First-Order Logic and Theories

CIS700 (Fall '24)
Kristopher Micinski

First-Order Logic

- FOL significantly expands propositional logic (which has only atomic propositions) to include *formulas* and *quantifiers*
  - $\forall$ — "for all." E.g., $\forall x.\ \forall y.\ \text{Manager}(x,y) \rightarrow \text{WorksFor}(y,x)$
  - $\exists$ — "there exists." E.g., $\forall x.\ \forall y.\ \exists z.\ x < z \wedge z < y$
- FOL also includes *functions* which operate on elements in a "domain of discourse."
  - $\forall x.\ \forall y.\ x+y \geq x$
  - Here, + is a function, but ≥ is a *relation*
- No ability to quantify over relations! That is beyond the scope of FOL: quantifying over a proposition takes you to *second* order logic

- In propositional logic, an **interpretation** was just a mapping from propositional variables to {T,F}
  - FOL is much more complex; we need interpretations for all functions, constants (zero-arity functions), relations, and we need a domain of discourse.
- Consider the formula from the last slide:
  - $\forall x.\ \forall y.\ \exists z.\ x < z \land z < y$
  - **Exercise**: Identify a domain of discourse (things x, y, and z could be) such that the formula is *true*, also identify one where the statement is *false*
- A formula by itself is meaningless! The meaning of relations, functions, etc… define the meaning (we could define $x + y = 0$ constantly, for example!)

First-Order Models

- A first-order model (*D,I*) is a structure that specifies
  - D — a domain of non-empty objects
  - An *interpretation*:
    - For each function symbol *f* of arity *n*, a function $f^I: D^n \rightarrow D$
    - For each relation of arity n, a subset $R^I \subseteq D^n$
    - D^n is the cartesian product of D n times
    - Each constant is mapped to some element of D
- We can also define *assignments in the model (D,I)*, which are mappings from (sets of) variables to elements in the model D

Examples of Models

- Integers with addition
  - The domain is Z, + is interpreted as addition in Z, = is equality on integers (equality is **not** free in FOL, it must be defined!)
- Natural numbers with < and successor
  - The domain is N, there is one function S(x), the relation < is interpreted as usual less than, and the constant 0 is defined
- A finite graph
  - D = {x, y, z}, a relation Edge(x,y), no constants
  - Sentences such as $\forall x.\ \forall y.\ Edge(x,y) \rightarrow Edge(y,x)$

Truth in the model

- A formula ϕ of L(R, F, C) is *true in the model* M = (D, I) if ϕ is assigned true for all assignments A
- A formula is *valid* if it is true for all models for the language
  - Suppose D is the naturals. Consider the formula $\exists y. =(x, y \oplus y)$, where $\oplus$ is addition, = is equality of naturals, and x is a constant in the interpretation.
  - The formula is true whenever x is an even number.
  - Consider $\forall x. \forall y. \exists z. >(x+y, z)$ where D is {1, 2, …} and I is an interpretation giving > and + their usual values. This sentence is *true* because there is always a z such that x+y>z. However, if D is (instead) {0, 1, …}, the sentence is not true
  - Consider $\forall x. \forall y. <(x,y) \rightarrow \exists z.\ x < z \wedge z < y$
    - True in the rationals, false in the integers

First-Order Theories

- A first-order theory is a set of sentences in FOL which are closed under logical consequence.
- Typically, we give first-order theories by their axioms, the theories are the deductive closure of these sets of axioms.
- Many interesting theories can be axiomatized via a set of first-order axioms: commutative semigroups, boolean algebras, partial orders, equality, dense linear orders, fields, etc…

Equality

- Reflexivity: $\forall x. (x=x)$
- Symmetry: $\forall x \forall y. (x=y \rightarrow y=x)$
- Transitivity: $\forall x \forall y \forall z. ((x=y \wedge y=z) \rightarrow x=z)$

