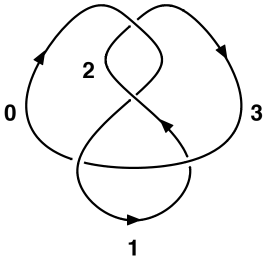
Quandles and the Towers of Hanoi

Bob McGrail, et al

Laboratory for Algebraic and Symbolic Computation
Reem-Kayden Center for Science and Computation
Bard College
Annandale-on-Hudson, NY 12504

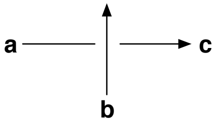
August 8, 2011

The Figure Eight (4_1) Knot

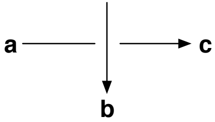


Knot Quandles

A **knot quandle** is a system of equations relating the arcs of a knot, one for each crossing.

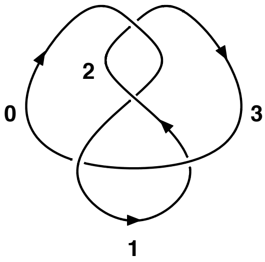


$$a * b = c$$



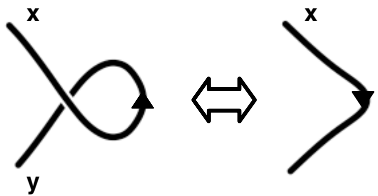
$$a / b = c$$

Figure Eight 4_1



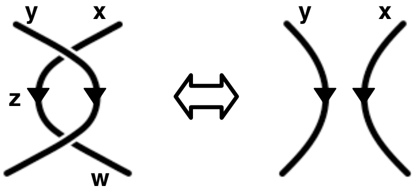
$$\mathcal{Q}(4_1) = \langle 0, 1, 2, 3 | 0/2 = 1, 1 * 3 = 2, 2/0 = 3, 3 * 1 = 0 \rangle$$

Type I Reidemeister Move



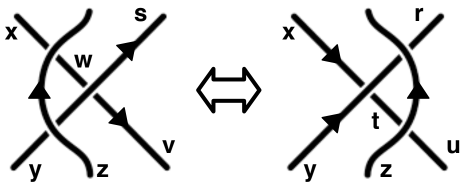
$$x * x = y = x$$

Type II Reidemeister Move



$$(x * y)/y = z/y = w = x$$

Type III Reidemeister Move



$$(x * z) * (y * z) = w * s =$$

$$v = u = t * z = (x * y) * z$$

Quandles

Definition

A quandle $(Q, *, /)$ is a set Q along with a binary operations $*$ and $/$ on Q satisfying:

I $\forall x(x * x = x)$;

IIa $\forall xy((x/y) * y = x)$;

IIb $\forall xy((x * y)/y = x)$; and

III $\forall xyz((x * y) * z = (x * z) * (y * z))$.

Since $*$ uniquely determines $/$, we can limit our mention of $/$. [Note: Axioms I, IIa, and IIb constitute the theory of **idempotent, right quasigroups**.]

Unary Quandle

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

Table: Unary Quandle U_3

Latin Quandle

*	0	1	2
0	0	2	1
1	2	1	0
2	1	0	2

Table: Latin (Quasigroup) Quandle

Basic Elements of a CSP

- A, a finite domain;
- $V = \{v_1, v_2, \ldots, v_n, \ldots\}$,a countable collection of variables; and
- Γ, which is a collection of relations $R \subseteq A^n$ for various positive integers n.

Example: SAT

Question

Does there exists a truth assignment for the proposition below?

$$\alpha = (\neg v_1 \vee v_2) \wedge (v_3 \vee \neg v_2)$$

The domain is easy: $A = \{0, 1\}$

Constraints

Definition (Constraint)

A **constraint over Γ** is a pair $\langle (v_{i_1}, v_{i_2}, \ldots, v_{i_m}), R \rangle$, where R is a relation in Γ of arity m.

$\alpha = (\neg v_1 \vee v_2) \wedge (v_3 \vee \neg v_2)$ translates to the following constraints:

$$C_1 = \langle (v_1, v_2), \{(0,0), (0,1), (1,1)\} \rangle$$

and

$$C_2 = \langle (v_3, v_2), \{(0,0), (1,0), (1,1)\} \rangle.$$

CSP(Γ)

Definition (CSP(Γ))

CSP(Γ) is the combinatorial decision problem with the following components.

