Finite quandles

Raúl Penaguião
raul.penegas@gmail.com
Professor : Pedro Lopes - Lisbon Tech
Lisbon Tech

2013 - 2014

Contents

Abstract

In this document, we introduce the notion of quandles, and construct some particular quandles of interest, with profile $\{1, p-1, p(p-1)\}$ for p prime. We develop some divisibility conditions on the length of cycles and with that we prove a generalisation of the theorem 1.9 in [1].

It is developed some theory initialized in [7], regarding a polynomial invariant of quandles, and is proved other relevant results.

We also restate some results and prove them from [1], regarding a combinatoric invariant of quandles.

1 Introduction

Quandles are a self-distributive algebraic structure that arrive in knot theory as quasi-groups. Those have been studied since 1940s, for example, in [3]. A fundamental quandle is constructed in a similar way to the construction of fundamental groups in topology, hence it plays an important role in knot theory [4, 5].

The algebraic properties of quandles have been studied since then. In 2011, the authors of [1] constructed an invariant for connected quandles, the number of canonical forms, which we will investigate.

In the same paper, it is proven that a certain condition on a profile implies a connected quandle to be latin. Here we establish the same result weakening the condition on the profile.

In this report, we will see some invariants on the quandle structures.

1.1 Preliminar definitions

1.1.1 A quandle

A quandle is an algebraic structure similar to a group: it is a set Q, with a multiplication operation, mainly written as $*$, which satisfies:

$$\begin{aligned} &a * a = a && \forall\, a \in Q \\ &a = b * c && \forall\, a, c \,\exists\, b \in Q \\ &(a * b) * c = (a * c) * (b * c) && \forall\, a, b, c \in Q \end{aligned} \tag{1.1}$$

We will assume that all quandles are finite, unless stated otherwise.

We note that we don't have necessarily $a * b = b * a$ or $a * (c * b) = (a * c) * (a * b)$, nor $a * (b * c) = (a * b) * c$.

The second axiom is called a right-invertibility axiom, and guarantees that the function $r_b : Q \to Q$ defined by $r_b(a) = a * b$ is bijective for each b. We define also the function "left multiplication" with $s_b(a) = b * a$, which may not be bijective.

Additionally, the third axiom is called the right distributivity, and can be restated as:

$$r_c(a*b) = r_c(a) * r_c(b) \tag{1.2}$$

$$r_c \circ r_b = r_{r_c(b)} \circ r_c \tag{1.3}$$

$$r_c \circ r_b \circ r_c^{-1} = r_{r_c(b)} \tag{1.4}$$

A function between two quandles $f : Q_1 \to Q_2$ is said to be a homomorphism if it satisfies

$$f(a*b) = f(a) * f(b)$$

A bijective homomorphism is said to be an isomorphism. If $Q_1 = Q_2$ we say that f is an endomorphism, and if it is bijective, an automorphism. Then, each r_c is an automorphism by (1.2).

The set of automorphisms Aut (Q) of Q forms a group with the composition.

Definition 1 (Inner Automorphisms)**.** For each $b \in Q$, the functions $r_b : Q \to Q$ are automorphisms, a consequence of axioms 2 and 3. These are called the *primitive inner automorphisms.*

The subgroup of automorphisms generated by $\{r_b | b \in Q\}$ is the Inn (Q) group of inner automorphisms. This subgroup of automorphisms is given by $\{r_{b_1}^{\delta_1} \circ \cdots \circ r_{b_j}^{\delta_j} | b_1, \cdots, b_j \in Q,\ \delta_1, \cdots, \delta_j \in \{-1, 1\}\}$

A quandle is said to be decomposible if there exists disjoint sets $Q_1 \subseteq Q$ and $Q_2 \subseteq Q$ closed under the operation $*$ such that $Q_1 \cup Q_2 = Q$. A quandle is said to be indecomposible if it is not decomposible.

1.1.2 Some propositions

We will now prove a result that has an analogous in group theory, that Inn (Q) is a normal subgroup on Aut(Q).

Lemma 1. If $\pi \in$ Aut (Q), then $\pi \circ r_b \circ \pi^{-1} = r_{\pi(b)}$ and $\pi \circ r_b^{-1} \circ \pi^{-1} = r_{\pi(b)}^{-1}$ for each $b \in Q$

Proof. Just note that $\pi \circ r_b(a) = \pi(a*b) = \pi(a) * \pi(b) = r_{\pi(b)}(\pi(a))$ so

$$\pi \circ r_b = r_{\pi(b)} \circ \pi \Leftrightarrow \pi \circ r_b \circ \pi^{-1} = r_{\pi(b)}$$

Inverting both sides of the equation we get the second equality. □

Proposition 2. Inn $(Q) \trianglelefteq$ Aut (Q)

Proof. Take an $\alpha \in$ Aut (Q) and a $\gamma \in$ Inn (Q). Then we can express $\gamma = r_{c_1}^{\epsilon_1} \circ \cdots \circ r_{c_k}^{\epsilon_k}$. Our goal is to prove that $\alpha \circ \gamma \circ \alpha^{-1}$ is an inner automorphism.

We use the Lemma 1:

$$\alpha \circ \gamma \circ \alpha^{-1} = \alpha \circ \left(\bigcirc_{j=1}^{k} r_{c_j}^{\epsilon_j} \right) \circ \alpha^{-1} = \bigcirc_{j=1}^{k} \left(\alpha \circ r_{c_j}^{\epsilon_j} \circ \alpha^{-1} \right) = \bigcirc_{j=1}^{k} r_{\alpha(c_j)}^{\epsilon_j} \in \text{ Inn } (Q)$$

□

Definition 2. The unique quandle $\mathcal{T}_m$ with m elements such that for each $b \in \mathcal{T}$, $r_b = id$, is the *trivial* quandle.

The trivial quandle does not have all the desired properties one would like for a quandle. One of the lacking properties is connectedness, which we will introduce later.

1.1.3 The Dual Quandle

Definition 3 (Dual Operation)**.** On a quandle structure Q, we can set a dual operation $\overline{*}$ given by $a \overline{*} b := r_b^{-1}(a)$, which is well defined since r_b is a bijective function.

