

Self-distributive quasigroups and quandles II

David Stanovský

Charles University, Prague, Czech Republic

Kazakh-British Technical University, Almaty, Kazakhstan

stanovsk@karlin.mff.cuni.cz

June 2015

Outline

1. Motivation: Where self-distributivity comes from
2. Medial, trimedial and distributive quasigroups
 - 2a. affine representation in general
 - 2b. representation of distributive and trimedial quasigroups over commutative Moufang loops
 - 2c. the structure of distributive quasigroups
3. Left distributive quasigroups (and quandles)
 - 3a. (almost) linear representation
 - 3b. homogeneous representation
 - 3c. the structure of left distributive quasigroups
4. Applications in knot theory

Recap

Quasigroups \leftrightarrow loops

quasigroups \longleftrightarrow loops

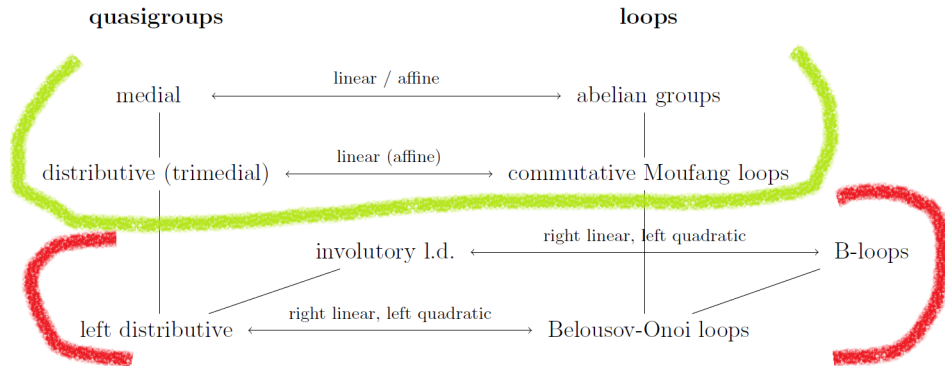
$(Q, *) \longleftrightarrow (Q, \cdot)$

- $x \cdot y = (x/e_1) * (e_2 \setminus y)$
- $x * y = \varphi(x) \cdot \psi(y)$

We can recover the quasigroup with $\varphi = R_{e_1}$, $\psi = L_{e_2}$.

Best case: both φ, ψ are linear / affine over (Q, \cdot) . Then, $(Q, *)$ is polynomially equivalent to a “*non-associative module*”.

An outline of the representation theorems



2c. The structure of distributive quasigroups

Recap

Distributive quasigroups are essentially the same objects as

- commutative Moufang loops with a 1-nuclear automorphism
- “1-nuclear commutative Moufang modules” over the ring of Laurent polynomials $\mathbb{Z}[t, t^{-1}]$

Idea: use known properties of commutative Moufang loops to reason about distributive quasigroups

Decomposition theorem

Theorem (Fischer-Smith)

Let Q be a finite distributive quasigroup of order $p_1^{k_1} \cdot \dots \cdot p_n^{k_n}$. Then

$$Q \simeq Q_1 \times \dots \times Q_n$$

where $|Q_i| = p_i^{k_i}$. Moreover, if Q_i is not medial, then $p_i = 3$ and $k_i \geq 4$.

... an analogy holds for commutative Moufang loops

Enumeration

$MI(n)$ = the number of medial idempotent quasigroups of order n up to isomorphism

$D(n)$ = the number of distributive quasigroups of order n up to isomorphism

Fisher-Smith says: with $p_i \neq 3$ pairwise different,

$$D(3^k \cdot p_1^{k_1} \cdot \dots \cdot p_n^{k_n}) = D(3^k) \cdot MI(p_1^{k_1}) \cdot \dots \cdot MI(p_n^{k_n}).$$

Moreover, $D(3^k) = MI(3^k)$ for $k < 4$.

Enumeration

Let $\mathcal{Q}(Q, \psi)$ denote the quasigroup $(Q, *)$ with $x * y = (1 - \psi)(x) + \psi(y)$.

