Computational Logic

Georg Moser

Institute of Computer Science @ UIBK

Winter 2012

Summary Last Lecture

Definition (Satisfaction Relation)

$\mathcal{I} = (\mathcal{A}, \ell)$ an interpretation; F a formula, we define $\mathcal{I} \models F$

$\mathcal{I} \models t_1 = t_2$	$:\Longleftrightarrow$	if $t_1^{\mathcal{I}} = t_2^{\mathcal{I}}$
$\mathcal{I} \models P(t_1, \dots, t_n)$	$:\Longleftrightarrow$	if $(t_1^{\mathcal{I}}, \dots, t_n^{\mathcal{I}}) \in P^{\mathcal{A}}$
$\mathcal{I} \models \neg F$	$:\Longleftrightarrow$	if $\mathcal{I} \not\models F$
$\mathcal{I} \models F \wedge G$	$:\Longleftrightarrow$	if $\mathcal{I} \models F$ and $\mathcal{I} \models G$
$\mathcal{I} \models F \vee G$	$:\Longleftrightarrow$	if $\mathcal{I} \models F$ or $\mathcal{I} \models G$
$\mathcal{I} \models F \rightarrow G$	$:\Longleftrightarrow$	if $\mathcal{I} \models F$, then $\mathcal{I} \models G$
$\mathcal{I} \models \forall x F$	$:\Longleftrightarrow$	if $\mathcal{I}\{x \mapsto a\} \models F$ holds for all $a \in A$
$\mathcal{I} \models \exists x F$	$:\Longleftrightarrow$	if $\mathcal{I}\{x \mapsto a\} \models F$ holds for some $a \in A$

Undecidability of First-Order Logic

Theorem

1. *the decision problem for the consequence relation is undecidable*
2. *the set of valid first-order formulas is not recursive*

Theorem

the set of valid first-order formulas (over a countable language) is recursive enumerable

Lessons Learnt

- first-order logic (FOL) extends PL
- becomes undecidable, but still semi-decidable

Outline of the Lecture

Propositional Logic

short reminder of propositional logic, soundness and completeness theorem, natural deduction, propositional resolution

First Order Logic

introduction, syntax, semantics, undecidability of first-order, Löwenheim-Skolem, compactness, model existence theorem, natural deduction, completeness

Extensions and Restrictions of First Order

intuitionistic logic, modal logic, second-order logic

Automated Reasoning

normal forms, Herbrand's Theorem, history of theorem proving, automated reasoning (with equality)

Definition

$\mathcal{A}$, $\mathcal{B}$ two structures over the same language; assume $\exists$ bijection $m\colon A \to B$ such that

1. $\forall$ individual constant c: $m(c^{\mathcal{A}}) = c^{\mathcal{B}}$
2. $\forall$ function constant f, $\forall\ a_1, \dots, a_n \in A$:
$$m(f^{\mathcal{A}}(a_1, \dots, a_n)) = f^{\mathcal{B}}(m(a_1), \dots, m(a_n)) \quad \text{and}$$
3. $\forall$ predicate constant P, $\forall\ a_1, \dots, a_n \in A$:
$$P^{\mathcal{A}}(a_1, \dots, a_n) \iff P^{\mathcal{B}}(m(a_1), \dots, m(a_n))$$

then m is called an isomorphism between $\mathcal{A}$ and $\mathcal{B}$ denoted $m\colon \mathcal{A} \cong \mathcal{B}$

Lemma

let A, B be sets; $m\colon A \to B$ be a bijection; if $\mathcal{A}$ is a structure with domain A, then $\exists$ structure $\mathcal{B}$ with $\mathcal{A} \cong \mathcal{B}$

Isomorphism Theorem

let $\mathcal{A}$, $\mathcal{B}$ be structures such that $m\colon \mathcal{A} \cong \mathcal{B}$, then for all sentences F: $\mathcal{A} \models F$ iff $\mathcal{B} \models F$

Proof.

