Topics in Automated Theorem Proving

Course (236714, 2013/14)

Johann A. Makowsky*

* Faculty of Computer Science,
Technion - Israel Institute of Technology,
Haifa, Israel
janos@cs.technion.ac.il

Course homepage
http://www.cs.technion.ac.il/~janos/COURSES/THPR

Lecture 4 (November 7, 2013)

Ground clauses

- A ground literal is an atomic or negated atomic formula with constant terms and no free variables.

- A ground clause is a clause consisting of ground literals. and no free variables.

We have reduced satisfiability of first order logic

to satisfiability of propositional logic.

Monadic First Order Logic

Let us look at the case of first order logic with the following restrictions:

- We have only unary relation symbols.
- We have no equality.
- We do allow equality.

We discuss Skolem normal form.

Homework: Show that in this case satisfiability is decidable.

Theorem: If we have only one binary relation symbol and equality, satisfiability is not decidable.

E. Börger and E. Grädel and Y. Gurevich,

The Classical Decision Problem, Springer-Verlag, 1997

Avoiding too many terms, I

Now look at a formula

$$\Phi = \forall \bar{x} \exists \bar{y} \, [\phi(\bar{x}) \wedge \psi(\bar{y})]$$

where ϕ, ψ are quantifierfree.

This is equivalent to

$$\Psi = \forall \bar{x} \, [\phi(\bar{x}) \wedge \exists \bar{y} \psi(\bar{y})]$$

- Skolemizing Φ produces several functions, hence infinitely many terms.

- Skolemizing Ψ produces only constant symbols, hence finitely many terms.

Conclusion: Putting first into prenex normal form and then introducing Skolem functions is not always preferable. **Homework: Discuss strategies to safe terms when Skolemizing.**

Avoiding too many terms, II

We do not want to instantiate all clauses with all the terms!

- Assume we have

$$S_1(y) \vee R(x) \text{ and } S_2(x) \vee \neg R(y^2)$$

- Substituting for y the term u^2 and for x the term u^4 we get

$$S_1(u^2) \vee R(u^4) \text{ and } S_2(u^4) \vee \neg R(u^4)$$

- Resolution gives

$$S_1(u^2) \vee S_2(u^4)$$

- Similarly

$$S_1(y) \vee R(x) \vee R(y^2)$$

gives

$$S_1(u^2) \vee R(u^4) \vee R(u^4)$$

and therefore

$$S_1(u^2) \vee R(u^4)$$

Handling substitutions

There is theory behind this!

Unification theory

John Alan Robinson, 1928 *

John Alan Robinson,
A Machine-Oriented Logic Based on the Resolution Principle,
Journal of the ACM, vol 12, 2341, 1965.

See Lecture 4

Unification (according to Wikipedia)

- (link to wikipedia)
- (relative)

The deduction rules

Let $\mathbf{Term}(\tau)$ be the set of terms over the vocabulary τ. Let σ be a substitution, a function from the variables $\mathbf{Var} \to \mathbf{Term}(\tau)$.
Let $C(x_1, \ldots, x_n)$, $D(x_1, \ldots, x_n)$ be clauses with free variable $\bar{x}$ and $L(x_1, \ldots, x_n)$ be a literal.

We have two deduction rules:

Factoring

$$\frac{C(x_1, \ldots, x_n)}{C(\sigma(x_1), \ldots, \sigma(x_n))}$$

Resolution

$$\frac{C(x_1, \ldots, x_n) \vee L(x_1, \ldots, x_n), D(x_1, \ldots, x_n) \vee \neg L(x_1, \ldots, x_n)}{C(\sigma(x_1), \ldots, \sigma(x_n) \vee D(\sigma(x_1), \ldots, \sigma(x_n))}$$

Soundness

- Factorization is a special case of the rule

$$\frac{\forall \bar{x} \phi(\bar{x})}{\phi(\bar{t})}$$

where $\bar{t}$ is a sequence of terms.

In human language: If all x are Human, so Socrates is a Human.

- Resolution combines the above with propositional resolution.

Completeness

We use Herbrand's Theorem.

Let Σ be a set of FOL(τ) and Σ_{sk} its Skolem Normal Form.

- Applying Factoring we can generate all ground clauses.
- Applying resolution we can check satsifiability.

