The structure and enumeration of quandles

David Stanovský

Charles University, Prague, Czech Republic
&
IITU, Almaty, Kazakhstan

based on joint research with
A. Hulpke, P. Jedlička, A. Pilitowska, P. Vojtěchovský, A. Zamojska-Dzienio

Ferrara, October 2014

Outline

1. From knots to quandles
2. Algebraically connected quandles
3. From connected to general

... *with emphasis on structure and enumeration*

Knots

knot = embedding of a circle into $\mathbb{R}^3$

K_1, K_2 *equivalent* = there is an ambient isotopy f of $\mathbb{R}^3$
such that $f(K_1) = K_2$

tame knot = equivalent to a finitely polygonal knot (or a smooth knot)

All knots in this talk are tame and *oriented*.

Knots

knot = embedding of a circle into $\mathbb{R}^3$

K_1, K_2 *equivalent* = there is an ambient isotopy f of $\mathbb{R}^3$
such that $f(K_1) = K_2$

tame knot = equivalent to a finitely polygonal knot (or a smooth knot)

All knots in this talk are tame and *oriented*.

Fundamental Problem

Given K_1, K_2, are they equivalent? Given K, is $K \sim \bigcirc$?

- Haken (1961): $\sim \bigcirc$ is decidable (in EXP-time)
- Haas-Lagarias-Pippinger (1999): $\sim \bigcirc$ is in NP
- Agol (2002, not published): $\not\sim \bigcirc$ is in NP assuming GRH
- Kuperberg (2011): $\not\sim \bigcirc$ is in NP assuming GRH

Reidemester moves

Knots are usually displayed by a *regular* projection into a plane.

Theorem (Reidemeister 1926, Alexander-Brigs 1927)

$K_1 \sim K_2$ if and only if they are related by a finite sequence of Reidemeister moves:

I. *twist/untwist a loop;*
II. *move a string over/under another;*
III. *move a string over/under a crossing.*

Reidemester moves

Knots are usually displayed by a *regular* projection into a plane.

Theorem (Reidemeister 1926, Alexander-Brigs 1927)

$K_1 \sim K_2$ if and only if they are related by a finite sequence of Reidemeister moves:

I. *twist/untwist a loop;*
II. *move a string over/under another;*
III. *move a string over/under a crossing.*

How many moves one needs?

$K \sim \bigcirc$ iff related by a sequence of at most $f(cross(K))$ Reidemeister moves, where:

- Haas-Lagarias (2001): f exponential
- Lackenby (2013): f polynomial, $(231n)^{11}$

Bad news: cross(K) may increase, Good news (Lackenby): not too much

Invariants

= mappings f assigning a value to every knot in a way that

$K_1 \sim K_2$ implies $f(K_1) = f(K_2)$.

- *mincross*(K) = the minimal number of crossings
- *col*(K) = the number of *colorings* of arcs by three colors such that no crossing has two colors
- the *knot group* $G(K) = \pi_1(\mathbb{R}^3 \smallsetminus K)$
- *Alexander-Conway polynomial* (1923/1969)

$$f(\bigcirc) = 1, \qquad f(L_+) - f(L_-) = xf(L_0)$$

- *Jones polynomial* (1984)

$$f(\bigcirc) = 1, \qquad x^{-1}f(L_+) - xf(L_-) = (x^{1/2} - x^{-1/2})f(L_0)$$

- etc.
- etc.

http://www.indiana.edu/~knotinfo

Coloring (oriented) knots

Fix a ternary relation T on a set X *(colors)*.

coloring of K $=$ a mapping c : arcs $\to$ colors s.t. $(c(\alpha), c(\beta), c(\gamma)) \in T$
for every crossing where α is the overpass, β is right, γ is left

$\mathrm{Col}_T(K) =$ the number of colorings of K by T

Coloring (oriented) knots

Fix a ternary relation T on a set X *(colors)*.

coloring of K = a mapping c : arcs $\to$ colors s.t. $(c(\alpha), c(\beta), c(\gamma)) \in T$
for every crossing where α is the overpass, β is right, γ is left

$\mathrm{Col}_T(K) =$ the number of colorings of K by T

Fact (implicitly Joyce, Matveev ('82), explicitly Fenn-Rourke ('92))

$\mathrm{Col}_T(K)$ *is an invariant if and only if for every* $x, y, z \in X$

I. $(x, x, x) \in T$

II. *there are unique* u, v *such that* $(x, y, u) \in T$ *and* $(x, v, y) \in T$
in particular, T *is a graph of an operation, let* $x * y$ *be the* u

III. $x * (y * z) = (x * y) * (x * z)$

Algebras $(X, *)$ satisfying I., II., III. are called quandles.

