Automorphism groups of Quandles

Mohamed Elhamdadi
University of South Florida*

Jennifer MacQuarrie
University of South Florida†

Ricardo Restrepo
Georgia Institute of Technology‡

Abstract

We prove that the automorphism group of the dihedral quandle with n elements is isomorphic to the affine group of the integers mod n, and also obtain the inner automorphism group of this quandle. In [9], automorphism groups of quandles (up to isomorphisms) of order less than or equal to 5 were given. With the help of the software Maple, we compute the inner and automorphism groups of all *seventy three* quandles of order six listed in the appendix of [4]. Since computations of automorphisms of quandles relates to the problem of classification of quandles, we also describe an algorithm implemented in C for computing all quandles (up to isomorphism) of order less than or equal to nine.

KEYWORDS: Quandles, isomorphisms, automorphism groups , inner automorphism groups
2000 MSC: 20B25, 20B20

1 Introduction

Quandles and racks are algebraic structures whose axiomatization comes from Reidemeister moves in knot theory. The earliest known work on racks is contained within 1959 correspondence between John Conway and Gavin Wraith who studied racks in the context of the conjugation operation in a group. Around 1982, the notion of a quandle was introduced independently by Joyce [10] and Matveev [11]. They used it to construct representations of the braid groups. Joyce and Matveev associated to each knot a quandle that determines the knot up to isotopy and mirror image. Since then quandles and racks have been investigated by topologists in order to construct knot and link invariants and their higher analogues (see for example [4] and references therein).

In this paper, we prove that the automorphism group of the dihedral quandle with n elements is isomorphic to the affine group of the integers mod n. In [9], Ho and Nelson gave the list of quandles (up to isomorphism) of orders $n = 3, n = 4$ and $n = 5$ and determined their automorphism groups. In this paper, with the help of the software Maple, we extend their results by computing

*Email: `emohamed@math.usf.edu`
†Email: `jmacquar@mail.usf.edu`
‡Email: `ricrest@gmail.com`

the inner and automorphism groups of all *seventy three* quandles of order six listed in the appendix of [4]. Since computations of automorphisms of quandles relates to the problem of classification of quandles, we also describe an algorithm implemented in C for computing all quandles (up to isomorphism) of order up to nine.

In Section 2, we review the basics of quandles, give examples and describes the automorphisms and inner automorphisms of dihedral quandles . The Inner and automorphism groups of all all *seventy three* quandles of order 6 are computed in section 3. A description of an algorithm which generates all quandles of order up to 9 (up to isomorphisms) is contained in section 4.

Notations Through the paper, the symbol $\mathbb{Z}_n$ will denote the set of integers modulo n and $\mathbb{Z}_n{}^{\times}$ will stand for the group of its units. The dihedral group of order $2m$ will be denoted by D_m. The symbol Σ_n will stand for the symmetric group on the set $\{1, 2, ..., n\}$ and A_n will be its alternating subgroup (even permutations).

2 Automorphism groups of quandles

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

A *quandle*, X, is a set with a binary operation $(a, b) \mapsto a * b$ such that

(1) For any $a \in X$, $a * a = a$.

(2) For any $a, b \in X$, there is a unique $x \in X$ such that $a = x * b$.

(3) For any $a, b, c \in X$, we have $(a * b) * c = (a * c) * (b * c)$.

Axiom (2) states that for each $u \in X$, the map $S_u : X \to X$ with $S_u(x) := x * u$ is a bijection. Its inverse will be denoted by the mapping $\overline{S}_u : X \to X$ with $\overline{S}_u(x) = x \bar{*} u$, so that $(x * u) \bar{*} u = x = (x \bar{*} u) * u$.

A *rack* is a set with a binary operation that satisfies (2) and (3).

Racks and quandles have been studied in, for example, [7, 10, 11].

The axioms for a quandle correspond respectively to the Reidemeister moves of type I, II, and III (see [7], for example).

Here are some typical examples of quandles.

- Any set X with the operation $x * y = x$ for any $x, y \in X$ is a quandle called the *trivial* quandle. The trivial quandle of n elements is denoted by T_n.
- A group $X = G$ with n-fold conjugation as the quandle operation: $a * b = b^{-n} a b^n$.
- Let n be a positive integer. For elements $i, j \in \mathbb{Z}_n$ (integers modulo n), define $i * j \equiv 2j - i \pmod{n}$. Then $*$ defines a quandle structure called the *dihedral quandle*, R_n. This set can be identified with the set of reflections of a regular n-gon with conjugation as the quandle operation.
- Any $\Lambda(= \mathbb{Z}[T, T^{-1}])$-module M is a quandle with $a * b = Ta + (1 - T)b$, $a, b \in M$, called an *Alexander quandle*. Furthermore for a positive integer n, a *mod-n Alexander quandle* $\mathbb{Z}_n[T, T^{-1}]/(h(T))$ is a quandle for a Laurent polynomial $h(T)$. The mod-n Alexander quandle is finite if the coefficients of the highest and lowest degree terms of h are units in $\mathbb{Z}_n$.

