Computational aspects of loop theory

Petr Vojtěchovský

Department of Mathematics
University of Denver

December 7, 2011
35th ACCMCC
Monash University, Melbourne, Australia

Loops

A set Q with a binary operation $\cdot$ is a loop if for every $x \in Q$

$$L_x : Q \to Q, \quad y \mapsto x \cdot y$$
$$R_x : Q \to Q, \quad y \mapsto y \cdot x$$

are bijections of Q, and if there is a neutral element $1 \in Q$ such that $1 \cdot x = x \cdot 1 = x$ for every $x \in Q$.

Multiplication tables of finite loops $=$ normalized Latin squares.

Loop theory usually studies loops with algebraic properties.

Basic concepts

Let Q be a loop with neutral element 1. We define:

commutator	$xy = (yx) \cdot [x, y]$
associator	$(xy)z = x(yz) \cdot [x, y, z]$
center	$Z(Q) = \{x \in Q;\ [x,y]=[x,y,z]=[y,x,z]=1\}$
multiplication group	$\mathrm{Mlt}(Q) = \langle L_x,\ R_x;\ x \in Q \rangle$
inner mapping group	$\mathrm{Inn}(Q) = \{f \in \mathrm{Mlt}(Q);\ f(1) = 1\}$

A subloop $S \leq Q$ is normal if $f(S) = S$ for every $f \in \mathrm{Inn}(Q)$.

Outline of the talk

We will discuss:

- Lagrange's theorem for loops
- enumeration of centrally nilpotent loops
- existence of simple automorphic loops
- loops with commuting inner mappings

Our approach is mostly computational. We will use:

- combinatorial algorithms
- linear algebraic methods (cohomology)
- graphs based on primitive permutation groups
- automated deduction

Lagrange's theorem for loops

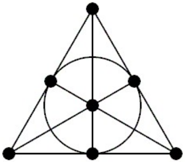
General Lagrange's theorem

When does $S \leq Q$ imply that $|S|$ divides $|Q|$?

- Hardly ever.
- When Q is associative or $S \trianglelefteq Q$. (Easy.)
- When Q is a Moufang loop, that is, a loop satisfying

$$((xy)z)y = x(y(zy)).$$

(Hard [Grishkov, Zavarnitsine, Hall, Gagola 2005].
Proof uses classification of finite simple groups.)



Problem

If S is a subloop of a finite Moufang loop Q, is there a selection of left cosets of S that partition Q?

Incidence properties of cosets

In groups we have $xS = yS$ or $xS \cap yS = \emptyset$.

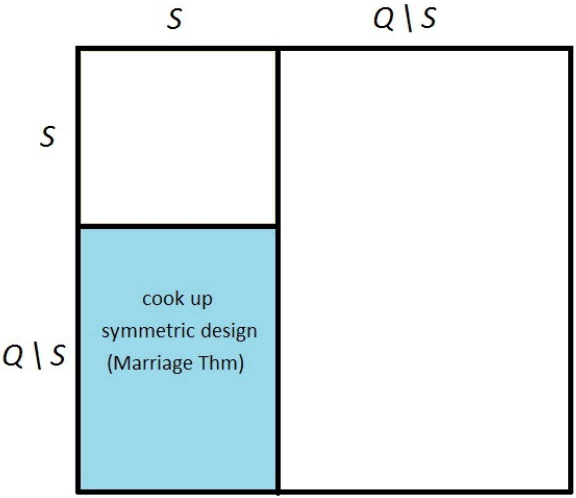
For general loops, anything can happen:

Theorem (Kinyon, Pula, V 2011)
If Q is a loop and $S \leq Q$ then

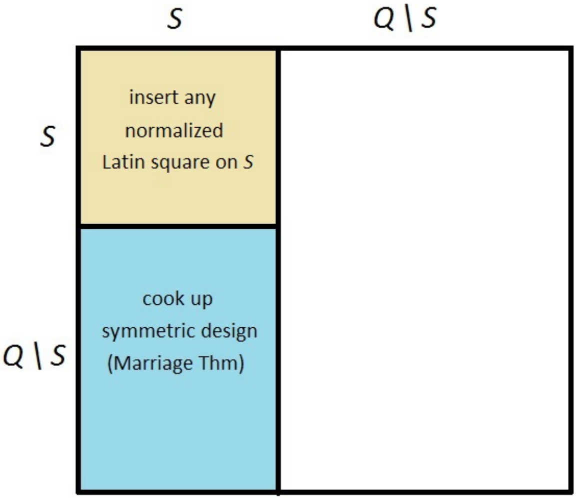
$$(Q \setminus S, \{xS;\ x \in Q \setminus S\})$$

is a symmetric design, and every symmetric design arises in this way.

