Predikátová logika 1. řádu — shrnutí

Symboly:

- Logické symboly:
  - **proměnné**: $x \in Var$, kde $Var = \{x_0, x_1, x_2, \ldots\}$
  - **logické spojky**: $\neg$, $\wedge$, $\vee$, $\rightarrow$, $\leftrightarrow$
  - **kvantifikátory**: $\forall$, $\exists$
  - **závorky**:), (
  - **symbol pro rovnost**: $=$
- Mimologické symboly — dány signaturou $S = (\mathcal{P}, \mathcal{F}, \mathcal{C}, \text{arity})$:
  - **predikátové symboly**: $P \in \mathcal{P}$
  - **funkční symboly**: $f \in \mathcal{F}$
  - **konstantní symboly**: $c \in \mathcal{C}$

Syntaxe:

$$
\begin{array}{rcl}
t & ::= & x \mid c \mid f(t, t, \ldots, t) \\
\varphi & ::= & P(t, t, \ldots, t) \mid t = t \mid \bot \mid \top \mid \neg\varphi \mid \varphi \wedge \varphi \mid \varphi \vee \varphi \\
& & \mid \varphi \rightarrow \varphi \mid \varphi \leftrightarrow \varphi \mid \forall x \varphi \mid \exists x \varphi
\end{array}
$$

Predikátová logika 1. řádu — shrnutí

Sémantika:

Hodnota termu při $\mathfrak{I} = (\mathfrak{A}, v)$:

- pro $x \in Var$: $\quad \mathfrak{I}(x) = v(x)$
- pro $c \in \mathcal{C}$: $\quad \mathfrak{I}(c) = c^{\mathfrak{A}}$
- pro $f \in \mathcal{F}$ (kde $\mathrm{arity}(f) = n$) a termy $t_1, t_2, \ldots, t_n$:
  $\mathfrak{I}(f(t_1, t_2, \ldots, t_n)) = f^{\mathfrak{A}}(\mathfrak{I}(t_1), \mathfrak{I}(t_2), \ldots, \mathfrak{I}(t_n))$

Predikátová logika 1. řádu — shrnutí

Pravdivost formule při $\mathfrak{I} = (\mathfrak{A}, \mathfrak{a})$:

- Pro $P \in \mathcal{P}$, kde $\mathrm{arity}(P) = n$, a pro termy $t_1, t_2, \ldots, t_n$ platí $\mathfrak{I} \models P(t_1, t_2, \ldots, t_n)$ právě tehdy, když $(\mathfrak{I}(t_1), \mathfrak{I}(t_2), \ldots, \mathfrak{I}(t_n)) \in P^{\mathfrak{A}}$
- Pro termy t_1, t_2 platí $\mathfrak{I} \models t_1 = t_2$ právě tehdy, když $\mathfrak{I}(t_1) = \mathfrak{I}(t_2)$
- $\mathfrak{I} \models \bot$ neplatí nikdy, tj. vždy platí $\mathfrak{I} \not\models \bot$
- $\mathfrak{I} \models \top$ platí vždy
- $\mathfrak{I} \models \neg\varphi$ platí právě tehdy, když $\mathfrak{I} \not\models \varphi$
- $\mathfrak{I} \models \varphi \wedge \psi$ platí právě tehdy, když $\mathfrak{I} \models \varphi$ a $\mathfrak{I} \models \psi$
- $\mathfrak{I} \models \varphi \vee \psi$ platí právě tehdy, když $\mathfrak{I} \models \varphi$ nebo $\mathfrak{I} \models \psi$
- $\mathfrak{I} \models \varphi \rightarrow \psi$ platí právě tehdy, když $\mathfrak{I} \not\models \varphi$ nebo $\mathfrak{I} \models \psi$
- $\mathfrak{I} \models \varphi \leftrightarrow \psi$ platí právě tehdy, když $\mathfrak{I} \models \varphi$ a $\mathfrak{I} \models \psi$, nebo když $\mathfrak{I} \not\models \varphi$ a $\mathfrak{I} \not\models \psi$
- $\mathfrak{I} \models \forall x \varphi$ platí právě tehdy, když pro každé $a \in A$ platí $\mathfrak{I}[x \mapsto a] \models \varphi$
- $\mathfrak{I} \models \exists x \varphi$ platí právě tehdy, když existuje nějaké $a \in A$ takové, že $\mathfrak{I}[x \mapsto a] \models \varphi$