1. let $\mathcal{I} = (\mathcal{A}, \ell)$, define $\ell^m = m \circ \ell$, set $\mathcal{J} = (\mathcal{B}, \ell^m)$
2. $\forall$ terms t: $m(t^{\mathcal{I}}) = t^{\mathcal{J}}$ (follows by induction on t)
3. $\forall$ formulas F: $\mathcal{I} \models F \iff \mathcal{J} \models F$
   - base case $F = (s = t)$
$$\mathcal{I} \models s = t \iff s^{\mathcal{I}} = t^{\mathcal{I}} \iff m(s^{\mathcal{I}}) = m(t^{\mathcal{I}}) \iff \mathcal{J} \models s = t$$
   - step case $F = \exists x G$
$$\begin{aligned} \mathcal{I} \models \exists x G \quad &\iff \quad \text{there exists } a \in A,\ \mathcal{I}\{x \mapsto a\} \models G \\ &\iff \quad \text{there exists } a \in A,\ \mathcal{J}\{x \mapsto m(a)\} \models G \\ &\iff \quad \text{there exists } b \in B,\ \mathcal{J}\{x \mapsto b\} \models G \\ &\iff \quad \mathcal{J} \models \exists x G \end{aligned}$$

∎

Corollary

1. *$\forall$ formula F that has a finite model has a model in the domain $\{0, 1, 2, \dots, n\}$*
2. *$\forall$ formula F that has a countable infinite model has a model whose domain is $\mathbb{N}$*

Proof.

combination of both lemmas ∎

Example

consider $\mathcal{L} = \{\leftrightharpoons\}$ and

$$\begin{aligned} E &:\iff \forall x\ x \leftrightharpoons x \land \forall x \forall y\ (x \leftrightharpoons y \land y \leftrightharpoons x) \land \\ &\qquad \forall x \forall y \forall z\ ((x \leftrightharpoons y \land y \leftrightharpoons z) \to x \leftrightharpoons z) \\ F &:\iff \forall x \forall y\ x \leftrightharpoons y \end{aligned}$$

if $\mathcal{M} \models E \land F$, $\mathcal{N} \models E \land F$, then $\mathcal{M} \cong \mathcal{N}$

Compactness and Löwenheim-Skolem

Theorem (Compactness Theorem)

if every finite subset of a set of formulas $\mathcal{G}$ has a model, then $\mathcal{G}$ has a model

Theorem (Löwenheim-Skolem Theorem)

if a set of formulas $\mathcal{G}$ has a model, then $\mathcal{G}$ has a countable model

Corollary

if a set of formulas $\mathcal{G}$ has arbitrarily large finite models, then it has a countable infinite model

Proof Idea.

employ compactness to show that $\mathcal{G}$ has an infinite model and Löwenheim-Skolem to show that this model is countable ∎

Corollary

1. *any satisfiable set of formulas $\mathcal{G}$ has a model whose domain is either the set of natural numbers $< n$ or $\mathbb{N}$*
2. *if $\mathcal{G}$ is a satisfiable set of formulas, no function symbols, no identity in language, then $\mathcal{G}$ has a model whose domain is $\mathbb{N}$*

Proof (of second item).

1. suppose $\mathcal{G}$ has a model $\mathcal{I}$ with domain $\{0, \dots, n-1\}$
2. define $f \colon \mathbb{N} \to \{0, 1, \dots, n-1\}$ as:
$$f(m) = \min\{m, n-1\}$$
3. define $\mathcal{J}$ with domain $\mathbb{N}$ and look-up table ℓ
   - $c^{\mathcal{J}} = f(c)^{\mathcal{I}}$
   - $\forall$ predicate constants P, $\forall\ n_1, \dots, n_k$
     $(n_1, \dots, n_k) \in P^{\mathcal{J}}$ iff $(f(n_1), \dots, f(n_k)) \in P^{\mathcal{I}}$
4. f is a surjective homomorphism, the isomorphism lemma holds

