{Q}_8$ and $v_1, v_2, w \in \mathbb{Z}_p^2$ such that

$$\begin{cases} f_{\gamma_2(\mathcal{G}_k)} = \left\{ x \mapsto h \quad y \mapsto g, \quad z \mapsto z, \quad \textit{is an automorphism of } \mathcal{Q}_8, \right. \\ F\rho_x = \rho_h F, \\ F\rho_y = \rho_g F, \\ v_1 = 2^{-1}(1 + \rho_h)(w), \\ v_2 = 2^{-1}(1 + \rho_g)(w). \end{cases}$$

In particular, $|\mathrm{Aut}(\mathcal{G}_k)| = 24(p-1)p^2$.

Proof. If $f \in \mathrm{Aut}(\mathcal{G}_k)$ then $\gamma_2(\mathcal{G}_k)$ is an invariant subgroup and $f_{\gamma_2(\mathcal{G}_k)} \in \mathrm{Aut}(\mathcal{Q}_8)$ and so f is as in (9) and in particular h, g do not commute. A mapping f as in (9) is an automorphism of $\mathcal{G}_k$ if and only if it respects the relation between the generators of $\mathcal{G}_k$. Hence for every $v \in \mathbb{Z}_p^2$ we have

$$\begin{cases} f(xvx^{-1}) = F\rho_x(v) = f(x)f(v)f(x)^{-1} = \rho_h F(v), \\ f(yvy^{-1}) = F\rho_y(v) = f(y)f(v)f(y)^{-1} = \rho_g F(v). \end{cases} \tag{10}$$

Moreover the mapping f has to satisfy

$$\begin{cases} f(x)^2 = hv_1hv_1 = h^2\rho_h^{-1}(v_1)v_1 = zw = f(z), \\ f(y)^2 = gv_2gv_2 = g^2\rho_g^{-1}(v_2)v_2 = zw = f(z), \\ [f(x), f(y)] = v_1^{-1}h^{-1}v_2^{-1}g^{-1}hv_1gv_2 = f(z) = zw. \end{cases} \tag{11}$$

After a straightforward manipulation and using that ρ_h is fixed-point-free and that $(1 - \rho_h)^{-1} = 2^{-1}(1 + \rho_h)$ for every non central element $h \in \mathcal{Q}_8$ we have that (11) is equivalent to

$$\begin{cases} v_1 = 2^{-1}(1+\rho_h)(w), \\ v_2 = 2^{-1}(1+\rho_g)(w), \\ w = 2^{-1}\left((1-\rho_h)(1+\rho_g) + (1-\rho_g)(1+\rho_h)\right)(w). \end{cases} \tag{12}$$

Using that $\rho_g\rho_h + \rho_h\rho_g = 0$ we have that the last condition is trivially satisfied by any $w \in \mathbb{Z}_p^2$. The elements v_1 and v_2 are uniquely determined by w.
The mapping

$$\mathrm{Aut}(\mathcal{G}_k) \longrightarrow \mathrm{Aut}(\mathcal{Q}_8), \quad f \mapsto f_{\gamma_2(\mathcal{G}_k)} \tag{13}$$

is a surjective group homomorphism. Indeed, setting $w = v_1 = v_2 = 0$, the system of equation (10) has a solution for every $f_{\gamma_2(\mathcal{G}_k)} \in \mathrm{Aut}(\mathcal{Q}_8)$. The kernel of the homomorphism (13) has size $(p-1)p^2$, since if $h = x$ and $g = y$ then (10) is satisfied just by scalar matrices and v_1, v_2 are uniquely determined by the choice of w. Therefore $|\mathrm{Aut}(\mathcal{G}_k)| = |\mathrm{Aut}(\mathcal{Q}_8)|(p-1)p^2$. □

The following proposition identify the automorphisms of $\mathcal{G}_k$ providing connected subdirectly irreducible quandles of size $4p$.

