Toward a Classification of Finite Quandles

G. Ehrman, A. Gurpinar
M. Thibault, D.N. Yetter
Department of Mathematics
Kansas State University
Manhattan, KS 66503 *

ABSTRACT

This paper summarizes substantive new results derived by a student team (the first three authors) under the direction of the fourth author at the 2005 session of the KSU REU "Brainstorming and Barnstorming". The main results are a decomposition theorem for quandles in terms of an operation of 'semidisjoint union' showing that all finite quandles canonically decompose via iterated semidisjoint unions into connected subquandles, and a structure theorem for finite connected quandles with prescribed inner automorphism group. The latter theorem suggests a new approach to the classification of finite connected quandles.

Keywords: quandle, connected, decomposition theorem, inner automorphism group

Mathematics Subject Classification 2000: 57M27, 20N99

1. Introduction

Quandles were introduced by Joyce [1] [2] as an algebraic invariant of classical knots and links.

Definition 1.1. [1] [2] A *quandle* $(Q, \triangleright)$ is a set Q equipped with an binary operation $\triangleright$ such that the following conditions hold:

- every element in the set is *idempotent* with respect to $\triangleright$: $\forall x \in Q, x \triangleright x = x$
- $\triangleright$ is *invertible* as a right-acting operator: $\forall a, b \in Q, \exists! y \in Q : y \triangleright a = b$
- $\triangleright$ is *right-distributive* over itself: $\forall a, b, c \in Q, (a \triangleright b) \triangleright c = (a \triangleright c) \triangleright (b \triangleright c)$

When the operation is clear from context, we will denote the quandle by its underlying set.

The second axiom is equivalent to the existence of a second operation $\triangleright^{-1}$ for which $\triangleright^{-1} y$ is the inverse to $\triangleright y$ for all $y \in Q$.

*Current addresses: G. Ehrman, 568 W. Sturbridge Dr., Medina, OH 44246 U.S.A.; A. Gurpinar, 1126 Commonwealth Ave., Apt 2, Allston, MA 02134 U.S.A.; M. Thibault, Dept. of Mathematics, University of Chicago, 5734 S. University Avenue, Chicago, Illinois 60637

Quandles may be regarded as an abstraction from groups in as much as many important examples arise as conjugation invariant subsets of groups with the operation $\triangleright y$ given by right conjugation by y. (Indeed it is a theorem of Joyce [1] that free quandles are isomorphic to disjoint unions of conjugacy classes in groups, and thus that the equational theory of quandles is 'the equational theory of groups under conjugation'.)

The knot quandle [1] [2], though it admits a homotopy theoretic definition, can be described most simply by generators and relations: modify the Wirtinger presentation of the knot group by replacing right conjugation with $\triangleright$ and left conjugation with $\triangleright^{-1}$.

Finite quandles, in particular, are of some interest, since they give rise both to 'counting invariants', of classical knots and link, which generalize Tait's notion of three-coloring a knot, to ''counting invariants' of monodromy situations (cf. [3]), and form the basis for more refined topological invariants derived from quandle cohomology (cf. [4,5]).

The present work is intended as a contribution to the problem of classifying finite quandles.

2. Notation, Examples, and Basic Concepts

Definition 2.1. A *quandle homomorphism*, given $(Q, \triangleright)$ and $(Q', \triangleright')$, is a mapping $\rho : Q \to Q'$ such that $\forall x, y \in Q, (x \triangleright y)\rho = (x)\rho \triangleright' (y)\rho$.

Note, for the sake of agreement with the action of elements of a quandle on the quandle itself, which is written as a right action by quandle homomorphisms, we write quandle homomorphisms to the right of their arguments.

Example 2.2. $\mathbf{n}$ is the trivial quandle of order n. Given $|Q| = n, \mathbf{n} := (Q, \triangleright)$ where $\forall x, y \in Q, x \triangleright y = x$.

Example 2.3. The Tait quandle $(\mathbf{T}_3, \triangleright)$ is the quandle with underlying set $\{a, b, c\}$ and operation

$\triangleright$	a	b	c
a	a	c	b
b	c	b	a
c	b	a	c

This quandle is so named because Tait's notion of three-coloring a knot is equivalent to the existence of a non-trivial quandle homomorphism from the knot quandle (cf. Joyce [1]) to $\mathbf{T}_3$.

Definition 2.4. Quandles $(Q, \triangleright)$ and $(Q', \triangleright')$ are *isomorphic* when there exists a bijective quandle homomorphism ρ (the *isomorphism* from Q to Q'. We denote the existence of such an isomorphism by $(Q, \triangleright) \cong (Q', \triangleright')$.

