Computer-Aided Investigation of Abstract Algebras

(Or, The Computer Solved My Thesis Problem...)

David Failing

Department of Mathematics
Iowa State University
http://dfailing.public.iastate.edu

Truman State University
March 21, 2013

Outline

Real Numbers

Multiplication in $\mathbb{R}$ is...

- Commutative
  Ex: $2 * 3 = 3 * 2$
- Associative
  Ex: $2 * (3 * 4) = (2 * 3) * 4$
- Anything times 1 is itself.
  Ex: $2 * 1 = 2$
- Every nonzero real number has a multiplicative inverse (in $\mathbb{R}$).
  Ex: $2 * \frac{1}{2} = 1$

Real Numbers

Multiplication in $\mathbb{R}$ is...

- Commutative
  Ex: $2 * 3 = 3 * 2$
- Associative
  Ex: $2 * (3 * 4) = (2 * 3) * 4$
- Anything times 1 is itself.
  Ex: $2 * 1 = 2$
- Every nonzero real number has a multiplicative inverse (in $\mathbb{R}$).
  Ex: $2 * \frac{1}{2} = 1$

Real Numbers

Multiplication in $\mathbb{R}$ is...

- Commutative
  Ex: $2 * 3 = 3 * 2$
- Associative
  Ex: $2 * (3 * 4) = (2 * 3) * 4$
- Anything times 1 is itself.
  Ex: $2 * 1 = 2$
- Every nonzero real number has a multiplicative inverse (in $\mathbb{R}$).
  Ex: $2 * \frac{1}{2} = 1$

Real Numbers

Multiplication in $\mathbb{R}$ is...

- Commutative
  Ex: $2 * 3 = 3 * 2$
- Associative
  Ex: $2 * (3 * 4) = (2 * 3) * 4$
- Anything times 1 is itself.
  Ex: $2 * 1 = 2$
- Every nonzero real number has a multiplicative inverse (in $\mathbb{R}$).
  Ex: $2 * \frac{1}{2} = 1$

Real Numbers

Multiplication in $\mathbb{R}$ is...

- Commutative
  Ex: $2 * 3 = 3 * 2$
- Associative
  Ex: $2 * (3 * 4) = (2 * 3) * 4$
- Anything times 1 is itself.
  Ex: $2 * 1 = 2$
- Every nonzero real number has a multiplicative inverse (in $\mathbb{R}$).
  Ex: $2 * \frac{1}{2} = 1$

Real Numbers

Multiplication in $\mathbb{R}$ is...

- Commutative
  Ex: $2 * 3 = 3 * 2$
- Associative
  Ex: $2 * (3 * 4) = (2 * 3) * 4$
- Anything times 1 is itself.
  Ex: $2 * 1 = 2$
- Every nonzero real number has a multiplicative inverse (in $\mathbb{R}$).
  Ex: $2 * \frac{1}{2} = 1$

Integers

Multiplication in $\mathbb{Z}$ is...

- Commutative
  Ex: $2 * 3 = 3 * 2$
- Associative
  Ex: $2 * (3 * 4) = (2 * 3) * 4$
- Anything times 1 is itself.
  Ex: $2 * 1 = 2$
- Every nonzero integer has a multiplicative inverse (in $\mathbb{R}$).
  Ex: $2 * \frac{1}{2} = 1$

Integers

Multiplication in $\mathbb{Z}$ is...

- Commutative
  Ex: $2 * 3 = 3 * 2$
- Associative
  Ex: $2 * (3 * 4) = (2 * 3) * 4$
- Anything times 1 is itself.
  Ex: $2 * 1 = 2$
- Every nonzero integer has a multiplicative inverse (in $\mathbb{R}$).
  Ex: $2 * \frac{1}{2} = 1$

Integers

Multiplication in $\mathbb{Z}$ is...

- Commutative
  Ex: $2 * 3 = 3 * 2$
- Associative
  Ex: $2 * (3 * 4) = (2 * 3) * 4$
- Anything times 1 is itself.
  Ex: $2 * 1 = 2$
- Every nonzero integer has a multiplicative inverse (in $\mathbb{R}$).
  Ex: $2 * \frac{1}{2} = 1$

Integers

Multiplication in $\mathbb{Z}$ is...

- Commutative
  Ex: $2 * 3 = 3 * 2$
- Associative
  Ex: $2 * (3 * 4) = (2 * 3) * 4$
- Anything times 1 is itself.
  Ex: $2 * 1 = 2$
- Every nonzero integer has a multiplicative inverse (in $\mathbb{R}$).
  Ex: $2 * \frac{1}{2} = 1$

Integers

Multiplication in $\mathbb{Z}$ is...

- Commutative
  Ex: $2 * 3 = 3 * 2$
- Associative
  Ex: $2 * (3 * 4) = (2 * 3) * 4$
- Anything times 1 is itself.
  Ex: $2 * 1 = 2$
- Every nonzero integer has a multiplicative inverse (in $\mathbb{R}$).
  Ex: $2 * \frac{1}{2} = 1$

Integers

Multiplication in $\mathbb{Z}$ is...