Yesterday's theorems:

- $\mathcal{Q}(Q, \psi)$ is medial iff (Q, \cdot) is an abelian group
- $\mathcal{Q}(Q, \psi)$ is distributive iff (Q, \cdot) is a commutative Moufang loop and ψ is 1-nuclear

Lemma (Kepka-Němec)

Let (Q_1, \cdot) , (Q_2, \cdot) be commutative Moufang loops, ψ_1, ψ_2 their 1-nuclear automorphisms. TFAE:

- $\mathcal{Q}(Q_1, \psi_1) \simeq \mathcal{Q}(Q_2, \psi_2)$
- there is a loop isomorphism $\rho : Q_1 \simeq Q_2$ such that $\psi_2 = \rho\psi_1\rho^{-1}$

Enumeration

Recall:

- $G_1 = (\mathbb{Z}_3)^4$ and $G_2 = (\mathbb{Z}_3)^2 \times \mathbb{Z}_9$
- $Q_i = (G_i, \cdot)$ with $x \cdot y = x + y + t_i(x, y, x - y)$

Distributive quasigroups of order 81 (Kepka-Němec 1981):

- 1 $Q(G_1, \psi)$ with $\psi(y) = y^{-1}$
- 2 $Q(G_1, \psi)$ with $\varphi(x) = (x_2 - x_1)e_1 - x_2e_2 - x_3e_3 - x_4e_4$ and $\psi = 1 - \varphi$
- 3 $Q(G_2, \psi)$ with $\psi(y) = \sqrt{y}$
- 4 $Q(G_2, \psi)$ with $\psi(y) = y^2$
- 5 $Q(G_2, \psi)$ with $\psi(y) = y^{-1}$
- 6 $Q(G_2, \psi)$ with $\varphi(x) = -x_1e_1 - x_2e_2 - (3x_1 + x_3)e_3$ and $\psi = 1 - \varphi$

Enumeration

Theorem (Hou 2012)

- $MI(p) = p - 2$
- $MI(p^2) = 2p^2 - 3p - 1$
- $MI(p^3) = 3p^3 - 6p^2 + p$
- $MI(p^4) = 5p^4 - 9p^3 + p^2 - 2p + 1$

n	3	3^2	3^3	3^4	3^5	3^6
$CML^*(n)$	0	0	0	2	6	≥ 8
$3M^*(n)$	0	0	0	35		
$D^*(n)$	0	0	0	6		
$DS^*(n)$	0	0	0	1	1	3
$MI(n)$	1	8	30	166		

Here $X^*(n) = X(n) - MI(n)$.

3a. Loop isotopes of left distributive quasigroups

(Belousov-Onoi 1972)

Linear representation?

Let (Q, \cdot) be a left distributive quasigroup.

Let $x * y = (x/e) * (e \setminus y)$ with a carefully chosen e .

Is $(Q, *)$ a nice kind of a loop? Is (Q, \cdot) linear over it?

Linear representation?

Let (Q, \cdot) be a left distributive quasigroup.

Let $x * y = (x/e) * (e \setminus y)$ with a carefully chosen e .

Is $(Q, *)$ a nice kind of a loop? Is (Q, \cdot) linear over it?

Bad news: not really in general

Good news: it is nice in some special cases (distributive, involutory)

Good news: L_e is linear, R_e is quadratic over (Q, \cdot)

Belousov-Onoi modules

Let (Q, \cdot) be a loop and ψ its automorphism.

(Q, \cdot, ψ) is a *Belousov-Onoi module* if

$$\varphi(ab) \cdot \psi(ac) = a \cdot \varphi(b)\psi(c)$$

where $\varphi(x) = x/\psi(x)$ is the *companion mapping* for ψ .

(the companion is defined in order to have $x * x = \varphi(x) \cdot \psi(x) = x$)

Examples:

- 1 loop $(Q, \cdot) \longrightarrow$ BO-module (Q, \cdot, id)
- 2 group (Q, \cdot) with an automorphism $\psi \longrightarrow$ BO-module (Q, \cdot, ψ)
- 3 Bruck loop $(Q, \cdot) \longrightarrow$ BO-module $(Q, \cdot, {}^{-1})$

From Belousov-Onoi modules to self-distributive objects

Fact

Let (Q, \cdot, ψ) be a Belousov-Onoi module. Define

$$a * b = \varphi(a) \cdot \psi(b).$$

Then $(Q, *)$ is a quandle. It is a quasigroup iff φ is a permutation.