Definition 2.5. The *automorphism group* of a quandle $(Q, \triangleright)$, denoted $Aut(Q)$, is the group of all isomorphisms $\rho : Q \to Q$. The elements of $Aut(Q)$ act on those of Q by right action.

Definition 2.6. The *inner automorphism group* of a quandle $(Q, \triangleright)$, denoted $Inn(Q)$, is the subgroup of $Aut(Q)$ generated by all S_x, where $\forall x, y \in Q, S_x(y) := y \triangleright x$.

Definition 2.7. The *orbit* of $s \in Q$ is the subset of elements $t \in Q$ such that there exists some $p \in Inn(Q)$ where p maps s to t.

Definition 2.8. A quandle $(Q, \triangleright)$ is *(algebraically) connected* when there exists exactly one orbit in Q–that is, $\forall x \in Q$, the orbit of x *is* all of Q.

Definition 2.9. Given a set Q and a group G with a right action by quandle homomorphisms on Q, an *augmentation map* is a map $|\cdot| : Q \to G$ such that the following hold:

- $\forall q \in Q, q|q| = q$
- $\forall q \in Q, g \in G, |qg| = g^{-1}|q|g$

Definition 2.10. The *universal augmentation group* of the quandle Q, denoted, Γ_Q, is the group freely generated by all formal augmentations $|x|$ of the elements $x \in Q$ modulo relations $\forall x, y \in Q, |x \triangleright y| = |y|^{-1}|x||y|$.

Joyce [1] showed that the inclusion of generators into Γ_Q is the universal augmentation of Q in the sense that the quandle operation induces an action of Γ_Q on Q by quandle homomorphisms such that the inclusion of generators is an augmentation, and given any other augmentation $\langle\cdot\rangle : Q \to G$, there is a unique group homomorphism $c : \Gamma_Q \to G$ such that $\forall q \in Q, c(|q|) = \langle q\rangle$ and $\forall q \in Q, \forall g \in \Gamma_Q, qc(g) = qg$.

3. Semidisjoint Union of Quandles

Let $(Q_1, \triangleright_1)$, $(Q_2, \triangleright_2), \ldots, (Q_n, \triangleright_n)$ be quandles. For each quandle $(Q_i, \triangleright_i)$, we have the universal augmentation map $|\cdot|$ from it to Γ_{Q_i}. In particular, for all $x, y \in Q_i$, $x|y| := x \triangleright_i y$. Note that this is an augmentation map since $\forall x \in Q_i, x|x| = x \triangleright_i x = x$ and, given some $g = |y_1|^{\pm 1}|y_2|^{\pm 1} \ldots |y_k|^{\pm 1} \in \Gamma_{Q_i}$,

$$\begin{aligned} |xg| = |x|y_1|^{\pm 1}|y_2|^{\pm 1} \ldots |y_k|^{\pm 1}| &= |(\ldots(x \triangleright_i^{\pm 1} y_1) \triangleright_i^{\pm 1} y_2) \ldots \triangleright_i^{\pm 1} y_k)| \\ &= |y_k|^{\mp 1} \ldots |y_1|^{\mp 1}|x||y_1|^{\pm 1} \ldots |y_k|^{\pm 1} \\ &= g^{-1}|x|g. \end{aligned}$$

Now, observe that the orbits of $Inn(Q)$ are subquandles of any quandle Q, and that if Q has orbits $Q_1, \ldots, Q_n$, the augmentation of Q in $Inn(Q)$ induces an augmentation of each Q_i in $Inn(Q)$, and thus a group homomorphism from Γ_{Q_i} to $Inn(Q)$. These, in turn induce group homomorphisms from Γ_{Q_i} to $Aut(Q_j)$ for each j (with the homomorphism from Γ_{Q_i} to $Aut(Q_i)$ being that induced by the universal property of Γ_{Q_i}). Notice, for $i \neq j$, these do not necessarily factor through the subgroup $Inn(Q_j)$.

This observation suggests the following construction:

For $1 \leq i, j \leq n$, let $g_{i,j}$ be a group homomorphism from Γ_{Q_i} to $Aut(Q_j)$, such that $g_{i,i}$ is the canonical group homomorphism from Γ_{Q_i} to $Aut(Q_i)$. Let G be the $n \times n$ matrix of group homomorphisms with entries $g_{i,j}$. Define the operation

$$\#(Q_1, Q_2, \ldots Q_n, G) := (\coprod_{i=1}^{n} Q_i, \triangleright)$$

where $x \triangleright y := x g_{i,j}(|y|)$ if $x \in Q_j, y \in Q_i$. We have the following theorem.

