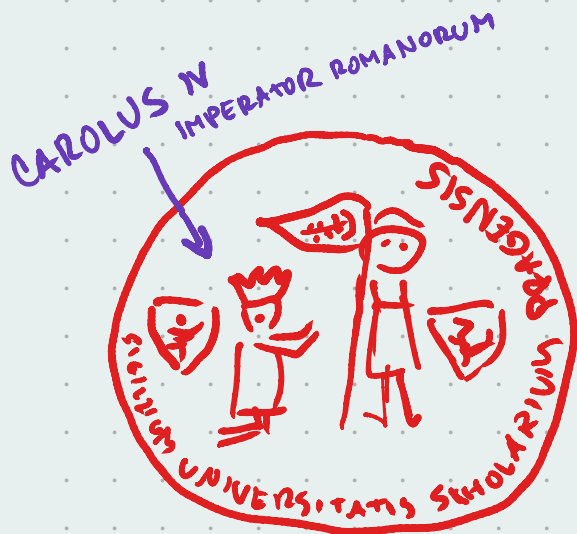


(REPRESENTATION &)

ENUMERATION OF QUANDLES

PART II

David Stanovsky
Charles University, Prague



AGTA 2025, Napoli



Thanks to my COAUTHORS :

- B Marco Bonatto (Ferrara)
- J Přemysl Jedlička (Praha)
- P Agata Pilitowska (Warsaw)
- V Petr Vojtěchovský (Denver)
- Z Anna Zamojska-Dzienio (Warsaw)

Part IIa : Medial quandles via affine meshes

Part IIb : Latin quandles via affine representation over loops

Part IIc : Central extensions

RACKS, QUANDLES & the associated groups

A rack is a binary algebra $Q = (Q, *)$ such that

all left translations $L_a: Q \rightarrow Q$
 $x \mapsto a * x$ are automorphisms of $(Q, *)$

(i.e., we have unique left division & the identity $x * (y * z) = (x * y) * (x * z)$)

A quandle is an idempotent rack. (i.e., $x * x = x$)

$$\text{LMet}(Q) := \langle L_x : x \in Q \rangle \trianglelefteq \text{Aut}(Q)$$

$$\text{Dis}(Q) := \langle L_x L_y^{-1} : x, y \in Q \rangle \trianglelefteq \text{LMet}(Q)$$

... since $a L_x a^{-1} = L_{a * x}$

Easy fact: the action of $\text{LMet}(Q)$ and $\text{Dis}(Q)$ on Q has the same orbits.

A rack is called connected if there is a single orbit.

A rack is called latin if the right translations are also bijective.
(i.e., a quasigroup)

RACKS, QUANDLES & the associated groups

A rack is a binary algebra $Q = (Q, *)$ such that
 all left translations $L_a: Q \rightarrow Q$ are automorphisms of $(Q, *)$
 $x \mapsto a * x$
 (i.e., we have unique left division & the identity $x * (y * z) = (x * y) * (x * z)$)

A quandle is an idempotent rack. (i.e., $x * x = x$.)

$$\text{LMet}(Q) := \langle L_x : x \in Q \rangle \trianglelefteq \text{Aut}(Q)$$

$$\text{Dis}(Q) := \langle L_x L_y^{-1} : x, y \in Q \rangle \trianglelefteq \text{LMet}(Q)$$

$$\dots \text{since } d L_x d^{-1} = L_{d(x)}$$

Easy fact: the action of $\text{LMet}(Q)$ and $\text{Dis}(Q)$ on Q has the same orbits.

A rack is called connected if there is a single orbit.

Example:

	a	b	c	1	2	3
a	a	c	b	3	2	1
b	c	b	a	2	1	3
c	b	a	c	1	3	2
1	b	a	c	1	3	2
2	a	c	b	3	2	1
3	c	b	a	2	1	3

... two orbits $\{a, b, c\}, \{1, 2, 3\}$

$$\dots \text{LMet}(Q) = \langle (bc)(13), (ac)(12), (ab)(23) \rangle$$

$$\dots \text{Dis}(Q) = \langle (abc)(123) \rangle$$

$$\uparrow \\ \cong A_3$$

$$\uparrow \\ \cong S_3$$

AFFINE QUANDLES

Let $(A, +)$ be an abelian group, $\varphi \in \text{Aut } A$.