Instance: A triple $\mathcal{I} = (V', A, \mathcal{C})$ where $\mathcal{C}$ is a finite set of constraints over Γ and V' is a finite subset of V.

Solution: A function $\theta : V' \to A$ such that for every constraint $\langle (v_1, v_2, \ldots, v_m), R \rangle \in \mathcal{C}$,

$$(\theta(v_1), \theta(v_2), \ldots, \theta(v_m)) \in R.$$

Tractable and NP-Complete CSP

Definition

Let Γ be a collection of relations over a finite domain *A*.

- $\mathrm{CSP}(\Gamma)$ is **tractable** if $\mathrm{CSP}(\Gamma')$ is in *P* for all finite $\Gamma' \subseteq \Gamma$.
- $\mathrm{CSP}(\Gamma)$ is **NP-complete** if $\mathrm{CSP}(\Gamma')$ is NP-complete for some finite $\Gamma' \subseteq \Gamma$.

Complexity of CSP's

Tractable:

- 2-COLOR
- 2-SAT

NP-Complete:

- k-COLOR for $k > 2$
- k-SAT for $k > 2$
- SCHEDULE
- n-QUEENS

CSP(Q)

Definition (Subpower)

Recall that a **subpower** of a quandle Q is a subquandle of Q^n. Let $\mathrm{Sub}(Q)$ stand for the class of subpowers of Q.

Definition (CSP(Q))

$\mathrm{CSP(Q)} = \mathrm{CSP}(\Gamma)$ where $\Gamma = \mathrm{Sub}(Q)$.

Definition

Q is **NP-complete** if $\mathrm{CSP(Q)}$ is NP-complete and is **tractable** if $\mathrm{CSP(Q)}$ is tractable.

U_2

$*$	0	1
0	0	0
1	1	1

Table: U_2

Theorem

U_2 is NP-complete.

Proof.

$\mathrm{Sub}(U_2)$ includes all relations over $\{0, 1\}$. So 3-SAT is a finite, NP-complete subproblem of $\mathrm{CSP(Q)}$ where $Q = U_2$. □

Connectedness

Definition (Connected)

A quandle Q is **connected** if its right Cayley graph for $*$ is connected.

Proposition

A quandle Q is disconnected iff there exists a surjective homomorphism $h : Q \to U_2$.

Definition (Totally Connected)

A quandle Q is **totally connected** if every element of $\mathrm{Sub}(Q)$ is connected.

Homomorphic Images

Theorem

Suppose $h : Q \longrightarrow Q'$ is a surjective quandle homomorphism.

- *If Q is tractable, so is Q'.*
- *If Q' is NP-complete, so is Q.*

Corollary

Disconnected quandles are NP-complete.

Subpowers

Theorem

Suppose $Q' \in \mathrm{Sub}(Q)$.

- *If* Q *is tractable, so is* Q'.
- *If* Q' *is NP-complete, so is* Q.

Corollary

If Q *is not totally connected, then it is NP-complete.*

If Q is not totally connected, then U_2 appears in its variety.

Merling Terms

Definition

A **Merling term** $t(x, y)$ for a quandle Q satisfies the following

1. $t(x, y) = y$ in Q; and
2. $t(x, y) = x$ in U_2.

Note: If such a term exists for Q, then Q and U_2 have **independent varieties**.

Proposition

Every totally connected quandle has a Merling term.

Why? $F(2, Q)$ is a subpower of Q, so it is connected. $t(x, y)$ is the "path" from x to y in $F(2, Q)$.

From Merling to Malcev

Lemma

If a quandle Q has a Merling term, then it also has a Mal'cev term.

This follows from a two-stage transformation of $t(x, y)$:

1. Construct term $s(x, y, z)$ via selective substitution.
2. Use right cancellation to form $m(x, y, z)$.

This transformation is demonstrated on the term

$$t(x, y) = ((x * (y * x)) * (x * y)) * (y * x).$$

$s(x, y, z)$

To construct $s(x, y, z)$ from $t(x, y)$:

- Replace all instances of y with z, and
- Replace every instance of x except the first with y.

For example,

$$t(x, y) = ((x * (y * x)) * (x * y)) * (y * x)$$

yields

$$s(x, y, z) = ((x * (z * y)) * (y * z)) * (z * y).$$

Properties of $s(x, y, z)$

Hence, if $t(x, y) = y$, then

$$
\begin{aligned}
s(x, x, y) &= t(x, y) \\
&= y, \\
s(x, y, y) &= ((x * (y * y)) * (y * y)) * (y * y) \\
&= ((x * y) * y) * y.
\end{aligned}
$$

$m(x, y, z)$

To determine $m(x, y, z)$ from $s(x, y, z)$, use right cancellation to “unravel” $s(x, y, y)$.

