Predicate Logic - Part II
Semantics & Proof Theory

Outline

- Interpretations and models $\mathcal{M}$
- Satisfaction $\mathcal{M} \models \phi$
- Semantic Entailment $\Gamma \models \psi$
- Proofs $\Gamma \vdash \psi$

Interpretations

When we write a formula we usually have a particular setting or *interpretation* in mind. This involves specifying a *universe* of discourse A, a non-empty set of things we want to reason about.

(e.g. $\mathbb{R}$, set of people at McMaster, or set of sensor inputs values and actuator output values for a control system).

Just as in a program, constants are assigned values from A, function and predicate symbols are interpreted as specific functions or relation. We can then interpret the meaning of a formula in our particular *interpretation structure* or *model*.

Notation: Let ϕ and ψ be predicate logic formulas and Γ be a sequence of formulas.

Models

Let Γ be a set of formulas in which occur the predicate symbols $P_1, \ldots, P_k$, function symbols $f_1, \ldots, f_j$ and constants $c_1, \ldots, c_m$. These formulas have the predicate vocabulary

$$(\mathcal{F}, \mathcal{P}) = (\{f_1, \ldots, f_j, c_1, \ldots, c_m\}, \{P_1, \ldots, P_k\})$$

Def: A *model* $\mathcal{M}$ *for* $(\mathcal{F}, \mathcal{P})$ provides

1. A is a nonempty set. The *universe* (of concrete values).
2. for each $f \in \mathcal{F}$ such that $arity(f) = n$, a concrete function

   $$f^{\mathcal{M}} : A^n \to A$$

3. for each $P \in \mathcal{P}$ such that $arity(P) = n$, a relation

   $$P^{\mathcal{M}} \subseteq A^n$$

Note: For for a constant symbol, $c \in \mathcal{F}$ with $arity(c) = 0$, we have $c^{\mathcal{M}} \in A$ is a specific value in A.

Creating a Model:

To create a model for Γ, do the following:

1. Determine the predicate vocabulary $(\mathcal{F}, \mathcal{P})$.

2. Determine *signature* or required *type* of each symbol (e.g. $f^{\mathcal{M}} : A^2 \to A$, $P^{\mathcal{M}} \subseteq A^4$).

3. Choose a universe $A \neq \emptyset$.

4. Define interpretation for each symbol with required properties.

   E.g. To create $\mathcal{M}$ making $\forall x(P(x) \to Q(x))$ true, chose $P^{\mathcal{M}}, Q^{\mathcal{M}} \subseteq A$ such that $P^{\mathcal{M}} \subseteq Q^{\mathcal{M}}$. Why?

Note 1: Keep it simple! Use a finite or numerical A when possible.

Note 2: You must interpret symbols consistently (the same) in every occurrence in all formulas.

Do interpretation structure example:

- create interpretation structure for a sentence

- create interpretation structure that makes a sentence or sentence form true/false.
note: not always possible!

- every sentence is either true or false in an interpretation structure $\mathcal{M}$ but this is not always the case for sentence forms

Interpretation of Terms, Sentences and Sentence Forms

Let t be a term with $FV(t) = \{x_1, \ldots, x_n\}$. Then the interpretation of t defines an n-ary function $t^{\mathcal{M}} : A^n \to A$.

Let ϕ be a formula with $FV(\phi) = \{x_1, \ldots, x_n\}$ then the interpretation of ϕ defines an n-ary relation $\phi^{\mathcal{M}} \subseteq A^n$.

E.g. Consider interpretation of t, the term $f(a, y)$ and ϕ and ψ the formulas $P(a, x)$ and $\forall x P(f(y, b), f(x, a))$ respectively in $\mathcal{M}$ where

$A = \mathbb{N}$
$P^{\mathcal{M}} = \{(x, y) \in \mathbb{N}^2 | x \leq y\}$
$f^{\mathcal{M}}(x, y) = x + y$
$a^{\mathcal{M}} = 1$ and $b^{\mathcal{M}} = 0$.
Then $f^{\mathcal{M}}(a, y) : \mathbb{N} \to \mathbb{N}$ i.e. $y \mapsto 1 + y$
and $\psi^{\mathcal{M}} = \{0, 1\} \subseteq \mathbb{N}$ in $\mathcal{M}$.

Satisfaction

Let ϕ be a formula with at most k free variables $x_1, x_2, \ldots, x_k$ and $\mathcal{M}$ be a model for ϕ with universe A. To determine the truth value of ϕ, we need to assign values to $x_1, x_2, \ldots, x_k$ from A.