Volné a vázané výskyty proměnných

Každý výskyt proměnné x ve v podformuli tvaru $\exists x \varphi$ nebo $\forall x \varphi$ je **vázaný**.

Výskyt proměnné, který není vázaný, je **volný**.

$\mathrm{free}(t)$ — množina proměnných, které se vyskytují jako volné proměnné v termu t:

- $\mathrm{free}(x) = \{x\}$ pro $x \in \mathit{Var}$
- $\mathrm{free}(c) = \emptyset$ pro $c \in \mathcal{C}$
- $\mathrm{free}(f(t_1, t_2, \ldots, t_n)) = \mathrm{free}(t_1) \cup \mathrm{free}(t_2) \cup \ldots \cup \mathrm{free}(t_n)$ pro $f \in \mathcal{F}$

$\mathrm{free}(\varphi)$ — množina proměnných, které se vyskytují jako volné proměnné ve formuli φ:

- $\mathrm{free}(P(t_1, t_2, \ldots, t_n)) = \mathrm{free}(t_1) \cup \mathrm{free}(t_2) \cup \cdots \cup \mathrm{free}(t_n)$ pro $P \in \mathcal{P}$
- $\mathrm{free}(t_1 = t_2) = \mathrm{free}(t_1) \cup \mathrm{free}(t_2)$
- $\mathrm{free}(\bot) = \mathrm{free}(\top) = \emptyset$
- $\mathrm{free}(\neg\varphi) = \mathrm{free}(\varphi)$
- $\mathrm{free}(\varphi * \psi) = \mathrm{free}(\varphi) \cup \mathrm{free}(\psi)$ pro $* \in \{\wedge, \vee, \rightarrow, \leftrightarrow\}$
- $\mathrm{free}(\mathrm{Q}x\varphi) = \mathrm{free}(\varphi) - \{x\}$ pro $\mathrm{Q} \in \{\exists, \forall\}$ a $x \in \mathit{Var}$

Volné a vázané výskyty proměnných

Pravdivost formule φ při $\mathfrak{I} = (\mathfrak{A}, v)$ závisí pouze na $\mathfrak{A}$ a hodnotách, které v přiřazuje proměnným z množiny $\mathsf{free}(\varphi)$.

Speciálně v případě, kdy $\mathsf{free}(\varphi) = \emptyset$, tak pravdivost φ při $\mathfrak{I} = (\mathfrak{A}, v)$ závisí pouze na interpretaci $\mathfrak{A}$.

Pro formule φ, kde $\mathsf{free}(\varphi) = \emptyset$, můžeme psát

$$\mathfrak{A} \models \varphi \qquad \text{nebo} \qquad \mathfrak{A} \not\models \varphi$$

Formule φ, kde $\mathsf{free}(\varphi) = \emptyset$, se nazývá **uzavřená formule** neboli **sentence**.

Substituce

φ – formule, x – proměnná, t – term

Formule, kterou dostaneme, když dosadíme term t za **volné** výskyty proměnné x ve formuli φ:

$$\varphi[t/x]$$

Příklad: $\varphi := \forall x(P(x) \rightarrow R(f(x,z),y))$, $t := g(f(y,w))$

Formule $\varphi[t/z]$:

$$\forall x(P(x) \rightarrow R(f(x,g(f(y,w))),y))$$

Poznámka: Je třeba dát pozor na to, aby se volný výskyt proměnné v termu t nestal po dosazení vázaným.

