Quasigroups and the Yang-Baxter equation

David Stanovský

Charles University, Prague, Czech Republic

Loops'19

Outline

1. The quantum Yang-Baxter equation

2. Left distributive quasigroups / latin quandles
(some new results since Loops'15)

3. Involutive quasigroup solutions / latin rumples
[Bonatto, Kinyon, S, Vojtěchovský, 2019]

4. Idempotent quasigroup solutions / latin ???les
(open problem)

The quantum Yang-Baxter equation

Consider

- a monoidal category $\mathcal{C}$
- an object X in $\mathcal{C}$
- $\sigma : X \otimes X \to X \otimes X$

Think about (Set, $\times$) and (Vect, $\otimes$).

The quantum Yang-Baxter equation for σ:

$$(\sigma \otimes I)(I \otimes \sigma)(\sigma \otimes I) = (I \otimes \sigma)(\sigma \otimes I)(I \otimes \sigma)$$

The quantum Yang-Baxter equation

Consider

- a monoidal category $\mathcal{C}$
- an object X in $\mathcal{C}$
- $\sigma : X \otimes X \to X \otimes X$

Think about (Set, $\times$) and (Vect, $\otimes$).

The quantum Yang-Baxter equation for σ:

$$(\sigma \otimes I)(I \otimes \sigma)(\sigma \otimes I) = (I \otimes \sigma)(\sigma \otimes I)(I \otimes \sigma)$$

- (Vect) matrix representation of braid groups
- (Vect) quantum physics
- (Set) knot invariants

Set is a special case of Vect: permutation matrices
Set to Vect: by linearization and deformation

Set-theoretical solutions of the Yang-Baxter equation

[Drinfeld 1990]

Let X be a set and $\sigma : X \times X \to X \times X$ a mapping, denote

$$\sigma(x, y) = (x * y, x \circ y).$$

Hence, we have *an algebra* $(X, *, \circ)$.

The set-theoretical quantum Yang-Baxter equation

$$(\sigma \times id)(id \times \sigma)(\sigma \times id) = (id \times \sigma)(\sigma \times id)(id \times \sigma)$$

Set-theoretical solutions of the Yang-Baxter equation

[Drinfeld 1990]

Let X be a set and $\sigma : X \times X \to X \times X$ a mapping, denote

$$\sigma(x, y) = (x * y, x \circ y).$$

Hence, we have *an algebra* $(X, *, \circ)$.

The set-theoretical quantum Yang-Baxter equation

$$(\sigma \times id)(id \times \sigma)(\sigma \times id) = (id \times \sigma)(\sigma \times id)(id \times \sigma)$$

is equivalent to three identities:

$$x * (y * z) = (x * y) * ((x \circ y) * z)$$
$$(z \circ y) \circ x = (z \circ (y * x)) \circ (y \circ x)$$
$$(x * y) \circ ((x \circ y) * z) = (x \circ (y * z)) * (y \circ z)$$

Examples

$\sigma(x,y) = (x * y, x \circ y)$ such that

$$x * (y * z) = (x * y) * ((x \circ y) * z)$$

$$(z \circ y) \circ x = (z \circ (y * x)) \circ (y \circ x)$$

$$(x * y) \circ ((x \circ y) * z) = (x \circ (y * z)) * (y \circ z)$$

$\sigma(x,y) = (y,x)$

$\sigma(x,y) = (x * y, 1)$ ... YBE = associativity of $*$ ... *monoids*

$\sigma(x,y) = (x * y, x)$ ... YBE = left self-distributivity ... *racks and quandles*

$\sigma(x,y) = (x \vee y, x \wedge y)$ on a lattice ... always satisfies YBE

Examples

$\sigma(x,y) = (x * y, x \circ y)$ such that

$$x * (y * z) = (x * y) * ((x \circ y) * z)$$
$$(z \circ y) \circ x = (z \circ (y * x)) \circ (y \circ x)$$
$$(x * y) \circ ((x \circ y) * z) = (x \circ (y * z)) * (y \circ z)$$

$\sigma(x,y) = (y,x)$

$\sigma(x,y) = (x * y, 1)$ ... YBE = associativity of $*$ ... *monoids*

$\sigma(x,y) = (x * y, x)$ ... YBE = left self-distributivity ... *racks and quandles*

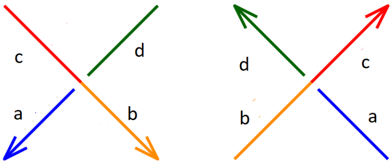
$\sigma(x,y) = (x \vee y, x \wedge y)$ on a lattice ... always satisfies YBE

Mostly interested in *non-degenerate solutions*:

$*$ is a left quasigroup, $\circ$ is a right quasigroup

Knot coloring

[Kauffman? early 2000s?]