Quandles

Quandle is an algebra $Q = (Q, *)$ such that for every $x, y, z \in Q$

- $x * x = x$ *(idempotent)*
- there is a unique u such that $x * u = y$ *(unique left division)*
- $x * (y * z) = (x * y) * (x * z)$ *(selfdistributivity)*

Examples:

- group conjugation $x * y = y^x = xyx^{-1}$
  - conjugation in $\pi_1(\mathbb{R}^3 - K) \rightsquigarrow$ the *knot quandle*
  - *Kuperberg's algorithm:* color by conjugation quandles over $SL_2(p)$
- affine quandles $x * y = (1 - r)x + ry$ over any module, r invertible
  - coloring by affine quandles = (essentially) the *Alexander invariant*

Motivation:

- coloring knots, braids
- Hopf algebras, discrete solutions to the Yang-Baxter equation
- combinatorial algebra: a natural generalization of selfdistributive quasigroups (since 1923!)


SCORE: 75
HI-SCORE:1201


PARATROOPER
by
Greg Kuperberg
PRESS 'I' FOR INSTRUCTIONS
PRESS space bar FOR KEYBOARD PLAY
OR joystick button FOR JOYSTICK PLAY
OR ctrl-J FOR JOYSTICK adjustment
(C)1982 ORION SOFTWARE, INC.

Enumerating small groups

1..10	1	1	1	2	1	2	1	5	2	2
11..20	1	5	1	2	1	14	1	5	1	5
21..30	2	2	1	15	2	2	5	4	1	4
31..40	1	51	1	2	1	14	1	2	2	14
41..50	1	6	1	4	2	2	1	52	2	5
51..60	1	5	1	15	2	13	2	2	1	13
61..70	1	2	4	267	1	4	1	5	1	4
71..80	1	50	1	2	3	4	1	6	1	52
81..90	15	2	1	15	1	2	1	12	1	10
91..100	1	4	2	2	1	231	1	5	2	16

(Besche, Eick, O'Brien around 2000: a table up to 2047)

- size p: $\mathbb{Z}_p$
- size p^2: $\mathbb{Z}_{p^2}, \mathbb{Z}_p^2$
- size $2p$: $\mathbb{Z}_{2p}, D_{2p}$

Methods: deep structure theory and efficient programming

Enumerating small quasigroups

quasigroup = latin square

loop = quasigroup with a unit

	loops	quasigroups
1	1	1
2	1	1
3	1	5
4	2	35
5	6	1411
6	109	1130531
7	23746	12198455835
8	106228849	2697818331680661
9	9365022303540	15224734061438247321497
10	20890436195945769617	2750892211809150446995735533513

(McKay, Meynert, Myrvold 2007)

Methods: smart combinatorics and efficient programming

Enumerating quandles: an elementary approach

1..9	1	1	3	7	22	73	298	1581	11079

- exhaustive search over all tables: SAT-solver up to size 7
- exhaustive search over all permutations: Ho, Nelson up to size 8
- smarter elementary approach: McCarron up to size 9

Enumerating quandles: an elementary approach

1..9	1	1	3	7	22	73	298	1581	11079

- exhaustive search over all tables: SAT-solver up to size 7
- exhaustive search over all permutations: Ho, Nelson up to size 8
- smarter elementary approach: McCarron up to size 9

Our idea:

- think about the orbit decomposition of Q
- find a representation theorem
- count the configurations

Our results: two special cases

- *algebraically connected quandles* = with a single orbit, up to size 47
- *medial quandles* (in a sense the abelian case), up to size 13

Translations (aka inner mappings)

In a quandle Q:

- *translations* $L_x(y) = x * y$ are permutations
- *multiplication group* $\mathrm{LMlt}(Q) = \langle L_x : x \in Q \rangle$ is a permutation group

Quandles = idempotent binary algebras with $\mathrm{LMlt}(Q) \leq \mathrm{Aut}(Q)$.

