Enumeration of quandles: Part 1

Petr Vojtěchovský

UNIVERSITY OF DENVER

Advances in Group Theory and Applications 2025
Napoli
June 23-28, 2025

Coauthors

H = Alexander Hulpke

K = Louis Kauffman

M = Sujoy Mukherjee

P = Jesse Parrish

S = David Stanovský

Y = Seung-Yeop Yang

Outline

Coloring rules

Color a diagram of an oriented knot K by an algebra $(X, \triangleleft, \triangleright)$ according to these rules:

Coloring rules

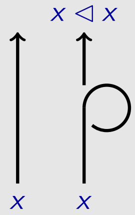
Color a diagram of an oriented knot K by an algebra $(X, \lhd, \rhd)$ according to these rules:

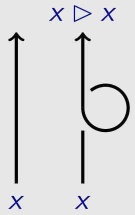
Coloring rules

Color a diagram of an oriented knot K by an algebra $(X, \triangleleft, \triangleright)$ according to these rules:

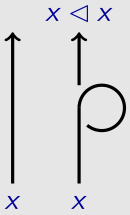
Which properties must $\triangleleft$, $\triangleright$ satisfy for the coloring to be invariant under Reidemeister moves? There are many oriented Reidemeister moves, but all are consequences of the following five:

Reidemeister I



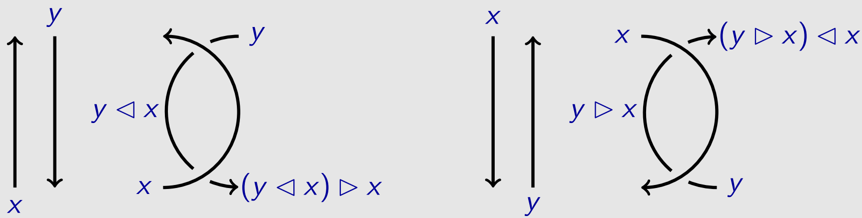


Reidemeister I

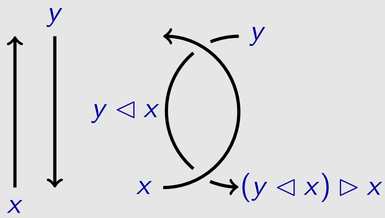


So far we have $x \lhd x = x = x \rhd x$.

Reidemeister II



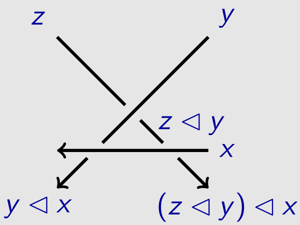
Reidemeister II



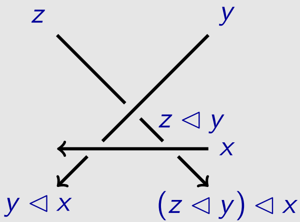
So far we have $x \triangleleft x = x = x \triangleright x$, $(y \triangleleft x) \triangleright x = y$ and $(y \triangleright x) \triangleleft x = y$.

Hence $R_x^{\triangleleft} = (R_x^{\triangleright})^{-1}$ and we don't need to keep track of $\triangleright$ anymore.

Reidemeister III



Reidemeister III



Altogether, we have: $(X, \triangleleft)$ such that $x \triangleleft x = x$ and $R_x \in \mathrm{Aut}(X, \triangleleft)$.

Racks and quandles

Definition

A magma $(Q, \cdot)$ is a **rack** if

- R_x is a permutation of Q for every $x \in Q$,
- $(yx)(zx) = (yz)x$ for every $x, y, z \in Q$.

A rack $(Q, \cdot)$ is a **quandle** if

- $xx = x$ for every $x \in Q$.

Racks and quandles

Definition

A magma $(Q,\cdot)$ is a **rack** if

- R_x is a permutation of Q for every $x \in Q$,
- $(yx)(zx) = (yz)x$ for every $x, y, z \in Q$.

A rack $(Q,\cdot)$ is a **quandle** if

- $xx = x$ for every $x \in Q$.

Definition

For a rack Q, let

$$\mathrm{Mlt_r(Q)} = \langle R_x : x \in Q\rangle \leq \mathrm{Aut}(Q)$$

be the **right multiplication group** of Q.

Examples of quandles

Projection quandle

$x * y = x$

on a set X

Examples of quandles

Projection quandle

$x * y = x$

on a set X

Conjugation quandle

$x * y = yxy^{-1}$

on a group $(G, \cdot)$, or on a union of some conjugacy classes

Examples of quandles

Projection quandle

$x * y = x$

on a set X

Conjugation quandle

$x * y = yxy^{-1}$

on a group $(G, \cdot)$, or on a union of some conjugacy classes

Affine quandle

$x * y = \varphi(x) + (1 - \varphi)(y)$

for a group $(G, +)$ and $\varphi \in \mathrm{Aut}(G)$

Examples of quandles

Projection quandle

$x * y = x$

on a set X

Conjugation quandle

$x * y = yxy^{-1}$

on a group $(G, \cdot)$, or on a union of some conjugacy classes

Affine quandle

$x * y = \varphi(x) + (1 - \varphi)(y)$

for a group $(G, +)$ and $\varphi \in \mathrm{Aut}(G)$

Coset quandle

$Hx * Hy = H\varphi(xy^{-1})y$

for a group $(G, \cdot)$, subgroup $H \leq G$ and $\varphi \in \mathrm{Aut}(G)$ centralizing H

Outline

Key properties of racks and quandles

Denote by g^G the conjugacy class of g in G.

If G acts on X, let $O(x)$ be the orbit of x and X/G a complete set of orbit representatives.

Key properties of racks and quandles

Denote by g^G the conjugacy class of g in G.

If G acts on X, let $O(x)$ be the orbit of x and X/G a complete set of orbit representatives.

