Sketches and Hints

for a Conjecture in Modular Ortholattices

William McCune
Mathematics and Computer Science Division
Argonne National Laboratory

Robert Veroff
Computer Science Department
University of New Mexico

Dagstuhl
April 2003

A Hard Equational Theorem

$$f(f(y,x),f(f(f(x,x),z),f(f(f(f(f(x,y),z),z),x),f(x,u)))) = x$$

$$\Longrightarrow$$

$$f(x,f(f(x,f(y,y)),f(x,z))) = f(x,f(y,f(x,z)))$$

- What does this mean?

- Where did it come from?

- How was it proved?

A Chain of Lattice Varieties

- LT - Lattice Theory
  Consider an equational basis in terms of *meet* ($\wedge$) and *join* ($\vee$).

- OL - Ortholattices
  Introduce 0, 1, and a complement operation (c) satisfying
  $x \wedge c(x) = 0$, $x \vee c(x) = 1$, $c(c(x)) = x$, and the DeMorgan laws.

- OML - Orthomodular Lattices
  Include $x \vee (c(x) \wedge (x \vee y)) = x \vee y$.

- MOL - Modular Ortholattices
  Include $x \vee (y \wedge (x \vee z)) = (x \vee y) \wedge (x \vee z)$.

- BA - Boolean Algebras
  Include distributivity.

Single Axioms - f is the Sheffer stroke: $f(x,y) = c(x) \vee c(y)$

- LT - Lattice Theory [1]
  $(((y{\vee}x){\wedge}x){\vee}(((z{\wedge}(x{\vee}x)){\vee}(u{\wedge}x)){\wedge}v)){\wedge}(w{\vee}((s{\vee}x){\wedge}(x{\vee}t))) = x$
- OL - Ortholattices [2]
  $f(f(f(f(y,x),f(x,z)),u),f(x,f(f(x,f(f(y,y),y)),z))) = x$
- OML - Orthomodular Lattices [2]
  $f(f(f(f(y,x),f(x,z)),u),f(x,f(f(z,f(f(x,x),z)),z))) = x$
- MOL - Modular Ortholattices [2]
  $\boxed{f(f(y,x),f(f(f(x,x),z),f(f(f(f(f(x,y),z),z),x),f(x,u)))) = x}$
- BA - Boolean Algebra [3]
  $c(c(c(x \vee y) \vee z) \vee c(x \vee c(c(z) \vee c(z \vee u)))) = z$
  $f(f(x,f(f(y,x),x)),f(y,f(z,x))) = y$

MOL Single Axiom Problem

- MOL 4-basis in terms of the Sheffer Stroke

$$
\begin{array}{ll}
f(f(x,x),f(x,y)) = x & \text{(absorption)} \\
f(x,f(x,x)) = f(y,f(y,y)) & \text{(one)} \\
f(x,f(f(y,z),f(y,z))) = f(z,f(f(y,x),f(y,x))) & \text{(associativity)} \\
f(x,f(f(x,f(y,y)),f(x,z))) = f(x,f(y,f(x,z))) & \text{(modularity v1)}
\end{array}
$$

- Problem: *Find a single equation equivalent to the MOL 4-basis.*
- Method
  - enumerate (carefully) well-formed equations
  - use finite MOLs to remove some of the non-identities (decidable??)
  - use finite non-MOLs to remove some of the non-singleaxioms
  - use a theorem prover on the surviving candidates

Finding Finite MOLs and non-MOLs

- Mace 4 (called ICGNS in CASC-2002) [4]
  - searches for finite models of first-order statements
  - good performance for equations (SEM-like algorithm)
  - postfilter eliminates isomorphic models
- For eliminating non-identities (MOL): use MOLs up through size 20.
- For eliminating non-singleaxioms (MOL):
  - collect a set non-MOLs that satisfy candidates;
  - use the non-MOL OMLs up through size 20.

A Promising MOL Candidate

- All candidates up through length 19 were eliminated.
- 238 length-21 candidates remain (none seems promising).
- Two length-27 candidates proved to be single axioms.
- A promising length-25 candidate (MOL-25A):

$$f(f(y,x),f(f(f(x,x),z),f(f(f(f(f(x,y),z),z),x),f(x,u)))) = x$$

  - The absorption and “one” properties can be proved easily.
  - The associativity property was proved, with some difficulty.
  - The modularity property resisted . . .

The Method of Proof Sketches

- Background
  - context
  - motivation
  - mechanics
  - challenges
- Proving modularity from MOL-25A

Context

- Resolution / paramodulation
- Focus on finding proofs to “difficult” theorems
  - difficulty characterized in terms of search
  - other approaches may be more suitable
- Designing sequences of experiments
- Automation is a longer-term objective

Proof Sketches (Motivation)

- Example: $x^3 = x$ problem (ring theory)

  1. $6x = 0$
  2. $3xy + 3yx = 0$
  3. $4xy + 2yx = 0$
  4. $xy = yx$

- Provide guidance without constraining search

As in approaches bases on analogy, proof planning, and abstraction, the point is to have high-level control of the proof search based on some notion of mapping and/or matching.