This amounts to give another quandle structure, written as Q^{op}, since $\overline{*}$ satisfies the quandle axioms. This should be verified:

- Axiom 1:

  Note that $a \overline{*} a = r_a^{-1}(a) = a$ because $r_a(a) = a * a = a$.

- Axiom 2

  This is equivalent to state that r_b^{-1} is bijective, which is clear since r_b is bijective as we have seen.

- Axiom 3

  This is equivalent to state that r_b^{-1} is an homomorphism, which is clear since r_b is an automorphism.

A familiarisation exercise is always a good exercise. Here we settle conditions of the associativity of the multiplication, so it's only a minor proposition.

Proposition 3 (A Condition of associativity)**.** The only associative quandle is the trivial. Additionally, $(a * b) * c = a * (b * c) \Leftrightarrow r_c(a) = a$, then, the local associativeness doesn't depend on b.

Proof. By the 3rd axiom, $(a*b)*c = (a*c)*(b*c)$, and by the 2nd axiom, $(a*c)*(b*c) = a*(b*c) \Leftrightarrow a*c = a \Leftrightarrow r_c(a) = a$ so $(a*b)*c = a*(b*c) \Leftrightarrow r_c(a) = a$, therefore the only associative quandle is the trivial one. □

The following relations between Q and Q^{op} hold:

$$\text{For any } a, b, c \in Q,\ (a * b) \overline{*} c = (a \overline{*} c) * (b \overline{*} c) \tag{1.5}$$

$$\text{For any } a, b, c \in Q,\ (a \overline{*} b) * c = (a * c) \overline{*} (b * c) \tag{1.6}$$

$$\text{For any } a, b, c \in Q,\ a * (b * c) = ((a \overline{*} c) * b) * c \tag{1.7}$$

Incidentally, they can be rewritten using inner automorphisms:

$$\text{For any } b, c \in Q,\ r_c^{-1} \circ r_b = r_{r_c^{-1}(b)} \circ r_c^{-1} \tag{1.8}$$

$$\text{For any } b, c \in Q,\ r_c \circ r_b^{-1} = r_{r_c(b)}^{-1} \circ r_c \tag{1.9}$$

$$\text{For any } b, c \in Q,\ r_{r_c(b)} = r_c \circ r_b \circ r_c^{-1} \tag{1.10}$$

Which are all trivially equivalent to axiom 3. The first two equations set the distributivity between the operations $*$ and $\overline{*}$.

1.1.4 Examples and Properties

We shall study some examples on quandles. The first one we already noted, the trivial quandle. Given a set X, the operation $a * b = a$ equips X with a trivial quandle structure. There are more quandles that will suit our properties.

Example 1 (Dihedral quandles). The dihedral quandles have basis set $\mathbb{Z}_n$ for a positive integer n. The quandle operation is given by

$$m * n = 2n - m$$

Naturally $n * n = 2n - n = n$ and $r_c(b) = a \Leftrightarrow r_c(a) = b$ so r_c is bijective and it's is own inverse $r_c = r_c^{-1}$. This proves axiom 1 and 2. For the third axiom, we brute-force it

$$r_c(a * b) = r_c(2b - a) = a + 2c - 2b$$

$$r_c(a) * r_c(b) = (2c - a) * (2c - b) = 4c - 2b - 2c + a = 2c - 2b + a$$

As a case of example, we place here the operation table for $\mathbb{Z}_4$ and $\mathbb{Z}_5$

$*$	0	1	2	3
0	0	3	2	1
1	2	1	0	3
2	0	3	2	1
3	2	1	0	3

(1.11)

$*$	0	1	2	3	4
0	0	4	3	2	1
1	2	1	0	4	3
2	4	3	2	1	0
3	1	0	4	3	2
4	3	2	1	0	4

(1.12)

A group G can have a quandle structure for each n, if we set $a * b = b^n a b^{-n}$, it is called the n-fold conjugacy quandle. It is possible to consider the conjugacy class of one element $G^{(g)}$ in G and equip it with the former operation.

In fact, $a * a = aaa^{-1} = a$ and $a * b = c \Leftrightarrow aba^{-1} = c \Leftrightarrow b = a^{-1}ca$, so axiom 1 and 2 are verified. The 3rd axiom holds because each r_b is an homomorphism of groups, then preserves the group operation, so also preserves the quandle operation.

For example, consider the symmetric group on three numbers with composition as the group operation $S_3 = \{\mathrm{id}, (12), (13), (23), (123), (132)\}$, then the quandle operation for $n = 1$ is the following

$*$	id	(12)	(13)	(23)	(123)	(132)
id	id	(12)	(13)	(23)	(123)	(132)
(12)	id	(12)	(23)	(13)	(132)	(123)
(13)	id	(23)	(13)	(12)	(132)	(123)
(23)	id	(13)	(12)	(23)	(132)	(123)
(123)	id	(23)	(12)	(13)	(123)	(132)
(132)	id	(13)	(23)	(12)	(123)	(132)

(1.13)

And for $A_4^{(123)}$, the conjugacy class of (123) inside the alternate group of permutations on 4 elements.

$*$	(123)	(324)	(341)	(142)
(123)	(123)	(134)	(142)	(324)
(324)	(142)	(243)	(231)	(341)
(341)	(324)	(421)	(341)	(123)
(142)	(413)	(312)	(324)	(142)

(1.14)

Another class of examples arise in [8], which is proven in the same paper that every quandle is in that form.

Definition 4 (Homogeneous Quandles)**.** Let G be a group and $H \leq G$ a subgroup. Let $s \in$ Aut (G) such that $s(h) = h\ \forall h \in H$. Then then define in $\frac{G}{H}$ a quandle operation with

$$xH * yH = y\ ,\ s(\,y^{-1}\,x\,)\,H$$

First, it is well defined, sense if $x = x'h$ and $y = y'h$ then

$$xH\ *\ y'H = yhs(\,h^{-1}\,y^{-1}\,x\,h\,)H = y\,h\,h^{-1}\,s(\,y^{-1}\,x\,)h\,H = y\,s(\,y^{-1}\,x\,)\,H$$

This is a quandle since $xH * xH = xs(x^{-1}x)H = x$ id $H = xH$ and $xH * yH = zH \Leftrightarrow ys(y^{-1}x) = zh \Leftrightarrow x = ys^{-1}(y^{-1}z)h \Leftrightarrow xH = ys^{-1}(y^{-1}z)H$

For the 3rd axiom, we note that the equations $(xH*yH)*zH$ and $(xH*zH)*(yH*zH)$ both yield $zs(z)^{-1}s(y)s^2(y)^{-1}s^2(x)H$.