In any magma Q, if $x \in Q$ and $\varphi \in \mathrm{Aut}(Q)$ then $\varphi R_x \varphi^{-1} = R_{\varphi(x)}$.

Key properties of racks and quandles

Denote by g^G the conjugacy class of g in G.

If G acts on X, let $O(x)$ be the orbit of x and X/G a complete set of orbit representatives.

In any magma Q, if $x \in Q$ and $\varphi \in \mathrm{Aut}(Q)$ then $\varphi R_x \varphi^{-1} = R_{\varphi(x)}$.

Let Q be a rack and $G = \mathrm{Mlt_r(Q)}$. Then:

- $R_x \in C_G(G_x)$,
- $R_x^G = \{R_{\varphi(x)} : \varphi \in G\} = \{R_y : y \in O(x)\}$,
- $G = \langle \bigcup_{x \in Q/G} R_x^G \rangle$,
- if Q is a quandle, then $R_x \in Z(G_x)$ since $R_x(x) = xx = x$.

Joyce-Blackburn representation for racks

Theorem (Blackburn, VY)

Let G be a group acting on X. Then there is a one to one correspondence between:

- *racks Q defined on X with $\mathrm{Mlt_r(Q)} = G$, and*
- **rack envelopes** *for G, that is, tuples $(\rho_x : x \in X/G)$ such that $\rho_x \in C_G(G_x)$ and $\langle \bigcup_{x \in X/G} \rho_x^G \rangle = G$.*

Joyce-Blackburn representation for quandles

Theorem (Blackburn, VY)

Let G be a group acting on X. Then there is a one to one correspondence between:

- *quandles Q defined on X with $\mathrm{Mlt_r(Q)} = G$, and*
- **quandle envelopes** *for G, that is, tuples $(\rho_x : x \in X/G)$ such that $\rho_x \in Z(G_x)$ and $\langle \bigcup_{x \in X/G} \rho_x^G \rangle = G$.*

From a quandle envelope to a quandle: An example

Let $G = \langle (2,3,4),(2,3) \rangle \cong S_3$ act on $\{1,2,3,4\}$. The orbits are $\{1\},\{2,3,4\}$ and we can take $X/G = \{1,2\}$.

From a quandle envelope to a quandle: An example

Let $G = \langle (2,3,4),(2,3)\rangle \cong S_3$ act on $\{1,2,3,4\}$. The orbits are $\{1\},\{2,3,4\}$ and we can take $X/G = \{1,2\}$.

We have $G_1 = G$, $Z(G_1) = 1$ and $G_2 = \langle (3,4)\rangle = Z(G_2)$.

From a quandle envelope to a quandle: An example

Let $G = \langle (2,3,4),(2,3) \rangle \cong S_3$ act on $\{1,2,3,4\}$. The orbits are $\{1\},\{2,3,4\}$ and we can take $X/G = \{1,2\}$.

We have $G_1 = G$, $Z(G_1) = 1$ and $G_2 = \langle (3,4) \rangle = Z(G_2)$.

Let us take $\rho_1 = ()$ and $\rho_2 = (3,4)$. Then $\langle \rho_2^G \rangle = G$.

From a quandle envelope to a quandle: An example

Let $G = \langle (2,3,4),(2,3) \rangle \cong S_3$ act on $\{1,2,3,4\}$. The orbits are $\{1\},\{2,3,4\}$ and we can take $X/G = \{1,2\}$.

We have $G_1 = G$, $Z(G_1) = 1$ and $G_2 = \langle (3,4) \rangle = Z(G_2)$.

Let us take $\rho_1 = ()$ and $\rho_2 = (3,4)$. Then $\langle \rho_2^G \rangle = G$.

With $\varphi = (2,3,4) \in G$, we have
$\rho_3 = \varphi\rho_2\varphi^{-1} = (2,4)$ and $\rho_4 = \varphi^{-1}\rho_2\varphi = (2,3)$.

From a quandle envelope to a quandle: An example

Let $G = \langle (2,3,4),(2,3) \rangle \cong S_3$ act on $\{1,2,3,4\}$. The orbits are $\{1\},\{2,3,4\}$ and we can take $X/G = \{1,2\}$.

We have $G_1 = G$, $Z(G_1) = 1$ and $G_2 = \langle (3,4) \rangle = Z(G_2)$.

Let us take $\rho_1 = ()$ and $\rho_2 = (3,4)$. Then $\langle \rho_2^G \rangle = G$.

With $\varphi = (2,3,4) \in G$, we have
$\rho_3 = \varphi\rho_2\varphi^{-1} = (2,4)$ and $\rho_4 = \varphi^{-1}\rho_2\varphi = (2,3)$.

We obtain the quandle

Q	1	2	3	4
1	1	1	1	1
2	2	2	4	3
3	3	4	3	2
4	4	3	2	4

Outline

Isomorphisms and conjugation

Proposition (folklore for right quasigroups)

Let X be a set.

- *If $(X,*)$, $(X,\circ)$ are isomorphic racks then $\mathrm{Mlt_r}(X,*)$, $\mathrm{Mlt_r}(X,\circ)$ are conjugate subgroups of S_X.*
- *Let G, H be conjugate subgroups of S_X. Then the set of racks on X with right multiplication group equal to G contains the same isomorphism types as the set of racks on X with right multiplication group equal to H.*

(iii) *Let $(X,*)$, $(X,\circ)$ be two racks with $\mathrm{Mlt_r}(X,*) = G = \mathrm{Mlt_r}(X,\circ)$. Then $(X,*)$, $(X,\circ)$ are isomorphic if and only if there is an isomorphism $f:(X,*)\to(X,\circ)$ satisfying $f\in N_{S_X}(G)$.*

Action on parameter spaces

For a group $G \leq S_X$ let

$$\mathrm{Par}_r(G) = \prod_{x \in X/G} C_G(G_x), \quad \mathrm{Par}_q(G) = \prod_{x \in X/G} Z(G_x).$$