Problem: How to choose the right substitutions efficiently?

The unification problem.

The problem we are facing now:

Given two sequences terms

$t_1(\bar{x}), \ldots, t_n(\bar{x})$ and $u_1(\bar{x}), \ldots, u_n(\bar{x})$

- does there exist a substitution σ such that for all $i \leq n$

  $$t_i(\sigma(\bar{x})) = u_i(\sigma(\bar{x}))$$

  as terms.

- If yes, how can we find it, of no, how can we be sure?

A substitution σ with the above properties is called a
unifier for $t_1(\bar{x}), \ldots, t_n(\bar{x})$ and $u_1(\bar{x}), \ldots, u_n(\bar{x})$.

Note: It is enough to solve the unification for pairs of terms $t(\bar{x})$ and $u(\bar{x})$.

Comparing unifiers

Let σ_1, σ_2 be two unifiers for t and u.

- σ_1 is more general than σ_2 if the is a substitution ρ such that
$$\rho \circ \sigma_1 = \sigma_2$$
- σ_1 is a most general unifier, of for every other unifier σ_2 there exists a substitution ρ such that
$$\rho \circ \sigma_1 = \sigma_2$$

Proposition: If σ is a most general unifier for t and u,

then it is unique up to renaming variables.

Lecture 5, November 14, 2013

- To be written

Tirgul 5, November 21, 2013

- We complete the QE for equality only.

- The following formulas are logically equivalent:

$$\exists x(\phi(x) \wedge x = y) \text{ and } \phi(x) \mid^x_y$$

where $\phi(x) \mid^x_y$ is the result of substituting y for x in ϕ.

Proof:
Use the definition of the meaning function for $\exists$ and the definition of substitution. Q.E.D.

Lecture 6, November 21, 2013

Fourier-Dines-Motzkin Procedure

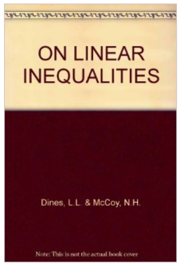
Fourier 1826, Dines 1918, Motzkin 1936

- The structure: $\mathcal{R}_+ = \langle \mathbb{R}, +, \leq, 0, 1 \rangle$
- The Theorem: $\mathcal{R}_+$ allows QE.
- Some history

Jean Baptiste Joseph Fourier (1768 – 1830)

Lloyd L. Dines (1885 – 1964)

Theodore Samuel Motzkin (1908 – 1970)

- Wikipedia on Jean Baptiste Joseph Fourier, (web), (relative),
- 

  L.L. Dines and N.H. McCoy, On Linear Inequalities, Trans Royal Soc Canada (1933)
- Obituary of Theodore Motzkin, (web), (relative),

Terms and atomic formulas for $\mathcal{R}_+$.

Atomic Terms: Variables x_i, constants $0, 1$,

Constant Terms: Using commutativity, associativity and $(x + 0) = x$, we can reduce every constant term to

$$(n) = \underbrace{1 + 1 + \ldots + 1}_{n}$$

We write $\mathbf{n} \cdot t$ for $(\underbrace{t + t + \ldots + t}_{n})$.

Terms: If s, s_i, t, t_i $(i \in \mathbb{N})$are terms, so are

$(s = t)$, $\sum_{i=0}^{k} \mathbf{n}_i t_i$

Atomic Formulas: $t_1 \approx t_2$, $t_1 \leq t_2$, $\mathbf{n}t_1 \approx \mathbf{m}t_2$

$$\sum_{i=0}^{k} \mathbf{n}_i t_i \approx \sum_{j=0}^{\ell} \mathbf{m}_j s_j$$

Normal form for quantifier-free formulas

- Every term $t(x_1, \ldots, x_n)$ can be writen as
$$t = \mathbf{n}_1 \cdot x_1 + \mathbf{m}_1 + \sum_{i=2}^{n} \mathbf{m}_i \cdot x_i = \mathbf{n}_1 \cdot x_1 + s(x_2, \ldots, x_n)$$
where x_1 does not occur in s.

- We introduce a new function symbol minus$(t) = -t$ with the rules $-t + t = t + (-t) = 0$, $-(-t) = t$ and $-(s + t) = (-s) + (-t)$.
and binary relation symbols $\{<, =, >, \geq\}$ with the obvious interpretations.