Consider a set of colors C and a quaternary relation $R \subseteq C^4$.

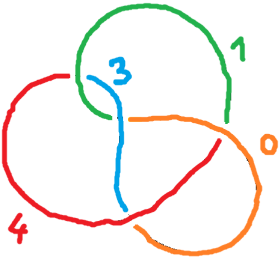
To every semi-arc, assign one of the colors from C.

For every crossing, demand

$$(col(a), col(b), col(c), col(d)) \in R$$

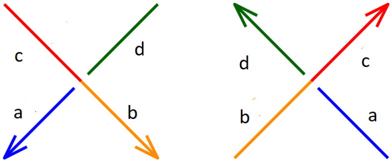
?? Invariant ??: count the number of admissible colorings

Knot coloring (example)



$$C = \{0, 1, 2, 3, 4\}, \quad R = \{(a, b, b, c) : a + b \equiv c \pmod 5\}$$

Knot coloring



Fact

Coloring by (C, R) is an invariant for knot/link equivalence if and only if R is a graph of an algebra $(C, *, \circ)$ such that it is

- III *a solution of the Yang-Baxter equation,*
- II *non-degenerate, σ bijective,*
- I *there is a permutation t on C s.t. $t(a) * a = a$ and $a \circ t(a) = t(a)$.*

Interesting classes of solutions of YBE

- *racks and quandles:* non-degenerate and $\sigma(x, y) = (x * y, x)$
- *involutive solutions:* non-degenerate and $\sigma^2 = id_{X \times X}$
- *idempotent solutions:* non-degenerate and $\sigma^2 = \sigma$

In all cases, $\circ$ is uniquely determined by $*$.

Interesting classes of solutions of YBE

- *racks and quandles:* non-degenerate and $\sigma(x,y)=(x*y,x)$
- *involutive solutions:* non-degenerate and $\sigma^2=id_{X\times X}$
- *idempotent solutions:* non-degenerate and $\sigma^2=\sigma$

In all cases, $\circ$ is uniquely determined by $*$.

After a boring calculation (replacing $*$ for $\backslash$, etc.), these are term-equivalent to a variety of left quasigroups axiomatized by a single identity:

- *racks and quandles:* $(x*y)*(x*z)=x*(y*z)$ [obvious]
- *involutive solutions:* $(x*y)*(x*z)=(y*x)*(y*z)$ [Rump]
- *idempotent solutions:* $(x*y)*(x*z)=(y*y)*(y*z)$

Yang-Baxter quasigroups

Definition

A quasigroup $(Q,*)$ is called *Yang-Baxter quasigroup*, if $(Q,\backslash,\circ)$ is a solution to YBE, for some operation $\circ$.

Examples:

- *latin quandles* = *left distributive quasigroups*:
  $$(x*y)*(x*z)=x*(y*z)$$
  extensively studied since 1950s (Stein, Belousov&co., Galkin, ...)
  [DS, *A guide to self-distributive quasigroups, or latin quandles*, 2015]
- *involutive solutions*: $(x*y)*(x*z)=(y*x)*(y*z)$
  [Bonatto, Kinyon, DS, Vojtěchovský, 2019]
- *idempotent solutions*: $(x*y)*(x*z)=(y*y)*(y*z)$
  to do

Problem: other interesting classes?