A function $f : (X, *) \to (Y, \triangleright)$ between quandles X and Y is a *homomorphism* if $f(a * b) = f(a) \triangleright f(b)$ for any $a, b \in X$. We will denote the group of automorphisms of the quandle X by $Aut(X)$. Axioms (2) and (3) respectively state that for each $u \in X$, the map $S_u : X \to X$ is respectively a bijection and a quandle homomorphism. Lets call the subgroup of $Aut(X)$, generated by the *symmetries* S_x, the *inner* automorphism group of X denoted by $Inn(X)$. By axiom (3), the map $S : X \to Inn(X)$ sending u to S_u satisfies the equation $S_z\ S_y = S_{y*z}\ S_z, \quad \forall y, z \in X$, which can be written as $S_z\ S_y\ {S_z}^{-1} = S_{y*z}$. Thus, if the group $Inn(X)$ is considered as a quandle with conjugation then the map S becomes a quandle homomorphism. As noted in [1] p 184, the map S is not injective in general. The quandle $(X, *)$ is called $faithful$ when the map S is injective. If $(X, *)$ is $faithful$ then the center of $Inn(X)$ is trivial.

2.1 Automorphism groups and Inner Automorphism groups of dihedral quandles

Now we characterize the automorphisms of the dihedral quandles. For any non-zero element a in $\mathbb{Z}_n$ and any $b \in \mathbb{Z}_n$, consider the mapping $f_{a,b} : \mathbb{Z}_n \to \mathbb{Z}_n$ sending x to $ax + b$, called affine transformation over $\mathbb{Z}_n$.

Theorem 2.1 *Let $R_n = \mathbb{Z}_n$ be the dihedral quandle with the operation $i * j = 2j - i\ (mod\ n)$. Then the automorphism group $Aut(R_n)$ is isomorphic to the affine group $A\!f\!f(\mathbb{Z}_n)$.*

Proof. It is clear that for $a \neq 0$, the mapping $f_{a,b}$ (with $f_{a,b}(x) = ax + b$) is a quandle homomorphism. It is a bijective mapping if and only if $a \in {\mathbb{Z}_n}^{\times}$. Now we show that any quandle automorphism of $\mathbb{Z}_n$ (with the operation $x * y = 2y - x$) is an affine transformation $f_{a,b}$ for some $a \in {\mathbb{Z}_n}^{\times}$ and $b \in \mathbb{Z}_n$. Let $f \in Aut(\mathbb{Z}_n)$, then $\forall x, y \in \mathbb{Z}_n, f(2y - x) = 2f(y) - f(x)$. Now consider the mapping $g : \mathbb{Z}_n \to \mathbb{Z}_n$ given by $g(x) = f(x) - f(0)$. The mapping g also satisfies $g(2y - x) = 2g(y) - g(x)$. We have $g(0) = 0$ and thus $g(-a) = -g(a)$. We now prove linearity of g, that is $g(\lambda x) = \lambda g(x)$ for any $\lambda \in \mathbb{Z}_n$. We have $g(2b - a) = 2g(b) - g(a)$, thus $g(2b) = 2g(b)$ and by induction on even integers $g(2ka) = 2kg(a)$, for all k. Now we do induction on odd integers: $g[(2k+1)a] = g[2ka - (-a)] = 2kg(a) - g(-a) = 2kg(a) + g(a) = (2k+1)g(a)$. Now g is a bijection if and only if $\lambda \in {\mathbb{Z}_n}^{\times}$ which ends the proof ■

Since the affine group Aff($\mathbb{Z}_n$) is semi-direct product group $\mathbb{Z}_n \rtimes {\mathbb{Z}_n}^{\times}$, we have

Corollary 2.2 *The cardinal of $Aut(\mathbb{Z}_n)$ is $n\ \phi(n)$, where ϕ denotes the Euler function.*

For the dihedral quandle $R_n = \mathbb{Z}_n$ and for each $i \in \mathbb{Z}_n$ the symmetry S_i given by $S_i(j) = 2i - j\ (mod\ n)$, can be though of as a reflection of a regular n-gon. If n is odd, the axis of symmetry of S_i connects the vertex i to the mid-point of the side opposite to i. If $n = 2m$ is even, the axis of symmetry of S_i passes through the opposite vertices i and $i+m$ (mod $2m$). From these observations, we have the easy characterization of the inner automorphism group of dihedral quandles given by the following

Theorem 2.3 *The inner automorphism group $Inn(R_n)$ of the dihedral quandle R_n is isomorphic to the dihedral group $D_{\frac{m}{2}}$ of order m where m is the least common multiple of n and 2.*

Theorem 2.4 *Let G be a group and let the quandle X be the group G as a set with the conjugation $x * y = yxy^{-1}$ as operation. This quandle is usually denoted by $Conj(G)$. Then the Inner automorphism group of X is isomorphic (as a group) to the quotient of G by its center $Z(G)$.*

Proof. The proof is straightforward from the fact that in this case the surjective map $S : X \to Inn(X)$ sending $a \in X$ to S_a is a quandle homomorphism with kernel the center $Z(G)$ of G. ∎

Example The symetric group Σ_3 is the smallest group with trivial center then $Inn(Conj(\Sigma_3)) \cong \Sigma_3$.