- Commutative
  Ex: $2 * 3 = 3 * 2$
- Associative
  Ex: $2 * (3 * 4) = (2 * 3) * 4$
- Anything times 1 is itself.
  Ex: $2 * 1 = 2$
- Every nonzero integer has a multiplicative inverse
  (but it's not in $\mathbb{Z}$!)

How do we "fix" this?

- Define $\equiv_m$ on $\mathbb{Z}$ by $x \equiv_m y \Leftrightarrow m \mid x - y$.
  Say that x and y are equivalent "mod" m.
  Ex: $13 - 7 = 6$, so $13 \equiv_6 7$.
- Define $\mathbb{Z}_m = \mathbb{Z}/\equiv_m = \{\overline{0}, \overline{1}, \ldots, \overline{m-1}\}$
  The set of possible remainders when dividing by m

How do we "fix" this?

- Define $\equiv_m$ on $\mathbb{Z}$ by $x \equiv_m y \Leftrightarrow m \mid x - y$.
  Say that x and y are equivalent "mod" m.
  Ex: $13 - 7 = 6$, so $13 \equiv_6 7$.
- Define $\mathbb{Z}_m = \mathbb{Z}/\equiv_m = \{\overline{0}, \overline{1}, \ldots, \overline{m-1}\}$
  The set of possible remainders when dividing by m

If $x * y = \overline{x * y}$ in $\mathbb{Z}_m$, does every nonzero element have a multiplicative inverse?

In $\mathbb{Z}_6$

$$3 * 0 = 0,\ 3 * 1 = 3,\ 3 * 2 = 0,$$
$$3 * 3 = 3,\ 3 * 4 = 0,\ 3 * 5 = 3$$

Exercise: Every nonzero element of $\mathbb{Z}_m$ has a multiplicative inverse if and only if m is a prime.

If $x * y = \overline{x * y}$ in $\mathbb{Z}_m$, does every nonzero element have a multiplicative inverse?

In $\mathbb{Z}_6$

$$3 * 0 = 0,\ 3 * 1 = 3,\ 3 * 2 = 0,$$
$$3 * 3 = 3,\ 3 * 4 = 0,\ 3 * 5 = 3$$

Exercise: Every nonzero element of $\mathbb{Z}_m$ has a multiplicative inverse if and only if m is a prime.

If $x * y = \overline{x * y}$ in $\mathbb{Z}_m$, does every nonzero element have a multiplicative inverse?

In $\mathbb{Z}_6$

$$3 * 0 = 0,\ 3 * 1 = 3,\ 3 * 2 = 0,$$
$$3 * 3 = 3,\ 3 * 4 = 0,\ 3 * 5 = 3$$

Exercise: Every nonzero element of $\mathbb{Z}_m$ has a multiplicative inverse if and only if m is a prime.

Integers Modulo p

Multiplication in $\mathbb{Z}_5$ is...

- Commutative
  Ex: $2 * 3 = 3 * 2 = 6 \equiv_5 1$
- Associative
  Ex: $2 * (3 * 4) = (2 * 3) * 4 = 24 \equiv_5 4$
- Anything times 1 is itself.
  Ex: $2 * 1 = 2$
- Every nonzero element has a multiplicative inverse.
  Ex: $2 * 3 = 6 \equiv_5 1$

Integers Modulo p

Multiplication in $\mathbb{Z}_5$ is...

- Commutative
  Ex: $2 * 3 = 3 * 2 = 6 \equiv_5 1$
- Associative
  Ex: $2 * (3 * 4) = (2 * 3) * 4 = 24 \equiv_5 4$
- Anything times 1 is itself.
  Ex: $2 * 1 = 2$
- Every nonzero element has a multiplicative inverse.
  Ex: $2 * 3 = 6 \equiv_5 1$

Integers Modulo p

Multiplication in $\mathbb{Z}_5$ is...

- Commutative
  Ex: $2 * 3 = 3 * 2 = 6 \equiv_5 1$
- Associative
  Ex: $2 * (3 * 4) = (2 * 3) * 4 = 24 \equiv_5 4$
- Anything times 1 is itself.
  Ex: $2 * 1 = 2$
- Every nonzero element has a multiplicative inverse.
  Ex: $2 * 3 = 6 \equiv_5 1$

Integers Modulo p

Multiplication in $\mathbb{Z}_5$ is...

- Commutative
  Ex: $2 * 3 = 3 * 2 = 6 \equiv_5 1$
- Associative
  Ex: $2 * (3 * 4) = (2 * 3) * 4 = 24 \equiv_5 4$
- Anything times 1 is itself.
  Ex: $2 * 1 = 2$
- Every nonzero element has a multiplicative inverse.
  Ex: $2 * 3 = 6 \equiv_5 1$

Integers Modulo p

Multiplication in $\mathbb{Z}_5$ is...