We can do this via a lookup table l which maps variables var to values in A creating an *environment* to determine the truth of ϕ:

$$l : \text{var} \to A$$

Modifying a lookup table:

Suppose we want to change the value for variable x in an existing lookup table l, then we write $l[x \mapsto a]$ to denote the map:

$$l[x \mapsto a](y) = \begin{cases} a & \text{when } y = x \\ l(y) & \text{otherwise} \end{cases}$$

Satisfaction (cont)

Given a model $\mathcal{M}$ and a mapping $l : var \rightarrow A$, such that $l(x_i) = a_i$, we can now interpret a terms in our model.

Given a term t, the interpretation of t in model $\mathcal{M}$ with environment l is given as follows:

If t is c (a constant) then $t^{\mathcal{M}}$ is $c^{\mathcal{M}}$.

If t is x_i then $t^{\mathcal{M}}$ is $l(x_i) = a_i$.

If t is $f(t_1, \ldots, t_n)$ then $t^{\mathcal{M}}$ is $f^{\mathcal{M}}(t_1^{\mathcal{M}}, \ldots, t_n^{\mathcal{M}})$.

For a formula ϕ, with model $\mathcal{M}$ and environment l we can now define a satisfaction relation

$$\mathcal{M} \models_l \phi$$

which means that ϕ evaluates to T (true) when free variables are assigned values according to l in model $\mathcal{M}$.

Satisfaction (cont)

Def: Given a model $\mathcal{M}$ for $(\mathcal{F}, \mathcal{P})$ an environment l, and a formula ϕ over $(\mathcal{F}, \mathcal{P})$, we write $\mathcal{M} \models_l \phi$ if:

P : ϕ is of the form $P(t_1, \ldots, t_n)$ and $(t_1^{\mathcal{M}}, \ldots, t_n^{\mathcal{M}}) \in P^{\mathcal{M}}$ when the variables of t_i are replaced by values in A according to l, then

$$\mathcal{M} \models_l P(t_1, \ldots, t_n)$$

$\forall x$: ϕ is $\forall x \psi$ and $\mathcal{M} \models_{l[x \mapsto a]} \psi$ for all $a \in A$ then $\mathcal{M} \models_l \forall x \psi$.

$\exists x$: ϕ is $\exists x \psi$ and $\mathcal{M} \models_{l[x \mapsto a]} \psi$ for some $a \in A$ then $\mathcal{M} \models_l \exists x \psi$.

Satisfaction (cont)

$\neg$: ϕ is $\neg\psi$ and $\mathcal{M} \not\models_l \psi$ then $\mathcal{M} \models_l \neg\psi$.

$\vee$: ϕ is $\psi_1 \vee \psi_2$ and $\mathcal{M} \models_l \psi_1$ or $\mathcal{M} \models_l \psi_2$ then $\mathcal{M} \models_l \psi_1 \vee \psi_2$.

$\wedge$: ϕ is $\psi_1 \wedge \psi_2$ and $\mathcal{M} \models_l \psi_1$ and $\mathcal{M} \models_l \psi_2$ then $\mathcal{M} \models_l \psi_1 \wedge \psi_2$.

$\rightarrow$: ϕ is $\psi_1 \rightarrow \psi_2$ and if $\mathcal{M} \models_l \psi_1$ then $\mathcal{M} \models_l \psi_2$, then $\mathcal{M} \models_l \psi_1 \rightarrow \psi_2$.

$\leftrightarrow$: ϕ is $\psi_1 \leftrightarrow \psi_2$ and $\mathcal{M} \models_l \psi_1$ iff $\mathcal{M} \models_l \psi_2$, then $\mathcal{M} \models_l \psi_1 \leftrightarrow \psi_2$.

In the above $\mathcal{M} \not\models_l \phi$ denotes that $\mathcal{M} \models_l \phi$ does not hold.

Def: If $\mathcal{M} \models_l \phi$ holds for all possible l, then we say that model $\mathcal{M}$ *satisfies* ϕ or $\mathcal{M}$ *is a model for* ϕ and write $\mathcal{M} \models \phi$.

Truth, Models & Validity

Note: Its possible that $\mathcal{M} \not\models \phi$ and $\mathcal{M} \not\models \neg\phi$ (i.e. ϕ is neither true nor false in $\mathcal{M}$). This is only true for sentence forms (i.e. ϕ has free variables).

How does this work? If there exist environments l and l' such that $\mathcal{M} \models_l \phi$ and $\mathcal{M} \not\models_{l'} \phi$.

Note: Any sentence is either true or false in $\mathcal{M}$. (Why?)

For a sequence of predicate logic formulas $\Gamma = \phi_1, \ldots, \phi_n$, we say $\mathcal{M}$ is a *model* for Γ, written $\mathcal{M} \models \Gamma$ iff $\mathcal{M} \models \phi_i$ for every $\phi_i \in \Gamma$.