The converse of theorem 2.4 is also true, namely if $(X, *)$ is a quandle for which the map $S : X \to Inn(X)$ is one-to-one and onto then $(X, *) \cong Conj(Inn(X))$ with $Z(Inn(X))$ being trivial group. An interesting question would be to calculate the automorphism groups $Aut(Conj(G))$. Obviously for the symmetric group Σ_3, we have $Aut(Conj(\Sigma_3)) \cong Inn(Conj(\Sigma_3)) \cong \Sigma_3$.

3 Automorphism and Inner Automorphism groups of quandles of order 6

In this section, we compute the automorphism groups and the inner automorphism groups of all *seventy three* quandles of order six. The computation is accomplished with the help of the software Maple which also allows the computation of the inner and automorphism groups for quandles of order 7 and 8. Since the numbers of isomorphism classes of quandles of order 7 and 8 are respectively 298 and 1581, we decided not to include these two cases in this paper.
We describe each quandle Q_j of order 6 for $1 \leq j \leq 73$ by explicitly giving each symmetry S_k for $1 \leq k \leq 6$, in terms of products of disjoint cycles. The symmetries are the columns in the Cayley table of the quandle. For example the quandle, denoted Q_{46} in table 2 below, with the Cayley table

$$\begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 \\ 2 & 2 & 5 & 5 & 2 & 5 \\ 3 & 4 & 3 & 3 & 4 & 4 \\ 4 & 3 & 4 & 4 & 3 & 3 \\ 5 & 5 & 2 & 2 & 5 & 2 \\ 6 & 6 & 6 & 6 & 6 & 6 \end{bmatrix}$$

is described by the permutations of the six elements set $\{1, 2, 3, 4, 5, 6\}$, $S_1 = (1)$, $S_2 = (34)$, $S_3 = (25)$, $S_4 = (25)$, $S_5 = (34)$, $S_6 = (25)(34)$. Here and through the rest of the paper, every permutation is written as a product of transpositions. For example, $S_1 = (1)$ means that S_1 is the identity permutation. The permutation $S_4 = (25)$ stands for the transposition sending 2 to 5 and $S_6 = (25)(34)$ stands for the product of the two transpositions (25) and (34).
In this example $Aut(Q_{46}) = D_4$, the dihedral group of 8 elements and $Inn(Q_{46}) = \mathbb{Z}_2 \times \mathbb{Z}_2$ is the direct product of two copies of $\mathbb{Z}_2$. Another example given in table 3 is $Aut(Q_{49}) = D_5$ the dihedral group of order 10 and $Inn(Q_{46}) = \mathbb{Z}_5 \rtimes \mathbb{Z}_4$, the semidirect product of the cyclic group $\mathbb{Z}_5$ by $\mathbb{Z}_4$.

Quandle	Disjoint Cycle Notation for the Columns of the Quandle
Q_1	$(1),(1),(1),(1),(1),(1)$
Q_2	$(1),(1),(1),(1),(1),(12)$
Q_3	$(1),(1),(1),(1),(1),(132)$
Q_4	$(1),(1),(1),(1),(1),(1243)$
Q_5	$(1),(1),(1),(1),(1),(12)(34)$
Q_6	$(1),(1),(1),(1),(1),(15234)$
Q_7	$(1),(1),(1),(1),(1),(134)(25)$
Q_8	$(1),(1),(1),(1),(12),(12)$
Q_9	$(1),(1),(1),(1),(12),(12)(34)$
Q_{10}	$(1),(1),(1),(1),(12),(34)$
Q_{11}	$(1),(1),(1),(1),(132),(132)$
Q_{12}	$(1),(1),(1),(1),(132),(123)$
Q_{13}	$(1),(1),(1),(1),(1243),(1243)$
Q_{14}	$(1),(1),(1),(1),(1243),(1342)$
Q_{15}	$(1),(1),(1),(1),(1243),(14)(23)$
Q_{16}	$(1),(1),(1),(1),(12)(34),(12)(34)$
Q_{17}	$(1),(1),(1),(1),(12)(34),(13)(24)$
Q_{18}	$(1),(1),(1),(12),(12),(12)$
Q_{19}	$(1),(1),(1),(12),(12),(12)(45)$
Q_{20}	$(1),(1),(1),(12),(12),(45)$
Q_{21}	$(1),(1),(1),(132),(132),(132)$
Q_{22}	$(1),(1),(1),(132),(132),(123)$
Q_{23}	$(1),(1),(1),(132),(132),(45)$
Q_{24}	$(1),(1),(1),(132),(132),(123)(45)$
Q_{25}	$(1),(1),(1),(132),(132),(132)(45)$
Q_{26}	$(1),(1),(1),(12)(56),(12)(46),(12)(45)$
Q_{27}	$(1),(1),(1),(12)(56),(13)(46),(23)(45)$
Q_{28}	$(1),(1),(1),(56),(46),(45)$
Q_{29}	$(1),(1),(1),(123)(56),(123)(46),(123)(45)$
Q_{30}	$(1),(1),(12),(12),(12),(12)$
Q_{31}	$(1),(1),(12),(12),(12),(12)(34)$
Q_{32}	$(1),(1),(12),(12),(12),(34)$
Q_{33}	$(1),(1),(12),(12),(12),(345)$
Q_{34}	$(1),(1),(12),(12),(12),(12)(345)$
Q_{35}	$(1),(1),(12),(12),(12)(34),(12)(34)$
Q_{36}	$(1),(1),(12),(12),(12)(34),(34)$
Q_{37}	$(1),(1),(12),(12),(34),(34)$