- Commutative
  Ex: $2 * 3 = 3 * 2 = 6 \equiv_5 1$
- Associative
  Ex: $2 * (3 * 4) = (2 * 3) * 4 = 24 \equiv_5 4$
- Anything times 1 is itself.
  Ex: $2 * 1 = 2$
- Every nonzero element has a multiplicative inverse.
  Ex: $2 * 3 = 6 \equiv_5 1$

Multiplication in $\mathbb{Z}_5$

Multiplication Table

$*_5$	0	1	2	3	4
0	0	0	0	0	0
1	0	1	2	3	4
2	0	2	4	1	3
3	0	3	1	4	2
4	0	4	3	2	1

GROUP AXIOMS:

Associativity:
$(\forall a, b, c)[(ab)c = a(bc)]$

Identity:
$(\exists e)[ae = ea = a]$

Inverses:
$(\forall a)[aa^{-1} = a^{-1}a = e]$

Multiplication in $\mathbb{Z}_5$

Multiplication Table

$*_5$	0	1	2	3	4
0	0	0	0	0	0
1	0	1	2	3	4
2	0	2	4	1	3
3	0	3	1	4	2
4	0	4	3	2	1

GROUP AXIOMS:

Associativity:

$(\forall a, b, c)[(ab)c = a(bc)]$

Identity:

$(\exists e)[ae = ea = a]$

Inverses:

$(\forall a)[aa^{-1} = a^{-1}a = e]$

Multiplication in $\mathbb{Z}_5$

Multiplication Tables

$*_5$	1	2	3	4
1	1	2	3	4
2	2	4	1	3
3	3	1	4	2
4	4	3	2	1

$*_5$	0
0	0

Abstract vs. Universal Algebra

- **Abstract algebra:** studies properties of axiomatically defined structures arising from concrete objects
  e.g. Groups, rings, fields,...
- **Universal algebra:** studies axiom systems for their own sake.
  e.g. "the theory of groups,"
  What equations are true of all groups?
  Or of certain kinds of groups?
- How can we investigate these?

Abstract vs. Universal Algebra

- **Abstract algebra:** studies properties of axiomatically defined structures arising from concrete objects
  e.g. Groups, rings, fields,...
- **Universal algebra:** studies axiom systems for their own sake.
  e.g. "the theory of groups,"
  What equations are true of all groups?
  Or of certain kinds of groups?
- How can we investigate these?

Abstract vs. Universal Algebra

- **Abstract algebra:** studies properties of axiomatically defined structures arising from concrete objects
  e.g. Groups, rings, fields,...
- **Universal algebra:** studies axiom systems for their own sake.
  e.g. "the theory of groups,"
  What equations are true of all groups?
  Or of certain kinds of groups?
- How can we investigate these?

Prover9 and Mace4

- **Prover9** is an automated theorem prover for first-order and *equational logic*.
- **Mace4** searches for finite models and *counterexamples*.
- **Input:** a set of *assumptions* and one or more *goals*.
- **Output:** either *proofs* of the goals, or *counterexample(s)* where the assumptions are true but the goals are false.

Prover9 and Mace4

- **Prover9** is an automated theorem prover for first-order and *equational logic*.
- **Mace4** searches for finite models and *counterexamples*.
- **Input:** a set of *assumptions* and one or more *goals*.
- **Output:** either *proofs* of the goals, or *counterexample(s)* where the assumptions are true but the goals are false.

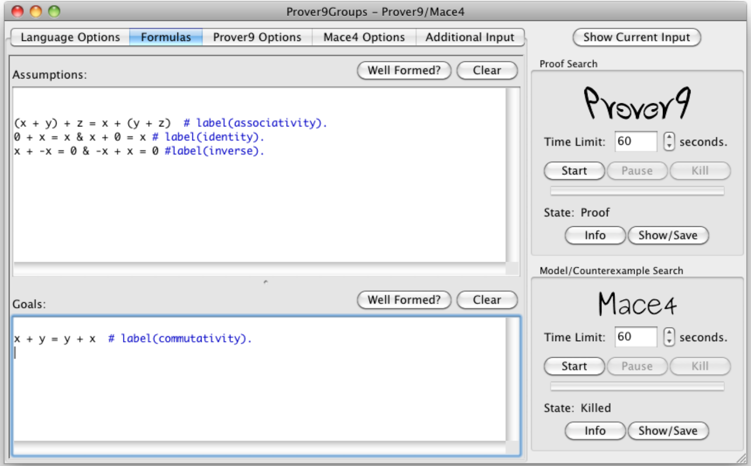
Prover9 and Mace4

- **Prover9** is an automated theorem prover for first-order and *equational logic*.
- **Mace4** searches for finite models and *counterexamples*.
- **Input:** a set of *assumptions* and one or more *goals*.
- **Output:** either *proofs* of the goals, or *counterexample(s)* where the assumptions are true but the goals are false.