Action on parameter spaces

For a group $G \leq S_X$ let

$$\mathrm{Par}_r(G) = \prod_{x \in X/G} C_G(G_x), \quad \mathrm{Par}_q(G) = \prod_{x \in X/G} Z(G_x).$$

The above isomorphism relation induces an action of $N_{S_X}(G)$ on $\mathrm{Par}_r(G)$

Action on parameter spaces

For a group $G \le S_X$ let

$$\mathrm{Par}_r(G) = \prod_{x \in X/G} C_G(G_x), \quad \mathrm{Par}_q(G) = \prod_{x \in X/G} Z(G_x).$$

The above isomorphism relation induces an action of $N_{S_X}(G)$ on $\mathrm{Par}_r(G)$

Difficulties:

- $\mathrm{Par}_r(G)$ can be large, especially if G is an elementary abelian 2-group. There is a nonabelian $G \le S_{13}$ for which $\mathrm{Par}_r(G)$ has over 2 billion elements.
- Not every $(\rho_x^G : x \in X/G) \in \mathrm{Par}_r(G)$ generates G. This must be explicitly tested.
- Not clear how to use Burnside's Lemma efficiently for envelopes.

Conjugacy classes of subgroups of symmetric groups

It is a nontrivial problem to calculate subgroups of S_n up to conjugation. The following takes several hours in GAP:

n	1	2	3	4	5	6	7	8	9	10	11	12	13
$s(n)$	1	2	4	11	19	56	96	296	554	1593	3094	10723	20832

Conjugacy classes of subgroups of symmetric groups

It is a nontrivial problem to calculate subgroups of S_n up to conjugation. The following takes several hours in GAP:

n	1	2	3	4	5	6	7	8	9	10	11	12	13
$s(n)$	1	2	4	11	19	56	96	296	554	1593	3094	10723	20832

State of the art:

Theorem (Holt)

There are 7598016157515302757 subgroups of S_{18}, partitioned into 7274651 conjugacy classes.

The enumeration algorithm

Let $r(n)$ (resp. $q(n)$) denote the number of racks (resp. quandles) of order n up to isomorphism.

The enumeration algorithm

Let $r(n)$ (resp. $q(n)$) denote the number of racks (resp. quandles) of order n up to isomorphism.

The algorithm:

- confirms all previously known results $r(\leq 8)$, $q(\leq 9)$ in 3 seconds,

The enumeration algorithm

Let $r(n)$ (resp. $q(n)$) denote the number of racks (resp. quandles) of order n up to isomorphism.

The algorithm:

- confirms all previously known results $r(\leq 8)$, $q(\leq 9)$ in 3 seconds,
- takes about a day to find isomorphism types for $r(11)$ and $q(12)$,

The enumeration algorithm

Let $r(n)$ (resp. $q(n)$) denote the number of racks (resp. quandles) of order n up to isomorphism.

The algorithm:

- confirms all previously known results $r(\leq 8)$, $q(\leq 9)$ in 3 seconds,
- takes about a day to find isomorphism types for $r(11)$ and $q(12)$,
- crashes on $r(12)$, $r(13)$ and $q(13)$,

The enumeration algorithm

Let $r(n)$ (resp. $q(n)$) denote the number of racks (resp. quandles) of order n up to isomorphism.

The algorithm:

- confirms all previously known results $r(\leq 8)$, $q(\leq 9)$ in 3 seconds,
- takes about a day to find isomorphism types for $r(11)$ and $q(12)$,
- crashes on $r(12)$, $r(13)$ and $q(13)$,
- takes 3 weeks to determine isomorphism types of racks of order 13 with **nonabelian** right multiplication groups.

Racks with commuting right translations

Theorem

The following conditions are equivalent for a rack Q:

- $\mathrm{Mlt_r(Q)}$ *is abelian,*
- $(xy)z = (xz)y$,
- $x(yz) = xy$,
- Q *is* 2-**reductive** *(that is, $x(yu) = x(yv)$),*
- Q *is* **medial** *(that is, $(xu)(vy) = (xv)(uy)$) and* **paragraphic** *(that is, $x(yx) = xy$).*

Jedlička, Pilitowska, Stanovský and Zamojska-Dzienio used **affine meshes** to construct all 2-reductive racks, in principle. They used Burnside's Lemma efficiently to count 2-reductive racks up to $n \leq 14$. Using their counts for the abelian case, we determined $r(12)$, $r(13)$ and $q(13)$.

Enumeration results: Racks and quandles

n	$q(n)$	$r(n)$	comments
1	1	1	
2	1	2	
3	3	6	
4	7	19	
5	22	74	
6	73	353	
7	298	2080	easy; add column, test, backtrack

Enumeration results: Racks and quandles

n	$q(n)$	$r(n)$	comments
1	1	1	
2	1	2	
3	3	6	
4	7	19	
5	22	74	
6	73	353	
7	298	2080	easy; add column, test, backtrack
8	1581	16023	McCarron
9	11079	159526	$q(9)$ McCarron

Enumeration results: Racks and quandles

n	$q(n)$	$r(n)$	comments
1	1	1	
2	1	2	
3	3	6	
4	7	19	
5	22	74	
6	73	353	
7	298	2080	easy; add column, test, backtrack
8	1581	16023	McCarron
9	11079	159526	$q(9)$ McCarron
10	102771	2093244	

Enumeration results: Racks and quandles

n	$q(n)$	$r(n)$	comments
1	1	1	
2	1	2	
3	3	6	
4	7	19	
5	22	74	
6	73	353	
7	298	2080	easy; add column, test, backtrack
8	1581	16023	McCarron
9	11079	159526	$q(9)$ McCarron
10	102771	2093244	
11	1275419	36265070	