Examples:

- 1 loop (Q, \cdot) \longrightarrow BO-module (Q, \cdot, id)
 \longrightarrow quandle with $a * b = b$.
- 2 group (Q, \cdot) with an automorphism ψ \longrightarrow BO-module (Q, \cdot, ψ)
 \longrightarrow homogeneous quandle with $a * b = a\psi(a^{-1}b)$.
- 3 Bruck loop (Q, \cdot) \longrightarrow BO-module $(Q, \cdot, {}^{-1})$
 \longrightarrow involutory quandle with $a * b = a^2b^{-1}$ (core).

We shall see that all involutory left distributive quasigroups result as in (3).

From left distributive quasigroups to Belousov-Onoi loops

Belousov-Onoi loop = there is an automorphism ψ such that (Q, \cdot, ψ) is a Belousov-Onoi-module and *the companion* φ is a permutation.

Fact

Let $(Q, *)$ be a left distributive quasigroup, $e \in Q$ and let

$$a \cdot b = (a/e) * (e \setminus b).$$

Then (Q, \cdot) is a Belousov-Onoi loop with respect to $\psi = L_e$.

Moreover, different choices of e result in isomorphic loops.

Bad news: φ is usually not an automorphism. It is so iff (Q, \cdot) is commutative Moufang.

Good news: $\varphi(x) = x/\psi(x)$ can be considered *quadratic* over (Q, \cdot, ψ) .

Good news: $(Q, *)$ is **polynomially equivalent** to the BO-module (Q, \cdot, ψ)

Left distributive quasigroups = Belousov-Onoi loops

Theorem (Belousov-Onoi, 1972)

*The following are equivalent for a quasigroup $(Q, *)$:*

- 1 *it is left distributive,*
- 2 *it is right linear over a Belousov-Onoi loop.*

Left distributive quasigroups = Belousov-Onoi loops

The smallest non-associative Belousov-Onoi loops have order 15.

1. uniquely 2-divisible Bruck loop

Consider the loop $(\mathbb{Z}_5 \times \mathbb{Z}_3, \cdot)$ with $(a, x) \cdot (b, y) = (\varphi_{x,y}a + b, x + y)$

$\varphi_{x,y}$	0	1	2
0	1	2	2
1	1	3	1
2	1	1	3

2. a non-Bol loop

Consider the loop $(\mathbb{Z}_5 \times \mathbb{Z}_3, \cdot)$ with $(a, x) \cdot (b, y) = (\varphi_{x,y}a + b + \theta_{x,y}, x + y)$

$\theta_{x,y}$	0	1	2
0	0	0	0
1	0	-1	1
2	0	-2	2

This is a BO-loop with respect to the automorphism

$(a, x) \mapsto (-a + \delta_{x,2}, -x)$ where $\delta_{x,y} = 1$ if $x = y$ and $\delta_{x,y} = 0$ otherwise.

Left distributive quasigroups = Belousov-Onoi loops

Hence, the smallest non-medial left distributive quasigroups have order 15.

1. that uniquely 2-divisible Bruck loop

The corresponding quasigroup is $(Q, *)$ with $x * y = x^2 \cdot y^{-1}$.

Explicitly, it is $(\mathbb{Z}_5 \times \mathbb{Z}_3, *)$ with $(a, x) * (b, y) = (\mu_{x,y}a - b, -x - y)$

$\mu_{x,y}$	0	1	2
0	2	-1	-1
1	-1	2	-1
2	-1	-1	2

2. that non-Bol loop

The corresponding quasigroup is $(\mathbb{Z}_5 \times \mathbb{Z}_3, *)$ with

$$(a, x) * (b, y) = (\mu_{x,y}a - b + \tau_{x,y}, -x - y)$$

where $\tau_{x,y} = \delta_{x-y,1}$.

(Part of) Kepka's theorem as a consequence

Proposition

Let (Q, \cdot) be a loop, ψ its automorphism and assume its companion mapping φ is a permutation. Then any two of the following properties imply the third:

- (Q, \cdot) is a Belousov-Onoi loop with respect to ψ ;
- (Q, \cdot) is a commutative Moufang loop;
- φ is an automorphism.

