# Automated Reasoning Methods Used to Prove the Robbins Conjecture

Joe Hurd

joe.hurd@comlab.ox.ac.uk.

Intelligent Systems I

Computer Science
University of Oxford

# History of the Robbins Conjecture

- Definition (George Boole 1854)
  Boolean algebras satisfy the following ten axioms:
  - $x \cup y = y \cup x$
  - $x \cap y = y \cap x$
  - $x \cup (y \cup z) = (x \cup y) \cup z$
  - $x \cap (y \cap z) = (x \cap y) \cap z$
  - $x \cup (x \cap y) = x$
  - $x \cap (x \cup y) = x$
  - $x \cap (y \cup z) = (x \cap y) \cup (x \cap z)$
  - $x \cup (y \cap z) = (x \cup y) \cap (x \cup z)$
  - $x \cup \overline{x} = 1$
  - $x \cap \overline{x} = 0$
- See Boole's classic book *An investigation into the Laws of Thought*.

# History of the Robbins Conjecture

- Theorem (E. V. Huntington 1933)
  The following three equations are a basis for Boolean algebras:
  - $x \cup y = y \cup x$ (Commutativity)
  - $x \cup (y \cup z) = (x \cup y) \cup z$ (Associativity)
  - $\overline{\overline{x} \cup \overline{y}} \cup \overline{\overline{x} \cup y} = x$ (Huntington equation)
- Plus: $x \cap y \equiv \overline{\overline{x} \cup \overline{y}}$, $0 \equiv x \cap \overline{x}$, and $1 \equiv x \cup \overline{x}$.
- These three equations being a basis means:
  - Each equation must follow from the axioms for Boolean algebras. (Easy)
  - No equation must follow from the others. (Easy)
  - Each Boolean algebra axiom must follow from these equations. (Hard part)

# History of the Robbins Conjecture

- Conjecture (Herbert Robbins 1933)
  The following three equations are a basis for Boolean algebras:
  - $x \cup y = y \cup x$ (Commutativity)
  - $x \cup (y \cup z) = (x \cup y) \cup z$ (Associativity)
  - $\overline{\overline{x \cup y} \cup \overline{x \cup \overline{y}}} = x$ (Robbins equation)
- Note: the Robbins equation is simpler than the Huntington equation (one fewer occurrence of $^{-}$).
- It is sufficient to show that the Huntington equation holds in these so-called *Robbins algebras*.
- Tarski worked on the problem, and gave it to graduate students and visiting mathematicians.

# History of the Robbins Conjecture

- Theorem (William McCune 1997)
  Robbins algebras are Boolean.

  Proof: McCune implemented an automated reasoning system called EQP which found a proof that showed the Huntington equation logically followed from the equations for Robbins algebras. □

- In this lecture: some of the automated reasoning methods used to prove the Robbins Conjecture.

# Reasoning in First Order Logic

- Resolution for first order logic was invented by Alan Robinson in 1965.

$$\frac{A \vee C \quad \neg B \vee D}{(C \vee D)[\sigma]}$$

where $\sigma = mgu(A, B)$.

- The same as resolution for propositional logic.
- Unification used to set first order logic variables.
- To be complete it also needs the factorization rule:

$$\frac{A \vee B \vee C}{(A \vee C)[\sigma]}$$

where $\sigma = mgu(A, B)$.

# First Order Logic with Equality

- Resolution is complete for first order logic, but not for first order logic with equality.
  - The set of clauses $\{\neg(c = c)\}$ is unsatisfiable, but resolution can't find a contradiction.
- The problem is that resolution implicitly considers all models, but we only want to consider normal models in which '$=$' is interpreted as equality.
  - In the above example, the clause set *is* satisfiable if we interpret '$=$' as a binary relation that is always false.

