

Lecture 12

Pete Manolios
Northeastern

First Order Logic

- ▶ Example: Group Theory

- ▶ (G1) For all x, y, z : $(x \cdot y) \cdot z = x \cdot (y \cdot z)$

- ▶ (G2) For all x : $x \cdot e = x$

- ▶ (G3) For all x there is a y such that: $x \cdot y = e$

- ▶ Theorem: For every x , there is a y such that $y \cdot x = e$

- ▶ Examples of groups: Nat, +, 0?; Int, +, 0?, Real, *, 1?

- ▶ Proof:

By (G3) there is: a y s.t. $x \cdot y = e$ and a z s.t. $y \cdot z = e$

Now: $y \cdot x = y \cdot x \cdot e = y \cdot x \cdot y \cdot z = y \cdot e \cdot z = y \cdot z = e$

- ▶ Is this true for all groups? Why?

- ▶ How many groups are there?

- ▶ Are there true statements about groups with no proof?

First Order Logic

- ▶ First Order Logic forms the foundation of mathematics
- ▶ We study various objects, e.g., groups
- ▶ Properties of objects captured by “non-logical” axioms
 - ▶ (G1-G3 in our example)
- ▶ Theory consists of all consequences of “non-logical” axioms
 - ▶ Derivable via logical reasoning alone
 - ▶ That’s it; no appeals to intuition
- ▶ Separation into non-logical axioms logical reasoning is astonishing: all theories use exactly same reasoning
- ▶ But, what is a proof ($\Phi \vdash \phi$)?
- ▶ Question leads to computer science
- ▶ Proof should be so clear, even a machine can check it

First Order Logic: Syntax

- ▶ Every FOL (first order language) includes
 - ▶ Variables v_0, v_1, v_2, \dots
 - ▶ Boolean connectives: \vee, \neg
 - ▶ Equality: $=$
 - ▶ Parenthesis: $(,)$
 - ▶ Quantifiers: \exists
- ▶ The symbol set of a FOL contains (possibly empty) sets of
 - ▶ relation symbols, each with an arity > 0
 - ▶ function symbols, each with an arity > 0
 - ▶ constant symbols
- ▶ Example: groups 2-ary function symbol \cdot and constant e
- ▶ Set theory: \in , a 2-ary relation symbol, ...

First Order Logic: Terms

- ▶ Terms denote objects of study, e.g., group elements
- ▶ The set of S -terms is the least set closed under:
 - ▶ Every variable is a term
 - ▶ Every constant is a term
 - ▶ If t_1, \dots, t_n are terms and f is an n -ary function symbol, then $f(t_1, \dots, t_n)$ is a term

First Order Logic: Formulas

- ▶ Formulas: statements about the objects of study
- ▶ An atomic formula of S is
 - ▶ $t_1 = t_2$ or
 - ▶ $R(t_1, \dots, t_n)$, where t_i is an S -term and R is an n -ary relation symbol in S
- ▶ The set of S -formulas is the least set closed under:
 - ▶ Every atomic formula is a formula
 - ▶ If ϕ, ψ are S -formulas and x is a variable, then $\neg\phi$, $(\phi \vee \psi)$, and $\exists x\phi$ are S -formulas
- ▶ All Boolean connectives can be defined in terms of \neg and \vee
- ▶ We can define $\forall x\phi$ to be $\neg\exists x\neg\phi$

Definitions on Terms & Formulas

- ▶ Define the notion of a free variable for an S-formula
- ▶ The definition of formula depends on that of term
- ▶ So, we're going to need an auxiliary definition:

$$\text{var}(x) = \{x\}$$

$$\text{var}(c) = \{\}$$

$$\text{var}(f(t_1, \dots, t_n)) = \text{var}(t_1) \cup \dots \cup \text{var}(t_n)$$

- ▶ Is this a definition? (termination!)

$$\text{free}(t_1 = t_2) = \text{var}(t_1) \cup \text{var}(t_2)$$

$$\text{free}(R(t_1, \dots, t_n)) = \text{var}(t_1) \cup \dots \cup \text{var}(t_n)$$

$$\text{free}(\neg\phi) = \text{free}(\phi)$$

$$\text{free}((\phi \vee \psi)) = \text{free}(\phi) \cup \text{free}(\psi)$$

$$\text{free}(\exists x\phi) = \text{free}(\phi) \setminus \{x\}$$

Semantics of First Order Logic

- ▶ What does $\exists v_0 R(v_0, v_1)$ mean?
- ▶ It depends on:
 - ▶ What R means (what relation over what domain?)
 - ▶ What v_1 means (what element of the domain?)
- ▶ What if the is domain \mathbb{N} , R is $<$, and v_1 is 1? If v_1 is 0?
- ▶ An S-interpretation $\mathcal{I} = \langle A, a, \beta \rangle$ where ($\langle A, a \rangle$ is an S-structure)
 - ▶ A is a non-empty set (domain or universe)
 - ▶ a is a function with domain S
 - ▶ $\beta: \text{Var} \rightarrow A$ is an assignment
 - ▶ If $c \in S$ is a constant, then $a.c \in A$
 - ▶ If $f \in S$ is an n -ary function symbol, then $a.f : A^n \rightarrow A$
 - ▶ If $R \in S$ is an n -ary relation symbol, then $a.R \subseteq A^n$

