QUANDLES

ROBERT W. MCGRAIL, MONA MERLING, AND JAPHETH WOOD

Abstract. Feder and Vardi (1993) discovered a strong correspondence between finite algebras and computational complexity through the constraint satisfaction problem (CSP). It allows a classification of algebras according to their complexity within **NP**. We focus on quandles, algebras that arise via knot theory. In particular, we demonstrate that all finite quandles that are not locally connected are **NP-complete**. Furthermore, we will present recent progress on the classification of locally connected quandles.

1. Quandles

Definition 1.1. A **quandle** $\mathbf{Q} = \langle Q, \triangleright \rangle$ is a set Q along with a binary operation $\triangleright$ that satisfies the following conditions:

- (Idempotence:) $x \triangleright x = x$.
- (Right Cancellation:) If $x \triangleright r = y \triangleright r$ then $x = y$.
- (Right Self-Distributivity:) $(x \triangleright y) \triangleright z = (x \triangleright z) \triangleright (y \triangleright z)$.

Example 1.2. This is the operation table of a quandle of size 3:

$\triangleright$:	0	1	2
0	0	0	1
1	1	1	0
2	2	2	2

Table 1. Quandle of size 3

Right translation by an element of a finite quandle Q defines a permutation on the underlying set. Hence each column of the operation table of a quandle is a permutation.

Lemma 1.3. *For $q \in Q$ define $\sigma_q : Q \to Q$ by*

$$\sigma_q(x) = x \triangleright q.$$

Then σ_q is an monomorphism of Q. If Q is finite, σ_q is an automorphism.

Proof. For $x, y \in Q$

$$\begin{aligned}\sigma_q(x \triangleright y) &= (x \triangleright y) \triangleright q \\ &= (x \triangleright q) \triangleright (y \triangleright q) = \sigma_q(x) \triangleright \sigma_q(y).\end{aligned}$$

□

Definition 1.4. Let $Inn(Q)$ be the subgroup of Sym_Q generated by $\{\sigma_q | q \in Q\}$. We will call it the *inner automorphism group of Q*.

Note that several right translations of an element x by the elements x_1,x_2,..,x_n are equivalent to permutation multiplication:

$$((..((x \triangleright x_1) \triangleright x_2) \triangleright ..) \triangleright x_n) = (\sigma_{x_1}\sigma_{x_2}...\sigma_{x_n})(x)$$

Lemma 1.5. $\sigma_{x \triangleright y}(i) = (\sigma_y^{-1}\sigma_x\sigma_y)(i)$.

Proof. Define $j = \sigma_y^{-1}(i)$. So, $\sigma_y(j) = i$.
By the distributive law, $(j \triangleright y) \triangleright (x \triangleright y) = (j \triangleright x) \triangleright y$.
So,

$$\begin{aligned} \sigma_{x \triangleright y}(\sigma_y(j)) &= \sigma_y(\sigma_x(j)) \\ &= \sigma_y(\sigma_x(\sigma_y^{-1}(i))) \end{aligned}$$

So, $\sigma_{x \triangleright y}(i) = (\sigma_y^{-1}\sigma_x\sigma_y)(i)$. □

Inn(Q) is acting on the set of elements of the quandle Q, so the group action splits the set into distinct orbits. If the action is transitive, all the elements of the quandle will lie in the same orbit.

Definition 1.6. A quandle Q is *connected* if the action of *Inn(Q)* on the set of elements is transitive.

Definition 1.7. A quandle is *locally connected* if all of its subalgebras are *connected.*

Theorem: If Q is a connected quandle, and $\theta \in \mathrm{Con}\mathbf{Q}$, then each congruence class of θ has the same size.

Proof. The right-cancellation property of quandles is equivalent to the statement that unary polynomials of the form $f_c(x) = x \triangleright c$ (where c is a constant) are permutations of Q. We have assumed that Q is connected, so *Inn(Q)* acts transitively on Q.