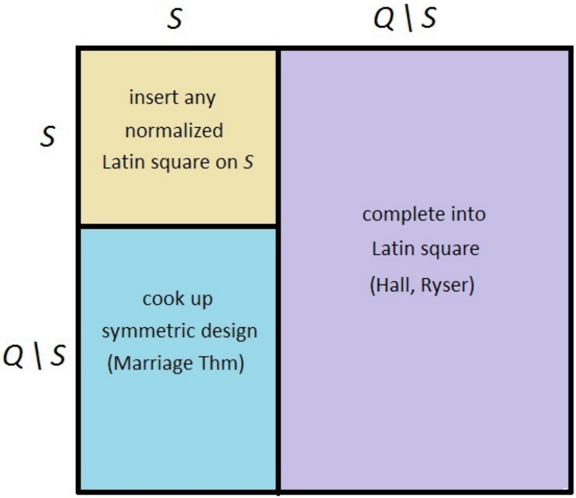
Proof of the “symmetric design theorem”



Proof of the "symmetric design theorem"



Proof of the "symmetric design theorem"



Cosets in Bol loops

A loop Q is (right) Bol if $((xy)z)y = x((yz)y)$ holds.

Example (Einstein's velocity addition)

Define $\oplus$ on $\{v \in \mathbb{R};\ \|v\| < c\}$ by

$$u \oplus v = \frac{1}{1 + (u \cdot v)/c^2} \left(u + \frac{1}{\gamma_u} v + \frac{1}{c^2} \frac{\gamma_u}{1+\gamma_u} (u \cdot v) u \right),$$

where $\gamma_u = (1 - \|u\|^2/c^2)^{-1/2}$.

Problem

Does Lagrange's theorem hold for Bol loops?

- yes, if $S = \langle x \rangle$ [Robinson 1966]
- yes, if $|Q|$ is odd [Foguel, Kinyon, Phillips 2006]
- yes, for certain small subloops S [Kinyon, Pula, V 2011]

Greedy orbits of $\langle R_x;\ x \in S\rangle$

We assume that $S \leq Q$, S is known, Q is not known.

	s_1 id	s_2 σ	s_3 $\sigma\rho$	s_4 ρ	s_5 ρ^2	s_6 $\sigma\rho^2$
1	1	2	3	4	5	6
2	2	1	7	8	9	10
3	3	10	1			$\boxed{?}$
4	4					
5	5					
6	6					

$$3s_2 = 10 = 2s_6$$
$$3 = (2s_6)s_2^{-1}$$
$$3s_6 = ((2s_6)s_2^{-1})s_6$$

recall $((xy)z)y = x((yz)y)$

$$3s_6 = 2((s_6 s_2^{-1})s_6) = 2s_3 = 7$$

$$\boxed{?} = 7$$

It so happens here that every “orbit” closes at a size (number of rows) divisible by $6 = |S|$. Hence $|S|$ divides $|Q|$.

Similarly for some other small Bol loops S.

Observations about greedy orbits

The greedy orbits can get very long (e.g., 720 for $|S| = 12$).

Often a few select rows partition the greedy orbit.

Problem

Let S be a Bol loop. Consider greedy orbits of $\langle R_x;\ x \in S\rangle$ in a Bol loop Q.