In fact, it is proved in [8] Theorem 3.1 that every indecomposible quandle is isomorphic to an homogeneous quandle.

We will construct a family of quandles that may be useful when finding examples of medial quandles. These quandles are a quite general family of quandles.

Definition 5 (Alexander Quandles)**.** Let Q be a Γ-module, where $\Gamma = \mathbb{Z}[t, t^{-1}]$ is the ring of Lambert polynomials in integers. Define in Q the operation $* : Q \times Q \to Q$ as

$$a * b = at + b(1-t), \quad a, b \in Q$$

In particular, each r_b is given by $r_b(a) = b(1-t) + at = a + t(b-a)$

These structures form a quandle, as we can note that $a * a = at + a(1-t) = a$ and $a * b = c \Leftrightarrow a = t^{-1}(c - b(1-t))$ so axiom 2 holds.

For axiom 3, we can see

$$(a * b) * c = c(1-t) + (a * b)t = c(1-t) + at^2 + bt(1-t) \tag{1.15}$$

$$(a * c) * (b * c) = (b * c)(1-t) + (a * c)t = bt(1-t) + c(1-t)^2 + at + c(1-t)t \tag{1.16}$$

Which are incidentally the same. In the same manner we can see that

$$(a * c) * (b * d) = (b * c)(1-t) + (a * d)t = bt(1-t) + d(1-t)^2 + at + c(1-t)t \tag{1.17}$$

Are symmetric in b and c, so $(a * b) * (c * d) = (a * c) * (b * d)$

Definition 6 (Medial Quandles)**.** If in the quandle Q it is satisfied for all $a, b, c, d \in Q$ the following $(a * b) * (c * d) = (a * c) * (b * d)$, we say that Q is a *medial* quandle.

The classification of all Alexander finite quandles can be found in [6]

We can see that dihedral quandles are particular cases of Alexander quandles: consider the case of $Q = \frac{\mathbb{Z}_n[t,t^{-1}]}{<t+1>}$, then each $r_b(a) = b(1-t) + at = 2b - a$

For us, the Alexander Quandles of the form $\frac{\mathbb{Z}_n}{<h(t)>}$ will be of great interest, because we can test easily if is a Latin Quandle, as we will see in the relevant section.

Definition 7 (Latin Quandles)**.** A quandle is said to be *latin* if for every $a, b \in Q$ the equation $a = b * c$ as an unique solution in c.

This is a dual condition of Axiom 2, so we have defined a function $s_b : Q \to Q$ such that $s_b(c) = b * c$. In a latin quandle, each s_b is a bijection.

Our main goal is to encounter conditions to force quandles to be latin.

Definition 8 (Connected quandle, k-transitivity, weakly connected quandle)**.** A quandle is said to be *connected* if Inn (Q) acts transitively on Q, that means, for every $x, y \in Q$ there is $\rho \in$ Inn (Q) such that $\rho(x) = y$.

A quandle is said to be *weakly connected* if Aut (Q) acts transitively on Q, that means, for every $x, y \in Q$ there is $\rho \in$ Aut (Q) such that $\rho(x) = y$.

Additionally, it is introduced the notion of k-transitivity later. Roughly, a quandle Q is said to be *k-transitive* if for any distinct $x_1, \cdots, x_k$ and distinct $y_1, \cdots, y_k \in Q$ there is $\rho \in$ Inn (Q) such that $\rho(x_i) = y_i$ for $i = 1, \cdots k$.

It is known that connected quandles and indecomposible quandles are the same from [9]. In fact, it is quite simple to prove that an indecomposible quandle is connected, the other way around is done in [9].

Connected quandles are useful in the context of knot theory, because the fundamental quandle of a knot is connected. Note that latin quandles are connected, but there are examples of connected non-latin quandles, like $Q_{6,1}$ from the list in [8].

Example 2. Consider the operation given by the following *operation table*:

$*$	1	2	3	4	5	6
1	1	2	5	6	3	4
2	1	2	6	5	4	3
3	5	6	3	4	1	2
4	6	5	3	4	2	1
5	3	4	1	2	5	6
6	4	3	2	1	5	6

(1.18)

The fact that $6 = r_4(1)$, $5 = r_3(1)$, $4 = r_6(1)$, $3 = r_5(1)$ and $1 = r_5(r_6(1))$ means that the action of Inn (Q) under Q is transitive, although s_1 is not a bijection, so Q is a connected not latin quandle.

The dihedral quandles are latin for any odd n, since in such case 2 is invertible, then for any $a, b \in \mathbb{Z}_n$, $r_{\frac{a+b}{2}}(a) = b$ as envisaged.

We note that a latin quandle is always connected, so dihedral quandles are also connected for n odd. This is so since in a latin quandle, s_b is invertible, then to Inn (Q) act from b to c we only have to consider $r_a \in$ Inn (Q) such that $a = s_b^{-1}(c)$ which satisfies $r_a(b) = b * a = l_b(a) = c$ [1].

Proposition 4. Let Q be a weakly connected quandle. Then the primitive inner automorphisms have all the same cyclic type, called *profile*.

Proof. Let r_a and r_b be two distinct primitive inner automorphisms. Since Q is weakly connected, $b = \sigma(a)$ for some $\sigma \in$ Aut (Q), then take any $k \in Q$ and compute

$$r_b \circ \sigma(k) = \sigma(k) * b$$

$$\sigma \circ r_a(k) = \sigma(k * a) = \sigma(k) * \sigma(a) = \sigma(k) * b$$

So $r_b \circ \sigma = \sigma \circ r_c \Leftrightarrow r_b = \sigma \circ r_c \circ \sigma^{-1}$. Hence r_b and r_c are conjugated permutations, so they should have the same cyclic type. □

We hereby denote $\{1, l_1, \cdots, l_k\}$ the cyclic type of all r_b, and k is the number of cycles without the trivial one.

