Logic (master program)

Georg Moser

Institute of Computer Science @ UIBK

Winter 2008

Summary of Last Lecture

premise	conclusion	name
$\Gamma \vdash \varphi(t)$	$\Gamma \vdash \exists x \varphi(x)$	$\exists$-introduction
$\Gamma \vdash \varphi(c)$	$\Gamma \vdash \forall x \varphi(x)$	$\forall$-introduction
$\Gamma \vdash \varphi \to \psi$	$\Gamma \vdash \exists x \varphi(x) \to \exists x \psi(x)$	$\exists$-distribution
$\Gamma \vdash \varphi \to \psi$	$\Gamma \vdash \forall x \varphi(x) \to \forall x \psi(x)$	$\forall$-distribution
$\Gamma \vdash Q_1 x (Q_2 y \varphi)$	$\Gamma \vdash Q_1 x Q_2 y \varphi$	parentheses rule
	$\Gamma \vdash t = t$	reflexivity
$\Gamma \vdash \varphi(t), \Gamma \vdash t = t'$	$\Gamma \vdash \varphi(t')$	equality substitution

- t is a term
- c is constant $\notin \Gamma$
- $Q \in \{\forall, \exists\}$

extend by definition rules

Soundness Theorem

Definition (formal proof)

- a formal proof is a finite sequence of statements $\Gamma \vdash \varphi$
- each statement follows from previous ones, by the stated rules
- we say φ is derived from Γ if there is a formal proof of $\Gamma \vdash \varphi$

Theorem (soundness)

if $\Gamma \vdash \varphi$ then $\Gamma \models \varphi$

Theorem (closure theorem)

let $\varphi(x_1, \ldots, x_n)$ be a formula and let $\forall x_1 \ldots \forall x_n \varphi(x_1, \ldots, x_n)$ its universal closure, then $\Gamma \vdash \varphi(x_1, \ldots, x_n)$ if and only if $\Gamma \vdash \forall x_1 \ldots \forall x_n \varphi(x_1, \ldots, x_n)$, where Γ is a set of sentences

Theorem

let x, y be variables that do not occur in $\varphi(z)$

- $\forall x \varphi(x)$ and $\forall y \varphi(y)$ are provably equivalent
- $\exists x \varphi(x)$ and $\exists y \varphi(y)$ are provably equivalent

Definition (prenex normal form)

- a formula φ s in prenex normal form if it has the form

$$Q_1 x_1 \ldots Q_n x_n \psi \qquad Q_i \in \{\forall, \exists\}$$

  ψ is quantifier-free
- if ψ is a conjunction of disjunctions of literals, we say φ is in conjunctive (prenex) normal form

Theorem

any first-order formula is transformable into conjunctive normal form

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

Skolemisation

Definition

a sentence is in Skolem normal form (SNF for short), if it is universal and in CNF

Definition

given a sentence φ, we define its Skolemisation φ^S as follows

1. transform φ into a CNF φ' such that $\varphi' = Q_1 x_1 \cdots Q_m x_m \psi(x_1, \dots, x_m)$
2. repeatedly replace ϕ
$$\forall x_1 \cdots \forall x_{i-1} \exists x_i Q_{i+1} x_{i+1} \cdots Q_m x_m \ \chi(x_1, \dots, x_m)$$
by $s(\phi)$
$$\forall x_1 \cdots \forall x_{i-1} Q_{i+1} x_{i+1} \cdots Q_m x_m \ \chi(x_1, \dots, f(x_1, \dots, x_{i-1}), \dots, x_m)$$
where f denotes a fresh function symbol of arity $i - 1$

Theorem

let φ be a sentence and φ^S its Skolemisation, then φ is satisfiable if and only if φ^S is satisfiable

Proof

without loss of generality we assume φ is in CNF, we show φ is satisfiable only if $s(\varphi)$ is satisfiable

1. define
$$\varphi = \forall x_1 \cdots \forall x_{i-1} \exists x_i Q_{i+1} x_{i+1} \cdots Q_m x_m \ \chi$$
$$s(\varphi) = \forall x_1 \cdots \forall x_{i-1} Q_{i+1} x_{i+1} \cdots Q_m x_m \ \chi[f(x_1, \dots, x_{i-1})/x_i]$$
$$\psi(x_1, \dots, x_i) = Q_{i+1} x_{i+1} \cdots Q_m x_m \ \chi(x_1, \dots, x_m)$$
2. suppose $\forall x_1 \cdots \forall x_{i-1} \exists x_i \psi$ is satisfiable then there $\exists$ model $\mathcal{M}$, let $\mathcal{M}_f$ denote an expansion of $\mathcal{M}_C$ (by f) such that
$$\mathcal{M}_f \models \psi(c_1, \dots, c_{i-1}, f(c_1, \dots, c_{i-1}))$$
for all $c_1, \dots, c_{i-1} \in \mathcal{V}(\mathcal{M})$
3. hence $\forall x_1 \cdots \forall x_{i-1} \psi(x_1, \dots, f(x_1, \dots, x_{i-1}))$ is satisfiable ∎

