Quandles and universal algebra

Quandles and knots, and groups, and universal algebra

David Stanovský

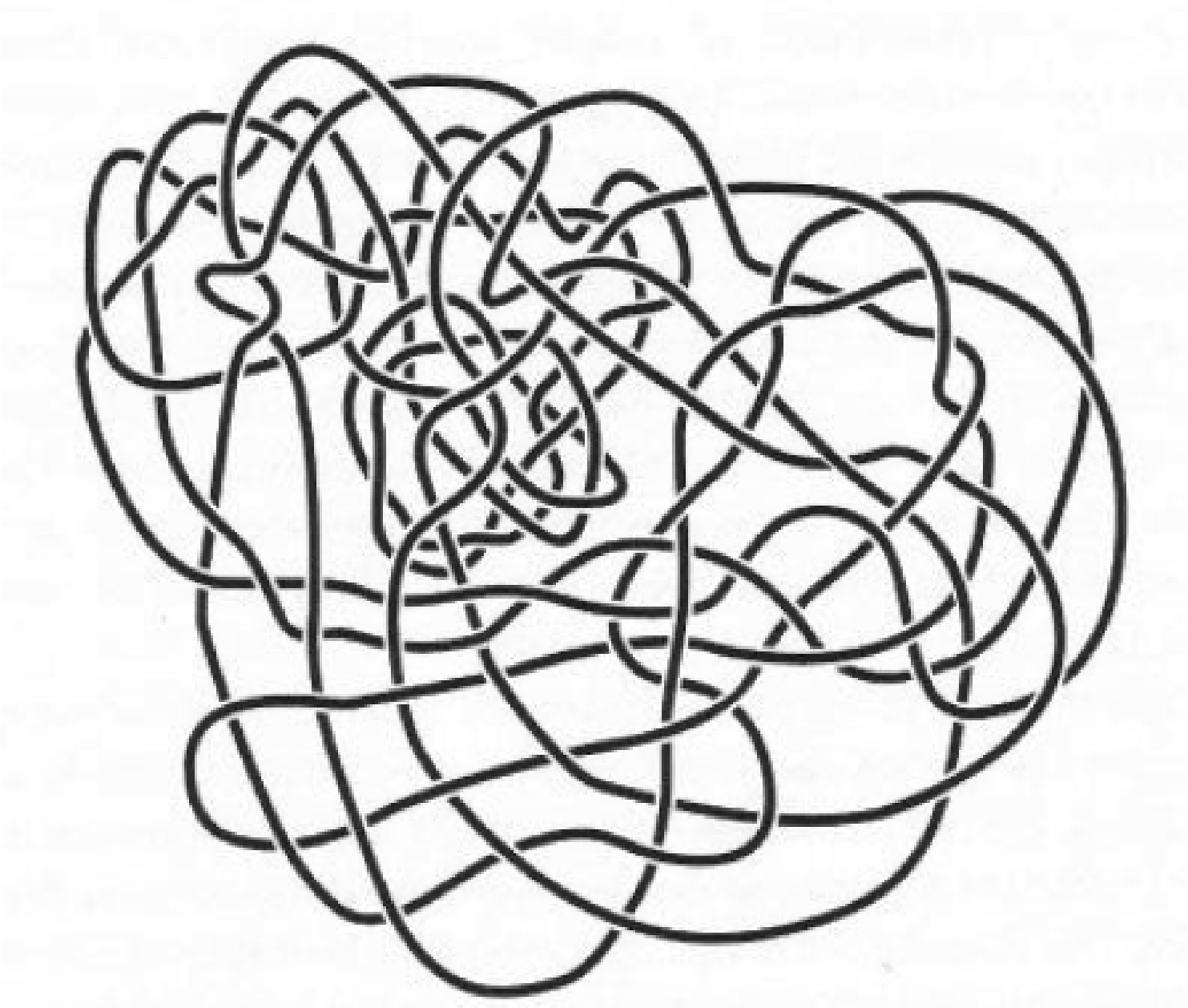
Charles University, Prague, Czech Republic