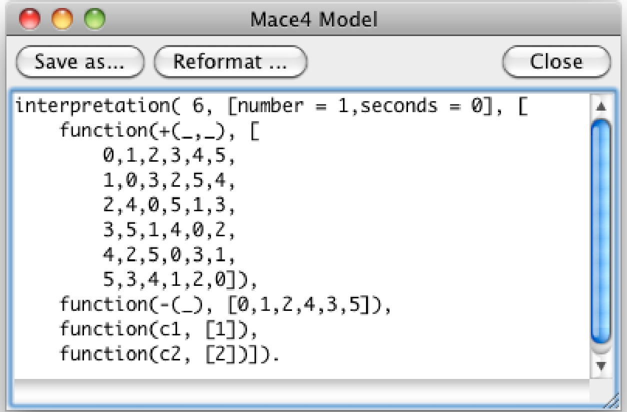
Prover9 and Mace4

- **Prover9** is an automated theorem prover for first-order and *equational logic*.
- **Mace4** searches for finite models and *counterexamples*.
- **Input:** a set of *assumptions* and one or more *goals*.
- **Output:** either *proofs* of the goals, or *counterexample(s)* where the assumptions are true but the goals are false.

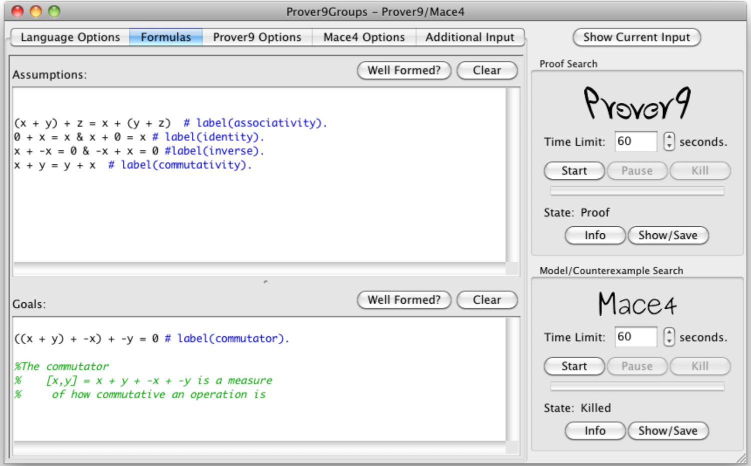
Mace4


Prover9Groups – Prover9/Mace4
Language Options
Formulas
Prover9 Options
Mace4 Options
Additional Input
Show Current Input
Assumptions:
Well Formed?
Clear
(x + y) + z = x + (y + z) # label(associativity).
0 + x = x & x + 0 = x # label(identity).
x + -x = 0 & -x + x = 0 #label(inverse).
Goals:
Well Formed?
Clear
x + y = y + x # label(commutativity).
Proof Search
Prover9
Time Limit: 60 seconds.
Start
Pause
Kill
State: Proof
Info
Show/Save
Model/Counterexample Search
Mace4
Time Limit: 60 seconds.
Start
Pause
Kill
State: Killed
Info
Show/Save

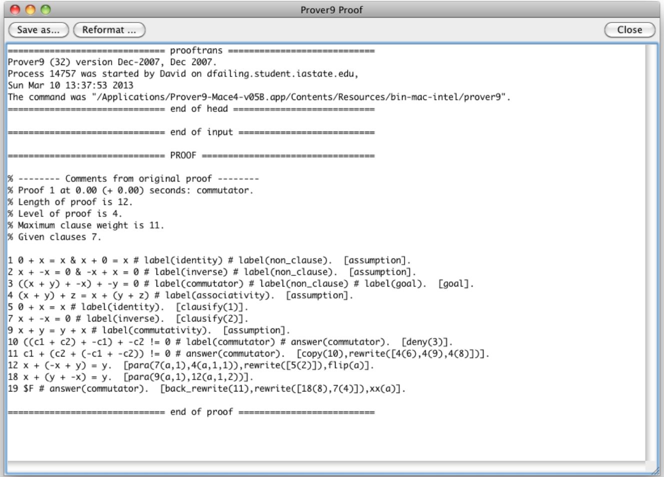
Mace4


Mace4 Model
Save as...
Reformat ...
Close
interpretation(6, [number = 1,seconds = 0], [
function(+(_,_), [
0,1,2,3,4,5,
1,0,3,2,5,4,
2,4,0,5,1,3,
3,5,1,4,0,2,
4,2,5,0,3,1,
5,3,4,1,2,0]),
function(-(_), [0,1,2,4,3,5]),
function(c1, [1]),
function(c2, [2])]).