Intermezzo: definitions

Left multiplication group: $\mathrm{LMlt}(Q) = \langle L_a : \ a \in Q \rangle$

Displacement group: $\mathrm{Dis}(Q) = \langle L_a L_b^{-1} : \ a, b \in Q \rangle$

algebraically connected means $\mathrm{LMlt}(Q)$ transitive on Q
(quasigroups are algebraically connected)

Intermezzo: definitions

Left multiplication group: $\mathrm{LMlt}(Q) = \langle L_a : \ a \in Q \rangle$

Displacement group: $\mathrm{Dis}(Q) = \langle L_a L_b^{-1} : \ a, b \in Q \rangle$

algebraically connected means $\mathrm{LMlt}(Q)$ transitive on Q
(quasigroups are algebraically connected)

Affine quasigroups: A an abelian group, $\varphi, \psi \in \mathrm{Aut}(A)$, $c \in A$

$$\mathrm{Aff}(A, \varphi, \psi, c) = (A, *)$$
$$x * y = \varphi(x) + \psi(y) + c$$

Outline

1. The quantum Yang-Baxter equation
2. Left distributive quasigroups / latin quandles
3. Involutive quasigroup solutions / latin rumples
4. Idempotent quasigroup solutions / latin ???les

Left distributive quasigroups / latin quandles

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

i.e., $\mathrm{LMlt}(Q) \leq \mathrm{Aut}(Q)$
(hence latin quandles are homogeneous, unlike other YB quasigroups)

Examples:

- point reflection in euclidean geometry
- affine quasigroups $\mathrm{Aff}(A, 1-\varphi, \varphi, 0)$,
- $(A, 2x-y)$ for any uniquely 2-divisible Bruck loop
- ...
- embed into conjugation quandles
- non-affine examples of orders 15, 21, 27, 28, 33, 36, 39, 45, ...

Problem: Determine the existence spectrum of non-affine latin quandles.

[See the lecture by Tomáš Nagy.]

Coset construction

G group, $H \leq G$, $\psi \in \mathrm{Aut}(G)$ s.t. $\psi(a) = a$ for all $a \in H$ $\rightsquigarrow$

$\mathcal{Q}(G, H, \psi) = (G/H, *)$ with $aH * bH = a\psi(a^{-1}b)H$

Fact

- $\mathcal{Q}(G, H, \psi)$ *is a homogeneous quandle*
- *(in finite case)* $\mathcal{Q}(G, H, \psi)$ *is a quasigroup iff for every* $a, u \in G$

  $a\psi(a^{-1}) \in H^u \;\Rightarrow\; a \in H.$

Every connected quandle Q is isomorphic to $\mathcal{Q}(G, G_e, -^{L_e})$ with $G = \mathrm{LMlt}(Q)$, or $G = \mathrm{Dis}(Q)$ (minimal representation).

Canonical representation

Fix a set Q and an element e.

Quandle envelope $= (G, \zeta)$ where G is a transitive group on Q and $\zeta \in Z(G_e)$ such that $\langle \zeta^G \rangle = G$.

Theorem (Hulpke, S., Vojtěchovský, 2016)

The following are mutually inverse mappings:

$$\begin{aligned} \text{connected quandles} &\leftrightarrow \text{quandle envelopes} \\ (Q, *) &\rightarrow (\mathrm{LMlt}(Q, *), L_e) \\ \mathcal{Q}(G, G_e, -^\zeta) &\leftarrow (G, \zeta) \end{aligned}$$

(in finite case) (G, ζ) *corresponds to a latin quandle iff* $\zeta^{-1}\zeta^\alpha$ *has no fixed point for every* $\alpha \in G \setminus G_e$.

Hayashi's conjecture

Conjecture (Hayashi)

Let Q be a finite connected quandle.
In L_x, the length of every cycle divides the length of the longest cycle.

Hayashi's conjecture

Conjecture (Hayashi)

Let Q be a finite connected quandle.
In L_x, the length of every cycle divides the length of the longest cycle.

... use the canonical representation to translate the problem to groups:

Conjecture (Hayashi translated)

Let G be a transitive group over a finite set and $\zeta \in Z(G_e)$ such that $\langle \zeta^G \rangle = G$.
In ζ, the length of every cycle divides the length of the longest cycle.

