Logic (master program)

Georg Moser

Institute of Computer Science @ UIBK

Winter 2008

Summary of Last Lecture

premise	conclusion	name
$G \in \mathcal{F}$	$\mathcal{F} \vdash G$	assumption
$\mathcal{F} \vdash G \wedge \mathcal{F} \subset \mathcal{F}'$	$\mathcal{F}' \vdash G$	monotonicity
$\mathcal{F} \vdash G$	$\mathcal{F} \vdash \neg\neg G$	double negation
$\mathcal{F} \vdash F, \mathcal{F} \vdash G$	$\mathcal{F} \vdash (F \wedge G)$	$\wedge$-introduction
$\mathcal{F} \vdash (F \wedge G)$	$\mathcal{F} \vdash F$	$\wedge$-elimination
$\mathcal{F} \vdash (F \wedge G)$	$\mathcal{F} \vdash (G \wedge F)$	$\wedge$-symmetry
$\mathcal{F} \vdash F$	$\mathcal{F} \vdash F \vee G$	$\vee$-introduction
$\mathcal{F} \vdash (F \vee G), \mathcal{F} \cup \{F\} \vdash H, \mathcal{F} \cup \{G\} \vdash H$	$\mathcal{F} \vdash H$	$\vee$-elimination
$\mathcal{F} \vdash (F \vee G)$	$\mathcal{F} \vdash (G \vee F)$	$\vee$-symmetry
$\mathcal{F} \cup \{F\} \vdash G$	$\mathcal{F} \vdash (F \rightarrow G)$	$\rightarrow$-introduction
$\mathcal{F} \vdash (F \rightarrow G), \mathcal{F} \vdash F$	$\mathcal{F} \vdash G$	$\rightarrow$-elimination

More Rules

premise	conclusion	name
$\mathcal{F} \vdash F$	$\mathcal{F} \vdash (F)$	()-introduction
$\mathcal{F} \vdash (F)$	$\mathcal{F} \vdash F$	()-elimination
$\mathcal{F} \vdash ((F \wedge G) \wedge H)$	$\mathcal{F} \vdash (F \wedge G \wedge H)$	$\wedge$-parentheses
$\mathcal{F} \vdash ((F \vee G) \vee H)$	$\mathcal{F} \vdash (F \vee G \vee H)$	$\vee$-parentheses
$\mathcal{F} \vdash (F \vee G)$	$\mathcal{F} \vdash \neg(\neg F \wedge \neg G)$	$\vee$-definition
$\mathcal{F} \vdash \neg(\neg F \wedge \neg G)$	$\mathcal{F} \vdash (F \vee G)$	
$\mathcal{F} \vdash (F \rightarrow G)$	$\mathcal{F} \vdash (\neg F \vee G)$	$\rightarrow$-definition
$\mathcal{F} \vdash (\neg F \vee G)$	$\mathcal{F} \vdash (F \rightarrow G)$	
$\mathcal{F} \vdash (F \leftrightarrow G)$	$\mathcal{F} \vdash (F \rightarrow G) \wedge (G \rightarrow F)$	$\leftrightarrow$-definition
$\mathcal{F} \vdash (F \rightarrow G) \wedge (G \rightarrow F)$	$\mathcal{F} \vdash (F \leftrightarrow G)$	

Resolution

Definition (clause)

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

Convention

we assert equivalence under commutativity and associativity and $\neg\neg A \equiv A$ for literals

Definition ((propositional) resolution)

$$\frac{C \vee A \quad D \vee \neg A}{C \vee D}$$

Definition ((propositional) factoring)

$$\frac{C \vee A \vee A}{C \vee A}$$

Soundness, Completeness and Compactness

Theorem — soundness

if a formula G is derivable from a set of formulas $\mathcal{F}$, then G is a consequence of $\mathcal{F}$

Theorem — compactness

a set of formulas of propositional logic is satisfiable iff every finite subset is satisfiable

Theorem — completeness

if a formula G is a consequence of a set of formulas $\mathcal{F}$, then G is derivable from $\mathcal{F}$

- Exercise 1.1.
- Exercise 1.2.
- Exercise 1.21.
- Exercise 1.34.
- Exercise 1.35.