Theorem 3.1. *Let $(Q, \triangleright)$ be a quandle. Then if it is not connected, $(Q, \triangleright)$ may be expressed uniquely as $\#(Q_1, Q_2, \ldots, Q_n, G)$ for some G, where $(Q_i, \triangleright_i)$ are quandles, Q_i are the orbits of the action of the inner automorphism group of Q on Q, and $\triangleright_i$ is the operation $\triangleright$ restricted to $Q_i \times Q_i$.*

Proof. Suppose $(Q, \triangleright)$ is not connected. Since orbits of elements in Q are the equivalence classes of an equivalence relation, Q is uniquely expressed as a disjoint union of orbits in Q under the group action of $Inn(Q)$, say $Q = \coprod_{i=1}^{n} Q_i$. Since each Q_i is an orbit, we have that $Q_i \triangleright Q = Q_i$. Define $\triangleright_i := \triangleright|_{Q_i \times Q_i}$ ($\triangleright$ restricted to $Q_i \times Q_i$). Then for each $i = 1 \ldots n$, $(Q_i, \triangleright_i)$ is a quandle. ($\triangleright_i$ inherits the quandle structure of $\triangleright$, so all that is still required to show that $(Q_i, \triangleright_i)$ to be a quandle is closure.)

Now we define the entries of matrix G, $g_{i,j}$. For Q_i, we have the augmentation map $|\cdot|_{Q_i}$ from Q_i to Γ_{Q_i}. For each $x \in Q_i$, let $g_{i,j}(|x|_{Q_i}) := \phi_x^j$, a right-action, where $\phi_x^j : Q_j \to Q_j$ and $y\phi_x^j = y \triangleright x$ for each $y \in Q_j$. Extend the map g so that g is a homomorphism from Γ_{Q_i} to $Aut(Q_j)$. (For $|x_1|_{Q_i}, |x_2|_{Q_i}, \ldots, |x_n|_{Q_i} \in \Gamma_{Q_1}$, let $g_{i,j}(|x_1|^{\pm 1}|x_2|^{\pm 1} \ldots |x_n|^{\pm 1}) = [g_{i,j}(|x_1|)]^{\pm 1}[g_{i,j}(|x_2|)]^{\pm 1} \ldots [g_{i,j}(|x_n|)]^{\pm 1}$.)

We must now check that $g_{i,j}$ is well-defined. $g_{i,j}(|x \triangleright y|)$ is defined both as $\phi_{x \triangleright y}^j$ and $g_{i,j}(|y|^{-1}|x||y|) = [g_{i,j}(|y|)]^{-1} g_{i,j}(|x|) g_{i,j}(|y|) = (\phi_y^j)^{-1}\phi_x^j\phi_y^j$. Choose arbitrary $z \in Q_j$. Then $z\phi_y^j\phi_{x \triangleright y}^j = (z \triangleright y) \triangleright (x \triangleright y) = (z \triangleright x) \triangleright y = z\phi_x^j\phi_y^j$. Since $z \in Q_j$ was arbitrary, we see that $\phi_y^j\phi_{x \triangleright y}^j\phi_x^j\phi_y^j$, i.e. $\phi_{x \triangleright y}^j = (\phi_y^j)^{-1}\phi_x^j\phi_y^j$. Hence $g_{i,j}$ is well-defined.

For all $y, z \in Q_j$, $(y \triangleright z)\phi_x^j = (y \triangleright z) \triangleright x = (y \triangleright x) \triangleright (z \triangleright x) = (y\phi_x^j) \triangleright (z\phi_x^j)$. Also since Q is a quandle, we see that for each $q \in Q_j$ and $y \in Q_i$, there exists a unique element, $q \triangleright^{-1} y \in Q_j$, such that $(q \triangleright^{-1} y) g_{i,j}(|y|) = q$. Thus the image of $g_{i,j}$ is in $Aut(Q_j)$.

So $Q = \#(Q_1, Q_2, \ldots, Q_n, G)$ by construction.

