Applications of Automated Equational Deduction

William McCune
mccune@mcs.anl.gov

Mathematics and Computer Science Division
Argonne National Laboratory
U.S.A.

Presented at the AMS Sectional Meeting
Atlanta, Georgia
October 19, 1997

Outline

- Programs
  - Otter
  - EQP
  - MACE
- Applications
  - The Robbins Problem
  - Quantum Logic
  - Algebraic Geometry

Otter

- Applies to first order logic with equality
- Searches for proofs
- Uses resolution and paramodulation inference rules
  - equality reasoning is similar to unfailing Knuth-Bendix completion
- Modes of use
  - automatic mode
  - the user can adjust the search strategy
  - iteration

EQP (EQuational Prover)

- Similar to Otter, *but*,
  - restricted to equational logic,
  - associativity and commutativity of binary operations are built into the inference rules,
  - more refined strategies for equational reasoning.

MACE (Models and Counter-Examples)

- Applies to first order logic with equality
- Searches for finite models (e.g., counterexamples)
- Complements Otter and EQP
- Limitations
  - cannot handle large formulas
  - cannot handle many variables
  - cannot find large models
- (better programs of this type are available)

The Robbins Problem

- A well-known basis for Boolean algebra [Huntington, 1933]:

$x+y=y+x$	(C) Commutativity
$(x+y)+z=x+(y+z)$	(A) Associativity
$\overline{(\overline{x}+y)}+\overline{(\overline{x}+\overline{y})}=x$	(H) Huntington

- The Robbins Problem:

  $\overline{(\overline{(x+\overline{y})}+\overline{(x+y)})}=x$ (R) Robbins

  Is $\{C, A, R\}$ basis for Boolean algebra?

- A proof of the following would suffice.

  Robbins $\Longrightarrow_{\mathrm{AC}}$ *Huntington.*

- A lemma (Steve Winker, 1980):

  $$\left\{\begin{array}{l}\textit{Robbins}\\ \exists c\exists d\ (c+d=c)\end{array}\right\} \Longrightarrow_{\mathrm{AC}} \textit{Huntington.}$$

The Proof that Solved the Robbins Problem

Theorem. *Robbins* $\Longrightarrow_{\mathrm{AC}} \exists c\exists d\ (c+d=c)$.

Proof (found by EQP in 8 days of search.)

7	$\overline{\overline{\overline{x}+y}+\overline{x+y}}=y$	[Robbins Equation]
10	$\overline{\overline{\overline{x+y}+\overline{x}+y}+y}=\overline{x+y}$	[7 → 7]
11	$\overline{\overline{\overline{\overline{x}+y}+x+y}+y}=\overline{\overline{x}+y}$	[7 → 7]
29	$\overline{\overline{\overline{\overline{x}+y}+x+2y}+\overline{\overline{x}+y}}=y$	[11 → 7]
54	$\overline{\overline{\overline{\overline{\overline{x}+y}+x+2y}+\overline{\overline{x}+y}}+z+\overline{y+z}}=z$	[29 → 7]
217	$\overline{\overline{\overline{\overline{\overline{x}+y}+x+2y}+\overline{\overline{x}+y}+\overline{y+z}+z}+z}=\overline{y+z}$	[54 → 7]
674	$\overline{\overline{\overline{\overline{\overline{\overline{x}+y}+x+2y}+\overline{\overline{x}+y}+\overline{y+z}+z}+z+u}+\overline{\overline{y+z}+u}}=u$	[217 → 7]
6736	$\overline{\overline{\overline{\overline{3x}+x}+\overline{3x}}+\overline{\overline{\overline{3x}+x}+5x}}=\overline{\overline{3x}+x}$	[10 → 674]
8855	$\overline{\overline{\overline{3x}+x}+5x}=\overline{3x}$	[6736 → 7 :54]
8865	$\overline{\overline{\overline{\overline{3x}+x}+\overline{3x}+2x}+\overline{3x}}=\overline{\overline{3x}+x}+2x$	[8855 → 7]
8866	$\overline{\overline{\overline{3x}+x}+\overline{3x}}=x$	[8855 → 7: 11]
8870	$\overline{\overline{\overline{\overline{3x}+x}+\overline{3x}+y}+\overline{x+y}}=y$	[8866 → 7]
8871	$\overline{\overline{3x}+x}+2x=2x$	[8865 :8870]

Equation 8871 asserts the existence of an object c, namely $2x$, and an object d, namely $\overline{\overline{3x}+x}$, such that $c+d=c$. Q.E.D.

Quantum Logic

An *Ortholattice* satisfies

$x \vee y = y \vee x$	$x \wedge y = y \wedge x$
$(x \vee y) \vee z = x \vee (y \vee z)$	$(x \wedge y) \wedge z = x \wedge (y \wedge z)$
$x \vee (x \wedge y) = x$	$x \wedge (x \vee y) = x$
$x'' = x$	
$(x \wedge y)' = x' \vee y'$	
$x \vee x' = 1$	$x \wedge x' = 0$
$x \vee 1 = 1$	$x \wedge 0 = 0$

An *orthomodular lattice* also satisfies

$$x \vee (x' \wedge (x \vee y)) = x \vee y$$

Ordinary probability: Boolean algebra over a set of events.

Probability in quantum dynamics: Orthomodular lattice over a Hilbert space.