Enumeration results: Racks and quandles

n	$q(n)$	$r(n)$	comments
1	1	1	
2	1	2	
3	3	6	
4	7	19	
5	22	74	
6	73	353	
7	298	2080	easy; add column, test, backtrack
8	1581	16023	McCarron
9	11079	159526	$q(9)$ McCarron
10	102771	2093244	
11	1275419	36265070	
12	21101335	836395102	

Enumeration results: Racks and quandles

n	$q(n)$	$r(n)$	comments
1	1	1	
2	1	2	
3	3	6	
4	7	19	
5	22	74	
6	73	353	
7	298	2080	easy; add column, test, backtrack
8	1581	16023	McCarron
9	11079	159526	$q(9)$ McCarron
10	102771	2093244	
11	1275419	36265070	
12	21101335	836395102	BUT WAIT, THERE IS MORE

Enumeration results: Racks and quandles

n	$q(n)$	$r(n)$	comments
1	1	1	
2	1	2	
3	3	6	
4	7	19	
5	22	74	
6	73	353	
7	298	2080	easy; add column, test, backtrack
8	1581	16023	McCarron
9	11079	159526	$q(9)$ McCarron
10	102771	2093244	
11	1275419	36265070	
12	21101335	836395102	BUT WAIT, THERE IS MORE
13	469250886	25794670618	VY

Asymptotic growth

Theorem (Blackburn 2013)

For all sufficiently large orders n, we have

$$2^{n^2/4-o(n\log(n))} \le q(n) \le r(n) \le 2^{cn^2},$$

where c is a constant approximately equal to 1.5566.

Theorem (Ashford and Riordan 2017)

For every $\varepsilon > 0$ and for all sufficiently large orders n we have

$$2^{n^2/4-\varepsilon} \le q(n) \le r(n) \le 2^{n^2/4+\varepsilon}.$$

Outline

Connected quandles

Definition

A quandle Q is **connected** if $\mathrm{Mlt_r(Q)}$ acts transitively on Q.

Theorem

Let G be a group acting transitively on X. Let $x \in X$. There is a one-to-one correspondence between:

- *connected quandles Q on X with $\mathrm{Mlt_r(Q)} = G$, and*
- *the set of all $\rho_x \in C_G(G_x)$ such that $\langle \rho_x^G \rangle = G$.*

Enumeration results: Connected quandles

The enumeration of connected quandles was carried out independently by HSV and by Vendramin.

n	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
$c(n)$	1	0	1	1	3	2	5	3	8	1	9	10	11	0	7	9

n	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32
$c(n)$	15	12	17	10	9	0	21	42	34	0	65	13	27	24	29	17

n	33	34	35	36	37	38	39	40	41	42	43	44	45	46	47
$c(n)$	11	0	15	73	35	0	13	33	39	26	41	9	45	0	45

Enumeration results: Connected quandles

The enumeration of connected quandles was carried out independently by HSV and by Vendramin.

n	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
$c(n)$	1	0	1	1	3	2	5	3	8	1	9	10	11	0	7	9

n	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32
$c(n)$	15	12	17	10	9	0	21	42	34	0	65	13	27	24	29	17

n	33	34	35	36	37	38	39	40	41	42	43	44	45	46	47
$c(n)$	11	0	15	73	35	0	13	33	39	26	41	9	45	0	45

(Note $c(2p)$ for primes $p > 5$.)

Commuting translations and connectedness

For a rack Q let $\mathrm{Dis_r(Q)} = \langle R_x^{-1}R_y : x, y \in Q\rangle$ be the **right displacement group**.

Proposition (Joyce)

Let Q be a rack. Then $\mathrm{Dis_r(Q)} \trianglelefteq \mathrm{Mlt_r(Q)}$ and $\mathrm{Mlt_r(Q)}/\mathrm{Dis_r(Q)}$ is cyclic.

Commuting translations and connectedness

For a rack Q let $\mathrm{Dis_r(Q)} = \langle R_x^{-1}R_y : x, y \in Q\rangle$ be the **right displacement group**.

Proposition (Joyce)

Let Q be a rack. Then $\mathrm{Dis_r(Q)} \trianglelefteq \mathrm{Mlt_r(Q)}$ *and* $\mathrm{Mlt_r(Q)}/\mathrm{Dis_r(Q)}$ *is cyclic.*

Corollary

Let Q be a connected rack. Then $\mathrm{Mlt_r(Q)}' = \mathrm{Dis_r(Q)}$.

Proof.

For $x, y \in Q$ let $\varphi \in \mathrm{Mlt_r(Q)}$ be such that $\varphi(x) = y$. Then
$R_x^{-1}R_y = R_x^{-1}R_{\varphi(x)} = R_x^{-1}\varphi R_x\varphi^{-1} = [R_x, \varphi^{-1}] \in \mathrm{Mlt_r(Q)}'$. □

Commuting translations and connectedness

For a rack Q let $\mathrm{Dis_r(Q)} = \langle R_x^{-1} R_y : x, y \in Q \rangle$ be the **right displacement group**.

Proposition (Joyce)

Let Q be a rack. Then $\mathrm{Dis_r(Q)} \trianglelefteq \mathrm{Mlt_r(Q)}$ and $\mathrm{Mlt_r(Q)}/\mathrm{Dis_r(Q)}$ is cyclic.

Corollary

Let Q be a connected rack. Then $\mathrm{Mlt_r(Q)}' = \mathrm{Dis_r(Q)}$.

Proof.

For $x, y \in Q$ let $\varphi \in \mathrm{Mlt_r(Q)}$ be such that $\varphi(x) = y$. Then
$R_x^{-1} R_y = R_x^{-1} R_{\varphi(x)} = R_x^{-1} \varphi R_x \varphi^{-1} = [R_x, \varphi^{-1}] \in \mathrm{Mlt_r(Q)}'$. □

Corollary

Let Q be a connected quandle with $\mathrm{Mlt_r(Q)}$ abelian. Then $Q = 1$.

