Tomáš Nagy

Left distributive quasigroups of order 2^k

Left distributive structures

Definition.

Let Q be a set with binary operation $*$. The structure $(Q, *)$ is called:

- *left (self-)distributive*, if all left translations are automorphisms, i. e. for all $a, b \in Q$:

$$a * (b * c) = (a * b) * (a * c);$$

- *quandle* if it is a left distributive, idempotent left quasigroup;
- *medial*, if $(a * b) * (c * d) = (a * c) * (b * d)$ for all a, b, c, d;

Left distributive quasigroup = latin quandle.

Affine quandles

Let $A = (A, +)$ be an abelian group, $\phi \in Aut(A)$ and set

$$x * y = (1 - \phi)(x) + \phi(y).$$

Then, $(A, *)$ is a quandle, called *affine*, to be denoted by $Aff(A, \phi)$.

Theorem. [Toyoda, Bruck]

A left distributive quasigroup is affine if and only if it is medial.

- Affine quandle is a quasigroup iff $(1 - \phi) \in Aut(A)$.

Theorem. [Etinghof, Guralnik, Soloviev, 2001]

All left distributive quasigroups of order p and p^2 are affine.

Cores of Bol loops

Let $L = (Q, \cdot)$ be a Bol loop, and set

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

Then, $(Q, *)$ is a non-affine quandle, called the *core* of L.

- $(Q, *)$ is a quasigroup iff $(Q, \cdot)$ is uniquely 2-divisible.
- The smallest example is of size 15.
- There exists one of order pq (p, q odd primes, $p > q$) iff $q|p^2 - 1$ [Kinyon, G. Nagy, Vojtěchovský, 2017].

Non-affine left distributive quasigroups

Problem.

Determine all n such that there exists a non-affine left distributive quasigroup of order n

State of the art:

order	exists iff	reference
2^k	$k = 6$ or $k \geq 8$	N, 2019
p^k	$k \geq 3$	EGS, 2001; Bianco, Bonatto 2019
pq, $p > q$	$q \mid p^2 - 1$	KNV, 2017; Bonatto, 2019
$4n + 2$	(none)	Stein, 1957
$4p$	$p \equiv 1 \pmod 3$	Bonatto, 2019

(p, q odd primes)

Left distributive quasigroups not isotopic to a Bol loops

Problem. [Belousov]

Is there a left distributive quasigroup not isotopic to a Bol loop?

- First counterexample due to Onoi (1970), of order 2^{16}.
- Galkin's theory of representation of left distributive quasigroups over transitive groups shows that the smallest left distributive quasigroup not isotopic to a Bol loop has order 15.

Central extensions

Definition.

Let $(Q, *_Q)$ be a left distributive quasigroup, $(A, +, -, 0)$ an abelian group, $\phi, \psi \in Aut(A)$ and $\theta : Q \times Q \to A$.
Let us define an operation $*$ on $Q \times A$ by

$$(a, x) * (b, y) = (a *_Q b, \phi(x) + \psi(y) + \theta_{a,b}).$$

Then, $Q \times_{\phi,\psi,\theta} A = (Q \times A, *)$ is a quasigroup, we call it a *central extension* of Q by ϕ, ψ, θ.

Lemma.

The central extension $E = Q \times_{\phi,\psi,\theta} A$ is a left distributive quasigroup if and only if $\varphi + \psi = 1$, $\theta_{a,a} = 0$, and

$$\psi(\theta_{b,c}) + \theta_{a,b*c} = \psi(\theta_{a,c}) + \phi(\theta_{a,b}) + \theta_{a*b,a*c} \qquad \text{(LD)}$$

for every $a, b, c \in Q$. The extension E is medial if and only if, additionally,

$$\phi(\theta_{a,b}) + \psi(\theta_{c,d}) + \theta_{a*b,c*d} = \phi(\theta_{a,c}) + \psi(\theta_{b,d}) + \theta_{a*c,b*d} \qquad \text{(M)}$$

for every $a, b, c, d \in Q$.

