Automatic Proofs and Counterexamples With Applications to Short Single Axioms

William McCune
Mathematics and Computer Science Division
Argonne National Laboratory

October 2004

Lattice Theory Single Axioms

Standard LT basis:

$$x \wedge y = y \wedge x \qquad x \vee y = y \vee x$$
$$(x \wedge y) \wedge z = x \wedge (y \wedge z) \qquad (x \vee y) \vee z = x \vee (y \vee z)$$
$$(x \vee y) \wedge x = x \qquad (x \wedge y) \vee x = x$$

McKenzie's absorption 4-basis for LT,

$$y \vee (x \wedge (y \wedge z)) = y \qquad y \wedge (x \vee (y \vee z)) = y$$
$$((x \wedge y) \vee (y \wedge z)) \vee y = y \qquad ((x \vee y) \wedge (y \vee z)) \wedge y = y$$

led to his proof that LT is 1-based (1970).

The proof is constructive, and it produces *big* axioms.

Lattice Theory Single Axioms – Automated Deduction

- Modifying the construction procedure.

Single axiom for LT (length 79, 7 variables, 1996):

$$(((x \wedge y) \vee (y \wedge (x \vee y))) \wedge z) \vee (((x \wedge (((w \wedge y) \vee (y \wedge v)) \vee y)) \vee (((y \wedge (((w \vee (y \vee v)) \wedge (s \vee y)) \wedge y)) \vee (u \wedge (y \vee (((w \vee (y \vee v)) \wedge (s \vee y)) \wedge y)))) \wedge (x \vee (((w \wedge y) \vee (y \wedge v)) \vee y)))) \wedge (((x \wedge y) \vee (y \wedge (x \vee y))) \vee z)) = y$$

- Starting small, generating and filtering candidates.

Single axiom for LT (length 29, 8 variables, 2003):

$$(((y \vee x) \wedge x) \vee (((z \wedge (x \vee x)) \vee (u \wedge x)) \wedge v)) \wedge (((w \vee x) \wedge (s \vee x)) \vee t) = x$$

OL, OML, MOL, and BA in Terms of the Sheffer Stroke

Consider the equations

Assoc:	$x \mid ((y \mid z) \mid (y \mid z)) = y \mid ((x \mid z) \mid (x \mid z))$
Absorb:	$(x \mid x) \mid (x \mid y) = x$
One:	$x \mid (x \mid x) = y \mid (y \mid y)$
OM:	$x \mid (x \mid (x \mid y)) = x \mid y$
Mod:	$x \mid (y \mid (x \mid (z \mid z))) = x \mid (z \mid (x \mid (y \mid y)))$
Cut:	$(x \mid (y \mid y)) \mid (x \mid y) = x$

The varieties in question can be defined as follows.

Variety	Type	Independent Basis
$\mathcal{OL}$	$\langle 2 \rangle$	{ Assoc, Absorb, One }
$\mathcal{OML}$	$\langle 2 \rangle$	{ Assoc, Absorb, OM }
$\mathcal{MOL}$	$\langle 2 \rangle$	{ Assoc, Absorb, One, Mod }
$\mathcal{BA}$	$\langle 2 \rangle$	{ Assoc, Cut }

Searching for Single Axioms, Smallest First

- Enumerate well-formed equations (under some constraints)
- Remove non-identities
  - use a decision procedure if available (LT, OL, BA)
  - otherwise use a set of finite algebras (OML, MOL)
- Collect a set S of finite counterexamples, e.g., non-OLs.
  Given a candidate identity C,

  If C is true in any member of S
  reject C;
  else if a counterexample M can be found
  reject C and add M to S;
  else
  try to prove that C is a single axiom.

Sheffer Stroke Single Axioms

- Ortholattices (OL): length 23, none shorter
  $(((y \mid x) \mid (x \mid z)) \mid u) \mid (x \mid ((x \mid ((y \mid y) \mid y)) \mid z)) = x$
- Orthomodular Lattices (OML): length 23
  $(((y \mid x) \mid (x \mid z)) \mid u) \mid (x \mid ((z \mid ((x \mid x) \mid z)) \mid z)) = x$
  - none of length less than 21
  - 58 open candidates of length 21
- Modular Ortholattices (MOL): length 25 (very difficult proof)
  $(y \mid x) \mid (((x \mid x) \mid z) \mid (((((x \mid y) \mid z) \mid z) \mid x) \mid (x \mid u))) = x$
  - none of length less than 21
  - 238 open candidates of length 21
  - many open candidates of length 23
- Boolean Algebras (BA): length 15, none shorter
  $(y \mid ((x \mid y) \mid y)) \mid (x \mid (z \mid y)) = x$

