Logic (master program)

Georg Moser

Institute of Computer Science @ UIBK

Winter 2008

Summary of Last Lecture

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

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 $\mathcal{V}$:

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

Semantics of First-Order Logic

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 all constants c_m as the element m

Definition

$\mathcal{M} \models \varphi$

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

$$\begin{aligned} \mathcal{M} &\models \exists x \varphi && \text{if } \mathcal{M}_C \models \varphi(c) \text{ for some } c \in \mathcal{V}(\mathcal{M}) \\ \mathcal{M} &\models \forall x \varphi && \text{if } \mathcal{M}_C \models \varphi(c) \text{ for all } c \in \mathcal{V}(\mathcal{M}) \end{aligned}$$

Definition

let $\mathcal{M}$ be a $\mathcal{V}$-structure, let φ be a $\mathcal{V}(\mathcal{M})$-sentence

$$\mathcal{M} \models \varphi \qquad \text{if } \mathcal{M}_C \models \varphi$$

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

Definition

let φ be a $\mathcal{V}$-sentence

φ holds in $\mathcal{M}$	if $\mathcal{M} \models \varphi$
φ is valid	if $\forall$ $\mathcal{V}$-structures $\mathcal{M} \models \varphi$
φ is satisfiable	if $\exists$ $\mathcal{V}$-structure $\mathcal{M} \models \varphi$
φ is unsatisfiable	if $\neg\, \exists$ $\mathcal{V}$-structure $\mathcal{M} \models \varphi$

Definition

$\models \varphi$	φ is a valid (or a tautology)
$\varphi \models \psi$	ψ is a consequence of φ
$\varphi \equiv \psi$	φ and ψ are equivalent

Definition

a formula $\varphi(x_1, \ldots, x_n)$ is valid if $\forall x_1 \cdots \forall x_n \varphi(x_1, \ldots, x_n)$ is valid

Motivation

Model theory is a technique, that given
a model of a system and a formal property
checks whether this property holds
for that model

Structures of First-Order Logic

Definition

definable

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

- $\varphi(\mathcal{M}) = \{(a_1, \dots, a_n) \in U^n \mid \mathcal{M} \models \varphi(a_1, \dots, a_n)\}$
- $\varphi(\mathcal{M})$ is called $\mathcal{V}$-definable subset of $\mathcal{M}$

Example

let $\mathcal{V}_< = \{<\}$, let $\mathbf{R}_< = (\mathbb{R}, <)$, consider the $\mathcal{V}_<(\mathbf{R}_<)$-formulas

$$\varphi(x, y) = (x < y) \vee (x > y) \vee (x = y)$$

$$\psi(x) = (\neg(x < 3) \wedge \neg(x = 3) \wedge \neg(5 < x)) \vee (x = 5) \vee (x < -2)$$

- $\mathbf{R}_< \models \varphi(a, b)$ for all $(a, b) \in \mathbb{R}^2$
  hence the set defined by $\varphi(x, y)$ is all of $\mathbb{R}^2$
- the set defined by $\psi(x)$ is $a \in (-\infty, -2) \cup (3, 5]$

Definition

- a (undirected) graph is a set of points, called nodes (or vertices) and edges that connect nodes
- two vertices are adjacent if connected by an edge

Example

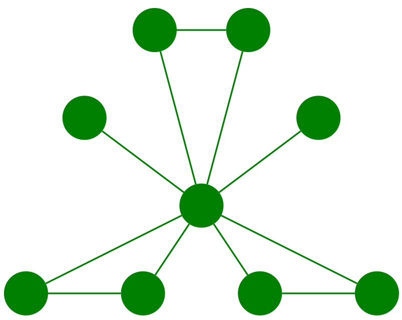
- each graph G forms a structure (U, R), where U denotes the nodes and R is interpreted as the edge relation
- hence any graph models the following sentences

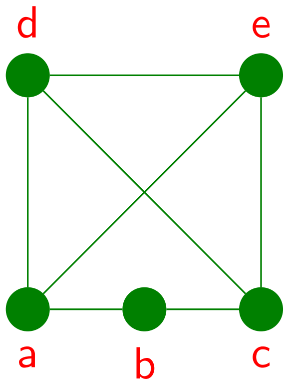
$$\forall x \neg R(x, x) \qquad \forall x \forall y (R(x, y) \leftrightarrow R(y, x))$$

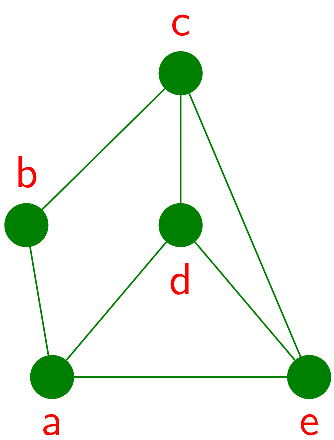
Definition

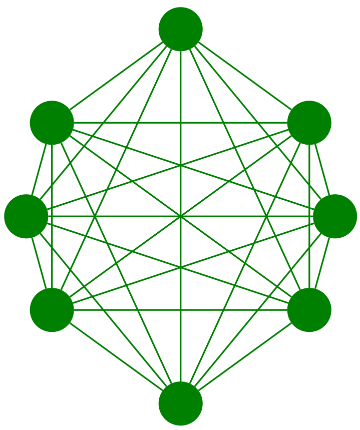
- a path from a to b (in a graph G) is a sequence of vertices beginning with a and ending in b such that each vertex other than a is adjacent to the previous vertex
- G is connected if for any two vertices a and b in G, exists a path from a to b