... fairly straightforward, using Pflugfelder's theorem

... it easily follows that *distributive quasigroups are linear over commutative Moufang loops* (apply the BO theorem from both sides)

The Kikkawa-Robinson theorem as a consequence

Proposition

Let (Q, \cdot) be a loop and $\psi(x) = x \setminus 1$. Then (Q, \cdot) is a *Belousov-Onoi loop* with respect to ψ iff it is a *uniquely 2-divisible Bruck loop* (aka *B-loop*).

As an easy corollary, we obtain:

Theorem (Robinson 1964, Kikkawa 1973)

The following are equivalent for a quasigroup $(Q, *)$:

- 1 it is *involutory* left distributive,
- 2 there is a *B-loop* (Q, \cdot) such that $a * b = a^2 \cdot b^{-1}$.

involutory, aka *left symmetric*: $L_a^2 = id$ for all $a \in Q$

3b. Homogeneous representation of quandles

(Galkin 1979, Hulpke - S. - Vojtěchovský 2015)

Connected and homogeneous quandles

quandle = idempotent binary algebra such that all L_a 's are automorphisms

left multiplication group: $\text{LMlt}(Q) = \langle L_a : a \in Q \rangle \leq \text{Aut}(Q)$

homogeneous quandle: $\text{Aut}(Q)$ acts transitively on Q

connected quandle: $\text{LMlt}(Q)$ acts transitively on Q

Examples:

- left distributive quasigroups are connected: given $a, b \in Q$, we have $L_{b/a}(a) = (b/a) * a = b$
- there are many connected quandles which are not quasigroups, e.g. any conjugacy class in a simple group, operation conjugation
- $(\mathbb{Z}_4, 2x - y)$ is homogeneous, disconnected
- there are many non-homogeneous quandles

Constructing homogeneous quandles

Let (G, \cdot) be a group, H its subgroup, and ψ an automorphism of (G, \cdot) such that $\psi(a) = a$ for every $a \in H$.

Denote G/H the set of left cosets $\{aH : a \in G\}$.

Let $\mathcal{Q}(G, H, \psi) = (G/H, *)$ 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 $a, u \in G$
 $a\psi(a^{-1}) \in H^u \Rightarrow a \in H$.

Note: If $H = 1$, this is the same construction as we have seen for the group-derived Belousov-Onoi modules (G, \cdot, ψ) .

Homogeneous representation

Proposition

Q a quandle, $e \in Q$, $G \trianglelefteq \text{Aut}(Q)$, denote e^G the orbit of e .
Then the orbit subquandle $(e^G, *)$ is isomorphic to $\mathcal{Q}(G, G_e, -^{L_e})$.

- *Homogeneous representation*: Every homogeneous quandle $(Q, *)$ is isomorphic to $\mathcal{Q}(G, G_e, -^{L_e})$ with $G = \text{Aut}(Q, *)$.
- *Canonical representation*: Every connected quandle $(Q, *)$ is isomorphic to $\mathcal{Q}(G, G_e, -^{L_e})$ with $G = \text{LMlt}(Q, *)$.
- *Minimal representation*: Every connected quandle $(Q, *)$ is isomorphic to $\mathcal{Q}(G, G_e, -^{L_e})$ with $G = \text{LMlt}(Q, *)'$.

Corollary (Joyce)

A quandle is isomorphic to some $\mathcal{Q}(G, H, \psi)$ if and only if it is homogeneous.

Canonical representation

Fix a set Q and an element e .

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

Theorem (H. S. V.)

The following are mutually inverse mappings:

connected quandles \leftrightarrow *quandle envelopes*

$$(Q, *) \rightarrow (\text{LMlt}(Q, *), L_e)$$

$$\mathcal{Q}(G, G_e, -^\zeta) \leftarrow (G, \zeta)$$

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

Two envelopes (G_1, ζ_1) and (G_2, ζ_2) yield isomorphic quandles iff there is a permutation f of Q such that $f(e) = e$, $\zeta_1^f = \zeta_2$ and $G_1^f = G_2$.