[1] for this reason, it is called some times to latin quandles also *Strongly connected quandles*, as in [7]

Definition 9. For each $i, k \in Q$, we denote $l_{i,k}$ as the length of the cycle in r_k containing i, this notation does not depend on the quandle being weakly connected. We say that $i, j \in Q$ share a cycle of k if there is a cycle in r_k written in the disjoint cycle decomposition form that contains both i, j. Equivalently, we can say that there is some integer m such that $r_k^m(i) = j$

1.1.5 A result on Transitivity

We now develop a property or limitations of the connectedness.

Definition 10. A quandle Q is said to be k-transitive if for any $2k$ elements $x_1, \cdots, x_k$ and $y_1, \cdots, y_k$, being the x's distinct and y's distinct, there is some inner automorphism τ such that $\tau(x_i) = y_i \ \forall 1 \leq i \leq k$

It turns out that there are only k-transitive quandles for $k \leq 2$, except $\mathbb{Z}_3$, the dihedral quandle.

Proposition 5. If Q is a k-transitive quandle with $\#Q \geq 4$, then $k \leq 2$.

Proof. Suppose for sake of contradiction that $k \geq 3$, so Q is, in particular, 3-transitive. Let's choose some x, y such that $y \neq x \neq x * y \neq y$ for now, we will see later that this should be possible. It is, then impossible to choose τ such that $\tau(x) = x$, $\tau(y) = y$ and $\tau(x*y) \neq x*y$, contradicting the 3-transitivity. Here we need to assume that there is some $\tau(x*y) \neq x*y, x, y$ so $\#Q \geq 4$.

Suppose now that every $x \neq y$ are such that $x = x * y$ (it is impossible that $x * y = y$ for the first and second axiom). So $r_y(x) = x \ \forall y \neq x$, and from axiom 1, $r_y(y) = y$, so $r_y = id$ and Q is the trivial quandle, which is impossible since Q is connected. □

2 Connection between cycles

This section is the result of a work done in the sequence of the conjecture 1.1 on [1], which is:

Conjecture. *Suppose that a connected quandle Q has profile $\{1, l_1, \cdots, l_n\}$. Then $l_j \mid l_n \ \forall j$.*

We construct the sets $Q_{i,k} = \{l \in Q | r_i^k(l) = l\}$, and $Q'_{i,k} = \{l \in Q | r_i^k(l) \neq l\}$. Here we prove that $Q_{i,k}$ is always a quandle, and conjecture that Q'_{i,l_n} is also a quandle. Then when Q is connected, we conclude $Q'_{i,l_n} = \emptyset$, using Proposition 2.3 of [2], this will settle the conjecture 1.1 on [1].

Lemma 6. Suppose that $a = b * c$ on the quandle Q, and suppose $k \in Q$. We have the following:

$$(r \equiv l_{a,k} \mod l_{b,k} \wedge r \equiv l_{a,k} \mod l_{c,k}) \Rightarrow l_{a,k} \mid r \quad \forall r \in \mathbb{Z}$$

Proof. Suppose that $r \equiv l_{a,k} \mod l_{b,k}$ and $r \equiv l_{a,k} \mod l_{c,k}$, then $a = r_k^{l_{a,k}}(a) = r_k^{l_{a,k}}(b * c) = r_k^{l_{a,k}}(b) * r_k^{l_{a,k}}(c) = r_k^r(b) * r_k^r(c) = r_k^r(b * c) = r_k^r(a)$ i.e. $r_i^r(a) = a$, so $l_{a,k} \mid r$. □

Using some number-theoretic insights, the following lemma provides some good use to the latter lemma.

We denote the smallest common multiple of two integers x, y as $[x, y]$.

Lemma 7. Let x, y, z be integers, then:

$$((r \equiv x \mod y \wedge r \equiv x \mod z) \Rightarrow x \mid r \quad \forall r \in \mathbb{Z}) \Leftrightarrow x \mid [y, z]$$

Proof. $(\rightarrow)$ Let's choose $r = [y, z] + x$. Then we have trivially $r \equiv x \mod y$ and $r \equiv x \mod z$, so by hypothesis $x \mid r = [y, z] + x$, then $x \mid [y, z]$

$(\leftarrow)$ Suppose that $x \mid [y, z]$, and that $r \equiv x \mod y \wedge r \equiv x \mod z$, so we can state that as $r \equiv x \mod [y, z]$. Then $r = [y, z]k + x$ so $x \mid r$, as envisaged. □

Theorem 8. If $a = b * c$, then $l_{k,a} \mid [l_{k,b}, l_{k,c}]$.

Proof. Just apply the Lemma 2 to Lemma 1. □

Given a connected quandle Q, we define $Q_{i,j} = \{l \in Q | r_i^j(l) = l\}$. It has a multiplicative structure inherited from Q.

In an analogous form, $Q'_{i,j} = \{l \in Q | r_i^j(l) \neq l\} = Q \setminus Q_{i,j}$ is defined.

The previous Theorem has a direct application on the following proposition:

Proposition 9. Each $Q_{i,j}$ is always a non-empty subquandle of Q.

Proof. That it is non-empty is clear, since $i \in Q_{i,k}$ for any $i \in Q,\ j \in \mathbb{Z}$

In fact, we only have to prove that the operation $*$ is defined in $Q_{i,k}$ and that it satisfies axiom 2, because axioms 1 and 3 are inherited from Q.

Take $a, b \in Q_{i,k}$, then $l_{a,i}, l_{b,i} \mid k$ so $[l_{a,i}, l_{b,i}] \mid k$. From Theorem 1 we conclude that, as $l_{a*b,i} \mid [l_{a,i}, l_{b,i}] \mid k$, $r_i^k(a * b) = a * b$.

Take $c, b \in Q_{i,k}$, we will show that there is some $a \in Q_{i,k}$ such that $a * b = c$. There is such $a \in Q$, so $c = a * b = r_i^k(a * b) = r_i^k(a) * r_i^k(b) = r_i^k(a) * b$. By the uniqueness of the solution on $x * b = c$, $a = r_i^k(a)$ and $a \in Q_{i,k}$. □

Dually to the theorem stated before, we build a conjecture.

Conjecture. *If Q is a connected quandle with profile $\{1, l_1, \cdots, l_k\}$, then each Q'_{i,l_n} is a subquandle of Q.*

It is known that a connected quandle is always indecomposable, and $Q = Q_{i,l_k} \cup Q'_{i,l_k}$, then Q'_{i,l_k} should be empty, solving the conjecture 1 in [1].

