Semantic Guidance

(and other methods)

for Saturation Provers

8th International Conference on
ARTIFICIAL INTELLIGENCE AND SYMBOLIC COMPUTATION

Beihang University, Beijing, September 2006

William McCune
Downers Grove, Illinois
U.S.A.

An Equational Problem

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

$$\overset{?}{\Rightarrow}$$

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

Saturation Provers for First-order and Equational Logic

- Inference
  - Proof by refutation
  - Make inferences (under some restrictions), keeping formulas simplified
- Completeness
  - If the conjecture is a theorem, a proof will eventually be found
- Strategy
  - Term ordering for inference and simplification
  - Selection function for application of inference rules
  - Special-purpose strategies (may be incomplete)
- Examples: Otter, E, Vampire, Waldmeister, Prover9

The Inference Loop

- Maintain two sets of formulas
  - *active*: available for making inferences
  - *passive*: waiting to participate in the search
- Loop:
  - Select a formula C from *passive* (the *given clause*);
  - move C from passive to *active*;
  - make inferences from C and other formulas in *active*;
  - simplify inferred formulas and append to *passive*;
- Two versions: *Otter loop* and *Discount loop*
  - differ on when and how simplification occurs

Theory vs. Practice

Completeness Results

- Even though an inference is not needed,
  - it might be very helpful in practice.
- Even though an inference may be necessary in general,
  - it might be wasteful in practice.

Restriction vs. Guidance

- Restriction: Constrain application of inference rules
- Guidance: Selection of the *given clause*

Three Promising Strategies

1. Semantic Guidance

   – using interpretations to help select the *given clause*

2. Variable Ordering

   – extending the term ordering with variables

   – $(y * x) \succ (x * y)$

   – incomplete

3. Introduce Equational Definitions

   – emphasize “important” terms, e.g.,

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

Programs for Experimenting with Strategies

- Prover9
  - theorem prover for first-order and equational logic
  - Otter's (and EQP's) successor
- Mace4
  - searches for finite models and counterexamples

Semantic Guidance

Using interpretations to help select the *given clause*

Semantic Inference Rules for First-order and Equational Deduction

- Based on *interpretations* (explicit or implicit, finite or infinite)
- Semantic Resolution (Slagle 1965)
  - given an interpretation I, for each (binary) inference, at least one parent must be false in I.
  - example: *positive resolution* uses the (implicit) interpretation in which all atomic formulas are false.
- *Set of support resolution* (Wos, 1964): justified by any interpretation of the axioms, and the semantic restriction applies only to input clauses.

Semantic Inference Rules (continued)

- Semantic Paramodulation
- Semantic Resolution for Horn Sets (Henschen 1976)
  - If one of the parents is a positive unit false in I, the child must also be false in I.
  - applies also to paramodulation

Semantic Inference with Explicit Interpretations

- not much work, not much success
  - incompatibilities with inference rules based on term orderings and simplification
- Powerful finite-model finding programs, starting about 1990
  - Finder, MGTP, Mace2, Falcon, SEM, Mace4, Paradox.
- The SCOTT series of provers (Slaney, Hodgson, et al).
  - dynamic interpretations, partial interpretations, multiple interpretations
  - guidance and well as restriction

Semantic Guidance

- Assume the *Otter loop* or the *Discount loop*.
- Selecting the next clause for making inferences (the *given clause*).
  - weighting function: lightest first
  - age: breadth first
  - age/weight ratio
- For semantic guidance, specify a 3-way ratio:
  - age,
  - lightest clause *false* in I,
  - lightest clause *true* in I.

Lattice Theory Example: The Problem

In lattice theory (LT), what is the relationship between the following two identities?

$$x \wedge (y \vee (x \wedge z)) = x \wedge (y \vee (z \wedge ((x \wedge (y \vee z)) \vee (y \wedge z)))) \qquad \text{(H2)}$$

$$(x \wedge y) \vee (x \wedge z) = x \wedge ((y \wedge (x \vee z)) \vee (z \wedge (x \vee y))) \qquad \text{(H82)}$$

- LT, H2 $\rightarrow$ H82 ? *No*. Mace4 easily finds a counterexample of size 6.
- LT, H82 $\rightarrow$ H2 ?