Meaning via Interpretations

- ▶ The meaning of a term in an interpretation $\mathcal{I} = \langle A, a, \beta \rangle$
 - ▶ If $v \in \text{Var}$, then $\mathcal{I}.v = \beta.v$
 - ▶ If $c \in S$ is a constant, then $\mathcal{I}.c = a.c$
 - ▶ If $f(t_1, \dots, t_n)$ is a term, then $\mathcal{I}(f(t_1, \dots, t_n))$ is $(a.f)(\mathcal{I}.t_1, \dots, \mathcal{I}.t_n)$
- ▶ What it means for an interpretation to satisfy a formula:
 - ▶ $\mathcal{I} \models (t_1 = t_2)$ iff $\mathcal{I}.t_1 = \mathcal{I}.t_2$
 - ▶ $\mathcal{I} \models R(t_1, \dots, t_n)$ iff $\langle \mathcal{I}.t_1, \dots, \mathcal{I}.t_n \rangle \in a.R$
 - ▶ $\mathcal{I} \models \neg\phi$ iff not $\mathcal{I} \models \phi$
 - ▶ $\mathcal{I} \models (\phi \vee \psi)$ iff $\mathcal{I} \models \phi$ or $\mathcal{I} \models \psi$
 - ▶ $\mathcal{I} \models \exists x\phi$ iff for some $b \in A$, $\mathcal{I}(x \leftarrow b) \models \phi$

Models & Consequence

- ▶ Let Φ be a set of formulas and ϕ a formula
- ▶ $\mathcal{I} \models \Phi$ (\mathcal{I} is a model of Φ) iff for every $\phi \in \Phi$, $\mathcal{I} \models \phi$
- ▶ $\Phi \models \phi$ (ϕ is a consequence of Φ) iff for every interpretation, \mathcal{I} , which is a model of Φ , we have that $\mathcal{I} \models \phi$
- ▶ ϕ is *valid* iff $\emptyset \models \phi$, which we write as $\models \phi$
- ▶ A formula ϕ is satisfiable, written $Sat \phi$, iff there is an interpretation which is a model of ϕ
- ▶ A set of formulas Φ is satisfiable ($Sat \Phi$), iff there is an interpretation which is a model of all the formulas in Φ

Examples

- ▶ Consider symbol sets $S_{ar} := \{+, \cdot, 0, 1\}$ and $S_{ar}^< := \{+, \cdot, 0, 1, <\}$
- ▶ N denotes the S_{ar} -structure $\langle \omega, +^\omega, \cdot^\omega, 0^\omega, 1^\omega \rangle$, where $+^\omega, \cdot^\omega, 0^\omega, 1^\omega$ correspond to $+, \cdot, 0, 1$ on ω
- ▶ $N^<$ denotes the $S_{ar}^<$ -structure $\langle \omega, +^\omega, \cdot^\omega, 0^\omega, 1^\omega, <^\omega \rangle$, where $<^\omega$ corresponds to $<$ on ω
- ▶ R denotes the S_{ar} -structure $\langle R, +^R, \cdot^R, 0^R, 1^R \rangle$, where R is the set of real numbers
- ▶ $R^<$ denotes the $S_{ar}^<$ -structure $\langle R, +^R, \cdot^R, 0^R, 1^R, <^R \rangle$, where $+^R, \cdot^R, 0^R, 1^R, <^R$ correspond to $+, \cdot, 0, 1, <$ on R
- ▶ $+^R$ and $+^\omega$ are very different objects, but we will drop the subscripts when (we think) no ambiguity will arise

SAT & Validity

- ▶ Lemma: For all ϕ, Φ : $\Phi \models \phi$ iff not $Sat(\Phi \cup \{\neg\phi\})$
- ▶ Proof $\Phi \models \phi$
 - iff for all \mathcal{I} , $\mathcal{I} \models \Phi$ implies $\mathcal{I} \models \phi$
 - iff there is no \mathcal{I} such that $\mathcal{I} \models \Phi$ but not $\mathcal{I} \models \phi$
 - iff there is no \mathcal{I} such that $\mathcal{I} \models \Phi \cup \{\neg\phi\}$
 - iff not $Sat(\Phi \cup \{\neg\phi\})$
- ▶ As a consequence, ϕ is valid iff $\neg\phi$ is not satisfiable