Lecture 2 — First-Order Logic

Ondřej Lengál

Faculty of Information Technology
Brno University of Technology

IAM’19

First-Order Logic

First-Order Logic (FOL)

- also called (first-order) predicate logic, predicate calculus, ...
- generalizes propositional logic by
  - interpreting ("looking inside") propositions
  - talks about elements of a universe—denoted by terms formed from variables, constants, and functions
    - e.g., x, 5, $f(x, 2)$, $+(40, 2)$ [$= 40 + 2$], $\mathit{fatherOf}(\mathit{motherOf}(x))$, $\mathit{head}(\texttt{"abc"})$, $\sin(y)$, ...
  - propositions are substituted with predicates over terms
    - e.g., $x = y$, $\mathit{even}(x)$, $p(x, y, z)$, $\mathit{isFatherOf}(x, y)$, ...
  - introducing quantifiers to express existential or universal properties about elements of the universe (first-order quantification)
    - $\forall$, $\exists$
- much more expressive than propositional logic!
  - therefore, also more complex (in general undecidable)

First-Order Logic — Examples

What is expressible in FOL? (informal examples)

SPOILER ALERT!

- "All men are mortal. Socrates is a man. Therefore Socrates is mortal."

$$\models \big((\forall x.\ man(x) \rightarrow mortal(x)) \wedge man(Socrates)\big) \rightarrow mortal(Socrates)$$

- "All men are mortal. Elvis is immortal. Therefore Elvis is not a man."

$$\models \big((\forall x.\ man(x) \rightarrow mortal(x)) \wedge \neg mortal(Elvis)\big) \rightarrow \neg man(Elvis)$$

First-Order Logic — Examples

- "Luke is a Jedi.":

$$\models isJedi(Luke)$$

- "Anakin is the father of Luke.":

$$\models isFatherOf(Anakin, Luke) \quad \text{or}$$
$$\models Anakin = fatherOf(Luke)$$

- also means "Luke is a son of Anakin."

- "Gandalf is not the father of Luke.":

$$\models \neg isFatherOf(Gandalf, Luke) \quad \text{or}$$
$$\models \neg(Gandalf = fatherOf(Luke))$$
$$(\Leftrightarrow \models Gandalf \neq fatherOf(Luke))$$

First-Order Logic — Examples

- "Anakin is the father of Luke and Leia.":

$$\models \mathit{isFatherOf}(\mathit{Anakin}, \mathit{Luke}) \wedge \mathit{isFatherOf}(\mathit{Anakin}, \mathit{Leia})$$

- "Luke has a father.":

$$\models \exists x \,.\, \mathit{isFatherOf}(x, \mathit{Luke})$$

- "Luke has a father and Leia also has a father.":

$$\models (\exists x \,.\, \mathit{isFatherOf}(x, \mathit{Luke})) \wedge (\exists y \,.\, \mathit{isFatherOf}(y, \mathit{Leia}))$$

- "Luke and Leia have the same father!":

$$\models \exists x \,.\, \mathit{isFatherOf}(x, \mathit{Luke}) \wedge \mathit{isFatherOf}(x, \mathit{Leia})$$

First-Order Logic — Examples

- "There is a person who does not have a father.":

$$\models \exists x \, \neg \exists y. \, \mathit{isFatherOf}(y, x)$$
$$\big(\Leftrightarrow \; \models \exists x \forall y. \, \neg \mathit{isFatherOf}(y, x) \big)$$

- "All children of a Jedi are Jedis.":

$$\forall x, y. \, \big(\mathit{isJedi}(y) \wedge (\mathit{isFatherOf}(y, x) \vee \mathit{isMotherOf}(y, x))\big) \rightarrow \mathit{isJedi}(x)$$

First-Order Logic — Examples

- There are infinitely many primes [Euclid, c. 300 BC]

$$\forall x \exists y.\ y > x \land \big(\forall z.\ (1 < z \land z < y) \rightarrow y \bmod z \neq 0\big)$$

- Last Fermat's Theorem [Fermat, 1637] (proven in [Wiles, 1994])

$$\forall n, x, y \in \mathbb{N}.\ n > 2 \quad \rightarrow \quad (\neg \exists z \in \mathbb{N}.\ x^n + y^n = z^n)$$

- Goldbach Conjecture [Goldbach, 1742] (open as of 2017)

$$\forall x.\ (x > 2 \land even(x)) \rightarrow (\exists y, z\ .\ prime(y) \land prime(z) \land x = y + z)$$