For example, for

$$s(x, y, y) = ((x * y) * y) * y,$$

let

$$m(x, y, z) = ((s(x, y, z)/z)/z)/z.$$

$m(x, y, z)$ is Mal'cev

If $t(x, y) = y$, then

$$\begin{aligned} m(x,x,y) &= ((s(x,x,y)/y)/y)/y \\ &= ((y/y)/y)/y \\ &= y, \\ m(x,y,y) &= ((s(x,y,y)/y)/y)/y \\ &= (((((x*y)*y)*y)/y)/y)/y \\ &= x. \end{aligned}$$

Malv'cev Terms and Tractability

Theorem (Bulatov,Dalmau)

If an algebra has a Mal'cev term, then it is tractable.

Corollary

If a quandle Q is totally connected, then it is tractable.

CSP Dichotomy

Theorem

Every quandle that is not NP-complete is tractable.

In fact, since right self distributivity is never employed, this result extends as follows.

Theorem

Every idempotent, right quasigroup that is not NP-complete is tractable.

Types 4 and 5 Omitted

Theorem (Hobby)

The pseudo variety of a finite quandle omits types 4 and 5.

The proof does use right, self distributivity and so does not apply to idempotent, right quasigroups.

The Word Problem

Specific: Let $Q = \langle A | R \rangle$ be a finitely presented quandle. Does there exist an algorithm that decides whether two expressions q_1 and q_2 over the generators A represent the same element of Q?

General: Does there exist a general algorithm over all quandles that takes $\langle A | R \rangle$ as input and then proceeds with a correct decision method?

In groups the specific version depends on the group, so the general algorithm does not exist.

Conjugation Quandles

Given a group G, define a quandle structure $\mathrm{Conj}(G)$ via

$$g * h = h^{-1}gh$$

and

$$g/h = hgh^{-1}.$$

A **conjugation quandle** is a quandle Q that embeds into $\mathrm{Conj}(G)$ for some G.

$\mathrm{Conj}(G)$ Naively

Given a finitely presented group $G = \langle A|W \rangle$ with undecidable word problem, is $\mathrm{Conj}(G)$ a finitely presented quandle with undecidable work problem?

- $\mathrm{Conj}(G)$ is not necessarily finitely presented.
- $\mathrm{Conj}(G)$ does not faithfully reflect G (Groups omit type $1!$).
- $\mathrm{Conj}(G)$ is not sufficiently general among quandles.

Lopsided Quandle

The following quandle cannot arise through conjugation.

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

Table: Lopsided Quandle

Inner Automorphisms

Let Q be a quandle. For $q \in Q$ define

$$r_q, R_q : Q \longrightarrow Q$$

by right translation as follows

$$r_q(p) = p * q$$

and

$$R_q(p) = p/q.$$

Inner Automorphisms

- r_q is always a permutation:

$$R_q = r_q^{-1}.$$

- r_q is a quandle homomorphism:

$$r_q(a * b) = (a * b) * q = (a * q) * (b * q) = r_q(a) * r_q(b).$$

Let $\mathrm{Inn}(Q)$ be the group generated by the permutations $\{r_q | q \in Q\}$. We will show that $\mathrm{Inn}(Q)$ is general among groups.

The Quandle Q_G

Given a finitely presented group

$$G = \langle A | W \rangle,$$

we wish to construct a finitely presented quandle

$$Q_G = \langle A' | R_W \rangle.$$

Example: $G = C_2$

Consider the following group presentation:

$$C_2 = \langle a | aa \rangle.$$

Let x be a fresh generator and Q_{C_2} be the following quandle presentation:

$$Q_{C_2} = \langle a, x | (x * a) * a = x, (a * a) * a = a \rangle,$$

or, rather,

$$Q_{C_2} = \langle a, x | x^{aa} = x, a^{aa} = a \rangle.$$

The Quandle Q_G

Given

$$G = \langle A | W \rangle,$$

let x be a new generator not in A and let

$$Q_G = \langle A_x | R_W \rangle$$

where

$$A_x = A \cup \{x\}$$

and

$$R_W = \{a^w = a | a \in A_x, w \in W\}.$$

The Formal Expression q^g

Given a quandle expression q over A_x and a group expression g over A, define the quandle expression q^g over A_x by structural induction:

- $q^e = q$,
- $q^{e^{-1}} = q$,
- $q^a = q * a = r_a(q)$, for $a \in A$,
- $q^{a^{-1}} = q/a = R_a(q)$ for $a \in A$,
- $q^{g_1 g_2} = (q^{g_1})^{g_2}$,
- $q^{(g_1 g_2)^{-1}} = (q^{g_2^{-1}})^{g_1^{-1}}$.