Enumeration of latin quandles

n	1	2	3	4	5	6	7	8	9	10	11	12	13	14	**15**	16
non-aff(n)	0	0	0	0	0	0	0	0	0	0	0	0	0	0	**2**	0
aff(n)	1	0	1	1	3	0	5	2	8	0	9	1	11	0	3	9

n	17	18	19	20	**21**	22	23	24	25	26	**27**	**28**	29	30	31	32
non-aff(n)	0	0	0	0	**2**	0	0	0	0	0	**32**	**2**	0	0	0	0
aff(n)	15	0	17	3	5	0	21	2	34	0	30	5	27	0	29	8

	33	34	35	**36**	37	38	**39**	40	41	42	43	44	**45**	46	47
non-aff(n)	**2**	0	0	**1**	0	0	**2**	0	0	0	0	0	**12**	0	0
aff(n)	9	0	15	8	35	0	11	6	39	0	41	9	24	0	45

- none of order $4k+2$ [Stein 1957, Galkin 1979]
- non-aff(p)=non-aff(p^2)=0 [Etingof-Soloviev-Guralnick 2001, Graña 2004]
- non-aff($3p$)≥ 1 [Galkin 1981]
- non-aff(pq)$= 2$ if $q \mid p^2 - 1$, else $= 0$ [Bonatto 2019]

... various techniques, often translated to problems about finite permutation groups

Commutator theory for quandles

[Bonatto, S., 2019]

... adapt the general commutator theory of universal algebra to quandles

... abelianness, solvability, nilpotence for quandles

Commutator theory for quandles

[Bonatto, S., 2019]

... adapt the general commutator theory of universal algebra to quandles

... abelianness, solvability, nilpotence for quandles

abelian = "module-like" ($\neq$ commutative, $\neq$ medial)

... abelian groups = the only groups that can be considered as modules

Definition (JDH Smith 1970s)

An algebraic structure A is called abelian if the diagonal is a congruence block on A^2.
Equivalently, if

$$t(a, u_1, \ldots, u_n) = t(a, v_1, \ldots, v_n) \;\Rightarrow\; t(b, u_1, \ldots, u_n) = t(b, v_1, \ldots, v_n)$$

for every term operation $t(x, y_1, \ldots, y_n)$ and every a, b, u_i, v_i in A.

Abelian algebraic structures

Definition (JDH Smith 1970s)

An algebraic structure A is called abelian if

$$t(a, u_1, \dots, u_n) = t(a, v_1, \dots, v_n) \;\Rightarrow\; t(b, u_1, \dots, u_n) = t(b, v_1, \dots, v_n)$$

for every term operation $t(x, y_1, \dots, y_n)$ and every a, b, u_i, v_i in A.

Modules are abelian.
Proof: $t(x, y_1, \dots, y_n) = rx + \sum r_i y_i$, cancel ra, add rb.

An abelian group is commutative.
Proof: $t(x, y, z) = yxz, \quad a11 = 11a \;\Rightarrow\; ab1 = 1ba$

An abelian quandle is medial.
Proof: $t(x, y, u, v) = (xy)(uv)$,
$(yy)(uv) = (yu)(yv) \;\Rightarrow\; (xy)(uv) = (xu)(yv)$

Abelian algebras = modules, sometimes

polynomial operation = term operation with constants plugged in
A, B are *polynomially equivalent* = have the same polynomial operations

Mal'tsev operation: $m(x, y, y) = m(y, y, x) = x$

Theorem (Gumm-Smith 1970s)

TFAE for algebras with a Mal'tsev polynomial operation:

1. *abelian*
2. *polynomially equivalent to a module*

Examples: groups, loops, quasigroups

In particular, for latin quandles: abelian ⇔ medial ⇔ affine

Non-examples: quandles, monoids, semigroups

Quandles and abelianness

Theorem (Jedlička, Pilitowska, S., Zamojska-Dzienio 2018)

TFAE for a quandle Q:

1. *abelian*
2. *subquandle of an affine quandle*
3. $\mathrm{Dis}(Q)$ *abelian, semiregular*

Theorem (JPSZ 2018)

TFAE for a quandle Q:

1. *abelian and "balanced orbits"*
2. *affine*
3. $\mathrm{Dis}(Q)$ *abelian, semiregular and "balanced occurences of generators"*

Solvability and nilpotence

An algebraic structure A is solvable, resp. nilpotent, if there are congruences α_i such that

$$0_A = \alpha_0 \leq \alpha_1 \leq \ldots \leq \alpha_k = 1_A$$

and α_{i+1}/α_i is an abelian, resp. central congruence of A/α_i, for all i.

Need a good notion of *abelianness* and *centrality* for congruences.