Novi Sad, June 2017

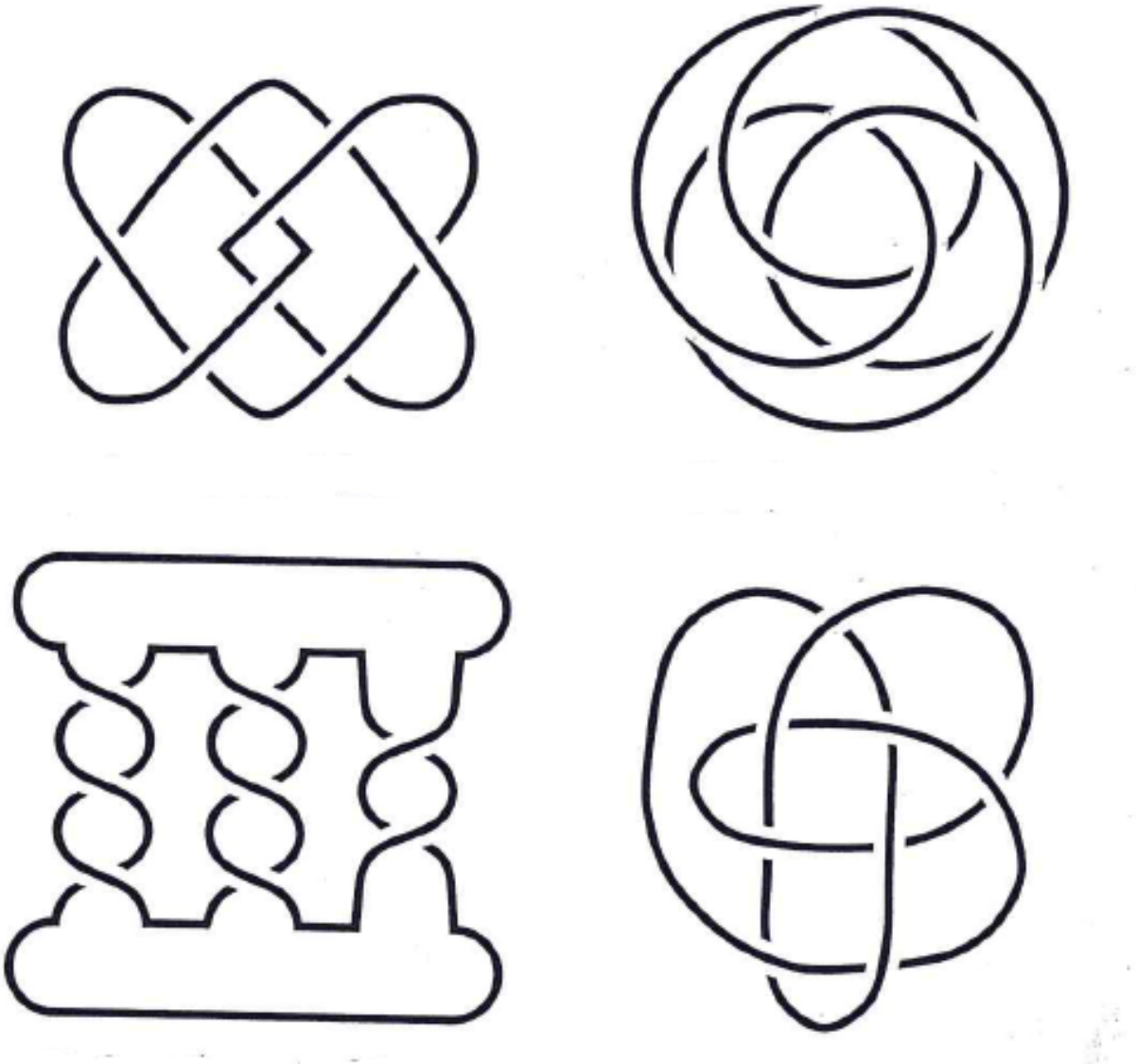
Outline

1. Quandles and knots
2. Quandles and groups
3. Quandles and universal algebra

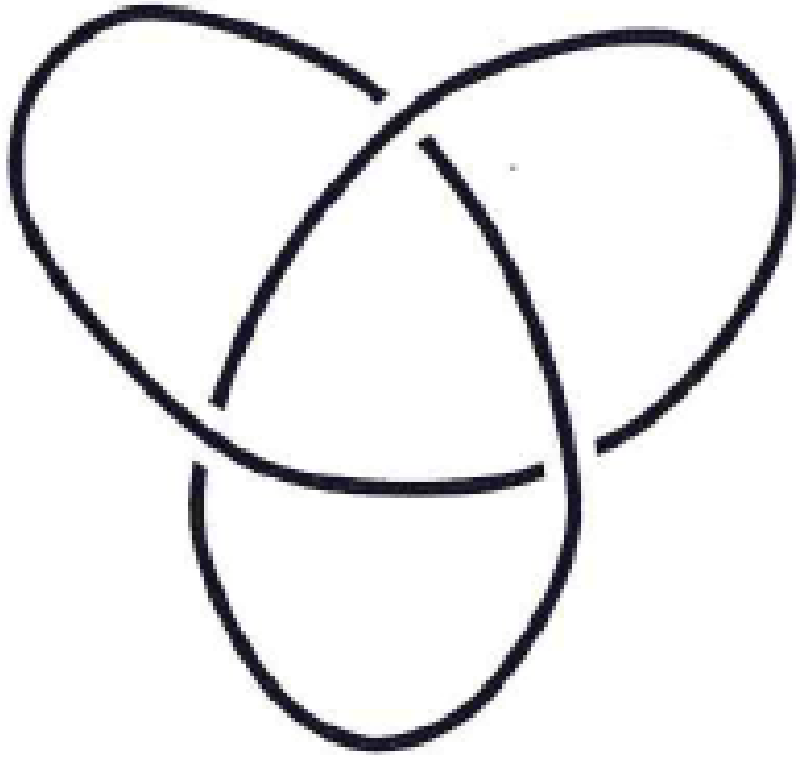
Is it really knotted?