Prover9


Prover9Groups – Prover9/Mace4
Language Options
Formulas
Prover9 Options
Mace4 Options
Additional Input
Show Current Input
Assumptions:
Well Formed?
Clear
(x + y) + z = x + (y + z) # label(associativity).
0 + x = x & x + 0 = x # label(identity).
x + -x = 0 & -x + x = 0 #label(inverse).
x + y = y + x # label(commutativity).
Goals:
Well Formed?
Clear
((x + y) + -x) + -y = 0 # label(commutator).
%The commutator
%   [x,y] = x + y + -x + -y is a measure
%   of how commutative an operation is
Proof Search
Prover9
Time Limit: 60 seconds.
Start
Pause
Kill
State: Proof
Info
Show/Save
Model/Counterexample Search
Mace4
Time Limit: 60 seconds.
Start
Pause
Kill
State: Killed
Info
Show/Save

Prover9




```
============================== prooftrans ============================
Prover9 (32) version Dec-2007, Dec 2007.
Process 14757 was started by David on dfailing.student.iastate.edu,
Sun Mar 10 13:37:53 2013
The command was "/Applications/Prover9-Mace4-v05B.app/Contents/Resources/bin-mac-intel/prover9".
============================== end of head ===========================

============================== end of input ==========================

============================== PROOF =================================

% -------- Comments from original proof --------
% Proof 1 at 0.00 (+ 0.00) seconds: commutator.
% Length of proof is 12.
% Level of proof is 4.
% Maximum clause weight is 11.
% Given clauses 7.

1 0 + x = x & x + 0 = x # label(identity) # label(non_clause).  [assumption].
2 x + -x = 0 & -x + x = 0 # label(inverse) # label(non_clause).  [assumption].
3 ((x + y) + -x) + -y = 0 # label(commutator) # label(non_clause) # label(goal).  [goal].
4 (x + y) + z = x + (y + z) # label(associativity).  [assumption].
5 0 + x = x # label(identity).  [clausify(1)].
7 x + -x = 0 # label(inverse).  [clausify(2)].
9 x + y = y + x # label(commutativity).  [assumption].
10 ((c1 + c2) + -c1) + -c2 != 0 # label(commutator) # answer(commutator).  [deny(3)].
11 c1 + (c2 + (-c1 + -c2)) != 0 # answer(commutator).  [copy(10),rewrite([4(6),4(9),4(8)])].
12 x + (-x + y) = y.  [para(7(a,1),4(a,1,1)),rewrite([5(2)]),flip(a)].
18 x + (y + -x) = y.  [para(9(a,1),12(a,1,2))].
19 $F # answer(commutator).  [back_rewrite(11),rewrite([18(8),7(4)]),xx(a)].

============================== end of proof ==========================
```

Why Use Software?

- Prover9 and Mace4 are **FAST**, so we can ask a lot of questions of this sort in a reasonable amount of time.
- **REMEMBER**, we can either get proofs of or counterexamples to the *satisfiability of equations*.

Why Use Software?

- Prover9 and Mace4 are **FAST**, so we can ask a lot of questions of this sort in a reasonable amount of time.
- **REMEMBER**, we can either get proofs of or counterexamples to the *satisfiability of equations*.

Definition

A **groupoid** is an algebraic structure $\mathbf{A} = \langle A, * \rangle$ with a single binary operation. Usually, we write xy for $x * y$.

Definition

We call **A** a **CI-groupoid** if $*$ is commutative and idempotent. That is,

$$x * y = y * x$$
$$x * x = x$$

Definition

A **groupoid** is an algebraic structure $\mathbf{A} = \langle A, * \rangle$ with a single binary operation. Usually, we write xy for $x * y$.

Definition

We call $\mathbf{A}$ a **CI-groupoid** if $*$ is commutative and idempotent. That is,

$$x * y = y * x$$
$$x * x = x$$

Definition

A **(join) semilattice** is an **associative** CI-groupoid $S = \langle S, \vee \rangle$.

Definition

Every (join) semilattice determines a partial order relation

$$x \leq_\vee y \Leftrightarrow x \vee y = y.$$

Example

The truth table for "or"

$\vee$	0	1
0	0	1
1	1	1

determines the ordering with $0 \leq 1$.

Definition

A **(join) semilattice** is an **associative** CI-groupoid $S = \langle S, \vee \rangle$.

Definition

Every (join) semilattice determines a partial order relation

$$x \leq_\vee y \Leftrightarrow x \vee y = y.$$

Example

The truth table for "or"

$\vee$	0	1
0	0	1
1	1	1

determines the ordering with $0 \leq 1$.

Definition

A **(join) semilattice** is an **associative** CI-groupoid $S = \langle S, \vee \rangle$.

Definition

Every (join) semilattice determines a partial order relation

$$x \leq_\vee y \Leftrightarrow x \vee y = y.$$

Example

The truth table for "or"

$\vee$	0	1
0	0	1
1	1	1

determines the ordering with $0 \leq 1$.

Weakenings of Associativity

Definition

A groupoid identity $p \approx q$ is of **Bol-Moufang type** if

- the same three variables appear on both sides, in the same order,
- one of the variables appears twice, and
- the remaining two variables appear only once.

Example

The groupoid identity

$$(xx)(yz) = (x(xy))z$$

is of Bol-Moufang type.