Ortholattice Questions
(from Norman Megill)

Consider the following three equations.

$$((a \wedge b') \vee a')' \vee ((a \wedge b') \vee ((a' \wedge ((a \vee b') \wedge (a \vee b))) \vee (a' \wedge ((a \vee b') \wedge (a \vee b))'))) = 1 \quad \text{(E1)}$$

$$(a \vee ((a' \wedge ((a \vee b') \wedge (a \vee b))) \vee (a' \wedge ((a' \wedge b) \vee (a' \wedge b'))))) = 1 \quad \text{(E2)}$$

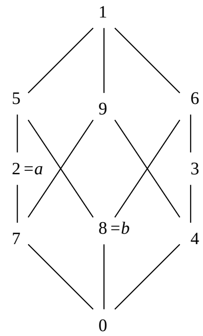
$$(((a' \wedge b) \vee (a' \wedge b')) \vee (a \wedge (a' \vee b)))' \vee (a' \vee b) = 1 \quad \text{(E3)}$$

Each was known to hold for orthomodular lattices.

Do they hold for ortholattices?

Ortholattice Answers

E1. MACE found a counterexample of size 10 (in 20 minutes):

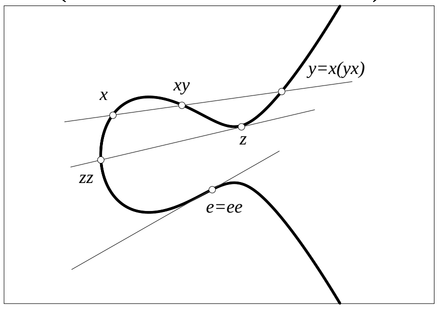


An ortholattice violating E1.

E2. EQP found a proof (in 4 seconds)

E3. EQP found a proof (in 23 hours)

Algebraic Geometry
(with R. Padmanabhan)



The chord-tangent construction: Consider a nonsingular cubic curve in the complex projective plane. Define a binary operation on the points of the curve.

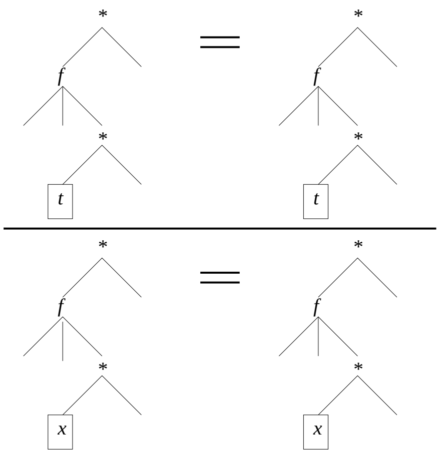
– If a line intersects the curve in 3 points, the product of any two points is the third point.

– zz is the point where the tangent at z intersects the curve.

– Inflection points are idempotent elements ($ee = e$).

– The operation is commutative, and the Steiner law holds: $x(yx) = y$.

The Rule $=(gL)\Rightarrow$
(R. Padmanabhan)



- If identical terms (t) occur in corresponding positions, and in the same nest of function symbols, replace both occurrences with a new variable (x).
- This inference rule was added to Otter.

New Results with $=\!(gL)\!\Rightarrow$ *(A)*

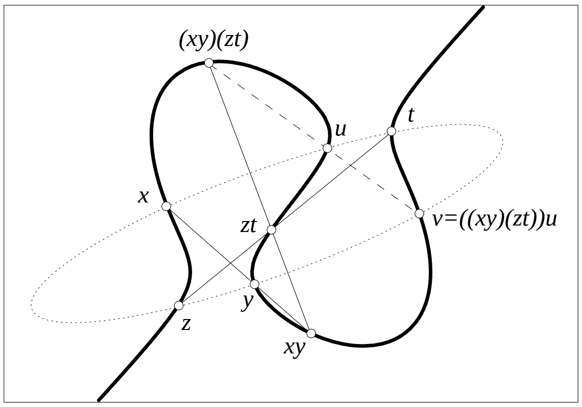
- General exploration of $=\!(gL)\!\Rightarrow$ algebras.
- A cancellative semigroup on a cubic curve must be commutative.
- Uniqueness inversive groupoid on a cubic curve.
- Uniqueness of the 5-ary Steiner Law:

$$\left\{\begin{array}{l}\text{full permutability of } f\\ f(e,e,e,e,e)=e\\ f(e,e,e,x,f(e,e,e,x,y))=y\\ \text{full permutability of } g\\ g(e,e,e,e,e)=e\\ g(e,e,e,x,g(e,e,e,x,y))=y\end{array}\right\} =\!(gL)\!\Rightarrow$$

$$g(x,y,z,u,v)=f(x,y,z,u,v).$$

A corollary: given 5 points of intersection of a cubic and a conic, the sixth point can be found be a simple ruler construction.

Conic-cubic Construction



Types of Use

- Stand-alone – (Robbins problem)
  - try to get the programs to prove the interesting theorems
  - TRC – combinatory logic - new foundations
- Support for higher-level work (quantum logic)
  - semigroup conjecture of Padmanabhan
  - formal methods, verification systems
- Exploration of new methods (cubic curves)

Summary

- Automatic deduction practical is practical in some cases for *simple* equational theories.
- How practical can it be for complicated theories?
  - equational (or nearly equational) versions of set theory
  - systems that need complicated expressions (e.g., combinatory logic)
  - lots of defined concepts
- See my Web pages for information about the programs and other applications:

`http://www.mcs.anl.gov/home/mccune/`