∎

Proof Plan for Completeness

first-order logic features the following three theorems

1. (soundness and) completeness
2. compactness
3. Löwenheim-Skolem

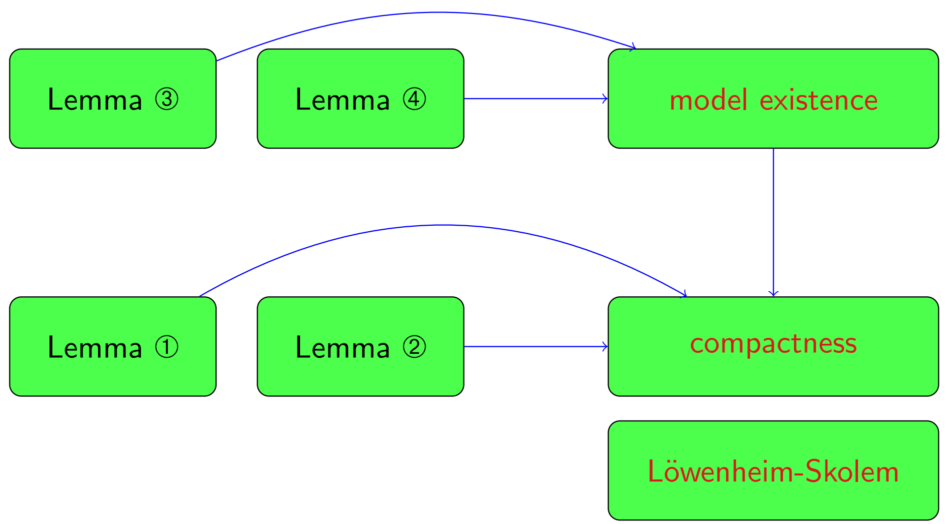
Observations

$\perp$ is not derivable

- any proof of completeness is indirect:
  suppose $\exists$ a consistent set $\mathcal{G}$, then $\mathcal{G}$ is satisfiable
- to show $\mathcal{G}$ is satisfiable one constructs a countable model $\mathcal{M}$
- then Löwenheim-Skolem and compactness follow
- the central piece of work is the construction of $\mathcal{M}$; this is independent on the proof system

in proof, we restrict to the logical symbols to $\neg$, $\vee$, $\exists$

Howto Prove Compactness and Löwenheim-Skolem



Satisfaction Properties

Lemma ①

let S be the set of satisfiable formula sets $\mathcal{G}$; pick $\mathcal{G} \in S$

1. *if $\mathcal{G}_0 \subseteq \mathcal{G}$, then $\mathcal{G}_0 \in S$*
2. *no formula F and $\neg F$ in $\mathcal{G}$*
3. *if $\neg\neg F \in \mathcal{G}$, then $\mathcal{G} \cup \{F\} \in S$*
4. *if $(E \vee F) \in \mathcal{G}$, then either $\mathcal{G} \cup \{E\} \in S$ or $\mathcal{G} \cup \{F\} \in S$*
5. *if $\neg(E \vee F) \in \mathcal{G}$, then $\mathcal{G} \cup \{\neg E\} \in S$ and $\mathcal{G} \cup \{\neg F\} \in S$*
6. *if $\exists x F(x) \in \mathcal{G}$, the constant c doesn't occur in $\mathcal{G}$, then $\mathcal{G} \cup \{F(c)\} \in S$*
7. *if $\neg\exists x F(x) \in \mathcal{G}$, then $\forall$ terms t, $\mathcal{G} \cup \{\neg F(t)\} \in S$*

Definition

we call the properties (of S) in the lemma satisfaction properties

Lemma ②

1. *assume S is a set of formula sets and S has the satisfaction properties*
2. *let S^* be the set of all formula sets $\mathcal{G}$ such that $\forall$ finite $\mathcal{G}_0 \subseteq \mathcal{G}$, $\mathcal{G}_0 \in S$*
3. *then S^* has the satisfaction properties*

Proof.