V takovém případě je potřeba vázanou proměnnou přejmenovat.

Dedukční systém pro predikátovou logiku 1. řádu

Dedukční systém obsahující stejná pravidla jako systém pro výrokovou logiku.

Navíc několik pravidel pro práci s kvantifikátory a s rovností.

$$\forall\mathrm{e}: \quad \frac{\Gamma \vdash \forall x A}{\Gamma \vdash A[t/x]}$$

Příklad:

$$\forall x(P(x) \rightarrow Q(x)),\ P(c) \vdash Q(c)$$

$$\begin{array}{lll} 1. & \Gamma \vdash \forall x(P(x) \rightarrow Q(x)) & (\mathrm{Assm}) \\ 2. & \Gamma \vdash P(c) \rightarrow Q(c) & (\forall\mathrm{e}\ 1) \\ 3. & \Gamma \vdash P(c) & (\mathrm{Assm}) \\ 4. & \Gamma \vdash Q(c) & (\rightarrow\mathrm{e}\ 2,3) \end{array}$$

$\Gamma := \forall x(P(x) \rightarrow Q(x)),\ P(c)$

Univerzální kvantifikátor

$$\forall\text{i:}\quad \frac{\Gamma \vdash A[y/x]}{\Gamma \vdash \forall x A}(y \notin \mathrm{free}(\Gamma, \forall x A))$$

Speciální případ:

$$\frac{\Gamma \vdash A}{\Gamma \vdash \forall x A}(x \notin \mathrm{free}(\Gamma))$$

Univerzální kvantifikátor

Příklad: $\forall x(P(x) \vee Q(x)), \forall x(Q(x) \to R(x)) \vdash \forall x(P(x) \vee R(x))$

1.	$\Gamma \vdash \forall x(P(x) \vee Q(x))$	(Assm)
2.	$\Gamma \vdash P(x) \vee Q(x)$	($\forall$e 1)
3.	$\Gamma, P(x) \vdash P(x)$	(Assm)
4.	$\Gamma, P(x) \vdash P(x) \vee R(x)$	($\vee$i$_1$ 3)
5.	$\Gamma, Q(x) \vdash \forall x(Q(x) \to R(x))$	(Assm)
6.	$\Gamma, Q(x) \vdash Q(x) \to R(x)$	($\forall$e 5)
7.	$\Gamma, Q(x) \vdash Q(x)$	(Assm)
8.	$\Gamma, Q(x) \vdash R(x)$	($\to$e 6,7)
9.	$\Gamma, Q(x) \vdash P(x) \vee R(x)$	($\vee$i$_2$ 8)
10.	$\Gamma \vdash P(x) \vee R(x)$	($\vee$e 2,4,9)
11.	$\Gamma \vdash \forall x(P(x) \vee R(x))$	($\forall$i 10)

$\Gamma := \forall x(P(x) \vee Q(x)), \forall x(Q(x) \to R(x))$

Existenční kvantifikátor

$$\exists\mathrm{i}:\quad \frac{\Gamma \vdash A[t/x]}{\Gamma \vdash \exists x A}$$

$$\exists\mathrm{e}:\quad \frac{\Gamma \vdash \exists x A \qquad\qquad \Gamma, A[y/x] \vdash B}{\Gamma \vdash B}(y \notin \mathrm{free}(\Gamma, \exists x A, B))$$

Speciální případ:

$$\frac{\Gamma \vdash \exists x A \qquad\qquad \Gamma, A \vdash B}{\Gamma \vdash B}(x \notin \mathrm{free}(\Gamma, B))$$

Rovnost

$$=\mathrm{i}: \quad \frac{}{\vdash t = t}$$

$$=\mathrm{e}: \quad \frac{\Gamma \vdash t = t' \qquad \Gamma \vdash A[t/x]}{\Gamma \vdash A[t'/x]}$$