3c. The structure of left distributive quasigroups

Enumeration

n	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	
$LD^*(n)$	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	2	0
$ILD^*(n)$	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0
$MI(n)$	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	
$LD^*(n)$	0	0	0	0	2	0	0	0	0	0	32	2	0	0	0	0	
$ILD^*(n)$	0	0	0	0	1	0	0	0	0	0	4	0	0	0	0	0	
$MI(n)$	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		
$LD^*(n)$	2	0	0	1	0	0	2	0	0	0	0	0	12	0	0		
$ILD^*(n)$	1	0	0	0	0	0	1	0	0	0	0	0	3	0	0		
$MI(n)$	9	0	15	8	35	0	11	6	39	0	41	9	24	0	45		

Enumeration

Theorem (Stein 1957)

$$LD(4k + 2) = 0$$

Theorem (Etingof-Soloviev-Guralnick 2001, Graña 2004)

Connected quandles of prime and prime square order are medial.

Theorem (McCarron / H. S. V.)

There are no connected quandles of order $2p$, $p > 5$.

Structural properties

Theorem (Kano-Nagao-Nobusawa / Galkin / Kik.-Rob.-Glauberman)

Finite *involutory* left distributive quasigroups are *solvable* and have the *Lagrange and Sylow properties*.

Theorem (Galkin)

Finite *solvable* left distributive quasigroups have the *Lagrange property*.
(Not Sylow, cf. example of order 15.)

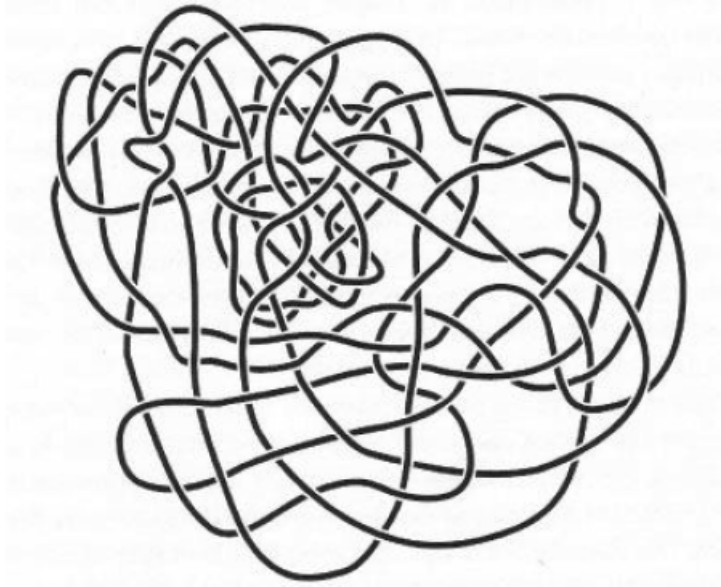
Sylow property holds under the additional assumption that the order of the quasigroup, and the order of its translations, are coprime.

And much more, see my paper in QRS.

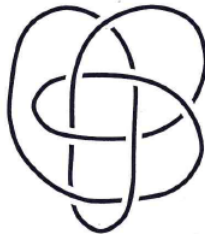
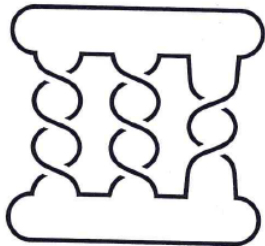
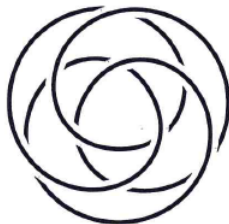
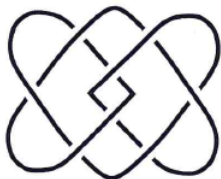
4. Applications in knot theory

(Joyce, Matveev 1980s; Fish-Lisitsa-S. 2015)

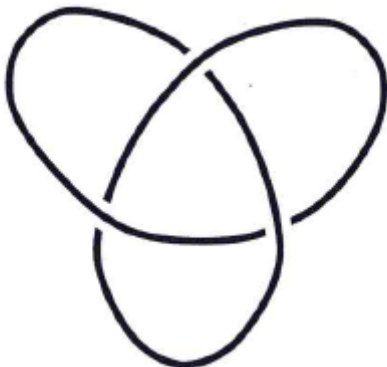
Is it really knotted?



Four pictures, one knot



Is it really knotted?



If you think it cannot be untangled, PROVE IT!

Knot recognition

Knot equivalence = a continuous deformation of space that transforms one knot into the other.