Main Result

Theorem

Given a finitely presented group G,

$$G \models g = e \text{ iff } Q_G \models x^g = x.$$

Corollary

The word problem for finitely presented quandles is, in general, undecidable.

Proof.

Let G be Novikov's group (1952), then Q_G must have undecidable word problem. □

Forward Direction

Proposition

If $G \vDash g = e$ *then* $Q_G \vDash x^g = x$.

Define $\rho : A \to \mathrm{Inn}(Q_G)$ by

$$\rho_a = r_a.$$

Then ρ extends to a group homomorphism

$$\rho : \mathrm{FG}A \to \mathrm{Inn}(Q_G).$$

Furthermore, for any $h \in G$ and $q \in Q_G$,

$$Q_G \vDash \rho_h(q) = q^h.$$

Forward Direction (Continued)

In particular, for each $w \in W$ and $a \in A_x$,

$$Q_G \vDash \rho_w(a) = a^w = a = \mathrm{id}(a)$$

so

$$\mathrm{Inn}(Q_G) \vDash \rho_w = \mathrm{id}.$$

It follows that

$$W \subseteq \ker(\rho).$$

Let $\pi_G : \mathrm{FG}A \to G$ be the canonical projection. Recall that $\ker(\pi_G)$ is the smallest normal subgroup containing W. Hence,

$$\ker(\pi_G) \subseteq \ker(\rho).$$

Forward Direction (Continued)

This means that ρ defines a homomorphism of type

$$\rho : G \to \mathrm{Inn}(Q_G).$$

Consequently, if

$$G \vDash g = e$$

then

$$\mathrm{Inn}(Q_G) \vDash \rho_g = \mathrm{id}$$

so that

$$Q_G \vDash x^g = \rho_g(x) = \mathrm{id}(x) = x.$$

Backward Direction

Proposition

If $Q_G \models x^g = x$ then $G \models g = e$.

First, consider the following finitely presented group: $G_x = \langle A_x | C_W \rangle$, where

$$C_W = \{w^{-1}aw = a | a \in A_x, w \in W\}.$$

The proposition is a consequence of the following:

Fact 1: If $Q_G \models x^g = x$ then $G_x \models g^{-1}xg = x$.

Fact 2: if $G_x \models g^{-1}xg = x$ then $G \models g = e$.

Fact 1

It is left to the audience to verify that for any $h \in \mathrm{FGA}$ and $a \in A_x$,

$$\mathrm{Conj}(G_x) \vDash a^h = a \text{ iff } G_x \vDash h^{-1}ah = a.$$

In particular, for all $w \in W$ and $a \in A_x$,

$$\mathrm{Conj}(G_x) \vDash a^w = a,$$

so that the relations in R_W hold in $\mathrm{Conj}(G_x)$. Therefore, there exists a quandle homomorphism

$$\phi : Q_G \to \mathrm{Conj}(G_x)$$

such that $\phi(a) = a$ for all $a \in A_x$.

Fact 1 (Continued)

Then if

$$Q_G \models x^g = x$$

the quandle homomorphism ϕ ensures

$$\mathrm{Conj}(G_x) \models x^g = x.$$

It follows that

$$G_x \models g^{-1}xg = x.$$

Fact 2

Let

$$G[x] = \langle A_x | W \rangle = G * \langle x \rangle,$$

the free product of G and $\langle x \rangle$.

Since the relations C_W hold in $G[x]$, there exists a unique homomorphism

$$\chi : G_x \longrightarrow G[x]$$

such that $\chi(a) = a$ for all $a \in A_x$.

Fact 2 (Continued)

Moreover, the following square commutes:

$$\chi \circ \pi_X = \iota_G \circ \pi_G$$

where π_X and π_G are the canonical homomorphisms that fix A.