Now we show that this decomposition is unique. Earlier, we showed that each Q_i is uniquely determined. Since $Q = \#(Q_1, Q_2, \ldots, Q_n, G)$, we see that for each $x, y \in Q_i$, $x \triangleright_i y$ must equal $x \triangleright y$. Thus $\triangleright_i$ is uniquely determined as well. Hence each subquandle $(Q_i, \triangleright_i)$ is uniquely determined. For each $y \in Q_i$ and $x \in Q_j$, we have that $x \triangleright y = xg_{i,j}(|y|_{Q_i})$. Thus $g_{i,j}(|y|_{Q_i})$ is uniquely determined for each $y \in Q_i$. (An automorphism is determined by where it takes each element of its domain to.) Since $g_{i,j}$ is a homomorphism on Γ_{Q_i}, and Γ_{Q_i} is generated by the elements $|q|_{Q_i}$ where $q \in Q_i$, we have that $g_{i,j}$ is uniquely determined on Γ_{Q_i}. Hence this decomposition is unique up to re-ordering. □

Now, unlike more familiar decomposition or factorization theorems, while this decomposition is unique, it does not decompose the quandle into indecomposable pieces, since, while they are single orbits under $Inn(Q)$, the Q_i may not be single orbits under their own groups of inner automorphisms. Nonetheless, iterating the construction of the previous theorem, every quandle can be iteratively decomposed into connected quandles. The uniqueness result of the previous theorem then gives the uniqueness of the iterative decomposition.

Of course, an arbitrary matrix G of group homomorphisms $g_{i,j} : \Gamma_{Q_i} \to Aut(Q_j)$ need not give rise to a quandle. We now give necessary and sufficient for $\#(Q_1, Q_2, \ldots Q_n, G)$ to be a quandle:

Theorem 3.2. [a] *Let $(Q_i, \triangleright_i)$ be quandles for $i = 1 \ldots n$, and let $g_{i,j}$ be homomorphisms from Γ_{Q_i} to $Aut(Q_j)$ for $1 \leq i, j \leq n$, with $g_{i,i}$ the canonical homomorphism from Γ_{Q_i} to $Aut(Q_i)$. Then*
$\#(Q_1, Q_2, \ldots Q_n, G) := (Q, \triangleright)$ is a quandle if and only if for all i, j, k distinct, $1 \leq i, j, k \leq n$, the following conditions hold:

(1) $(xg_{j,i}(|y|_{Q_j})) \triangleright_i z = (x \triangleright_i z)g_{j,i}(|yg_{i,j}(|z|_{Q_i})|_{Q_j})$
(2) $(xg_{j,i}(|y|_{Q_j}))g_{k,i}(|z|_{Q_k}) = (xg_{k,i}(|z|_{Q_k}))()g_{j,i}(|yg_{k,j}(|z|_{Q_k})|_{Q_j})$

Proof. Clearly Q is closed under the operation $\triangleright$. Since $Q_1, Q_2, \ldots Q_n$ are quandles, we see that $x \triangleright x = x$ for all $x \in Q$. Let $y, z \in Q$ be arbitrary. If $y, z \in Q_i$ for some i, then we see that $(z \ \triangleright^{-1} \ y) \triangleright y = z$. Alternatively, suppose $y \in Q_i$, $z \in Q_j$ for some $i \neq j$. Then since $g_{i,j}(|y|_{Q_i})$ is an automorphism from Q_j to Q_j, there exists a unique $x \in Q_j$ such that $xg_{i,j}(|y|_{Q_i}) = z$. Thus Q is a quandle if and only if the third property holds: $(x \triangleright y) \triangleright z = (x \triangleright z) \triangleright (y \triangleright z)$ for all $x, y, z \in Q$. If $x, y, z \in Q_i$ for some Q_i, this is given. Thus we have 4 cases:

(1) $x, y \in Q_i$, $z \in Q_j$

[a]Shortly after the conclusion of the KSU REU, Nelson and Wong [6] announced the independent discovery of a decomposition theorem equivalent to this theorem and the preceding, when viewed as a decomposition theorem, rather than a construction. In their result, the extra structure is expressed in terms of compatible rack actions, rather than compatible group homomorphisms from universal augmentation groups to automorphism groups.

(2) $x, z \in Q_i$, $y \in Q_j$
(3) $y, z \in Q_i$, $x \in Q_j$
(4) $x \in Q_i$, $y \in Q_j$, $z \in Q_k$.

Case 1: $(x \triangleright y) \triangleright z = (x \triangleright_i y) g_{j,i}(|z|_{Q_j})$.
$(x \triangleright z) \triangleright (y \triangleright z) = (x g_{j,i}(|z|_{Q_j})) \triangleright_i (y g_{j,i}(|z|_{Q_j}))$. But these coincide since $g_{j,i}(|z|)$ is an automorphism of Q_i.

