First-Order Logic

Maria João Frade

HASLab - INESC TEC
Departamento de Informática, Universidade do Minho

2022/2023

Roadmap

- **Classical First-Order Logic**
  - syntax; semantics; decision problems SAT and VAL;
  - normal forms; Herbrandization; Skolemization;
  - FOL with equality; many-sorted FOL.
- **Modeling with FOL**
  - Formalization of domain models in FOL.

(Classical) First-Order Logic

Introduction

First-order logic (FOL) is a richer language than propositional logic. Its lexicon contains not only the symbols $\wedge$, $\vee$, $\neg$, and $\rightarrow$ (and parentheses) from propositional logic, but also the symbols $\exists$ and $\forall$ for "there exists" and "for all", along with various symbols to represent variables, constants, functions, and relations.

There are two sorts of things involved in a first-order logic formula:

- *terms*, which denote the objects that we are talking about;
- *formulas*, which denote truth values.

Examples:

"Not all birds can fly."
"Every mother is older than her children."
"John and Peter have the same maternal grandmother."

Syntax

The alphabet of a first-order language is organised into the following categories.

- *Variables:* $x, y, z, \ldots \in \mathcal{X}$ (arbitrary elements of an underlying domain)
- *Constants:* $a, b, c, \ldots \in \mathcal{C}$ (specific elements of an underlying domain)
- *Functions:* $f, g, h, \ldots \in \mathcal{F}$ (every function f has a fixed arity, $\mathsf{ar}(f)$)
- *Predicates:* $P, Q, R, \ldots \in \mathcal{P}$ (every predicate P has a fixed arity, $\mathsf{ar}(P)$)
- *Logical connectives:* $\top$, $\bot$, $\wedge$, $\vee$, $\neg$, $\rightarrow$, $\forall$ (*for all*), $\exists$ (*there exists*)
- *Auxiliary symbols*: ".", "(" and ")".

We assume that all these sets are disjoint. $\mathcal{C}$, $\mathcal{F}$ and $\mathcal{P}$ are the non-logical symbols of the language. These three sets constitute the *vocabulary* $\mathcal{V} = \mathcal{C} \cup \mathcal{F} \cup \mathcal{P}$.

Syntax

Terms

The set of *terms* of a first-order language over a vocabulary $\mathcal{V}$ is given by the following abstract syntax

$$\mathbf{Term}_{\mathcal{V}} \ni t \ ::= \ x \mid c \mid f(t_1, \ldots, t_{\mathsf{ar}(f)})$$

Formulas

The set $\mathbf{Form}_{\mathcal{V}}$, of *formulas* of FOL, is given by the abstract syntax

$$\begin{aligned}\mathbf{Form}_{\mathcal{V}} \ni \phi, \psi \quad ::= \quad & P(t_1, \ldots, t_{\mathsf{ar}(P)}) \mid \bot \mid \top \mid (\neg\phi) \mid (\phi \wedge \psi) \mid (\phi \vee \psi) \\ & \mid (\phi \rightarrow \psi) \mid (\forall x.\, \phi) \mid (\exists x.\, \phi)\end{aligned}$$

An *atomic formula* has the form $\bot$, $\top$, or $P(t_1, \ldots, t_{\mathsf{ar}(P)})$. A *ground term* is a term without variables. *Ground formulas* are formulas without variables, i.e., quantifier-free formulas ϕ such that all terms occurring in ϕ are ground terms.

Syntax

Convention

We adopt some syntactical conventions to lighten the presentation of formulas:

- Outermost parenthesis are usually dropped.
- In absence of parentheses, we adopt the following convention about precedence. Ranging from the highest precedence to the lowest, we have respectively: $\neg$, $\wedge$, $\vee$ and $\rightarrow$. Finally we have that $\rightarrow$ binds more tightly than $\forall$ and $\exists$.
- All binary connectives are right-associative.
- Nested quantifications such as $\forall x. \forall y. \phi$ are abbreviated to $\forall x, y.\, \phi$.
- $\forall \overline{x}. \phi$ denotes the nested quantification $\forall x_1, \ldots, x_n.\, \phi$.

Modeling with FOL

"Not all birds can fly."

We can code this sentence assuming the two unary predicates B and F expressing

$B(x)$ – x is a bird
$F(x)$ – x can fly

The declarative sentence "Not all birds can fly" can now be coded as

$$\neg(\forall x.\, B(x) \rightarrow F(x))$$

or, alternatively, as

$$\exists x.\, B(x) \wedge \neg F(x)$$

Modeling with FOL

"Every mother is older than her children."
"John and Peter have the same maternal grandmother."

