# Quandle Basics

Jennifer Anderson,
Alexis Brownell,
Harrison Potter,
Dr. David Yetter
Kansas State University
Brainstorming and Barnstorming REU

July 31, 2006

**Abstract**

Basic theorems in quandle algebra are articulated and proven for the benefit of future beginning quandlers.

## 1 Definitions and Introductory Material

Quandles are algebraic structures that were first introduced by David Joyce in his Ph.D. thesis [3] and are used in fields such as topology in order to approach problems more naturally in an algebraic setting [6]. In order to develop solutions to these problems, it is necessary to understand the algebraic properties of quandles. The purpose of this paper is to prove some basic theorems of quandle algebra. Additional material on quandle algebra can be found in other papers, such as [1],[2],[4], and [5].

### 1.1 Quandle

A *quandle* is a binary algebraic structure $\langle Q, \triangleright \rangle$ satisfying the following axioms.

1. Idempotence: $\forall x \in Q$, $x \triangleright x = x$
2. Right Self-Distributivity: $\forall x, y, z \in Q$, $(x \triangleright y) \triangleright z = (x \triangleright z) \triangleright (y \triangleright z)$
3. Invertibility: $\forall x, y \in Q$, $\exists! z \in Q$ s.t. $z \triangleright x = y$

### 1.2 Quandle Homomorphism

A *quandle homomorphism* is a function $\phi : Q \to Q'$ s.t. $\forall x, y \in Q$, $\phi(x \triangleright y) = \phi(x) \triangleright' \phi(y)$.

## 1.3 Quandle Isomorphism

A *quandle isomorphism* is a bijective quandle homomorphism.

## 1.4 Quandle Automorphism

A *quandle automorphism* is a quandle isomorphism from a quandle $Q$ to itself.

## 1.5 Inner Automorphism Theorem

For any given $z \in Q$, $\phi(x) = x \triangleright z$ is an automorphism of the quandle Q.

**Proof** A quandle is a binary algebraic structure, and is thus closed under its binary operation. Thus $\phi(x) = x \triangleright z$ for $z \in Q$ implies $x \triangleright z \in Q$, and thus that $\phi : Q \to Q$. Thus, $\forall x, y \in Q$, $\phi(x \triangleright y) = (x \triangleright y) \triangleright z = (x \triangleright z) \triangleright (y \triangleright z) = \phi(x) \triangleright \phi(y)$, by the right self-distributivity axiom. Thus $\phi$ is a homomorphism.

Now suppose $\phi(x_1) = \phi(x_2)$. Then $x_1 \triangleright z = x_2 \triangleright z = y$, where $y$ is just some particular element in the quandle $Q$. Thus, by the invertibility axiom, $x_1 = x_2$, so $\phi$ is a one-to-one function.

Now take some $y \in Q$. Must there be an element $x \in Q$ s.t. $\phi(x) = y$? If there were such an element, it would have to satisfy $x \triangleright z = y$. But the invertibility axiom guarantees that for any given $y, z \in Q$ a unique element $x$ exists that satisfies this condition, so $\phi$ is an onto function.

$\therefore$ $\phi : Q \to Q$ defined by $\phi(x) = x \triangleright z$ for some $z \in Q$ is an isomorphism of Q with itself, and is thus an automorphism of Q.

## 1.6 Inner Automorphism

The group consisting of all compositions of such automorphisms $\phi$ of $Q$, and operating under function composition, is called the *inner automorphism group of Q*, and is denoted by $Inn(Q)$.

## 1.7 Orbit

The *orbit* of an element $x \in Q$ is $\{\varphi(x) \in Q | \varphi \in Inn(Q)\}$, and is denoted by $Orb(x)$. Conceptually, the orbit of $x$ is the set of all elements of $Q$ that can be reached by repeatedly acting on $x$ with other elements of $Q$ in any combination.

## 1.8 Connected Quandle

A *connected quandle* is a quandle with only one orbit.

# 2 Quandle Examples

## 2.1 Trivial Quandle

The *trivial quandle* of order $n$ is denoted by **n** and is defined by $\forall x, y \in \mathbf{n}$, $x \triangleright y = x$.

**Proof** The trivial quandle is a quandle if it satisfies the quandle axioms.

$\forall x \in \mathbf{n}$, $x \triangleright x = x$, so **n** is idempotent.

$\forall x, y, z \in \mathbf{n}$, $(x \triangleright y) \triangleright z = x \triangleright y = x$ and $(x \triangleright z) \triangleright (y \triangleright z) = x \triangleright z = x$, so **n** is right self-distributive.

$\forall x, y \in \mathbf{n}$, the equation $z \triangleright x = y$ has the unique solution $z = y$, so **n** is invertible.

$\therefore$ **n** is indeed a quandle.