Automated Deduction

We use

- Otter
  - searches for proofs of first-order statements
  - is mostly automatic, but it can accept guidance
- Mace4
  - searches for finite structures (models and counterexamples)
- Associated programs
  - isofilter: remove isomorphic structures
  - clausefilter: use finite structures to filter clauses

Computing Finite Algebras with Mace4 and Isofilter

Size of Lattice	Number of Lattices			
	OL	OML	MOL	BA
2	1	1	1	1
4	1	1	1	1
6	2	1	1	0
8	5	2	2	1
10	15	2	1	0
12	60	3	2	0
14	311	4	1	0
16	?	7	3	1
18	?	8	1	0
20	?	14	2	0

Table: Number of Nonisomorphic Lattices

Finding Counterexamples with Mace4

- Small counterexamples (size ≤ 4) are easy to find.
  - E.g., ask Mace4 for a noncommutative model of a candidate.
- Larger counterexamples usually require additional constraints.
  - OML candidate, length 21

    $$((y \mid x) \mid x) \mid (((z \mid x) \mid (y \mid x)) \mid ((y \mid y) \mid z)) = x$$

    Mace4 cannot find a noncommutative model in reasonable time; but Mace4 easily finds a quasigroup model (size 7) to eliminate it.
- Use lattices from the preceding slide.

Finding Proofs with Otter (OL)

OL candidate $\Rightarrow$ OL basis

- Given

$$(((y \mid x) \mid (x \mid z)) \mid u) \mid (x \mid ((x \mid ((y \mid y) \mid y)) \mid z)) = x$$
$$x \vee y = (x \mid x) \mid (y \mid y)$$
$$x \wedge y = (x \mid y) \mid (x \mid y)$$
$$x' = x \mid x$$

- Prove

$$x \vee (y \vee z) = y \vee (x \vee z) \qquad x'' = x$$
$$x \vee (x \wedge y) = x \qquad x \vee x' = y \vee y'$$
$$x \wedge y = (x' \vee y')' \qquad x \mid y = x' \vee y'$$

- Otter proves this in a few seconds (the proof is about 100 lines).

Finding Proofs with Otter (MOL)

- MOL candidate:

$$(y \mid x) \mid (((x \mid x) \mid z) \mid (((((x \mid y) \mid z) \mid z) \mid x) \mid (x \mid u))) = x$$

  - Otter cannot automatically prove a MOL basis.
  - Many Otter searches with a lot of (syntactic) guidance led to a proof.
  - The proof is 355 lines and incomprehensible.

470 [2->367] ((x|y)|(((y|((z|y)|(((y|y)|u)|(((((y|z)|u)|u)|y)|(y|v)))))|w)|((((((z|y)|(((y|y)|u)|(((((y|z)|u)|u)|y)|(y|v))))|x)|w)|w)|((z|y)|(((y|y)|u)|(((((y|z)|u)|u)|y)|(y|v)))))|(((y|y)|u)|(((((y|z)|u)|u)|y)|(y|v))))))=((z|y)|(((y|y)|u)|(((((y|z)|u)|u)|y)|(y|v))))

471 [2->470] ((x|y)|(((y|y)|z)|(((((((u|y)|(((y|y)|v)|(((((y|u)|v)|v)|y)|(y|w)))))|x)|z)|z)|((u|y)|(((y|y)|v)|(((((y|u)|v)|v)|y)|(y|w)))))|(((y|y)|v)|(((((y|u)|v)|v)|y)|(y|w))))))=((u|y)|(((y|y)|v)|(((((y|u)|v)|v)|y)|(y|w))))

472 [2->471] ((x|y)|(((y|y)|z)|(((((y|x)|z)|z)|((u|y)|(((y|y)|v)|(((((y|u)|v)|v)|y)|(y|w)))))|(((y|y)|v)|(((((y|u)|v)|v)|y)|(y|w))))))=((u|y)|(((y|y)|v)|(((((y|u)|v)|v)|y)|(y|w))))

473 [2->472] ((x|y)|(((y|y)|z)|(((((y|x)|z)|z)|y)|(((y|y)|u)|(((((y|v)|u)|u)|y)|(y|w))))))=((v|y)|(((y|y)|u)|(((((y|v)|u)|u)|y)|(y|w))))

474 [2->473] ((x|y)|(((y|y)|z)|(((((y|x)|z)|z)|y)|(((y|y)|u)|(((((y|v)|u)|u)|y)|(y|w))))))=y