- Weak Goldbach Conjecture (proven in [Helfgott, 2013])

$$\forall x.\ (x > 5 \land odd(x)) \rightarrow$$
$$(\exists y, z, w.\ prime(y) \land prime(z) \land prime(w) \land x = y + z + w)$$

First-Order Logic — Examples

What is **NOT** expressible with FOL:

- "Elendil is an ancestor of Aragorn." (using $\mathit{isParentOf}$)
  Attempts:
  - $\exists x_1, \ldots, x_n \,.\, \mathit{isParentOf}(x_1, \mathit{Aragorn}) \wedge \ldots \wedge \mathit{isParentOf}(\mathit{Elendil}, x_n)$
    [n is bounded]
  - $\exists_2^{\text{fin}} X \,.\, \mathit{Aragorn} \in X \wedge \mathit{Elendil} \in X \wedge \big(\forall y \in X.$
    $(\exists z \,.\, \mathit{isFatherOf}(z, y) \wedge z \in X) \vee y = \mathit{Elendil}\big)$
    [$\exists_2^{\text{fin}}$ — second-order finite quantification, cf. MSO]
  - $\mathit{isAncestorOf}(x, y) \overset{\text{def}}{\Leftrightarrow} \mathit{isParentOf}(x, y) \vee$
    $\big(\exists z \,.\, \mathit{isAncestorOf}(x, z) \wedge \mathit{isParentOf}(z, y)\big)$
    [recursive predicate, cf. PROLOG]

- "Anakin is more likely than Gandalf the father of Luke."
  Attempts:
  - ?!$#dk*#R&Q

Syntax

Syntax:

- **Alphabet**:
  - logical connectives: $\neg, \land, \lor, \rightarrow, \leftrightarrow, (\cdots)$ (from PL)
  - variables: $x, y, \ldots, x_1, x_2, \ldots$ (hold elements of a universe)
  - quantifiers: $\forall, \exists$
  - function symbols (with $/arity$): $f/2$, $(+)/2$, $\sin/1$, $fatherOf/1$, $\pi/0$, $42/0$, $(+1)/1$, ...
    - nullary functions (arity 0): constants
    - to be used as, e.g., $f(a, 3)$, $+(40, 2)$, $\sin(+1(x))$, $fatherOf(Luke)$, $\pi()$
    - we often simplify the notation: $+(40, 2) \mapsto 40 + 2$, $\pi() \mapsto \pi$, $+1(x) \mapsto x + 1, \ldots$
  - predicate symbols (with $/arity$): $p/3$, $=/2$, $isFatherOf/2$, $(= 0)/1$, $isJedi/1$, $</2$, ...
    - to be used as, e.g., $p(a, x, 9)$, $= (x, 42)$, $isFatherOf(Anakin, Luke)$, $(= 0)(x)$, $isJedi(Anakin)$, $< (x, \pi)$
    - we often simplify the notation: $= (x, 42) \mapsto x = 42$, $(= 0)(x) \mapsto x = 0$, $< (x, \pi) \mapsto x < \pi, \ldots$
- Signature = function symbols + predicate symbols
  - can be seen as a parameter of an instance of FOL
  - sometimes called vocabulary or language of FOL

Syntax

Syntax:

- **Grammar**:
  - term: $t ::= x$ — occurrence of a variable $x \in \mathbb{X}$
    $\mid f(t_1, \ldots, t_n)$ — where f/n is a function symbol
  - formula:

$$\varphi ::= p(t_1, \ldots, t_n) \quad \text{where } p/n \text{ is a predicate symbol}$$
$$\mid \bot \mid \top \mid \neg\varphi \mid \varphi_1 \wedge \varphi_2 \mid \varphi_1 \vee \varphi_2 \mid \varphi_1 \rightarrow \varphi_2 \mid \varphi_1 \leftrightarrow \varphi_2 \quad \text{PL}$$
$$\mid \exists x.\ \varphi \quad \text{exists, existential quantification}$$
$$\mid \forall x.\ \varphi \quad \text{for all, universal quantification}$$

Example

$$\forall x.\ p(x, f(3)) \rightarrow \exists y.\ q(y, f(f(f(z))))$$

- Precedence
  - PL connectives: as for PL
  - quantifiers: lowest—the scope of a quantifier extends to the right

Syntax — Variables

Variables in formulae:

- **bound**: occur in the scope of a quantifier
  - e.g. $bound(\exists x.\ x = 4 \wedge \neg(y = 5)) = \{x\}$
- **free**: there is an occurrence not bound by any quantifier
  - e.g. $free(x = 4 \wedge (\exists y.\ y = 5)) = \{x\}$
- a variable can occur both bound and free in a formula

Example

$$\forall x.\ p(f(x), y) \rightarrow \forall y.\ p(f(x), y)$$

- x only occurs bound
- y occurs both free (antecedent) and bound (consequent)

- we often write $\varphi(x_1, \ldots, x_n)$ when $free(\varphi) \subseteq \{x_1, \ldots, x_n\}$
  - $x_1, \ldots, x_n$ serve as the "interface" of φ
- φ is ground (or closed) if $free(\varphi) = \emptyset$

Semantics

Semantics of FOL:

- so far, the symbols *did not have any meaning*!
- more complicated than for PL

Interpretation $I = (D_I, \alpha_I)$: provides the *meaning* to the symbols

- domain (universe) of discourse D_I: a non-empty set of elements
  - e.g., $\mathbb{N}$, $\{0, 1, 2, 3, 4\}$, $\mathbb{R}^3$, $People$, $List[\mathbb{N}]$, Σ^*, ...
- assignment α_I:
  - for every function symbol f/n, a function $f_I : \overbrace{D_I \times \ldots \times D_I}^{n} \to D_I$
    - e.g., $(+) = \{(0,0) \mapsto 0, (0,1) \mapsto 1, (1,0) \mapsto 1, (1,1) \mapsto 2, \ldots\}$
    - e.g., $fatherOf = \{Luke \mapsto Anakin, KyloRen \mapsto HanSolo, \ldots\}$
    - for constants, this gives us one value, e.g., $\pi = \{() \mapsto 3.1415926\ldots\}$
  - for every predicate symbol p/n, a relation $p_I \subseteq \overbrace{D_I \times \ldots \times D_I}^{n}$
    - e.g., $isJedi = \{Luke, Anakin, Yoda, ObiWan, \ldots\}$
    - e.g., $(<) = \{(0,1), (0,2), (1,2), \ldots\}$
    - e.g., $(=0) = \{0\}$
    - e.g., $isFatherOf = \{(Anakin, Luke), (HanSolo, KyloRen), \ldots\}$
  - for every variable $x \in \mathbb{X}$ a value from D_I, e.g., $\{x \mapsto 42, y \mapsto 0\}$

Semantics

Truth value: inductive definition:

- base cases: $I \models \top, \quad I \not\models \bot$

  Evaluate nested terms recursively

  $$\alpha_I[f(t_1, \dots, t_n)] \stackrel{\text{def}}{=} \alpha_I[f](\alpha_I[t_1], \dots, \alpha_I[t_n])$$

  Then: $\quad I \models p(t_1, \dots, t_n)$ iff $\alpha_I[p](\alpha_I[t_1], \dots, \alpha_I[t_n])$

- logical connectives (same as for PL):

  $I \models \neg\psi$ iff $I \not\models \psi$

  $I \models \psi_1 \wedge \psi_2$ iff $I \models \psi_1$ and $I \models \psi_2$

  $I \models \psi_1 \vee \psi_2$ iff $I \models \psi_1$ or $I \models \psi_2$

  $I \models \psi_1 \rightarrow \psi_2$ iff, if $I \models \psi_1$ then $I \models \psi_2$

  $I \models \psi_1 \leftrightarrow \psi_2$ iff $I \models \psi_1$ and $I \models \psi_2$, or $I \not\models \psi_1$ and $I \not\models \psi_2$

- quantifiers: let $I \triangleleft \{x \mapsto v\}$ denote an interpretation obtained from I by substituting $x \mapsto ?$ by $x \mapsto v$ in α_I ($I \triangleleft \{x \mapsto v\}$ is a variant)

  $I \models \forall x.\, \varphi$ iff for all $v \in D_I$ we have $I \triangleleft \{x \mapsto v\} \models \varphi$

  $I \models \exists x.\, \varphi$ iff there exists $v \in D_I$ such that $I \triangleleft \{x \mapsto v\} \models \varphi$

- Question: we no more have Boolean variables! Is that a problem?