Proposition 7.6. *Let p be a prime such that $p = 1 \pmod 3$. The following are equivalent*:

(i) $Q = \mathcal{Q}(\mathcal{G}_k, \mathrm{Fix}(f), f)$ *is a connected subdirectly irreducible quandle of size* $4p$ *and* $\mathrm{Dis}(Q) \cong \mathcal{G}_k$.
(ii) $|\mathrm{Fix}(f)| = 2p$ *and* $|f| = |f_{\gamma_1(\mathcal{G}_k)}| = 3$.

Proof. (i) ⇒ (ii) By Proposition 5.4(iii) and to Lemma 1.2 the order of f is 3. The factor Q/γ_Q is connected and then $f_{\gamma_1(\mathcal{G}_k)} \neq 1$, so it has order 3.

(ii) ⇒ (i) Let $G = \mathcal{G}_k$, $T = \{gf(g)^{-1} \mid g \in G\}$ and $[G, f] = \langle T \rangle$. The automorphism $f_{\gamma_1(G)}$ has no fixed points, so $\mathrm{Fix}(f) \leq \gamma_1(G)$ and T contains a set of representatives of $G/\gamma_1(G)$. According to Proposition 3.7, $[G, f]$ contains also a set of representatives of the cosets $\gamma_1(G)/\gamma_2(G)$. Moreover, $[G, f] \cap \gamma_2(G) \neq 1$ ($\mathrm{Fix}(f|_{\gamma_2(G)})$ has size p) and so $\gamma_2(G) \leq [G, f]$ and so we can conclude that $G = [G, f]$.

The subgroup $C = \mathrm{Core}_G(\mathrm{Fix}(f))$ is a normal subgroup of $\gamma_1(G) \cong \gamma_2(G) \rtimes \mathbb{Z}_2$ and therefore $C < \gamma_2(G)$. Hence, using again the minimality of $\gamma_2(G)$ we have $C = 1$. Therefore $\mathrm{Dis}(Q) \cong [G, f] = G$ is transitive and so Q is a connected quandle of size $[G : \mathrm{Fix}(f)] = 4p$.

The quandle Q is not affine, so according to Theorem 5.2, Q is subdirectly irreducible. □

In the following Lemma we enumerate the relevant automorphisms of $\mathcal{G}_k$ addressed in Proposition 7.6.

Lemma 7.7. *The subset of* $\mathrm{Aut}(\mathcal{G}_k)$

$$\mathcal{F} = \{f \in \mathrm{Aut}(\mathcal{G}_k) \mid |f| = |f_{\gamma_1(\mathcal{G}_k)}| = 3,\ |\mathrm{Fix}(f)| = 2p\}$$

has size $16p$.

Proof. If $f \in \mathcal{F}$ then the order of $f_{\gamma_1(\mathcal{G}_k)}$ is 3 and so it is one of the two following matrices:

$$A = \begin{bmatrix} 0 & 1 \\ 1 & 1 \end{bmatrix}, \qquad B = \begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix}.$$

Let $f_{\gamma_1(\mathcal{G}_k)} = A$, then the image of f of the generators of $\mathcal{G}_k$ is

$$f = \left\{ x \mapsto yz^s v_1, \quad y \mapsto xyz^l v_2, \quad z \mapsto zw, \quad f|_{\gamma_1(\mathcal{G}_k)} = F \right.$$

for $s, l = 0, 1$ and $v_1, v_2, w \in \gamma_2(\mathcal{G}_k)$. The order of F is 3 and so it is diagonalizable by Lemma 7.1(i). Since $|\mathrm{Fix}(f) \cap \gamma_2(G)| = p$, the eigenvalues of F are 1 and λ and the order of λ is 3. So $\lambda = k^j$ where $j = 1, 2$ and $\det(F) = \mathrm{Tr}(F) - 1 = \lambda$. The matrix F has to satisfy the following conditions