Semantic guidance for LT, H82 $\rightarrow$ H2

- The conjecture has the form *theory, hypotheses* $\rightarrow$ *conclusion*.
- Consider a lattice (the theory) in which the H2 (the conclusion) is false.

Lattice Theory Example: Guiding Interpretation

Mace4 Input

```
formulas(assumptions).

  % Lattice theory

  x v y = y v x.
  (x v y) v z = x v (y v z).
  x ^ y = y ^ x.
  (x ^ y) ^ z = x^ (y ^ z).
  x ^ (x v y) = x.
  x v (x ^ y) = x.

end_of_list.

formulas(goals).  % falsify these formulas

  x ^ (y v (x ^ z)) = x ^ (y v (z ^ ((x ^ (y v z)) v (y ^ z)))) # label(H2).

end_of_list.
```

Lattice Theory: Guiding Interpretation

Mace4 Result

```
interpretation( 6, [number=1, seconds=0], [

        function(c1, [2]),
        function(c2, [3]),
        function(c3, [4]),

        function(^(_,_), [ 0, 0, 0, 0, 0, 0,
                           0, 1, 2, 3, 4, 5,
                           0, 2, 2, 0, 0, 0,
                           0, 3, 0, 3, 5, 5,
                           0, 4, 0, 5, 4, 5,
                           0, 5, 0, 5, 5, 5]),

        function(v(_,_), [ 0, 1, 2, 3, 4, 5,
                           1, 1, 1, 1, 1, 1,
                           2, 1, 2, 1, 1, 1,
                           3, 1, 1, 3, 1, 3,
                           4, 1, 1, 1, 4, 4,
                           5, 1, 1, 3, 4, 5])]).
```

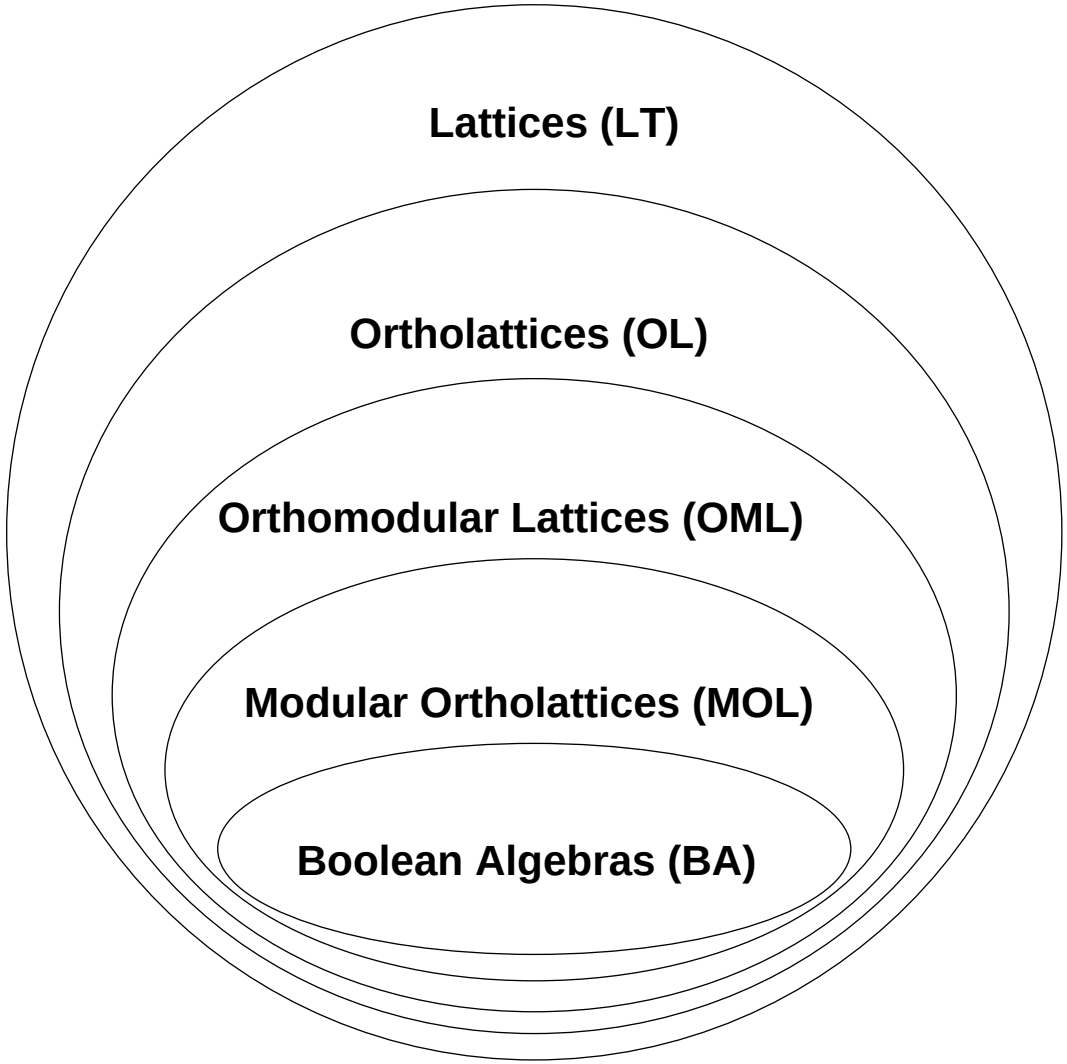
Lattice Theory: Search with Guiding Interpretation