Table 1: Quandles of order 6 in term of disjoint cycles of columns - part 1

Quandle	Disjoint Cycle Notation for the Columns of the Quandle
Q_{38}	$(1),(1),(12),(12)(56),(12)(46),(12)(45)$
Q_{39}	$(1),(1),(12),(56),(46),(45)$
Q_{40}	$(1),(1),(12)(45),(12)(36),(12)(36),(12)(45)$
Q_{41}	$(1),(1),(12)(45),(36),(36),(12)(45)$
Q_{42}	$(1),(1),(45),(36),(36),(45)$
Q_{43}	$(1),(1),(456),(365),(346),(354)$
Q_{44}	$(1),(1),(12)(456),(12)(365),(12)(346),(12)(354)$
Q_{45}	$(1),(34),(25),(25),(34),(34)$
Q_{46}	$(1),(34),(25),(25),(34),(25)(34)$
Q_{47}	$(1),(34),(256),(256),(34),(34)$
Q_{48}	$(1),(354),(26)(45),(26)(35),(26)(34),(345)$
Q_{49}	$(1),(36)(45),(25)(46),(23)(56),(26)(34),(24)(35)$
Q_{50}	$(1),(3546),(2456),(2365),(2643),(2534)$
Q_{51}	$(1),(3546),(2564),(2653),(2436),(2345)$
Q_{52}	$(23),(13),(12),(56),(46),(45)$
Q_{53}	$(23),(14),(14),(23),(23),(23)$
Q_{54}	$(23),(14),(14),(23),(23),(14)(23)$
Q_{55}	$(23),(14),(14),(23),(23),(14)$
Q_{56}	$(23),(14),(14),(23),(14)(23),(14)(23)$
Q_{57}	$(23),(154),(154),(23),(23),(23)$
Q_{58}	$(23),(154),(154),(23),(23),(154)(23)$
Q_{59}	$(23),(154),(154),(23),(23),(154)$
Q_{60}	$(23),(154),(154),(23),(23),(145)$
Q_{61}	$(23),(154),(154),(23),(23),(145)(23)$
Q_{62}	$(23),(45),(45),(16)(23),(16)(23),(23)$
Q_{63}	$(23),(45),(45),(16),(16),(23)$
Q_{64}	$(23),(1564),(1564),(23),(23),(23)$
Q_{65}	$(23),(15)(46),(15)(46),(23),(23),(23)$
Q_{66}	$(23),(15)(46),(15)(46),(15)(23),(23),(15)(23)$
Q_{67}	$(243),(165),(165),(165),(243),(243)$
Q_{68}	$(2354),(1463),(1265),(1562),(1364),(2453)$
Q_{69}	$(2354),(16)(34),(16)(25),(16)(25),(16)(34),(2453)$
Q_{70}	$(23)(45),(15)(36),(14)(26),(15)(36),(14)(26),(23)(45)$
Q_{71}	$(23)(45),(15)(46),(14)(56),(16)(23),(16)(23),(23)(45)$
Q_{72}	$(23)(45),(13)(46),(12)(56),(15)(26),(14)(36),(24)(35)$
Q_{73}	$(23)(45),(16)(45),(16)(45),(16)(23),(16)(23),(23)(45)$