- *Are all greedy orbits finite?*
- *Are all greedy orbits actually orbits?*
- *Is the length of greedy orbits divisible by $|S|$?*

Enumeration of centrally nilpotent loops

Enumeration of loops

Enumerations are usually considered up to

- isomorphism, a permutation of rows, columns and symbols by the same permutation
- isotopism, a permutation of rows, columns and symbols by three permutations (carefully with 1!)
- paratopism (or main classes), an isotopism plus a permutation of the roles of rows, columns and symbols

Note: Isotopic groups are already isomorphic.

Loops up to isomorphism

[McKay, Meynert, Myrvold 2005] for $8 \leq n \leq 10$
[Hulpke, Kaski, Östergård 2011] for $n = 11$

---

n	loops
4	2
5	6
6	109
7	$23,746$
8	$106,228,849$
9	$9,365,022,303,540$
10	$20,890,436,195,945,769,617$
11	$1,478,157,455,158,044,452,849,321,016$

Centrally nilpotent loops

A loop Q is centrally nilpotent if the series

$$Q, \quad Q/Z(Q), \quad (Q/Z(Q))/Z(Q/Z(Q)), \ldots$$

terminates with $\{1\}$ in finitely many steps.

Theorem

Let p be a prime. Then

- *groups of order p^k are centrally nilpotent*
- *Moufang loops of order p^k are centrally nilpotent* [Glauberman, Wright 1968]
- *Bol loops of order p^k are not necessarily centrally nilpotent* [Foguel, Kinyon 2010]

Central extensions

A loop Q is a central extension of Z by F if

$$Z \leq Z(Q) \text{ and } Q/Z \cong F.$$

Write $Z = (Z, +, 0)$ and $F = (F, \cdot, 1)$.

Theorem

A loop Q is a central extension of Z by F if and only if Q is isomorphic to the loop $\mathcal{Q}(\theta)$ defined on $F \times Z$ by

$$(x, a) * (y, b) = (xy,\ a + b + \theta(x, y)),$$

where $\theta : F \times F \to Z$ is a (loop) cocycle, that is, it satisfies

$$\theta(1, x) = \theta(x, 1) = 0$$

for all $x \in F$.

Cocycles and coboundaries

Suppose from now on that $Z = \mathbb{F}_p$ is a prime field.

The cocycles $F \times F \to Z$ form a vector space $C(F, Z)$ over $\mathbb{F}_p$.

Take any mapping $\tau : F \to Z$ such that $\tau(1) = 0$, and define

$$\widehat{\tau} : F \times F \to Z, \quad \widehat{\tau}(x, y) = \tau(xy) - \tau(x) - \tau(y).$$

Then $\widehat{\tau}$ is a cocycle called coboundary.

The coboundaries form a subspace $B(F, Z)$ of $C(F, Z)$.

Equivalences on cocycles

Theorem

For θ, $\mu \in C(F, Z)$, if $\theta - \mu \in B(F, A)$ then $\mathcal{Q}(\theta) \cong \mathcal{Q}(\mu)$.

Theorem

For $(\alpha, \beta) \in \mathrm{Aut}(F) \times \mathrm{Aut}(Z)$ and for $\theta \in C(F, Z)$ define

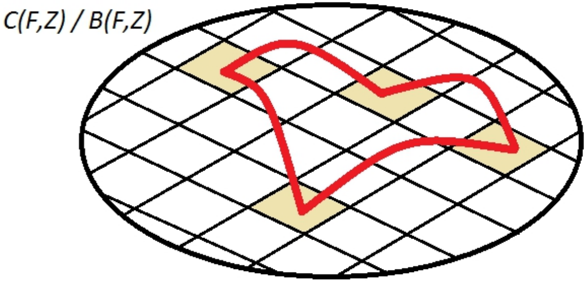
$$\theta^{(\alpha,\beta)} : F \times F \to Z, \quad \theta^{(\alpha,\beta)}(x, y) = \beta(\theta(\alpha^{-1}(x), \alpha^{-1}(y))).$$

Then $\theta^{(\alpha,\beta)} \in C(F, A)$ and $\mathcal{Q}(\theta) \cong \mathcal{Q}(\theta^{(\alpha,\beta)})$.

This defines an action of $\mathrm{Aut}(F) \times \mathrm{Aut}(Z)$ on $C(F, Z)$, in fact on $C(F, Z)/B(F, Z)$.