Fact 2 (Continued)

Consequently, if

$$G_x \vDash g^{-1}xg = x$$

then, via χ,

$$G[x] \vDash g^{-1}xg = x.$$

However, since $G[x] = G * \langle x \rangle$,

$$G[x] \vdash g = e,$$

which, since G is included in $G[x]$, means that

$$G \vDash g = e.$$

Main Result

Theorem

Given a finitely presented group G,

$$G \models g = e \ \text{ iff } \ Q_G \models x^g = x.$$

Corollary

The word problem for finitely presented quandles is, in general, undecidable.

Proof.

Let G be Novikov's group (1952), then Q_G must have undecidable word problem. □

$\mathcal{R}$, a Term Rewriting System

ι rules:

- $x * x \longrightarrow x$
- $x/x \longrightarrow x$

ρ rules:

- $(x * y)/y \longrightarrow x$
- $(x/y) * y \longrightarrow x$

δ rules:

- $x * (y * z) \longrightarrow ((x/z) * y) * z$
- $x * (y/z) \longrightarrow ((x * z) * y)/z$
- $x/(y * z) \longrightarrow ((x/z)/y) * z$
- $x/(y/z) \longrightarrow ((x * z)/y)/z)$

TRS Basics

Definition

Let t and t' be terms over $\{*, /\}$. We say

- $t \to t'$ if t rewrites to t' in one step,
- $t \to^* t'$ if t rewrites to t' in zero or more steps, and
- $t \to^+ t'$ if t rewrites to t' in one or more steps.

Strong Normalization

Definition

A term t is a **normal form** if whenever $t \longrightarrow^* t'$, t' is identical to t.

Theorem (Golbus, Gutierrez, McGrail (GGM))

The TRS $\mathcal{R}$ is **strongly normalizing** *(SN). That is, every infinite rewrite sequence $t_0 \longrightarrow^* t_1 \longrightarrow^* \ldots$ includes a normal form.*

Strong Normalization

Proof.

(Sketch) Assume without loss of generality that $t_i \rightarrow^+ t_{i+1}$ for each i. Define a function m from terms to the natural numbers as follows:

$$m(t) = \begin{cases} 0, & \text{if } t \text{ is a variable;} \\ 1 + m(t_1) + 3m(t_2), & \text{if } t = t_1 \ o \ t_2. \end{cases} \quad (1)$$

Then $\{m(t_i) | i \in \mathbb{N}\}$ is a subset of $\mathbb{N}$ with no least element. □

Confluence

Theorem (GGM)

The TRS $\mathcal{R}$ is **confluent**. *That is whenever $t \longrightarrow^* u$ and $t \longrightarrow^* v$ there exists a term s with $u \longrightarrow^* w$ and $v \longrightarrow^* w$.*

Notes:

- If $\mathcal{S}$ is SN and confluent, it has unique normal forms.
- So $\mathcal{R}$ has unique normal forms.

$\mathcal{R}$ Decides $\mathcal{Q}$

Theorem (GGM)

The TRS $\mathcal{R}$ decides the pure equational theory of $\mathcal{Q}$. That is, the following are equivalent for any two terms t and s:

- *$t = s$ is a theorem of $\mathcal{Q}$*
- *t and s have the same normal form r over $\mathcal{R}$.*

The Towers of Hanoi

- There are n disks, each of unique size.
- There are k pegs.
- The disks are initially stacked on a **source peg** with smaller disks stacked directly on larger disks.
- The disks must all be moved to a **target peg**.
- Only one disk may be moved at one time.
- One may never stack a larger disk on a smaller disk.

Towers and the TRS

- The Towers of Hanoi encoded into TRS:

  Initial Term $y * (x_3 * (x_2 * x_1))$

  Normal Form $((((((y/x_1)/x_2) * x_1) * x_3)/x_1) * x_2) * x_1$

- Interpret both terms above in terms of number of pegs.
- Interpret $t = ((y/(x_2 * x_1)) * x_3) * (x_2 * x_1)$ as a four-peg solution.

Grand Daddy Term

Definition

For $n = 1, 2, \ldots$, define the term t_n as follows:

- $t_1 = x_1$; and
- $t_{n+1} = x_{n+1} * t_n$.

Definition

For $n = 1, 2, \ldots$, define g_n as below:

- $g_1 = y * x_1$; and
- $g_{n+1} = ((y/t_n) * x_{n+1}) * t_n$.

Solutions as Descendants

Definition

A **nice** solution to the *n*-disk Towers of Hanoi puzzle that uses no more than n pegs corresponds to some term s with $g_n \longrightarrow s$.

Question

If $g_n \longrightarrow s$, does s correspond to some solution?

Thank you!!! Any questions?