Solvability and nilpotence

An algebraic structure A is solvable, resp. nilpotent, if there are congruences α_i such that

$$0_A = \alpha_0 \leq \alpha_1 \leq ... \leq \alpha_k = 1_A$$

and α_{i+1}/α_i is an abelian, resp. central congruence of A/α_i, for all i.

Need a good notion of *abelianness* and *centrality* for congruences.

Alternatively:

$$\alpha^{(0)} = \alpha_{(0)} = 1_A, \qquad \alpha_{(i+1)} = [\alpha_{(i)}, \alpha_{(i)}], \qquad \alpha^{(i+1)} = [\alpha^{(i)}, 1_A]$$

An algebraic structure A is

- solvable iff $\alpha_{(n)} = 0_A$ for some n
- nilpotent iff $\alpha^{(n)} = 0_A$ for some n

Need a good notion of *commutator of congruences*.

Commutator theory

[mid 1970s by Smith, Gumm, Herrmann, ..., the Freese-McKenzie 1987 book]

Centralizing relation for congruences α, β, δ of A:

$C(\alpha, \beta; \delta)$ iff for every term $t(x, y_1, \dots, y_n)$ and every $a \overset{\alpha}{\equiv} b$, $u_i \overset{\beta}{\equiv} v_i$

$$t(a, u_1, \dots, u_n) \overset{\delta}{\equiv} t(a, v_1, \dots, v_n) \;\Rightarrow\; t(b, u_1, \dots, u_n) \overset{\delta}{\equiv} t(b, v_1, \dots, v_n)$$

Commutator theory

[mid 1970s by Smith, Gumm, Herrmann, ..., the Freese-McKenzie 1987 book]

Centralizing relation for congruences α, β, δ of A:

$C(\alpha, \beta; \delta)$ iff for every term $t(x, y_1, \dots, y_n)$ and every $a \overset{\alpha}{\equiv} b$, $u_i \overset{\beta}{\equiv} v_i$

$$t(a, u_1, \dots, u_n) \overset{\delta}{\equiv} t(a, v_1, \dots, v_n) \;\Rightarrow\; t(b, u_1, \dots, u_n) \overset{\delta}{\equiv} t(b, v_1, \dots, v_n)$$

The *commutator* $[\alpha, \beta]$ is the smallest δ such that $C(\alpha, \beta; \delta)$.

A congruence α is called

- abelian if $C(\alpha, \alpha; 0_A)$, i.e., if $[\alpha, \alpha] = 0_A$.
- central if $C(\alpha, 1_A; 0_A)$, i.e., if $[\alpha, 1_A] = 0_A$.

Commutator theory

[mid 1970s by Smith, Gumm, Herrmann, ..., the Freese-McKenzie 1987 book]

Centralizing relation for congruences α, β, δ of A:

$C(\alpha, \beta; \delta)$ iff for every term $t(x, y_1, \ldots, y_n)$ and every $a \overset{\alpha}{\equiv} b$, $u_i \overset{\beta}{\equiv} v_i$

$$t(a, u_1, \ldots, u_n) \overset{\delta}{\equiv} t(a, v_1, \ldots, v_n) \ \Rightarrow\ t(b, u_1, \ldots, u_n) \overset{\delta}{\equiv} t(b, v_1, \ldots, v_n)$$

The *commutator* $[\alpha, \beta]$ is the smallest δ such that $C(\alpha, \beta; \delta)$.

A congruence α is called

- abelian if $C(\alpha, \alpha; 0_A)$, i.e., if $[\alpha, \alpha] = 0_A$.
- central if $C(\alpha, 1_A; 0_A)$, i.e., if $[\alpha, 1_A] = 0_A$.

Fact (not difficult, certainly not obvious)

In groups, this gives the usual commutator, abelianness, centrality.

Deep theory: works well in varieties with modular congruence lattices.