- Give Prover9 the guiding interpretation.
- Tell Prover9 to use the selection ratio (age=1 : false=4 : true=1).
- Proof in 10 seconds.
- Proof in 1 hour without guidance.

How does the interpretation help to find a proof?

A Chain of Varieties: LT, OL, OML, MOL, BA

As structures (algebras):



A Chain of Varieties: LT, OL, OML, MOL, BA

Lattice Theory (LT)

$$\begin{array}{ll} (x \vee y) \vee z = x \vee (y \vee z). & (x \wedge y) \wedge z = x \wedge (y \wedge z). \\ x \vee y = y \vee x. & x \wedge y = y \wedge x. \\ x \vee (x \wedge y) = x. & x \wedge (x \vee y) = x. \end{array}$$

For Ortholattices (OL), include a unary operation with the following constraints.

$$\begin{array}{l} x \wedge y = (x' \vee y')'. \\ x'' = x. \\ x \vee x' = 1. \end{array}$$

For Orthomodular Lattices (OML), add the following constraint.

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

For Modular Ortholattices (MOL), add the following constraint.

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

For Boolean Algebras (BA), add the following constraint.

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

Modular Ortholattice (MOL) Single Axiom: The Problems

Consider the equations

$$f(f(y,x),f(f(f(x,x),z),f(f(f(f(f(x,y),z),z),x),f(x,u)))) = x \qquad \text{(MOL)}$$

$$f(x,f(y,f(x,f(z,z)))) = f(x,f(z,f(x,f(y,y)))) \qquad \text{(M)}$$

$$f(x,f(f(y,z),f(y,z))) = f(y,f(f(x,z),f(x,z))) \qquad \text{(A)}$$

- (MOL) is a single axiom for modular ortholattices in terms of the Sheffer stroke (NAND).
- Problem 1 (modularity property): (MOL) $\rightarrow$ (M).
- Problem 2 (associativity property): (MOL) $\rightarrow$ (A).

MOL Single Axiom: Selecting Interpretations

- Modularity property.
  - Consider the chain of varieties: OL, OML, MOL, BA

    (Ortholattices, Orthomodular Lattices, Modular Ortholattices, Boolean Algebra).
  - Let OML be the “theory”, and use the smallest non-modular OML (size 10) to guide the search.
  - Proof in 10 minutes with guidance; proof in 50 minutes without.
- Associativity property.
  - How do we find a nonassociative “theory” in which to work?
  - Simple answer: Consider nonassociative interpretations that satisfy other MOL properties. Pick one of size 8.
  - Proof in 44 seconds with guidance; proof in 162 seconds without.