Commuting translations in connected quandles

A subset S of a quandle Q is an **R-clique** if $[R_x, R_y] = 1$ for all $x, y \in S$.

Commuting translations in connected quandles

A subset S of a quandle Q is an **R-clique** if $[R_x, R_y] = 1$ for all $x, y \in S$.

It is easy to prove that maximal R-cliques are subquandles. We know from above that in a nontrivial connected quandle every R-clique must be proper. How big can it get? One third is achievable:

Commuting translations in connected quandles

A subset S of a quandle Q is an **R-clique** if $[R_x, R_y] = 1$ for all $x, y \in S$.

It is easy to prove that maximal R-cliques are subquandles. We know from above that in a nontrivial connected quandle every R-clique must be proper. How big can it get? One third is achievable:

Theorem (KMV 2025)

Let $m > 0$ and $e \in \mathbb{Z}_2^m$. Let $Q = (\mathbb{Z}_3 \times \mathbb{Z}_2^m, *)$, where

$$(i,a)*(j,b) = \begin{cases} (-i-j, a), & \textit{if } i-j \equiv 0 \pmod 3, \\ (-i-j, a+b), & \textit{if } i-j \equiv 1 \pmod 3, \\ (-i-j, a+b+e), & \textit{otherwise.} \end{cases}$$

Then Q is a connected quandle in which the 2^m right translations $R_{(0,a)}$ are pairwise distinct and pairwise commute.

Outline

Principal quandles

Recall coset quandles:
$Hx * Hy = H\varphi(xy^{-1})y$,
$(G, \cdot)$ a group, $H \leq G$, $\varphi \in \mathrm{Aut}(G)$ centralizing H

Recall affine quandles:
$x * y = \varphi(x) + (1-\varphi)(y) = \varphi(x-y) + y$
for a group $(G, +)$ and $\varphi \in \mathrm{Aut}(G)$

Principal quandles

Recall coset quandles:
$Hx * Hy = H\varphi(xy^{-1})y$,
$(G, \cdot)$ a group, $H \leq G$, $\varphi \in \mathrm{Aut}(G)$ centralizing H

Recall affine quandles:
$x * y = \varphi(x) + (1 - \varphi)(y) = \varphi(x - y) + y$
for a group $(G, +)$ and $\varphi \in \mathrm{Aut}(G)$

Definition

Let $(G, \cdot, 1)$ be a group and $\varphi \in \mathrm{Aut}(Q)$. Then the **principal quandle** $Q(G, \varphi)$ is defined on G by

$$x * y = \varphi(xy^{-1})y.$$

Basic properties of principal quandles

Let $Q = Q(G, \varphi)$ be a principal quandle.
Let $\theta(x) = \varphi(x)^{-1}x$.
Then:

Basic properties of principal quandles

Let $Q = Q(G, \varphi)$ be a principal quandle.
Let $\theta(x) = \varphi(x)^{-1}x$.
Then:

- $R_1 = \varphi$,

Basic properties of principal quandles

Let $Q = Q(G, \varphi)$ be a principal quandle.
Let $\theta(x) = \varphi(x)^{-1}x$.
Then:

- $R_1 = \varphi$,
- $F = F(G, \varphi) = \{x \in G : \varphi(x) = x\} \leq G$,

Basic properties of principal quandles

Let $Q = Q(G, \varphi)$ be a principal quandle.
Let $\theta(x) = \varphi(x)^{-1}x$.
Then:

- $R_1 = \varphi$,
- $F = F(G, \varphi) = \{x \in G : \varphi(x) = x\} \leq G$,
- $S = S(F, \varphi) = \langle \theta(x) : x \in G \rangle \trianglelefteq G$,

Basic properties of principal quandles

Let $Q = Q(G, \varphi)$ be a principal quandle.
Let $\theta(x) = \varphi(x)^{-1}x$.
Then:

- $R_1 = \varphi$,
- $F = F(G, \varphi) = \{x \in G : \varphi(x) = x\} \leq G$,
- $S = S(F, \varphi) = \langle \theta(x) : x \in G \rangle \trianglelefteq G$,
- $(SF)/S \cong F/(S \cap F)$ (let $m(Q) = [F : S \cap F]$),

Basic properties of principal quandles

Let $Q = Q(G, \varphi)$ be a principal quandle.
Let $\theta(x) = \varphi(x)^{-1}x$.
Then:

- $R_1 = \varphi$,
- $F = F(G, \varphi) = \{x \in G : \varphi(x) = x\} \leq G$,
- $S = S(F, \varphi) = \langle \theta(x) : x \in G \rangle \trianglelefteq G$,
- $(SF)/S \cong F/(S \cap F)$ (let $m(Q) = [F : S \cap F]$),
- Q is connected iff $S = G$,

Basic properties of principal quandles

Let $Q = Q(G, \varphi)$ be a principal quandle.
Let $\theta(x) = \varphi(x)^{-1}x$.
Then:

- $R_1 = \varphi$,
- $F = F(G, \varphi) = \{x \in G : \varphi(x) = x\} \leq G$,
- $S = S(F, \varphi) = \langle \theta(x) : x \in G \rangle \trianglelefteq G$,
- $(SF)/S \cong F/(S \cap F)$ (let $m(Q) = [F : S \cap F]$),
- Q is connected iff $S = G$,
- any union of cosets of S is a subquandle of Q.

Essential subquandles

Lemma

Let $Q = Q(G, \varphi)$ *and* $S = S(G, \varphi)$. *For any* $x, y \in G$ *we have* $\theta(Sx) = \theta(Sy)$ *or* $\theta(Sx) \cap \theta(Sy) = \emptyset$.

Essential subquandles

Lemma

Let $Q = Q(G,\varphi)$ and $S = S(G,\varphi)$. For any $x, y \in G$ we have $\theta(Sx) = \theta(Sy)$ or $\theta(Sx) \cap \theta(Sy) = \emptyset$.