Using constants symbols j and p for John and Peter, and predicates $=$, $mother$ and $older$ expressing that

$mother(x, y)$ – x is mother of y
$older(x, y)$ – x is older than y

these sentences could be expressed by

$$\forall x.\forall y.\ mother(x, y) \to older(x, y)$$

$$\forall x, y, u, v.\ mother(x, y) \wedge mother(y, j) \wedge mother(u, v) \wedge mother(v, p) \to x = u$$

A different and more elegant encoding is to represent y'mother in a more direct way, by using a function instead of a relation. We write $m(y)$ to mean y'mother. This way the two sentences above have simpler encondings.

$$\forall x.\ older(m(x), x) \qquad \text{and} \qquad m(m(j)) = m(m(p))$$

Modeling with FOL

Assume further the following predicates and constant symbols

$flower(x)$ – x is a flower $likes(x, y)$ – x likes y
$sport(x)$ – x is a sport $brother(x, y)$ – x is brother of y
a – Anne

- "Anne likes John's brother." $\exists x.\ brother(x, j) \wedge likes(a, x)$
- "John likes all sports." $\forall x.\ sports(x) \to likes(j, x)$
- "John's mother likes flowers." $\forall x.\ flower(x) \to likes(m(j), x)$
- "John's mother does not like some sports." $\exists y.\ sport(y) \wedge \neg likes(m(j), y)$
- "Peter only likes sports." $\forall x.\ likes(p, x) \to sports(x)$
- "Anne has two children."

$$\exists x_1, x_2.\ mother(a, x_1) \wedge mother(a, x_2) \wedge x_1 \neq x_2 \wedge \forall z.\ mother(a, z) \to z = x_1 \vee z = x_2$$

Free and bound variables

- The *free variables* of a formula ϕ are those variables occurring in ϕ that are not quantified. FV(ϕ) denotes the set of free variables occurring in ϕ.
- The *bound variables* of a formula ϕ are those variables occurring in ϕ that do have quantifiers. BV(ϕ) denote the set of bound variables occurring in ϕ.

Note that variables can have both free and bound occurrences within the same formula. Let ϕ be $\exists x.\ R(x, y) \wedge \forall y.\ P(y, x)$, then

$$\text{FV}(\phi) = \{y\} \ \text{ and } \ \text{BV}(\phi) = \{x, y\}.$$

- A formula ϕ is *closed* (or *a sentence*) if it does not contain any free variables.
- If FV(ϕ) $= \{x_1, \ldots, x_n\}$, then
  - its *universal closure* is $\forall x_1. \ldots \forall x_n.\ \phi$
  - its *existential closure* is $\exists x_1. \ldots \exists x_n.\ \phi$

Substitution

Substitution

- We define $u[t/x]$ to be the term obtained by replacing each occurrence of variable x in u with t.
- We define $\phi[t/x]$ to be the formula obtained by replacing each free occurrence of variable x in ϕ with t.

Care must be taken, because substitutions can give rise to undesired effects!

Substitution

Let us illustrate the problem...

Let ϕ be $\exists x.\, likes(x, y) \wedge \forall y.\, older(y, x)$, and t be the term $m(x)$.

- Now let us perform the substitution $\phi[t/y]$

  $$(\exists x.\, likes(x, y) \wedge \forall y.\, older(y, x))[(m(x)/y] \;=\; \exists x.\, likes(x, m(x)) \wedge \forall y.\, older(y, x)$$

  which is **wrong!**

  - The meaning of the formula has completly changed.
  - The free variable x in $m(x)$ was captured inadvertently by the $\exists x$.

- This can be fixed if we change the name of the bounded varible in $\exists x$, by renaming it to a fresh variable.

  $$(\exists z.\, likes(z, y) \wedge \forall y.\, older(y, z))[(m(x)/y] \;=\; \exists z.\, likes(z, m(x)) \wedge \forall y.\, older(y, z)$$

  which is **OK!**

Substitution

Given a term t, a variable x and a formula ϕ, we say that *t is free for x in ϕ* if no free x in ϕ occurs in the scope of $\forall z$ or $\exists z$ for any variable z occurring in t.

From now on we will assume that all substitutions satisfy this condition. That is when performing the $\phi[t/x]$ we are always assuming that t is free for x in ϕ.

Substitution

Convention

We write $\phi(x_1, \ldots, x_n)$ to denote a formula having free variables $x_1, \ldots, x_n$. We write $\phi(t_1, \ldots, t_n)$ to denote the formula obtained by replacing each free occurrence of x_i in ϕ with the term t_i. When using this notation, it should always be assumed that each t_i is free for x_i in ϕ.