Weakenings of Associativity

Definition

A groupoid identity $p \approx q$ is of **Bol-Moufang type** if

- the same three variables appear on both sides, in the same order,
- one of the variables appears twice, and
- the remaining two variables appear only once.

Example

The groupoid identity

$$(xx)(yz) = (x(xy))z$$

is of Bol-Moufang type.

Identities of Bol-Moufang Type (Philips and Vojtěchovský)

A	$xxyz$
B	$xyxz$
C	$xyyz$
D	$xyzx$
E	$xyzy$
F	$xyzz$

1	$o(o(oo))$
2	$o((oo)o)$
3	$(oo)(oo)$
4	$(o(oo))o$
5	$((oo)o)o$

Representable as X_{ij}, the identity with:

- variable order X
- LHS bracketed by i, and RHS bracketed by j.

There are $6 * (4 + 3 + 2 + 1) = 60$ nontrivial such identities.

Identities of Bol-Moufang Type (Philips and Vojtěchovský)

A	$xxyz$
B	$xyxz$
C	$xyyz$
D	$xyzx$
E	$xyzy$
F	$xyzz$

1	$o(o(oo))$
2	$o((oo)o)$
3	$(oo)(oo)$
4	$(o(oo))o$
5	$((oo)o)o$

Representable as X_{ij}, the identity with:

- variable order X
- LHS bracketed by i, and RHS bracketed by j.

There are $6 * (4 + 3 + 2 + 1) = 60$ nontrivial such identities.

Definition

Identities X and Y are **equivalent** relative to a set Σ of axioms when

$$\Sigma \,\&\, X \Leftrightarrow \Sigma \,\&\, Y.$$

Example

$x * y = y * x$ and $x^{-1} * y^{-1} * x * y = 1$ are equivalent, relative to the group axioms of associativity, identity, and inverses.

Problem

Determine which of the Bol-Moufang identities are equivalent for CI-groupoids. (i.e. for $\Sigma = \{x * y = y * x, x * x = x\}$)

Definition

Identities X and Y are **equivalent** relative to a set Σ of axioms when

$$\Sigma \,\&\, X \Leftrightarrow \Sigma \,\&\, Y.$$

Example

$x * y = y * x$ and $x^{-1} * y^{-1} * x * y = 1$ are equivalent, relative to the group axioms of associativity, identity, and inverses.

Problem

Determine which of the Bol-Moufang identities are equivalent for CI-groupoids. (i.e. for $\Sigma = \{x * y = y * x, x * x = x\}$)

Definition

Identities X and Y are **equivalent** relative to a set Σ of axioms when

$$\Sigma \,\&\, X \Leftrightarrow \Sigma \,\&\, Y.$$

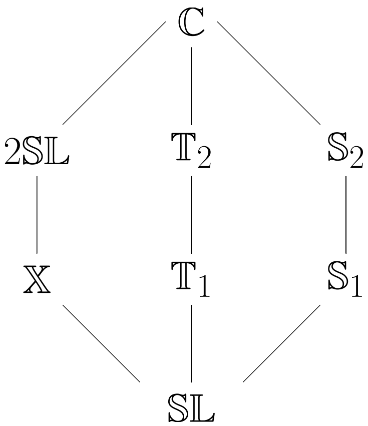
Example

$x * y = y * x$ and $x^{-1} * y^{-1} * x * y = 1$ are equivalent, relative to the group axioms of associativity, identity, and inverses.

Problem

Determine which of the Bol-Moufang identities are equivalent for CI-groupoids. (i.e. for $\Sigma = \{x * y = y * x, x * x = x\}$)

The 8 Varieties of CI-Groupoids of Bol-Moufang Type



The 8 Varieties of CI-Groupoids of Bol-Moufang Type

$\mathbb{C}$	$B45$: $(x(yx))z = ((xy)x)z$
$2\mathbb{SL}$	$A13$: $x(x(yz) = (xx)(yz)$
$\mathbb{X}$	$A24$: $x((xy)z) = (x(xy))z$
$\mathbb{SL}$	$A12$: $x(x(yz)) = x((xy)z)$
$\mathbb{T}_2$	$C15$: $x(y(yz)) = ((xy)y)z$
$\mathbb{T}_1$	$A14$: $x(x(yz)) = (x(xy))z$
$\mathbb{S}_2$	$B12$: $x(y(xz)) = x((yx)z)$
$\mathbb{S}_1$	$B13$: $x(y(xz)) = (xy)(xz)$

The 8 Varieties of CI-Groupoids of Bol-Moufang Type

$\mathbb{C}$	All CI-groupoids
$2\mathbb{SL}$	$x(xy) = xy$
$\mathbb{X}$	$A24$: $x((xy)z) = (x(xy))z$
$\mathbb{SL}$	Semilattices
$\mathbb{T}_2$	$C15$: $x(y(yz)) = ((xy)y)z$
$\mathbb{T}_1$	$A14$: $x(x(yz)) = (x(xy))z$
$\mathbb{S}_2$	$B12$: $x(y(xz)) = x((yx)z)$
$\mathbb{S}_1$	$B13$: $x(y(xz)) = (xy)(xz)$