## 2.2 n-fold Conjugation Quandle

Given any group $G$, the *n-fold conjugation quandle* is denoted by $Conj_n(G)$ and is defined on the set $G$ by $\forall x, y \in Conj_n(G)$, $x \triangleright y = y^{-n}xy^n$.

**Proof** The n-fold conjugation quandle is a quandle if it satisfies the quandle axioms.

$\forall x \in Conj_n(G)$, $x \triangleright x = x^{-n}xx^n = x^{-n}x^{n+1} = x$, so $Conj_n(G)$ is idempotent.

$\forall x, y, z \in Conj_n(G)$, $(x \triangleright z) \triangleright (y \triangleright z) = (z^{-n}xz^n) \triangleright (z^{-n}yz^n) = (z^{-n}y^{-1}z^n)^n(z^{-n}xz^n)(z^{-n}yz^n)^n = z^{-n}y^{-n}xy^nz^n$, after cancellation, while $(x \triangleright y) \triangleright z = z^{-n}(x \triangleright y)z^n = z^{-n}y^{-n}xy^nz^n$, so $Conj_n(G)$ is right self-distributive.

$\forall x, y \in Conj_n(G)$, the equation $z \triangleright x = x^{-n}zx^n = y$ has the solution $z = x^nyx^{-n} = (x^{-1})^{-n}y(x^{-1})^n \in Conj_n(G)$, which is unique because G is a group. Thus $Conj_n(G)$ is invertible.

$\therefore Conj_n(G)$ is indeed a quandle.

## 2.3 Closed Subset Theorem

Any finite closed subset $P$ of a quandle $Q$ is a subquandle of $Q$.

**Proof** $Q$ is a quandle, so $\forall x \in Q$, $x \triangleright x = x$. Since $P \subseteq Q$, this implies that $\forall x \in P$, $x \triangleright x = x$. Thus $P$ is idempotent. Similarly, $P \subseteq Q$ implies forthwith that $P$ is right self-distributive.

The difficulty lies in demonstrating that if $P$ is closed, then the unique solution $z \in Q$ to the equation $z \triangleright x = y$, where $x, y \in P$, must be in $P$. Suppose that $z \notin P$. Since $Q$ is a quandle, each column in its operation table is a permutation of its elements by the Inner Automorphism Theorem. Thus, since $P$ is closed, the portion of any column in $Q$ corresponding to those elements in $P$ must be a permutation of the elements in $P$. But then if element $y \in P$ appears in column $x \in P$ in a row corresponding to an element $z \notin P$, then the element $z \in Q$ must appear twice in column $x$. But this contradicts the fact that $Q$ is a quandle because it would violate the invertibility axiom. Thus it must be that $z \in P$, so $P$ is invertible.

$\therefore$ Any finite closed subset $P$ of a quandle $Q$ is indeed a subquandle of $Q$.

## 2.4 Transposition Quandle

The *transposition quandle* of order $\frac{n(n-1)}{2}$ is denoted by $T_n$ and is defined on the set of all transpositions in the group $S_n$ by $x \triangleright y = y^{-1}xy$.

**Proof** The elements of $T_n$ are a subset of those in the group $S_n$. Since $S_n$ is a group, $Conj_1(S_n)$ is a known quandle. Thus, by the Closed Subset Theorem, $T_n$ is also a quandle if it is closed. There are three cases that must be considered to verify closure. Note that a transposition is its own inverse.

**Case** $1$**:** The transpositions have 2 numbers in common.
Consider $(a, b), (a, b) \in T_n$. Then $(a, b) \triangleright (a, b) = (a, b)(a, b)(a, b) = (a, b) \in T_n$.

**Case**$2$**:** The transpositions have $1$ number in common.
Consider $(a, b), (a, c) \in T_n$. Then $(a, b) \triangleright (a, c) = (a, c)(a, b)(a, c) = (b, c) \in T_n$.

**Case** $3$**:** The transpositions have no number in common.
Consider $(a, b), (c, d) \in T_n$. Then $(a, b) \triangleright (c, d) = (c, d)(a, b)(c, d) = (a, b) \in T_n$.

Thus $T_n$ is closed in all three possible cases.
$\therefore T_n$ is indeed a quandle.

## 2.5 Cyclic Quandle

The *cyclic quandle* of order $n$ is denoted by $C_n$ and is defined on the set $\mathbb{Z}_n$ by
$\forall x, y \in C_n$, $x \triangleright y = 2y - x (\text{mod } n)$.

**Proof** The cyclic quandle is a quandle if it satisfies the quandle axioms.

$\forall x \in C_n$, $x \triangleright x = 2x - x = x(\text{mod } n)$, so $C_n$ is idempotent.