475 [385->404] ((x|((x|(((x|x)|x)|((x|x)|x)))|((((x|x)|x)|(x|x))|((x|x)|y)))))|((((((x|x)|(x|x))|(((x|x)|x)|((x|x)|x)))|((((x|x)|x)|(x|x))|((x|x)|y))))|((((x|x)|(x|x))|(((x|x)|x)|((x|x)|x)))|((((x|x)|x)|(x|x))|((x|x)|y))))|(x|x))|((x|x)|(((x|x)|x)|(x|x))|((x|x)|y)))))=((((x|x)|(x|x))|(((x|x)|x)|((x|x)|x)))|((((x|x)|x)|(x|x))|((x|x)|y)))

476 [387->475] ((x|(((x|x)|x)|((((x|x)|x)|(x|x))|((x|x)|y)))))|(((((((x|x)|(x|x))|(((x|x)|x)|((x|x)|x)))|((((x|x)|x)|(x|x))|((x|x)|y)))|((((x|x)|(x|x))|(((x|x)|x)|((x|x)|x)))|((((x|x)|x)|(x|x))|((x|x)|y)))))|(x|x))|((x|x)|((((x|x)|x)|(x|x))|((x|x)|y)))))=((((x|x)|(x|x))|(((x|x)|x)|((x|x)|x)))|((((x|x)|x)|(x|x))|((x|x)|y)))

Appendix: More Applications of Mace4

Quantum Logic Problem

Lattice Axioms

$$x \wedge y = y \wedge x \qquad x \vee y = y \vee x$$
$$(x \wedge y) \wedge z = x \wedge (y \wedge z) \qquad (x \vee y) \vee z = x \vee (y \vee z)$$
$$(x \vee y) \wedge x = x \qquad (x \wedge y) \vee x = x$$

Add these for Ortholattices

$$x \vee c(x) = 1 \qquad x \wedge c(x) = 0$$
$$c(c(x)) = x \qquad c(x \vee y) = c(x) \wedge c(y)$$

Weak Orthomodular Law

$$(c(x) \wedge (x \vee y)) \vee (c(y) \vee (x \wedge y)) = 1$$

Does the following hold in all weakly orthomodular lattices? [Norm Megill].

$$x \wedge (y \vee (x \wedge (c(x) \vee (x \wedge y)))) = x \wedge (c(x) \vee (x \wedge y)) \qquad \text{(*3-M68)}$$

Quantum Logic Counterexample from Mace4

Model 1 at 0.87 seconds

^	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19
0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19
2	0	2	2	6	0	0	6	10	12	13	10	0	12	13	10	19	13	13	0	19
3	0	3	6	3	0	0	6	11	6	6	0	11	6	6	11	11	3	6	0	0
4	0	4	0	0	4	0	0	4	4	0	0	0	0	0	4	4	0	4	0	0
5	0	5	0	0	0	5	0	5	0	5	0	0	0	0	18	18	0	0	18	0
6	0	6	6	6	0	0	6	0	6	6	0	0	6	6	0	0	6	6	0	0
7	0	7	10	11	4	5	0	7	4	5	10	11	0	0	14	15	11	4	18	19
8	0	8	12	6	4	0	6	4	8	12	0	0	12	12	4	4	12	8	0	0
9	0	9	13	6	0	5	6	5	12	9	0	0	12	13	18	18	13	13	18	0
10	0	10	10	0	0	0	0	10	0	0	10	0	0	0	10	19	0	0	0	19
11	0	11	0	11	0	0	0	11	0	0	0	11	0	0	11	11	11	0	0	0
12	0	12	12	6	0	0	6	0	12	12	0	0	12	12	0	0	12	12	0	0
13	0	13	13	6	0	0	6	0	12	13	0	0	12	13	0	0	13	13	0	0
14	0	14	10	11	4	18	0	14	4	18	10	11	0	0	14	15	11	4	18	19
15	0	15	19	11	4	18	0	15	4	18	19	11	0	0	15	15	11	4	18	19
16	0	16	13	3	0	0	6	11	12	13	0	11	12	13	11	11	16	13	0	0
17	0	17	13	6	4	0	6	4	8	13	0	0	12	13	4	4	13	17	0	0
18	0	18	0	0	0	18	0	18	0	18	0	0	0	0	18	18	0	0	18	0
19	0	19	19	0	0	0	0	19	0	0	19	0	0	0	19	19	0	0	0	19