Def: Suppose ϕ is a formula over $(\mathcal{F}, \mathcal{P})$. Then ϕ is *(universally) valid*, written $\models \phi$, if ϕ is true in <u>every</u> model for $(\mathcal{F}, \mathcal{P})$.

Example: Find an interpretation such that

$$P(x) \to Q(x)$$

is neither true nor false.

Example valid formulas:

$$P(x) \to P(x)$$

$$\forall x(P(x) \wedge (P(x) \to Q(x)) \to Q(x))$$

Universal Closure and PVS

Def: For ϕ with free variables $x_1, \ldots, x_n$, the formula $\forall x_1 \forall x_2 \ldots \forall x_n \phi$ is the *universal closure of* ϕ. Note that

$$\mathcal{M} \models \phi \text{ iff } \mathcal{M} \models (\forall x_1)(\forall x_2) \ldots (\forall x_n)\phi$$

(follows immediately from definition of $\models$.)

PVS uses this as a short cut to implicitly quantify theorem statements. E.g.

```
x,y,z:VAR nat
f(x,y):nat = x + y

T1: THEOREM f(x,y)=f(y,x)
```

in prover becomes:

```
T1 :


  |-------
{1} (FORALL (x: nat, y: nat): f(x, y) = f(y, x))

Rule?
```

“Reality” Check

A set of logical formulas Γ can be used to specify system requirements.

A program $\mathcal{M}$ is an interpretation or *model* of the function and predicate symbols of the logical formulas in the specification Γ.

If the program is a model of the specification ($\mathcal{M} \models \Gamma$). Then the program satisfies each requirement $\phi_i \in \Gamma$.

Thus given a set of requirements Γ, an important question is:
Does a model exist for Γ? (i.e. Is there a program that meets the requirements?)

If the requirements are contradictory (inconsistent), then no model will exist! E.g.

$$\Gamma = \exists x(P(x)), \forall x(P(x) \to Q(x)), \forall x(P(x) \to \neg Q(x))$$

Γ is a *trivial* specification if it is satisfied by every interpretation of Γ.

Semantic Entailment $\models$

Recall that for propositional logic we say that premises $\phi_1, \ldots, \phi_n$ *semantically entail* conclusion ψ, denoted

$$\phi_1, \phi_2, \ldots, \phi_n \models \psi$$

if whenever all the ϕ_is evaluate to T, then ψ evaluates to T.

We now extend this concept to predicate logic formulas.

Def: We say $\phi_1, \ldots, \phi_n$ *semantically entail* ψ denoted

$$\phi_1, \phi_2, \ldots, \phi_n \models \psi$$

if whenever $\mathcal{M} \models_l \phi_i$, for all $i = 1, \ldots, n$ then $\mathcal{M} \models_l \psi$ for all models $\mathcal{M}$ and lookup tables l.

Semantic Entailment $\models$ (cont)

When $\phi_1, \ldots \phi_n, \psi$ are all sentences, then this reduces to

$$\phi_1, \phi_2, \ldots, \phi_n \models \psi$$

if whenever $\mathcal{M} \models \phi_i$, for all $i = 1, \ldots, n$ then $\mathcal{M} \models \psi$ for all models $\mathcal{M}$.

Example: $\forall x(P(x) \rightarrow Q(x)) \models \forall x P(x) \rightarrow \forall x Q(x)$. Why?

We could, in theory at least, show that $\Gamma \models \psi$ computationally for propositional logic by checking the truth table.

In general, showing $\Gamma \models \psi$ computationally for predicate logic is not possible. Why? We have to check *all* models $\mathcal{M}$ and *all* lookup tables l which might be tough for models with an infinite universe A.

As we will see, instead we show $\Gamma \vdash \psi$.

Semantic Entailment $\models$ (cont)

How do we show that $\Gamma \not\models \psi$?

Just as with propositional logic, we find a counter example.

Assuming Γ is $\phi_1, \ldots, \phi_n$, in this case we find a model $\mathcal{M}$ such that, $\mathcal{M} \models \phi_i$ for all $i = 1, \ldots, n$ but $\mathcal{M} \not\models \psi$.

Example:

$$\forall x P(x) \to \forall x Q(x) \not\models \forall x (P(x) \to Q(x))$$

Semantics of Equality

In interpretation structures (models), by convention, = must always be interpreted as the "diagonal relation".