3 Latin vs profile

A question raised in [1] is to find a connection between profile and latin quandles. In the referred paper, a theorem due to Kanako Oshiro states that all connected quandles of a certain profile is latin. In this report, a generalisation of the ideas used in that Theorem are used to prove the envisaged for a weaker condition on quandles.

3.1 Cyclic profiles, other types of profile

In [1], Theorem 1.9 states and proves:

Theorem 10. If a connected quandle Q has $\{1, l_1\}$ as profile, $1 < l_1$, then Q is a latin quandle.

Proof. We note firstly that each r_a has only one fixed point, and that is clear by the cyclic type, and since $a * a = a$, a is the unique fixed point. We will obtain some equalities in this way.

Suppose, for sake of a contradiction, that there are some $i, j, k \in Q$, $i \neq j$ such that $k * i = k * j$, i.e., that contradicts Q being latin.

We argue that $i \neq k \neq j$. This is so because if wlog $i = k$, $k * j = k * i = i * i = i = k$, so k is a fixed point of r_j then $k = j$, so $i = j$, a contradiction.

Finally, we argue that there is some integer $0 < m < l_i$ that satisfies $i = r_k^m(j)$. This is true because i, j share a cycle in r_k. Then

$$r_k^m(k * i) = k * r_k^m(i) = k * j = k * i$$

So $k * i$ is a fixed point of r_k^m, and so (recall from preliminary definitions Definition 9) $l_{k*i,k} \mid m < l_1$, so $l_{k*i,k} = 1$ and $k * i$ is a fixed point on r_k. This amounts to say that $k * i = k$, and again k is a fixed point of r_i, so $k = i$ and a contradiction is encountered. □

We can extend this method to a weaker condition on the profile. There should be emphasized that no example was found so far.

Theorem 11. If a connected quandle Q has $\{1 < l_1 < \cdots < l_n\}$ as profile, where $l_i \nmid l_j$ for each $i \neq j$, Q is a latin quandle.

We will denote the greatest common multiple of two integers a, b by (a, b).

Proof. We have already noted that each r_a has only one fixed point, a, in this cyclic characterisation, as in the previous theorem.

Consider $i, j, k \in Q$, such that $k * i = k * j$. Our goal is to prove that $i = j$, proving that s_k is bijective (is injective in a finite set, hence surjective).

We argue that we only have to work with the case $i \neq k \neq j$, as in the previous theorem. This is so because if, wlog, $i = k$, $k * j = k * i = i * i = i = k$, so k is a fixed point of r_j then $k = j$, so $i = j$, as envisaged.

Let $\beta = k * i = k * j$. So

$$\beta = k * j \neq k \tag{3.1}$$

Because k cannot be a fixed point of r_j, by $k \neq j$. Since $\beta \neq k$, β isn't the fixed point of r_k, which is to say that $l_{\beta,k} \neq 1$.

By Theorem 8, we know that $l_{\beta,k} \mid [l_{k,k}, l_{i,k}] = l_{i,k}$ and $l_{\beta,k} \mid [l_{k,k}, l_{j,k}] = l_{j,k}$ so

$$l_{\beta,k} \mid (l_{i,k}, l_{j,k})$$

This can only be possible if (1) $l_{\beta,k} = 1$, which is to say $k = \beta$, or else if (2) $l_{\beta,k} = l_h$ for some h, and $l_h \mid l_{i,k}, l_{j,k}$ implies $l_{i,k} = l_{j,k} = l_h$, we already excluded (1) in Equation 3.1, so $l_{i,k} = l_{j,k} = l_{\beta,k}$.

Then, as all l_m are distinct, i, j, β share the same cycle in r_k so $l_{i,k} = l_{j,k} \Rightarrow \exists m \in \mathbb{Z}^+{}_{<l_{i,k}} r_k^m(i) = j$. Here we are assuming for sake of contradiction that $i \neq j$.

Since i has order $l_{i,k}$, $l_k^{l_{i,k}-m}(j) = i$. We will note that β is a fixed point of both r_k^m and $r_k^{l_{i,k}-m}$, and show that this implies $\beta = k$

$$r_k^m(\beta) = r_k^m(k * i) = k * r_k^m(i) = k * j = \beta$$
$$r_k^{l_{i,k}-m}(\beta) = r_k^{l_{i,k}-m}(k * j) = k * r_k^{l_{i,k}-m}(j) = k * i = \beta$$

Contradicting the fact that $l_{i,k} = l_{j,k} = l_{\beta,k}$. □

4 A polynomial invariant

To distinguish quandles, it was constructed in [7] a polynomial which depends only on the isomorphism class of a quandle. The goal is to distinguish isomorphism classes, as the profile does for the weakly connected quandles. However, we will see some examples of quandles that have the same polynomial invariant.

4.1 Sam Nelson's definition and facts

Definition 11. Let Q be a finite quandle. Define

$$r(k) = \#\{y \in Q \mid y * k = y\}$$

$$c(k) = \#\{y \in Q \mid k * y = k\}$$

We note that there is no guarantee for $r(x)$ and $c(x)$ to be finite for infinite quandles.

Example 3. We will compute those functions for the case $Q_{6,1}$, as is given in Example 2, for convenience, the operation table is the following:

*	1	2	3	4	5	6
1	1	2	5	6	3	4
2	1	2	6	5	4	3
3	5	6	3	4	1	2
4	6	5	3	4	2	1
5	3	4	1	2	5	6
6	4	3	2	1	5	6

(4.1)

In fact, as $2 * 1 = 2$, and 2 is the only element that satisfies $x * 1 = x$, we have $r(1) = 2$.

We have seen that this quandle is connected, so, to avoid tedious calculations, we appeal to the Proposition 15, which is proven after, to see that we have $r(x) = 1$ for any $x \in Q$.

Additionally, we can see that $c(x) = 2$ for any $x \in Q$.

Definition 12 (Polynomial Invariant)**.** For each finite quandle Q, define the following quandle:

$$qp_Q(x, y) = \sum_{k \in Q} x^{r(k)} y^{c(k)}$$

For infinite quandles, qp_Q may not be a polynomial, as $r(x)$ or $c(x)$ may explode. Also we end up with a formal series which is not a polynomial.