v	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19
0	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19
1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
2	2	1	2	1	1	1	2	1	1	1	2	1	2	2	1	1	1	1	1	2
3	3	1	1	3	1	1	3	1	1	1	1	3	16	16	1	1	16	1	1	1
4	4	1	1	1	4	7	8	7	8	1	14	15	8	17	14	15	1	17	15	15
5	5	1	1	1	7	5	9	7	1	9	7	7	9	9	7	7	1	1	5	7
6	6	1	2	3	8	9	6	1	8	9	2	3	12	13	1	1	16	17	9	2
7	7	1	1	1	7	7	1	7	1	1	7	7	1	1	7	7	1	1	7	7
8	8	1	1	1	8	1	8	1	8	1	1	1	8	17	1	1	1	17	1	1
9	9	1	1	1	1	9	9	1	1	9	1	1	9	9	1	1	1	1	9	1
10	10	1	2	1	14	7	2	7	1	1	10	14	2	2	14	14	1	1	14	10
11	11	1	1	3	15	7	3	7	1	1	14	11	16	16	14	15	16	1	15	15
12	12	1	2	16	8	9	12	1	8	9	2	16	12	13	1	1	16	17	9	2
13	13	1	2	16	17	9	13	1	17	9	2	16	13	13	1	1	16	17	9	2
14	14	1	1	1	14	7	1	7	1	1	14	14	1	1	14	14	1	1	14	14
15	15	1	1	1	15	7	1	7	1	1	14	15	1	1	14	15	1	1	15	15
16	16	1	1	16	1	1	16	1	1	1	1	16	16	16	1	1	16	1	1	1
17	17	1	1	1	17	1	17	1	17	1	1	1	17	17	1	1	1	17	1	1
18	18	1	1	1	15	5	9	7	1	9	14	15	9	9	14	15	1	1	18	15
19	19	1	2	1	15	7	2	7	1	1	10	15	2	2	14	15	1	1	15	19

c	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19
	1	0	4	5	2	3	7	6	10	11	8	9	14	15	12	13	18	19	16	17

A = 2 B = 3

A Weakly Orthomodular Lattice Violating (*3-M68)