$$F\rho_x = (-1)^s \rho_y F, \quad F\rho_y = (-1)^l \rho_x \rho_y F. \tag{14}$$

A case-by-case discussion on the values of s and l shows that for each choice of s, l there exists just one solution to (14). Moreover, since $\mathrm{Fix}(f) \leq \gamma_1(\mathcal{G}_k)$ ($f_{\gamma_1(\mathcal{G}_k)}$ acts irreducibly) there exists $v \in \gamma_2(\mathcal{G}_k)$ such that $f(zv) = zv$. Then $f(zv) = zwf(v) = zv$ holds if and only if $w = (1 - F)(v)$. Hence there exists p choices for w, since the image of $1 - F$ has dimension 1. So there exists $8p$ such automorphisms.
Note that $f \in \mathcal{F}$ if and only if $f^2 \in \mathcal{F}$ and moreover $f_{\gamma_1(\mathcal{G}_k)} = A$ if and only if $f^2_{\gamma_1(\mathcal{G}_k)} = B$. Therefore there are $8p$ automorphisms in $\mathcal{F}$ such that the induced automorphism over $\mathcal{G}_k/\gamma_1(\mathcal{G}_k)$ is B. Hence the size of $\mathcal{F}$ is $16p$. □

Lemma 7.8. *Let $f_j \in \mathrm{Aut}(\mathcal{G}_k)$ given by*

$$f_j = \left\{ x \mapsto y, \quad y \mapsto xy, \quad z \mapsto z, \quad F_j = f_j|_{\gamma_2(\mathcal{G}_k)} = \begin{bmatrix} -k(1+k^j) & -(1+k^j) \\ 0 & -k^2(1+k^j) \end{bmatrix} \right.$$

where $j = 1, 2$. Then $f_j \in \mathcal{F}$ and $|C_{\mathrm{Aut}(\mathcal{G}_k)}(f_j)| = 3p(p-1)$ for $j = 1, 2$.

Proof. A direct computation shows that $f_j \in \mathcal{F}$ for $j = 1, 2$. If $h \in C_{\mathrm{Aut}(\mathcal{G}_k)}(f_j)$ then $h_{\gamma_2(\mathcal{G}_k)}$ centralizes $(f_j)_{\gamma_2(\mathcal{G}_k)}$ and therefore $h_{\gamma_2(\mathcal{G}_k)}$ is a power of $(f_j)_{\gamma_2(\mathcal{G}_k)}$. Hence

$$h = \left\{ x \mapsto tv_1, \quad y \mapsto gv_2, \quad z \mapsto zw, \quad H = h|_{\gamma_2(\mathcal{G}_k)} \in GL_2(p) \right.$$

and (t, g) is (x, y) or (y, xy) or (xy, x).
If $(t, g) = (x, y)$ then

$$\begin{cases} hf_j(x) = h(y) = yv_2 = f_j h(x) = yF_j(v_1), \\ hf_j(y) = h(xy) = xv_1 yv_2 = f_j h(y) = xyF_j(v_2), \\ hf_j(z) = h(z) = zw = f_j h(z) = zF_j(w), \end{cases} \Leftrightarrow \quad \begin{cases} v_2 = F_j(v_1), \\ (1 - F_j)(v_2) - \rho_y(v_1) = 0, \\ w = F_j(w). \end{cases} \tag{15}$$

Moreover H is a scalar matrix and therefore it centralizes F_j. Using that $v_1 = (1-\rho_x)^{-1}(w) = 2^{-1}(1+\rho_x)(w)$ we have that every choice of $w \in \mathrm{Fix}(F_j)$ provides a solution to (15) and so it defines an element of the centralizer of f_j. Hence there are $p(p-1)$ such automorphisms. Similarly it can be proved that there exists $p(p-1)$ automorphisms in the centralizer of f_j for the other choices of t and g. Hence the size of the centralizer is $3p(p-1)$. □

ACKNOWLEDGEMENTS. The author wants to thank Daniele Toller and Giuliano Bianco for the useful comments and remarks on the drafts of the present work.