Also note that when writhing $\phi(x_1, ..., x_n)$ we do not mean that $x_1, ..., x_n$ are the only free variables of ϕ.

Semantics

$\mathcal{V}$-structure

Let $\mathcal{V}$ be a vocabulary. A *$\mathcal{V}$-structure* $\mathcal{M}$ is a pair $\mathcal{M} = (D, I)$ where D is a nonempty set called the *interpretation domain*, and I is an *interpretation function* that assigns constants, functions and predicates over D to the symbols of $\mathcal{V}$ as follows:

- for each constant symbol $c \in \mathcal{C}$, the interpretation of c is a constant $I(c) \in D$;
- for each $f \in \mathcal{F}$, the interpretation of f is a function $I(f) : D^{\mathsf{ar}(f)} \to D$;
- for each $P \in \mathcal{P}$, the interpretation of P is a function $I(P) : D^{\mathsf{ar}(P)} \to \{0, 1\}$. In particular, 0-ary predicate symbols are interpreted as truth values.

$\mathcal{V}$-structures are also called *models* for $\mathcal{V}$.

Semantics

Assignment

An *assignment* for a domain D is a function $\alpha : \mathcal{X} \to D$.

We denote by $\alpha[x \mapsto a]$ the assignment which maps x to a and any other variable y to $\alpha(y)$.

Given a $\mathcal{V}$-structure $\mathcal{M} = (D, I)$ and given an assignment $\alpha : \mathcal{X} \to D$, we define an *interpretation function for terms*, $\alpha_{\mathcal{M}} : \mathbf{Term}_{\mathcal{V}} \to D$, as follows:

$$\begin{array}{lcl} \alpha_{\mathcal{M}}(x) & = & \alpha(x) \\ \alpha_{\mathcal{M}}(c) & = & I(c) \\ \alpha_{\mathcal{M}}(f(t_1, \ldots, t_n)) & = & I(f)(\alpha_{\mathcal{M}}(t_1), \ldots, \alpha_{\mathcal{M}}(t_n)) \end{array}$$

Semantics

Satisfaction relation

Given a $\mathcal{V}$-structure $\mathcal{M} = (D, I)$ and given an assignment $\alpha : \mathcal{X} \to D$, we define the *satisfaction relation* $\mathcal{M}, \alpha \models \phi$ for each $\phi \in \mathbf{Form}_{\mathcal{V}}$ as follows:

$$\begin{array}{lll} \mathcal{M}, \alpha \models \top & & \\ \mathcal{M}, \alpha \not\models \bot & & \\ \mathcal{M}, \alpha \models P(t_1, \ldots, t_n) & \text{iff} & I(P)(\alpha_{\mathcal{M}}(t_1), \ldots, \alpha_{\mathcal{M}}(t_n)) = 1 \\ \mathcal{M}, \alpha \models \neg\phi & \text{iff} & \mathcal{M}, \alpha \not\models \phi \\ \mathcal{M}, \alpha \models \phi \wedge \psi & \text{iff} & \mathcal{M}, \alpha \models \phi \text{ and } \mathcal{M}, \alpha \models \psi \\ \mathcal{M}, \alpha \models \phi \vee \psi & \text{iff} & \mathcal{M}, \alpha \models \phi \text{ or } \mathcal{M}, \alpha \models \psi \\ \mathcal{M}, \alpha \models \phi \to \psi & \text{iff} & \mathcal{M}, \alpha \not\models \phi \text{ or } \mathcal{M}, \alpha \models \psi \\ \mathcal{M}, \alpha \models \forall x.\, \phi & \text{iff} & \mathcal{M}, \alpha[x \mapsto a] \models \phi \text{ for all } a \in D \\ \mathcal{M}, \alpha \models \exists x.\, \phi & \text{iff} & \mathcal{M}, \alpha[x \mapsto a] \models \phi \text{ for some } a \in D \end{array}$$

Validity and satisfiability

When $\mathcal{M}, \alpha \models \phi$, we say that $\mathcal{M}$ *satisfies* ϕ *with* α.

We write $\mathcal{M} \models \phi$ iff $\mathcal{M}, \alpha \models \phi$ holds for every assignment α.

A formula ϕ is

- *valid* iff $\mathcal{M}, \alpha \models \phi$ holds for all structure $\mathcal{M}$ and assignments α. A valid formula is called a *tautology*. We write $\models \phi$.
- *satisfiable* iff there is some structure $\mathcal{M}$ and some assigment α such that $\mathcal{M}, \alpha \models \phi$ holds.
- *unsatisfiable* iff it is not satisfiable. An unsatisfiable formula is called a *contradiction*.
- *refutable* iff it is not valid.