The equivalence $\equiv$

Let $\equiv$ be the closure of the two equivalences. Then $\equiv$ can be seen as an equivalence relation on isomorphism classes.



The trouble is that distinct equivalence classes of $\equiv$ can yield the same isomorphism type of loops. Understanding $\equiv$ is the isomorphism problem for centrally nilpotent loops.

Cocycles in varieties

Cocycles and coboundaries restrict well to varieties.

Recall $(x, a) * (y, b) = (xy, a + b + \theta(x, y))$.

property	equivalent cocycle condition
commutativity	$\theta(x, y) = \theta(y, x)$
associativity	$\theta(x, y) + \theta(xy, z) = \theta(y, z) + \theta(x, yz)$
Moufang	$\theta(x, y) + \theta(xy, z) + \theta((xy)z, y)$ $= \theta(z, y) + \theta(y, zy) + \theta(x, y(zy))$
etc.	

Enumeration of nilpotent loops in varieties

- a cocycle $\theta : F \times F \to Z$ is given by $|F|^2$ variables $\theta(x, y)$
- a cocycle condition yields several linear equations on θ, for instance, associativity $\theta(x, y) + \theta(xy, z) = \theta(y, z) + \theta(x, yz)$ is equivalent to $|F|^3$ linear equations
- the resulting system of linear equations is sparse and can be calculated with efficiently
- solving the system yields a subspace of all cocycles in a given variety
- the equivalence $\equiv$ can be used to replace the subspace with a smaller set of isomorphism classes
- without additional ideas, the rest is a direct isomorphism check

Enumeration of small Moufang loops

[Chein 1978, Goodaire, May, Raman 1999] for $n \leq 63$
[Nagy, V 2007] for $n = 64, 81$
[Slattery, Zenisek 2011] for $n = 243$

---

n	groups	nonassociative Moufang loops
12	5	1
$\vdots$		
32	51	71
$\vdots$		
64	267	$4,262$
81	15	5
243	67	72

Spectrum of Moufang loops

For which orders n is there a nonassociative Moufang loop?

- none of order p, p^2, p^3
- none of order p^4 unless $p \in \{2, 3\}$
- precisely 4 of order p^5 if $p > 3$ [NAGY, VALSECCHI 2007]
- of even order $2m$ iff there is a nonabelian group of order m [CHEIN, RAJAH 2003]

Much more is known but the problem is open in general.

Separability

... returning to enumeration of general nilpotent loops:

Call $C(F,Z)$ separable if the isomorphism classes coincide with the equivalence classes of $\equiv$.

In the separable case, the number of isomorphism classes is the number of orbits of the action of $\mathrm{Aut}(F) \times \mathrm{Aut}(Z)$ on $C(F,Z)/B(F,Z)$.

For instance, if $Z = \mathbb{F}_p$, then Q with $|Q| = pq$ or $[Q : Z(Q)] = 2$ are separable.

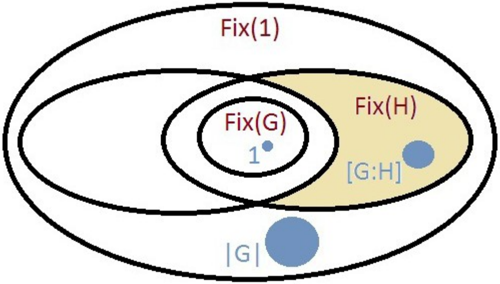
Counting orbits

$G = \mathrm{Aut}(F) \times \mathrm{Aut}(Z)$, $H \leq G$

$\mathrm{Fix}(H) = \{\theta \in C(F,Z);\ \theta^h - \theta \in B(F,Z)$ for all $h \in H\}$

Orbits in $\mathrm{Fix}^*(H) = \mathrm{Fix}(H) \setminus \bigcup_{K>H} \mathrm{Fix}(K)$ have size $[G:H]$.

They can thus be counted by the inclusion-exclusion principle, if we know how big the fixed spaces are.