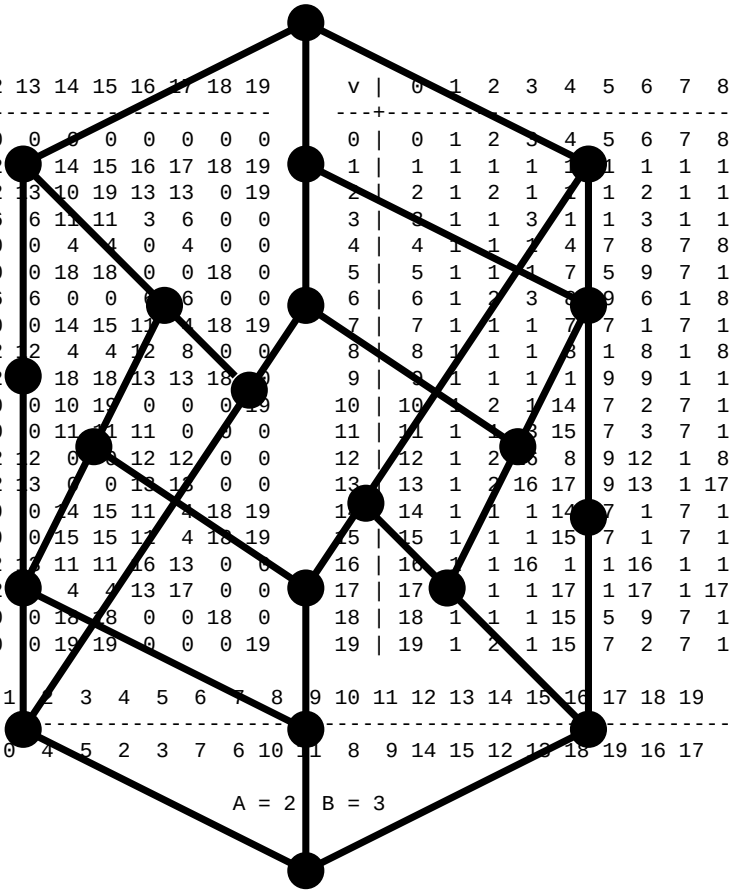
Quantum Logic Counterexample from Mace4

Model 1 at 0.87 seconds

^	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19
0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19
2	0	2	2	6	0	0	6	10	12	13	10	0	12	13	10	19	13	13	0	19
3	0	3	6	3	0	0	6	11	6	6	0	11	6	6	11	11	3	6	0	0
4	0	4	0	0	4	0	0	4	4	0	0	0	0	0	4	4	0	4	0	0
5	0	5	0	0	0	5	0	5	0	5	0	0	0	0	18	18	0	0	18	0
6	0	6	6	6	0	0	6	0	6	6	0	0	6	6	0	0	6	6	0	0
7	0	7	10	11	4	5	0	7	4	5	10	11	0	0	14	15	11	4	18	19
8	0	8	12	6	4	0	6	4	8	12	0	0	12	12	4	4	12	8	0	0
9	0	9	13	6	0	5	6	5	12	9	0	0	12	13	18	18	13	13	18	0
10	0	10	10	0	0	0	0	10	0	0	10	0	0	0	10	19	0	0	0	19
11	0	11	0	11	0	0	0	11	0	0	0	11	0	0	11	11	11	0	0	0
12	0	12	12	6	0	0	6	0	12	12	0	0	12	12	0	0	12	12	0	0
13	0	13	13	6	0	0	6	0	12	13	0	0	12	13	0	0	13	13	0	0
14	0	14	10	11	4	18	0	14	4	18	10	11	0	0	14	15	11	4	18	19
15	0	15	19	11	4	18	0	15	4	18	19	11	0	0	15	15	11	4	18	19
16	0	16	13	3	0	0	6	11	12	13	0	11	12	13	11	11	16	13	0	0
17	0	17	13	6	4	0	6	4	8	13	0	0	12	13	4	4	13	17	0	0
18	0	18	0	0	0	18	0	18	0	18	0	0	0	0	18	18	0	0	18	0
19	0	19	19	0	0	0	0	19	0	0	19	0	0	0	19	19	0	0	0	19

v	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19
0	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19
1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
2	2	1	2	1	1	1	2	1	1	1	2	1	2	2	1	1	1	1	1	2
3	3	1	1	3	1	1	3	1	1	1	1	3	16	16	1	1	16	1	1	1
4	4	1	1	1	4	7	8	7	8	1	14	15	8	17	14	15	1	17	15	15
5	5	1	1	1	7	5	9	7	1	9	7	7	9	9	7	7	1	1	5	7
6	6	1	2	3	8	9	6	1	8	9	2	3	12	13	1	1	16	17	9	2
7	7	1	1	1	7	7	1	7	1	1	7	7	1	1	7	7	1	1	7	7
8	8	1	1	1	8	1	8	1	8	1	1	1	8	17	1	1	1	17	1	1
9	9	1	1	1	1	9	9	1	1	9	1	1	9	9	1	1	1	1	9	1
10	10	1	2	1	14	7	2	7	1	1	10	14	2	2	14	14	1	1	14	10
11	11	1	1	3	15	7	3	7	1	1	14	11	16	16	14	15	16	1	15	15
12	12	1	2	3	8	9	12	1	8	9	2	16	12	13	1	1	16	17	9	2
13	13	1	2	16	17	9	13	1	17	9	2	16	13	13	1	1	16	17	9	2
14	14	1	1	1	14	7	1	7	1	1	14	14	1	1	14	14	1	1	14	14
15	15	1	1	1	15	7	1	7	1	1	14	15	1	1	14	15	1	1	15	15
16	16	1	1	16	1	1	16	1	1	1	1	16	16	16	1	1	16	1	1	1
17	17	1	1	1	17	1	17	1	17	1	1	1	17	17	1	1	1	17	1	1
18	18	1	1	1	15	5	9	7	1	9	14	15	9	9	14	15	1	1	18	15
19	19	1	2	1	15	7	2	7	1	1	10	15	2	2	14	15	1	1	15	19

c	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19
	1	0	4	5	2	3	7	6	10	11	8	9	14	15	12	13	18	19	16	17



A = 2 B = 3

A Weakly Orthomodular Lattice Violating (*3-M68)

Ring Models for Group Candidates

```
% Mace4 input file

% Fix [+,-,*,0,1] as the ring of integers (mod n).
set(integer_ring).

clauses(theory).

f(f(x,y),f(y,g(f(f(g(f(g(x),z)),y),y)))) = z.  % candidate
f(f(A,B),C) != f(A,f(B,C)).      % denial of associativity

g(x)   =  M * x.
f(x,y) = (H * x) + (K * y).

end_of_list.
```

Ring Models for Group Candidates

In a few minutes, Mace4 finds a counterexample of size 41:

```
f(f(x,y),f(y,g(f(f(g(f(g(x),z)),y),y)))) = z.  % candidate
f(f(A,B),C) != f(A,f(B,C)).      % denial of associativity

g(x)   =  38 * x.
f(x,y) = (38 * x) + (40 * y).
```