First-order logic

Boulder is the capital of Colorado. ✗

Boulder is a city.

Denver is a city.

City(Boulder) Truth of City(x) depends on
City(Denver) value taken by parameter x
City(Colorado) ✗

Expresses some concepts more succinctly than propositional logic.

Consider "All States contain cities"

FOL: $\forall x.\ State(x) \rightarrow \exists y.\ City(y) \wedge Contains(x,y)$

Prop: $\bigwedge_{j \in Domain} \left(\neg State_j \vee \bigvee_{i \in Domain} City_i \wedge Contains_{j,i} \right)$

Signature τ: relation symbols $r \in R$

function symbols $f \in F$

constant symbols $c \in C$

Example: $\tau = \text{Graph}_{s,t}$ $\begin{cases} E \in R^2 \subseteq R \\ s, t \in C \end{cases}$

τ-Structure: $M = (D, r_1^D, \ldots, f_1^D, \ldots, c_1^D, \ldots)$

D: "carrier" set or "domain" or "universe"

$r_i^M \subseteq \underbrace{D \times \cdots \times D}_{\text{arity}(r_i)}$ $\quad r_i \in R$

$f_i^M : \underbrace{D \times \cdots \times D}_{\text{arity}(f_i)} \to D$ $\quad f_i \in F$

$c_i^M \in D$ $\quad c_i \in C$

Example : M : 1 (s) — 2 — 3 — 4 (t)

$D = \{1, 2, 3, 4\}$

$E' = \{(1,2), (2,3), (3,4)\}$

$E^M = E' \cup (E')^{-1}$ ← inverse of a relation

undirected graph

$s^M = 1$

$t^M = 4$

Syntax

Variables $x_0, x_1, x_2, \ldots \in V$

Terms $t ::= x \in V \mid c \in C \mid f(t_1, \ldots, t_m), \quad f \in F^m$

Atomic formulas $A ::= t = t' \mid r(t_1, \ldots, t_n), \quad r \in R^n$

Formulas $\varphi ::= A \mid \neg\varphi \mid \exists x.\varphi \mid \forall x.\varphi \mid$

$\varphi \wedge \varphi' \mid \varphi \vee \varphi'$

Assignment

$\gamma : V \to D(M)$

Given γ, variable $x \in V$, and $a \in D(M)$,

updated assignment $\gamma[x \mapsto a](y) = \begin{cases} a & \text{if } y = x \\ \gamma(y) & \text{else} \end{cases}$

Semantics

"Satisfaction" relation $M \models \varphi$.

$M \models \varphi$ holds if for all $\gamma : V \to D(M)$,

$M, \gamma \models \varphi$, where:

$M, \gamma \models \varphi \wedge \varphi'$ iff $M, \gamma \models \varphi$ and $M, \gamma \models \varphi'$

$M, \gamma \models \varphi \vee \varphi'$ iff $M, \gamma \models \varphi$ or $M, \gamma \models \varphi'$

$M, \gamma \models \neg \varphi$ iff $M, \gamma \not\models \varphi$

$M, \gamma \models \exists x . \varphi$ iff for some $d \in D(M)$,
$M, \gamma[x \mapsto d] \models \varphi$

$M, \gamma \models \forall x . \varphi$ iff for every $d \in D(M)$,
$M, \gamma[x \mapsto d] \models \varphi$