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 provably efficient algorithm known.

Knottedness

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

Fundamental Problem

Given a knot (or a knot diagram), is it equivalent to the plain circle?

Is it (algorithmically) decidable?

If so, what is the complexity?

Knottedness

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

Fundamental Problem

Given a knot (or a knot diagram), is it equivalent to the plain circle?

Is it (algorithmically) decidable?

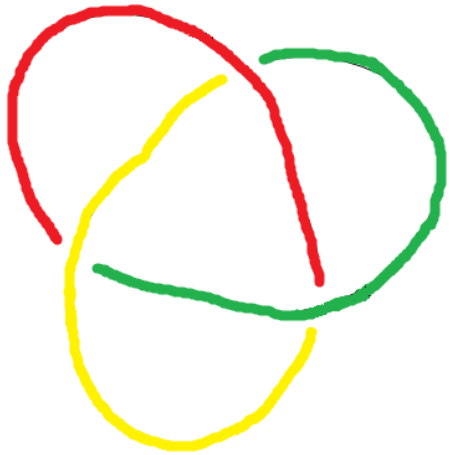
Yes, hard to prove. (Haken, < 1962)

If so, what is the complexity?

Nobody knows. Known to be in NP $\cap$ coNP (under GRH).

[Haas-Lagarias-Pippenger 1999, Lackenby 2016; Kuperberg 2014]

Combinatorial approach: 3-coloring



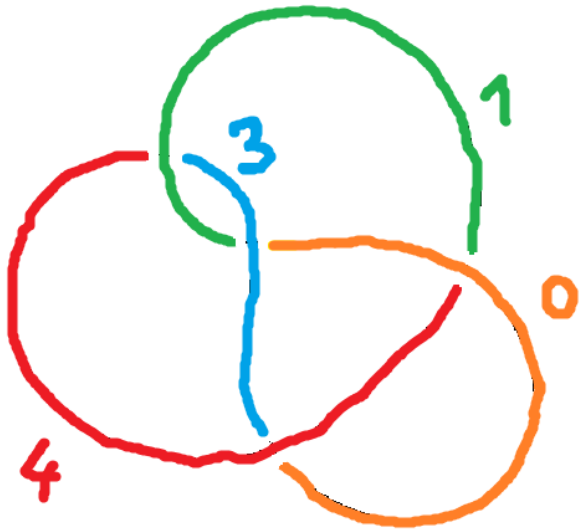
To every arc, assign one of three colors in a way that

every crossing has one or three colors.

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

(Formally: if $K_1 \sim K_2$, then $col(K_1) = col(K_2)$.)

Combinatorial approach: n-coloring

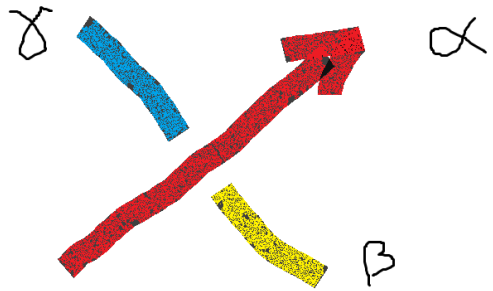


To every arc, assign one of n colors, $0, \ldots, n-1$, in a way that

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

Invariant: count non-trivial colorings.

Combinatorial approach: quandle coloring



Fix a ternary relation T on a set of colors C.
To every arc, assign one of the colors from C in a way that

$$(c(\alpha), c(\beta), c(\gamma)) \in T$$

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

Which relations T really provide an invariant?

Example: $C = \{0, ..., n-1\}$, $T = \{(x, y, z) : \ 2x = y + z \pmod{n}\}$.

