LOOPS: Computing with quasigroups and loops in GAP

GAP Workshop 2007, Braunschweig

Gábor P. Nagy (nagyg@math.u-szeged.hu) and
Petr Vojtěchovský (Univ Denver, CO)

September 15, 2007

Overview

Loops and quasigroups

Permutation groups associated to loops

Presentation of loops

The isomorphism problem for loops

TODOs

Basic concepts

Definition: Quasigroup and loop

The set Q endowed with a binary operation "$\cdot$" is a quasigroup provided for all $a, b \in Q$, the equations

$$a \cdot x = b, \qquad y \cdot a = b$$

have unique solutions $x = a \backslash b, y = b/a$.
A quasigroup with a distinguished element e satisfying

$$e \cdot x = x \cdot e = x$$

is a loop.

Roughly speaking, a loop is a non-associative group.

My favorite example

Example

$\cdot$	1	2	3	4	5
1	1	2	3	4	5
2	2	1	5	3	4
3	3	5	4	2	1
4	4	3	1	5	2
5	5	4	2	1	3

- $2 \cdot 2 = 1$, Lagrange's theroem does not hold.
- $3 \cdot (3 \cdot 3) \neq (3 \cdot 3) \cdot 3$, the order of elements is not well defined.
- Finite quasigroups are Latin squares. Finite loops are normalized Latin squares.

Some concepts from group theory

- Subloop, homomorphism.
- Normal subloop: $K \leq Q$ satisfying

$$xK = Kx, x(yK) = (xy)K, x(Ky) = (xK)y, K(xy) = (Kx)y.$$

- Factor loop, solvability, simple loop.
- Commutator $[x, y]$ and associator (x, y, z) elements. Commutator and associator subloops.
- Center, central nilpotence. There is a non-associative centrally nilpotent loop of order 6.
- Nuclei.

Multiplication maps

- In a quasigroup, the left and right multiplication maps

$$xL_a = a \cdot x, \qquad xR_a = x \cdot a$$

  are bijections.
- The set

$$\mathrm{RSec}(Q) = \{R_x \mid x \in Q\}$$

  of right multiplication maps is the right section of Q.
- In our favorite example:

$$\begin{array}{ccccc} 1 & 2 & 3 & 4 & 5 \\ 2 & 1 & 5 & 3 & 4 \\ 3 & 5 & 4 & 2 & 1 \\ 4 & 3 & 1 & 5 & 2 \\ 5 & 4 & 2 & 1 & 3 \end{array} \qquad \left.\begin{array}{l} () \\ (12)(354) \\ (13425) \\ (14523) \\ (15324) \end{array}\right\} \begin{array}{c} \text{sharply transitive} \\ \text{set of permutations} \end{array}$$

Multiplication groups of loops

Let Q be a loop. (Similar for quasigroups but less interesting.)

- The right multiplication group

$$\mathrm{RMlt}(Q) = \langle R_x \mid x \in Q \rangle$$

  generated by the right multiplication maps is a transitive permutation group on Q.
- The multiplication group $\mathrm{Mlt}(Q)$ is generated by all left and right multiplication maps.
- The stabilizer of 1 in the (right) multiplication group is the (right) inner mapping group $\mathrm{Inn}(Q)$ ($\mathrm{RInn}(Q)$).
- Problem for GAP: Too many generators for $\mathrm{RMlt}(Q)$ and $\mathrm{Mlt}(Q)$.

Some structure theorems on loops and multiplication groups

Theorem
$Z(Q) \cong Z(\mathrm{Mlt}(Q))$.

Theorem
The normal subloops of Q are precisely the imprimitivity blocks of $\mathrm{Mlt}(Q)$ containing 1. In particular, Q is simple if and only if $\mathrm{Mlt}(Q)$ is primitive.

Remark. Unfortunately, no similar result for $\mathrm{RMlt}(Q)$ in general. For special loop classes: yes.

Presentation of loops

Let Q be a loop of order n.

- Currently, we define loops by their Cayley table. This needs $4n^2$ bytes. The left and right sections are attributes.
- We will soon switch to a definition by left and right sections and forget about Cayley tables.
- The future is to use connected transversals. This will enable us to work with "huge" loops in pc groups and matrix groups.

Definition: Connected transversals

Let G be a group, H a subgroup, A, B transversals of H in G. A, B are connected transversals if $[a, b] \in H$ for all $a \in A$, $b \in B$.

Remark. The left and right sections are connected transversals in $\mathrm{Mlt}(Q)$ to $\mathrm{Inn}(Q)$.

The Baer correspondence

- Loops can be defined by right sections, that is, by sharply transitive sets of permutations containing 1.
- An abstract group theoretical formulation of the concept of sharply transitive permutation sets is the following:

Definition: Loop folders

The triple (G, H, K) is a loop folder if

  - G is a group, $H \leq G$, $K \subseteq G$ and $1 \in K$.
  - K is a transversal of each conjugate of H is G.

- This presentation is useful for loop classes where the multiplication on the right behaves good and on the left behaves bad.

Classification of small loops, libraries

The package LOOPS contains the following libraries:

- Moufang loops of order ≤ 64. There are 4262 non-associative Moufang loops of order 64. (267 groups of this order.)
- Bol loops of order ≤ 16.
- Steiner loops of order ≤ 16.
- All loops of order ≤ 6. Using the package GRAPE, order 7 is easy to do.

Theorem (McKay, Meynert, Myrvold)

The number of loops of order 10 is 20 890 436 195 945 769 617. (20 digits.)

Isomorphism problem of loops

The isomorphism problem is done for power-associative loops.
We find "small" blocks invariant under isomorphism "quickly".

The discriminator stores the following information on the element x:

- What is the order of x?
- How many times is x a square, a fourth power?
- With how many elements of given order does x commute?

Works great for Moufang 2-loops, say.

Fails miserably for Steiner loops: these are commutative loops of exponent 2.

TODO: Improve presentations of loops

TASK: Define polycyclic loops.

DIFFICULTY: In order to compute the product

$$x_1(x_2(\cdots x_n)) \quad \cdot \quad y_1(y_2(\cdots y_n)),$$

we need power, commutator and associator relations. The general theory of associator calculus of loops is not developed yet.

TODO: Interfaces for automated reasoning softwares

The category of loops and quasigroups is espacially suitable for automated theorem proving:

- Rich variety for small orders.
- Combinatorically well structured.
- You can play around with identities using one binary operation.

WORK IN PROGRESS: [M.K. Kinyon, J.D. Phillips]
Interfaces for automated theorem prover Prover9 and model builder software Mace4.

TODO: Improve isomorphisms and automorphisms

TASK: Use existing group isomorphism methods for loop isomorphism problems.

DIFFICULTY: The multiplication groups are too big for a brute force attack.
We needed isomorphism of group extending isomorphism of subgroups.

TASK: Assign graphs to loops and use `nauty`.

DIFFICULTY: Not really. We either have to use the package GRAPE or write our own interface.