Commutator theory for quandles

Let $N(Q) = \{N \leq \mathrm{Dis}(Q) : N \text{ is normal in } \mathrm{LMlt}(Q)\}$

There is a Galois correspondence

$$Con(Q) \longleftrightarrow N(Q)$$

$$\alpha \to \mathrm{Dis}_\alpha(Q) = \langle L_x L_y^{-1} : x\,\alpha\,y \rangle$$

$$\alpha_N = \{(x,y) : L_x L_y^{-1} \in N\} \leftarrow N$$

Commutator theory for quandles

Let $N(Q) = \{N \leq \mathrm{Dis}(Q) : N \text{ is normal in } \mathrm{LMlt}(Q)\}$

There is a Galois correspondence

$$Con(Q) \longleftrightarrow N(Q)$$
$$\alpha \to \mathrm{Dis}_\alpha(Q) = \langle L_x L_y^{-1} : x \,\alpha\, y\rangle$$
$$\alpha_N = \{(x,y) : L_x L_y^{-1} \in N\} \leftarrow N$$

Proposition (BS)

TFAE for $\alpha, \beta \in Con(Q)$, Q a quandle:

1. *α centralizes β over 0_Q, i.e., $C(\alpha, \beta; 0_Q)$*
2. *$\mathrm{Dis}_\beta(Q)$ centralizes $\mathrm{Dis}_\alpha(Q)$ and acts α-semiregularly on Q*

α-semiregularly means $g(a) = a \;\Rightarrow\; g(b) = b$ for every $b \overset{\alpha}{\equiv} a$

Abelian and central congruences

Corollary

TFAE for a congruence α of a quandle Q:

1. α *is abelian*
2. $\mathrm{Dis}_\alpha(Q)$ *is abelian and acts α-semiregularly*

Corollary

TFAE for a congruence α of a quandle Q:

1. α *is central*
2. $\mathrm{Dis}_\alpha(Q)$ *is central and* $\mathrm{Dis}(Q)$ *acts α-semiregularly*

If Q has certain transitivity conditions (e.g., if latin), then this is iff

- *Q is a central extension of $F = Q/\alpha$, i.e., $(F \times A, *)$ with*
$$(x, a) * (y, b) = (xy,\ (1 - f)(a) + f(b) + \theta_{x,y})$$
where A is an abelian group, $\theta : Q^2 \to A$ satisfying the quandle cocycle condition.

Abelian, nilpotent, and solvable quandles

Theorem (JPSZ, BS)

quandle		$\mathrm{Dis}(Q)$
affine	$\Leftrightarrow$	*abelian, semiregular, "balanced"*
$\Downarrow$		$\Downarrow$
abelian	$\Leftrightarrow$	*abelian, semiregular*
$\Downarrow$		$\Downarrow$
nilpotent	$\Leftrightarrow$	*nilpotent*
$\Downarrow$		$\Downarrow$
solvable	$\Leftrightarrow$	*solvable*

Moreover, for finite connected faithful quandles (latin in particular):
nilpotent $\Leftrightarrow$ *direct product of connected quandles of prime power size.*

Latin quandles are solvable

Theorem (A. Stein 2001)

If Q is a finite latin quandle, then $\mathrm{LMlt}(Q)$ is solvable.

Corollary

Finite latin quandles are solvable.

Application: enumeration of quandles

Corollary (S. Stein 1957)

No latin quandles of order $\equiv 2 \pmod 4$

Proof:

- it is not simple:
  solvable simple $\Rightarrow$ abelian $\Rightarrow$ affine $\Rightarrow$ of order p^k by [Joyce 1982]
- take the smallest counterexample Q, consider a non-trivial congruence with blocks of size m, quotient of size n
- $|Q| = mn$, hence m or n is $\equiv 2 \pmod 4$, hence either a block, or the quotient, is a smaller counterexample

Application: coloring knots by latin quandles

Theorem (Bae 2012)

Knots with trivial Alexander polynomial are not colorable by any affine quandle.

Corollary

Knots with trivial Alexander polynomial are not colorable by any latin quandle.

Proof:

- let c be a non-trivial coloring
- consider the subquandle S generated by $Im(c)$; it is also solvable
- the knot is colorable by every simple factor of S (easy to see)
- however, simple factors of a solvable quandle are abelian, hence affine, contradiction

Application: Bruck loops of odd order are solvable

Recall from Loops'15: [S, Vojtěchovský 2014]

solvability in the sense of Bruck $\neq$ solvability in the sense of Smith

Theorem (Glauberman 1964/68)

Bruck loops of odd order are

1. *solvable in the sense of Bruck.*
2. *nilpotent iff direct product of Bruck loops of prime power order.*

Theorem

Bruck loops of odd order are solvable in the sense of Smith.