$$\text{Aff}(A, \varphi) := (A, *) \quad \text{with} \quad x * y = (1 - \varphi)(x) + \varphi(y).$$

(alternative view: $\mathbb{Z}\langle t, t^{-1} \rangle$ -modules)

Example: previous slide $\simeq \text{Aff}(\mathbb{Z}_6, -1)$
($x * y = 2x - y$)

☹ $\text{Dis}(\mathbb{Q}) \simeq \text{Im}(1 - \varphi)$ is an abelian group

AFFINE QUANDLES

Let $(A, +)$ be an abelian group, $\varphi \in \text{Aut } A$.

$$\text{Aff}(A, \varphi) := (A, *) \text{ with } x * y = (1 - \varphi)(x) + \varphi(y).$$

Theorem [JPSZ 2018]: TFAE for a quandle Q :

(1) $Q \cong$ an affine quandle

(2) $\text{Dis}(Q)$ is abelian, acts semiregularly

$\forall g \neq \text{id}$ has no fixpoints

& ~~the~~ the multisets $\{L_a L_{a'}^{-1} : a \in T\}$ are balanced $\forall a, T$ ~~the~~
[see the paper]

A broader perspective: (Smith's) COMMUTATOR THEORY

An algebraic structure X is called abelian if

$$\forall \text{term } t \ \forall x, y \ \forall \bar{u}, \bar{v} \quad t(\underline{x}, \underline{\bar{u}}) = t(\underline{x}, \underline{\bar{v}}) \implies t(\underline{y}, \underline{\bar{u}}) = t(\underline{y}, \underline{\bar{v}})$$

Theorem [Gumm / Smith 1970s]:

Let X be a structure with a Maltsev polynomial.

$$m(x, y, y) = m(y, y, x) = x$$

Ex.: $m(x, y, z) = xy^{-1}z$
in grs.

Then X is abelian $\iff X$ is polynomially equivalent to a MODULE.

Theorem [JPSZ 2018]: TFAE for a quandle Q :

usually no Maltsev poly.

(1) Q is abelian

(2) $Q \iff$ an affine quandle

(3) $\text{Dis}(Q)$ is abelian, acts semiregularly

MEDIALITY

👁️ Q is affine $\Rightarrow Q$ satisfies
(or $Q \hookrightarrow$ affine)

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

Fun facts: • [Frink 1955] the abstract axiomatization of "weighted mean" should be latin medial quandles

• [Craus, Nelson 2014] $\text{Hom}(Q_1, Q_2)$ is a well defined quandle
 $\Leftrightarrow Q_2$ is medial
under $(f * g)(x) = f(x) * g(x)$

Lemma: Q is medial $\Leftrightarrow \text{Dis}(Q)$ is abelian

THE STRUCTURE OF MEDIAL QUANDLES

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

Idea: heterogeneous affine repre.

def: **AFFINE MESH** is $\mathcal{A} = ((A_i), (\varphi_{ij}), (c_{ij}))_{i,j \in I}$ such that

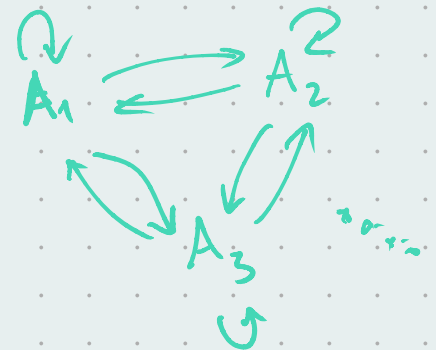
abelian groups $\uparrow$ $\uparrow$ $\uparrow$
 $\varphi_{ij}: A_i \rightarrow A_j$ group hom.
 $c_{ij} \in A_j$

(1) $1 - \varphi_{ii} \in \text{Aut}(A_i)$

(2) $c_{ii} = 0$

(3) $A_i \xrightarrow{\varphi_{ij}} A_j$
 $\downarrow \varphi_{ij} \quad \downarrow \varphi_{jk} \quad \text{commutes}$
 $A_j \xrightarrow{\varphi_{jk}} A_k$