Semantics — Examples

Consider the signature $(\{(+)/2\}, \{(=)/2\})$

- Addition in $\mathbb{N}$: $I = (\mathbb{N}, \alpha_I)$ where
  - $\alpha_I(+) = (+_\mathbb{N})$
  - $\alpha_I(=) = \{(n, n) \mid n \in \mathbb{N}\}$
  - $(=)$ is often considered an "inbuilt" predicate of FOL (regardless of the signature) with the standard meaning (identity)
- Addition in $\mathbb{R}^3$: $I = (\mathbb{R}^3, \alpha_I)$ where
  - $\alpha_I(+) = \{((x_1, y_1, z_1), (x_2, y_2, z_2)) \mapsto (x_1 + x_2, y_1 + y_2, z_1 + z_2)\}$
- Disjunction in Boolean algebra: $I = (\{0, 1\}, \alpha_I)$
  - $\alpha_I(+) = \vee$
- *Least common male-ancestor:* $I = (People, \alpha_I)$ where
  - $\alpha_I(+) = \{(a, b) \mapsto c \mid isFatherOf^*(c, a) \wedge isFatherOf^*(c, b) \wedge \forall z.\ (isFatherOf^*(z, a) \wedge isFatherOf^*(z, b)) \rightarrow isFatherOf^*(z, c)\}$
  - e.g., $Aragorn + Arwen = E\ddot{a}rendil$
- Modular addition in $\{0, 1, 2, 3\}$: $I = (\{0, 1, 2, 3\}, \alpha_I)$ where
  - $\alpha_I(+) = \{(x, y) \mapsto x + y \mod 4\}$

Satisfiability and Validity

- similar as for PL
  - satisfiability: is there an interpretation I such that $I \models \varphi$?
  - (logical) validity: does it for all interpretations I hold that $I \models \varphi$?
- technically, only applies to *ground* formulae; convention:
  - satisfiability of $\varphi \rightsquigarrow$ satisfiability of $\exists \mathit{free}(\varphi).\ \varphi$ (existential closure)
  - validity of $\varphi \rightsquigarrow$ validity of $\forall \mathit{free}(\varphi).\ \varphi$ (universal closure)
- **Important**:
  - note that an interpretation now also talks about the meaning of function and predicate symbols
  - therefore, a formula is valid (resp. satisfiable) in FOL *if it holds for all interpretations of function and predicate symbols*
  - later, we will introduce $\mathcal{T}$-validity and $\mathcal{T}$-satisfiability
  - $\mathcal{T}$ is a theory (provides axioms)
  - then, the interpretations of φ need to satisfy those

Semantic Argument for FOL

To decide validity of FOL formulae, we extend the semantic argument method from PL using the following proof rules:

- universal quantification 1: $$\frac{I \models \forall x.\ \varphi}{I \triangleleft \{x \mapsto v\} \models \varphi}$$ for any v
- existential quantification 1: $$\frac{I \not\models \exists x.\ \varphi}{I \triangleleft \{x \mapsto v\} \not\models \varphi}$$ for any v

  In practice, we often choose v that was already introduced earlier.

- universal quantification 2: $$\frac{I \not\models \forall x.\ \varphi}{I \triangleleft \{x \mapsto v\} \not\models \varphi}$$ for a *fresh* v
- existential quantification 2: $$\frac{I \models \exists x.\ \varphi}{I \triangleleft \{x \mapsto v\} \models \varphi}$$ for a *fresh* v

  The value v cannot have been used in the proof before.

The values v are not interpreted; they are **symbolic names**.

Semantic Argument for FOL

- contradiction:

$$\frac{\begin{array}{c} J : I \triangleleft \cdots \models p(s_1, \ldots, s_n) \\ K : I \triangleleft \cdots \not\models p(t_1, \ldots, t_n) \end{array}}{I \models \bot} \qquad \text{for } 1 \leq i \leq n : \alpha_J[s_i] = \alpha_K[t_i]$$

Substitution

Substitution

- again, more involved than for PL (because of quantifiers)
- **Renaming**: Let $\varphi = \forall x.\ \psi(x)$. The renaming of x to a fresh variable x' in φ is the formula $\varphi[x/x'] = \forall x'.\ \psi(x')$.
- **Substitution**: mapping from formulae to formulae

$$\sigma : \{F_1 \mapsto G_1, \ldots, F_n \mapsto G_n\}$$

- **Safe substitution**: $F\sigma$
  - for each quantified variable x in F that also occurs free in σ, rename x to a fresh variable x' to produce F'
    - the reason is to avoid binding previously free variables
  - compute $F'\sigma$

Proposition (Substitution of Equivalent Formulae)

If, given σ, for each i it holds that $F_i \Leftrightarrow G_i$, then $F \Leftrightarrow F\sigma$ where $F\sigma$ is computed as a safe substitution.