The separability formula

Theorem (Daly, V 2009)

Let F be a loop and Z an abelian group, $G = \mathrm{Aut}(F) \times \mathrm{Aut}(Z)$. Suppose that $C(F, Z)$ is separable. Then there are

$$\sum_H \frac{|\mathrm{Fix}^*(H)|}{|B(F,A)| \cdot [N_G(H) : H)]}$$

central extensions of Z by F up to isomorphism, where the summation runs over all subgroups $H \leq G$ up to conjugacy.

To determine the dimensions of the fixed spaces, calculate kernels of the linear operators

$$\theta \mapsto \theta - \theta^{(\alpha,\beta)}.$$

Some situations can be handled theoretically:

Centrally nilpotent loops of order $2q$

$N(n)$ = number of nilpotent loops of order n up to isomorphism.

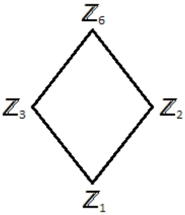
Theorem (Daly, V 2009)

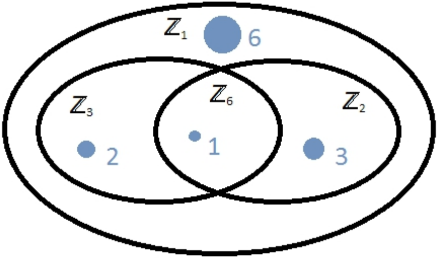
Let q be an odd prime. For an integer d, let $\mathrm{MaxDiv}(d)$ be the maximal proper divisors of d. Then

$$N(2q) = \sum_{d|q-1} \frac{1}{d}\left(2^{(q-2)d} + \sum_{\emptyset \neq D \subseteq \mathrm{MaxDiv(d)}} (-1)^{|D|} \cdot 2^{(q-2)\,\mathrm{gcd}(D)}\right).$$

In particular, $N(2q) \sim \frac{2^{(q-2)(q-1)}}{q-1}$.

Example: $N(14) = N(2 \cdot 7)$





$$\frac{1}{6}(2^{5\cdot 6} - 2^{5\cdot 3} - 2^{5\cdot 2} + 2^{5\cdot 1}) + \frac{1}{3}(2^{5\cdot 3} - 2^{5\cdot 1}) + \frac{1}{2}(2^{5\cdot 2} - 2^{5\cdot 1}) + \frac{1}{1}2^{5\cdot 1}$$

$N(14) = 178,962,784$

Small cases, $n \neq p, 2p$

[Daly, V 2009]

n	centrally nilpotent loops up to isomorphism
8	139
9	10
12	2, 623, 755
15	66, 630
16	466, 409, 543, 467, 341
18	157, 625, 998, 010, 363, 396
20	4, 836, 883, 870, 081, 433, 134, 085, 047
21	17, 157, 596, 742, 633
22	123, 794, 003, 928, 541, 545, 927, 226, 368
24	?

Existence of simple automorphic loops

Automorphic loops

A loop Q is automorphic if $\mathrm{Inn}(Q) \leq \mathrm{Aut}(Q)$.

Note: $\mathrm{Inn}(Q) = \langle L_{x,y},\ R_{x,y},\ T_x;\ x,\ y \in Q \rangle$, where

$$\begin{aligned} L_{x,y} &= L_{yx}^{-1} L_y L_x, \\ R_{x,y} &= R_{xy}^{-1} R_y R_x, \\ T_x &= L_x^{-1} R_x. \end{aligned}$$

Automorphic loops include groups, commutative Moufang loops, and several other varieties of loops.

Theorem (Kinyon, Kunen, Phillips 2002)

Diassociative automorphic loops are Moufang.

Primitive groups

A group G acts primitively on X if no nontrivial partition of X is invariant under G. The degree of G is the cardinality of X.

2-transitive groups $\subseteq$ primitive groups $\subseteq$ transitive groups.

A library of all primitive groups of order $n < 2,500$ is available in GAP.

Theorem (ALBERT 1943)

A loop Q is simple iff $\mathrm{Mlt}(Q)$ acts primitively on Q.

Naive search for simple loops, groups

Let G be a pritimive group on a set Q.