Examples of Graphs

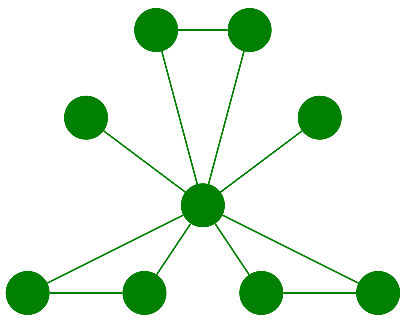


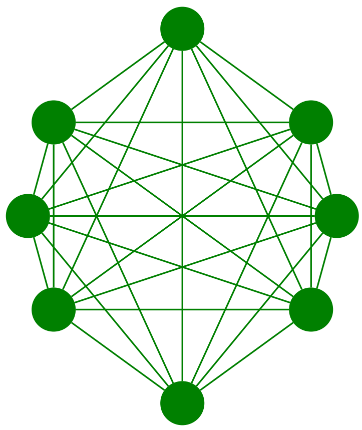






Separation Structures





$\varphi(x) \leftrightarrow \forall y(\neg(x = y) \to R(x, y))$ $\quad \forall x \forall y(\neg(x = y) \to R(x, y))$

$\exists y(\varphi(y) \land \forall z(\varphi(z) \to (z = y)))$

Definition

- any graph that models

$$\forall x \forall y(\neg(x = y) \to R(x, y))$$

  is a clique
- a clique with n nodes is called n-clique, denoted as K_n

Example

the fourth graph is the 8-clique K_8

Definition

graphs G_1 and G_2 are isomorphic if there exists a bijective function $f \colon G_1 \to G_2$ such that

$$a \; R \; b \quad \text{if and only if} \quad f(a) \; R \; f(b)$$

Example

- any two n-cliques are isomorphic
- graphs 2 and 3 are isomorphic

The Size of a Structure

Definition

- for any set U, the cardinality $|U|$ of U, denotes the number of elements in U
- for a structure $\mathcal{M}$, $|\mathcal{M}|$ denotes the cardinality of the universe of $\mathcal{M}$

Definition

let A, B be (possible infinite) sets, we set $|A| \leqslant |B|$ if $\exists\ f \colon A \to B$, such that f is injective

Definition

- we say A and B have the same size (denoted $|A| = |B|$) if $|A| \leqslant |B|$ and $|B| \leqslant |A|$
- we write $|A| < |B|$ if $|A| \leqslant |B|$ but not $|A| = |B|$

Example

let $I = (0, 1)$ denote the interval of reals between 0 and 1, the function $f \colon \mathbb{R} \to I$ defined as

$$f(x) = \frac{2}{\pi} \arctan x$$

is a bijection from $\mathbb{R}$ to I, hence $|\mathbb{R}| = |I|$

Theorem (Bernstein's Theorem)

sets A and B have the same size if and only if there exists a bijection between A and B

Proof Sketch

- suppose there exists a bijection $f \colon A \to B$
  then $|A| \leqslant |B|$ by definition as f is injective
  on the other hand $f^{-1} \colon B \to A$ exists and is injective, hence $|B| \leqslant |A|$
- for the reverse direction, $\exists$ injective $f \colon A \to B$ and $g \colon B \to A$
  build a bijection $h \colon A \to B$ ∎

Countable and Uncountable Sets

Definition

a set A

- is denumerable if $\exists$ bijection $f\colon A \to \mathbb{N}$
- is countable if A is finite or denumerable, otherwise it is uncountable

Example

the set of natural number, integers, and rational number $\mathbb{Q}$ is countable, the set of real number is uncountable

Theorem

the union of countable sets is countable

Theorem

if the vocabulary $\mathcal{V}$ is countable, so is the set of all $\mathcal{V}$-formulas

Theorem

for any set A, $|A| < |\mathcal{P}(A)|$

Proof

- define $f\colon A \to \mathcal{P}(A)$ as follows $f(a) = \{a\}$; hence $|A| \leqslant |\mathcal{P}(A)|$
- we show $|A| \neq |\mathcal{P}(A)|$
  1. suppose $g\colon A \to \mathcal{P}(A)$, such that g is injective, and g is surjective
  2. for each $a \in A$, either $a \in g(a)$ or $a \notin g(a)$
  3. set $X = \{a \mid a \notin g(a)\}$
  4. there exists no a such that $g(a) = X$
  5. contradiction ∎

Theorem

the set of all functions from $\mathbb{N}$ to $\mathbb{N}$ is uncountable

Proof Sketch

let F denote the set of all functions from $\mathbb{N}$ to $\mathbb{N}$, it suffices to show $|I| \leqslant |F|$ which is not too difficult ∎