Proof Sketches (Mechanics)

- Idea: subsumption as part of a search strategy
  - input list of *hint* clauses
  - hint subsumers are notable milestones
  - bias search accordingly
- Uses
  - proof checking and completion
  - convert proof to derivation (strictly forward, AC-free, demod free)
  - proof sketches
- A proof sketch is given as a set of hint clauses
  - emphasis on sufficiency rather than necessity
  - operationally, natural and convenient to use multiple proof sketches simultaneously

Proof Sketches (The Challenge)

The hints mechanism is straightforward. The interesting problem is the generation of proof sketches and the role these play in the solution to difficult problems.

An idea that has worked very well in several problem domains is to start with simplifying assumptions and systematically eliminate these assumptions in a sequence of experiments (using previous proofs as proof sketches).

What assumptions? (highly experimental at this point)

Example: Proving Modularity from the MOL Candidate

MOL-25A $\Longrightarrow$ Modularity-version-1

That is,

$$f(f(y,x),f(f(f(x,x),z),f(f(f(f(f(x,y),z),z),x),f(x,u)))) = x$$

$$\Longrightarrow$$

$$f(x,f(f(x,f(y,y)),f(x,z))) = f(x,f(y,f(x,z)))$$

Step One: Generated a Proof Sketch

- Proved modularity from MOL-25A, with

$$
\begin{aligned}
&f(f(x,y),f(x,f(y,z))) = x \\
&f(x,y) = f(y,x)
\end{aligned}
$$

  included as extra assumptions.

- These two equations are known to be a Sheffer 2-basis for Boolean algebra.

Step Two: Simplified the Assumptions

- Proved modularity from MOL-25A, with

$$
\begin{aligned}
&f(f(x,y),f(x,f(y,x))) = x \\
&f(x,y) = f(y,x)
\end{aligned}
$$

  included as extra assumptions.

- The first equation is a proper instance of the first equation from the 2-basis (substituting x for z).

Step Three: Eliminated the Simplified Assumptions

- Proved the assumptions,

$$
\begin{array}{l}
f(f(x,y),f(x,f(y,x))) = x \\
f(x,y) = f(y,x)
\end{array}
$$

from MOL-25A.

HBCK

Axioms for quasivariety HBCK:

$$
\begin{aligned}
x * 1 &= 1 && \text{(M3)}\\
1 * x &= x && \text{(M4)}\\
(x * y) * ((z * x) * (z * y)) &= 1 && \text{(M5)}\\
x * x &= 1 && \text{(M8)}\\
x * (y * z) &= y * (x * z) && \text{(M9)}\\
(x * y) * (x * z) &= (y * x) * (y * z) && \text{(H)}\\
(x * y = 1 \wedge y * x = 1) \Rightarrow x &= y && \text{(M7)}
\end{aligned}
$$

Challenge problem [7]; find a first-order proof of:

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

See `http://www.cs.unm.edu/~veroff/HBCK/`.

KA2

Axioms for many-valued logic:

$$i(x, i(y, x)) \qquad \text{(MV1)}$$
$$i(i(x, y), i(i(y, z), i(x, z))) \qquad \text{(MV2)}$$
$$i(i(i(x, y), y), i(i(y, x), x)) \qquad \text{(MV3)}$$
$$i(i(n(x), n(y)), i(y, x)) \qquad \text{(MV4)}$$

KA2: K distributes over A, direction 2 (KpAqr $\leftarrow$ AKpqKpr)

$$\begin{aligned} &i(i(i(n(i(i(n(x), n(y)), n(y))), n(i(i(n(x), n(z)), n(z)))), \\ &\quad n(i(i(n(x), n(z)), n(z)))), \\ &\quad n(i(i(n(x), n(i(i(y, z), z))), n(i(i(y, z), z))))) \end{aligned}$$

The proof we found is 140 steps long and contains several long formulas (up to length 71).

See `http://www.cs.unm.edu/~veroff/CD/`.

Summary

- Observations
  - Successfully applied to numerous difficult (in our terms) problems from different problem areas
  - Little prior knowledge
  - Individual steps still may be very difficult
- Issues
  - Common aspects, potential for automation
  - Potential negative impact of adding assumptions

References

1. McCune, Padmanabhan, Veroff, “Yet another single law for lattices”, to appear in *Algebra Universalis’*.
2. McCune, Rose, Veroff, “Sheffer stroke bases for ortholattices”, `www.mcs.anl.gov/~mccune/papers/olsax/`, 2003.
3. McCune, Veroff, Fitelson, Harris, Feist, Wos, “Short single axioms for Boolean algebra”, *J. Automated Reasoning* 29(1), 2002.
4. McCune, “Mace 4”, `www.mcs.anl.gov/~mccune/mace4/`, 2002.
5. Veroff, “Using hints to increase the effectiveness of an automated reasoning program: Case studies”, *J. Automated Reasoning* 16(3), 1996.
6. Veroff, “Solving open questions and other challenge problems using proof sketches”, *J. Automated Reasoning*, 27(2), 2001.
7. McCune, Padmanabhan, *Automated Deduction in Equational Logic and Cubic Curves*, Springer LNCS #1095, 1996.