Table 2: Quandles of order 6 in term of disjoint cycles of columns - part 2

Quandle X	Inn(X)	Aut(X)	Quandle X	Inn(X)	Aut(X)
Q_1	$\{1\}$	Σ_6	Q_{38}	$D_3 \times \mathbb{Z}_2$	$D_3 \times \mathbb{Z}_2$
Q_2	$\mathbb{Z}_2$	$D_3 \times \mathbb{Z}_2$	Q_{39}	$D_3 \times \mathbb{Z}_2$	$D_3 \times \mathbb{Z}_2$
Q_3	$\mathbb{Z}_3$	$\mathbb{Z}_6$	Q_{40}	$\mathbb{Z}_2 \times \mathbb{Z}_2$	$D_4 \times \mathbb{Z}_2$
Q_4	$\mathbb{Z}_4$	$\mathbb{Z}_4$	Q_{41}	$\mathbb{Z}_2 \times \mathbb{Z}_2$	$\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$
Q_5	$\mathbb{Z}_2$	D_4	Q_{42}	$\mathbb{Z}_2 \times \mathbb{Z}_2$	$D_4 \times \mathbb{Z}_2$
Q_6	$\mathbb{Z}_5$	$\mathbb{Z}_5$	Q_{43}	A_4	$A_4 \times \mathbb{Z}_2$
Q_7	$\mathbb{Z}_6$	$\mathbb{Z}_6$	Q_{44}	$A_4 \times \mathbb{Z}_2$	$A_4 \times \mathbb{Z}_2$
Q_8	$\mathbb{Z}_2$	$\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$	Q_{45}	$\mathbb{Z}_2 \times \mathbb{Z}_2$	$\mathbb{Z}_2 \times \mathbb{Z}_2$
Q_9	$\mathbb{Z}_2 \times \mathbb{Z}_2$	$\mathbb{Z}_2 \times \mathbb{Z}_2$	Q_{46}	$\mathbb{Z}_2 \times \mathbb{Z}_2$	D_4
Q_{10}	$\mathbb{Z}_2 \times \mathbb{Z}_2$	D_4	Q_{47}	$\mathbb{Z}_6$	$\mathbb{Z}_6$
Q_{11}	$\mathbb{Z}_3$	$\mathbb{Z}_6$	Q_{48}	D_3	D_3
Q_{12}	$\mathbb{Z}_3$	D_3	Q_{49}	D_5	$\mathbb{Z}_5 \rtimes \mathbb{Z}_4$
Q_{13}	$\mathbb{Z}_4$	$\mathbb{Z}_4 \times \mathbb{Z}_2$	Q_{50}	$\mathbb{Z}_5 \rtimes \mathbb{Z}_4$	$\mathbb{Z}_5 \rtimes \mathbb{Z}_4$
Q_{14}	$\mathbb{Z}_4$	D_4	Q_{51}	$\mathbb{Z}_5 \rtimes \mathbb{Z}_4$	$\mathbb{Z}_5 \rtimes \mathbb{Z}_4$
Q_{15}	$\mathbb{Z}_4$	$\mathbb{Z}_4$	Q_{52}	$D_3 \times D_3$	$(D_3 \times D_3) \rtimes \mathbb{Z}_2$
Q_{16}	$\mathbb{Z}_2$	$D_4 \times \mathbb{Z}_2$	Q_{53}	$\mathbb{Z}_2 \times \mathbb{Z}_2$	$\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$
Q_{17}	$\mathbb{Z}_2 \times \mathbb{Z}_2$	D_4	Q_{54}	$\mathbb{Z}_2 \times \mathbb{Z}_2$	$\mathbb{Z}_2 \times \mathbb{Z}_2$
Q_{18}	$\mathbb{Z}_2$	$D_3 \times \mathbb{Z}_2$	Q_{55}	$\mathbb{Z}_2 \times \mathbb{Z}_2$	D_4
Q_{19}	$\mathbb{Z}_2 \times \mathbb{Z}_2$	$\mathbb{Z}_2 \times \mathbb{Z}_2$	Q_{56}	$\mathbb{Z}_2 \times \mathbb{Z}_2$	$D_4 \times \mathbb{Z}_2$
Q_{20}	$\mathbb{Z}_2 \times \mathbb{Z}_2$	$\mathbb{Z}_2 \times \mathbb{Z}_2$	Q_{57}	$\mathbb{Z}_6$	$\mathbb{Z}_6$
Q_{21}	$\mathbb{Z}_3$	$D_3 \times \mathbb{Z}_3$	Q_{58}	$\mathbb{Z}_6$	$\mathbb{Z}_6$
Q_{22}	$\mathbb{Z}_3$	$\mathbb{Z}_6$	Q_{59}	$\mathbb{Z}_6$	$\mathbb{Z}_6$
Q_{23}	$\mathbb{Z}_6$	$\mathbb{Z}_6$	Q_{60}	$\mathbb{Z}_6$	$\mathbb{Z}_6$
Q_{24}	$\mathbb{Z}_6$	$\mathbb{Z}_6$	Q_{61}	$\mathbb{Z}_6$	$\mathbb{Z}_6$
Q_{25}	$\mathbb{Z}_6$	$\mathbb{Z}_6$	Q_{62}	$\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$	$\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$
Q_{26}	D_3	$D_3 \times \mathbb{Z}_2$	Q_{63}	$\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$	$A_4 \times \mathbb{Z}_2$
Q_{27}	D_3	D_3	Q_{64}	$\mathbb{Z}_4 \times \mathbb{Z}_2$	$\mathbb{Z}_4 \times \mathbb{Z}_2$
Q_{28}	D_3	$D_3 \times D_3$	Q_{65}	$\mathbb{Z}_2 \times \mathbb{Z}_2$	$D_4 \times \mathbb{Z}_2$
Q_{29}	$D_3 \times \mathbb{Z}_3$	$D_3 \times \mathbb{Z}_3$	Q_{66}	$\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$	$\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$
Q_{30}	$\mathbb{Z}_2$	$\Sigma_4 \times \mathbb{Z}_2$	Q_{67}	$\mathbb{Z}_3 \times \mathbb{Z}_3$	$D_3 \times \mathbb{Z}_3$
Q_{31}	$\mathbb{Z}_2 \times \mathbb{Z}_2$	$\mathbb{Z}_2 \times \mathbb{Z}_2$	Q_{68}	Σ_4	Σ_4
Q_{32}	$\mathbb{Z}_2 \times \mathbb{Z}_2$	$\mathbb{Z}_2 \times \mathbb{Z}_2$	Q_{69}	D_4	D_4
Q_{33}	$\mathbb{Z}_6$	$\mathbb{Z}_6$	Q_{70}	D_3	$D_3 \times \mathbb{Z}_2$
Q_{34}	$\mathbb{Z}_6$	$\mathbb{Z}_6$	Q_{71}	D_4	D_4
Q_{35}	$\mathbb{Z}_2 \times \mathbb{Z}_2$	$\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$	Q_{72}	Σ_4	Σ_4
Q_{36}	$\mathbb{Z}_2 \times \mathbb{Z}_2$	$\mathbb{Z}_2 \times \mathbb{Z}_2$	Q_{73}	$\mathbb{Z}_2 \times \mathbb{Z}_2$	$\Sigma_4 \times \mathbb{Z}_2$
Q_{37}	$\mathbb{Z}_2 \times \mathbb{Z}_2$	$\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$			

