

# Quasigroups and Undergraduate Research Projects

Mark Greer

University of North Alabama

MAA Southeast Sectional

25 March 2016

# Groups, Algorithms, Programming (GAP)- a System for Computational Discrete Algebra

[www.gap-system.org](http://www.gap-system.org)

<http://math.slu.edu/~rainbolt/manual8th.htm>

<http://web.cs.du.edu/~petr/loops/>

```

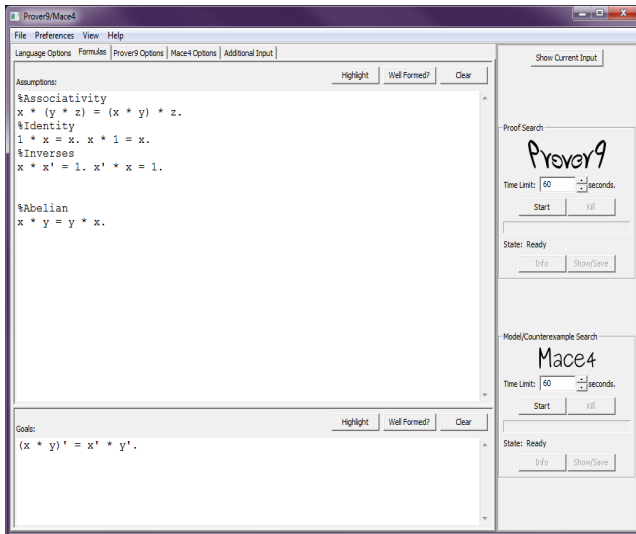
cygdrive/c/gap47/bin/gapx95.exe -l cygdrive/c/gap47
GAP
GAP, Version 4.7.2 of 01-Dec-2013 (free software, GPL)
http://www.gap-system.org
Architecture: i686-pc-cygwin-gcc-default32
Libs used: gmp, readline
Loading the library and packages ...
Components: trans 1.0, prim 2.1, small 1.0, id 1.0
Packages: AClib 1.1, Alnuth 3.0.0, AtlasRep 1.5.0, AutGpG 1.5, Browse 1.8.3, CRISP 1.3.7, Cryst 4.1.12, CrystCat 1.1.6, CtblLib 1.2,
IRREDSOL 1.2.3, LAGUNA 3.6.4, Polenta 1.3.1, Polycyclic 2.11, RadiRoot 2.6, ResClasses 3.3.2, Sophus 1.23, SpinSym 1.5, To
Try 'help' for help. See also 'copyright' and 'authors'
gap> LoadPackage("loops");
=====
LOOPS: Computing with quasigroups and loops in GAP
Gabor P. Nagy and Petr Vojtechovsky
=====
contact: nagy@math.u-szeged.hu or petr@math.du.edu
=====

This version of LOOPS is ready for GAP 4.5.
true
gap> l:=MoufangLoop(12,1);
Moufang loop 12,1:
gap> Display(CayleyTable(L));
[ [ 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12 ],
  [ 2, 1, 4, 3, 6, 5, 8, 7, 12, 11, 10, 9 ],
  [ 3, 6, 5, 2, 1, 4, 9, 10, 11, 12, 7, 8 ],
  [ 4, 5, 6, 1, 2, 3, 10, 9, 8, 7, 12, 11 ],
  [ 5, 4, 1, 6, 3, 7, 11, 12, 7, 8, 9, 10 ],
  [ 6, 3, 2, 5, 4, 1, 12, 11, 10, 9, 8, 7 ],
  [ 7, 8, 11, 10, 9, 12, 2, 1, 5, 6, 3 ],
  [ 8, 7, 12, 9, 10, 11, 2, 1, 4, 5, 6 ],
  [ 9, 12, 7, 8, 11, 10, 3, 4, 1, 6, 5 ],
  [ 10, 11, 8, 7, 12, 9, 4, 1, 6, 5 ],
  [ 11, 10, 9, 12, 7, 8, 5, 6, 3, 2, 1, 4 ],
  [ 12, 9, 10, 11, 8, 7, 6, 5, 2, 3, 4, 1 ] ]
gap>

```

# Prover9-Mace4

<https://www.cs.unm.edu/~mccune/mace4/>



## Definition

A *quasigroup*  $(Q, \cdot)$  is a set  $Q$  with binary operation  $\cdot$  such that for all  $a, b \in Q$ , such that

$$ax = b$$

$$ya = b$$

have unique solutions  $x, y \in Q$ .