So, in the latter example, we have

$$qp_{Q_{6,1}}(x, y) = 6x^2y^2$$

Proposition 12. $qp_Q(1, 1) = \#Q$

Proof. We can use directly the definition, stating:

$$qp_Q(1, 1) = \sum_{k \in Q} 1^{r(k)} 1^{c(k)} = \sum_{k \in Q} \quad = \#Q$$

□

Proposition 13 (Latin Case, Trivial Case)**.** Here we calculate the polynomial invariant on any latin quandle or trivial quandle. Let $n = \#Q$

If Q is a latin quandle, then $qp_Q(x, y) = nxy$

If Q is a trivial quandle, then $qp_Q(x, y) = nx^n y^n$

Proof. Suppose that Q is latin. Just note that s_b is bijective, and that $y * x = y \Leftrightarrow s_y(x) = y \Leftrightarrow s_y(x) = s_y(y) \Leftrightarrow x = y$ so $r(x) = \#\{y \in Q \,|\, y * x = y\} = \#\{x\} = 1$ and $c(x) = \#\{y \in Q \,|\, x * y = x\} = \#\{x\} = 1$

Suppose now that Q is trivial. Then $b * x = b$ so $r(x) = \#\{y \in Q \,|\, y * x = y\} = \#Q$ and $c(y) = \#\{x \in Q \,|\, y * x = y\} = \#Q$.

□

4.2 More results and conjectures

The first thing that comes up seeing Definition 11 is that it counts the vertical repetitions in it's table of operation (see Example 2) in two different ways. That is the main idea in Proposition 13, and we can make it more general.

The following results have not been seen in the literature by the author of this report.

Proposition 14. Let Q be a finite quandle. Then

$$\frac{\partial qp_Q(x,y)}{\partial x}(1,1) = \frac{\partial qp_Q(x,y)}{\partial y}(1,1)$$

Proof. This is a double counting problem, as we can restate the equality in the following fashion, using directly the definition. First note that $r(x) \geq 1$ and $c(x) \geq 1$, as $x * x = x$ implies that x is in both sets of Definition 11. Then we can derive:

$$\frac{\partial qp_Q(x,y)}{\partial x}(1,1) = \frac{\partial qp_Q(x,y)}{\partial y}(1,1) \Leftrightarrow \sum_{k\in Q} r(x)1^{r(x)-1}1^{c(x)} = \sum_{k\in Q} c(x)1^{c(x)-1}1^{r(x)}$$

So

$$\frac{\partial qp_Q(x,y)}{\partial x}(1,1) = \frac{\partial qp_Q(x,y)}{\partial y}(1,1) \Leftrightarrow \sum_{k\in Q} r(x) = \sum_{x\in Q} c(x) \tag{4.2}$$

Now consider the set $A = \{(x,y) \,|\, x*y = x\} \subseteq Q^2$, and denote $A_x = \{y \in Q \,|\, (x,y) \in A\}$ and $A^y = \{x \in Q \,|\, (x,y) \in A\}$.

It is clear that $\#A = \sum_{x\in Q} \#A_x = \sum_{y\in Q} \#A^y$. Also, $\#A_x = \#\{y \in Q \,|\, x*y = x\} = c(x)$, and similarly $\#A^y = \#\{x \in Q \,|\, x*y = x\} = r(y)$, so the previous equality becomes.

$$\sum_{x\in Q} \#A_x = \sum_{y\in Q} \#A^y \Leftrightarrow \sum_{x\in Q} \#c(x) = \sum_{y\in Q} \#r(y)$$

As required in Equation 4.2. The proof is now complete. □

Proposition 15 (r function behaviour)**.** Consider that Q is a weakly connected quandle. Then r is a constant function on Q.

Proof. We can see that $r(x)$ counts the number of "1's" in the cyclic decomposition of r_x.

That is true because $y \in \{y \in Q \,|\, y * x = y\} \Leftrightarrow r_x(y) = y \Leftrightarrow l_{y,x} = 1$

Then, as Q is a weakly connected quandle, for any $y \in Q$, r_y has the same cyclic type as r_x hence the same number of 1's in the cyclic type, then $r(y) = r(x)$. □

5 Canonical Forms

In this section, Q will be a finite connected quandle with support set $\{1, \cdots, n\}$ and profile $\{1, l_1, \cdots, l_k\}$, where $1 \leq l_1 \leq \cdots \leq l_k$.

In [1], another invariant was constructed, regarding the number of rearrangements of a quandle that preserves some property, the canonical form.

5.1 Natural reorderings and Canonical forms

Definition 13 (Natural reordering)**.** Let Q be a quandle as in the beginning of the section 5.

Let $q \in Q$ and $v : Q \to Q$ a bijection. Suppose that r_q can be written as $r_q = (i_{1,1}i_{1,2}\cdots i_{1,l_1})\cdots(i_{k,1}\cdots i_{k,l_k})(q)$, including trivial cycles and $1 \leq l_1 \leq \cdots \leq l_k$.

We say that v is a natural reordering with respect to r_q if $v(i_{s,t}) = t + \sum_{k=1}^{s-1} l_k$ and $v(q) = n$

We note that a way of writing r_q in disjoint cyclic components completely determines v.

We note that, in an equivalent way, we could say that v is a natural reordering with respect to q if $v \circ r_q \circ v^{-1} = (1\ 2 \cdots l_1)(l_1{+}1\ l_1{+}2\ \cdots l_1{+}l_2)\cdots(\left(\sum_{j=1}^{k-1} l_j\right){+}1 \cdots \left(\sum_{j=1}^{k-1} l_j\right){+}l_k)(n)$

There is exactly one natural reordering for each representation of r_q in a way of the form $r_q = (i_{1,1}i_{1,2}\cdots i_{1,l_1})\cdots(i_{k,1}\cdots i_{k,l_k})(q)$, so we could say that there are $\prod_{j=1}^{k} l_j s_j$ natural reorderings, where s_j stands for the number of l_i such that $i \leq j$ and $l_j = l_i$.

Example 4. Take the connected quandle $Q_{6,1}$, which it's table of operation is in the example Example 2.