Consequence and equivalence

Given a set of formulas Γ, a model $\mathcal{M}$ and an assignment α, $\mathcal{M}$ is said to *satisfy* Γ *with* α, denoted by $\mathcal{M}, \alpha \models \Gamma$, if $\mathcal{M}, \alpha \models \phi$ for every $\phi \in \Gamma$.

Γ *entails* ϕ (or that ϕ is a *logical consequence* of Γ), denoted by $\Gamma \models \phi$, iff for all structures $\mathcal{M}$ and assignments α, whenever $\mathcal{M}, \alpha \models \Gamma$ holds, then $\mathcal{M}, \alpha \models \phi$ holds as well.

ϕ is *logically equivalent* to ψ, denoted by $\phi \equiv \psi$, iff $\{\phi\} \models \psi$ and $\{\psi\} \models \phi$.

Deduction theorem

$\Gamma, \phi \models \psi \quad \text{iff} \quad \Gamma \models \phi \to \psi$

Consistency

The set Γ is *consistent* or *satisfiable* iff there is a model $\mathcal{M}$ and an assigment α such that $\mathcal{M}, \alpha \models \phi$ holds for all $\phi \in \Gamma$.

We say that Γ is *inconsistent* iff it is not consistent and denote this by $\Gamma \models \bot$.

Proposition

- $\{\phi, \neg\phi\} \models \bot$
- If $\Gamma \models \bot$ and $\Gamma \subseteq \Gamma'$, then $\Gamma' \models \bot$.
- $\Gamma \models \phi$ iff $\Gamma, \neg\phi \models \bot$

Substitution

- Formula ψ is a *subformula* of formula ϕ if it occurs syntactically within ϕ.
- Formula ψ is a *strict subformula* of ϕ if ψ is a subformula of ϕ and $\psi \neq \phi$

Substitution theorem

Suppose $\phi \equiv \psi$. Let θ be a formula that contains ϕ as a subformula. Let θ' be the formula obtained by safe replacing (i.e., avoiding the capture of free variables of ϕ) some occurrence of ϕ in θ with ψ. Then $\theta \equiv \theta'$.

Adquate sets of connectives for FOL

Renaming of bound variables

If y is free for x in ϕ and $y \notin \mathsf{FV}(\phi)$, then the following equivalences hold.

- $\forall x.\phi \equiv \forall y.\phi[y/x]$
- $\exists x.\phi \equiv \exists y.\phi[y/x]$

Lemma

The following equivalences hold in first-order logic.

$$\begin{array}{rclrcl}
\forall x.\phi \wedge \psi & \equiv & (\forall x.\phi) \wedge (\forall x.\psi) & \exists x.\phi \vee \psi & \equiv & (\exists x.\phi) \vee (\exists x.\psi) \\
\forall x.\phi & \equiv & (\forall x.\phi) \wedge \phi[t/x] & \exists x.\phi & \equiv & (\exists x.\phi) \vee \phi[t/x] \\
\neg\forall x.\phi & \equiv & \exists x.\neg\phi & \neg\exists x.\phi & \equiv & \forall x.\neg\phi
\end{array}$$

As in propositional logic, there is some redundancy among the connectives and quantifiers since $\forall x.\,\phi \equiv \neg\exists x.\,\neg\phi$ and $\exists x.\,\phi \equiv \neg\forall x.\,\neg\phi$.

Decidability

Given formulas ϕ and ψ as input, we may ask:

Decision problems

Validity problem:	"Is ϕ valid ?"
Satisfiability problem:	"Is ϕ satisfiable ?"
Consequence problem:	"Is ψ a consequence of ϕ ?"
Equivalence problem:	"Are ϕ and ψ equivalent ?"

These are, in some sense, variations of the same problem.

ϕ is valid	iff	$\neg\phi$ is unsatisfiable
$\phi \models \psi$	iff	$\neg(\phi \rightarrow \psi)$ is unsatisfiable
$\phi \equiv \psi$	iff	$\phi \models \psi$ and $\psi \models \phi$
ϕ is satisfiable	iff	$\neg\phi$ is not valid

Decidability

A *solution* to a decision problem is a program that takes problem instances as input and always terminates, producing a correct "yes" or "no" output.

- A decision problem is *decidable* if it has a solution.
- A decision problem is *undecidable* if it is not decidable.

Theorem (Church & Turing)

- The decision problem of validity in first-order logic is undecidable: no program exists which, given any ϕ, decides whether $\models \phi$.
- The decision problem of satisfiability in first-order logic is undecidable: no program exists which, given any ϕ, decides whether ϕ is satisfiable.