Fundamental Problem

Given two knots (or knot diagrams), are they equivalent?

Is it (algorithmically) decidable?

If so, what is the complexity?

Knot recognition

Knot equivalence = a continuous deformation of space that transforms one knot into the other.

Fundamental Problem

Given two knots (or knot diagrams), are they equivalent?

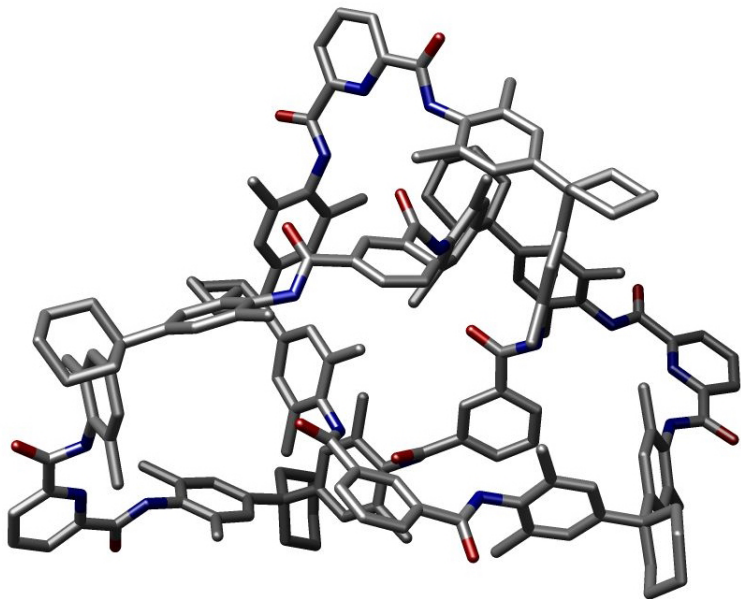
Is it (algorithmically) decidable?

Yes, very hard to prove. (Haken, 1962)

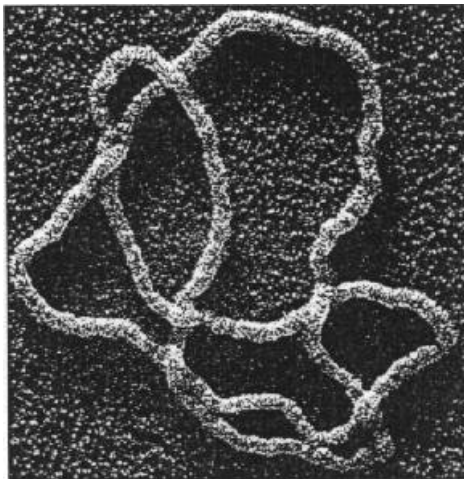
If so, what is the complexity?

Nobody knows. No efficient algorithm known.

Knots are in chemistry



Knots are in biology



... with applications towards **antibiotics production** (believe or not)

Knots are everywhere



... with applications towards **black magic** (believe or not)

Classical approach to knot recognition

Develop *invariants*, properties shared by equivalent knots.

$$K_1 \sim K_2 \quad \text{implies} \quad P(K_1) = P(K_2)$$

Classical invariants use various algebraic constructions to code some of the topological properties of a knot.

- the Alexander, Jones and other polynomials
- the fundamental group of the knot complement
- Khovanov homology, Heegaard-Floer homology, ...



Trade-off between complexity and ability to recognize knots.