Quandle coloring

Fact (implicitly Joyce, Matveev ('82), explicitly Fenn-Rourke ('92))

Coloring by (C, T) is an invariant if T is a graph of an operation $*$ such that for every x, y, z

- $x * x = x$
- *there is a unique u such that $x * u = y$*
- $x * (y * z) = (x * y) * (x * z)$

Such algebraic objects are called quandles.

(In a way, a coloring is an invariant if and only if the structure is a quandle.)

Knot recognition algorithm

[Old idea, recently developed by Fish, Lisitsa, S.]

IN: two knots K_1, K_2

run over $Q \in \mathcal{Q}$

if $col_Q(K_1) \neq col_Q(K_2)$, then return "they are different"

return "I have no idea"

Knot recognition algorithm

[Old idea, recently developed by Fish, Lisitsa, S.]

IN: two knots K_1, K_2

run over $Q \in \mathcal{Q}$
    if $col_Q(K_1) \neq col_Q(K_2)$, then return "they are different"
return "I have no idea"

Semidecision procedure: either stops with a certificate of inequivalence, or fails to say anything valuable

Can be turned into a decision procedure if $K_2 = \bigcirc$:
Use an automated theorem prover to prove $col_Q(K) = 0$ for every Q.

Knot recognition algorithm

The algorithm works well in practice.

- small quandles are sufficient
- SAT-solvers calculate colorings fast

Knot recognition algorithm

The algorithm works well in practice.

- small quandles are sufficient
- SAT-solvers calculate colorings fast

We do not know much about its theoretical complexity.

- upper bound on smallest $|Q|$ such that $col_Q(K) > 0$?
- given Q, K, can we calculate $col_Q(K)$ in polynomial time?
  ... special kind of CSP, solving equations over quandles

Kuperberg (2014): if $K \not\bigcirc$ and $\mathcal{Q}$ is a certain set of quandles derived from groups $SL(2, p)$, the algorithm produces a polynomial size certificate of unknottedness (under GRH). Thus, knottedness is in NP.

To prove more, and to make it faster in practice, we need to

know more about QUANDLES.


SCORE: 75
HI-SCORE:1201


PARATROOPER
by
Greg Kuperberg
PRESS 'I' FOR INSTRUCTIONS
PRESS space bar FOR KEYBOARD PLAY
OR joystick button FOR JOYSTICK PLAY
OR ctrl-J FOR JOYSTICK adjustment
(C)1982 ORION SOFTWARE, INC.

Outline

1. Quandles and knots
2. Quandles and groups
3. Quandles and universal algebra

Quandles

A binary algebra $(Q, *)$ is called a *quandle* if

- $x * x = x$
- all left translations $L_x(y) = x * y$ are automorphisms.

Examples:

- groups under conjugation: $x * y = xyx^{-1}$.
- affine quandles: abelian groups under $x * y = (1 - f)(x) + f(y)$, f an automorphism.
- ...
- (various constructions)
- ...
- geometry/topology: symmetric spaces, braids, knots...
- Hopf algebras, discrete solutions to the Yang-Baxter equation
- combinatorial algebra: a natural generalization of selfdistributive quasigroups (since 1923!)

Connected quandles

Multiplication group, displacement group:

$$\mathrm{LMlt}(Q) = \langle L_x : x \in Q \rangle \leq \mathrm{Aut}(Q)$$
$$\mathrm{Dis}(Q) = \langle L_x L_y^{-1} : x, y \in Q \rangle \leq \mathrm{LMlt}(Q)$$

A quandle is called *connected* if $\mathrm{LMlt}(Q)$ is transitive on Q.

Theorem (Hulpke, S., Vojtěchovský)

Fix a set Q and $e \in Q$.
Connected quandles $(Q, *)$ are in 1-1 correspondence to pairs (G, ζ) where

- *G is a transitive group over Q;*
- *$\zeta \in Z(G_e)$ and $\langle \zeta^G \rangle = G$.*

Proof: $Q \mapsto (\mathrm{LMlt}(Q), L_e)$.

Hayashi's conjecture

... translate problems from quandles to groups

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

... translate problems from quandles to groups

Conjecture (Hayashi)

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

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.

Connected quandles of prime size

... use finite group theory to prove fact about quandles

Theorem (Etingof, Soloviev, Guralnik, 2001)

Connected quandles of prime size are affine.

Sketch of the proof.

$\mathrm{LMlt}(Q)$ 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.

Enumerating connected quandles

... use computational tools to calculate with 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..40	29	17	11	0	15	73	35	0	13	33
41..47	39	26	41	9	45	0	45			

(Vedramin / HSV)

... count all (G, ζ) up to conjugacy,

using the full list of transitive groups of degree $n \leq 47$ (Holt, 2014).

