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 3 (October 31, 2013)

Herbrand's Theorem

A model theoretic (semantic) proof

- Prenex normal form and universal formulas
- Substructures
- Universal formulas are preserved under substructures
- Skolem normal form
- Term models and the Löwenheim-Skolem Theorem
- Compactness and Herbrand's Theorem

Prenex normal form and universal formulas

- A τ-formula ϕ is in prenex normal form (PNF) if
$$\phi = Q_1 x_1 Q_2 x_2 \ldots Q_n x_n B(x_1, \ldots, x_n, y_1, \ldots y_k)$$
where Q_i is $\forall$ or $\exists$, $x_i : i = 1, \ldots n$ are bound variables,
$y_j : j = 1, \ldots k$ are free variables, and B is quantifierfree.

- A τ-formula ϕ is universal (existential) if it is in PNF
and all the Q_i are $\forall$ ($\exists$).

- **Exercise:** Give inductive definitions of the above.

We showed in Logic and Sets:
Theorem: Every formula is equivalent to a formula in PNF with the same free variables.

How would you show that a formula ϕ is not equivalent to a universal formula?

Substructures

- Let $\mathfrak{B}$ be a τ-structure with universe B and $A \subseteq B$, $A \neq \emptyset$. A can be viewed as a τ-substructure $\mathfrak{A}$ of $\mathfrak{B}$, $\mathfrak{A} \subseteq \mathfrak{B}$, if
  (i) for every n-ary relation symbol $R \in \tau$ and every tuple $\bar{a} \in A^n$ we have $\bar{a} \in \mathfrak{A}(R)$ iff $\bar{a} \in \mathfrak{B}(R)$, and
  (ii) for every m-ary function symbol $F \in \tau$ and every tuple $\bar{a} \in A^m$ the meaning $\mathfrak{B}(F)(\bar{a}) \in A$.

- **Examples:** Discuss the substructures of the natural numbers, or the real numbers with various vocabularies.

- **Homework:** Discuss under which conditions the intersection of any family of substrcutures of $\mathfrak{B}$ is again a substructure of $\mathfrak{B}$.

Universal formulas are preserved under substructures

Principle: Let $A \subseteq B$. Assume all $b \in B$ have a property P.
Then all $a \in A$ have property P.

- Let $\mathfrak{A} \subseteq \mathfrak{B}$ be τ-structures and ϕ be a universal τ-formula, possibly with free variables. Let $z : \mathbf{VAR} \to A$ be an assignment such that $\mathfrak{B}, z \models \phi$.
- We show by induction on ϕ that $\mathfrak{A}, z \models \phi$.
- For quantifierfree ϕ we note that $\mathfrak{B}, z \models \phi$ iff $\mathfrak{A}, z \models \phi$.
- For universal quantification we use the principle above.

Q.E.D.

Homework: Formulate and prove the corresponding situation for existential formulas.

Tarski's Theorem: A first order sentence is preserved under substructures of models of Σ iff it is equvalent over Σ to a universal sentence.

Term models

* Terms are defined inductively: constant symbols and variables are terms. Then close under application of function symbols.

* constant terms are terms without free variables.

* A term model is a τ-structure where each element is the interpretation of a constant term.

Theorem: Let τ be a vocabulary with at least one constant symbol, and let Σ be a set of universal τ-sentences.

Then Σ is satisfiable iff it is satisfiable in a term model.

Proof

- Let $\mathfrak{A}$ be a model of Σ. Let $\mathfrak{A}_{term}$ be the substructure of $\mathfrak{A}$ which consists of the interpretations of the constant τ-terms in $\mathfrak{A}$.
- Show that, indeed, $\mathfrak{A}_{term}$ is a substructure of $\mathfrak{A}$.
- Now use the fact that universal sentences are preserved under substructures.

Q.E.D.

Herbrand's Theorem

Let $\phi = \forall x_1, \ldots, x_n B(x_1, \ldots, x_n)$ be a universal τ-sentence.