Proof:

- latin quandles are solvable
- involutory latin quandles are polynomially equivalent to Bruck loops of odd order [Kikkawa-Robinson]
- polynomial equivalence preserves commutator properties

Also, (2) is a direct consequence of our theorem for quandles.

Outline

1. The quantum Yang-Baxter equation
2. Left distributive quasigroups / latin quandles
3. Involutive quasigroup solutions / latin rumples
4. Idempotent quasigroup solutions / latin ???les

Involutive quasigroup solutions / latin rumples

[Bonatto, Kinyon, S, Vojtěchovský, 2019]

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

Examples:

	0	1	2	3
0	0	1	3	2
1	2	3	1	0
2	1	0	2	3
3	3	2	0	1

	0	1	2	3
0	1	3	0	2
1	0	2	1	3
2	2	0	3	1
3	3	1	2	0

Involutive quasigroup solutions / latin rumples

[Bonatto, Kinyon, S, Vojtěchovský, 2019]

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

Examples:

	0	1	2	3
0	0	1	3	2
1	2	3	1	0
2	1	0	2	3
3	3	2	0	1

	0	1	2	3
0	1	3	0	2
1	0	2	1	3
2	2	0	3	1
3	3	1	2	0

... are surprizingly HARD TO FIND !

- brute force (order ≤ 10) finds nothing else
- no "natural" examples (yet?)
- no "canonical representation" (yet?)
- even affine examples not easy to find

Affine latin rumples

Observation: $\mathrm{Aff}(A,\varphi,\psi,c)$ is involutive solution iff $[\varphi,\psi]=\varphi^2$

Example: $\mathrm{Aff}\left(\mathbb{Z}_2^2, \left(\begin{smallmatrix}0&1\\1&0\end{smallmatrix}\right), \left(\begin{smallmatrix}1&0\\1&1\end{smallmatrix}\right), \left(\begin{smallmatrix}0\\0\end{smallmatrix}\right)\right)$, $\mathrm{Aff}\left(\mathbb{Z}_2^2, \left(\begin{smallmatrix}0&1\\1&0\end{smallmatrix}\right), \left(\begin{smallmatrix}1&0\\1&1\end{smallmatrix}\right), \left(\begin{smallmatrix}1\\0\end{smallmatrix}\right)\right)$

Observation:

- $[\varphi,\psi]=\varphi^2$ iff $[\psi^{-1},\varphi]=1$
- if A is cyclic, there is no such φ,ψ (automorphisms commute)
- if $A=\mathbb{Z}_p^n$ then $p \mid n$ (calculate the trace: $0=n$)

Affine latin rumples

Observation: $\mathrm{Aff}(A,\varphi,\psi,c)$ is involutive solution iff $[\varphi,\psi]=\varphi^2$

Example: $\mathrm{Aff}\left(\mathbb{Z}_2^2, \left(\begin{smallmatrix}0&1\\1&0\end{smallmatrix}\right), \left(\begin{smallmatrix}1&0\\1&1\end{smallmatrix}\right), \left(\begin{smallmatrix}0\\0\end{smallmatrix}\right)\right)$, $\mathrm{Aff}\left(\mathbb{Z}_2^2, \left(\begin{smallmatrix}0&1\\1&0\end{smallmatrix}\right), \left(\begin{smallmatrix}1&0\\1&1\end{smallmatrix}\right), \left(\begin{smallmatrix}1\\0\end{smallmatrix}\right)\right)$

Observation:

- $[\varphi,\psi]=\varphi^2$ iff $[\psi^{-1},\varphi]=1$
- if A is cyclic, there is no such φ,ψ (automorphisms commute)
- if $A=\mathbb{Z}_p^n$ then $p \mid n$ (calculate the trace: $0=n$)

Theorem (BKSV)

A finite latin rumple of order $n=p_1^{n_1}\cdots p_r^{n_r}$ exists if and only $p_i \mid n_i$ $\forall i$.