$M, \gamma \models t = t'$ iff $t^M_\gamma = t'^M_\gamma$

$M, \gamma \models r(t_1, \ldots, t_n)$ iff $(t^M_{1\gamma}, \ldots, t^M_{n\gamma}) \in r^M$

$$x_\gamma^M = \gamma(x)$$

$$c_\gamma^M = c^M$$

$$f_\gamma^M(t_1, \dots, t_m) = f^M(t_{1\gamma}^M, \dots, t_{m\gamma}^M)$$

Sentence: φ s.t. $FV(\varphi) = \emptyset$

$FV(x) = \{x\}, \quad FV(c) = \emptyset$

$FV(f(t_1, \dots, t_m)) = \bigcup_{i \in [m]} FV(t_i)$

$FV(r(t_1, \dots, t_k)) = \bigcup_{i \in [k]} FV(t_k)$

$FV(t = t') = FV(t) \cup FV(t')$

$FV(Qx.\varphi) = FV(\varphi) \setminus \{x\} \quad Q \in \{\exists, \forall\}$

$FV(\varphi \ op \ \varphi') = FV(\varphi) \cup FV(\varphi')$

$FV(\neg\varphi) = FV(\varphi) \qquad op \in \{\wedge, \vee\}$

Satisfiable φ is sat if for some M and γ, $M, \gamma \models \varphi$.

Valid φ is valid if for every M and γ, $M, \gamma \models \varphi$.

"$\models \varphi$", φ is valid.

"$M, \gamma \models \Gamma$", $M, \gamma \models \varphi$ for every $\varphi \in \Gamma$.

"$\Gamma \models \varphi$", for every M, γ, $M, \gamma \models \Gamma \Rightarrow M, \gamma \models \varphi$.

Theory over signature τ is a set of sentences over τ.

Theory Γ is complete if for every φ, $\Gamma \cap \{\varphi, \neg\varphi\} \neq \emptyset$.

Theory Γ is inconsistent if $\{\varphi, \neg\varphi\} \subseteq \Gamma$ for some φ.

$\text{Theory}(M) = \{\varphi : M \models \varphi\}$.

$\text{Theory}(\mathcal{C}) = \bigcap_{M \in \mathcal{C}} \text{Theory}(M)$, $\mathcal{C}$ a set of structures.

Check $Th(K_{97})$ complete? Yes

Check $Th(\text{Finite, simple graphs})$ complete? No

Some results

Compactness: A set of sentences Γ is satisfiable iff it is finitely-satisfiable.

FOL Validity Problem: Given sentences Γ and sentence φ, determine whether $\Gamma \models \varphi$.

Gödel Completeness Theorem (1929): There is a sound & complete proof system for FOL.

$\Rightarrow$ FOL Validity is recursively enumerable (r.e.) for any r.e. set Γ.

Next: An "algorithmic" proof that FOL validity is r.e.

Church-Turing Theorem: FOL Validity is r.e.-hard with $\Gamma = \emptyset$.

Gödel's Incompleteness Theorem: $Th(\mathbb{N}, 0, 1, +, \times, <)$ is not R.E.

FOL Validity is r.e.

Proof by an algorithm with some comments on a more general proof...

A language L is <u>recursively enumerable</u> (r.e.) if there exists a Turing machine M s.t. $L = L(M) = \{ w \in \Sigma^* : M \text{ accepts } w \}$.

So we are after an algorithm which correctly concludes $\Gamma \vDash \varphi$ when it's true, but otherwise rejects or runs forever when $\Gamma \nvDash \varphi$.

We'll call the algorithm "systematic quantifier instantiation"

Intuition on quantifier instantiation

Signature for groups: $\Sigma_{Groups} = (*^2, e^0)$

$*^2$: binary group operation

e^0: identity element

Example: Rubik's Cube

$G = (D^G, *^G, e^G)$, where:

D^G = all "operations" on the cube

$*^G$ = composition of operations

e^G = the "do nothing" operation

A theorem of group theory expressible in FOL:

"identity is unique"

$\varphi_{unique} := \forall x.(\forall y.\ x * y = y \wedge y * x = y) \rightarrow x = e$

A theorem of group theory ?

$\Gamma_{Group} := \{\varphi_{id}, \varphi_{inv}, \varphi_{assoc}\}$

$\varphi_{assoc} := \forall x \forall y \forall z.\ (x * y) * z = x * (y * z)$

$\varphi_{id} := \forall x.\ e * x = x \wedge x * e = x$

$\varphi_{inv} := \forall x \exists y.\ x * y = e \wedge y * x = e$

Can we prove $\bigwedge_{\varphi \in \Gamma_{Group}} \varphi \models \varphi_{unique}$?