Content

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

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

introduction to computability, introduction to complexity, finite model theory

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

Language of First-Order Logic

fixed part	connectives	as for propositional logic
	quantifiers	$\forall$ reads "for all"
		$\exists$ reads "there exists"
	brackets	), (
	variables	$x, y, z, \ldots$
variable part	relation symbols	$=, P, Q, R, S, \ldots$
	function symbols	$f, g, h, \ldots$
	constant symbols	$a, b, c, \ldots$

Example

$$\exists x_1 \exists x_2 \exists x_3 (\neg(x_1 = x_2) \wedge \neg(x_1 = x_3) \wedge \neg(x_2 = x_3))$$

Definition — terms

terms are defined inductively as follows

- every variable and constant is a term
- if f is an n-ary function symbol, and $t_1, \dots, t_n$ are terms, then $f(t_1, \dots, t_n)$ is a term

Definition — atomic formula

an atomic formula is an expression of form $t_1 = t_2$ or $R(t_1, \dots, t_n)$, where R is an n-ary relation symbol and $t_1, \dots, t_n$ are terms

Definition — formulas

a formula is an expression that is either an atomic formula or generated through the following rules

- if φ is a formula, so is $\neg\varphi$
- if φ and ψ are formulas, so is $\varphi \wedge \psi$
- if φ is a formula, then so is $\exists x \varphi$

Definition — defined symbols

- the symbols $\vee$, $\rightarrow$, $\leftrightarrow$ are defined as in propositional logic
- we define $\forall x \varphi$ as $\neg\exists x \neg\varphi$

Priorities

$$\neg, \exists, \forall \quad > \quad \wedge, \vee, \rightarrow, \leftrightarrow$$

Definition — subformula

- any formula φ is a subformula of itself
- any subformula of φ is a subformula of $\neg\varphi$
- any subformula of φ and ψ is a subformula of $\varphi \wedge \psi$
- any subformula of φ is a subformula of $\exists x \varphi$

Definition — free(φ)

we define the set free(φ) of free variables inductively

- if φ is atomic, $\text{free}(\varphi) = \{x \mid \text{variable } x \text{ occurs in } \varphi\}$
- if $\varphi = \neg\psi$, then $\text{free}(\varphi) = \text{free}(\psi)$
- if $\varphi = \psi \wedge \theta$, then $\text{free}(\varphi) = \text{free}(\psi) \cup \text{free}(\theta)$
- if $\varphi = \exists x \psi$, then $\text{free}(\varphi) = \text{free}(\psi) \setminus \{x\}$

Definition — bnd(φ)

we define the set bnd(φ) of bound variables inductively

- if φ is atomic, $\text{bnd}(\varphi) = \varnothing$
- if $\varphi = \neg\psi$, then $\text{bnd}(\varphi) = \text{bnd}(\psi)$
- if $\varphi = \psi \wedge \theta$, then $\text{bnd}(\varphi) = \text{bnd}(\psi) \cup \text{bnd}(\theta)$
- if $\varphi = \exists x \psi$, then $\text{bnd}(\varphi) = \text{bnd}(\psi) \cup \{x\}$

Example

consider $\exists x(R(x, y) \wedge \exists y R(y, x))$

Semantics of First-Order Logic

Definition — vocabulary

a vocabulary is a set of function, relation and constant symbols

Definition — structure

a structure $\mathcal{M}$ is a pair (U, I), where U is called the universe of the structure and I denotes an interpretation of the vocabulary $\mathcal{V}$ such that

- $c^{\mathcal{M}} \in U$ for each constant in $\mathcal{V}$
- $f^{\mathcal{M}} \colon U^n \rightarrow U$ for each function symbol in $\mathcal{V}$
- $R^{\mathcal{M}} \subseteq U^n$ for each predicate symbol in $\mathcal{V}$

to emphasise the vocabulary, we sometimes speak of a $\mathcal{V}$-structure

Example

let $\mathcal{V} = \{c, f, R\}$, c constant, f is unary, R is binary

$$\underbrace{\mathcal{M} = (\mathbb{Z}, c^{\mathcal{M}}, f^{\mathcal{M}}, R^{\mathcal{M}})}_{\{c,f,R\}\text{-structure}}$$