How to Say Butterfly



Farfalla



Papillon



Butterfly

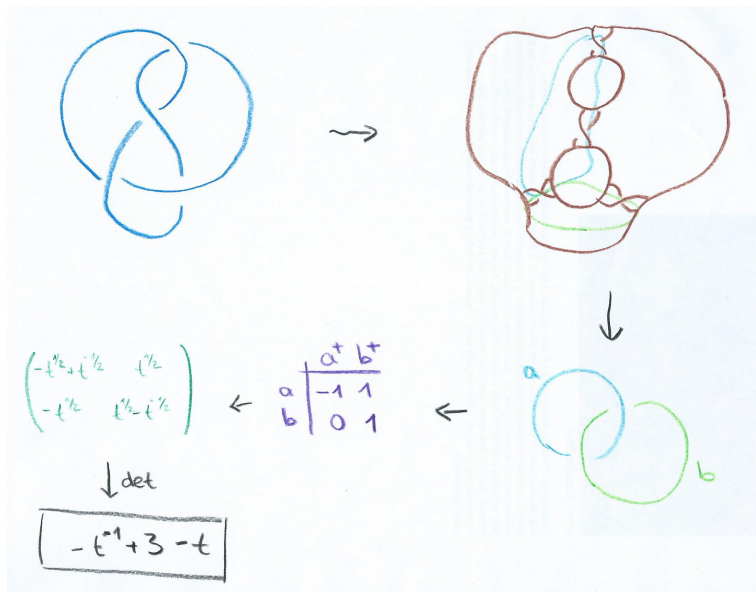


Mariposa

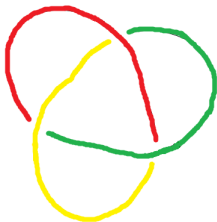


SCHMETTERLING!!!

Alexander polynomial



Combinatorial approach: 3-coloring

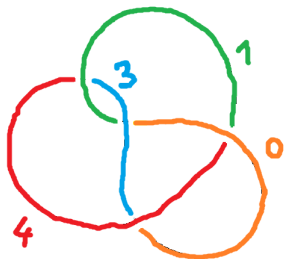


To every arc, assign one of **three colors** in a way that

every crossing has **one or three** colors.

Invariant: count non-trivial (non-monochromatic) colorings.

Combinatorial approach: Fox n -coloring



To every arc, assign one of n colors, $0, \dots, n - 1$, in a way that

at every crossing, $2 \cdot \text{bridge} = \text{left} + \text{right}$, modulo n

Invariant: count non-trivial colorings.

Combinatorial approach: quandle coloring



Let $(Q, *)$ be a quandle.

To every arc, assign one of the colors from a set Q in a way that

$$c(\alpha) * c(\beta) = c(\gamma).$$

Invariant: count non-trivial colorings, $col_Q(K)$. Really?

Combinatorial approach: quandle coloring



Let $(Q, *)$ be a quandle.

To every arc, assign one of the colors from a set Q in a way that

$$c(\alpha) * c(\beta) = c(\gamma).$$

Invariant: count non-trivial colorings, $col_Q(K)$. Really?

Fact (implicitly Joyce, Matveev (1982))

Quandle coloring is an invariant.

Knot recognition algorithm

Parameter: a (potentially infinite) set of quandles \mathcal{Q}

IN: two knots K_1, K_2 **OUT:** are they different?

run over \mathcal{Q} , if $col_{\mathcal{Q}}(K_1) \neq col_{\mathcal{Q}}(K_2)$, the knots are different

Semidecision procedure: either stops with a certificate of inequivalence, or runs forever

Knot recognition algorithm

Parameter: a (potentially infinite) set of quandles \mathcal{Q}

IN: two knots K_1, K_2 **OUT:** are they different?

run over \mathcal{Q} , if $col_{\mathcal{Q}}(K_1) \neq col_{\mathcal{Q}}(K_2)$, the knots are different

Semidecision procedure: either stops with a certificate of inequivalence, or runs forever

IN: one knot K **OUT:** can it be untangled?

two algorithms running **in parallel:**

run over \mathcal{Q} , if $col_{\mathcal{Q}}(K) > 0$, the knot is non-trivial

use an automated theorem prover to prove $col_{\mathcal{Q}}(K) = 0$ for every \mathcal{Q}

Decision procedure: either stops with a certificate of non-triviality, or a proof of triviality is found

Works very well for knots with < 100 crossings. [Fish, Lisitsa, S. 2015]

Where is the algebra?

The algorithm requires a suitable set of quandles \mathcal{Q} .

- conjugation quandles (rather special case)
- affine quandles (see 2b. Medial quasigroups)
- small quandles (see 3b. Homogeneous representation)
- simple quandles
- etc.

Fact: simple quandles are sufficient for unknot recognition

Fact: conjugation quandles over $PSL_2(q)$ are sufficient for unknot recognition [Kuperberg's NP algorithm]

Which quandles work best in practice?

Which quandles work for general recognition?

Affine colorings = Alexander invariant, what about other quandles?

Etc. (veery intersting topic, in my opinion)

Thank you for your attention...



... and come to visit me in Kazakhstan!