Useful Equivalences

$$
\begin{array}{rcll}
\forall x.\ \neg\varphi & \Leftrightarrow & \neg\exists x.\ \varphi & \\
\exists x.\ \neg\varphi & \Leftrightarrow & \neg\forall x.\ \varphi & \\
(\forall x.\ \varphi(x)) \wedge (\forall y.\ \psi(y)) & \Leftrightarrow & \forall x.\ \varphi(x) \wedge \psi(x) & \text{if } x \notin \mathit{free}(\psi) \\
(\exists x.\ \varphi(x)) \vee (\exists y.\ \psi(y)) & \Leftrightarrow & \exists x.\ \varphi(x) \vee \psi(x) & \text{if } x \notin \mathit{free}(\psi) \\
\forall x.\ \varphi & \Leftrightarrow & \varphi & \text{if } x \notin \mathit{free}(\varphi) \\
\exists x.\ \varphi & \Leftrightarrow & \varphi & \text{if } x \notin \mathit{free}(\varphi) \\
\forall x.\ \varphi \vee \psi & \Leftrightarrow & (\forall x.\ \varphi) \vee \psi & \text{if } x \notin \mathit{free}(\psi) \\
\exists x.\ \varphi \wedge \psi & \Leftrightarrow & (\exists x.\ \varphi) \wedge \psi & \text{if } x \notin \mathit{free}(\psi)
\end{array}
$$

Normal Forms (NNF)

Negation Normal Form (NNF):

- similar as for PL
- contains only $\wedge$, $\vee$, $\neg$, $\exists$, and $\forall$ as connectives
- $\neg$ appears only in front of predicates

Example

Let

$$F : \neg \exists n, x, y.\ n > 2 \quad \wedge \quad \exists z.\ x^n + y^n = z^n.$$

The formula

$$G : \forall n, x, y\ .\ \neg(n > 2) \quad \vee \quad \forall z\ .\ \neg(x^n + y^n = z^n)$$

is equivalent to F and is in NNF.

Normal Forms (PNF)

Prenex Normal Form (PNF):

- formula is of the form

$$\varphi = \underbrace{Q_1 x_1 \; . \; \ldots Q_n x_n}_{\text{prefix}} \; . \; \underbrace{\psi(x_1, \ldots, x_n, y_1, \ldots, y_m)}_{\text{matrix}}$$

  where $Q_i \in \{\forall, \exists\}$ and ψ is quantifier-free; $\{y_1, \ldots, y_m\}$ are the free variables of φ

Example

Let

$$G : \forall n, x, y \; . \; \neg(n > 2) \quad \vee \quad \forall z \; . \; \neg(x^n + y^n = z^n).$$

The formula

$$H : \forall n, x, y, z \; . \; \neg(n > 2) \quad \vee \quad \neg(x^n + y^n = z^n)$$

is equivalent to G and is in PNF.

Normal Forms (DNF, CNF)

- disjunctive normal form (DNF): PNF where matrix is in DNF
- conjuctive normal form (CNF): PNF where matrix is in CNF

Soundness and Completeness

Soundness

- a proof method is **sound** if it never proves a wrong formula:

$$\vdash \varphi \quad \Rightarrow \quad \models \varphi$$

$\vdash \varphi$: φ is provable

Theorem

The semantic argument is sound.

Completeness

- a proof method is **complete** if it can prove every valid formula:

$$\models \varphi \quad \Rightarrow \quad \vdash \varphi$$

Theorem

The semantic argument is complete.

There are also other sound and complete methods for FOL (e.g. natural deduction, Hilbert system).

Craig Interpolation Lemma

Theorem (Craig Interpolation Lemma (Craig, 1957))

If $\models \varphi \to \psi$*, then there exists a formula* χ *such that* $\models \varphi \to \chi$ *and* $\models \chi \to \psi$ *and whose predicates and free variables occur in both* φ *and* ψ*.*

Notes

- Exists exactly one:

$$\exists! x.\ \varphi(x) \quad \Leftrightarrow \quad \exists x.\ \varphi(x) \wedge \forall y.\ \varphi(y) \rightarrow x = y$$

  where y is not free in φ

- many-sorted logics:
  - capture the natural requirement to distinguish **types** of variables
  - e.g. in

$$\forall w \in \Sigma^* \ .\ \mathit{safe}(w) \rightarrow \#_{'('}(w) = \#_{')'}(w)$$

References

[A.R. Bradley and Z. Manna. The Calculus of Computation.]