We know that $r_3 = (4)(25)(16)(3)$, so the bijection given by

x	$v(x)$
1	4
2	2
3	6
4	1
5	5
6	3

(5.1)

Is a natural reordering with respect to 3, because $v \circ r_3 \circ v^{-1} = (1 \cdots l_1)(l_1 + 1 \cdots l_1 + l_2)\cdots(\left(\sum_{j=1}^{k-1} l_j\right) + 1 \cdots \left(\sum_{j=1}^{k-1} l_j\right) + l_k)(n)$. In fact $v \circ r_3 \circ v^{-1} = (1)(23)(45)(6)$

Definition 14 (Canonical Form)**.** A quandle Q is said to be in a canonical form, or *naturally ordered* if r_n can be written as $r_n = (1 \cdots l_1)(l_1 + 1 \cdots l_1 + l_2)\cdots(\left(\sum_{j=1}^{k-1} l_j\right) + 1 \cdots \left(\sum_{j=1}^{k-1} l_j\right) + l_k)(n)$

We should say that the matrix of a quandle is in the canonical form to stress that this is a property of the operation and not of the set.

We should see that a natural reordering gives a quandle naturally ordered, by defining a new operation $v(a) *' v(b) := v(a * b)$ which is an isomorphism. Each bijection on Q gives to Q another operation in this manner, called the *isomorphic inherited operation.*

Example 5. The quandle $Q_{6,1}$ given by the new operation inherited by v, given in the last example, should be in the canonical form. In fact we can see the new table operation:

$*$	1	2	3	4	5	6
1	1	5	4	3	2	6
2	5	2	6	4	1	3
3	4	6	3	1	5	2
4	3	2	1	4	6	5
5	2	1	3	6	5	4
6	1	3	2	5	4	6

(5.2)

And in fact $r_6 = (1)(23)(45)(6)$, which means that the new quandle is on the canonical form, as envisaged.

The following facts are proved in [1].

Proposition 16. Let Q be a quandle whose elements are naturally ordered. Then any automorphism is a natural reordering.

Proof. We note that the isomorphic inherited operation by an automorphism is the same operation as the one we begin with, and that is clear by $v(a) *' v(b) := v(a * b)$, hence the first is in the canonical form iff the second is in the canonical form.

□

Proposition 17. Suppose that Q is in the canonical form. Then, the set of natural reorderings Nat (Q) is a group that contains the automorphisms.

Proof. The only thing left to show is that natural reorderings are closed for composition. In fact, if u and v are natural reorderings in a quandle in the canonical form then $v \circ r_n \circ v^{-1} = r_n$ and $u \circ r_n \circ u^{-1} = r_n$ so $(u \circ v) \circ r_n \circ (u \circ v)^{-1} = r_n$.

The fact that the natural reorderings are closed under inversion follows from the fact that $v^{-1} = v^{ord(v)-1}$, so is a natural reordering as it is a composition of natural reorderings.

□

5.2 Examples

Here we explore examples of quandles that are distinguished for the number of canonical forms, using the calculations made in [1]. The number of canonical forms is the number of isomorphic quandles in the canonical form on the same set. That number may be calculated with $\frac{\#\ \text{Nat}\ (Q)}{\#\ \text{Aut}}$

Example 6. Consider the quandles $\mathbb{Z}_9$ and $\mathbb{Z}_3 \times \mathbb{Z}_3$, which the operation tables are given by

$*$	0	1	2	3	4	5	6	7	8
0	0	8	7	6	5	4	3	2	1
1	2	1	0	8	7	6	5	4	3
2	4	3	2	1	0	8	7	6	5
3	6	5	4	3	2	1	0	8	7
4	8	7	6	5	4	3	2	1	0
5	1	0	8	7	6	5	4	3	2
6	3	2	1	0	8	7	6	5	4
7	5	4	3	2	1	0	8	7	6
8	7	6	5	4	3	2	1	0	8

(5.3)

$*$	$(0,0)$	$(0,1)$	$(0,2)$	$(1,0)$	$(1,1)$	$(1,2)$	$(2,0)$	$(2,1)$	$(2,2)$
$(0,0)$	$(0,0)$	$(0,2)$	$(0,1)$	$(2,0)$	$(2,2)$	$(2,1)$	$(1,0)$	$(1,2)$	$(1,1)$
$(0,1)$	$(0,2)$	$(0,1)$	$(0,0)$	$(2,2)$	$(2,1)$	$(2,0)$	$(1,2)$	$(1,1)$	$(1,0)$
$(0,2)$	$(0,1)$	$(0,0)$	$(0,2)$	$(2,1)$	$(2,0)$	$(2,2)$	$(1,1)$	$(1,0)$	$(1,2)$
$(1,0)$	$(2,0)$	$(2,2)$	$(2,1)$	$(1,0)$	$(1,2)$	$(1,1)$	$(0,0)$	$(0,2)$	$(0,1)$
$(1,1)$	$(2,2)$	$(2,1)$	$(2,0)$	$(1,2)$	$(1,1)$	$(1,0)$	$(0,2)$	$(0,1)$	$(0,0)$
$(1,2)$	$(2,1)$	$(2,0)$	$(2,2)$	$(1,1)$	$(1,0)$	$(1,2)$	$(0,1)$	$(0,0)$	$(0,2)$
$(2,0)$	$(1,0)$	$(1,2)$	$(1,1)$	$(0,0)$	$(0,2)$	$(0,1)$	$(2,0)$	$(2,2)$	$(2,1)$
$(2,1)$	$(1,2)$	$(1,1)$	$(1,0)$	$(0,2)$	$(0,1)$	$(0,0)$	$(2,2)$	$(2,1)$	$(2,0)$
$(2,2)$	$(1,1)$	$(1,0)$	$(1,2)$	$(0,1)$	$(0,0)$	$(0,2)$	$(2,1)$	$(2,0)$	$(2,2)$

(5.4)

It is clear that the profile is the same in both cases, $\{1,2,2,2\}$, so other invariant shall be used. Those table operations are easily seen to not be in the canonical form.

Those can be rearanged naturally, and is pointed in [1] that for $\mathbb{Z}_9$ there are 64 canonical forms, and for $\mathbb{Z}_3 \times \mathbb{Z}_3$ there are 8 canonical forms, hence they are not isomorphic.

6 Special Quandles

Some examples have been given in the introduction section. The examples that we will provide in this section will be useful to understand some conjectures.