$\forall x, y, z \in C_n$, $(x \triangleright y) \triangleright z = 2z - [x \triangleright y] = 2z - 2y + x(\text{mod } n)$, and $(x \triangleright z) \triangleright (y \triangleright z) = 2(y \triangleright z) - (x \triangleright z) = 4z - 2y - 2z + x = 2z - 2y + x(\text{mod } n)$, so $C_n$ is right self-distributive.

$\forall x, y \in C_n$, the equation $z \triangleright x = 2x - z = y(\text{mod } n)$ has the unique solution $z = 2x - y(\text{mod } n)$, so $C_n$ is invertible.

$\therefore C_n$ is indeed a quandle.

## 2.6 Latin Quandle

A *latin quandle* is a quandle whose multiplication table is a latin square. A latin square on $n$ elements is an $n \times n$ matrix in which every element appears exactly once in every column and every row. It follows from this observation and the appropriate analog of the proof of the Inner Automorphism Theorem that a latin quandle is a quandle that satisfies the following latin condition.

**Latin Condition** $\forall x, y \in Q$, $\exists! z \in Q$ s.t. $x \triangleright z = y$

## 2.7 Latin Connectivity Theorem

Every latin quandle is a connected quandle.

**Proof** Take any element $x \in Q$. Since $Q$ is a latin quandle, every other element in $Q$ can be reached from $x$ by operating once by some element in $Q$. Thus $Q$ has only one orbit.

$\therefore Q$ is connected.

**Counterexample to Converse** Not every connected quandle is a latin quandle. For example, consider $T_4$, given below, which is connected but not latin.

| $\triangleright$ | (1,2) | (1,3) | (1,4) | (2,3) | (2,4) | (3,4) |
|---|---|---|---|---|---|---|
| (1,2) | (1,2) | (2,3) | (2,4) | (1,3) | (1,4) | (1,2) |
| (1,3) | (2,3) | (1,3) | (3,4) | (1,2) | (1,3) | (1,4) |
| (1,4) | (2,4) | (3,4) | (1,4) | (1,4) | (1,2) | (1,3) |
| (2,3) | (1,3) | (1,2) | (2,3) | (2,3) | (3,4) | (2,4) |
| (2,4) | (1,4) | (2,4) | (1,2) | (3,4) | (2,4) | (2,3) |
| (3,4) | (3,4) | (1,4) | (1,3) | (2,4) | (2,3) | (3,4) |

## 2.8 Cyclic Quandle Orbit Theorem

If $n$ is odd, then $C_n$ is a latin quandle. If $n$ is even, then $C_n$ has exactly two orbits, one containing all odd elements, and one containing all even elements.

**Proof** Consider the definition of $\triangleright$ in $C_n$: $x \triangleright y = 2y - x (\text{mod } n)$. If the rows and columns of the operation table are labeled in increasing order, from $0$ to $n-1$, then the table is easily filled in from the initial entry $0 \triangleright 0 = 0$ by observing relationships between the values of adjacent entries. Specifically, moving one entry right corresponds to increasing $y$ by one, and thus to adding $2$ modulo $n$, and moving one entry down corresponds to increasing $x$ by one, and thus to subtracting $1$ modulo $n$.

Thus, if $n$ is odd, then every row will contain each element exactly once because $2$ generates $\mathbb{Z}_n$ under addition modulo $n$. Thus, by definition of a latin quandle, $C_n$ is a latin quandle for odd $n$.

On the other hand, if $n$ is even, then each row will contain elements solely in either the coset $\langle 2 \rangle$, or in the coset $1 + \langle 2 \rangle$, which are the two elements in the factor group $\mathbb{Z}_n / \langle 2 \rangle$. Since this is true for any given row, an even element will never be made odd by any sequence of quandle operations, and an odd element will never be made even by any sequence of quandle operations. Thus when $n$ is even there are two orbits in $C_n$, one of which contains all of the even elements, and the other of which contains all of the odd elements.

$Q.E.D.$

**Illustration for $C_9$ and $C_8$** For illustrative purposes, consider the cyclic groups of order $9$ and $8$ as given below. Note that $C_9$ is indeed a latin quandle, and that $C_8$ does indeed have two orbits: $\{0, 2, 4, 6\}$ and $\{1, 3, 5, 7\}$.