Take two congruence classes $A = a/\theta$ and $B = b/\theta$. By transitivity, there is an element $g \in$ *Inn(Q)* such that $b = g(a)$. Since *Inn(Q)* is generated by the permutations of Q described above, there must be constants $c_1, \dots, c_n \in Q$ so that $g = f_{c_n} \circ f_{c_{n-1}} \circ \cdots \circ f_{c_1} \in \mathrm{Pol}_1\mathbf{Q}$.

Now, take $a' \in A$. Since $a'\theta a$, we have that $g(a')\theta g(a) = b$, so $g(a') \in B$. Thus $g(A) \subseteq B$. Since g is a permutation, we have shown that $|A| \leq |B|$. Likewise, we must have $|B| \leq |A|$, so in fact every two congruent classes are of equal size. □

Definition 1.8. A **quasigroup quandle** is a quandle that satisfies left-cancellation, so if $r \triangleright x = r \triangleright y$ then $x = y$.

Example 1.9. Here is an example of a quasigroup quandle of size 3:

$\triangleright$:	0	1	2
0	0	2	1
1	2	1	0
2	1	0	2

TABLE 2. Quasigroup Quandle

Note that in the operation table of a quasigroup quandle not only the columns are permutations on the underlying set, but the rows are also permutations; so the operation table is a latin square. Also, note that a quasigroup quandle is *connected.*

Definition 1.10. Distance in a quandle is a function $d : Q \times Q \to \mathbb{R} \cup \{\infty\}$ defined by

- $d(x, x) = 0$
- $d(x, y) = 1$ if $x \neq y$ and there is $z \in Q$ such that $x \triangleright z = y$
- $d(x, y) = n + 1$ if there is $w \in Q$ such that $d(x, w) = n$ and $d(w, y)$.
- $d(x, y) = \infty$ otherwise

Note that the the distance $d(x, y) = \infty$ for all x, y that are in different orbits of a *disconnected* quandle Q. Also, note that if $d(x, y) = 1$, then there is some $q \in Q$ such that $\sigma_q(x) = y$.

Lemma 1.11. *A quandle Q is a quasigroup quandle if and only if $d(x, y) = 1$ for all $x, y \in Q$.*

Proof. Assume Q is a quasigroup quandle. Let $x, \in Q$. Every element in $y \in Q$ can be reached by a right translation of x, so $d(x, y) = 1$.
Now let $x, y \in Q$ and assume $d(x, y) = 1$. So, there is some $z \in Q$ such that $x \triangleright z = y$ which is equivalent to left cancellation. So, Q is a quasigroup. □

Lemma 1.12. *Quandles are not locally finite. In fact, the free quandle on two generators is infinite.*

Proof. Let $\mathbf{G}$ be the free group on two generators $\{a, b\}$, and define $x \triangleright y := y^{-1}xy$. Then $\mathbf{Q} = \langle G, \triangleright \rangle$ is a quandle.

Now consider the subquandle of $\mathbf{Q}$ generated by a and b. The sequence $a, a \triangleright b, (a \triangleright b) \triangleright b, ((a \triangleright b) \triangleright b) \triangleright b, \ldots$ equals $a, b^{-1}ab, b^{-2}ab^2, b^{-3}ab^3, \ldots$ and is infinite. This shows that $\mathbf{Q}$, a 2-generated quandle, is infinite. Thus the free quandle on two generators must also be infinite. □

2. Dichotomy

There is only one quandle Q of size 2:

$\triangleright$:	0	1
0	0	0
1	1	1

Table 3. Quandle of Size 2

The following properties hold for this quandle:

- $\triangleright$ preserves all relations on $\{0, 1\}$.
- Satisfiability is an instance of $Inv(Q)$.
- Q is simple.
- Q is not connected.
- Q is **NP-complete**.

Since this quandle is **NP-complete** and since we know that the sublgebras and homomorphic images of a tractable algebra are tractable, we will use the 2-element quandle Q to show that a quandle Q' is **NP-complete** by constructing a homomorphic image of Q' onto the Q or by showing that Q is a subalgebra of Q'.