Semi-decidability

However, there is a procedure that halts and says "yes" if ϕ is valid.

A decision problem is *semi-decidable* if exists a procedure that, given an input,

- halts and answers "yes" iff "yes" is the correct answer,
- halts and answers "no" if "no" is the correct answer, or
- does not halt if "no" is the correct answer

Unlike a decidable problem, the procedure is only guaranteed to halt if the correct answer is "yes".

The decision problem of validity in first-order logic is semi-decidable.

Normal forms

A first-order formula is in *negation normal form (NNF)* if the implication connective is not used in it, and negation is only applied to atomic formulas.

If x does not occur free in ψ, then the following equivalences hold.

$$
\begin{array}{ll}
(\forall x.\phi) \wedge \psi \equiv \forall x.\phi \wedge \psi & \psi \wedge (\forall x.\phi) \equiv \forall x.\psi \wedge \phi \\
(\forall x.\phi) \vee \psi \equiv \forall x.\phi \vee \psi & \psi \vee (\forall x.\phi) \equiv \forall x.\psi \vee \phi \\
(\exists x.\phi) \wedge \psi \equiv \exists x.\phi \wedge \psi & \psi \wedge (\exists x.\phi) \equiv \exists x.\psi \wedge \phi \\
(\exists x.\phi) \vee \psi \equiv \exists x.\phi \vee \psi & \psi \vee (\exists x.\phi) \equiv \exists x.\psi \vee \phi
\end{array}
$$

The applicability of these equivalences can always be assured by appropriate renaming of bound variables.

Normal forms

A formula is in *prenex form* if it is of the form $Q_1x_1.Q_2x_2.\dots Q_nx_n.\psi$ where each Q_i is a quantifier (either $\forall$ or $\exists$) and ψ is a quantifier-free formula.

Prenex form of $\forall x.(\forall y.P(x,y) \vee Q(x)) \to \exists z.P(x,z)$

First we compute the NNF and then we go for the prenex form.

$$
\begin{array}{lll}
 & \forall x.(\forall y.P(x,y) \vee Q(x)) \to \exists z.P(x,z) & \equiv \\
 & \forall x.\neg(\forall y.P(x,y) \vee Q(x)) \vee \exists z.P(x,z) & \equiv \\
\text{(NNF)} & \forall x.\exists y.(\neg P(x,y) \wedge \neg Q(x)) \vee \exists z.P(x,z) & \equiv \\
\text{(prenex)} & \forall x.\exists y.\exists z.(\neg P(x,y) \wedge \neg Q(x)) \vee P(x,z) &
\end{array}
$$

Herbrand/Skolem normal forms

Let ϕ be a first-order formula in prenex normal form.

- The *Herbrandization* of ϕ (written ϕ^H) is an existential formula obtained from ϕ by repeatedly and exhaustively applying the following transformation:

$$\exists x_1,\ldots,x_n.\forall y.\psi \;\rightsquigarrow\; \exists x_1,\ldots,x_n.\psi[f(x_1,\ldots,x_n)/y]$$

  with f a fresh function symbol with arity n (i.e. f does not occur in ψ).

- The *Skolemization* of ϕ (written ϕ^S) is a universal formula obtained from ϕ by repeatedly applying the transformation:

$$\forall x_1,\ldots,x_n.\exists y.\psi \;\rightsquigarrow\; \forall x_1,\ldots,x_n.\psi[f(x_1,\ldots,x_n)/y]$$

  with f a fresh function symbol with arity n.

- *Herbrand normal form* (resp. *Skolem normal form*) formulas are those obtained by the process of Herbrandization (resp. Skolemization).

Herbrandization/Skolemization

A formula ϕ and its Herbrandization/Skolemization are not logically equivalent.

Proposition

Let ϕ be a first-order formula in prenex normal form.

- ϕ is valid iff its Herbrandization ϕ^H is valid.
- ϕ is satisfiable iff its Skolemization ϕ^S is satisfiable.

Herbrandization/Skolemization change the underlying vocabulary. These additional symbols are called *Herbrand/Skolem functions*.

FOL with equality

There are different conventions for dealing with equality in first-order logic.

- We have follow the approach of considering equality predicate ($=$) as a non-logical symbol, treated in the same way as any other predicate. We are working with what are usually known as *"first-order languages without equality"*.
- An alternative approach, usually called *"first-order logic with equality"*, considers equality as a logical symbol with a fixed interpretation.