Partial Orders

- Reflexivity: $\forall x. (x \leq x)$
- Antisymmetry: $\forall x \forall y ((x \leq y \land y \leq x) \to x = y)$
- Transitivity: $\forall x \forall y \forall z ((x \leq y \land y \leq z) \to x \leq z)$

Groups

- Associativity: $\forall x \forall y \forall z. ((x \cdot y) \cdot z = x \cdot (y \cdot z))$
- Identity: $\forall x (e \cdot x = x \wedge x \cdot e = x)$
- Inverses: $\forall x \exists y (x \cdot y = e \wedge y \cdot x = e)$

Boolean Algebras

- Now, $\wedge$ (and), and $\vee$ (or) are functions, along with $\neg$ and constants 0 / 1
- Commutativity
  - $\forall x,y.\ (x \vee y = y \vee x)$, $\forall x,y.\ (x \wedge y = y \wedge x)$
- Associativity
  - $\forall x,y,z.\ ((x \vee y) \vee z = x \vee (y \vee z))$, $\forall x,y,z ((x \wedge y) \wedge z = x \wedge (y \wedge z))$
- Distributivity
  - $\forall x,y,z.\ (x \vee (y \wedge z) = (x \vee y) \wedge (x \vee z))$, $\forall x,y,z.\ (x \wedge (y \vee z) = (x \wedge y) \vee (x \wedge z))$
- Identity / complement
  - $\forall x.\ (x \vee 0 = x)$, $\forall x.\ (x \wedge 1 = x)$, $\forall x.\ (x \vee \neg x = 1)$, $\forall x.\ (x \wedge \neg x = 0)$

Löwenheim-Skolem Theorem

- Let L be a first-order language, and let S be a set of sentences of L. If S is satisfiable, then it is satisfiable in a countable model
  - Every satisfiable first-order statement has a countable model!
  - First-order theories cannot control the size of their infinite models

Proving Theorems in FOL

- To prove a theorem in FOL, we can take the axioms of the theory, take the proposition we want to prove, and form a big conjunction
  - Then, we try to prove them using some method
    - E.g., by refutation of the negation of the statement
- Slam axioms + formula together, churn until you find a refutation
- Why don't we prove all theorems this way?
  - First-order logic is hard to reason about in general!
    - But provers do exist (e.g., https://vprover.github.io/), but relatively slow
  - Dealing with equality is tough! Equality often causes explosion / nontermination.
- In practice, it is often **much** easier to solve satisfiability modulo theories!

Satisfiability Modulo Theories

- SMT is a restriction of full FOL:
  - Allows *satisfiability* statements (no quantifiers) over some *specific* theory
  - Variables in SMT formulas are implicitly existentially quantified
    - $x + y > 2*z + y \land z = -2 * y$ (notice: no explicit quantifier)
- In this case, we don't hack on the axioms—instead, an SMT solver has specific theories built in (e.g., bit vectors, integers, datatypes, etc…)
- SMT solvers work quite differently than first-order provers!

Proving FOL statements

- Many proof systems can be extended to FOL: resolution, natural deduction, etc…
- An example is given here (from Melvin Fitting's book):

Example We give a resolution proof of $(\forall x)(P(x) \vee Q(x)) \supset ((\exists x)P(x) \vee (\forall x)Q(x))$.

1. $[\neg\{(\forall x)(P(x) \vee Q(x)) \supset ((\exists x)P(x) \vee (\forall x)Q(x))\}]$
2. $[(\forall x)(P(x) \vee Q(x))]$
3. $[\neg((\exists x)P(x) \vee (\forall x)Q(x))]$
4. $[\neg(\exists x)P(x)]$
5. $[\neg(\forall x)Q(x)]$
6. $[\neg Q(c)]$
7. $[\neg P(c)]$
8. $[P(c) \vee Q(c)]$
9. $[P(c), Q(c)]$
10. $[Q(c)]$
11. $[\,]$