The cyclic group of order $9$, $C_9$:

| $\triangleright$ | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 |
|---|---|---|---|---|---|---|---|---|---|
| 0 | 0 | 2 | 4 | 6 | 8 | 1 | 3 | 5 | 7 |
| 1 | 8 | 1 | 3 | 5 | 7 | 0 | 2 | 4 | 6 |
| 2 | 7 | 0 | 2 | 4 | 6 | 8 | 1 | 3 | 5 |
| 3 | 6 | 8 | 1 | 3 | 5 | 7 | 0 | 2 | 4 |
| 4 | 5 | 7 | 0 | 2 | 4 | 6 | 8 | 1 | 3 |
| 5 | 4 | 6 | 8 | 1 | 3 | 5 | 7 | 0 | 2 |
| 6 | 3 | 5 | 7 | 0 | 2 | 4 | 6 | 8 | 1 |
| 7 | 2 | 4 | 6 | 8 | 1 | 3 | 5 | 7 | 0 |
| 8 | 1 | 3 | 5 | 7 | 0 | 2 | 4 | 6 | 8 |

The cyclic group of order $8$, $C_8$:

| $\triangleright$ | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 |
|---|---|---|---|---|---|---|---|---|
| 0 | 0 | 2 | 4 | 6 | 0 | 2 | 4 | 6 |
| 1 | 7 | 1 | 3 | 5 | 7 | 1 | 3 | 5 |
| 2 | 6 | 0 | 2 | 4 | 6 | 0 | 2 | 4 |
| 3 | 5 | 7 | 1 | 3 | 5 | 7 | 1 | 3 |
| 4 | 4 | 6 | 0 | 2 | 4 | 6 | 0 | 2 |
| 5 | 3 | 5 | 7 | 1 | 3 | 5 | 7 | 1 |
| 6 | 2 | 4 | 6 | 0 | 2 | 4 | 6 | 0 |
| 7 | 1 | 3 | 5 | 7 | 1 | 3 | 5 | 7 |

# 3 Images

## 3.1 Quandle Image

Given a quandle homomorphism $\phi : Q \to Q'$, and $P \leq Q$, then the *image of $P$ in $Q'$* is $\{\phi(x) | x \in P\}$, and is denoted by $\phi[P]$.

## 3.2 Image Theorem

Given quandles $P$, $Q$, and $Q'$, a homomorphism $\phi : Q \to Q'$, and $P \leq Q$, it follows that $\phi[P] \leq \phi[Q] \leq Q'$.

**Proof** For any $\phi(x), \phi(y) \in \phi[P]$, $\phi(x) \triangleright' \phi(y) = \phi(x \triangleright y) \in \phi[P]$ because $\phi$ is a homomorphism, so $\phi[P]$ is closed.

Since $\phi[P] \subseteq Q'$ is closed, and $Q'$ is a quandle, $\phi[P] \leq Q'$ by the Closed Subset Theorem. Since $Q$ is its own improper subquandle, this also means that $\phi[Q] \leq Q'$. Since $P \subseteq Q$, $\phi[P] \subseteq \phi[Q]$. As both $\phi[P]$ and $\phi[Q]$ are quandles, this implies that $\phi[P] \leq \phi[Q]$.

$\therefore \phi[P] \leq \phi[Q] \leq Q'$

### 3.3 Quandle Inverse Image

Given a quandle homomorphism $\phi : Q \to Q'$, and $P' \leq Q'$, then the *inverse image of* $P'$ *in* $Q$ is $\{x \in Q | \phi(x) \in P'\}$, and is denoted by $\phi^{-1}[P']$.

Note that $\phi^{-1}[Q'] = Q$.

### 3.4 Inverse Image Theorem

Given quandles $Q$, $P'$, and $Q'$, a homomorphism $\phi : Q \to Q'$, and $P' \leq Q'$, it follows that $\phi^{-1}[P'] \leq Q$.

**Proof** If $x, y \in \phi^{-1}[P']$, then $\phi(x), \phi(y) \in P'$. Since $\phi$ is a homomorphism, this implies that $\phi(x) \triangleright' \phi(y) = \phi(x \triangleright y) \in P'$. This means that $(x \triangleright y) \in \phi^{-1}[P]$ for any $x, y \in \phi^{-1}[P]$. Thus $\phi^{-1}[P]$ is closed.

Since $\phi^{-1}[P'] \subseteq Q$ is closed, and $Q$ is a quandle, $\phi^{-1}[P'] \leq Q$ by the Closed Subset Theorem.

$\therefore \phi^{-1}[P'] \leq Q$

## 4 Direct Products

### 4.1 Quandle Direct Product

Given $n$ quandles $Q_1, Q_2, \ldots, Q_n$, the *direct product* of these quandles is the set of all possible ordered $n$-tuples whose $i$th entry is an element of $Q_i$ for all $1 \leq i \leq n$. Multiplication of two elements of a direct product of quandles is defined to be component-wise multiplication within each quandle. Such a direct product is denoted by $\prod_{i=1}^{n} Q_i$.

### 4.2 Direct Product Theorem

If $\forall i \in \{1, 2, \ldots, n\}$, $Q_i$ is a quandle, then $\prod_{i=1}^{n} Q_i$ is a quandle.