Variable Ordering

Extending the term ordering with variables

Variable Ordering: Background

- Proof search based on term ordering and term rewriting.
- A simplification ordering allows equations to be used as rewrite rules.
  - E.g., KBO (Knuth-Bendix Ordering), LPO (Lexicographic Path Ordering).
- Ordinarily, term rewriting always produces smaller terms.
  - Orientable rules, e.g, $x'' = x$, are always applied.
  - A non-orientable rule, e.g., $x * y = y * x$, is applied only if it produces a smaller term.
- Many proof procedures based on these term orderings are *complete*.

Variable Ordering: An Incomplete Strategy

- When deciding whether to apply a non-orientable rewrite rule, include variables in the term ordering:

  variables $\prec$ constants

  $x \prec y \prec z \prec u \prec v \prec \cdots$

  In other words, treat variables as constants when comparing terms.

- We have no theoretical basis for this method.
- The method is incomplete (it can block all proofs).
- It can be used with KBO or with LPO.

Variable Ordering: Median Algebra Problem

Axioms for Median Algebra

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

Conclusion

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

- Note that the first two axioms allow the arguments to be permuted in any way.

Variable Ordering: Canonicalization

- Consider the non-orientable rewrite rules

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

- If $v_1 \prec v_2 \prec v_3 \prec v_4 \prec v_5$,
  the canonical form of

$$f(v_4, f(v_3, v_5, v_1), v_2)$$

  is

$$f(v_2, v_4, f(v_1, v_3, v_5))$$

- This (incomplete) method drastically reduces the search space.

- Proof in about 15 minutes (no proof without variable ordering).

Introducing Equational Definitions

Introducing Equational Definitions

Emphasize “important” terms.

- A very simple, human-like strategy.
  - Input equational definitions, e.g., define a binary operation g:

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

  - Arrange the term ordering so that the defined operation is introduced whenever possible, that is, use the definition as a rewrite rule:

$$f(f(x, x), f(y, y)) \longrightarrow g(x, y)$$

Definition: Ortholattice Example

- The Problem (f is the Sheffer stroke, i.e., NAND):

  Given: $f(f(f(f(x,y),f(y,z)),u),f(y,f(f(y,f(f(x,x),x)),z))) = y$
  Prove: $f(x,f(f(y,z),f(y,z))) = f(y,f(f(x,z),f(x,z)))$

- Definitions:

  Join: $x \vee y = f(f(x,x),f(y,y))$
  Meet: $x \wedge y = f(f(x,y),f(x,y))$
  Complementation: $x' = f(x,x)$

- Much easier to prove with definitions

  – proof is in terms of the defined operations

  – shorter equations in proof

The Robbins Problem with Definitions(1)

- Given

$$x \vee y = y \vee x \qquad \text{(Commutativity)}$$
$$(x \vee y) \vee z = x \vee (y \vee z) \qquad \text{(Associativity)}$$
$$((x \vee y)' \vee (x \vee y')')' = x \qquad \text{(Robbins)}$$

- Prove

$$(x \vee y')' \vee (x' \vee y')' = y \qquad \text{(Huntington)}$$

- First proved by EQP in 1996.
- No proof (human or computer) since then?

The Robbins Problem with Definitions (2)

- No proof found without definitions (search for several weeks)
- Consider the definition.

$$f(x) = x + (x + x')'$$

  Proof in about half an hour.

- Consider the pair of definitions.

$$g(x) = (x + x')'$$
$$h(x) = x + (x + (x + g(x)))$$

  Proof in about 45 seconds.

Concluding Remarks

- Selecting interpretations and definitions.
  - input form expert (mathematician)
  - automatically, by some rules
- Incomplete strategies, e.g., variable ordering.
- Work is needed in the following areas.
  - experimentation on hard problems
  - analysis of hard proofs
  - application to non-equational problems
  - work with mathematicians on problems of interest to them

Thank You