To construct all simple loops with $\mathrm{Mlt}(Q) = G$, it suffices to find all subsets

$$\mathcal{R} = \{r_x;\ x \in Q\},$$

where $r_x(1) = x$, $r_1 = \mathrm{id}_Q$,

$$r_x r_y^{-1} \text{ is fixed-point free for } x \neq y, \qquad (*)$$

and then check that the resulting Latin square has $\mathrm{Mlt}(Q) = G$.

This is impossible already for very small orders.

Theorem (Cameron 1992)

As $n \to \infty$, the probability that a random loop Q of order n satisfies $\mathrm{Mlt}(Q) = S_n$ or $\mathrm{Mlt}(Q) = A_n$ approaches 1.

Right translations of automorphic loops

Let $G = \mathrm{Mlt}(Q)$, $H = \mathrm{Inn}(Q) = G_1$.

Lemma

Q is automorphic iff $hR_x h^{-1} = R_{h(x)}$ for every $x \in Q$, $h \in H$.

Proof.

The following are equivalent (with y universally quantified):

$$\begin{aligned} hR_x h^{-1}(y) &= R_{h(x)}(y), \\ h(h^{-1}(y)x) &= yh(x), \\ h(yx) &= h(y)h(x). \end{aligned}$$

$\square$

Lemma

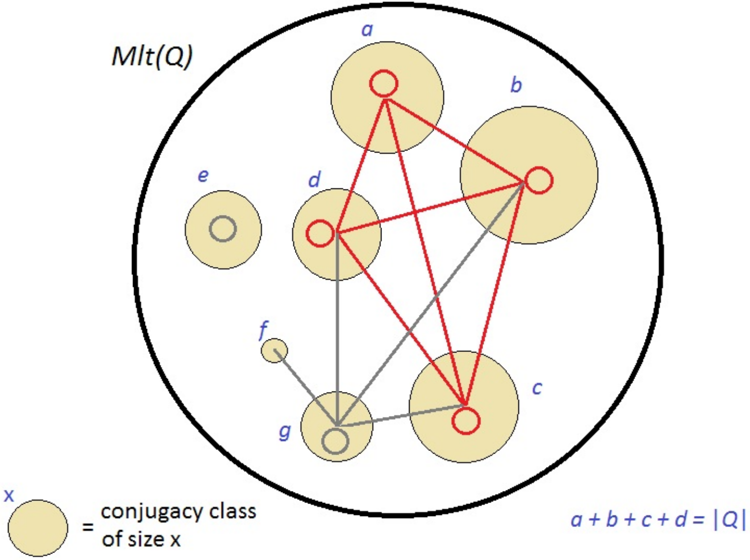
In an automorphic loop Q, R_x commutes with all elements of the stabilizer H_x.

Constructing all finite simple automorphic loops

Constructing the sets $\mathcal{R} = \{r_x;\ x \in Q\} \subseteq G$:

- we know where to start: $r_x \in C_G(H_x)$
- we must include entire conjugacy classes
- call two conjugacy classes A, B (possibly the same) compatible if ab^{-1} is fixed-point free for $a \in A$, $b \in B$, $a \neq b$
- construct a vertex-labeled graph Γ:
  vertices: self-compatible conjugacy classes
  edges: defined by compatibility
  label: the size of conjugacy class.
- find all cliques in Γ with vertex sum equal to $|Q|$
- keep cliques that yield loops with $\mathrm{Mlt}(Q) = G$

The algorithm



Restricting the primitive groups in the search

Lemma

If Q is an automorphic loop then $\mathrm{Mlt}(Q)$ cannot be 4-transitive.

Theorem (Vesanen 1996)

If $\mathrm{Mlt}(Q)$ is solvable then Q is solvable.

We can therefore skip solvable and highly transitive primitive groups. Generally speaking, if A_n, S_n cannot be excluded, the situation is hopeless.

Theorem (Johnson, Kinyon, Nagy, V 2011)

There are no nonassociative simple automorphic loops of order less than $2,500$.

Structural results on automorphic loops

Using Lie algebras:

Theorem (GRISHKOV, KINYON, NAGY 2011)

There are no finite simple nonassociative commutative automorphic loops.