# First Order Logic with Equality

- Restrict to normal models by adding equality axioms.
- Equality is an *equivalence relation*:
  - $\forall x.\ x = x$ (reflexivity)
  - $\forall x, y.\ x = y \Rightarrow y = x$ (symmetry)
  - $\forall x, y, z.\ x = y \wedge y = z \Rightarrow x = z$ (transitivity)
- Equality is a *congruence*:
  - For each $n$-ary function symbol $f$, add the axiom
    $$\forall x_1, \ldots, x_n, y_1, \ldots, y_n.\ x_1 = y_1 \wedge \cdots \wedge x_n = y_n \Rightarrow f(x_1, \ldots, x_n) = f(y_1, \ldots, y_n)$$
  - For each $n$-ary relation symbol $R$, add the axiom
    $$\forall x_1, \ldots, x_n, y_1, \ldots, y_n.\ x_1 = y_1 \wedge \cdots \wedge x_n = y_n \wedge R(x_1, \ldots, x_n) \Rightarrow R(y_1, \ldots, y_n)$$

# First Order Logic with Equality

- Theorem: The set of formulas $\Delta \cup \text{EqualityAxioms}(\Delta)$ is satisfiable if and only if the set of formulas $\Delta$ is satisfiable in a normal model.

  Proof: ($\Leftarrow$): Easy, since $\text{EqualityAxioms}(\Delta)$ is satisfied in any normal model.

  ($\Rightarrow$): Let $M$ be a model in which $\Delta \cup \text{EqualityAxioms}(\Delta)$ is satisfied. Quotient $M$ by the equivalence relation $M(=)$ to obtain a normal model in which $\Delta$ is satisfied. $\square$

- Corollary: Adding equality axioms makes resolution complete for first order logic with equality.

# Paramodulation

- Though complete, resolution with equality axioms is not efficient enough to prove the Robbins conjecture :-(
- Much more powerful is the paramodulation rule:

$$\frac{C \vee s \doteq t \quad D \vee P[s']}{(C \vee D \vee P[t])[\sigma]}$$

where $\sigma = mgu(s, s')$ and $s'$ is a non-variable.

- Theorem (Brand 1975)
Paramodulation plus resolution and the reflexivity axiom is refutationally complete for first order logic with equality.

# Paramodulation Refinements

- Paramodulation has been in use since the 1960s, and is not efficient enough to prove the Robbins conjecture :-(
- McCune implemented three main refinements of paramodulation to find a proof:
  - Demodulation.
  - The basic strategy.
  - AC unification and matching.

# Demodulation

- Suppose we have derived an equation $l = r$, where:
  - the size of the term $l$ is greater than the size of the term $r$; and
  - no variable appears more often in $r$ than $l$.
- The demodulation rule is as follows:

$$\frac{C \vee P[l[\sigma]]}{C \vee P[r[\sigma]]}$$

- Demodulation is used to simplify clauses and allow more unification.
- Resolution and paramodulation plus demodulation is still refutationally complete.

# The Basic Strategy

- Consider the paramodulation step

$$\frac{f(x) = h(x) \quad P(f(g(y)))}{P(h(g(y)))}$$

- In the conclusion it is redundant to apply paramodulation into the term $g(y)$, since we could have done that before applying this rule.
- The basic strategy generalizes this by blocking paramodulation at any term introduced as part of the substitution.
- The basic strategy cuts down the search space.
- Resolution and paramodulation with the basic strategy is refutationally complete, even when combined with demodulation.

# AC Unification

- The terms $f(x) \cup c \cup h(x)$ and $h(c) \cup c \cup f(y)$ do not unify.
- But if the unification procedure knew that $\cup$ was Associative and Commutative, then $\{x \mapsto c, y \mapsto c\}$ would be a valid unifier: this is AC unification.
- Potential problem: Given two terms both of the form $t_1 \cup \cdots \cup t_n$, AC unification can produce $n!$ unifiers.
- Solution: EQP uses a heuristic called the super-0 strategy to restrict the number of unifiers.
  - Given the terms $x \cup x \cup x$ and $y \cup z \cup u \cup v$:
  - without super-0 gives 1,044,569 unifiers; and
  - with super-0 gives 139 unifiers.
- The super-0 strategy makes EQP theoretically incomplete (though not observed in practice).

# Proving the Robbins Conjecture

- With all these refinements implemented in EQP, McCune was able to automatically prove the Robbins conjecture :-)
- It was the first case where a computer had found a checkable proof of a theorem that real mathematicians had failed on.
- The New York Times printed a story about it.
  - Robbins, then an 81 year old mathematician working at Rutgers, was quoted as saying “I’m glad I lived long enough to see it”.
  - McCune on automated reasoning: “It’s best, he said, to think of a computer as "just another colleague, one that is sometimes helpful, but often not.”