Enumerating small 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

AAA Warsaw, June 2014

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	269781831680661
9	9365022303540	1522473406143824732149 7
10	208904361959457696 17	2750892211809150446995735533513

(McKay, Meynert, Myrvold 2007)

Methods: smart combinatorics and efficient programming

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)*

Observe:

- *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 $\mathrm{LMlt}(Q) \leq \mathrm{Aut}(Q)$.

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)*

Observe:

- *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 $\mathrm{LMlt}(Q) \leq \mathrm{Aut}(Q)$.

Example: group conjugation $x * y = y^x = xyx^{-1}$

Motivation:

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

Enumerating quandles: elementary approach

1 1 3 7 22 73 298 1581 11079

- exhaustive search over all tables: Mace4 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: elementary approach

1 1 3 7 22 73 298 1581 11079

- exhaustive search over all tables: Mace4 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 by $\mathrm{LMlt}(Q)$
- find a representation theorem
- count the configurations

Our results: two special cases

- *algebraically connected quandles* = with a single orbit, up to size 35
- *medial quandles* (in a sense the abelian case), up to size 13

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

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..35	29	17	11	0	15					

(Vedramin 2012 / HSV independently)

We count all quandle envelopes, using the full list of transitive groups of degree $n \leq 35$ (Hulpke 2005).
Important trick: we have an efficient isomorphism theorem for envelopes.

Using deep 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 $2p$: 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.

Medial quandles

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

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

Example: *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.)

Medial quandles

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

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

Example: *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.

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)
- $\varphi_{j,k}(c_{i,j}) = \varphi_{k,k}(c_{i,k} - c_{j,k})$

sum of an affine mesh = disjoint union of A_i, for $a \in A_i$, $b \in A_j$

$$a * b = c_{i,j} + \varphi_{i,j}(a) + (1 - \varphi_{j,j})(b)$$

Theorem (JPSZ)

An algebra is a medial quandle if and only if it is the sum of an affine mesh.

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	20837449	
13	466087635	
14	1943042???	

We count all affine meshes, using an efficient isomorphism theorem.

Reductive medial quandles

Surprizingly, there is an important special case.

A medial quandle is called *2-reductive* if following equivalent cond's hold:

- $(x * y) * y = y$
- all compositions of right translations $R_u R_v$ are constant
- in the mesh representation, $\varphi_{i,j} = 0$ for every i, j

2-reductive medial quandles have very combinatorial character, they are merely just tables of numbers (operation $a * b = b + c_{i,j}$, no conditions upon $c_{i,j}$ except $c_{i,i} = 0$).

We count them by Burnside's theorem.

"Almost every" medial quandle is 2-reductive.

The numbers of non-2-reductive, and *non-n-reductive* (for any n) ones:

1	2	3	4	5	6	7	8	9	10	11	12	13	14
0	0	1	1	3	3	5	12	10	45	9	278	11	?
0	0	1	1	3	1	5	3	10	3	9	8	11	?

Enumerating assymptotically

Theorem (Blackburn 2013)

For every $c_1 < \frac{1}{4}$ *and every* $c_2 > \frac{1}{6}\log_2 24 + \frac{1}{2}\log_2 3 \approx 1.5566$

$$2^{c_1 n^2} < \textit{the number of quandles} < 2^{c_2 n^2}.$$

Lower bound: take $n/2$ copies of $\mathbb{Z}_2$, think about all $\frac{n}{2} \times \frac{n}{2}$ 0,1-matrices $(c_{i,j})$ with $c_{i,i} = 0$: there is $2^{\frac{1}{4}(n^2-n)}$ of them, hence at least

$$2^{\frac{1}{4}(n^2-n)}/n! = 2^{\frac{1}{4}n^2 - O(n\log n)}$$

isomorphism classes of 2-reductive (involutory) medial quandles

Upper bound: we can prove there is at most $2^{(\frac{1}{4}+o(1))n^2}$ 2-reductive m.q.

Conjecture

The upper bound (in medial case) is $c_2 = \frac{1}{4} + o(1)$.