Herbrand Theory

Definition

a Herbrand universe for $\mathcal{V}$ is the set of all closed $\mathcal{V}$-terms

Example

let $\mathcal{V} = \{c, f, R\}$, then the Herbrand universe H of $\mathcal{V}$ is defined as
$$H = \{c, f(c), f(f(c)), f(f(f(c))), \dots\}$$

Definition

a structure $\mathcal{M}$ is a Herbrand structure, if

1. its universe is the Herbrand universe U for $\mathcal{V}$
2. the interpretation function sets
$$c^{\mathcal{M}} = c \in U \qquad f^{\mathcal{M}}(t_1, \dots, t_n) = f(t_1, \dots, t_n)$$

constants and functions are interpreted as their names, i.e., as terms

Definition
the Herbrand vocabulary $\mathcal{V}_\Gamma$ for Γ is defined as follows:

- $\mathcal{V}_0$ denotes the symbols occurring in Γ
- if $\mathcal{V}_0$ contains a constant $\mathcal{V}_\Gamma = \mathcal{V}_0$, otherwise $\mathcal{V}_\Gamma = \mathcal{V}_0 \cup \{c\}$ for some constant c

Definition
- the Herbrand universe $H(\Gamma)$ for Γ is the Herbrand universe for $\mathcal{V}_\Gamma$
- $\mathcal{M}$ is a Herbrand model of Γ if $\mathcal{M}$ is a Herbrand structure that is also a model of Γ

Theorem
let Γ be set of equality-free sentences in SNF; then Γ is satisfiable if and only if Γ has a Herbrand model

Proof
suppose Γ is satisfiable, let $\mathcal{N}$ be a $\mathcal{V}_\Gamma$-structure that models each $\varphi \in \Gamma$

- we define a Herbrand structure $\mathcal{M}$
- the universe of $\mathcal{M}$ is the Herbrand universe $H(\Gamma)$
- $\forall\ R \in \mathcal{V}_\Gamma$

$$(t_1, \dots, t_n) \in R^{\mathcal{M}} \quad \text{if and only if} \quad \mathcal{N} \models R(t_1, \dots, t_n)$$

- $\forall$ quantifier- and equality-free sentences ψ

$$\mathcal{M} \models \psi \quad \text{if and only if} \quad \mathcal{N} \models \psi$$

  follows by induction on ψ
- $\forall$ equality-free SNF sentences ψ

$$\text{if} \quad \mathcal{N} \models \psi \quad \text{then} \quad \mathcal{M} \models \psi$$

  follows by induction on the number of (universal) quantifiers in ψ ■

Theorem
let φ be an SNF-sentence, then φ is satisfiable if and only if $\exists\ \varphi'$ such that φ' has a Herbrand model

Proof
$\exists\ \varphi_E$ such that φ_E is satisfiable if and only φ is satisfiable and φ_E doesn't contain equality signs

Definition — Herbrand Method
the following procedure certifies unsatisfiabilty of first-order formuals

- let φ be a formula in SNF

$$\forall x_1 \cdots \forall x_n \psi(x_1, \dots, x_n)$$

  where ψ is quantifer-free, define $E(\varphi)$ as the set

$$\{\psi(t_1, \dots, t_n) \mid t_1, \dots, t_n \in H(\varphi)\}$$

- φ is satisfiable if and only if $E(\varphi_E)$ is satisfiable
- use propositional resolution to verify unsatisfiablity of $E(\varphi_E)$

Content

Gödel's Completeness Theorem

every model has a theory and every theory has a model

recall

- a theory is a consistent set of formulas
- a set of formulas Γ is consistent if no contradiction follows from Γ
- the theory of $\mathcal{M}$ is the set $\mathrm{Th}(\mathcal{M}) = \{\varphi \text{ a sentence} \mid \mathcal{M} \models \varphi\}$

every model has a theory	every theory has a model
$\mathrm{Th}(\mathcal{M})$ is consistent	every consistent set of sentences is satisfiable

Proposition

if Γ is satisfiable then Γ is consistent

Proof

- if Γ is satisfiable, there exists $\mathcal{M}$, such that $\mathcal{M} \models \varphi \ \forall \ \varphi \in \Gamma$
- $\mathrm{Th}(\mathcal{M})$ is a complete theory, hence consistent by definition
- $\Gamma \subseteq \mathrm{Th}(\mathcal{M})$, hence 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 (naturally this enumeration includes the sentences in Γ)
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

$\forall \ m \geqslant 0 \ T_m$ is consistent

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 $f^{\mathcal{M}^+}(t_1, \dots, t_n) = s$, whenever $T^+ \vdash f(t_1, \dots, t_n) = s$
5. set $(t_1, \dots, t_n) \in R^{\mathcal{M}^+}$, if $T^+ \vdash R(t_1, \dots, t_n)$

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

Proof of Claim
by easy induction on φ ∎

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 $\Gamma \models \varphi$