Translations (aka inner mappings)

In a quandle Q:

- *translations* $L_x(y) = x * y$ are permutations
- *multiplication group* $\mathrm{LMlt}(Q) = \langle L_x : x \in Q \rangle$ is a permutation group

Quandles = idempotent binary algebras with $\mathrm{LMlt}(Q) \leq \mathrm{Aut}(Q)$.

Displacement group (aka transvection group):

$$\mathrm{Dis}(Q) = \langle L_x L_y^{-1} : \ x, y \in Q \rangle \leq \mathrm{LMlt}(Q)$$

- $\mathrm{LMlt}(Q)$ and $\mathrm{Dis}(Q)$ tell a lot about Q
- things usually work nicer for $\mathrm{Dis}(Q)$, than for $\mathrm{LMlt}(Q)$
- but I realized this too late, so our connected quandles project is based on $\mathrm{LMlt}(Q)$ (it has other advantages)

Connected quandles

$= \mathrm{LMlt}(Q)$ is transitive on Q

Galkin quandles: $\mathrm{Gal}(G, H, \varphi) = (G/H, *)$, $xH * yH = x\varphi(x^{-1})\varphi(y)H$,

- G is a group, H its subgroup
- $\varphi \in \mathrm{Aut}(G)$, $\varphi|_H = id$

Canonical representation: $Q \simeq \mathrm{Gal}(\mathrm{LMlt}(Q), \mathrm{LMlt}(Q)_e, -^{L_e})$

Connected quandles

$= \mathrm{LMlt}(Q)$ is transitive on Q

Galkin quandles: $\mathrm{Gal}(G,H,\varphi) = (G/H,*)$, $xH * yH = x\varphi(x^{-1})\varphi(y)H$,

- G is a group, H its subgroup
- $\varphi \in \mathrm{Aut}(G)$, $\varphi|_H = id$

Canonical representation: $Q \simeq \mathrm{Gal}(\mathrm{LMlt}(Q), \mathrm{LMlt}(Q)_e, -^{L_e})$

quandle envelope $= (G,\zeta)$ such that

- G a transitive group,
- $\zeta \in Z(G_e)$ such that $\langle \zeta^G \rangle = G$

Theorem (HSV)

There is 1-1 correspondence connected quandles $\leftrightarrow$ quandle envelopes

- *quandles to envelopes:* $Q \mapsto (\mathrm{LMlt}(Q), L_e)$
- *envelopes to quandles:* $(G,\zeta) \mapsto \mathrm{Gal}(G, G_e, -^{\zeta})$

Enumerating connected quandles

Important trick: we have an efficient *Isomorphism Theorem* for envelopes: $(G,\zeta) \simeq (K,\xi)$ iff there is $\psi : G \simeq K$ such that $\psi(G_e) = K_e$ and $\psi(\zeta) = \xi$.

1..10	1	0	1	1	3	2	5	3	8	1
11..20	9	10	11	0	7	9	15	12	17	10
21..30	9	0	21	42	34	0	65	13	27	24
31..40	29	17	11	0	15	73	35	0	13	33
41..47	39	26	41	9	45	0	45			

(Vedramin 2012 / HSV independently)

We count all quandle envelopes, using the full list of transitive groups of degree $n \leq 47$ (Holt 2014).

Using theory of transitive groups:

- size p: only affine, $p-2$ (Etingof, Soloviev, Guralnick 2001)
- size p^2: only affine, $2p^2-3p-1$ (Graña 2004)
- size p^3: .... (Bianco)
- size $2p$: none for $p>5$ (McCarron / HSV)

Connected quandles, prime size

Theorem (Etingof-Soloviev-Guralnik)

Connected quandles of prime size are affine.

Proof using envelopes.