Associated group

Associated group: $A(Q) = \langle Q \mid xyx^{-1} = z \text{ whenever } x * y = z \rangle$

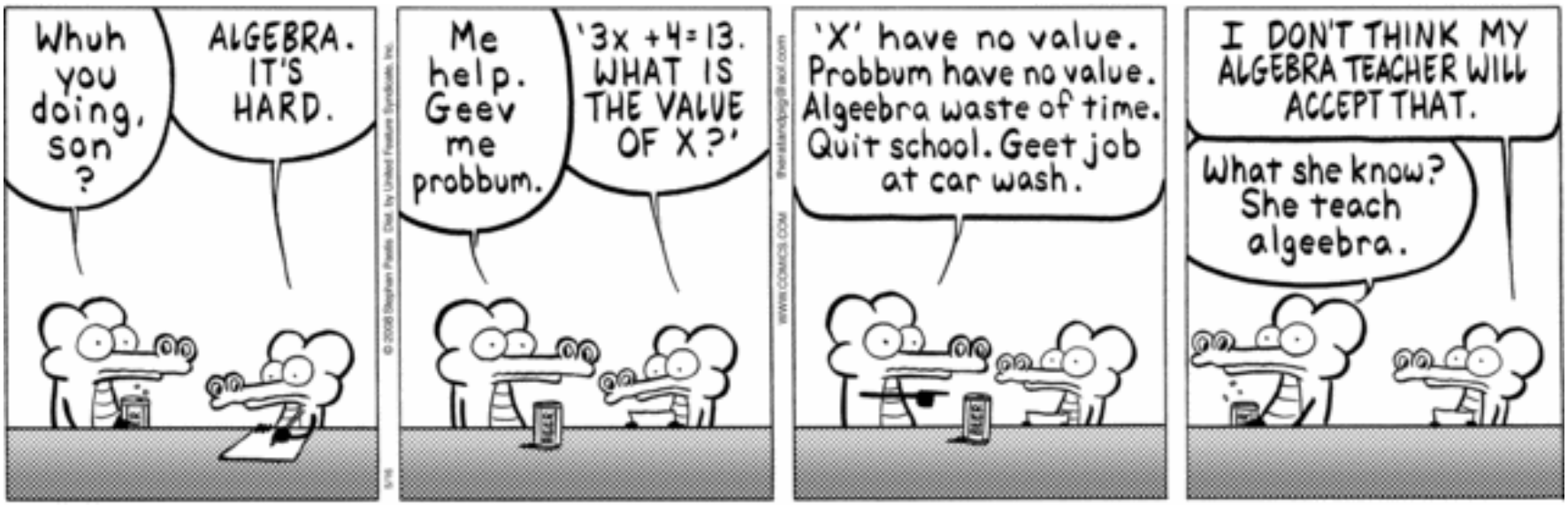
Some people say $A(Q)$ is a very useful.

Example (Eisermann, 2014):
$A(Q)$ determines connected strongly abelian extensions of Q.

(i.e., connected quandles E with a strongly abelian congruence α such that $E/\alpha \simeq Q$)

Joke...

Joke...


Whuh you doing, son ?
ALGEBRA. IT'S HARD.
Me help. Geev me probbum.
'3x +4=13. WHAT IS THE VALUE OF X?'
'X' have no value. Probbum have no value. Algeebra waste of time. Quit school. Geet job at car wash.
I DON'T THINK MY ALGEBRA TEACHER WILL ACCEPT THAT.
What she know? She teach algeebra.

Outline

1. Quandles and knots
2. Quandles and groups
3. Quandles and universal algebra

Affine and quasi-affine quandles

In universal algebra:

affine = polynomially equivalent to a module
quasi-affine = subreduct of affine

In quandles:

affine = reduct of a module
... $Aff(A, f)$: universe A, operation $x * y = (1 - f)(x) + f(y)$

Coloring by affine quandles

Coloring by affine quandles $\leftrightsquigarrow$ *Alexander invariant*

Theorem (Bae 2011)

Let K be a link and f its Alexander polynomial.

- $f = 0 \Rightarrow$ *colorable by every affine quandle*
- $f = 1 \Rightarrow$ *not colorable by any affine quandle*
- *else, colorable by* $Aff(\mathbb{Z}[t, t^{-1}]/(f), f)$.

Corollary:

- $f = 1 \Rightarrow$ not colorable by any solvable quandle

Problem: A quandle-theoretic description of solvable quandles?