6.1 Alexander Quandles

Proposition 18. A polynomial quotient Alexander Quandle $Q = \frac{\mathbb{Z}_n[t,t^{-1}]}{<h(t)>}$ is latin iff $h(1) \perp n$, hence connected.

Proof. We choose to write h in a polynomial form in t with no coefficients in t^{-k}. This can be done because $< h(t) >=< t^k h(t) >$ and t is a unit in Γ.

Note that the horizontal quandle function $s_j(i) = j * i$ is given by $s_j(a) = tj + (1-t)a$.

Write $h(t) = (1-t)q(t) + r$ as given in the polynomial division algorithm.

Evaluating on $t = 1$ helds that $h(1) \perp n \Leftrightarrow r \perp n$. Then, in the conditions of the proposition, there exists some integer s such that $rs \equiv 1 \mod n$.

So the inverse of $1-t$ is given by $(1-t)^{-1} = -q(t)s$, where $rs \equiv_n 1$.

Define the function $s_j^*(a) = -sq(t)(a-tj)$ in the Quandle Q, this function is actually an inverse function of s_j, since:

$$s_j^* \circ s_j(a) = s_j \circ s_j^*(a) = -sq(t)(1-t)a = -s(h(t)-r)a = -sah(t) + a = a$$

□

So we can construct some quandles that are trivially latin.

Example 7 (Linear quandles). The linear quandles are those alexander quandles of the form $Q = \frac{\mathbb{Z}_n[t,t^{-1}]}{<t-r>}$

Consider the quandles $\frac{\mathbb{Z}_p[t^{\pm 1}]}{<t-h>}$ for an odd prime p and $s \not\equiv_p 1, 0$. These are quandles with p elements, and are latin since $t-h$ is invertible, i.e, $(t-h)(1) = 1-h \perp p$.

6.2 Pattern profile $\{1, p-1, p(p-1)\}$

We will construct a family of Alexander quandles with a specific profile. The goal is to attain a pattern profile, a profile in which all cyclic components are of distinct lenght.

Take a prime number p, and $r \in \mathbb{Z}_p^*$ a primitive root of the multiplicative group. We will see that the quandle $Q = \frac{\mathbb{Z}_n[t,t^{-1}]}{<(t-r)^2>}$ has profile $\{1, p-1, p(p-1)\}$.

We can observe now that it is latin, as $h(1) = (1-r)^2 \neq 0$ in $\mathbb{Z}_p$. Then, it is connected.

Proposition 19. The quandle $Q = \frac{\mathbb{Z}_p[t,t^{-1}]}{<(t-r)^2>}$ has profile $\{1, p-1, p(p-1)\}$, where p is prime and r a primitive root module p.

We already observed that the quandle Q is connected. Then we have only to calculate the cyclic type of the permutation r_0: the inner automorphism given by $r_0(a) = a * 0 = at$. Recall that Q has p^2 elements, and we can rewrite $(t-r)^2 = 0 \Leftrightarrow t^2 = r(2t-r)$

In fact, we will see that (representing the arrow $\rightarrow$ as the application of r_0, and $\rightarrow^n$ the application of r_0^n, for short)

(1) $0 \rightarrow 0$

(2) $r^{j-1}t - r^j \rightarrow tr^j - r^{j+1}$

(3) 1 has a cycle of length $p(p-1)$

The affirmation (1) is trivial, (2) is also trivial, since $r_0(r^{j-1}(t-r)) = r^{j-1}(t^2-rt) = r^{j-1}(2rt - r^2 - rt) = r^{j-1}(rt - r^2) = r^j(t-r)$.

In fact, in order to prove that 1 has order $p(p-1)$, take the smallest positive integer m such that $r_0^m(1) = 1$, so $t^m - 1 = 0$, which means in $\mathbb{Z}_p[t]$ that $t^m - 1 = (t-r)^2 q(t)$, or $(t^m-1)(r) = 0$ and $\frac{\partial t^m - 1}{\partial t}(r) = 0$ Then,

$$r^m = 1 \wedge mr^{m-1} = 0$$

Or

$$r^m = 1 \wedge (p \mid m \vee p \mid r^{m-1})$$

Since r is a primitive root, $p-1 \mid m$, and $r^{m-1} \not\equiv_p 0$ so $p \mid m$.

So 1 has a cycle of length $p(p-1)$. Hence $r_0 = (0)((t-r)\ r(t-r)\ \cdots\ r^{p-2}(t-r))(1 \cdots ...)$ and the quandle has profile $\{1, p-1, p(p-1)\}$ as envisaged.

7 Acknowledgements

I would like to thank my professor Pedro Lopes for all the help in choosing suitable material for this work. Was also a valuable help in teaching how to do such work and in motivating me to go to the boundaries of the mathematical knowledge.

I would like to thanks to the Calouste Gulbenkian Institute for giving me and my colleagues this opportunity of starting a work in investigation.

8 Bibliography

References

[1] Chuichiro Hayashi (2013). *Canonical Forms for Operation Tables of Finite Connected Quandles,* Communications in Algebra, 41:9, 3340-3349, DOI: 10.1080/00927872.2012.685532

[2] Pedro Lopes & Dennis Roseman (2006) *On Finite Racks and Quandles,* Communications in Algebra, 34:1, 371-406, DOI: 10.1080/00927870500346347

[3] Takasaky, M., *Abstraction on symmetric transformations*, (In Japanese) Tohoku Math. J. 49 (1942/3), 145-207

[4] Joyce, D., *A classifiing invariant of knots, the knot quandle*, J.PureAppl. Alg., 23 - 1983, 37-65

[5] Matveev, S., *Distributive grupoids in knot theory*, (in Russian) Mat. Sb. (N.S.) 119(161), 1982 no. 1, 78-88, 160.

[6] Nelson, S., *Classification of Finite Alexander Quandles*, 2000 Mathematics Subject Classification. 57M27.

[7] Nelson, S., *A polynomial invariant of finite quandles*, 2000 MSC: 57M27, 176D99.

[8] Vendramin, L., *On the classification of Quandles of Low Order*, 2010 Mathematics Subject Classification. 57M27.

[9] Andruskiewitsch, N., Graña, M., *From raks to pointed Hopf algebras* 2003, Adv. Math. 178(2):177-243.