References

[1] N. Andruskiewitsch and M. Graña: *From racks to pointed Hopf algebras*. Adv. Math. **178** (2003), 177–243.
[2] C. Bergman: Universal algebra, Fundamentals and selected topics, Pure and Applied Mathematics (Boca Raton) **301**, CRC Press, Boca Raton, FL, 2012.
[3] G. Bianco and M. Bonatto: *On connected quandles of prime power order*, Beitr. Algebra Geom. Apr 2020.
[4] M. Bonatto: *Principal and doubly homogeneous quandles*, Monatsh. Math. **191** (2020), 691–717.
[5] M. Bonatto and D. Stanovský: *Commutator theory for racks and quandles*, J. Math. Soc. Japan **73** (2021), 41–75.
[6] M. Bonatto and P. Vojtěchovský: *Simply connected latin quandles*, J. Knot Theory Ramifications **27** (2018), 1843006, 32pp.
[7] L. Brickman and P.A. Fillmore: *The invariant subspace lattice of a linear transformation*. Canadian J. Math. **19** (1967), 810–822.
[8] E. Campedel, A. Caranti and I.D. Corso: *The automorphism groups of groups of order p^2q*. Int. J. Group Theory **10** (2021), 149–157.
[9] W.E. Clark, M. Elhamdadi, X.D. Hou, M. Saito and T. Yeatman: *Connected quandles associated with pointed abelian groups*. Pacific J. Math. **264** (2013), 31–60.
[10] W.E. Clark and X.D. Hou: *Galkin quandles, pointed abelian groups, and sequence A000712*, Electron. J. Combin. **20** (2013), Paper 45, 8pp.
[11] M. Elhamdadi, J. Macquarrie and R. Restrepo: *Automorphism groups of quandles*. J. Algebra Appl. **11** (2012), 1250008, 9pp.
[12] P. Etingof, T. Schedler and A. Soloviev: *Set-theoretical solutions to the quantum Yang-Baxter equation*. Duke Math. J. **100** (1999), 169–209.
[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), 709–719.
[14] R. Freese and R. McKenzie: *Commutator theory for congruence modular varieties*, London Mathematical Society Lecture Note Series **125**, Cambridge University Press, Cambridge, 1987.
[15] M. Graña: *Indecomposable racks of order p^2*, Beiträge Algebra Geom. **45** (2004), 665–676.
[16] X.D. Hou: *Finite modules over $\mathbb{Z}[t, t^{-1}]$*, J. Knot Theory Ramifications, **21** (2012), 1250079, 28pp.
[17] A. Hulpke, D. Stanovský and P. Vojtěchovský: *Connected quandles and transitive groups*. J. Pure Appl. Algebra **220** (2016), 735–758.
[18] D. Joyce: *A classifying invariant of knots, the knot quandle*. J. Pure Appl. Algebra **23** (1982), 37–65.
[19] M. Graña and L. Vendramin: Rig, a GAP package for racks, quandles and Nichols algebras.
[20] S.V. Matveev: *Distributive groupoids in knot theory*. Mat. Sb. (N.S.) **119 (161)** (1982), 78–88, 160.
[21] J. McCarron: *Connected Quandles with Order Equal to Twice an Odd Prime*, arXiv:1210.2150.
[22] P. Mayr: *Fixed-point-free representations over fields of prime characteristic*, Technical Report of the Mathematics Department - Univesität Linz, 554, 2000.
[23] M.W. Short: The primitive soluble permutation groups of degree less than 256, Lecture Notes in Mathematics **1519**, Springer-Verlag, Berlin, 1992.
[24] C.C. Sims: Computation with finitely presented groups, Encyclopedia of Mathematics and its Applications **48**, Cambridge University Press, Cambridge, 1994.
[25] D. Stanovský: *A guide to self-distributive quasigroups, or Latin quandles*. Quasigroups Related Systems, **23** (2015), 91–128.
[26] P. Vojtěchovský: *Bol loops and Bruck loops of order pq up to isotopism*, Finite Fields Appl, **52** (2018), 1–9.
[27] D.L. Winter: *The automorphism group of an extraspecial p-group*. Rocky Mountain J. Math. **2** (1972), 159–168.

Dipartimento di Matematica e Informatica UNIFE
via Machiavelli, 30-44121 Ferrara
Italy
e-mail: marco.bonatto.87@gmail.com