  In this approach the equality symbol ($=$) is interpreted as the equality relation in the domain of interpretation. So we have, for a structure $\mathcal{M} = (D, I)$ and an assignment $\alpha : \mathcal{X} \to D$, that

$$\mathcal{M}, \alpha \models t_1 = t_2 \quad \text{iff} \quad \alpha_{\mathcal{M}}(t_1) \text{ and } \alpha_{\mathcal{M}}(t_2) \text{ are the same element of } D$$

FOL with equality

To understand the significant difference between having equality with the status of any other predicate, or with a fixed interpretation as in first-order logic with equality, consider the formulas

- $\exists x_1, x_2.\forall y.\; y = x_1 \vee y = x_2$

  With a fixed interpretation of equality, the validity of this formula implies that the cardinality of the interpretation domain is at most two – the quantifiers can actually be used to fix the cardinality of the domain, which is not otherwise possible in first-order logic.

- $\exists x_1, x_2.\neg(x_1 = x_2)$

  The validity of this formula implies that there exist at least two distinct elements in the domain, thus its cardinality must be at least two.

Many-sorted FOL

- A natural variant of first-order logic that can be considered is the one that results from allowing different domains of elements to coexist in the framework. This allows distinct "sorts" or types of objects to be distinguished at the syntactical level, constraining how operations and predicates interact with these different sorts.
- Having full support for different sorts of objects in the language allows for cleaner and more natural encodings of whatever we are interested in modeling and reasoning about.
- By adding to the formalism of FOL the notion of sort, we can obtain a flexible and convenient logic called *many-sorted first-order logic*, which has the same properties as FOL.

Many-sorted FOL

- A many-sorted vocabulary (signature) is composed of a set of sorts, a set of function symbols, and a set of predicate symbols.
  - Each function symbol f has associated with a type of the form $S_1 \times \ldots \times S_{\mathsf{ar}(f)} \to S$ where $S_1, \ldots, S_{\mathsf{ar}(f)}, S$ are sorts.
  - Each predicate symbol P has associated with it a type of the form $S_1 \times \ldots \times S_{\mathsf{ar}(P)}$.
  - Each variable is associated with a sort.
- The formation of terms and formulas is done only accordingly to the typing policy, i.e., respecting the "sorts".
- The domain of discourse of any structure of a many-sorted vocabulary is fragmented into different subsets, one for every sort.
- The notions of assignment and structure for a many-sorted vocabulary, and the interpretation of terms and formulas are defined in the expected way.

SMT solvers

- When judging the validity/satisfiability of first-order formulas we are typically interested in a particular domain of discourse, which in addition to a specific underlying vocabulary includes also properties that one expects to hold. We work with respect to some *background theory*.
- The *Satisfiability Modulo Theories (SMT) problem* is a variation of the SAT problem for first-order logic, with the interpretation of symbols constrained by (a combination of) specific theories.
- SMT solvers are tools that aim to answer the SMT problem.
  - The underlying logic of SMT solvers is many-sorted first-order logic with equality.
  - SMT solvers are the core engine of many tools for analyzing and verifying software, planning, etc.
- We will see more about this topic later.

Modeling with FOL

Modeling with FOL

- Being able to express an idea in FOL is an <u>essential skill</u> for Formal Methods in Software Engineering.
- We will see some examples. In particular, we will formalize in FOL systems decribed by domain models.
- The underlying logic is first-order logic with equality (without sorts).

Modeling with FOL

Use the predicates

$\mathsf{admires}(x, y)$:	x admires y	$\mathsf{Professor}(x)$:	x is a professor
$\mathsf{attended}(x, y)$:	x attended y	$\mathsf{Student}(x)$:	x is a student
		$\mathsf{Lecture}(x)$:	x is a lecture

and the constant Mary to translate the following into predicate logic:

- *Mary admires every professor.*

  $$\forall x.\, \mathsf{Professor}(x) \to \mathsf{admires}(\mathsf{Mary}, x)$$

- *Some professor admires Mary.*

  $$\exists x.\, \mathsf{Professor}(x) \land \mathsf{admires}(x, \mathsf{Mary})$$

- *Mary admires herself.*

  $$\mathsf{admires}(\mathsf{Mary}, \mathsf{Mary})$$

Modeling with FOL

Use the predicates

$\mathsf{admires}(x, y)$:	x admires y	$\mathsf{Professor}(x)$:	x is a professor
$\mathsf{attended}(x, y)$:	x attended y	$\mathsf{Student}(x)$:	x is a student
		$\mathsf{Lecture}(x)$:	x is a lecture

and the constant Mary to translate the following into predicate logic:

- *No student attended every lecture.*

  $$\neg(\exists x.\, \mathsf{Student}(x) \land (\forall y.\, \mathsf{Lecture}(y) \to \mathsf{attended}(x, y)))$$

- *No lecture was attended by every student.*

  $$\neg(\exists x.\, \mathsf{Lecture}(x) \land (\forall y.\, \mathsf{Student}(y) \to \mathsf{attended}(y, x)))$$

- *No lecture was attended by any student.*

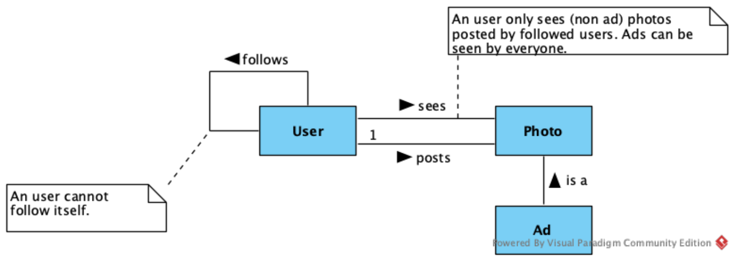
  $$\neg(\exists l.\, \mathsf{Lecture}(l) \land \forall s.\, \mathsf{Student}(s) \to \neg \mathsf{attended}(s, l))$$

  or equivalently

  $$\forall l.\, \mathsf{Lecture}(l) \to \exists s.\, \mathsf{Student}(s) \land \mathsf{attended}(s, l)$$

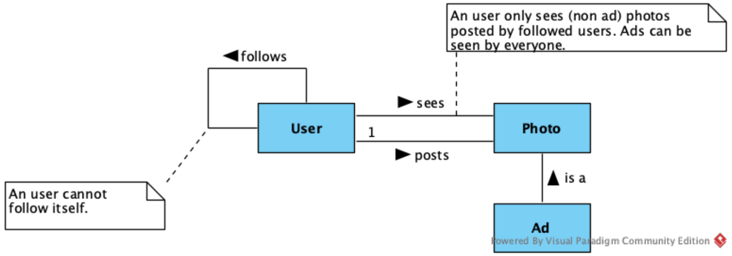
Domain models

- A **domain model** is a conceptual model of a system that describes the various entities involved in that system and their relationships.



- It is used in software development as a first step to realize a new domain and resolve ambiguities in requirements.
- A domain model is a selective and structured representation of domain knowledge relevant to a given software development project.

Domain models



A domain model is a diagram where

- entities are represented by boxes and
- relationships between entities by arcs annotated with
  - the name of the relationship/association,
  - the reading direction (indicated by an arrow) and
  - its multiplicity (annotated at the tip of the arcs).
- annotations with restrictions that are informally indicated in boxes may also appear in the diagram.

Domain models

- There is no standard notation for domain models.
- We are going to use the notation used in the *Desenvolvimento de Sistemas de Software* course. So, we assume that:
  - all entities present in a diagram are disjoint, unless between two entities there is a relation/association *"is a"* which denotes a specialization/extension;
  - if there are multiple specializations for the same entity, those specializations are disjoint;
  - the relation/association *"is a"* may be a subset or a membership relation. If it is a membership relation, the entity that "belongs to" another will be modeled as a constant.

Formalizing a domain model

We start by establish the logical language that we are going to use, i.e., the vocabulary of the language.

- a unary predicate for each entity (these predicates will act as the "type" of the entity, in a domain that is untyped);
- a predicate for each association, except specializations (which will be codified by formulas that establish the kind of specialization);
- a constant for each entity belonging to an "enumerated type".

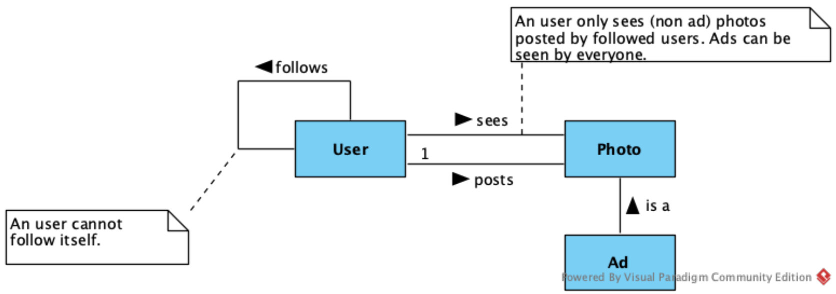
Formalizing a domain model

Next we write the set of formulas that describe the system. These formulas are of a different nature:

- codification of specialization relationships (which may be subset or membership relations, depending on the case);
- partitioning the universe of discourse with the types of the entities;
- disjunction of specialization entities;
- typing associations;
- multiplicity restrictions on associations;
- restrictions annotated informally.