Let $\phi = 1 - \psi$ be bijective. Cocycles satisfying (LD) form a subgroup of the direct power A^{Q^2}, to be denoted $\mathrm{Z}(Q, A, \psi)$.

Central extensions

Theorem. [Bonatto, Stanovský 2019]

Let Q be a left distributive quasigroup of prime power size. Then $Q \simeq F \times_{1-\psi,\psi,\theta} A$ for some left distributive quasigroup F with $|F| < |Q|$, an abelian group A and $\psi \in Aut(A)$ and $\theta \in \mathrm{Z}(Q, A, \psi)$.

Proof.

Left distributive quasigroups are nilpotent and hence $Q \simeq F \times_{1-\psi,\psi,\theta} A$ for some A, ψ, θ and $F \simeq Q/\zeta(Q)$.

Onoi rings

Definition.

We will say that an algebraical structure $\mathbf{A} = (A, +, \cdot, 0, \alpha)$ with two binary operations $+, \cdot$, a constant 0 and a mapping α is an *Onoi ring* if it satisfyes the following properties:

- $(A, +, \cdot, 0)$ is a ring;
- $a + a = 0$ for all $a \in A$,
- α is an automorphism of the ring $(A, +, \cdot, 0)$,
- $\alpha^2(a) + \alpha(a) + a = 0$ for all $a \in A$,
- $\alpha(a) \cdot b = a \cdot \alpha(b)$ for all $a, b \in A$.

- Each Onoi ring $\mathbf{O}$ has size 2^{2k}.
  - O is elementary abelian group with $a + a = 0$ (and hence of size 2^l), $\alpha^3 = id$ and $\alpha(a) \neq a, a \neq 0$ (hence α disjoint union of 3-cycles, therefore $|O| \equiv 1 \ (mod\ 3)$)

Let $O = \{0, 1, 2, 3\}$ and let us define the operations $+, \cdot$ by the following tables:

$+$	0	1	2	3
0	0	1	2	3
1	1	0	3	2
2	2	3	0	1
3	3	2	1	0

$\cdot$	0	1	2	3
0	0	0	0	0
1	0	1	3	2
2	0	3	2	1
3	0	2	1	3

Let us define α as the permutation $(1, 2, 3)$.

This is an Onoi ring.

Let $\mathbf{O}$ be an Onoi ring and $\sigma \in \Sigma_n$, we can construct an Onoi ring $\mathbf{O}^{\mathbf{n}}_{\sigma}$ where all operations are given componentwise and the multiplication is defined by
$(a_1, a_2, \ldots, a_n) \cdot_\sigma (b_1, b_2, \ldots, b_n) = (a_{\sigma(1)} \cdot b_1, a_{\sigma(2)} \cdot b_2, \ldots, a_{\sigma(n)} \cdot b_n)$.

Definition.

Let $\mathbf{O_1}, \mathbf{O_2}$ be two Onoi rings. A mapping $\mu : O_1^3 \to O_2$ is called *Onoi mapping* between O_1 and O_2 if it is trilinear (with respect to the additive ring) and the following three identities hold:

$$\mu \circ (\alpha \times \alpha \times \alpha) = \alpha \circ \mu,$$
$$\mu \circ (\alpha \times 1 \times 1) = \mu \circ (1 \times \alpha \times \alpha),$$
$$\mu \circ (1 \times \alpha \times 1) = \mu \circ (1 \times 1 \times \alpha).$$

Example: Let $\mathbf{O}$ be an Onoi ring and $\mu : O^3 \to O$ given by $\mu(a, b, c) = a \cdot (b \cdot c)$. Then, μ is an Onoi mapping.

Theorem.