For $A = \{a, b, c, \ldots\}$ the characteristic function for the equality predicate, $=^{\mathcal{M}}: A^2 \rightarrow \{T, F\}$, is given by:

$=^{\mathcal{M}}$	a	b	c	$\ldots$
a	T	F	F	F
b	F	T	F	F
c	F	F	T	F
$\vdots$	F	F	F	$\ddots$

That is $=^{\mathcal{M}} \subseteq A^2$ is given by:

$$=^{\mathcal{M}} := \{(a, a), (b, b), (c, c), \ldots\}$$

In general, $=^{\mathcal{M}}$ is the subset $\mathbf{A} \times \mathbf{A}$ given by:

$$\{(x, x) | x \in A\}$$

i.e. $a = b$ is true in $\mathcal{M}$ iff $a^{\mathcal{M}}$ and $b^{\mathcal{M}}$ are the same element.

Proofs

Can use all rules from Propositional logic + additional rules for dealing with quantifiers.

$\Gamma \vdash \phi$ means that from set of premises Γ, there is a formal proof of ϕ.

Proofs in Predicate Logic are even more important than in Propositional Logic because there is no *decision procedure* or algorithm for arbitrary predicate logic formulas like truth tables.

Proof Rules: $\forall e$

Suppose we have been able to show $\Gamma \vdash \forall x \phi$. i.e., Assuming the premises are true we have shown ϕ is true for all evaluations of x.

Thus if $\phi[t/x]$ is a valid substitution then clearly we should be able to conclude $\Gamma \vdash \phi[t/x]$.

We will call this rule "forall elimination" (aka. Universal Specification) denoted $\forall e$ and summarized as follows:

$$\frac{\forall x \phi}{\phi[t/x]} \forall e$$

where $\phi[t/x]$ is a valid substitution.

Why do we need the *side condition* about a valid substitution? Consider $\forall x \exists y (x < y)$.

Take ϕ to be $\exists y (x < y)$ so $\phi[y/x]$ is $\exists y (y < y)$!

Proof Rules: $\forall i$

Given Γ, a set of formulas, the free variables Γ is the union of the free variables of each $\phi_i \in \Gamma$. I.e.

$$FV(\Gamma) = \bigcup_{\phi_i \in \Gamma} FV(\phi_i)$$

If $\Gamma \vdash \phi[x_0/x]$ and $x_0 \notin FV(\Gamma)$ then $\Gamma \vdash \forall x \phi$.

We will call this rule "forall introduction" (aka. Universal Generalization) denoted $\forall i$ and summarize it as follows:

$$\frac{\boxed{\begin{array}{l} x_0 \\ \quad\quad\vdots \\ \quad\quad \phi[x_0/x] \end{array}}}{\forall x \phi} \; \forall i$$

where x_0 is a "fresh" or new variable not appearing in our premises or assumptions.

Examples Using $\forall e$ **&** $\forall i$

For $\Gamma := P(y), \forall x(P(x) \rightarrow Q(x)$ you **cannot** conclude $\Gamma \vdash \forall x P(x)$

Reconsider our Oscar example. Recall we translated:

No student who likes math also likes Oscar.

as

$$\forall x(S(x) \land M(x) \rightarrow \neg L(x,o))$$

and

$$\forall x(S(x) \rightarrow \neg(M(x) \land L(x,o)))$$

Show that

$$\vdash \quad \forall x(S(x) \land M(x) \rightarrow \neg L(x,o)) \leftrightarrow \forall x(S(x) \rightarrow \neg(M(x) \land L(x,o)))$$

Proof Rules: $\exists i$

Suppose we have been able to show $\Gamma \vdash \phi[t/x]$. i.e., Assuming the premises are true we have shown ϕ is true when free occurrences of x are replaced by the term t.

If $\phi[t/x]$ is a valid substitution there exists a value for x, namely the value that t evaluates to, that can make ϕ true. Thus if $\Gamma \vdash \phi[t/x]$, we conclude $\Gamma \vdash \exists x \phi$.

We will call this rule "exists introduction" (aka. Existential Generalization) denoted $\exists i$ and summarized as follows:

$$\frac{\phi[t/x]}{\exists x \phi} \exists e$$

where $\phi[t/x]$ is a valid substitution.

Proof Rules: $\exists e$

If $\Gamma, \phi[x_0/x] \vdash \chi$ where:

1. $\phi[x_0/x]$ is a valid substitution, and
2. $x_0 \notin FV(\Gamma) \cup FV(\chi)$.

Then $\Gamma, (\exists x)\phi \vdash \chi$.

We will call this rule "exists elimination" (aka. Existential Premise) denoted $\exists e$ and summarize it as follows:

$$\dfrac{\exists x \phi \quad \boxed{\begin{array}{ll} x_0 & \phi[x_0/x] \\ & \quad\vdots \\ & \quad\chi \end{array}}}{\chi} \; \exists e$$

where x_0 is a "fresh" or new variable not appearing in our other premises and assumptions, or in the conclusion and $\phi[x_0/x]$ is a valid substitution.