**Proof** Consider multiplying any two elements of $\prod_{i=1}^{n} Q_i$ together, component by component. Since each component is a quandle, and multiplication is component-wise, closure, idempotence, and right self-distributivity follow immediately. Upon further consideration, invertibility also follows. If in each component quandle $Q_i$ there is a unique solution $z_i$ to the equation $z_i \triangleright x_i = y_i$, then the collection of these component-wise unique solutions is the corresponding unique solution to $(z_1, \ldots, z_n) \triangleright (x_1, \ldots, x_n) = (y_1, \ldots, y_n)$ in $\prod_{i=1}^{n} Q_i$.

$\therefore \prod_{i=1}^{n} Q_i$ is a quandle

### 4.3 Connected Direct Product Theorem

If $\forall i \in \{1, 2, \ldots, n\}$, $Q_i$ is a connected quandle, then $\prod_{i=1}^{n} Q_i$ is a connected quandle.

**Proof** By the Direct Product Theorem, it is known that $\prod_{i=1}^{n} Q_i$ is a quandle. Thus connectivity must be demonstrated.

Take any elements $(x_1, \ldots, x_n), (y_1, \ldots, y_n) \in \prod_{i=1}^{n} Q_i$. It must be shown that $(y_1, \ldots, y_n)$ can be obtained from $(x_1, \ldots, x_n)$ by repeatedly applying the quandle operation. Since each component quandle is connected, it is known that this can be done in each component independently, if only the elements in all of the other components could be held fixed while this was achieved. The idempotence of quandles, however, guarantees that this can indeed be done. Simply take $(x_1, x_2, \ldots, x_n)$ to $(y_1, x_2, \ldots, x_n)$ using whatever elements of $Q_1$ are required, but always keeping the remaining elements fixed by using idempotence. Proceed through each component similarly until each $x_i$ has been taken to its corresponding $y_i$, one component at a time. This procedure demonstartes that any $(y_1, \ldots, y_n)$ can be obtained from any $(x_1, \ldots, x_n)$ by repeatedly applying the quandle operation.

$\therefore \prod_{i=1}^{n} Q_i$ is a connected quandle if each $Q_i$ is a connected quandle.

**Illustration for $C_3 \times C_5$** For illustrative purposes, consider the quandle $C_3 \times C_5$, as given by the following table. Note that connectivity is preserved, and also note the projections of the component quandles in the larger quandle.

Let the elements $(0,0), (1,0), (2,0), (0,1), \ldots, (2,4)$ in the direct product quandle be renamed by the single numbers $1, 2, 3, \ldots, 15$ in the table so that the projections of each component quandle can easily be read off of the table.

| $\triangleright$ | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 1 | 1 | 3 | 2 | 7 | 9 | 8 | 13 | 15 | 14 | 4 | 6 | 5 | 10 | 12 | 11 |
| 2 | 3 | 2 | 1 | 9 | 8 | 7 | 15 | 14 | 13 | 6 | 5 | 4 | 12 | 11 | 10 |
| 3 | 2 | 1 | 3 | 8 | 7 | 9 | 14 | 13 | 15 | 5 | 4 | 6 | 11 | 10 | 12 |
| 4 | 13 | 15 | 14 | 4 | 6 | 5 | 10 | 12 | 11 | 1 | 3 | 2 | 7 | 9 | 8 |
| 5 | 15 | 14 | 13 | 6 | 5 | 4 | 12 | 11 | 10 | 3 | 2 | 1 | 9 | 8 | 7 |
| 6 | 14 | 13 | 15 | 5 | 4 | 6 | 11 | 10 | 12 | 2 | 1 | 3 | 8 | 7 | 9 |
| 7 | 10 | 12 | 11 | 1 | 3 | 2 | 7 | 9 | 8 | 13 | 15 | 14 | 4 | 6 | 5 |
| 8 | 12 | 11 | 10 | 3 | 2 | 1 | 9 | 8 | 7 | 15 | 14 | 13 | 6 | 5 | 4 |
| 9 | 11 | 10 | 12 | 2 | 1 | 3 | 8 | 7 | 9 | 14 | 13 | 15 | 5 | 4 | 6 |
| 10 | 7 | 9 | 8 | 13 | 15 | 14 | 4 | 6 | 5 | 10 | 12 | 11 | 1 | 3 | 2 |
| 11 | 9 | 8 | 7 | 15 | 14 | 13 | 6 | 5 | 4 | 12 | 11 | 10 | 3 | 2 | 1 |
| 12 | 8 | 7 | 9 | 14 | 13 | 15 | 5 | 4 | 6 | 11 | 10 | 12 | 2 | 1 | 3 |
| 13 | 4 | 6 | 5 | 10 | 12 | 11 | 1 | 3 | 2 | 7 | 9 | 8 | 13 | 15 | 14 |
| 14 | 6 | 5 | 4 | 12 | 11 | 10 | 3 | 2 | 1 | 9 | 8 | 7 | 15 | 14 | 13 |
| 15 | 5 | 4 | 6 | 11 | 10 | 12 | 2 | 1 | 3 | 8 | 7 | 9 | 14 | 13 | 15 |

## 4.4 Orbit Product Theorem

Let $\mathcal{O}(Q)$ denote the number of orbits in the quandle $Q$. Then $\mathcal{O}(\prod_{i=1}^{n} Q_i) = \prod_{i=1}^{n} \mathcal{O}(Q_i)$.

