Logic (master program)

Georg Moser

Institute of Computer Science @ UIBK

Winter 2008

Summary of Last Lecture

Proposition

if Γ is satisfiable then Γ is consistent

Theorem

let Γ be countable set of sentences, if Γ consistent then Γ is satisfiable

Proof Plan

- let $C = \{c_1, c_2, c_3, \dots\}$ set of fresh constants and let $\mathcal{V}^+ = \mathcal{V} \cup C$
- we define a complete $\mathcal{V}^+$-theory T^+ with $\Gamma \subseteq T^+$ and
- $\forall$ sentences $\exists x \varphi(x) \in T^+$, we have $\varphi(c_i) \in T^+$ for some $c_i \in C$

based on this we construct a model $\mathcal{M}^+$ of T^+ and hence of Γ

Definition

T^+

we define T^+ in stages

1. set $T_0 = \Gamma$
2. enumerate the set of all $\mathcal{V}^+$-sentences

$$\varphi_1, \varphi_2, \varphi_3, \ldots$$

3. define T_{m+1} based on T_m and consider sentence φ_{m+1}; assume T_m has only used finitely many constants from C
4. if $T_m \cup \{\neg\varphi_{m+1}\}$ is consistent, set

$$T_{m+1} = T_m \cup \{\neg\varphi_{m+1}\}$$

5. if $T_m \cup \{\neg\varphi_{m+1}\}$ is not consistent, then $T_m \cup \{\varphi_{m+1}\}$ is consistent
6. in this case suppose $\varphi_{m+1} \neq \exists x \psi(x)$, then

$$T_{m+1} = T_m \cup \{\varphi_{m+1}\}$$

7. otherwise $T_{m+1} = T_m \cup \{\varphi_{m+1}\} \cup \{\psi(c_i)\}$ for fresh $c_i \in C$

finally let $T^+ = \bigcup_{m \geqslant 0} T_m$

Claim

the set T^+ is a complete theory, such that (i) $\Gamma \subseteq T^+$ and (ii) $\forall$ sentences $\exists x \varphi(x) \in T^+$, we have $\varphi(c_i) \in T^+$ for some $c_i \in C$

Proof of Claim

- T^+ is consistent; this follows from the consistence of each T_m
- T^+ is a complete theory such that $\Gamma \subseteq T^+$ and property (ii) holds follow by construction ∎

Definition

$\mathcal{M}^+$

we define $\mathcal{M}^+$ as a $\mathcal{V}^+$-structure such that

1. the universe of $\mathcal{M}^+$ is a set U^+ of closed $\mathcal{V}^+$-terms
2. in U^+ we identify all terms s, t such that $T^+ \vdash s = t$
3. set $c^{\mathcal{M}^+} = t \in U^+$, whenever $T^+ \vdash t = c$
4. set $f^{\mathcal{M}^+}(t_1, \ldots, t_n) = s$, whenever $T^+ \vdash f(t_1, \ldots, t_n) = s$
5. set $(t_1, \ldots, t_n) \in R^{\mathcal{M}^+}$, if $T^+ \vdash R(t_1, \ldots, t_n)$

Claim

for any sentence $\mathcal{M}^+ \models \varphi$ if and only if $T^+ \vdash \varphi$

■

Corollary — downward Löwenheim-Skolem

let Γ be a countable set of formulas, if Γ is consistent, then Γ has a countable model

Corollary — compactness

a countable set of formulas is satisfiable if and only if every finite subset is satisfiable

Corollary

for any countable set of sentences Γ, $\Gamma \vdash \varphi$ if and only if $\Gamma \models \varphi$

Homework

- Give a (correct) proof of "Corollary" 3.8.
- Exercise 3.7.
- Give a (correct) proof of "Corollary" 3.10.
- Exercise 3.19.
- Exercise 3.21.