Table 3: A table of the quandles of order 6 with their Inner and Automorphism groups

4 Algorithm description

In the quest of finding computationally the quandles of certain order up to isomorphism, we are cursed by the fact that any sort of naive algorithm will take an exponential time (in the order of the quandle) to do such task. Therefore, we are required to exploit structural or logical aspects of the quandle theory to reduce the running time at least by a proportional factor, making the algorithm 'less-galactic', in CS jargon.

4.1 Phase 1: List generation.

In initial versions of the *quandles algorithm* [8], the set of all matrices such that every row is a permutation $[n]$, is generated. After this, the matrices that do not correspond to the operation table of a quandle (i.e., such that do not satisfy the quandle axiom), are ruled out. We call this initial process the *list generation*, and its purpose is to **list a set of quandles such that among then, we are guaranteed to find representatives for all isomorphic classes of quandles of order** n. A further improvement in this process consists in verifying the quandles axiom *on-line*, this means that, during the generation of the matrices, the axioms are immediately verified, a process that was also carried out in [8]. We elaborate this improvement to a higer level: Besides verifying the quandle axioms on-line, we also fill in online, entries that are implied by the quandle axioms. To exemplify such process, suppose that at a certain step our algorithm has completed the following partial table of a quandle

$$\begin{bmatrix} a & a & & & \\ c & b & b & & \\ b & c & c & & \\ & & & d & \\ & & & & e \end{bmatrix}$$

then, by use of the property $(a * c) * a = a * (c * a)$, we have that $(a * c) * a = a$. Therefore $(a * c) = a \bar{*} a = a$, so that the table completes as

$$\begin{bmatrix} a & a & a & & \\ c & b & b & & \\ b & c & c & & \\ & & & d & \\ & & & & e \end{bmatrix}.$$

A more interesting example is the following. Starting with the following partial quandle table

$$\begin{bmatrix} a & a & a & b & \\ c & b & b & & \\ b & c & c & & \\ & & & d & \\ & & & c & e \end{bmatrix},$$

through the application of the quandle axioms several times, we complete some fewer entries, concluding at the end that such partial table cannot be extended to a valid quandle table:

$$\xrightarrow{(e*a)*d=(e*d)*(a*d)} \begin{bmatrix} a & a & a & b & \\ c & b & b & & \\ b & c & c & & \\ & & & d & \\ e & & & c & e \end{bmatrix} \xrightarrow{(a*e)*d=(a*d)*(e*d)} \begin{bmatrix} a & a & a & b & a \\ c & b & b & & \\ b & c & c & & \\ & & & d & \\ e & & & c & e \end{bmatrix}$$

$$\xrightarrow{\text{uniqueness}} \begin{bmatrix} a & a & a & b & a \\ c & b & b & & \\ b & c & c & & \\ d & & & d & \\ e & & & c & e \end{bmatrix}$$

and this last table contradicts the axiom $(a * d) * a = a * (d * a)$.

In general, the rules that are used for this 'completion' process are the following:

Suppose that $j * i = k$, then

Rule 1: $k * a = (j * a) * (i * a)$

1. If $(j * a) * (i * a)$ cannot be retrieved from the table and $k * a$, $i * a$ and $j * a$ can be retrieved from the table, then
   (a) If $(k * a) \bar{*} (i * a)$ can be retrieved from the table, the table is not valid.
   (b) Otherwise, necesarily $(j * a) * (i * a) = k * a$.
2. Otherwise, if $k * a$ cannot be retrieved from the table and $(j * a) * (i * a)$ can be retrieved from the table, then
   (a) If $((j * a) * (i * a)) \bar{*} a$ can be retrieved from the table, the table is not valid.
   (b) Otherwise, necesarily $k * a = (j * a) * (i * a)$.
3. Otherwise, if $(j * a) * (i * a)$ and $k * a$ can be retrieved from the table and $(j * a) * (i * a) \neq k * a$, the table is not valid.

Rule 2: $(a * j) * i = (a * i) * k$

1. If $(a * i) * k$ cannot be retrieved from the table and $(a * j) * i$ and $a * i$ can be retrieved from the table, then
   (a) If $((a * j) * i) \bar{*} k$ can be retrieved from the table, the table is not valid.
   (b) Otherwise, necesarily $(a * i) * k = (a * j) * i$.
2. Otherwise, if $(a * j) * i$ cannot be retrieved from the table and $(a * j)$ and $(a * i) * k$ can be retrieved from the table, then

(a) If $((a * i) * k) \bar{*} i$ can be retrieved from the table, the table is not valid.