The 8 Varieties of CI-Groupoids of Bol-Moufang Type

$\mathbb{C}$	All CI-groupoids
$2\mathbb{SL}$	$x(xy) = xy$
$\mathbb{X}$	$A24$: $x((xy)z) = (x(xy))z$
$\mathbb{SL}$	Semilattices
$\mathbb{T}_2$	$C15$: $x(y(yz)) = ((xy)y)z$
$\mathbb{T}_1$	$A14$: $x(x(yz)) = (x(xy))z$
$\mathbb{S}_2$	$B12$: $x(y(xz)) = x((yx)z)$
$\mathbb{S}_1$	$B13$: $x(y(xz)) = (xy)(xz)$

Further Research

- Investigate equivalences in other large families of identities. Generalized Bol-Moufang identities? $\Sigma = \{x * y = y * x\}$? $\Sigma = \{x * x = x\}$?
- Investigate the "(normal) subgroup lattices" of groupoids. The Universal Algebra Calculator (uacalc.org) is good for this.
- Make the UACalc and Prover9/Mace4 *interoperable* using Python and Sage.
- Prover9/Mace4 also do *propositional logic*.

Further Research

- Investigate equivalences in other large families of identities.
  Generalized Bol-Moufang identities?
  $\Sigma = \{x * y = y * x\}$? $\Sigma = \{x * x = x\}$?
- Investigate the "(normal) subgroup lattices" of groupoids.
  The Universal Algebra Calculator (uacalc.org) is good for this.
- Make the UACalc and Prover9/Mace4 *interoperable* using Python and Sage.
- Prover9/Mace4 also do *propositional logic*.

Further Research

- Investigate equivalences in other large families of identities.
  Generalized Bol-Moufang identities?
  $\Sigma = \{x * y = y * x\}$? $\Sigma = \{x * x = x\}$?
- Investigate the "(normal) subgroup lattices" of groupoids.
  The Universal Algebra Calculator (uacalc.org) is good for this.
- Make the UACalc and Prover9/Mace4 *interoperable* using Python and Sage.
- Prover9/Mace4 also do *propositional logic*.

Further Research

- Investigate equivalences in other large families of identities.
  Generalized Bol-Moufang identities?
  $\Sigma = \{x * y = y * x\}$? $\Sigma = \{x * x = x\}$?
- Investigate the "(normal) subgroup lattices" of groupoids.
  The Universal Algebra Calculator (uacalc.org) is good for this.
- Make the UACalc and Prover9/Mace4 *interoperable* using Python and Sage.
- Prover9/Mace4 also do *propositional logic*.


One more thing...

The 8 Varieties of CI-Groupoids of Bol-Moufang Type

$\mathbb{C}$	All CI-groupoids
$2\mathbb{SL}$	$x(xy) = xy$
$\mathbb{X}$	$A24$: $x((xy)z) = (x(xy))z$
$\mathbb{SL}$	Semilattices
$\mathbb{T}_2$	$C15$: $x(y(yz)) = ((xy)y)z$
$\mathbb{T}_1$	$A14$: $x(x(yz)) = (x(xy))z$
$\mathbb{S}_2$	$B12$: x(y(xz))=x((yx)z)
$\mathbb{S}_1$	$B13$: x(y(xz))=(xy)(xz)

Definition

CI-groupoids satisfying $x * (x * y) = y$ are known as Steiner quasigroups (*squags*).

Theorem

Every squag is in $\mathbb{T}_1$.

Proof.

For squags,

$$x * (x * (y * z)) = y * z = (x * (x * y))z$$

so $A14$ holds. □

Definition

CI-groupoids satisfying $x * (x * y) = y$ are known as Steiner quasigroups (*squags*).

Theorem

Every squag is in $\mathbb{T}_1$.

Proof.

For squags,

$$x * (x * (y * z)) = y * z = (x * (x * y))z$$

so $A14$ holds. □

Definition

CI-groupoids satisfying $x * (x * y) = y$ are known as Steiner quasigroups (*squags*).

Theorem

Every squag is in $\mathbb{T}_1$*.*

Proof.

For squags,

$$x * (x * (y * z)) = y * z = (x * (x * y))z$$

so $A14$ holds. □

Definition

Given

- $\mathbf{S} = \langle S, \vee \rangle$ a semilattice,
- $\{\mathbf{A}_s \mid s \in S\}$ a set of groupoids, and
- $\{\phi_{s,t} : \mathbf{A}_s \to \mathbf{A}_t \mid s \leq_\vee t\}$ a set of homomorphisms,

the **Płonka sum** over S of the groupoids $\{\mathbf{A}_s : s \in S\}$ is the groupoid $\mathbf{A}$ with universe $\dot{\bigcup}_{s \in S} A_s$ and multiplication given by:

$$x_1 *^{\mathbf{A}} x_2 = \phi_{s_1,s}(x_1) *^{\mathbf{A}_s} \phi_{s_2,s}(x_2)$$

where $x_i \in \mathbf{A}_{s_i}$, $s = s_1 \vee s_2$.

