Lecture 15

Pete Manolios
Northeastern

First Order Logic

- Example: Group Theory
  - (G1) For all x, y, z: (x • y) • z = x • (y • z)
  - (G2) For all x: x • e = x
  - (G3) For all x there is a y such that: x • y = e
- Theorem: For every x, there is a y such that y • x = e
- Examples of groups: Nat, +, 0?; Int, +, 0?, Real, *, 1?
- Proof:

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

  Now: y • x = y • x • e = y • x • y • z = y • e • z = y • 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, ...
  - 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 • 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, ..., t_n are terms and *f* is an *n*-ary function symbol, then $f(t_1, ..., t_n)$ 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
  - $R(t_1, ..., t_n)$, 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:

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

  $var(c) = \{\}$

  $var(f(t_1, ..., t_n)) = var(t_1) \cup \cdots \cup var(t_n)$

- Is this a definition? (termination!)

  $free(t_1 = t_2) = var(t_1) \cup var(t_2)$

  $free(R(t_1, ..., t_n)) = var(t_1) \cup \cdots \cup var(t_n)$

  $free(\neg\phi) = free(\phi)$

  $free((\phi \vee \psi)) = free(\phi) \cup free(\psi)$

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

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

Models & Consequence

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

SAT & Validity

- Lemma: For all ϕ, Φ: $\Phi \models \phi$ iff not *Sat* $(\Phi \cup \{\neg\phi\})$
- Proof $\Phi \models \phi$

  iff for all $\mathscr{I}$, $\mathscr{I} \models \Phi$ implies $\mathscr{I} \models \phi$

  iff there is no $\mathscr{I}$ such that $\mathscr{I} \models \Phi$ but not $\mathscr{I} \models \phi$

  iff there is no $\mathscr{I}$ such that $\mathscr{I} \models \Phi \cup \{\neg\phi\}$

  iff not *Sat* $\Phi \cup \{\neg\phi\}$
- As a consequence, ϕ is valid iff $\neg\phi$ is not satisfiable

Examples

- Consider symbol sets S_{ar} := {+,·,0,1} and $S_{ar}^<$:= {+,·,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 +,·,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 +,·,0,1,< on R
- $+^R$ and $+^\omega$ are very different objects, but we will drop the subscripts when (we think) no ambiguity will arise