(b) Otherwise, necesarily $(a * j) * i = (a * i) * k$.

3. Otherwise, if $(a * j) * i$ and $(a * i) * k$ can be retrieved from the table and $(a * j) * i \neq (a * i) * k$, the table is not valid.

Rule 3: $(j * a) * i = k * (a * i)$

1. If $k * (a * i)$ cannot be retrieved from the table and $(j * a) * i$ and $a * i$ can be retrieved from the table, then

   (a) If $((j * a) * i) \bar{*} (a * i)$ can be retrieved from the table, the table is not valid.

   (b) Otherwise, necesarily $k * (a * i) = (j * a) * i$.

2. Otherwise, if $(j * a) * i$ cannot be retrieved from the table and $(j * a)$ and $k * (a * i)$ can be retrieved from the table, then

   (a) If $(k * (a * i)) \bar{*} i$ can be retrieved from the table, the table is not valid.

   (b) Otherwise, necesarily $(j * a) * i = k * (a * i)$.

3. Otherwise, if $(j * a) * i$ and $k * (a * i)$ can be retrieved from the table and $(j * a) * i \neq k * (a * i)$, the table is not valid.

Rule 4: $((j \bar{*} a) * (i \bar{*} a)) * a = k$

1. If $((j \bar{*} a) * (i \bar{*} a)) * a$ cannot be retrieved from the table and $((j \bar{*} a) * (i \bar{*} a))$ can be retrieved from the table, then

   (a) If $k \bar{*} a$ can be retrieved from the table, the table is not valid.

   (b) Otherwise, necesarily $((j \bar{*} a) * (i \bar{*} a)) * a = k$.

2. Otherwise, if $((j \bar{*} a) * (i \bar{*} a)) * a$ can be retrieved from the table and $((j \bar{*} a) * (i \bar{*} a)) * a \neq k$, the table is not valid.

Rule 5: $k = ((j \bar{*} a) * i) * (a * i)$

1. If $((j \bar{*} a) * i) * (a * i)$ cannot be retrieved from the table and $(a * i)$ and $((j \bar{*} a) * i)$ can be retrieved from the table, then

   (a) If $k \bar{*} (a * i)$ can be retrieved from the table, the table is not valid.

   (b) Otherwise, necesarily $((j \bar{*} a) * i) * (a * i) = k$.

2. Otherwise, if $((j\bar{*}a)*i)*(a*i)$ can be retrieved from the table and $k \neq ((j\bar{*}a)*i)*(a*i)$, the table is not valid.

Another easy improvement, which certainly reduces considerably the size of the list of quandles to output in this first step of the quandles algorithm, comes from elementary logic: When you are trying to generate all the models of cardinality n of a theory (in our case the theory of quandles), we can start introducing constants and the corresponding relations between these constants one by one (in a valid way), until we get n constants (so, the possible ways to generate the relations between constants will correspond to the models of the theory). This is exactly what any algorithm will do, just in the language of logic, but the point to emphasize is that, when a new constant is introduced, the name of such constant is irrelevant. This is a trivial logic fact, but one that was not used in previous versions of this listing procedure. For example, if we aim to complete the entry $b*a$ of the partial table

$$\begin{bmatrix} a & & & & \\ & b & & & \\ & & c & & \\ & & & d & \\ & & & & e \end{bmatrix},$$

then among the options $b*a=c$, $b*a=d$ and $b*a=e$, the choice is irrelevant, because at such step, the constants c, d, e are not in context.

The following are some benchmarks concerning this first step of the process:

size	quandles	time (sec.)
2	1	0
3	5	0
4	27	0
5	190	0
6	1833	0
7	22104	1 to 2
8	359859	24 to 34

4.2 Phase 2: Isomorphic comparison

After the previous listing procedure has been elaborated (or more precisely, **while** the listing procedure is elaborated), we want to eliminate irrelevant quandles, that is, we want to leave only one representative per isomorphism class. For such comparison process, instead of doing a brute force algorithm that takes all possible bijections and checks for isomorphic equivalence, we can do two things:

(1) Use simple invariant checks, like number of cycles in every row action, to discard rapidly some nonisomorphic pairs of quandles.

(2) Use the quandle axioms to reduce the complexity of the isomorphic comparison process.

Regarding (2), we employ the quandle axioms to extend appropriately a partial isomorphism among valid possibilities, using the following rules:

Suppose that $\phi(i) = j$.

Rule 1: $\phi(b) *' j = \phi(b*i)$

1. If $\phi(b)$ and $\phi(b*i)$ are defined, and $\phi(b)*' j \neq \phi(b*i)$, then the isomorphism is not valid.

2. If $\phi(b*i)$ is not defined and $\phi(b)$ is defined, necessarily $\phi(b*i) = \phi(b)*' j$, and this may or may not contradict the injectivity of ϕ.

3. If $\phi(b*i)$ is defined and $\phi(b)$ is not defined, necessarily $\phi(b) = \phi(b*i)\,\bar{*}' j$, and this may or may not contradict the injectivity of ϕ.