Definition

An **essential subquandle** of Q is any subquandle of the form

$$E = \bigcup_{x \in X} Sx$$

such that $\theta(E) = \theta(G)$ and $\theta(Sx) \cap \theta(Sy) = \emptyset$ for $x \neq y \in X$.

Essential subquandles

Lemma

Let $Q = Q(G,\varphi)$ *and* $S = S(G,\varphi)$*. For any* $x, y \in G$ *we have* $\theta(Sx) = \theta(Sy)$ *or* $\theta(Sx) \cap \theta(Sy) = \emptyset$*.*

Definition

An **essential subquandle** of Q is any subquandle of the form

$$E = \bigcup_{x \in X} Sx$$

such that $\theta(E) = \theta(G)$ and $\theta(Sx) \cap \theta(Sy) = \emptyset$ for $x \neq y \in X$.

Lemma (PV)

Any two essential subquandles are isomorphic.

The isomorphism problem for principal quandles

Theorem

If φ, ψ are conjugate in $\mathrm{Aut}(G)$ then $Q(G,\varphi) \cong Q(G,\psi)$.

The isomorphism problem for principal quandles

Theorem

If φ, ψ are conjugate in $\mathrm{Aut}(G)$ then $Q(G, \varphi) \cong Q(G, \psi)$.

Problem

For which groups G is the converse true? That is, which groups G have the property that whenever $Q(G, \varphi) \cong Q(G, \psi)$ then the automorphisms φ, ψ are conjugate in $\mathrm{Aut}(G)$?

The isomorphism problem for principal quandles

Theorem

If φ, ψ are conjugate in $\mathrm{Aut}(G)$ then $Q(G, \varphi) \cong Q(G, \psi)$.

Problem

For which groups G is the converse true? That is, which groups G have the property that whenever $Q(G, \varphi) \cong Q(G, \psi)$ then the automorphisms φ, ψ are conjugate in $\mathrm{Aut}(G)$?

- for simple groups [SV]
- for symmetric groups [Higashitani-Kurihara 2023]
- for dihedral groups D_{2p}, p prime [same]

An isomorphism theorem for principal quandles

Theorem (PSV)

For $i \in \{1, 2\}$ *let* $(G_i, \cdot, e_i)$ *be a group,* $\varphi_i \in \mathrm{Aut}(G_i)$, $Q_i = Q(G_i, \varphi_i)$, $S_i = S(G_i, \varphi_i)$ *and* $m_i = m(Q_i)$. *Let* $E_1 = \bigcup_{x \in X_1} S_1 x$ *be an essential subquandle of* Q_1. *Then* $Q_1 \cong Q_2$ *if and only if*

- $m_1 = m_2$,
- *there is a group isomorphism* $\psi : S_1 \to S_2$ *such that* $\psi\varphi_1 = \varphi_2\psi$ *on* S_1,
- *there is a mapping* $\sigma : X_1 \to Q_2$ *such that* $\sigma(e_1) = e_2$ *and* $\psi\theta_1 = \theta_2\sigma$ *on* X_1.

An isomorphism theorem for principal quandles

Theorem (PSV)

For $i \in \{1,2\}$ *let* $(G_i, \cdot, e_i)$ *be a group,* $\varphi_i \in \mathrm{Aut}(G_i)$, $Q_i = Q(G_i, \varphi_i)$, $S_i = S(G_i, \varphi_i)$ *and* $m_i = m(Q_i)$. *Let* $E_1 = \bigcup_{x \in X_1} S_1 x$ *be an essential subquandle of* Q_1. *Then* $Q_1 \cong Q_2$ *if and only if*

- $m_1 = m_2$,
- *there is a group isomorphism* $\psi : S_1 \to S_2$ *such that* $\psi\varphi_1 = \varphi_2\psi$ *on* S_1,
- *there is a mapping* $\sigma : X_1 \to Q_2$ *such that* $\sigma(e_1) = e_2$ *and* $\psi\theta_1 = \theta_2\sigma$ *on* X_1.

This generalizes results of Hou and Holmes for affine quandles.

Hayashi's conjecture

Note: In a connected rack, any two right translations have the same cycle structure (since they are conjugate).

Hayashi's conjecture

Note: In a connected rack, any two right translations have the same cycle structure (since they are conjugate).

Definition

A permutation φ on a finite set X has a **regular cycle** if it has a cycle of length $|\varphi|$.

Hayashi's conjecture

Note: In a connected rack, any two right translations have the same cycle structure (since they are conjugate).

Definition

A permutation φ on a finite set X has a **regular cycle** if it has a cycle of length $|\varphi|$.

Conjecture (Hayashi)

Let Q be a finite connected quandle. Then every right translation of Q has a regular cycle.

Towards disproving Hayashi's conjecture

Proposition

Suppose that G *is a finite group and* $\varphi \in \mathrm{Aut}(G)$ *is such that* $S(G,\varphi) = \langle \varphi(x)^{-1}x : x \in G\rangle = G$ *and* φ *does* **not** *have a regular cycle. Then the principal quandle* $Q = Q(G,\varphi)$ *is a counterexample to Hayashi's conjecture.*

Towards disproving Hayashi's conjecture

Proposition

Suppose that G is a finite group and $\varphi \in \mathrm{Aut}(G)$ is such that $S(G,\varphi) = \langle \varphi(x)^{-1}x : x \in G\rangle = G$ and φ does **not** *have a regular cycle. Then the principal quandle $Q = Q(G,\varphi)$ is a counterexample to Hayashi's conjecture.*

- There are finite groups possessing an automorphism without a regular cycle [Horoshevskii].
- For all such group automorphisms I tested, the best I could see was $[G : S(G,\varphi)] = 4$.