**Proof** Take any element $(x_1, \ldots, x_n) \in \prod_{i=1}^{n} Q_i$. Each $x_i$ is in some orbit of its respective $Q_i$. Since multiplication in $\prod_{i=1}^{n} Q_i$ is defined in terms of component-

wise multiplication within each component quandle, and the orbits of a quandle define a partition of the quandle into equivalence classes, the orbit of each $(x_1, \ldots, x_n) \in \prod_{i=1}^{n} Q_i$ is just the direct product of the component-wise orbits of all of the $x_i$ in their respective $Q_i$.

Thus $Orb((x_1, \ldots, x_n)) = \prod_{i=1}^{n} Orb(x_i)$ for any $(x_1, \ldots, x_n) \in \prod_{i=1}^{n} Q_i$. It follows combinatorially that the number of orbits in $\prod_{i=1}^{n} Q_i$ is the number of distinct ways to choose the component-wise orbit for $Q_1$, times ..., times the number of distinct ways to choose the component-wise orbit for $Q_n$.

$\therefore \mathcal{O}(\prod_{i=1}^{n} Q_i) = \prod_{i=1}^{n} \mathcal{O}(Q_i)$

# 5 Equivalence Relations

## 5.1 Equivalence Class

If $Q$ is a quandle, and $\equiv$ is an equivalence relation defined on $Q$, then $Q$ is partitioned into equivalence classes by the equivalence relation such that the *equivalence class* containing $x \in Q$ is denoted by $[x]$ and is defined by $[x] := \{q \in Q \mid q \equiv x\}$.

## 5.2 Quotient Quandle

Given an equivalence relation $\equiv$ on a quandle $Q$, the quotient of $Q$ modulo the equivalence relation $\equiv$ is denoted by $Q/\equiv$ and is defined by $Q/\equiv := \{[x] \mid x \in Q\}$. If $Q/\equiv$ has a quandle structure, then it is called a *quotient quandle*.

## 5.3 Set Multiplication

Given two equivalence classes $[x]$ and $[y]$, the *through set multiplication* of these two equivalence classes is denoted by $[x] \blacktriangleright [y]$ and is defined by $[x] \blacktriangleright [y] := \{\xi \triangleright \gamma \mid \xi \in [x], \gamma \in [y]\}$.

Similarly, the *back-through set multiplication* of two equivalence classes $[x]$ and $[y]$ is denoted by $[x] \blacktriangleright^{-1} [y]$ and is defined by $[x] \blacktriangleright^{-1} [y] := \{\xi \triangleright^{-1} \gamma \mid \xi \in [x], \gamma \in [y]\}$.

## 5.4 Congruence Theorem

The *congruence condition*, namely that $[x] \triangleright [y] := [x \triangleright y]$ gives a well-defined quandle structure on $Q/\equiv$, holds $\iff$ $[x] \blacktriangleright [y] = [x \triangleright y]$ and $[x] \blacktriangleright^{-1} [y] = [x \triangleright^{-1} y]$.

**Note:** "$[x] \triangleright [y] := [x \triangleright y]$ gives a well-defined quandle structure on $Q/\equiv$" means that $Q/\equiv$ is a quotient quandle. Also, *well-definition* guarantees that $[x] \triangleright [y] = [x \triangleright y]$ holds regardless of the representative elements chosen in $[x]$ and $[y]$ for the computation: $\forall \xi \in [x], \gamma \in [y]$, it always follows that $[\xi \triangleright \gamma] = [x \triangleright y]$.

**Proof** $\Rightarrow$**:**

It must be shown that $[x] \blacktriangleright [y] = [x \triangleright y]$.

First show that $[x] \blacktriangleright [y] \subseteq [x \triangleright y]$:

For any $z \in [x] \blacktriangleright [y]$, $z = \xi \triangleright \gamma$ for some $\xi \in [x]$ and some $\gamma \in [y]$. Since $[x] \triangleright [y] = [x \triangleright y]$ is well-defined, $\xi \in [x]$ and $\gamma \in [y]$ means that $(\xi \triangleright \gamma) \in [x \triangleright y]$ and so $z \in [x \triangleright y]$. Thus $[x] \blacktriangleright [y] \subseteq [x \triangleright y]$.