(4) $\varphi_{jk}(c_{ij}) = \varphi_{ik}(c_{ij} - c_{jk})$



$\Rightarrow \mathcal{Q}(\mathcal{A}) = (\cup A_i, *)$ with $a * b = c_{ij} + \varphi_{ij}(a) + (1 - \varphi_{jj})(b)$



this is a medial quandle

THE STRUCTURE OF MEDIAL QUANDLES

def: **AFFINE MESH** is $\mathcal{A} = ((A_i), (\varphi_{ij}), (c_{ij}))_{i,j \in I}$ such that

abelian groups $\uparrow$ $\uparrow$ $\uparrow$
 $\varphi_{ij}: A_i \rightarrow A_j$ group hom.
 $c_{ij} \in A_j$

(1) $1 - \varphi_{ii} \in \text{Aut}(A_i)$

(2) $c_{ii} = 0$

(3) $A_i \xrightarrow{\varphi_{ij}} A_j$
 $\downarrow \varphi_{ij} \quad \downarrow \varphi_{jk} \quad \text{commutes}$
 $A_j \xrightarrow{\varphi_{jk}} A_k$

(4) $\varphi_{jk}(c_{ij}) = \varphi_{ik}(c_{ik} - c_{jk})$

$Q(\mathcal{A}) = (\cup A_i, *)$

with $a * b = c_{ij} + \varphi_{ij}(a) + (1 - \varphi_{jj}(b))$

👁 this is a medial quandle

Example:

	a	b	c	1	2	3
a	a	c	b	3	2	1
b	c	b	a	2	1	3
c	b	a	c	1	3	2
1	b	a	c	1	3	2
2	a	c	b	3	2	1
3	c	b	a	2	1	3

$\cong \text{Aff}(\mathbb{Z}_6, -1) = Q((\mathbb{Z}_6), (-1), (0))$

$\cong Q((\mathbb{Z}_3, \mathbb{Z}_3), \begin{pmatrix} 2 & 2 \\ 2 & 2 \end{pmatrix}, \begin{pmatrix} 0 & 2 \\ 1 & 0 \end{pmatrix})$

better: it reflects orbit decomposition

THE STRUCTURE OF MEDIAL QUANDLES

def: **AFFINE MESH** is $\mathcal{A} = ((A_i), (\varphi_{ij}), (c_{ij}))_{i,j \in I}$ such that

abelian groups $\uparrow$ $\uparrow$ $\uparrow$
 $\varphi_{ij}: A_i \rightarrow A_j$ group hom.
 $c_{ij} \in A_j$

(1) $1 - \varphi_{ii} \in \text{Aut}(A_i)$

(2) $c_{ii} = 0$

(3) $A_i \xrightarrow{\varphi_{ij}} A_j$
 $\downarrow \varphi_{ij} \quad \downarrow \varphi_{jk} \quad \text{commutes}$
 $A_j \xrightarrow{\varphi_{jk}} A_k$

(4) $\varphi_{jk}(c_{ij}) = \varphi_{ik}(c_{ik} - c_{jk})$

$Q(\mathcal{A}) = (\cup A_i, *)$

with $a * b = c_{ij} + \varphi_{ij}(a) + (1 - \varphi_{jj})(b)$

👁 this is a medial quandle

It is called indecomposable if $\forall j \quad A_j = \langle \bigcup_{i \in I} c_{ij} + \text{Im } \varphi_{ij} \rangle$

Theorem [JPS2 2015]:

A quandle Q is medial $\Leftrightarrow Q \cong Q(\mathcal{A})$ for some indec. affine mesh
 & the mesh reflects the orbit decomposition.

EXAMPLE: Medial quandles of order 4

1 orbit: $(\mathbb{Z}_2^2, (\varphi), (0))$ where $\varphi = \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}$

(Note: $\mathbb{Z}_4$ does not provide any example)

2 orbits: $((\mathbb{Z}_3, \mathbb{Z}_1), 0, \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix})$

$((\mathbb{Z}_2, \mathbb{Z}_2), 0, \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix})$

3 orbits: $((\mathbb{Z}_2, \mathbb{Z}_1, \mathbb{Z}_1), 0, \begin{pmatrix} 0 & 0 & 0 \\ 1 & c & 0 \\ 0 & 0 & 0 \end{pmatrix})$ $c = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$

4 orbits: $((\mathbb{Z}_1, \mathbb{Z}_1, \mathbb{Z}_1, \mathbb{Z}_1), 0, 0)$

$\leadsto$ 6 medial quandles of order 4

(really?)