The following are equivalent:

(i) ϕ is not satisfiable.

(ii) $\neg\phi$ is valid.

(iii) The set $G(\phi) = \{B(t_1, \ldots, t_n) : t_i \text{ is a } \tau-\text{term}\}$ is not satisfiable.

(iv) There is a finite set T of τ-terms such that the set $\{B(t_1, \ldots, t_n) : t_i \in T\}$ is not satisfiable.

(v) There is a finite set T of τ-terms such that the formula $\bigvee_{t_1,\ldots,t_n \in T^n} \neg B(t_1, \ldots, t_n)$ is valid.

Proof of Herbrand's Theorem

(i) $\leftrightarrow$**(ii)** Basic.

(i) $\leftrightarrow$**(iii)** Assume ϕ has a model $\mathfrak{B}$. As ϕ is universal, the term submodel $\mathfrak{B}_{term}$ of $\mathfrak{B}$ satisfies $G(\phi)$.
Conversely, assume $G(\phi)$ has a model $\mathfrak{B}$. As each formula in $G(\phi)$ is quantifier free, the term submodel $\mathfrak{B}_{term}$ of $\mathfrak{B}$ satisfies $G(\phi)$ and also ϕ.

(iii) $\leftrightarrow$**(iv)** This is compactness.

(iv) $\leftrightarrow$**(v)** Basic

Q.E.D.

Problem: How to find T?

Semantic vs syntactic proof of Herbrand's Theorem

- Our proof was purely semantic.
- Using suitable deduction systems for which the Completeness Theorem holds, one can read from a proof sequence for $\neg\phi$ (ii) a finite set T of terms needed in (v).
- However, we don't have that proof sequence, and want to find it using computers.
- Herbrand's original proof was syntactic and had a gap.
- Syntactic proofs of Herbrand's Theorem can be obtained using Gentzen calculus or Tableaux proofs.

Skolem functions (motivation)

Look at $\tau = \{R\}$ with one binary relation symbol and
at the sentence $\phi = \forall x \exists y R(x, y)$.

- ϕ is satisfiable in a τ-structure $\mathfrak{A}$ iff there is a function $f : A \to A$ such that for all $a \in A$ we have that $(a, f(a)) \in \mathfrak{A}(R)$.

  Here $\mathfrak{A}(R)$ is the interpretation of R in $\mathfrak{A}$.
  To show this we also use the Axiom of Choice.

- In other words,

$$\forall x \exists y R(x, y)$$

  is satisfiable iff the second order sentence

$$\exists F \forall x R(x, F(x))$$

  is satisfiable.

- Let $\tau' = \{R, F\}$ where F is a unary function symbol.
  Then $\forall x \exists y R(x, y)$ is satisfiable (as a τ-sentence)
  iff $\forall x R(x, F(x))$ is satisfiable (as a τ'-sentence).

Skolem functions (theorem)

Theorem: For every τ-sentence ϕ there is a vocabulary $\tau_{sk} = \tau \cup \{F_1, \ldots, F_k\}$ with additional function symbols, and a universal τ_{sk}-sentence ψ such that

ϕ is satisfiable iff ψ is satisfiable.

Furthermore, if $\phi(x_1, \ldots, x_m)$ has free variables the $\psi(x_1, \ldots, x_m)$ has the same free variables.

The interpretations of the function symbols $F_1, \ldots, F_k$
are called Skolem functions

ψ is called the Skolem Normal Form of ϕ.

Skolem Normal Form (proof)

- First we put ϕ into Prenex Normal Form (PNF) and obtain ϕ_1.
- Then we proceed by induction over the number of quantifier alternations.
- If
$$\phi_1 = \forall x_1, \dots x_{k_1} \exists y_1 \dots, y_{m_1} B_1(\bar{x}, \bar{y}, z_1, \dots, z_{k_2})$$
we introduce m_1 many $k_1 + k_2$-ary function symbols $F_1, \dots, F_{m_1}$ and form
$$\psi = \forall x_1, \dots x_{k_1} B_1(\bar{x}, F_1(\bar{x}, \bar{z}) \dots, F_{m_1}(\bar{x}, \bar{z}))$$
Note that the functions also depend on the free variables!
- Like this we eliminate successively all the existential quantifiers.
- Check it for $\forall z \exists u R(x, y, z, u)$ and for $\forall x \exists y \forall z \exists u R(x, y, z, u)$.