Example: Instagram (simplified)

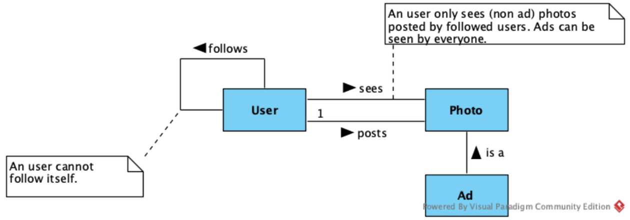
A simplified domain model for *Instagram*:



Predicates:

User(-)   Photo(-)   Ad(-)
sees(-,-)   posts(-,-)   follows(-,-)

Example: Instagram (simplified)



- Codification of specialization relationships (in this case, a subset relation).

  $\forall x.\, \mathsf{Ad}(x) \to \mathsf{Photo}(x)$

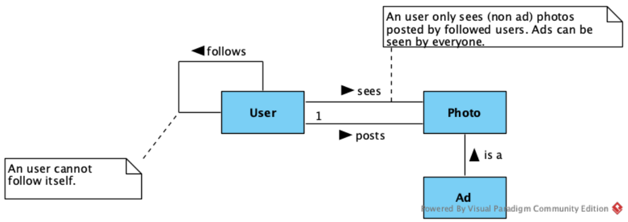
- Partitioning the universe of discourse with the types of the entities.

  $\forall x.\, \mathsf{User}(x) \leftrightarrow \neg \mathsf{Photo}(x)$

  Alternative: any element of the universe

  - at most is of one these "types" $\forall x.\, \mathsf{User}(x) \to \neg \mathsf{Photo}(x)$
  - must be of one of these "types" $\forall x.\, \mathsf{User}(x) \lor \mathsf{Photo}(x)$

Example: Instagram (simplified)



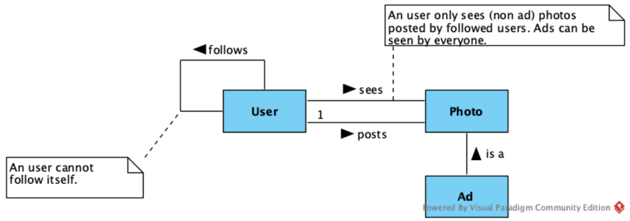
- Disjunction of specialization entities.

  (there is nothing to add)

- Typing associations.

$$\forall x, y.\, \mathsf{follows}(x, y) \to \mathsf{User}(x) \land \mathsf{User}(y)$$
$$\forall x, y.\, \mathsf{sees}(x, y) \to \mathsf{User}(x) \land \mathsf{Photo}(y)$$
$$\forall x, y.\, \mathsf{posts}(x, y) \to \mathsf{User}(x) \land \mathsf{Photo}(y)$$

Example: Instagram (simplified)



- Multiplicity restrictions on associations.

$$(\forall y.\, \mathsf{Photo}(y) \to \exists x.\, \mathsf{posts}(x, y)) \land (\forall x, y, z.\, \mathsf{posts}(x, z) \land \mathsf{posts}(y, z) \to x = y)$$

That is:

- every photo has to be posted by some user

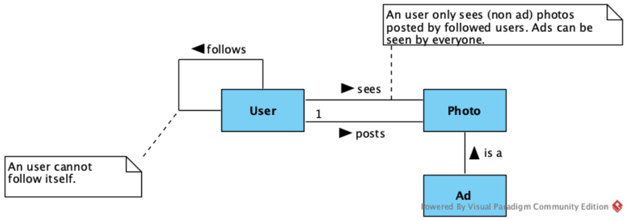
  $\forall y.\, \mathsf{Photo}(y) \to \exists x.\, \mathsf{posts}(x, y)$

- every photo is posted by no more than one user

  $\forall x, y, z.\, \mathsf{posts}(x, z) \land \mathsf{posts}(y, z) \to x = y$

Therefore, every photo é posted by a single user.

Example: Instagram (simplified)



- Restrictions annotated informally.
  - *An user cannot follow itself.*

    $\forall x.\, \neg \mathsf{follows}(x, x)$
  - *An user only sees (non ad) photos posted by followed users. Ads can be seen by everyone.*

    $\forall x, y.\, \mathsf{sees}(x, y) \rightarrow (\mathsf{Ad}(y) \vee (\forall z. \mathsf{posts}(z, y) \rightarrow \mathsf{follows}(x, z)))$