ISOMORPHISM THEOREM

Theorem [JPS2 2015]:

$$Q(\mathcal{A}) \simeq Q(\mathcal{A}') \iff \exists \pi \in S_I \quad \exists \varphi_i : A_i \simeq A'_{\pi i} \quad \exists d_i \in A'_{\pi i}$$

such that

$$(1) \quad \begin{array}{ccc} A_i & \xrightarrow{\varphi_{ij}} & A_j \\ \downarrow \varphi_i & & \downarrow \varphi_j \\ A_{\pi i} & \xrightarrow{\varphi'_{ij}} & A'_{\pi j} \end{array}$$

$$(2) \quad \varphi_j(c_{ij}) = c'_{\pi i, \pi j} + \varphi'_{\pi i, \pi j}(d_i) - \varphi'_{\pi j, \pi j}(d_j)$$

$\leadsto$ ENUMERATION: fix tuple $(\underbrace{A_1, \dots, A_1}_{m_1}, \underbrace{A_2, \dots, A_2}_{m_2}, \dots, \underbrace{A_n, \dots, A_n}_{m_n})$

$\Downarrow$

action of $\prod_{j=1}^n (A_j \rtimes \text{Aut}(A_j)) \wr S_{n_j}$ on meshes over that tuple

of MEDIAL QUANDLES of order n UP TO $\simeq$

orbit counting + a few structural features

exhaustive search

$|Q| = 13 \rightarrow$

$|Q| = 15 \rightarrow$

1
1
3
6
18
58
251
1410
10311
98577
1246488
20837439
466087635
?
563753074951
?
...

$$\simeq 2^{n^2/4}$$

FUN FACT / ESSENTIAL OBSERVATION:

Nearly all of them have $(\varphi_{ij}) = 0$ (zero matrix)

def.: 2-REDUCTIVE

of medial quadrangles that are NOT 2-reductive:

0 6 1 1 3 3 5 12 10 45 9 268 11 ? 36 ?
 $\uparrow$ $\uparrow$
 $|Q|=13$ $|Q|=15$

Proposition: $\nexists$ AE for a medial quadrangle:

- (1) $\varphi_{ij} = 0 \quad \forall i, j$
- (2) it satisfies the identity $(x * y) * y = y$
- (3) $R_u \circ R_v$ is constant $\forall u, v$

much easier. iso. thm.

- group action
- orbit counting

} $\rightarrow$ enumeration up to $|Q|=16$
 30784745506212

Theorem [Ashford-Riordan 2017]:

of quandles up to $\cong$ is $\sim 2^{n^2/4}$ [in a precise sense, see Petr's talk]

Fact: 2-reductive medial quandles achieve lower bound:

Assume meshes over $(\underbrace{\mathbb{Z}_p, \dots, \mathbb{Z}_p}_m)$ with $(e_{ij}) = 0$.

There are $(p^{m-1} - 1)^m$ matrices (c_{ij}) with columns $\neq 0$.

At most $(pm)!$ are isomorphic.

Hence, for $p=2, m=n/2$, we obtain AT LEAST

$$\frac{(p^{m-1} - 1)^m}{(pm)!} \geq 2^{n^2/4 - n(1+\log n)} \text{ non-isomorphic medial quandles}$$

PART II b

Let $(Q, +)$ be a loop, $\varphi \in \text{Aut}(Q, +)$ such that $x \mapsto x - \varphi(x)$ is bijective.
(not necessarily commutative)

Define $x * y = x - \varphi(x) + \varphi(y)$.

Then $(Q, *)$ is an idempotent quasigroup,

called **AFFINE** over the loop $(Q, +)$,

denoted **Aff** (Q, φ) .