Constructing $\mathbb{Z}_5$

Multiplication Tables

$*_5$	1	2	3	4
1	1	2	3	4
2	2	4	1	3
3	3	1	4	2
4	4	3	2	1

$*_5$	0
0	0

$\vee$	0	1
0	0	1
1	1	1

Constructing $\mathbb{Z}_5$

Multiplication Table

$*_5$	0	1	2	3	4
0	0	0	0	0	0
1	0	1	2	3	4
2	0	2	4	1	3
3	0	3	1	4	2
4	0	4	3	2	1

$\mathbb{Z}_5$ is the Płonka sum of
$\mathbf{A}_0 = \langle \{1, 2, 3, 4\}, *_5 \rangle$ and
$\mathbf{A}_1 = \langle \{0\}, *_5 \rangle$,
over the "or" semilattice.

Płonka's Theorem

Let **V** be the variety defined by $\Sigma \cup \{x \vee y = x\}$ for some set Σ of regular identities, and $x \vee y$ a composite operation. The following classes of algebras coincide:

1. The class Pł(**V**) of Płonka sums of groupoids from **V**.
2. The class of groupoids defined by Σ and the identities:

$$
\begin{aligned}
x \vee x &= x \\
(x \vee y) \vee z &= x \vee (y \vee z) \\
x \vee y \vee z &= x \vee z \vee y \\
x \vee (y * z) &= x \vee y \vee z \\
(x * y) \vee z &= (x \vee z) * (y \vee z)
\end{aligned}
$$

Theorem

$\mathbb{T}_1$ *is the class of Płonka sums of squags.*

Proof.

- Let $\Sigma = \{x * x = x, x * y = y * x, x * (x * (y * z)) = (x * (x * y)) * z\}$, and $x \vee y := y * (y * x)$.
- For squags, $x \vee y = x$. $\mathbb{T}_1$ contains the class of squags, so it is enough to show that Σ entails each of the identities in the theorem.
- Ask Prover9 to do it for you. Verify by hand over several days. Celebrate.

$\square$

Theorem

$\mathbb{T}_1$ is the class of Płonka sums of squags.

Proof.

- Let $\Sigma = \{x * x = x, x * y = y * x, x * (x * (y * z)) = (x * (x * y)) * z\}$, and $x \vee y := y * (y * x)$.
- For squags, $x \vee y = x$. $\mathbb{T}_1$ contains the class of squags, so it is enough to show that Σ entails each of the identities in the theorem.
- Ask Prover9 to do it for you. Verify by hand over several days. Celebrate.

$\square$

Theorem

$\mathbb{T}_1$ is the class of Płonka sums of squags.

Proof.

- Let $\Sigma = \{x * x = x, x * y = y * x, x * (x * (y * z)) = (x * (x * y)) * z\}$, and $x \vee y := y * (y * x)$.
- For squags, $x \vee y = x$. $\mathbb{T}_1$ contains the class of squags, so it is enough to show that Σ entails each of the identities in the theorem.
- Ask Prover9 to do it for you. Verify by hand over several days. Celebrate.

$\square$

Theorem

$\mathbb{T}_1$ is the class of Płonka sums of squags.

Proof.

- Let $\Sigma = \{x * x = x, x * y = y * x, x * (x * (y * z)) = (x * (x * y)) * z\}$, and $x \vee y := y * (y * x)$.
- For squags, $x \vee y = x$. $\mathbb{T}_1$ contains the class of squags, so it is enough to show that Σ entails each of the identities in the theorem.
- Ask Prover9 to do it for you. Verify by hand over several days. Celebrate.

□

Theorem

$\mathbb{T}_1$ *is the class of Płonka sums of squags.*

Proof.

- Let $\Sigma = \{x * x = x, x * y = y * x, x * (x * (y * z)) = (x * (x * y)) * z\}$, and $x \vee y := y * (y * x)$.
- For squags, $x \vee y = x$. $\mathbb{T}_1$ contains the class of squags, so it is enough to show that Σ entails each of the identities in the theorem.
- Ask Prover9 to do it for you. Verify by hand over several days. Celebrate.

□

Theorem

$\mathbb{T}_1$ *is the class of Płonka sums of squags.*

Proof.

- Let $\Sigma = \{x * x = x, x * y = y * x, x * (x * (y * z)) = (x * (x * y)) * z\}$, and $x \vee y := y * (y * x)$.
- For squags, $x \vee y = x$. $\mathbb{T}_1$ contains the class of squags, so it is enough to show that Σ entails each of the identities in the theorem.
- Ask Prover9 to do it for you. Verify by hand over several days. Celebrate.

$\square$

Questions?