Proof by "quantifier instantiation"

1. Γ_{Group} is in prenex normal form.

φ_{unique} is not...

$\forall x.(\forall y.\ x * y = y \wedge y * x = y) \rightarrow x = e$

equiv. $\forall x.\ (\exists y.\ x * y \neq y \vee y * x \neq y) \vee x = e$

equiv. $\forall x.\ \exists y.\ x * y \neq y \vee y * x \neq y \vee x = e \quad =: \varphi'_{unique}$

2. "Skolemize" to obtain universal formulas

→ φ_{assoc} and φ_{id} are already universal

→ φ_{inv} is not...

$\varphi_{inv}' := \forall x.\ x * g(x) = e \wedge g(x) * x = e$ (picks an inverse for x)

The negation of φ_{unique}' is

$\psi := \exists x.\ \forall y.\ x * y = y \wedge y * x = y \wedge x \neq e$

Skolemizing gives us

$\psi' := \forall y.\ c * y = y \wedge y * c = y \wedge c \neq e$

3. Let $X := \{\varphi_{assoc}, \varphi_{id}, \varphi_{inv}', \psi'\}$.

Check: $\Gamma \vDash \varphi_{unique}$ iff X is unsat.

Now we will need a lemma.

Term Expansion Lemma: A set Γ of universal sentences is satisfiable iff $\Gamma^* := \{ \varphi[\bar{t}/\bar{x}] : \forall \bar{x}. \varphi \in \Gamma, t \in GT(\tau) \}$ is satisfiable.

"ground" terms over τ, i.e. no variables

Thus, X is unsat iff X^* is unsat.

Observe that the formulas of X^* are in the quantifier-free theory of equality, for which unsat is decidable.

But, there are infinitely-many formulas in X^*, so we cannot conjuct them all and use a solver.

We instead use compactness of FOL.

By compactness, X^* is unsat iff there is a finite subset $Y \subseteq X^*$ which is unsat.

What this means for our proof:

If indeed $\Gamma_{\text{Group}} \models \varphi_{\text{unique}}$ then some finite subset $Y \subseteq X^*$ is unsat.

Idea: Repeatedly instantiate the quantifiers of formulas in X with more and more terms $t \in GT(\tau)$, in stages.

In each stage with terms T_i, check satisfiability of $\bigwedge_{\varphi \in X_i} \varphi$, where

$$X_i := \{ \varphi[\bar{t}/\bar{x}] : \forall \bar{x}.\varphi \in X,\ t \in T_i \},$$

and $T_i := t_i \cup T_{i-1}$, $T_0 := \emptyset$, and $t_1, t_2, \ldots$ is an enumeration of $GT(\tau)$.

Let's apply this to our set X.

$T_0 = \emptyset$ sat

$T_1 = \{c, e\}$ terms of depth 0

$T_2 = \{c, e, g(c), g(e), c * e, c * c, \ldots\}$ terms of depth 1

Recall, X contains the formulas:

$\varphi_{assoc} := \forall x \forall y \forall z.\ (x * y) * z = x * (y * z)$

$\varphi_{id} := \forall x.\ e * x = x \wedge x * e = x$

$\varphi_{inv'} := \forall x.\ x * g(x) = e \wedge g(x) * x = e$

$\psi' := \forall y.\ c * y = y \wedge y * c = y \wedge c \neq e$

$\psi'[g(c)/y]$

$X_2 \supseteq \{ c * g(c) = g(c) \wedge g(c) * c = g(c) \wedge c \neq e,$

$c * g(c) = e \wedge g(c) * c = e,\ \varphi'_{inv}[c/x]$

$e * c = c \wedge c * e = c,\ \varphi_{id}[c/x] \}$

Claim: X_2 is unsat

$c * g(c) = g(c),\ c * g(c) = e \Rightarrow g(c) = e$

$g(c) = e,\ c * g(c) = e,\ c * e = c \Rightarrow c = e$

But $c \neq e$

Our proof relied on compactness of FOL and also the "term expansion lemma".