Abelian vs. quasi-affine

quasi-affine $\Rightarrow$ abelian

- the diagonal is a congruence block on $\mathbf{A}^2$
- for every term t and $\bar{a}, \bar{b}, \bar{c}, \bar{d} \in A$

$$t(\bar{a}, \bar{c}) = t(\bar{a}, \bar{d}) \quad \Rightarrow \quad t(\bar{b}, \bar{c}) = t(\bar{b}, \bar{d})$$

Abelian vs. quasi-affine

quasi-affine $\Rightarrow$ abelian

- the diagonal is a congruence block on $\mathbf{A}^2$
- for every term t and $\bar{a}, \bar{b}, \bar{c}, \bar{d} \in A$

$$t(\bar{a}, \bar{c}) = t(\bar{a}, \bar{d}) \quad \Rightarrow \quad t(\bar{b}, \bar{c}) = t(\bar{b}, \bar{d})$$

(Quackenbush) abelian $\not\Rightarrow$ quasi-affine

abelian $\Rightarrow$ affine if

- (TCT) finite, Taylor
- (Kearnes, Szendrei) a Mal'tsev condition that fails in semilattices

in both cases: $\Rightarrow$ Mal'tsev term $\Rightarrow$ Gumm-Smith construction

abelian $\Rightarrow$ quasi-affine if

- (TCT) finite simple
- (Kearnes, Szendrei) Taylor
- (Kearnes, Szendrei) simple idempotent
- ...

Quasi-affine and affine quandles

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

TFAE for a quandle Q:

1. *quasi-affine*
2. $\mathrm{Dis}(Q)$ *abelian, semiregular*
3. $Q \simeq Ext(A, f, \bar{d})$
4. *abelian*

Theorem (dtto)

TFAE for a quandle Q:

1. *affine*
2. $\mathrm{Dis}(Q)$ *abelian, semiregular and "balanced occurences of generators"*
3. $Q \simeq Ext(A, f, \bar{d})$ *and* $\bar{d}$ *is a multi-transversal of* $A/\mathrm{Im}(1-f)$
4. *abelian and "balanced orbits"*

Quasi-affine theorem explained

Theorem

TFAE for a quandle Q:

1. *quasi-affine*
2. $\mathrm{Dis}(Q)$ *abelian, semiregular*
3. $Q \simeq Ext(A, f, \bar{d})$
4. *abelian*

semiregular: g has a fixed point $\Rightarrow g = id$

$Ext(A, f, \bar{d})$: A an abelian group, $f \in \mathrm{Aut}(A)$, $\bar{d} = (d_i : i \in I) \subseteq A$:

- universe $I \times A$
- operation $(i, a) * (j, b) = (j,\ (1 - f)(a) + f(b) + d_i - d_j)$

(a special type of central extension)

Affine theorem explained

Theorem

TFAE for a quandle Q:

1. *affine*
2. $\mathrm{Dis}(Q)$ *abelian, semiregular and "balanced occurences of generators"*
3. $Q \simeq Ext(A, f, \bar{d})$ *and* $\bar{d}$ *is a multi-transversal of* $A/\mathrm{Im}(1-f)$
4. *abelian and "balanced orbits"*

balanced:

- (in general) $\{\{L_a L_e^{-1} : a \in T\}\}$ is a multi-transversal of $\mathrm{Dis}(Q)/[\mathrm{Dis}Q, L_e]$ for any multi-transversal T of the orbit decomposition
- (for finite) in every orbit, every column of the multiplication table contains the same number of entries of each kind

Consequences

Polynomial time algorithm for checking (quasi-)affineness

... check whether $\mathrm{Dis}(Q)$ is abelian, semiregular(, "balanced")

Enumeration of quasi-affine quandless

n	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
quasi-affine	1	1	2	3	4	4	6	9	12	7	10	17	12	10	14
affine	1	1	2	3	4	2	6	7	11	4	10	6	12	6	8

... enumerate $Ext(A, f, \bar{d})$ up to isomorphism

Congruences of quandles

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

There is a Galois correspondence

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

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

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

Congruences of 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 (Bonatto, S.)

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

1. *α centralizes β (over 0_Q)*
2. *$\mathrm{Dis}_\beta(Q)$ centralizes $\mathrm{Dis}_\alpha(Q)$ and acts semiregularly on every α-block*

Abelian congruences and solvable quandles

Proposition

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

1. α *is abelian*
2. $\mathrm{Dis}_\alpha(Q)$ *is abelian and acts semiregularly on every block of* α
3. Q *is an abelian extension of* $F = Q/\alpha$, *i.e.,* $(F \times A, *)$ *with*
$$(x, a) * (y, b) = (xy,\ \varphi_{x,y}(a) + \psi_{x,y}(b) + \theta_{x,y})$$
where A *is an abelian group,* $\varphi : Q^2 \to End(A)$, $\psi : Q^2 \to Aut(A)$, $\theta : Q^2 \to A$ *satisfying the cocycle condition.*