A detailed example: Linear orderings

We have one binary relation symbol R.

The axioms for a linear order $\leq$ are universal:
transitivity, reflexivity, comparability.

Add some of the following axioms:

- There is a first element.
- There is no last element.
- The order is dense.
- The order is discrete.

Discuss term models and Skolem functions!

Another example: the ordered field of the real numbers

The vocabulary consists of a binary relation symbol R for order and two binary function symbols $F_+, F_\times$ for addition and multiplication and **two constant symbols** 0 **and** 1.

We write the axioms of an ordered field: $\langle K, 0, 1, +, \times, \leq \rangle$.

- $\langle K, 0, + \rangle$ is an abelian group.
- $\langle K - \{0\}, 1, \times \rangle$ is an abelian group.
- $\langle K, \leq \rangle$ is a linear order.
- $\langle K, 0, 1, +, \times \rangle$ is a field.
- $\langle K, 0, 1, +, \times, \leq \rangle$ is an ordered field.
- $\langle K, 0, 1, +, \times, \leq \rangle$ is a real closed ordered field.

Discuss term models and Skolem functions!

The Löwenheim-Skolem Theorem

Theorem: Let Σ be a countable set of τ-sentences. If Σ is satisfiable then it is also satisfiable in a finite or countable domain.

Proof:

- We put each $\phi \in \Sigma$ into Skolem Normal Form by using different function symbols for each ϕ. The result of this is τ_{sk} and Σ_{sk} which are both countable.
- Σ_{sk} is a set of universal τ_{sk}-sentences.
- Let T_{sk} be the set of τ_{sk}-terms. T_{sk} is also countable.
- Let $\mathfrak{A}$ be an uncountable model of Σ_{sk}, and let $\mathfrak{A}_{term}$ be its term submodel.
- $\mathfrak{A}_{term}$ is countable and $\mathfrak{A}_{term} \models \Sigma_{sk}$.

Q.E.D.

Herbrand's Theorem with Skolem functions

Given a set of τ-sentences Σ we want to check satisfiability.

We want to combine **Herbrand's Theorem** with **Skolem functions** so we can use **resolution**:

- We first put Σ into Skolem Normal Form and obtain Σ_{sk}.
- Each $\phi \in \Sigma_{sk}$ is universal and of the form $\forall \bar{x} B_\phi(\bar{x})$. We put $B_\phi(\bar{x})$ into CNF and obtain a set of clauses S_ϕ in the variables $\bar{x}$ which are universally quantified.
- Next we form

$$S(\Sigma) = \{C(\bar{t}) : C \in S_\phi, \phi \in \Sigma_{sk}, \bar{t} \in T^\infty_{sk}\}$$

  where T^∞_{sk} is the set of finite sequences of constant terms over τ_{sk}.

Theorem: Σ is not satisfiable iff

the set of variable-free clauses $S(\Sigma)$ is not satisfiable

iff some finite subset $S_0 \subseteq S(\Sigma)$ is not satisfiable.

Homework for Lecture 3

Practice (truly practice)

- converting First Order formulas into Prenex Normal Form
- converting First Order formulas into Skolem Normal Form

If you feel insecure with Logic read again the Logic Notes at

http://www.cs.technion.ac.il/ janos/COURSES/THPR/2013-14/logic-notes-fixed.pdf

Tutorial 3 (November 7, 2013)

Substitutions

- Definition of substitutions of variables by terms.
- Properties of Substitutions
- Many examples

We also discuss the homework for lecture 3.