- Using minus$(t) = -t$ we now can show that every atomic formula is equivalent to a formula of the form
$$x \Delta t(\bar{y}) \text{ or } s(\bar{y}) \Delta x$$
where $\Delta \in \{\leq, <, =, > \geq\}$.

- Conversely, every atomic formula $A(x_1, \ldots, x_n)$ in which minus is used is equivalent to an atomic formula $B(x_1, \ldots, x_n)$ in which minus is not used.

- Similarily, the symbols $\{<, =, > \geq\}$ can be eliminated from quantifier-free formulas without introducing quantifiers.

To be done by induction!

The theory $Th(\mathfrak{R}_+)$ admits effective QE and hence is complete.

Fourier 1826, Dines 1918, Motzkin 1936

It is enough to prove it for formulas of the form

$$\exists x \left(\bigwedge_i t_i(\bar{y}) \Delta_i x \wedge \bigwedge_j x \Delta_j t'_j(\bar{y}) \wedge \bigwedge_k s_k(\bar{y}) \Delta_k 0 \right)$$

Where $\Delta_i, \Delta_j \in \{\leq, <\}$.

This is equivalent to

$$\exists x \left(\bigwedge_i t_i(y) \Delta_i x \wedge \bigwedge_j x \Delta_j t'_j(\bar{y}) \right) \wedge \left(\bigwedge_j s_j(\bar{y}) \Delta_j 0 \right)$$

Proof continued

But

$$\exists x \left(\bigwedge_i t_i(y) \Delta_i x \wedge \bigwedge_j x \Delta_j t'_j(\bar{y}) \right)$$

is equivalent to

$$\bigwedge_{i,j} t_i(\bar{y}) \Delta_{i,j} t'_j(\bar{y})$$

where

$$\Delta_{i,j} = \begin{cases} \leq & \text{if both } \Delta_i = \Delta_j =\leq \\ < & \text{if } \Delta_i =< \text{ or } \Delta_j =< \end{cases}$$

Q.E.D.

The structure $\mathcal{Z}_+ = \langle \mathbb{Z}, +, \leq, 0, 1 \rangle$, Presburger Arithmetic.

- Can we have QE also in this case?
- We can add unary relation symbols $D_m(x)$ with the interpretation x is divisible by m.
- **Theorem:**(M. Presburger) $\mathcal{Z}_+ = \angle \mathbb{Z}, +, \leq, D_m(x), 0, 1 \rangle$ for $m \in \mathbb{N}$ has QE,

Mojżesz Presburger (19041943) (web), (relative),

$\mathcal{Z}_+ = \langle \mathbb{Z}, +, \leq, 0, 1 \rangle$ has no QE

- Let $A \subset \mathbb{Z}$. A is a ray, if A is finite or there is $a \in \mathbb{Z}$ with $A = A_+(a) = \{b \in \mathbb{Z} : b \geq a\}$ or $A = A_-(a) = \{b \in \mathbb{Z} : b \leq a\}$.
- Every quantifier-free definable set over $\mathcal{Z}_+$ is a ray.

  Use induction!
- $\exists x(x + x = y)$ defines a set which is not a ray.

  It defines the even numbers.

The real numbers

$$\mathcal{R}_{field} = \langle \mathbb{R}, +, \times, 0, 1 \rangle \text{ and } \mathcal{R}_{ofield} = \langle \mathbb{R}, +, \times, \leq 0, 1 \rangle$$

Theorem:(A. Tarski)

- $\mathcal{R}_{ofield}$ has EQ.
- $\mathcal{R}_{field}$ does not have EQ. We showed this already.

Alfred Tarski-Teitelbaum (1901 – 1983) (web), (relative),

Examples for QE over the reals

- Solvability of polynomial equations: $\exists x \sum_{i=0}^{k} a_i x_i = 0$.

  k odd and $a_k \neq 0$ this is always true.

  k even and $a_k \neq 0$ this may be difficult......

- More sophistigated examples may be found in:
  D. Lazard
  Quantifier elimination: Optimal solutions for two classical examples,
  Journal of Symbolic Computation, vol. 5 (1988) pp. 261–266.