The last item only assuming that α *has connected blocks.*

Abelian congruences and solvable quandles

Proposition

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

1. α *is abelian*
2. $\mathrm{Dis}_\alpha(Q)$ *is abelian and acts semiregularly on every block of* α
3. Q *is an abelian extension of* $F = Q/\alpha$, *i.e.,* $(F \times A, *)$ *with*
$$(x, a) * (y, b) = (xy,\ \varphi_{x,y}(a) + \psi_{x,y}(b) + \theta_{x,y})$$
where A *is an abelian group,* $\varphi : Q^2 \to End(A)$, $\psi : Q^2 \to Aut(A)$, $\theta : Q^2 \to A$ *satisfying the cocycle condition.*

The last item only assuming that α *has connected blocks.*

Corollary

- Q *solvable (of rank* n*)* $\Rightarrow \mathrm{Dis}(Q)$ *solvable (of rank* $\leq 2n - 1$*)*
- $\mathrm{Dis}(Q)$ *solvable,* Q *has Mal'tsev term* $\Rightarrow$ Q *solvable*

Abelian normal subloops and solvable loops

Proposition (S., Vojtěchovský)

TFAE for a normal subloop $A \trianglelefteq Q$, Q a loop:

1. *A is abelian*
2. *$\varphi_{r,s}(a) = \varphi_{u,v}(a)$ for every $a, r/u, s/v \in A$, $\varphi \in \{L, R, T\}$*
3. *Q is an abelian extension of $F = Q/A$, i.e., $(F \times A, *)$ with*
$$(x, a) * (y, b) = (xy,\ \varphi_{x,y}(a) + \psi_{x,y}(b) + \theta_{x,y})$$
where A is an abelian group, $\theta : Q^2 \to A$ satisfying the cocycle condition.

Here $L_{x,y}(z) = (xy)\backslash(x \cdot yz)$, $R_{x,y}(z) = (zy \cdot x)/(yx)$, $T_x(z) = xz/z$.

These are the mapping that generate the *inner mapping group*.

Abelian normal subloops and solvable loops

Proposition (S., Vojtěchovský)

TFAE for a normal subloop $A \trianglelefteq Q$, Q a loop:

1. *A is abelian*
2. *$\varphi_{r,s}(a) = \varphi_{u,v}(a)$ for every $a, r/u, s/v \in A$, $\varphi \in \{L, R, T\}$*
3. *Q is an abelian extension of $F = Q/A$, i.e., $(F \times A, *)$ with*
$$(x, a) * (y, b) = (xy,\ \varphi_{x,y}(a) + \psi_{x,y}(b) + \theta_{x,y})$$
where A is an abelian group, $\theta : Q^2 \to A$ satisfying the cocycle condition.

Here $L_{x,y}(z) = (xy)\backslash(x \cdot yz)$, $R_{x,y}(z) = (zy \cdot x)/(yx)$, $T_x(z) = xz/z$.

These are the mapping that generate the *inner mapping group*.

No relation of solvability of Q to solvability of its multiplication group is known!

Central congruences and nilpotent quandles

Proposition

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

1. α *is central*
2. $\mathrm{Dis}_\alpha(Q)$ *is central and* $\mathrm{Dis}(Q)$ *acts semiregularly on every block of* α
3. Q *is a central extension of* $F = Q/A$, *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 cocycle condition.*

The last item only assuming that Q *has a Mal'tsev term.*

Central congruences and nilpotent quandles

Proposition

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

1. α *is central*
2. $\mathrm{Dis}_\alpha(Q)$ *is central and* $\mathrm{Dis}(Q)$ *acts semiregularly on every block of* α
3. Q *is a central extension of* $F = Q/A$, *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 cocycle condition.*

The last item only assuming that Q *has a Mal'tsev term.*

Proposition

- Q *nilpotent (of rank* n*)* $\Rightarrow$ $\mathrm{Dis}(Q)$ *nilpotent (of rank* $\leq 2n - 1$*)*
- $\mathrm{Dis}(Q)$ *nilpotent,* Q *has Mal'tsev term* $\Rightarrow$ Q *nilpotent*

Central normal subloops and nilpotent loops

Proposition (folklore)

TFAE for a normal subloop $A \trianglelefteq Q$, Q a loop:

1. *A is central*
2. *$\varphi_{r,s}(a) = a$ for every $a \in A$, $r, s \in Q$, $\varphi \in \{L, R, T\}$*
3. *Q is an central extension of $F = Q/A$, i.e., $(F \times A, *)$ with*
$$(x, a) * (y, b) = (xy,\ \ a + b + \theta_{x,y})$$
where A is an abelian group, $\theta : Q^2 \to A$ satisfying the cocycle condition.