SEVERAL REPRESENTATION THEOREMS

Theorem [Toyoda / Bruck / Murdoch 1940s]:

A quasigroup Q is

medial & idempotent $\Leftrightarrow Q \cong \text{Aff}(A, \psi)$ for an **abelian group** A

aka latin medial quandle

Theorem [Belousov / Soubelin 1960s]:

A quasigroup Q is

(left & right) self-distributive $\Leftrightarrow Q \cong \text{Aff}(A, \psi)$ for a **commutative Moufang loop** A

aka both-sided quandle

Theorem [Belousov - Ono 1970s]:

A quasigroup Q is

left self-distributive $\Leftrightarrow Q \cong \text{Aff}(A, \psi)$ for a **B.O. loop** A

latin quandle

~~assoc.~~ $\leadsto$ $x + (y + (x + z))$
 $((x + y) + x) + z$

$\uparrow$

Isomorphism Theorem: For reasonably behaved loop (incl. CML)

$$\text{Aff}(A, \varphi) \cong \text{Aff}(B, \psi) \Leftrightarrow \exists \rho: A_1 \cong A_2 \text{ group iso.} \\ \text{such that } \psi = \rho \varphi \rho^{-1}.$$

→ enumeration method, provided:

- classification of the underlying loops A
- efficient handling of the conjugacy problem in $\text{Aut}(A)$

→ medial idempotent quasigroups: easy in principle

[Hou] formulas up to $|Q| = p^4$

latin quandles: hopeless (BO-loops hard)

both-sided quandles: doable

[JSV] the smallest unknown order is 729

The structure of COMMUTATIVE MOUFANG LOOPS

Theorem: A finite CML Q admits direct decomposition

$$Q \simeq A \times T$$

↑ ↑
abelian group nilpotent CML
 of order 3^k
 $3 + |A|$

→ only orders 3^k are interesting

[Kepka - Némec 1981] the smallest non-associative CML has 81 elements
there are two of them

there are 6 both-sided quandles of order 81

[Kepka - Némec 1981] there are six non-associative CML with 243 elements

[JSV 2017] there are 92 both-sided quandles of order 243

PART IIc

How to enumerate nilpotent structures, such as CMLs?

Via CENTRAL EXTENSIONS.

A broader perspective: (Smith's) COMMUTATOR THEORY

An algebraic structure X is called abelian if

$$\forall \text{term } t \ \forall x, y \ \forall \bar{u}, \bar{v} \quad t(\underline{x}, \bar{u}) = t(\underline{x}, \bar{v}) \implies t(\underline{y}, \bar{u}) = t(\underline{y}, \bar{v})$$

A congruence $\sim$ of X is called central if

$$\forall \text{term } t \ (\forall x \sim y) \ \forall \bar{u}, \bar{v} \quad t(\underline{x}, \bar{u}) = t(\underline{x}, \bar{v}) \implies t(\underline{y}, \bar{u}) = t(\underline{y}, \bar{v})$$

Theorem:

Let X be a structure with a Mal'tsev term, and $\sim$ a central congruence of X .

Then

$$X \cong F \wr_{\theta} A$$

for some abelian structure A over a group $(A, +)$
cocycle $\theta: F^2 \rightarrow A$
 $F = X/\sim$

binary op.:

$$(x, a) * (y, b) = (x * y, (a * b) + \theta_{x, y})$$

loops: A itself is an abelian group

quandles: A is an affine quandle

{BS 2021}

ENUMERATING CENTRAL EXTENSIONS

cocycle space: $C(F, A) = \{ \theta : F^2 \rightarrow A \}$

coboundary subspace: $B(F, A) = \langle \hat{\tau} : \tau : F \rightarrow A \rangle$

$$\hat{\tau}_{x,y} := \tau(x * y) - \tau(x) - \tau(y)$$

Fact: $\theta' = \theta + \hat{\tau} \Rightarrow$ extensions are isomorphic

$\leadsto$ consider the space $C(F, A) / B(F, A)$

Fact: $\theta'_{x,y} = \beta(\theta_{\alpha(x), \alpha(y)})$ for some $\alpha \in \text{Aut } F$, $\beta \in \text{Aut } A$

$\Rightarrow$ extensions are isomorphic

$\leadsto$ fairly efficient (although incomplete) isomorphism checking

APPLICATIONS :

- commutative Moufang loops up to 3^5
- nilpotent loops up to order 22 [Daly-Vojtěchovský 2015]
- can be adapted to racks & quandles, for example:

Theorem [BS] :

Connected racks are central extensions of connected quandles.

(Implemented by my student Pudlich, enumerated up to order ~ 40 .)