Content

introduction, propositional logic, semantics, formal proofs, resolution (propositional)

first-order logic, semantics, structures, theories and models, formal proofs, Herbrand theory, completeness of first-order logic, properties of first-order logic, resolution (first-order)

introduction to computability, introduction to complexity, finite model theory

beyond first order: modal logics in a general setting, higher-order logics, introduction to Isabelle

Resolution (first-order)

Example

consider the following formula φ (over vocabulary $\mathcal{V} = \{a, b, c, d\}$)

$$(c \neq d) \wedge (b = d) \wedge ((a = d) \rightarrow (a = c)) \wedge ((a = b) \vee (a = d))$$

Question

is φ satisfiable?

Answer

no! observe

$$\{(a = b) \vee (a = d), (b = d)\} \models (a = d)$$
$$\{(a = d), ((a = d) \rightarrow (a = c))\} \models (c = d)$$

Question

how to show this automatically?

Paramodulation

Definition

(ground) paramodulation

$$\frac{C \vee s = t \quad D \vee u[s] = v}{C \vee D \vee u[t] = v}$$

Example

consider the formulas in CNF

$$c \neq d \qquad b = d$$

$$(a \neq d) \vee (a = c) \qquad (a = b) \vee (a = d)$$

$$\frac{b = d \quad (a = b) \vee (a = d)}{(a = d) \vee (a = d)}$$

not (refutationally) complete yet!

Definition

most general unifier

- a substitution σ is a mapping from variables to terms, denoted as
$$\{x_1 \mapsto t_1, \ldots, x_n \mapsto t_n\}$$
- a substitution σ is more general than τ, if $\exists\ \rho$ such that $\sigma\rho = \tau$
- a unifer σ of terms s and t is a substitution such that $s\sigma = t\sigma$
- a unifer σ (of s, t) is most general if σ is more general than any other unifier (of s, t)

Definition

clause

- $\square$ is a clause
- literals are clauses
- if C, D are clauses, then $C \vee D$ is a clause

we use the equivalences $C \vee \square \vee D \equiv C \vee D$, $\square \vee \square \equiv \square$

Paramodulation Calculus

Definition superposition (left, right)

$$\frac{C \vee s = t \quad D \vee \neg A[s']}{C\sigma \vee D\sigma \vee \neg A[t]\sigma} \qquad \frac{C \vee s = t \quad D \vee A[s']}{C\sigma \vee D\sigma \vee A[t]\sigma}$$

- σ is mgu of s and s'
- s' is not a variable

Example

$$\cfrac{g(x) = x \qquad \cfrac{f(a) = f(b) \quad \neg P(g(x)) \vee Q(f(x))}{\neg P(g(a)) \vee Q(f(b))}\ \sigma = \{x \mapsto a\}}{\neg P(a) \vee Q(f(b))}\ \sigma = \{x \mapsto a\}$$

Resolution

Definition factoring (ordered, equality)

$$\frac{C \vee A \vee B}{C\sigma \vee A\sigma} \qquad \frac{C \vee s = t \vee s' = t'}{C\sigma \vee t\sigma \neq t'\sigma \vee s'\sigma = t'\sigma}$$

- σ is mgu of A and B or mgu of s and s'

Definition resolution (equality, standard)

$$\frac{C \vee s \neq t}{C\sigma} \qquad \frac{C \vee P(s_1, \ldots, s_n) \quad D \vee \neg P(t_1, \ldots, t_n)}{C\sigma \vee D\sigma}$$

- σ is mgu of s and t or of $P(s_1, \ldots, s_n)$, $P(t_1, \ldots, t_n)$ respectively

Observation

factoring is only necessary for positive atoms

Example

$$\dfrac{\dfrac{\dfrac{a \neq d \vee a = c \qquad \dfrac{\dfrac{b = d \quad (a = b) \vee (a = d)}{(a = d) \vee (a = d)}\ \textit{s}'\textit{pos}}{a = d}\ \textit{fact}}{a = c}\ \textit{res} \qquad a = d}{c = d}\ \textit{s}'\textit{pos} \qquad c \neq d}{\Box}\ \textit{res}$$

Theorem

paramodulation is sound and complete

Definition (informal)

superposition calculus

- extend the above rules with an order $\succ$ on terms and literals
- apply operations only on maximal literals and
  apply superposition only to equations $s = t$ if $s \succ t$

Theorem

superposition is sound, complete, and can be efficiently implemented