Idea of the proof:

- only prime powers are interesting
- find an example of order p^p for every p, and use direct products
- inductively, factor out the subgroup pA to get a smaller counterexample

Nilpotent latin rumples

Central extension: given an abelian group A, a quasigroup Q, $\phi, \psi \in \mathrm{Aut}(A)$, $\theta : Q^2 \to A$

$$(Q \times A, *), \qquad (x, a) * (y, b) = (x * y, \phi(a) + \psi(b) + \theta(x, y))$$

If Q is a latin rumple and $[\phi, \psi] = \phi^2$, then we obtain a rumple iff

$$\phi(\theta(x, y) - \theta(y, x)) + \psi(\theta(x, z) - \theta(y, z)) = \theta(y * x, y * z) - \theta(x * y, x * z)$$

Nilpotent latin rumples

Central extension: given an abelian group A, a quasigroup Q, $\phi, \psi \in \mathrm{Aut}(A)$, $\theta : Q^2 \to A$

$$(Q \times A, *), \qquad (x,a) * (y,b) = (x * y, \phi(a) + \psi(b) + \theta(x,y))$$

If Q is a latin rumple and $[\phi, \psi] = \phi^2$, then we obtain a rumple iff

$$\phi(\theta(x,y) - \theta(y,x)) + \psi(\theta(x,z) - \theta(y,z)) = \theta(y * x, y * z) - \theta(x * y, x * z)$$

Computer calculation of cocycles:

- solving a system of linear equations for $\theta(x,y)$ over A (e.g., $= \mathbb{Z}_p^k$)
- affine solutions must be removed
- (tricky part: filtering up to isomorphism)

Enumeration / examples of latin rumples

Affine:

- order 2^2 ... 2, both over $\mathbb{Z}_2^2$
- order 2^4 ... 14, all over $\mathbb{Z}_2^4$
- order 2^6 ... many, over $\mathbb{Z}_2^6$ or $\mathbb{Z}_4^2 \times \mathbb{Z}_2^2$
- order 3^3 ... 6, all over $\mathbb{Z}_3^3$

Non-affine, nilpotent:

- several of order 2^4, with various displacement groups
- an example of order 2^6 not isotopic to a group,
- an example of order $108 = 2^2 3^3$ with non-nilpotent displacement gp
- ...

Enumeration / examples of latin rumples

Affine:

- order 2^2 … 2, both over $\mathbb{Z}_2^2$
- order 2^4 … 14, all over $\mathbb{Z}_2^4$
- order 2^6 … many, over $\mathbb{Z}_2^6$ or $\mathbb{Z}_4^2 \times \mathbb{Z}_2^2$
- order 3^3 … 6, all over $\mathbb{Z}_3^3$

Non-affine, nilpotent:

- several of order 2^4, with various displacement groups
- an example of order 2^6 not isotopic to a group,
- an example of order $108 = 2^2 3^3$ with non-nilpotent displacement gp
- …

A bit of good news: [Etingof, Schedler, Soloviev, 1999]
the displacement group is always solvable (in finite case)

Problems

Open problems:

- simple constructions!
- find non-nilpotent (non-solvable?) examples
- determine existence spectrum for non-affine
- commutator theory, relate nilpotence / solvability of Q and $\mathrm{Dis}(Q)$
- describe simple latin rumples
- ...

Outline

1. The quantum Yang-Baxter equation
2. Left distributive quasigroups / latin quandles
3. Involutive quasigroup solutions / latin rumples
4. Idempotent quasigroup solutions / latin ???les

Idempotent quasigroup solutions

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

Examples:

- $(A, -)$ for any abelian group
- $\mathrm{Aff}(A, \varphi, \psi, c)$ if and only if $\varphi = -\psi$
- non-affine examples of order 6

Open problems: everything (spectrum, examples, enumeration, structure theory, ...)

Things to remember

- finite group theory is a strong tool
  (BUT, give your group-theoretical friend a quizz: If G is a transitive group over a finite set, and $\zeta \in Z(G_e)$ such that $\langle \zeta^G \rangle = G$, prove that in ζ, the length of every cycle divides the length of the longest cycle.)
- commutator theory of universal algebra is a strong tool, too
  (and offers a different definition of solvability for loops)
- understanding latin / connected rumples ($xy \cdot xz = yx \cdot yz$) seems to be a major challenge
- study Yang-Baxter quasigroups! (i.e., $(Q, \backslash, \circ)$ is a solution to YBE)

Thank you for your attention!