Case 2: $(x \triangleright y) \triangleright z = (x g_{j,i}(|y|_{Q_j})) \triangleright_i z$.
$(x \triangleright z) \triangleright (y \triangleright z) = (x \triangleright_i z) g_{j,i}(|y g_{i,j}(|z|_{Q_i})|_{Q_j})$. Thus for all $i \neq j$, $1 \leq i, j \leq n$,

$$(x g_{j,i}(|y|_{Q_j})) \triangleright_i z = (x \triangleright_i z) g_{j,i}(|y g_{i,j}(|z|_{Q_i})|_{Q_j}),$$

which is condition (1).

Case 3: $(x \triangleright y) \triangleright z = (x g_{i,j}(|y|_{Q_i})) g_{i,j}(|z|_{Q_i})$.

$$\begin{aligned}
(x \triangleright z) \triangleright (y \triangleright z) &= (x g_{i,j}(|z|_{Q_i})) g_{i,j}(|y \triangleright_i z|_{Q_i}) \\
&= x g_{i,j}(|z|_{Q_i} |y \triangleright_i z|_{Q_i}) \\
&\qquad \text{since } g_{i,j} \text{ is a group homomorphism.} \\
&= x g_{i,j}(|z|_{Q_i} |z|_{Q_i}^{-1} |y|_{Q_i} |z|_{Q_i}) \\
&\qquad \text{since } |\cdot|_{Q_i} \text{ is an augmentation.} \\
&= x g_{i,j}(|y|_{Q_i} |z|_{Q_i}) \\
&= (x g_{i,j}(|y|_{Q_i})) g_{i,j}(|z|_{Q_i}).
\end{aligned}$$

Thus in this case, $(x \triangleright y) \triangleright z = (x \triangleright z) \triangleright (y \triangleright z)$.

Case 4: $(x \triangleright y) \triangleright z = (x g_{j,i}(|y|_{Q_j})) g_{k,i}(|z|_{Q_k})$.
$(x \triangleright z) \triangleright (y \triangleright z) = (x g_{k,i}(|z|_{Q_k})) g_{j,i}(|y g_{k,j}(|z|_{Q_k})|_{Q_j})$. Thus for all i, j, k distinct, $1 \leq i, j, k \leq n$,

$$x g_{j,i}(|y|_{Q_j})) g_{k,i}(|z|_{Q_k}) = (x g_{k,i}(|z|_{Q_k})) g_{j,i}(|y g_{k,j}(|z|_{Q_k})|_{Q_j}),$$

which is condition (2).

Therefore the given conditions are necessary and sufficient for $(Q, \triangleright)$ to be a quandle. □

In principle, at least, this result reduces the classification problem to the classification problem for connected quandles. To generate every quandle, we iteratively specify which quandles to compose, and use the conditions above to determine all matrices G for which the composition is a quandle.

The previous theorem also provides a means of constructing new quandles from old:

Definition 3.3. A *mesh* for a sequence of quandles $Q_1, \ldots, Q_n$ is a matrix G of group homomorphism $g_{ij} : \Gamma_{Q_i} \to Aut(Q_j)$ satisfying the conditions of Theorem 3.2.

Notice that the matrix whose off-diagonal entries are each the appropriate trivial group homomorphism, with diagonal entries given by the canonical homomorphisms is always a mesh.

Finally we name the construction described above:

Definition 3.4. Given a finite sequence of quandles $Q_1, \ldots, Q_n$ and a mesh G, the quandle $\#(Q_1, \ldots, Q_n, G)$ is the *semidisjoint union of* $Q_1, \ldots, Q_n$ *with respect to* G.

For G the mesh with trivial off-diagonal entries, $\#(Q_1, \ldots, Q_n, G)$ is the *disjoint union of* $Q_1, \ldots, Q_n$.

A final note before turning to connected quandles: the disjoint union of quandles is not the coproduct in the category of quandles–the coproduct is the quotient of the quandle freely generated by the disjoint union by the congruence which enforces all equations holding in the individual quandles.

4. On the Classification of Connected Quandles

Here we investigate conditions on a group for it to arise as the group of inner automorphisms of a connected quandle, and derive a structure theorem relating connected quandles and their groups of inner automorphisms. In this section, we denote $Inn(Q)$ by G, where Q is an connected quandle. Note that this G is not related to the matrix of group homomorphisms in the previous section.