Theorem (KINYON, KUNEN, PHILLIPS, V 2011)

Automorphic loops of odd order are solvable.

More results on automorphic loops

Using derived operations:

Theorem (JEDLIČKA, KINYON, V 2010)

Let p be an odd prime. Commutative automorphic loops of order p^k are centrally nilpotent. There is an automorphic loop of order p^3 with trivial center.

Using $\mathbb{Z}_p$-modules:

Theorem (BARROS, GRISHKOV, V 2011)

For every prime p there are precisely 7 commutative automorphic loops of order p^3 up to isomorphism.

Loops with commuting inner mappings

Nilpotency class

Nilpotency class $\mathrm{cls}(Q)$ is the length of the upper-central series. Thus:

$\mathrm{cls}(Q) = 1$ if Q is an abelian group

$\mathrm{cls}(Q) = 2$ if $Q/Z(Q)$ is an abelian group but Q is not

$\dots$

Theorem

Let Q be a group. Then $Q/Z(Q) \cong \mathrm{Inn}(Q)$. In particular, $\mathrm{Inn}(Q)$ is abelian iff $\mathrm{cls}(Q) \leq 2$.

Theorem (Bruck)

Let Q be a loop. If $\mathrm{cls}(Q) \leq 2$ then $\mathrm{Inn}(Q)$ is abelian.

First examples

If $\mathrm{Inn}(Q)$ is abelian, what can be said about $\mathrm{cls}(Q)$?

Theorem (Niemenmaa, Kepka 1994)

If Q is finite with $\mathrm{Inn}(Q)$ abelian then Q is centrally nilpotent.

[Csörgő 2007] obtained an ad hoc example of a loop Q (of order 128) such that $\mathrm{Inn}(Q)$ is abelian and $\mathrm{cls}(Q) = 3$.

[Drápal, V 2008] constructed many such examples systematically. The construction is ultimately based on the determinant and the way it controls the associator mapping. (It looks like $|Q| \geq 128$ is necessary.)

[Nagy, V 2009] a Moufang example of order 2^{14}

First human results

Theorem (Csörgő, Drápal 2005)
Let Q be a loop where left translations form a set closed under conjugation. If $\mathrm{Inn}(Q)$ is abelian then $\mathrm{cls}(Q) \leq 2$.

Theorem (Nagy, V 2009)
If Q is a uniquely 2-divisible (that is, $x \mapsto x^2$ is a bijection) Moufang loop with $\mathrm{Inn}(Q)$ abelian then $\mathrm{cls}(Q) \leq 2$.

Inhuman results

Theorem (Phillips, Stanovský 2010)

Let Q be a Bol loop such that $(xy)^{-1} = x^{-1}y^{-1}$. If $\mathrm{Inn}(Q)$ is abelian then $\mathrm{cls}(Q) \le 2$.

Proof.

$16,000$ clauses in Waldmeister $=$ $1,068$ pages of pdf output

1068

Theorem 1: $unit() = asoc(asoc(a(), b(), c()), d(), e())$

$$\underbrace{unit()}$$

$=$ by Lemma 2840 RL with $\{x5 \leftarrow e(), x4 \leftarrow c(), x3 \leftarrow a(), x2 \leftarrow b(), x1 \leftarrow d()\}$

$$\underbrace{\overbrace{asoc(d(), asoc(b(), a(), c()), e())}}$$

$=$ by Lemma 2785 LR with $\{x5 \leftarrow e(), x3 \leftarrow c(), x2 \leftarrow a(), x1 \leftarrow b(), x4 \leftarrow d()\}$

$$\underbrace{\overbrace{asoc(d(), rd(d(), asoc(a(), b(), c())), e())}}$$

$=$ by Lemma 2726 LR with $\{x3 \leftarrow e(), x2 \leftarrow asoc(a(), b(), c()), x1 \leftarrow d()\}$

$$\overbrace{asoc(asoc(a(), b(), c()), d(), e())}$$

$\square$

More inhuman results

Similar results were obtained with Prover9, mainly by Veroff.