Second show that $[x \triangleright y] \subseteq [x] \blacktriangleright [y]$:

Pick any $z \in [x \triangleright y]$ and any $\gamma \in [y]$. Since $z$ and $\gamma$ are both members of the original quandle $Q$, $\exists! \omega \in Q$ s.t. $\omega \triangleright \gamma = z$. This gives us that $[z] = [\omega \triangleright \gamma] = [\omega] \triangleright [y]$. But $z \in [x \triangleright y]$ implies $[z] = [x \triangleright y] = [x] \triangleright [y]$. Summarizing, we now have $[x] \triangleright [y] = [z]$ and $[\omega] \triangleright [y] = [z]$. But since $Q/\equiv$ is a quandle, $[x] = [\omega]$ follows by invertibility. Since $[x] = [\omega] \Rightarrow \omega \in [x]$, we now have that $z = \omega \triangleright \gamma$, where $\omega \in [x]$ and $\gamma \in [y]$, which gives us $z \in [x] \blacktriangleright [y]$ by the definition of through set multiplication. Thus $[x \triangleright y] \subseteq [x] \blacktriangleright [y]$.

Thus we have that $[x] \blacktriangleright [y] = [x \triangleright y]$.

A similar argument gives us that $[x] \blacktriangleright^{-1} [y] = [x \triangleright^{-1} y]$. It then follows that the forward implication is proven.

$\Leftarrow$**:**

$[x] \blacktriangleright [y] = [x \triangleright y]$ implies that $\forall \xi \in [x], \gamma \in [y]$, $(\xi \triangleright \gamma) \in [x \triangleright y]$, which means that $[x] \triangleright [y] = [x \triangleright y]$ is well-defined (it does not depend on the choice of elements in $[x]$ and $[y]$ that are used to carry out the computation). Similarly, $[x] \blacktriangleright^{-1} [y] = [x \triangleright^{-1} y]$ implies that $[x] \triangleright^{-1} [y] = [x \triangleright^{-1} y]$ is well-defined.

It must also be shown that $Q/\equiv$ is a quandle, which can be done by verifying that the 3 quandle axioms hold.

1. For any $[x] \in Q/\equiv$, $[x] \triangleright [x] = [x \triangleright x] = [x]$ ($x \triangleright x = x$ by the idempotence of $Q$). Thus $Q/\equiv$ is idempotent.

2. For any $[y], [z] \in Q/\equiv$, we must show that there is a unique $[x] \in Q/\equiv$ s.t. $[x] \triangleright [y] = [z]$.

   Take $y, z \in Q$, so that $\exists! x \in Q$ s.t. $x \triangleright y = z$. Thus $[z] = [x \triangleright y] = [x] \triangleright [y]$. So it is possible to find at least one element $[x]$ in $Q/\equiv$ s.t. $[x] \triangleright [y] = [z]$. Now take different elements $\gamma \in [y]$, $\zeta \in [z]$. Again, $\exists! \xi \in Q$ s.t. $\xi \triangleright \gamma = \zeta$, and so $[\xi] \triangleright [y] = [z]$. It must be shown that $[\xi] = [x]$ and thus that $[x]$ is unique.

   But $x \triangleright y = z \Rightarrow z \triangleright^{-1} y = x \Rightarrow [z \triangleright^{-1} y] = [x]$, which gives $[z] \triangleright^{-1} [y] = [x]$. Similarly, $\xi \triangleright \gamma = \zeta \Rightarrow \zeta \triangleright^{-1} \gamma = \xi \Rightarrow [\zeta \triangleright^{-1} \gamma] = [\xi]$, which gives $[\zeta] \triangleright^{-1} [\gamma] = [\xi]$. But this implies that $[z] \triangleright^{-1} [y] = [\xi]$, so that $[x] = [z] \triangleright^{-1} [y] = [\xi]$. Thus we have that $[x] = [\xi]$, which means that $[x]$ is unique, so that $Q/\equiv$ is indeed invertible.

3. For any $[x], [y], [z] \in Q/\equiv$, $([x] \triangleright [y]) \triangleright [z] = [x \triangleright y] \triangleright [z] = [(x \triangleright y) \triangleright z] = [(x \triangleright z) \triangleright (y \triangleright z)]$ by right self-distributivity in the quandle $Q$. This then becomes $[x \triangleright z] \triangleright [y \triangleright z] = ([x] \triangleright [z]) \triangleright ([y] \triangleright [z])$, so that $Q/\equiv$ is indeed right self-distributive.

Since $Q/\equiv$ satisfies the quandle axioms, $Q/\equiv$ is indeed a quandle, and the backward implication is proven.

$\therefore$ The congruence condition holds $\iff$ $[x] \blacktriangleright [y] = [x \triangleright y]$ and $[x] \blacktriangleright^{-1} [y] = [x \triangleright^{-1} y]$.

**Note:** Since the equivalence classes $[x]$ are cells in a partition of $Q$ into mutually disjoint closed sets, it follows from the Closed Subset Theorem that $[x] \leq Q$.