The key to the structure theorem is the fact that connected quandles are single orbits of their inner automorphism groups, and thus by standard results can be identified as G-sets with a homogeneous space of cosets. In particular

Proposition 4.1. *Let Q be an connected quandle on n elements. Then n divides the order of G, and, moreover, any choice of $q \in Q$ induces a G-equivariant bijection between Q and $H\backslash G$, where H is the stablizer of q.*

In the case of n prime, the converse of the first conclusion also holds:

Theorem 4.2. *Let Q be a quandle with p elements, where p is prime. Then Q connected $\Leftrightarrow$ p divides the order of G.*

Proof. ($\Rightarrow$) This follows immediately from the above lemma.
($\Leftarrow$) Suppose p divides $|G|$. Then $|G| = p^a b$ for some positive integers a and b. By the 1st Sylow theorem, G has a subgroup of order p^a. Choose one such subgroup H. Hence every element in H has order which divides p^a. Since G and thus H is a subgroup of $\mathfrak{S}_p$, every element of H has order which divides $p!$. Thus every element

of H has order 1 or p. Choose an element of order p. An element of $G \subset \mathfrak{S}_p$ which has order p must be of the form $(a_1\ a_2\ \ldots\ a_p)$ where the a_is are the p distinct elements of quandle Q. In particular, a_{i+1} is in the orbit of a_i under the group action of G. Hence $a_1, a_2, \ldots, a_n$ are in the same orbit under the group action of G, i.e. G is connected. □

By the Proposition, Q is in bijection with the right cosets $H\backslash G$. Hence we may represent Q by $(\{Hg_1, Hg_2, Hg_3, \ldots, Hg_n\}, \triangleright)$, where $Hg_i \triangleright Hg_j = Hg_k$ if $q_i \triangleright q_j = q_k$.

Assume Q has the representation $(\{Hg_1, Hg_2, Hg_3, \ldots, Hg_n\}, \triangleright)$. We define an augmentation map, $|\cdot| : Q = H\backslash G \to G$, such that Hg_i is mapped to $g \in G$ which takes $x \in Q$ to $x \triangleright Hg_i$ for $i = 1, \ldots, n$. To distinguish between this augmentation and existing notation for the order of a group, consider $|H|$ to be the order of the subgroup H and $|Hh|$ to be the augmentation of H as a right-coset in $H\backslash G$. Also denote the center of H as $Z(H)$.

Theorem 4.3. *Let Q be an connected quandle on n elements. Let $G = Inn(Q)$, H, g_i, and $|\cdot|$ be defined as above. Then $H \subset G \subset \mathfrak{S}_n$, $\frac{|G|}{|H|} = n$, $|Hh| \in Z(H)$, and G is generated by $|Hh|, |Hg_2|, \ldots, |Hg_n|$, where $|Hg_i| = g_i^{-1}|Hh|g_i$.*

Proof. By construction, $H \subset G$. G is contained in the group of bijective maps from the elements of Q to the elements of Q, so $G \subset \mathfrak{S}_n$. Since there are exactly n cosets of H in G, we see that $\frac{|G|}{|H|} = n$. Also by definition, $G = Inn(Q)$ is generated by $|Hh|, |Hg_2|, \ldots, |Hg_n| \in G$. It remains to prove that $|Hh| \in Z(H)$ and $|Hg_i| = g_i^{-1}|Hh|g_i$.

Claim 4.4. For all $g \in G$, $|Hg_i g| = g^{-1}|Hg_i|g$.

Proof. The RHS maps $Hg_j g$ to $(Hg_j \triangleright Hg_i)g$. The LHS maps $Hg_j g$ to $Hg_j g \triangleright Hg_i g$. But since $g \in Inn(Q)$,

$$\begin{aligned}(Hg_j \triangleright Hg_i)g &= (\ldots(Hg_j \triangleright Hg_i) \triangleright^{\pm 1} Hg_{k_1}) \triangleright^{\pm 1} Hg_{k_2}) \ldots \triangleright^{\pm 1} Hg_{k_n}) \ldots) \\ &= (\ldots(Hg_j \triangleright^{\pm 1} Hg_{k_1}) \triangleright^{\pm 1} Hg_{k_2}) \ldots \triangleright^{\pm 1} Hg_{k_n}) \ldots) \\ &\qquad \triangleright(\ldots(Hg_i \triangleright^{\pm 1} Hg_{k_1}) \triangleright^{\pm 1} Hg_{k_2}) \ldots \triangleright^{\pm 1} Hg_{k_n}) \ldots) \\ &= Hg_j g \triangleright Hg_i g.\end{aligned}$$

Hence the LHS and the RHS coincide. □

Choosing g to be the identity element in G, we see that $|Hg_i| = g_i^{-1}|Hh|g_i$. Taking $i = 1$ and $g \in H$ arbitrary, we see that $|Hh| = |Hg| = |Hg_1 g| = g^{-1}|Hg_1|g = g^{-1}|Hh|g$. Hence $|Hh|$ commutes with any element in H. Since $H = Hg_1 = Hg_1|Hg_1| = H|Hh|$, we see that $|Hh| \in H$. Hence $|Hh| \in Z(H)$.