Theorem (Kinyon, Veroff, V 2011)
Let Q be a Moufang loop with $\mathrm{Inn}(Q)$ abelian. Then $\mathrm{cls}(Q) \leq 3$.

Theorem (Kinyon, Veroff 2011)
Let Q be a Bol loop with $\mathrm{Inn}(Q)$ abelian. Then $\mathrm{cls}(Q) \leq 3$.

The proofs are probably longest ever produced by automated deduction: $20,000$–$30,000$ clauses.

Syntax of the problem - easy!

Suppose we want to prove with Prover9:
If Q is a group and $\mathrm{Inn}(Q)$ is abelian then $\mathrm{cls}(Q) \leq 2$.

```
% assumptions
1*x=x.
x*1=x.
x*x'=1.
x'*x=1.
x*(y*z) = (x*y)*z.
T(x,y) = x'*(y*x).
T(z,T(x,y)) = T(x,T(z,y)).
comm(x,y) = (y*x)'*(x*y).
% goal
comm(x,y)*z = z*comm(x,y).
```

Prover9 finds a proof of length 24 in 0.01 seconds.

Syntax of a loopy example

Here is an input file for the conjecture:
If Q is a loop and $\mathrm{Inn}(Q)$ is abelian then $\mathrm{cls}(Q) \leq 3$.

```
% assumptions
x*1=x. 1*x=x. x\(x*y)=y. x*(x\y)=y. (x*y)/y=x. (x/y)*y=x. % loop
T(x,y) = x\(y*x). % conjugations
L(x,y,z) = (y*x)\(y*(x*z)). % left inner mappings
R(x,y,z) = ((z*x)*y)/(x*y) = z. % right inner mappings
T(x,T(y,z)) = T(y,T(x,z)). % Inn(Q) abelian
T(x,L(y,z,u)) = L(y,z,T(x,u)).
T(x,R(y,z,u)) = R(y,z,T(x,y)).
L(x,y,L(z,u,v)) = L(z,u,L(x,y,v)).
L(x,y,R(z,u,v)) = R(z,u,L(x,y,v)).
R(x,y,R(z,u,v)) = R(z,u,R(x,y,v)).
assc(x,y,z) = (x*(y*z))\((x*y)*z). % associators
comm(x,y,z) = (y*x)\(x*y). % commutators

% goal (one of many, prove them one by one)
% this one says: [x,[y,z,u]] commutes with all elements
comm(x,assc(y,z,u))*v = v*comm(x,assc(y,z,u)).
```

Coaxing the proof out - not so easy!

In Prover9 power users apply three techniques, in addition to the tweaking of technical parameters of the search:

- hints: provide the prover with clauses from proofs of similar results, and ask the prover to give such clauses priority in the search
- sketches: prove a weaker theorem with (several) extra assumptions, then use the proof as hints for the next round where an assumption has been removed; repeat
- semantic guidance: generate examples (by finite model builder), sort clauses by true/false on examples, use these to construct a bidirectional proof (by contradition)

Automated deduction in loop theory

Automated deduction often provides a key technical step in a high-level proof. For instance, while proving . . .

Theorem (Decomposition for comm. automorphic loops)

A finite commutative automorphic loop is a direct product of a loop of odd order and a loop of order a power of 2.

. . . we needed to show that a product of two squares is a square. Prover9 discovered that $A^2 * B^2$ is equal to the square of

```
((((((A * A) \ A) * (B * (A * A)))
\ (B * (A * A))) \ 1) * (((((((A * A) \ A) * (B * (A * A))) \ (B * (A *A))) \ 1)
\ ((((A * A) \ A) * ((A * A) \ A)) * (B * (A * A)))) \ 1))
\ ((((((A * A) \ A) * (B * (A * A))) \ (B * (A * A))) \ 1)
* ((((((((A * A) \ A) * (B * (A * A))) \ (B * (A * A))) \ 1)
\ ((((A * A) \ A) * ((A *A) \ A)) * (B * (A * A)))) \ 1)
* ((((((A * A) \ A) * (B * (A * A)))
\ (B * (A * A))) \ 1) \ ((((A * A) \ A) * ((A * A) \ A)) * (B * (A * A))))))
```

The End