$\mathrm{LMlt}(Q)$ is a transitive group acting on a prime number of elements, hence $\mathrm{LMlt}(Q)$ is primitive.
A theorem of Kazarin says that if G is a group, $a \in G$, $|a^G|$ is a prime power, then $\langle a^G \rangle$ is solvable. In our case $|L_e^{\mathrm{LMlt}(Q)}| = |Q|$ is prime, hence $\mathrm{LMlt}(Q) = \langle L_e^{\zeta} \rangle$ is solvable.
A theorem attributed to Galois says that primitive solvable groups are affine, hence $\mathrm{LMlt}(Q)$ is affine, and so is Q.

From connected to general

1. Describe connected *(we just did it)*

2. Describe orbits *(similar approach works, they are homogeneous)*

3. How orbits are assembled to obtain a quandle?

... *we will show for medial quandles*

Medial quandles

... $\mathrm{Dis}(Q) = \langle L_x L_y^{-1} : x, y \in Q \rangle$ is an abelian group

... $(x * y) * (u * v) = (x * u) * (y * v)$ for every x, y, u, v

Affine quandles: $\mathrm{Aff}(G, \varphi) = (G, *)$ with $x * y = (1 - \varphi)(x) + \varphi(y)$, where G is an abelian group, $\varphi \in \mathrm{Aut}(G)$

Fact

A connected quandle is medial iff affine.

Connected quandles of prime size: $\mathrm{Aff}(\mathbb{Z}_p, k)$ with $k = 2, \dots, p - 1$.
(Classification of affine quandles up to p^4 by Hou 2011.)

Medial quandles

... $\mathrm{Dis}(Q) = \langle L_x L_y^{-1} : x, y \in Q \rangle$ is an abelian group

... $(x * y) * (u * v) = (x * u) * (y * v)$ for every x, y, u, v

Affine quandles: $\mathrm{Aff}(G, \varphi) = (G, *)$ with $x * y = (1 - \varphi)(x) + \varphi(y)$,
where G is an abelian group, $\varphi \in \mathrm{Aut}(G)$

Fact

A connected quandle is medial iff affine.

Connected quandles of prime size: $\mathrm{Aff}(\mathbb{Z}_p, k)$ with $k = 2, \ldots, p - 1$.
(Classification of affine quandles up to p^4 by Hou 2011.)

Fact

Orbits in medial quandles are affine quandles,

$$Qe = \mathrm{Aff}(\mathrm{Dis}(Q)/\mathrm{Dis}(Q)_e, -^{L_e}).$$

The structure of medial quandles

affine mesh = triple $((A_i)_{i\in I}, (\varphi_{i,j})_{i,j\in I}, (c_{i,j})_{i,j\in I})$ indexed by I where

- A_i are abelian groups
- $\varphi_{i,j} : A_i \to A_j$ homomorphisms
- $c_{i,j} \in A_j$ constants

such that for every $i, j, j', k \in I$

- $1 - \varphi_{i,i}$ is an automorphism of A_i
- $c_{i,i} = 0$
- $\varphi_{j,k}\varphi_{i,j} = \varphi_{j',k}\varphi_{i,j'}$ (they commute naturally)
- $\varphi_{j,k}(c_{i,j}) = \varphi_{k,k}(c_{i,k} - c_{j,k})$
- $A_j = \langle c_{i,j} + \mathrm{Im}(\varphi_{i,j}) : i \in I\rangle$

Theorem (JPSZ)

There is 1-1 correspondence medial quandles $\leftrightarrow$ affine meshes

- *meshes to quandles:* $a * b = c_{i,j} + \varphi_{i,j}(a) + (1 - \varphi_{j,j})(b)$
- *quandles to meshes:* $A_e = \mathrm{Dis}(Q)/\mathrm{Dis}(Q)_e$, $\varphi_{ef}(x) = xf - ef$, $c_{ef} = ef$

Enumerating medial quandles

	medial quandles	quandles
1	1	1
2	1	1
3	3	3
4	6	7
5	18	22
6	58	73
7	251	298
8	1410	1581
9	10311	11079
10	98577	
11	1246488	
12	20837439	
13	466087635	
14	1394304 2???	
15	563753074951	

The combinatorics behind

Again, we have an efficient *Isomorphism Theorem* for meshes:

$(A_i, \varphi_{i,j}, c_{i,j}) \simeq (A'_i, \varphi'_{i,j}, c'_{i,j})$ iff $\exists\ \pi \in S_I\ \exists\ \psi_i : A_i \simeq A'_{\pi i}\ \exists\ d_i \in A'_i$

1. *... (you don't want to know) ...*
2. *... (you don't want to know) ...*

Reformulation: groups B_j, each occurs n_j-times

Isomorphism classes are precisely the orbits under an action of

$$G = \prod (B_j \rtimes \mathrm{Aut}(B_j)) \wr S_{n_j}.$$

Using *Burnside's orbit counting lemma*, we have

$$\#\ \text{orbits} = \frac{1}{|G|} \sum_{g \in R} |g/\sim| \cdot \mathit{fix}(g)$$

where $\sim$ is a subconjugacy equivalence and R a set of class representatives

Reductive medial quandles

Surprizingly, there is an important special case:

$$\varphi_{i,j} = 0 \text{ for every } i, j$$

Call them *2-reductive*. Then:

- we can simplify $G = \prod \mathrm{Aut}(B_j) \wr S_{n_j}$
- we know a formula for $\mathit{fix}(g)$ (complicated)

Burnside works awesome.

1 1 2 5 15 55 246 1398 10301 98532 1246479 20837171

466087624 13943041873 563753074915 30784745506212

Reductive medial quandles

Surprizingly, there is an important special case:

$$\varphi_{i,j} = 0 \text{ for every } i, j$$

Call them *2-reductive*. Then:

- we can simplify $G = \prod \mathrm{Aut}(B_j) \wr S_{n_j}$
- we know a formula for $fix(g)$ (complicated)

Burnside works awesome.

1 1 2 5 15 55 246 1398 10301 98532 1246479 20837171

466087624 13943041873 563753074915 30784745506212

There are very few other medial quandles!

0 0 1 1 3 3 5 12 10 45 9 278 11 ? 36

Reductive medial quandles

Surprizingly, there is an important special case:

$$\varphi_{i,j} = 0 \text{ for every } i,j$$

Call them *2-reductive*. Then:

- we can simplify $G = \prod \mathrm{Aut}(B_j) \wr S_{n_j}$
- we know a formula for $fix(g)$ (complicated)

Burnside works awesome.

1 1 2 5 15 55 246 1398 10301 98532 1246479 20837171

466087624 13943041873 563753074915 30784745506212

There are very few other medial quandles!

0 0 1 1 3 3 5 12 10 45 9 278 11 ? 36

Conjecture (:-0)

There are more 2-reductive than non-2-reductive, for every size.

Reductive medial quandles II

A medial quandle is called *m-reductive* if following equivalent cond's hold:

- all compositions of right translations $R_{u_1}...R_{u_m}$ are constant
- the orbits are $\varphi^{m-1} = 0$.

Fact: 2-reductive iff $\varphi_{i,i} = 0\ \forall i$ iff $\varphi_{i,j} = 0\ \forall i, j$

Reductive medial quandles II

A medial quandle is called *m-reductive* if following equivalent cond's hold:

- all compositions of right translations $R_{u_1} \dots R_{u_m}$ are constant
- the orbits are $\varphi^{m-1} = 0$.

Fact: 2-reductive iff $\varphi_{i,i} = 0\ \forall i$ iff $\varphi_{i,j} = 0\ \forall i, j$

Fact: all $\varphi_{i,i}$ permutations iff all orbits latin quandles

n	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
non-2-red.	0	0	1	1	3	3	5	12	10	45	9	268	11		36
red., not 2-red.	0	0	0	0	0	2	0	9	0	42	0	260	0		12
non-red.	0	0	1	1	3	1	5	3	10	3	9	8	11	5	24
latin orbits	0	0	1	1	3	1	5	3	9	3	9	3	11	5	7
latin	1	0	1	1	3	0	5	2	8	0	9	1	11	0	3

Conclusion

- few groups, many quasigroups
- few connected quandles, many quandles
- few non-2-reductive medial quandles, many 2-reductive medial quandles

WHY???