Theorem 4.5. *Suppose that for groups G and H, we have that $H \subset G \subset \mathfrak{S}_n$, $\frac{|G|}{|H|} = n$. Let $g_1, g_2, \ldots, g_n$ be coset representatives of H in G. Suppose also that G is generated by $g_1^{-1}|Hh|g_1$, $g_2^{-1}|Hh|g_2$, $g_3^{-1}|Hh|g_3$, $\ldots$, $g_n^{-1}|Hh|g_n$ for some $|Hh| \in Z(H)$. Then $Hg_i \triangleright Hg_j = Hg_i g_j^{-1}|Hh|g_j$ defines an connected quandle with n elements.*

Proof. Note that if $Hg_j = Hg'_j$, then $g_j^{-1}|Hh|g_j = (hg'_j)^{-1}|Hh|(hg'_j) = (g'_j)^{-1}h^{-1}|Hh|hg'_j$ for some $h \in H$. But since $|Hh| \in Z(H)$, this is equal to $(g'_j)^{-1}|Hh|g'_j$. Hence the staitment that G is generated by $g_1^{-1}|Hh|$, $g_2^{-1}|Hh|g_2$, $g_3^{-1}|Hh|g_3, \ldots, g_n^{-1}|Hh|g_n$ for some $|Hh| \in Z(H)$ makes sense, and also $Hg_i \triangleright Hg_j$ is well-defined. We now check to see if this defines a quandle. $Hg_i \triangleright Hg_i = Hg_i g_i^{-1}|Hh|g_i = H|Hh|g_i = Hg_i$ since $|Hh| \in Z(H)$. Now for j, k arbitrary, $Hg_i \triangleright Hg_j = Hg_k$ implies that $Hg_i = Hg_k g_j^{-1}|Hh|^{-1}g_j$. Note that such an i exists and is unique. Finally, we have that $(Hg_i \triangleright Hg_k) \triangleright (Hg_j \triangleright Hg_k) = (Hg_i g_k^{-1}|Hh|g_k) \triangleright (Hg_j g_k^{-1}|Hh|g_k)$.
Let $Hg_j g_k^{-1}|Hh|g_k = Hg_m$ for some m. Then $g_m = hg_j g_k^{-1}|Hh|g_k$ for some $h \in H$. Hence

$$\begin{aligned}
(Hg_i \triangleright Hg_k) \triangleright (Hg_j \triangleright Hg_k) &= (Hg_i g_k^{-1}|Hh|g_k) \triangleright Hg_m \\
&= Hg_i g_k^{-1}|Hh|g_k g_m^{-1}|Hh|g_m \\
&= Hg_i g_k^{-1}|Hh|g_k g_k^{-1}|Hh|^{-1}g_k g_j^{-1} \\
&\qquad h^{-1}|Hh|hg_j g_k^{-1}|Hh|g_k \\
&= Hg_i g_j^{-1}h^{-1}|Hh|hg_j g_k^{-1}|Hh|g_k \\
&= Hg_i g_j^{-1}|Hh|g_j g_k^{-1}|Hh|g_k \\
&= (Hg_i \triangleright Hg_j) \triangleright Hg_k.
\end{aligned}$$

Since $g_1^{-1}|Hh|g_1$, $g_2^{-1}|Hh|g_2$, $g_3^{-1}|Hh|g_3$, $\ldots$, $g_n^{-1}|Hh|g_n$ generate G, we see that for all i, j, $g_i^{-1}g_j \in G$ is generated by $g_1^{-1}|Hh|g_1$, $g_2^{-1}|Hh|g_2$, $g_3^{-1}|Hh|g_3$, $\ldots$, $g_n^{-1}|Hh|g_n$. Hence for each i, j, there exist $k_1, k_2, \ldots, k_n$ such that

$$Hg_j = Hg_i g_i^{-1}g_j = (\ldots(Hg_i \triangleright Hg_{k_1}) \triangleright Hg_{k_2}) \triangleright \ldots \triangleright Hg_{k_n},$$

i.e. the quandle defined by $Hg_i \triangleright Hg_j = Hg_i g_j^{-1}|Hh|g_j$ is connected. □

The above theorems provide a program for constructing all finite connected quandles more satisfactory than the brute force approach of [7]: for each n, test the generation condition of Theorem 4.5 for all triples of a subgroup G of $\mathfrak{S}_n$, a subgroup $H \subset G$, and a central element of H.

