Quasigroups and Undergraduate Research Projects

Mark Greer

University of North Alabama

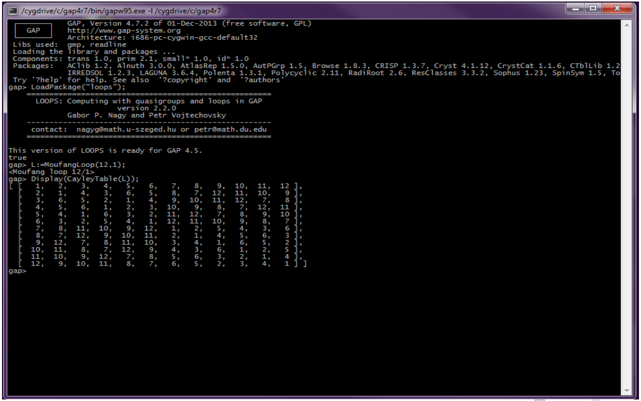
MAA Southeast Sectional
25 March 2016

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

www.gap-system.org

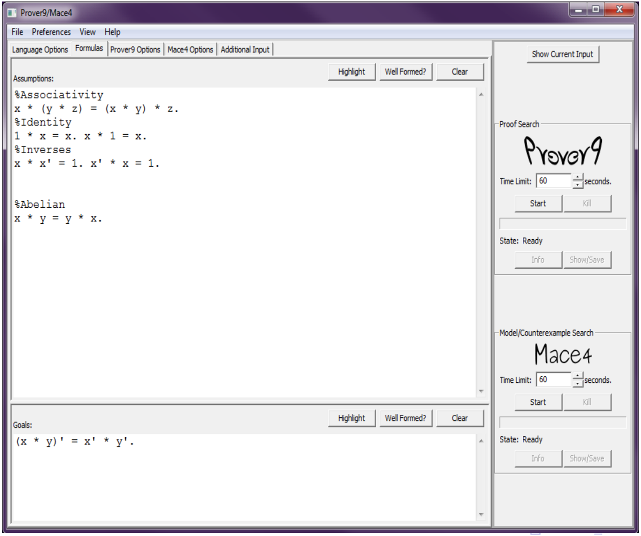
http://math.slu.edu/∼rainbolt/manual8th.htm

http://web.cs.du.edu/∼petr/loops/



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

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

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

2×2 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

2×2 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 α, β, γ 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,·)	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

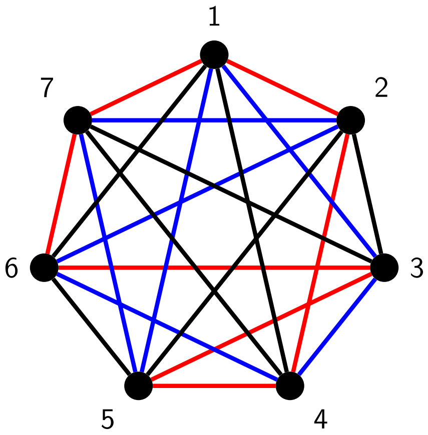
$(Q, \cdot) \simeq (\mathbb{Z}, +)$ are isotopic, with $\alpha = (), \beta = (12), \gamma = ()$

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 $a, b, c \in Q$.

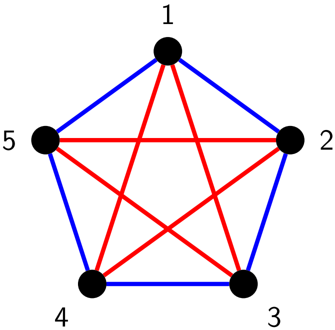
Definition

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

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

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

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



$\sim$

(Q,·)	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
- $\mathrm{Mlt}_\rho(Q)$, $\mathrm{Mlt}_\lambda(Q)$ are characteristic in $\mathrm{Mlt}(Q)$
- $\mathrm{Aut}(Q) \cong \mathrm{Mlt}(Q)$
- $\mathrm{Mlt}_\rho(Q) \cong D_{2p}$
- 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).

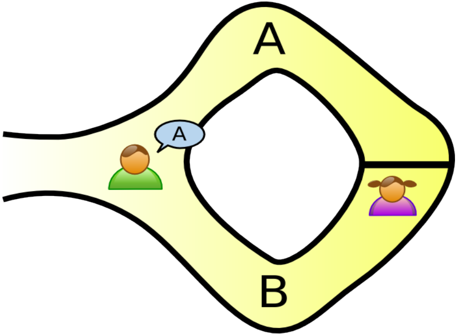


Figure : Source: CC BY 2.5,
https://commons.wikimedia.org/w/index.php?curid=313645

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!