we treat the case of disjunction

- assume $\mathcal{G} \in S^*$, $(E \vee F) \in \mathcal{G}$, $\mathcal{G} \cup \{E\} \notin S^*$ and $\mathcal{G} \cup \{F\} \notin S^*$
- $\forall$ finite $\mathcal{G}_0 \subseteq \mathcal{G}$, $\mathcal{G}_0 \in S$,
- $\exists$ finite $\mathcal{G}_1 \subseteq \mathcal{G} \cup \{E\}$, $\mathcal{G}_1 \notin S$, $\exists$ finite $\mathcal{G}_2 \subseteq \mathcal{G} \cup \{F\}$, $\mathcal{G}_2 \notin S$
- wlog $\mathcal{G}_1 = \mathcal{G}_1' \cup \{E\}$, $\mathcal{G}_2 = \mathcal{G}_2' \cup \{F\}$, and $\mathcal{G}_1', \mathcal{G}_2' \subseteq \mathcal{G}$ finite
- $\mathcal{G}_1' \cup \mathcal{G}_2' \cup \{(E \vee F)\} \subseteq \mathcal{G}$, hence $\mathcal{G}_1' \cup \mathcal{G}_2' \cup \{(E \vee F)\} \in S$
- hence $\mathcal{G}_1' \cup \mathcal{G}_2' \cup \{E\} \in S$ or $\mathcal{G}_1' \cup \mathcal{G}_2' \cup \{F\} \in S$
- contradiction ■

$\mathcal{L}$ base language; $\mathcal{L}^+ \supseteq \mathcal{L}$ infinitely many new individual constants

Theorem (Model Existence Theorem)

1. *if S^* is a set of formula sets of $\mathcal{L}^+$ having the satisfaction properties, then $\forall$ formula sets $\mathcal{G} \in S^*$ of $\mathcal{L}$, $\exists$ $\mathcal{M}$, $\mathcal{M} \models \mathcal{G}$*
2. *$\forall$ elements m of $\mathcal{M}$: m denotes term in $\mathcal{L}^+$*

Compactness Theorem

if every finite subset of a set of formulas $\mathcal{G}$ has a model, then $\mathcal{G}$ has a model

Remark

the statement and the proof of the compactness theorem do not refer to provability; compactness is extensible to non-enumerable language

we only consider the simplified case where $\mathcal{L}$ does not contain function constants nor $=$

Proof (of compactness).

- consider the set S of satisfiable formula sets (over $\mathcal{L}$) (as in Lemma ①)
- consider the set S^* of all formulas set $\mathcal{G}$, $\forall$ $\mathcal{G}_0 \subseteq \mathcal{G}$, $\mathcal{G}_0$ finite, $\mathcal{G}_0 \in S$ (as in Lemma ②)
- Lemma ① yields that S admits the satisfaction properties
- Lemma ② yields that S^* admits the satisfaction properties
- by assumption $\mathcal{G}$ is in S^*
- by model existence $\mathcal{G}$ has a model $\mathcal{M}$ ■

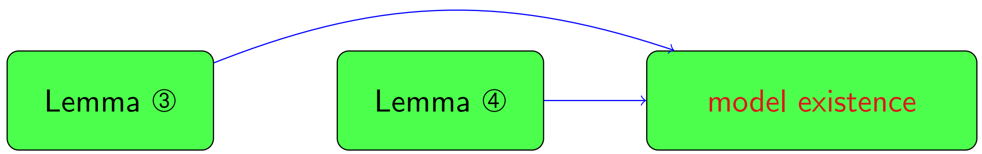
Theorem (Löwenheim-Skolem Theorem)

if a set of formulas $\mathcal{G}$ has a model, then $\mathcal{G}$ has a countable model

Proof.

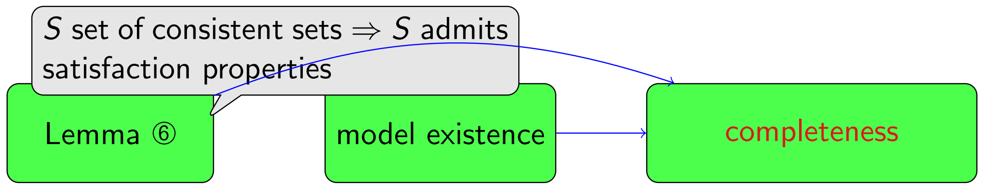
the model $\mathcal{M}$ constructed is countable ■

Howto (eventually) Prove Completeness



Definition

for any formal system; if $\neg\,\exists$ proof of $\perp$ from a formula set $\mathcal{G}$, we say $\mathcal{G}$ is consistent



Later We Exploit the Proof