We conclude with a number of restrictions on groups that arise as inner automorphism groups of finite quandles, which follow easily from Theorem 4.5:

Corollary 4.6. *For $(Q, \triangleright)$ connected and $n > 1$, G is not abelian.*

Proof. We proceed by contradiction: suppose G were abelian. Then for all $g \in G$, $|Hg| = |Hg_1g| = g^{-1}|Hg_1|g = |Hg_1| = |Hh|$. Since $|Hg_i|$ fixes Hg_i for $i = 1, \ldots, n$, $|Hh|$ must also fix Hg_i for each $i = 1, \ldots, n$. Hence $|Hh|$ is trivial, and thus $|Hg_i|$ is trivial for all i. But, since the G is generated by the $|Hg_i|$,G is trivial. Therefore $(Q, \triangleright)$ is not connected unless $n = 1$, which contradicts the hypothesis that $n > 1$. Thus, the corollary holds. □

Corollary 4.7. *For Q connected on n elements, $G = \mathfrak{S}_n$ implies that $n = 1, 3$.*

Proof. Since $\frac{|G|}{|H|} = n$, then $|H| = (n-1)!$. But $H \subset \mathfrak{S}_{n-1}$, so $H = \mathfrak{S}_{n-1}$. For $n \geq 4, Z(\mathfrak{S}_{n-1}) = \mathbf{1}$, the trivial one-element group. Since $|Hh| \in Z(H)$, $|Hh|$ must equal $\mathbf{1}$. But then $|Hg_i| = \mathbf{1}$ for all i, so $G = \mathbf{1}$, a contradiction. Hence $n \leq 3$. For $n = 2$, $H = \mathbf{1}$ and $G = \mathfrak{S}_2 \neq \mathbf{1}$, a contradiction as above. This gives the desired result. □

Corollary 4.8. *For Q connected on n elements and $n > 1$, $G = A_n$ implies that $n = 4$.*

Proof. Since $\frac{|G|}{|H|} = n$, then $|H| = \frac{1}{2}(n-1)!$. But $H \subset \mathfrak{S}_{n-1}$ and $H \subset A_n$, so $H = A_{n-1}$. For $n \geq 5$, $Z(A_{n-1}) = \mathbf{1}$. Since $|Hh| \in Z(H)$, $|Hh|$ must equal $\mathbf{1}$. But then $|Hg_i| = 1$ for all i, so $G = 1$, a contradiction. Hence $n \leq 4$. But, for $n = 2, 3$, A_n of order 1 or is abelian. □

The results of this section suggest an approach to classifying finite connected quandles which should be more computationally effective than the brute force approach of Ho and Nelson [7]: for a given order, determine (up to conjugacy) all towers of groups $H \subset G \subset \mathfrak{S}_n$ for which the index of H in G is n, and in which H has a non-trivial center. Central elements of H can then be tested against the generating condition of Theorems 4.3 and 4.5.

5. Acknowledgements

The authors were partially supported by the Kansas State University REU and NSF grant GOMT530725.

References

[1] D.E. Joyce. *An algebraic approach to symmetry with applications to knot theory.* PhD thesis, University of Pennsylvania, 1979.
[2] D.E. Joyce. A classifying invariant of knots, the knot quandle. *Journal of Pure and Applied Algebra*, 23:37–65, 1982.
[3] D.N Yetter. Quandles and monodromy. 12(4):523–541, 2003.
[4] S. Carter, D. Jelovsky, S. Kamada, L. Langford, and M. Saito. Quandle cohomology and state-sum invariants of knotted curves and surfaces. e-print, abstract at xxx.lanl.gov/abs/math.GT/9903135, revised December 12, 2001, 1999.

[5] S. Carter, D. Jelovsky, S. Kamada, and M. Saito. Quandle homology groups, the betti numbers, and virtual knots. *Journal of Pure and Applied Algebra*, 157(2-3):135–155, 2001.

[6] S. Nelson and C.-Y. Wong. On the orbit decomposition of finite quandles. e-print, abstract at www.arxiv.org/abs/math.GT/0508247, received August 14, 2005, 2005.

[7] B. Ho and S. Nelson. Matrices and finite quandles. e-print, abstract at www.arXiv.org/abs/math.GT/0412417, 2004.