Towards disproving Hayashi's conjecture

Proposition

Suppose that G is a finite group and $\varphi \in \mathrm{Aut}(G)$ is such that $S(G,\varphi) = \langle \varphi(x)^{-1}x : x \in G \rangle = G$ and φ does **not** *have a regular cycle. Then the principal quandle $Q = Q(G,\varphi)$ is a counterexample to Hayashi's conjecture.*

- There are finite groups possessing an automorphism without a regular cycle [Horoshevskii].
- For all such group automorphisms I tested, the best I could see was $[G : S(G,\varphi)] = 4$.

Problem

Is there a finite group G and an automorphism φ of G such that $\langle \varphi(x)^{-1}x : x \in G \rangle = G$ and φ does not have a regular cycle?

Towards proving Hayashi's conjecture

Hayashi's conjecture is true for:

Towards proving Hayashi's conjecture

Hayashi's conjecture is true for:

- **primitive quandles** (that is, $\mathrm{Mlt_r(Q)}$ acts primitively on Q, not just transitively),

Towards proving Hayashi's conjecture

Hayashi's conjecture is true for:

- **primitive quandles** (that is, $\mathrm{Mlt_r(Q)}$ acts primitively on Q, not just transitively),
- affine quandles,

Towards proving Hayashi's conjecture

Hayashi's conjecture is true for:

- **primitive quandles** (that is, $\mathrm{Mlt_r(Q)}$ acts primitively on Q, not just transitively),
- affine quandles,
- whenever φ has at most three cycles [Watanabe],

Towards proving Hayashi's conjecture

Hayashi's conjecture is true for:

- **primitive quandles** (that is, $\mathrm{Mlt_r(Q)}$ acts primitively on Q, not just transitively),
- affine quandles,
- whenever φ has at most three cycles [Watanabe],
- whenever φ has at most five cycles [Lages-Lopes],

Towards proving Hayashi's conjecture

Hayashi's conjecture is true for:

- **primitive quandles** (that is, $\mathrm{Mlt_r(Q)}$ acts primitively on Q, not just transitively),
- affine quandles,
- whenever φ has at most three cycles [Watanabe],
- whenever φ has at most five cycles [Lages-Lopes],
- for connected quandles of order ≤ 47.

Outline

The isomorphism problem for magmas

Consider all magmas on a finite set X. Here is a naive approach to the classification of the magmas up to isomorphism:

The isomorphism problem for magmas

Consider all magmas on a finite set X. Here is a naive approach to the classification of the magmas up to isomorphism:

- The symmetric group S_X acts on the magmas via $f:(X,\cdot)\to(X,*)$, $x*y=f(f^{-1}(x)\cdot f^{-1}(y))$.

The isomorphism problem for magmas

Consider all magmas on a finite set X. Here is a naive approach to the classification of the magmas up to isomorphism:

- The symmetric group S_X acts on the magmas via $f : (X, \cdot) \to (X, *)$, $x * y = f(f^{-1}(x) \cdot f^{-1}(y))$.
- The orbits of this action are precisely the isomorphism types.

The isomorphism problem for magmas

Consider all magmas on a finite set X. Here is a naive approach to the classification of the magmas up to isomorphism:

- The symmetric group S_X acts on the magmas via $f:(X,\cdot)\to(X,*)$, $x*y=f(f^{-1}(x)\cdot f^{-1}(y))$.
- The orbits of this action are precisely the isomorphism types.
- The space it too large.

The isomorphism problem for magmas

Consider all magmas on a finite set X. Here is a naive approach to the classification of the magmas up to isomorphism:

- The symmetric group S_X acts on the magmas via $f : (X, \cdot) \to (X, *)$, $x * y = f(f^{-1}(x) \cdot f^{-1}(y))$.
- The orbits of this action are precisely the isomorphism types.
- The space it too large.
- Good news: The action restricts to the set of magmas in a given variety V.

The isomorphism problem for magmas

Consider all magmas on a finite set X. Here is a naive approach to the classification of the magmas up to isomorphism:

- The symmetric group S_X acts on the magmas via $f : (X, \cdot) \to (X, *)$, $x * y = f(f^{-1}(x) \cdot f^{-1}(y))$.
- The orbits of this action are precisely the isomorphism types.
- The space it too large.
- Good news: The action restricts to the set of magmas in a given variety V.
- Bad news: The space is typically still too large.

Partial magmas

A **partial magma** on X is a mapping $t : D \to X$, where $D \subseteq X \times X$ is the (partial) domain of t.

Partial magmas

A **partial magma** on X is a mapping $t : D \to X$, where $D \subseteq X \times X$ is the (partial) domain of t.

- The above action of S_X extends to partial magmas.

Partial magmas

A **partial magma** on X is a mapping $t : D \to X$, where $D \subseteq X \times X$ is the (partial) domain of t.

- The above action of S_X extends to partial magmas.
- The partial domain D changes to $D^f = \{(f(x), f(y)) : (x, y) \in D\}$.

Partial magmas

A **partial magma** on X is a mapping $t : D \to X$, where $D \subseteq X \times X$ is the (partial) domain of t.

- The above action of S_X extends to partial magmas.
- The partial domain D changes to $D^f = \{(f(x), f(y)) : (x, y) \in D\}$.
- Main idea: Built the magmas up by enlarging the partial domain in several steps.

Partial magmas

A **partial magma** on X is a mapping $t : D \to X$, where $D \subseteq X \times X$ is the (partial) domain of t.

- The above action of S_X extends to partial magmas.
- The partial domain D changes to $D^f = \{(f(x), f(y)) : (x, y) \in D\}$.
- Main idea: Built the magmas up by enlarging the partial domain in several steps.

Theorem

The only invariant domains under the action of S_X are the diagonal $\Delta = \{(x, x) : x \in X\}$ and its complement $(X \times X) \setminus \Delta$.