Theorem 2.1. *If a quandle Q is* not connected, *then Q contains then 2-element quandle as a homomorphic image.*

Proof. Since Q is not connected, we can choose $x, y \in Q$ in different orbits of Q. Define a homomorphism from Q to the 2-element quandle (with the multiplication table above) by

$$H(q) = \begin{cases} 0, & q \in (x\text{-orbit}) \\ 1, & \textit{otherwise} \end{cases}$$

Let $a, b \in Q$. Then note that $(a \triangleright b)$ and a are going to be in the same orbit. Also, $H(a)$ and $(H(a) \triangleright H(b))$ are in the same orbit.

$$H(a \triangleright b) = \begin{cases} 0 = 0 \triangleright H(b) = H(a) \triangleright H(b), & a \in (x\text{-orbit}) \\ 1 = 1 \triangleright H(b) = H(a) \triangleright H(b), & \textit{otherwise} \end{cases}$$

So, H is indeed a homomorphism. □

Corollary 2.2. *If a quandle Q is* not locally connected*, then Q is **NP-complete**.*

Proof. If Q is *not locally connected*, there is a subalgebra Q' of Q which is *not connected*. Then, there Q' has a homomorphic image onto the 2-element quandle which is an **NP-complete** algebra, so Q' and therefore Q are **NP-complete**. □

Lemma 2.3. *If there exist distinct $r, x \in Q$ such that $r \triangleright x = r$, then Q contains a 2-element subalgebra.*

Proof. Let Q be a quandle and $r, x \in Q$ such that $r \triangleright x = r$ and $x \neq r$. Consider the subalgebra Q' generated by $< x, r >$.
We say that $q \in Q'$ *starts* with r if

- $q = r$ or
- $q = q_1 \triangleright q_2$ and q_1 *starts* with r.

Note that if q *starts* with r, then $q = r$ since $r \triangleright x = r$ and $r \triangleright r = r$. Define a homomorphism from Q' to the 2-element quandle by

$$H(q) = \begin{cases} 0, & \textit{if } q \textit{ starts with } r \\ 1, & \textit{otherwise} \end{cases}$$

Let $a, b \in Q'$. Note that a *starts* with r if and only if $a \triangleright b$ *starts* with r. So,

$$H(a \triangleright b) = \begin{cases} 0 = 0 \triangleright H(b) = H(a) \triangleright H(b), & \textit{if } a \textit{ starts with } r \\ 1 = 1 \triangleright H(b) = H(a) \triangleright H(b), & \textit{otherwise} \end{cases}$$

So, H is indeed a homomorphism.

□

Corollary 2.4. *If there exist distinct $r, x \in Q$ such that $r \triangleright x = r$, then Q is **NP-complete**.*

Lemma 2.5. *A quandle Q is* locally connected *iff for all $r, x \in Q$, $r \triangleright x = r$ implies that $x = r$.*

Proof. Let Q be a locally connected quandle. Assume that there are $r, x \in Q$, $r \triangleright x = r$ and $x \neq r$. Then, by lemma 2.3, Q contains the 2-element quandle which is not connected as a homomorphic image of a subalgebra, a contradiction to the fact that connectedness is closed under homomorphic images, subalgebras and products. So, for all $r, x \in Q$, $r \triangleright x = r$ implies that $x = r$.
Now assume that for all $r, x \in Q$, $r \triangleright x = r$ implies that $x = r$. Assume Q is not locally connected, so we have a not connected subalgebra Q'. Then, by theorem 2.1, Q' contains the 2-element quandle as a subalgebra. Looking at its multiplication table we see that $0 \triangleright 1 = 0$, but $0 \neq 1$, so we have a contradiction because the operation we assumed to be true is not preserved under subalgebra. So, Q must be locally connected. □

Lemma 2.6. *If Q is* connected *and there are distinct $r, x, y \in Q$ such that $r \triangleright x = r \triangleright y$, then for every $w \in Q$ we can find $x', y' \in Q$ such that $w \triangleright x' = w \triangleright y'$.*

Proof. Since Q is connected, we can get to w by doing right translations of r. So,

$$((..((r \triangleright w_1) \triangleright w_2) \triangleright ..) \triangleright w_n) = w$$