- $c^{\mathcal{M}} = 3$
- $f^{\mathcal{M}}(x) = x^2$
- $(x, y) \in R^{\mathcal{M}} \iff x < y$

Convention

we write $\mathcal{M} = (\mathbb{Z}, c, f, R)$ for the above structure, if no confusion can arise

Example

- $\mathcal{V} = \{+, \cdot, 0, 1\}$
- $\mathbf{R} = (\mathbb{R}, +, \cdot, 0, 1)$ denotes the "usual" structure of the reals, where the constants and functions admit their standard interpretation

Definition

- a $\mathcal{V}$-formula contains only the function, relation, constants in $\mathcal{V}$
- a $\mathcal{V}$-sentence is a $\mathcal{V}$-formula that doesn't contain free variables

Definition $\mathcal{M} \models \varphi$

we define $\mathcal{M} \models \varphi$ for sentences φ by structural induction

$\mathcal{M} \models t_1 = t_2$	if t_1, t_2 are interpreted as the same element in universe U of $\mathcal{M}$
$\mathcal{M} \models P(t_1, \dots, t_n)$	if $(t_1^{\mathcal{M}}, \dots, t_n^{\mathcal{M}}) \in P^{\mathcal{M}}$
$\mathcal{M} \models \neg\varphi$	if $\mathcal{M} \not\models \varphi$
$\mathcal{M} \models \varphi \wedge \psi$	if $\mathcal{M} \models \varphi \wedge \mathcal{M} \models \psi$
$\mathcal{M} \models \exists x \varphi$	if $\mathcal{M} \models \varphi(x)$ for some x

this is not well-defined!

Definition expansion

let $\mathcal{V}$ be a vocabulary, $\mathcal{M}$ a $\mathcal{V}$-structure

- an expansion $\mathcal{V}'$ of $\mathcal{V}$ is any vocabulary that is superset of $\mathcal{V}$
- an expansion $\mathcal{M}'$ of $\mathcal{M}$ if $\mathcal{M}'$
  1. has the same universe as $\mathcal{M}$
  2. interprets the elements of $\mathcal{V}$ as in $\mathcal{M}$
- if $\mathcal{M}'$ is an expansion of $\mathcal{M}$, then $\mathcal{M}$ is a reduct of $\mathcal{M}'$

Lemma

let $\mathcal{M}$ be $\mathcal{V}$-structure and $\mathcal{M}'$ an $\mathcal{V}'$-structure; suppose $\mathcal{M}'$ is an expansion of $\mathcal{M}$; then $\mathcal{V}'$ is an expansion of $\mathcal{V}$

Example

consider

$$\mathcal{M}' = (\mathbb{R}, +, -, \cdot, <, 0, 1) \qquad \mathcal{M} = (\mathbb{R}, +, \cdot, 0, 1)$$

$\mathcal{M}'$ is an expansion of $\mathcal{M}$

Definition

let $\mathcal{M}$ be a $\mathcal{V}$-structure with universe U

- $\mathcal{V}(\mathcal{M}) = \mathcal{V} \cup \{c_m \mid m \in U\}$
- $\mathcal{M}_C$ denotes the expansion to a $\mathcal{V}(\mathcal{M})$-structure that interprets constants c_m as the element m

Definition $\mathcal{M} \models \varphi$ cont'd

$$\mathcal{M} \models \exists x \varphi \qquad \text{if } \mathcal{M}_C \models \varphi(c) \text{ for some } c \in \mathcal{V}(\mathcal{M})$$

Observation

$\mathcal{M} \models \varphi$ extends in the natural way to sentences containing defined symbols

Example

$$\mathcal{M} \models \forall x \varphi \qquad \text{if } \mathcal{M}_C \models \varphi(c) \text{ for all } c \in \mathcal{V}(\mathcal{M})$$