A funny result

Let V be any variety of magmas and let $n > 0$ be fixed.

A funny result

Let V be any variety of magmas and let $n > 0$ be fixed.
For $1 \leq i \leq n$, let $m_i(V)$ be the number of magmas of order n in V satisfying $1 * 1 = i$.

A funny result

Let V be any variety of magmas and let $n > 0$ be fixed.
For $1 \leq i \leq n$, let $m_i(V)$ be the number of magmas of order n in V satisfying $1 * 1 = i$.

Theorem

$m_2(V) = m_3(V) = \cdots = m_n(V)$. *(But $m_1(V) \neq m_2(V)$ in general.)*

Proof.

For $1 < i < j$, consider $f \in S_X$ such that $f(1) = 1$ and $f(i) = j$. $\square$

Mapping types

A partial magma $t : \Delta \to X \times X$ can be identified with the endofunction $x \mapsto t(x, x)$ of X.

Mapping types

A partial magma $t : \Delta \to X \times X$ can be identified with the endofunction $x \mapsto t(x,x)$ of X.

The orbits of S_X on the space of endofuctions are known as **mapping types**. These were first studied by Davis in 1953. In 1972, De Bruijn came up with a recursive (and hard to evaluate) formula for the number a_n of mapping types.

$$\begin{array}{rcrrrrrrrrr} n & = & 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ a_n & = & 1 & 3 & 7 & 19 & 47 & 130 & 343 & 961 & 2615 \end{array}$$

See the sequence OEIS A001372 for a_n with $n \leq 1000$.

Minimal representatives of endofunctions

Endofunctions on $X_n = \{1, \ldots, n\}$ can be ordered lexicographically.

Minimal representatives of endofunctions

Endofunctions on $X_n = \{1, \dots, n\}$ can be ordered lexicographically.

Theorem (Mitchell-M-V 2024)

There is an $O(n^2)$ algorithm that for a given endofunction t on X_n returns the minimal representative of the same mapping type as t.

Stratified group action

- We can therefore quickly find all possible diagonals up to isomorphism.

Stratified group action

- We can therefore quickly find all possible diagonals up to isomorphism.
- Bad news: For a given diagonal, the space might still be very large.

Stratified group action

- We can therefore quickly find all possible diagonals up to isomorphism.
- Bad news: For a given diagonal, the space might still be very large.
- Next idea: If the stabilizer H of the given diagonal (as a function) is large, there can be larger H-invariant domains, e.g., add the first column, then add the first row, etc.

Stratified group action

- We can therefore quickly find all possible diagonals up to isomorphism.
- Bad news: For a given diagonal, the space might still be very large.
- Next idea: If the stabilizer H of the given diagonal (as a function) is large, there can be larger H-invariant domains, e.g., add the first column, then add the first row, etc.
- This results in a stratified group action which can be controlled by the orbit-stabilizer theorem.

Stratified group action

- We can therefore quickly find all possible diagonals up to isomorphism.
- Bad news: For a given diagonal, the space might still be very large.
- Next idea: If the stabilizer H of the given diagonal (as a function) is large, there can be larger H-invariant domains, e.g., add the first column, then add the first row, etc.
- This results in a stratified group action which can be controlled by the orbit-stabilizer theorem.
- We tried this for the variety of right self-distributive magmas, that is, magmas satisfying $(xy)z = (xz)(yz)$.

Results of Ježek

Theorem (Ježek 1997)

The number of right self-distributive magmas of order n in absolute terms and up to isomorphism is

$$
\begin{array}{rcrrrrrr}
n & = & 1 & 2 & 3 & 4 & 5 & 6 \\
a_n & = & 1 & 9 & 224 & 14067 & 3717524 & 25488943921 \\
i_n & = & 1 & 6 & 48 & 720 & 33425 & 35527077^{*}
\end{array}
$$

Results of Ježek

Theorem (Ježek 1997)

The number of right self-distributive magmas of order n in absolute terms and up to isomorphism is

$$\begin{array}{rcrrrrrr} n & = & 1 & 2 & 3 & 4 & 5 & 6 \\ a_n & = & 1 & 9 & 224 & 14067 & 3717524 & 25488943921 \\ i_n & = & 1 & 6 & 48 & 720 & 33425 & 35527077^* \end{array}$$

- The entry i_6 was corrected by us [MV].
- With the stratified group action, the calculation takes 2 seconds for $n \le 5$, and a few minutes for $n = 6$.

The number of right self-distributive magmas of order 7

The problem of finding a_7 is very challenging.

The number of right self-distributive magmas of order 7

The problem of finding a_7 is very challenging.

- We considered 108404 orbits of partial domains.

The number of right self-distributive magmas of order 7

The problem of finding a_7 is very challenging.

- We considered 108404 orbits of partial domains.
- All but two orbits finished in about 10 days.

The number of right self-distributive magmas of order 7

The problem of finding a_7 is very challenging.

- We considered 108404 orbits of partial domains.
- All but two orbits finished in about 10 days.
- The diagonals 1111223 and 1111123 are trouble. We handled them interactively.

The number of right self-distributive magmas of order 7

The problem of finding a_7 is very challenging.

- We considered 108404 orbits of partial domains.
- All but two orbits finished in about 10 days.
- The diagonals 1111223 and 1111123 are trouble. We handled them interactively.

Theorem (MV)

There are $3,021,268,037,534,480$ *right self-distributive groupoids of order* 7*, counted absolutely.*

The number of right self-distributive magmas of order 7

The problem of finding a_7 is very challenging.

- We considered 108404 orbits of partial domains.
- All but two orbits finished in about 10 days.
- The diagonals 1111223 and 1111123 are trouble. We handled them interactively.

Theorem (MV)

There are $3,021,268,037,534,480$ right self-distributive groupoids of order 7, counted absolutely.

(Disclaimer: We are redoing the calculations to see if we get the same answer with different orbits.)