Rule 2: $j *' \phi(b) = \phi(i*b)$

1. If $\phi(b)$ and $\phi(i*b)$ are defined, and $j *' \phi(b) \neq \phi(i*b)$, then the isomorphism is not valid.

2. If $\phi(i*b)$ is not defined and $\phi(b)$ is defined, necessarily $\phi(i*b) = j *' \phi(b)$, and this may or may not contradict the injectivity of ϕ.

Rule 3: $\phi(i\bar{*}b) *' \phi(b) = j$

1. If $\phi(b)$ and $\phi(i\bar{*}b)$ are defined, and $\phi(i\bar{*}b) *' \phi(b) \neq j$, then the isomorphism is not valid.

2. If $\phi(b)$ is defined and $\phi(i\bar{*}b)$ is not defined, necessarily, $\phi(i\bar{*}b) = j\bar{*}'\phi(b)$, and this may or may not contradict the injectivity of ϕ.

For the following benchmark, we do an exhaustive algorithm for isomorphism comparison. Notice that is tractable up to $n = 6$.

size	quandles	time (sec.)
2	1	0
3	3	0
4	7	0
5	22	0
6	73	29 – 32

For the following benchmark we apply the improved isomorphism comparison, by using the rules described previously. This improves the running time by a factor of 10 approx.

size	quandles	time (sec.)
2	1	0
3	3	0
4	7	0
5	22	0
6	73	3
7	298	330

Checking invariants:

Certainly, it is not necessary to do an isomorphism comparison (improved or not), if we know before hand that the quandles to be compared are ‘too different’. Therefore, a pre-comparison of some invariants fast to calculate, would boost the running time. For early versions of the algorithm, we introduced invariants based on the permutation structure of the columns of the quandle table. For example, for the following benchmark, we simply count the total number of cycles among all columns of the quandle table. The comparison of such invariant improves the running time by another factor of 10:

size	quandles	time (sec.)
2	1	0
3	3	0
4	7	0
5	22	0
6	73	0
7	298	34

For the following benchmark we go down one more level, now taking as invariant the superset consisting of the number of cycles of every columns. This improves the running time by a factor of 4 approx.

size	quandles	time (sec.)
2	1	0
3	3	0
4	7	0
5	22	0
6	73	0
7	298	9

For the following benchmark we refine the previous invariant, by considering the superset of supersets of cycle lengths of every column, At this level of improvement, the case $n = 8$ is computationally tractable.

size	quandles	time (sec.)
2	1	0
3	3	0
4	7	0
5	22	0
6	73	0
7	298	6
8	1581	458

Further improvements will be introduced in next versions of the algorithm, whose source is available at the web address http://people.math.gatech.edu/~restrepo/quandles.html.
Another invariants suggested by Professor Edwin Clark, which according to his experiments seem to distinguish isomorphic classes effectively, take in account the structure of the rows of the quandle. The number of isomorphism of quandles of order 3, 4, 5, 6, 7, 8 and 9 we obtain are respectively 3, 7, 22, 73, 298, 1581, 11079. These same numbers are obtained by James McCarron in [12].
Acknowledgments The authors would like to thank professor Edwin Clark for his help and fruitful suggestions.

References

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

[2] Brieskorn E., 1988. *Automorphic sets and singularities,* Contemporary math. 78, 45–115.

[3] Carter S., Elhamdadi M., Nikifourou M., and Saito M., 2003. *Extensions of quandles and cocycle knot invariants,* J. Knot Theory Ramifications 12, no. 6, 725-738.

[4] Carter S., Kamada S., and Saito M., 2004 *Surfaces in 4-space,* Encyclopaedia of Mathematical Sciences, 142. Low-Dimensional Topology, III. Springer-Verlag, Berlin.

[5] Creel, C. ; Nelson, S. *Symbolic computation with finite biquandles,* J. Symbolic Comput. 42 (2007), no. 10, 9921000.

[6] Ellis G., *Computing group resolutions,* J. Symbolic Comput. 38 (2004), no. 3, 10771118.

[7] Fenn R., and Rourke C., 1992. *Racks and links in codimension two,* J. Knot Theory Ramifications, 1, 343-406.

[8] Henderson, R. ; Macedo, T. ; Nelson, S. *Symbolic computation with finite quandles,* J. Symbolic Comput. 41 (2006), no. 7, 811817.

[9] Ho, B.; Nelson S. *Matrices and finite quandles,* Homology Homotopy Appl. 7 (2005), no. 1, 197–208.

[10] Joyce, D., *A classifying invariant of knots, the knot quandle,* J. Pure Appl. Alg., 23, 37–65.

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

[12] McCarron J., *The On-Line Encyclopedia of integer sequences,* http://oeis.org/A181769.

[13] Ryder, H., *The congruence structure of racks,* Comm. Algebra 23 (1995), no. 13, 49714989.

[14] Ehrman, G.; Gurpinar, A.; Thibault, M.; Yetter, D. N. , *Toward a classification of finite quandles,* J. Knot Theory Ramifications 17 (2008), no. 4, 511520.