## 5.5 Equivalence Class Isomorphism Theorem

Define $Q$ and $Q/\equiv$ as above, and let $[x] \triangleright [y] = [x \triangleright y]$ give a well-defined quandle structure on $Q/\equiv$. Then the mapping $Y : [x] \to [x \triangleright y]$ defined by $Y(\xi) = \xi \triangleright y$ for $y \in Q$ and $\xi \in [x]$ is a quandle isomorphism between equivalence classes.

**Proof** Remember that $[x]$ and $[x \triangleright y]$ are subquandles of Q. Then the fact that for any $x, \xi \in [x]$ we have $Y(x) \triangleright Y(\xi) = (x \triangleright y) \triangleright (\xi \triangleright y) = (x \triangleright \xi) \triangleright y = Y(x \triangleright \xi)$ leads to the conclusion that $Y$ is a quandle homomorphism.

That $Y$ is one-to-one follows from the invertibility axiom of Q:

For any $z \in [x \triangleright y]$, suppose that $\exists \xi, \omega \in [x]$ s.t. $Y(\xi) = Y(\omega) = z$. But because $y$ and $z$ are in $Q$, the element $q \in Q$ s.t. $q \triangleright y = z = Y(q)$ must be unique. Thus, it must be the case that $\xi = \omega$, so $Y$ is one-to-one.

That $Y$ is also onto can be shown by demonstrating that $\forall z \in [x \triangleright y]$ there is a $\chi \in [x]$ s.t. $Y(\chi) = z$:

The invertibility axiom implies that $\exists! \xi \in Q$ s.t. $\xi \triangleright y = z$, so it must be shown that $\xi \in [x]$. By the Congruence Theorem, $[x \triangleright y] = [x] \blacktriangleright [y]$, so $z \in [x \triangleright y] \Rightarrow$ for some $\omega \in [x], \gamma \in [y]$, $z = \omega \triangleright \gamma$, which gives $\xi \triangleright y = \omega \triangleright \gamma$. So $[\xi \triangleright y] = [\omega \triangleright \gamma]$, which gives $[\xi] \triangleright [y] = [\omega] \triangleright [\gamma] = [x] \triangleright [y]$ (because $\omega \in [x]$ and $\gamma \in [y]$, so $[\omega] = [x]$ and $[\gamma] = [y]$). But since $[\xi]$, $[y]$ and $[x]$ are all elements of the quandle $Q/\equiv$, if $[\xi] \triangleright [y] = [x] \triangleright [y]$ then by the invertibility axiom it follows that $[\xi] = [x] \Rightarrow \xi \in [x]$, so $Y$ is onto.

$\therefore Y : [x] \to [x \triangleright y]$ given by $Y(x) = x \triangleright y$ is a quandle isomorphism.

**Corollary** If $Q$ is connected, then all the equivalence classes $[x]$,$[y]$, etc. are isomorphic.

**Proof** For any $x, z \in Q$ there is a sequence of operations that takes $x$ to $z$, namely $(\ldots((x \triangleright y_1) \triangleright y_2) \triangleright \ldots \triangleright y_n) = z$, since $Q$ is connected. This implies that for $[x], [z] \in Q/\equiv$ there is a sequence of mappings $Y_1, Y_2, \ldots, Y_n$ that takes $[x]$ to $[z]$ (where $Y_i$ is the bijective mapping, defined in the Equivalence Class Isomorphism Theorem, from some element $[x] \in Q/\equiv$ to $[x \triangleright y_i]$):

$Y_n(\ldots(Y_2(Y_1([x]))) \ldots) = Y_n(\ldots(Y_2([x \triangleright y_1])) \ldots) = [(\ldots((x \triangleright y_1) \triangleright y_2) \triangleright \ldots \triangleright y_n)] = [z]$. Each $Y_i$ in this sequence is a bijection, so the overall mapping is a bijective function from $[x]$ to $[z]$, which implies that $[x]$ is isomorphic to $[z]$.

# 6 Acknowledgements

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

# References

[1] Ehrman, G. and Gurpinar, A. and Thibault, M. and Yetter, D. N. Toward a Classification of Finite Quandles. July 2005.

[2] Ho, Benita and Nelson, Sam. Matrices and Finite Quandles. November 2005. arXiv.org: math.GT/0412417.

[3] Joyce, David Edward. An Algebraic Approach to Symmetry with Applications to Knot Theory. 1979. Ph.D. thesis, University of Pennsylvania.

[4] Murillo, Gabriel and Nelson, Sam and Thompson, Anthony. Matrices and Finite Alexander Quandles. April 2006.

[5] Nelson, Sam and Wong, Chau-Yim. On the Orbit Decomposition of Finite Quandles. June 2006. arXiv.org: math.GT/0508247.

[6] Yetter, D. N. Quandles and Monodromy. May 2002.