**Note:** If  $Q$  has an identity element, it is a *loop*.

## Translations

For a quasigroup  $Q$ , we define the *left* and *right translations* of  $x$  by  $a$  as

$$xL_a = ax \quad xR_a = xa.$$

Since  $Q$  is a quasigroup,  $L_a, R_a$  are bijections for all  $a \in Q$ .

## Examples

(1) Groups.

(2)  $(\mathbb{Z}, -)$  is a quasigroup.

$$2^3 = (2 - 2) - 2 = -2 \neq 2 = 2 - (2 - 2) = 2^3$$

$(Q, \cdot)$	1	2	3
1	2	3	1
2	1	2	3
3	3	1	2

Quasigroup of order 3

$(Q, \cdot)$	1	2	3	4	5
1	1	2	3	4	5
2	2	1	4	5	3
3	3	5	1	2	4
4	4	3	5	1	2
5	5	4	2	3	1

Loop of order 5

## Definition

1	3	2	4
2	4	3	1
3	1	4	2
4	2	1	3

$2 \times 2$  Sudoku sub-blocks

## Properties

Sudoku tables have 3 properties:

Each digit appears exactly once in each row.

Each digit appears exactly once in each column.

Each digit appears exactly once in each sub-block.

$(\mathbb{Z}_4, +)$	0	2	1	3
0	0	2	1	3
1	1	3	2	0
2	2	0	3	1
3	3	1	0	2

$2 \times 2$  Sudoku sub-blocks

$(\mathbb{Z}_4, +)$	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

No Sudoku sub-blocks

## Note

Both multiplication tables are the same and represent  $\mathbb{Z}_4$ .

Note the columns are permuted in order to achieve the Sudoku property.

## Question

Can every “composite” group’s multiplication table be permuted to have the Sudoku property?

**Answer** Yes: “Cosets and Cayley-Sudoku Tables” by Carmichael, Schloeman, and Ward.

The authors gave two constructions based on subgroups, cosets and group transversals.

## Question

Can we extend their ideas to more general Latin squares?

**Yes-ish...**



## Theorem (Carr)

Let  $Q$  be a quasigroup with  $|Q| = k \times l$  and  $H$  a subquasigroup with  $|H| = k$ . Then, if

$$(ah)H = aH,$$

$$H(ha) = Ha,$$

for all  $a \in Q$  and for all  $h \in H$ , then the Cayley table of  $Q$  can be arranged in such a way that it has  $k \times l$  Sudoku sub-blocks.

## Question

Suppose you have a Sudoku quasigroup. Is it related to a group?

$(Q, \cdot)$	0	1	2	3
0	0	2	1	3
1	1	3	2	0
2	2	0	3	1
3	3	1	0	2

$(\mathbb{Z}_4, +)$	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

## Definition

Two quasigroups  $(Q, \cdot)$  and  $(Q, \circ)$  are *isotopic* if there exists  $\alpha, \beta, \gamma$  bijections such that

$$\alpha(x) \cdot \beta(y) = \gamma(x \circ y)$$

for all  $x, y \in Q$ . We write  $(Q, \cdot) \simeq (Q, \circ)$ .

$(Q, \cdot)$	0	1	2	3
0	0	2	1	3
1	1	3	2	0
2	2	0	3	1
3	3	1	0	2

$(\mathbb{Z}_4, +)$	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

## Note

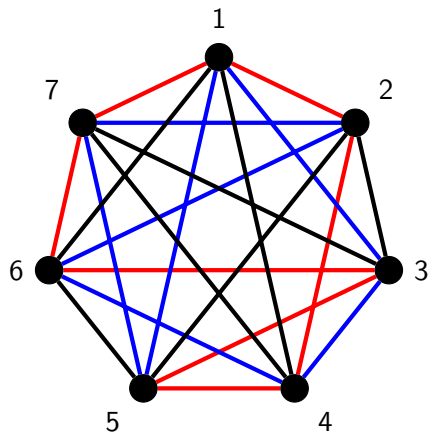
$(Q, \cdot) \simeq (\mathbb{Z}_4, +)$  are isotopic, with  $\alpha = ()$ ,  $\beta = (12)$ ,  $\gamma = ()$

## Theorem (Carr)

If  $Q$  is a Sudoku quasigroup and  $|Q| = 4$ , then  $Q \simeq \mathbb{Z}_4$  or  $\mathbb{Z}_2 \times \mathbb{Z}_2$ .

