# Lab 3 — First-Order Theories

Ondřej Lengál

Faculty of Information Technology
Brno University of Technology

IAM'19

# Transformation to PNF

- 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 $\psi$ is QF; $\{y_1, \ldots, y_m\}$ are the free vars of $\varphi$

Transformation to PNF:

1. remove useless quantifiers
2. substitute $\leftrightarrow$ with equivalent formulae: $\varphi \leftrightarrow \psi \Leftrightarrow (\varphi \rightarrow \psi) \wedge (\psi \rightarrow \varphi)$
3. rename variables (we need to avoid binding previously free variables when moving quantifiers to the left)
4. move negation inside
5. move quantifiers to the left

# Equivalences for FOL

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

# (proof rules)

- negation:

$$\frac{I \models \neg\varphi}{I \not\models \varphi} \qquad \frac{I \not\models \neg\varphi}{I \models \varphi}$$

- conjunction:

$$\frac{I \models \varphi \wedge \psi}{\begin{array}{c} I \models \varphi \\ I \models \psi \end{array}} \qquad \frac{I \not\models \varphi \wedge \psi}{I \not\models \varphi \quad \mid \quad I \not\models \psi}$$

('|' forks computation in two branches that both need to be proved)

- disjunction:

$$\frac{I \models \varphi \vee \psi}{I \models \varphi \quad \mid \quad I \models \psi} \qquad \frac{I \not\models \varphi \vee \psi}{\begin{array}{c} I \not\models \varphi \\ I \not\models \psi \end{array}}$$

# (proof rules)

- implication:

$$\frac{I \models \varphi \to \psi}{I \not\models \varphi \quad | \quad I \models \psi} \qquad \frac{I \not\models \varphi \to \psi}{\begin{array}{c} I \models \varphi \\ I \not\models \psi \end{array}}$$

- iff:

$$\frac{I \models \varphi \leftrightarrow \psi}{I \models \varphi \land \psi \quad | \quad I \not\models \varphi \lor \psi} \qquad \frac{I \not\models \varphi \leftrightarrow \psi}{I \models \varphi \land \neg\psi \quad | \quad I \models \neg\varphi \land \psi}$$

- contradiction:

$$\frac{I \models \varphi \qquad I \not\models \varphi}{I \models \bot}$$

# 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 $v \in D_I$

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

  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* $v \in D_I$

- existential quantification 2: $$\frac{I \models \exists x \,.\, \varphi}{I \triangleleft \{x \mapsto v\} \models \varphi}$$ for a *fresh* $v \in D_I$

  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:

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

# Theory of Equality $\mathcal{T}_E$

Theory of Equality $\mathcal{T}_E$ (with Uninterpreted Functions):

- Signature: $\{=, f, g, h, \ldots, p, q, r, \ldots\}$
  - equality $(=)/2$ and all function and predicate symbols
- Axioms:
  1. $\forall x.\ x = x$ (reflexivity)
  2. $\forall x, y.\ x = y \quad \rightarrow \quad y = x$ (symmetry)
  3. $\forall x, y, z.\ x = y \wedge y = z \quad \rightarrow \quad x = z$ (transitivity)
  4. for every positive integer $n$ and $n$-ary function symbol $f$,

     $$\forall \overline{x}, \overline{y}.\ \left( \bigwedge_{i=1}^{n} x_i = y_i \right) \quad \rightarrow \quad f(\overline{x}) = f(\overline{y}) \qquad \text{(function congruence)}$$

  5. for every positive integer $n$ and $n$-ary predicate symbol $p$,

     $$\forall \overline{x}, \overline{y}.\ \left( \bigwedge_{i=1}^{n} x_i = y_i \right) \quad \rightarrow \quad (p(\overline{x}) \leftrightarrow p(\overline{y})) \qquad \text{(predicate congruence)}$$

  $\overline{x}$ denotes a list of variables $x_1, \ldots, x_n$
- Note that only the $(=)$ predicate symbol is interpreted.
- Note that [4] and [5] are *axiom schemata*.

# Peano Arithmetic $\mathcal{T}_{\mathsf{PA}}$

(first-order arithmetic):

- Signature: $\{0, S, +, \cdot, =\}$
  - $0/0$ is a constant (nullary functions)
  - $S/1$ is a unary function symbol (called *successor*)
  - $(+)/2$ and $(\cdot)/2$ are binary function symbols
  - equality $(=)/2$ is a binary predicate symbol
- Axioms:
  1. $\forall x.\ \neg(S(x) = 0)$ (zero)
  2. $\forall x, y.\ S(x) = S(y) \quad \rightarrow \quad x = y$ (successor)
  3. for every $\Sigma_{\mathcal{T}_{\mathsf{PA}}}$-formula $\varphi$ with precisely one free variable,

     $$\big(\varphi(0) \wedge (\forall x.\ \varphi(x) \rightarrow \varphi(S(x)))\big) \quad \rightarrow \quad \forall x.\ \varphi(x) \qquad \text{(induction)}$$

  4. $\forall x.\ x + 0 = x$ (plus zero)
  5. $\forall x, y.\ x + S(y) = S(x + y)$ (plus successor)
  6. $\forall x.\ x \cdot 0 = 0$ (times zero)
  7. $\forall x, y.\ x \cdot S(y) = x \cdot y + x$ (times successor)