Let $\mathbf{O_1}$ and $\mathbf{O_2}$ be Onoi rings and $\mu : O_1^3 \to O_2$ an Onoi mapping. Let us define

$$\theta_{a,b} = \mu(a, a+b, a+b)$$

for $a, b \in O_1$.
Then, $Aff(O_1, \alpha) \times_{\alpha^2,\alpha,\theta} (O_2, +)$ is a left distributive quasigroup. Moreover, it is affine if and only if the following two identities hold for all $a, b, c \in O_1$:

$$\mu(a, b, b) = \mu(b, a, a),$$

$$\mu(a, b, c) = \mu(a, c, b).$$

We will denote this quasigroup by $\mathbf{Q(O_1, O_2}, \mu)$.

Non-affine left distributive quasigroups

Example.

- Let $\mathbf{O}$ be an Onoi ring and $e \in O$ such that $e(ee) \neq 0$.
- Consider $\mathbf{O}_\sigma^\mathbf{k}$ and $k > 1$ where $\sigma \in \Sigma_k$ such that $\sigma(1) = 2$ and $\sigma(2) = 1$, and denote $e_i = (0, ..., 0, e, 0, ..., 0)$ where e appears at the position i.
- Define $\mu : O^3 \to O$ by $\mu(a, b, c) = a \cdot (b \cdot c)$ (clearly an Onoi mapping).
- It is easy to check that $\mu(e_1, e_1, e_2) = (0, e(ee), 0, \ldots, 0) \neq (0, \ldots, 0) = \mu(e_1, e_2, e_1)$
- Hence, $\mathbf{Q}(\mathbf{O}_\sigma^\mathbf{k}, \mathbf{O}_\sigma^\mathbf{k}, \mu)$ is a non-affine left distributive quasigroup.

Non-affine left distributive quasigroups

Example.

- Let $\mathbf{O}$ be an Onoi ring and $e \in O$ such that $e(ee) \neq 0$.
- Consider the mapping

$$\mu : O^2 \times O^2 \times O^2 \to O, \quad ((a,b),(c,d),(e,f)) \mapsto b \cdot (d \cdot e)$$

  (it is straightforward to check that this is an Onoi mapping).
- We have $\mu((0,e),(0,e),(e,0)) = e(ee)$, but $\mu((0,e),(e,0),(0,e)) = 0$.
- Hence, $\mathbf{Q}(\mathbf{O^2}, \mathbf{O}, \mu)$ is a non-affine left distributive quasigroup.

Proving nonexistence

Algorithm (k fixed):

for every $l \in \{2, \cdots, k-2\}$, for every abelian group A of order 2^l
  for every $\phi \in Aut(A)$ up to conjugacy such that $1 - \phi$ is bijective,
    for every latin quandle Q s.t. $|Q| = 2^{k-l}$,
      find a generating set Θ of the group $\mathrm{Z}(Q, A, \phi)$,
      if every $\theta \in \Theta$ satisfies the cocycle condition (M)
        then answer NO;
        else answer YES.

For $k = 7$ it reveals that there exists no non-affine left distributive quasigroup of size 2^7.

- This could be extended to enumeration algorithm, but the number of cocycles is too large even for $k = 6$.

Summary

Theorem. [N, 2019]

A non-affine left distributive quasigroup of order 2^k exists if and only $k = 6$ or $k \geq 8$.

Outline of the proof.

For existence:

- For orders $2^{4k}, k \geq 2$ use Slide 14;
- for orders 2^{6k}, $k \geq 1$ use Slide 15;
- for the remaining orders use the direct product with one of the 8-element affine left distributive quasigroups.

For non-existence:

- For orders $2^k, k \leq 5$ use RIG library of quandles;
- for order 2^7 use results of [BS, 2019]: every non-affine left distributive quasigroup can be represented as a central extension $Q \times_{1-\psi,\psi,\theta} A$. A computer search over all parameters Q, A, ψ, θ reveals that all central extensions of order 2^7 are affine.

Thank you for your attention!