## Conjecture

Let  $Q$  be a Sudoku quasigroup.  $Q \simeq G$  for some abelian group  $G$  *if and only if*  $Q$  is medial ( $(xy)(zw) = (xz)(yw)$  for all  $x, y, z, w \in Q$ ).



$K_7$  with 3 Hamiltonian Cycles

## Correspondence (Kotzig)

Label the vertices of the graph with the elements of the quasigroup and prescribe that the edges  $(a, b)$  and  $(b, c)$  shall belong to the same closed path if and only if  $a \cdot b = c$ ,  $a \neq b$  where  $a, b, c \in Q$ .

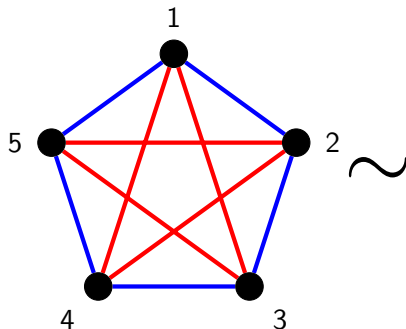
## Definition

A *P-Quasigroup*  $(Q, \cdot)$  is a quasigroup with the three following properties:

$$a \cdot a = a \quad \forall a \in Q \text{ (Idempotence)}$$

$$a \neq b \Rightarrow a \neq a \cdot b \neq b \quad \forall a, b \in Q$$

$$a \cdot b = c \iff c \cdot b = a \quad \forall a, b, c \in Q.$$



$$\sim$$

$(Q, \cdot)$	1	2	3	4	5
1	1	3	5	2	4
2	5	2	4	1	3
3	4	1	3	5	2
4	3	5	2	4	1
5	2	4	1	3	5

## Lemma

Let  $Q_1$  and  $Q_2$  be two P-Groupoids. Then  $Q_1 \cong Q_2$  if and only if the corresponding decompositions of the associated complete graph are isomorphic.

## Theorem (Carr, G.)

Let  $Q$  be the P-Quasigroup corresponding to the Hamiltonian Decomposition of  $K_p$  where  $p$  is an odd prime. Then

$Q$  is medial

$\text{Mlt}_\rho(Q)$ ,  $\text{Mlt}_\lambda(Q)$  are characteristic in  $\text{Mlt}(Q)$

$\text{Aut}(Q) \cong \text{Mlt}(Q)$

$\text{Mlt}_\rho(Q) \cong D_{2p}$

If  $H \leq Q$ , then  $|H|$  divides  $|Q|$



## Zero Knowledge Proof

Prove the validity of a statement, without conveying any information (other than the statement is true).

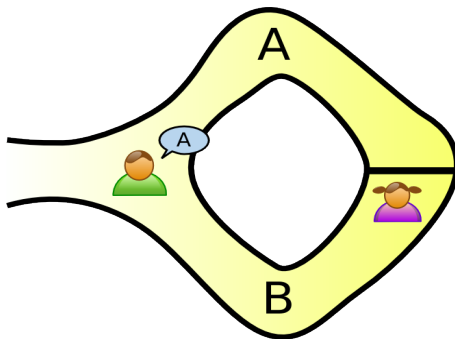


Figure : Source: CC BY 2.5,  
<https://commons.wikimedia.org/w/index.php?curid=313645>

## Algorithm

Public:  $L_1$  &  $L_2$  two latin squares of size  $n \times n$

Private:  $I$  isotopy

- (1) Sender randomly permutes  $L_1$  to produce another latin square  $H$ .
- (2) Sender sends  $H$  to Receiver.
- (3) Receiver asks Sender either to:
  - (a) prove that  $H$  and  $L_1$  are isotopic
  - (b) prove that  $H$  and  $L_2$  are isotopic
- (4) Sender and Receiver repeat steps 1 through 3  $n$  times.

# THANKS!