A brief explanation of how to prove these and obtain the general theorem that $\Gamma \vDash \varphi$ is r.e. for an r.e. Γ.

Claim: Universal sentences are preserved by taking submodels. If $M \vDash \varphi$ then $M' \vDash \varphi$ for any $M' \subseteq M$.

$M' \subseteq M$: M' is a submodel of M, sometimes "substructure", if $D(M') \subseteq D(M)$, and the interpretations of functions and relations over $D(M')$ is the same.

Fully accessible model: Model M is fully accessible if for every $a \in D(M)$, there is a term $t \in GT(\tau)$ s.t. $t^M = a$.

Claim*: A satisfiable universal φ is satisfied by a fully accessible model.

Proof: Let $M \models \varphi$. Form M' with $D(M')$ being the set of all accessible elements of M, and interpretations of relations and functions being the same as in M. By construction, $M' \subseteq M$ and so $M' \models \varphi$.

Return now to the term expansion lemma...

Term Expansion Lemma: A set Γ of universal sentences is satisfiable iff $\Gamma^* := \{ \varphi[\bar{t}/\bar{x}] : \forall \bar{x}.\varphi \in \Gamma,\ t \in GT(\tau) \}$ is satisfiable.

Proof

($\Rightarrow$) If $M \models \Gamma$ then $M \models \Gamma^*$ is trivial.

($\Leftarrow$) Suppose Γ^* is sat. Then by Herbrand's Theorem, it is satisfied by a Herbrand model, since Γ^* consists of universal sentences, quantifier-free in fact. Clearly this Herbrand model satisfies Γ, because all its elements are accessible using terms. *

* next slides

Herbrand Model A Herbrand model M is one satisfying:

1) $D(M)$ consists of equivalence classes of ground terms modulo a functional congruence $\sim$,

$$D(M) = \{ [t]_\sim : t \in GT(\Sigma) \}$$

2) $c^M = [c]_\sim$

3) $f^M([t_1]_\sim, \ldots, [t_n]_\sim) = [f(t_1, \ldots, t_n)]_\sim$

For every $f \in \mathcal{F}^n$ and $t_1, \ldots, t_n \in GT(\Sigma)$

Claim: Any Herbrand model is fully accessible, because $[t]_\sim$ is accessed by t.

Proof: By induction on structure of t.

Herbrand's Theorem (1930): If a universal sentence has a model then it has a Herbrand model.

Proof: Suppose $M \models \varphi$, with φ being universal.

Define a model H as follows.

First, let $\sim_M$ be the smallest equivalence relation on $GT(\tau)$ s.t.:

$t \sim_M t'$ for any t, t' s.t. $t^M = t'^M$.

Have $f(t_1, \ldots t_n)^M = f(t_1', \ldots, t_n')^M$

whenever $t_i \sim_M t_i'$, and thus

$$f(t_1, \ldots, t_n) \sim_M f(t_1', \ldots, t_n')$$

whenever $t_i \sim_M t_i'$, so $\sim_M$ is a congruence w.r.t. F.

Now, we define H.

$$D(H) = \{ [t]_{\sim_M} : t \in GT(\tau) \}.$$

$$c^H = [c]_{\sim_M}$$

$$f^H([t_1]_{\sim_M}, \ldots, [t_n]_{\sim_M}) = [f(t_1, \ldots, t_n)]_{\sim_M}.$$

$$([t_1]_{\sim_M}, \ldots, [t_k]_{\sim_M}) \in r^H$$

$$\text{iff} \quad (t_1, \ldots, t_k) \in r^M.$$

Check: The case for function symbols is well defined because $\sim_M$ is congruent w.r.t. F.