Then, by rearranging terms we get

$$\begin{aligned} w \triangleright ((..((x \triangleright w_1) \triangleright w_2) \triangleright ..) \triangleright w_n) &= ((..((r \triangleright w_1) \triangleright w_2) \triangleright ..) \triangleright w_n) \triangleright ((..((x \triangleright w_1) \triangleright w_2) \triangleright ..) \triangleright w_n) \\ &= (((..((r \triangleright w_1) \triangleright w_2) \triangleright ..) \triangleright w_{n-1}) \triangleright ((..((x \triangleright w_1) \triangleright w_2) \triangleright ..) \triangleright w_{n-1})) \triangleright w_n \\ &= ... \\ &= (r \triangleright x)(w_1 \triangleright (w_2 \triangleright (... \triangleright w_n))) \end{aligned}$$

Similarly we get

$$w \triangleright ((..((y \triangleright w_1) \triangleright w_2) \triangleright ..) \triangleright w_n) = (r \triangleright y)(w_1 \triangleright (w_2 \triangleright (... \triangleright w_n)))$$

Since $r \triangleright x = r \triangleright y$,

$$w \triangleright ((..((x \triangleright w_1) \triangleright w_2) \triangleright ..) \triangleright w_n) = w \triangleright ((..((y \triangleright w_1) \triangleright w_2) \triangleright ..) \triangleright w_n)$$

Let

$$\begin{aligned} x' &= ((..((x \triangleright w_1) \triangleright w_2) \triangleright ..) \triangleright w_n) \\ y' &= ((..((y \triangleright w_1) \triangleright w_2) \triangleright ..) \triangleright w_n) \end{aligned}$$

So, we found x', y' such that $w \triangleright x' = w \triangleright y'$. □

Note that if there are distinct $r, x, y \in Q$ such that $r \triangleright x = r \triangleright y$, then we also have

$$\begin{aligned} r \triangleright (x \triangleright r) &= r \triangleright (y \triangleright r) \\ r \triangleright ((x \triangleright r) \triangleright r) &= r \triangleright ((y \triangleright r) \triangleright r), etc. \end{aligned}$$

If $x = x \triangleright r$ or $y = y \triangleright r$, then we are reduced to the case of lemma 2.3, so Q is **NP-complete**.
If $x = y \triangleright r$, then

$$\begin{aligned} r \triangleright y &= r \triangleright x \\ &= r \triangleright (y \triangleright r) \\ &= (r \triangleright y) \triangleright r. \end{aligned}$$

Again, $r \triangleright y$ gets fixed by r, so we are reduced to lemma 2.3. The case for $y = x \triangleright r$ is similar. This suggests that if on a row r in the multiplication table of Q we have a repetition of a value that is different from r itself, we have to have a second repetition of some value different from r on that row; otherwise Q must be **NP-complete**.

Definition 2.7. Given a group $\mathbf{G} = \langle G; \circ, ^{-1}, e \rangle$, define $a \triangleright b = b^{-1} \circ a \circ b$. Then $\langle G; \triangleright \rangle$ is called a **group quandle**. A subquandle of G is called a **conjugation quandle**.

Lemma 2.8. *Let Q be a quandle of size n and define $\sigma : Q \to S_n$ as $\sigma(x) = \sigma_x$. If σ is injective, then Q is a conjugation quandle.*

Proof. Since $\sigma(x \triangleright y) = \sigma_{x \triangleright y} = (\sigma_y^{-1} \sigma_x \sigma_y)$, ϕ is a homomorphism from Q to the group quandle of S_n. If σ is injective, Q is isomorphic to the conjugation quandle of $\sigma(Q) \subseteq S_n$. □

Lemma 2.9. *Every locally connected quandle is a conjugation quandle.*

Proof. Let Q be a locally connected quandle, and assume that Q is not a conjugation quandle. By lemma 2.8, ϕ is then not injective where $\phi : Q \to S_n$ and $\phi(x) = \sigma_x$. So, $\sigma_x = \sigma_y$ for some $x, y \in Q$. Since we can always relabel elements, assume without loss of genrality that $x = 0$ and $y = 1$. Then the 2-element quandle is a subalgebra of Q which is not connected, a contradiction. So, Q must be a conjugation quandle. $\square$