Central normal subloops and nilpotent loops

Proposition (folklore)

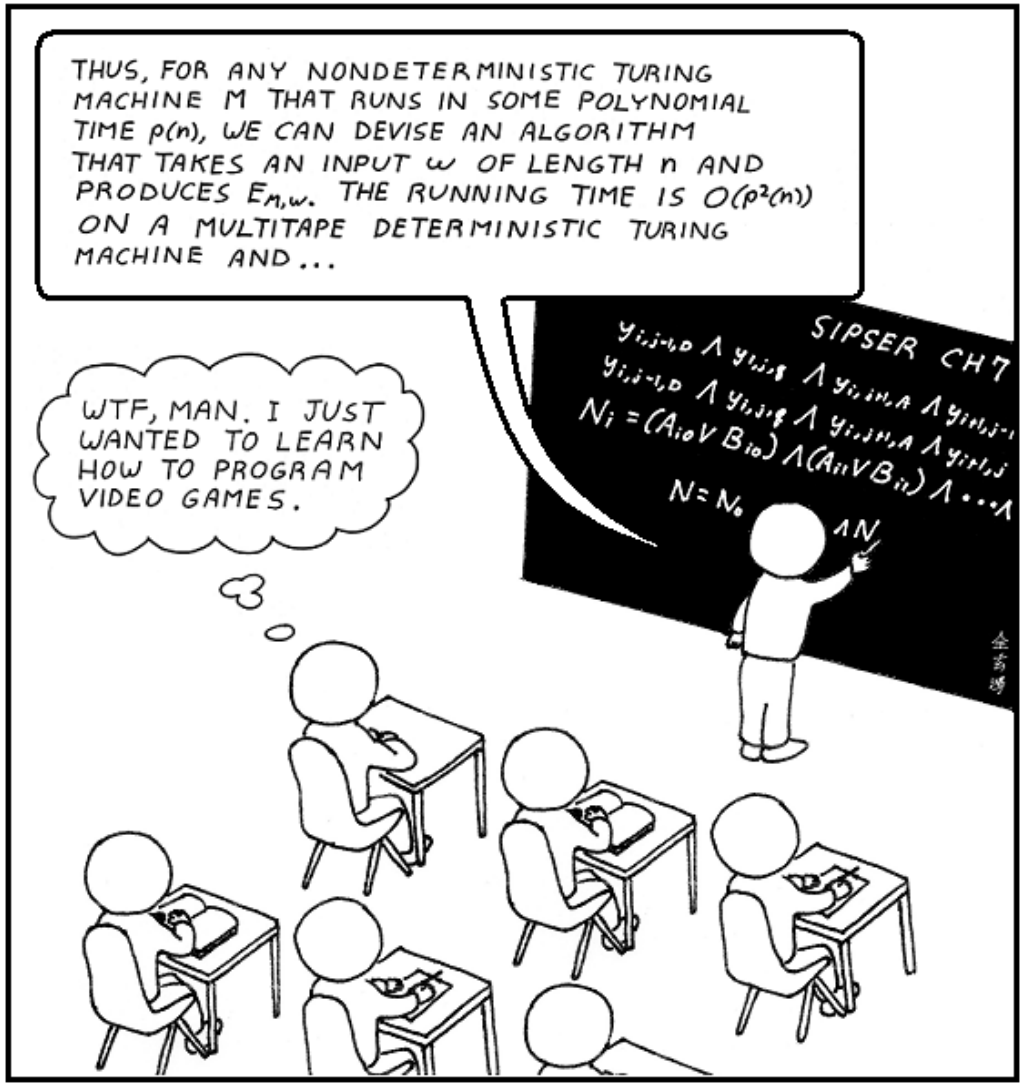
TFAE for a normal subloop $A \trianglelefteq Q$, Q a loop:

1. *A is central*
2. *$\varphi_{r,s}(a) = a$ for every $a \in A$, $r, s \in Q$, $\varphi \in \{L, R, T\}$*
3. *Q is an central extension of $F = Q/A$, i.e., $(F \times A, *)$ with*
$$(x, a) * (y, b) = (xy,\ \ a + b + \theta_{x,y})$$
where A is an abelian group, $\theta : Q^2 \to A$ satisfying the cocycle condition.

Proposition (Bruck)

$Mlt(Q)$ nilpotent $\Rightarrow$ Q nilpotent $\Rightarrow$ $Mlt(Q)$ solvable

Thank you for your attention...



[xkcd.com]