Check: The case for relation symbols is well defined because $t_i \sim_M t_i'$ implies $t_i^M = t_i'^M$ by definition.

Claim: $H \models \varphi$.

Proof: H is in fact isomorphic to a substructure $M' \subseteq M$, with

$$D(M') = \{ t^M : [t]_{\sim M} \in D(H) \}.$$

Since universal sentences are preserved by substructures, $M' \models \varphi$ and hence $H \models \varphi$ since $H \cong M'$.

This concludes our proof of Herbrand's Theorem.

Observe: We were able to define H without reference to φ's specifics, so we have:

Corollary: A set of universal sentences is Sat iff it is satisfied by a Herbrand model.

Compactness Theorem for quantifier-free ground formulas.

Claim: A set Γ of quantifier-free ground formulas is sat iff it is finitely-sat.

($\Rightarrow$) trivial

($\Leftarrow$) Given the signature is countable, we can enumerate atomic ground atomic formulas

$A_1, A_2, A_3, \ldots$

Consider propositions $p_1, p_2, p_3, \ldots$

For $\varphi \in \Gamma$, let φ_{prop} be the propositional formula obtained from φ by replacing each occurrence of A_i by p_i.

Let $\Gamma_{prop} := \{ \varphi_{prop} : \varphi \in \Gamma \}$.

Because Γ is finitely-sat, Γ_{prop} also is.

Let $W \subseteq \Gamma_{prop}$ be finite. Because Γ is finitely-set, we have that W is sat.

Since

$$W[A_i/p_i] = \{ \varphi_{prop}[A_i/p_i] : \varphi_{prop} \in W \} \subseteq \Gamma$$

is satisfied by some model M,

we can construct a model v s.t. $v \vDash W$

where $v(p_i) = 1$ iff $M \vDash A_i$.

So Γ_{prop} is finitely-set and by compactness of propositional logic, Γ_{prop} is sat.

Let $v \vDash \Gamma_{prop}$. Define

M s.t. $M \vDash A_i$ iff $v(p_i) = 1$.

Oops... Why would this be possible?

We might have $A_i := c_1 = c_2$ and
$A_j := f(c_1) = f(c_2)$,

but $v(p_i) = 1$ and $v(p_j) = 0$.

Add congruence properties to Γ_{prop} ...

For every $t, t', t_1, \ldots, t_n, t_1', \ldots, t_n' \in GT(\tau)$:

$$P_{t=t} \quad , \quad P_{t=t'} \rightarrow P_{t'=t} \quad ,$$

$$P_{t_1=t_2} \wedge P_{t_2=t_3} \rightarrow P_{t_1=t_3} \quad ,$$

$$\bigwedge_{i \in [n]} P_{t_i=t_i'} \rightarrow \left(P_{R(t_1,\ldots,t_n)} \leftrightarrow P_{R(t_1',\ldots,t_n')} \right) \quad ,$$

$$\bigwedge_{i \in [k]} P_{t_i=t_i'} \rightarrow P_{f(t_1,\ldots,t_n)=f(t_1',\ldots,t_n')}$$

Let Δ be the set of formulas specified above.

Now we can finish the proof.

Suppose Γ is unsat. We want to prove a finite subset of it is unsat.

Claim: Γ is sat iff $\Gamma_{prop} \cup \Delta$ is sat.

Proof: Exercise

Now, if Γ is unsat, then $\Gamma_{prop} \cup \Delta$ is too.

By propositional compactness, there is a finite subset $W \subseteq \Gamma_{prop} \cup \Delta$ that is unsat.

Consider $W \cap \Gamma_{prop} =: W'$. Let F be the formulas of Γ corresponding to those in W'. Then F is finite, and it is unsat because $W' \cup \Delta$ is unsat (since $W \subseteq W' \cup \Delta$ is already unsat).