Příklad:

$$\frac{\Gamma \vdash t_1 = t_2}{\Gamma \vdash t_2 = t_1}$$

1. $\Gamma \vdash t_1 = t_2$	(premisa)
2. $\vdash t_1 = t_1$	($=\mathrm{i}$)
3. $\Gamma \vdash t_1 = t_1$	(Ant 2)
4. $\Gamma \vdash (x = t_1)[t_1/x]$	(rep. 3, $x \notin \mathrm{free}(t_1)$)
5. $\Gamma \vdash (x = t_1)[t_2/x]$	($=\mathrm{e}$ 1,4)
6. $\Gamma \vdash t_2 = t_1$	(rep. 5)

Některé důležité ekvivalence

Poznámka: Všechny následující ekvivalence jsou i dokazatelné ($\dashv\vdash$)

$$\neg\forall x\varphi \;\Leftrightarrow\; \exists x\neg\varphi$$
$$\neg\exists x\varphi \;\Leftrightarrow\; \forall x\neg\varphi$$

Pokud $x \notin \mathrm{free}(\psi)$:

$$(\forall x\varphi) \wedge \psi \;\Leftrightarrow\; \forall x(\varphi \wedge \psi)$$
$$(\forall x\varphi) \vee \psi \;\Leftrightarrow\; \forall x(\varphi \vee \psi)$$
$$(\exists x\varphi) \wedge \psi \;\Leftrightarrow\; \exists x(\varphi \wedge \psi)$$
$$(\exists x\varphi) \vee \psi \;\Leftrightarrow\; \exists x(\varphi \vee \psi)$$

Některé důležité ekvivalence

$$(\forall x\varphi) \wedge (\forall x\psi) \Leftrightarrow \forall x(\varphi \wedge \psi)$$
$$(\exists x\varphi) \vee (\exists x\psi) \Leftrightarrow \exists x(\varphi \vee \psi)$$

$$\forall x \forall y \varphi \Leftrightarrow \forall y \forall x \varphi$$
$$\exists x \exists y \varphi \Leftrightarrow \exists y \exists x \varphi$$

Pokud $y \notin \mathrm{free}(\varphi)$:

$$\forall x\varphi \Leftrightarrow \forall y(\varphi[y/x])$$
$$\exists x\varphi \Leftrightarrow \exists y(\varphi[y/x])$$

Pokud $x \notin \mathrm{free}(\varphi)$:

$$\forall x\varphi \Leftrightarrow \varphi$$
$$\exists x\varphi \Leftrightarrow \varphi$$

Existuje právě jeden

Předpokládejme, že:

- φ je formule
- proměnná y je různá od proměnné x
- $y \in \mathrm{free}(\varphi)$

Tvrzení „pro právě jeden prvek x platí φ" se dá zapsat formulí

$$\exists x(\varphi \wedge \forall y(\varphi[y/x] \rightarrow x = y))$$

Označuje se také:

$$\exists_{=1} x \varphi$$

Poznámka: Ve stejném významu jako $\exists_{=1}$ se používají například symboly $\exists_1$, $\exists^{=1}$, $\exists!$.

Přirozená čísla

Signatura $(\{<\}, \{\sigma, +, \cdot\}, \{0\}, \text{arity})$, kde $\text{arity}(<) = 2$, $\text{arity}(\sigma) = 1$, $\text{arity}(+) = 2$, $\text{arity}(\cdot) = 2$

Příklady formulí:

- $\forall x \exists y (x < y)$ — ke každému přirozenému číslu existuje větší přirozené číslo
- $\sigma(0) + \sigma(0) = \sigma(\sigma(0))$ — platí, že $1 + 1 = 2$
- $\sigma(0) < x \land \neg\exists y \exists z (\sigma(0) < y \land \sigma(0) < z \land y \cdot z = x)$ — formule s volnou proměnnou x reprezentující tvrzení, že x je prvočíslo

Přirozená čísla — Robinsonova a Peanova aritmetika

Axiomy:

- $\forall x(\sigma(x) \neq 0)$
- $\forall x \forall y(\sigma(x) = \sigma(y) \;\rightarrow\; x = y)$
- $\forall x(x = 0 \;\vee\; \exists y(\sigma(y) = x))$
- $\forall x(x + 0 = x)$
- $\forall x \forall y(x + \sigma(y) = \sigma(x + y))$
- $\forall x(x \cdot 0 = 0)$
- $\forall x \forall y(x \cdot \sigma(y) = (x \cdot y) + x)$
- $\forall x \forall y(x < y \;\leftrightarrow\; \exists z(\sigma(z) + x = y))$

Schéma axiomů indukce:

- $\forall y_1 \cdots \forall y_n(\varphi[0/x] \;\wedge\; \forall x(\varphi \rightarrow \varphi[\sigma(x)/x]) \;\rightarrow\; \forall x \varphi)$

— φ je libovolná formule, kde $\mathsf{free}(\varphi) \subseteq \{x, y_1, \ldots, y_n\}$

Definice

Předpokládejme, že je dána množina axiomů Γ.

- Definice predikátového symbolu P, kde $\mathrm{arity}(P) = n$:

$$\forall x_1 \cdots \forall x_n \, (P(x_1, \ldots, x_n) \;\leftrightarrow\; \varphi)$$

kde $\mathrm{free}(\varphi) \subseteq \{x_1, \ldots, x_n\}$

- Definice funkčního symbolu f, kde $\mathrm{arity}(f) = n$:

$$\forall x_1 \cdots \forall x_n \forall y \, (f(x_1, \ldots, x_n) = y \;\leftrightarrow\; \varphi)$$

kde $\mathrm{free}(\varphi) \subseteq \{x_1, \ldots, x_n, y\}$, přičemž $\Gamma \vdash \forall x_1 \cdots \forall x_n \exists_{=1} y(\varphi)$

- Definice konstantního symbolu c:

$$\varphi[c/x]$$

kde $\mathrm{free}(\varphi) \subseteq \{x\}$, přičemž $\Gamma \vdash \exists_{=1} x(\varphi)$

Teorie grup

Signatura $(\emptyset, \{\circ\}, \{e\}, \mathrm{arity})$, kde $\mathrm{arity}(\circ) = 2$

Axiomy:

- $\forall x \forall y \forall z((x \circ y) \circ z = x \circ (y \circ z))$
- $\forall x(x \circ e = x)$
- $\forall x \exists y(x \circ y = e)$

Teorie množin

Signatura $(\{\in\}, \emptyset, \emptyset, \mathrm{arity})$, kde $\mathrm{arity}(\in) = 2$

Příklady některých axiomů teorie množin:

- **Axiom extenzionality**:

$$\forall x \forall y (\forall z (z \in x \leftrightarrow z \in y) \rightarrow x = y)$$

- **Schéma axiomů vydělení**:

$$\forall y \exists z \forall x (x \in z \leftrightarrow (x \in y \wedge \varphi))$$

  kde φ je libovolná formule, kde $z \notin \mathrm{free}(\varphi)$

  Množina tvořená těmi prvky x množiny y, pro které platí φ:

$$\{x \in y \mid \varphi\}$$

Často používané zkratky

- Tvrzení „existuje x z množiny A takové, že pro x platí φ“:

$$\exists x(x \in A \ \wedge \ \varphi)$$

Zkrácený zápis:

$$(\exists x \in A)(\varphi)$$

- Tvrzení „pro každé x z množiny A platí φ“:

$$\forall x(x \in A \ \rightarrow \ \varphi)$$

Zkrácený zápis:

$$(\forall x \in A)(\varphi)$$

Formální jazyky

Abeceda a slovo

Definice

Abeceda je libovolná neprázdná konečná množina **symbolů** (**znaků**).

Poznámka: Abeceda se často označuje řeckým písmenem Σ (velké sigma).

Definice

Slovo v dané abecedě je libovolná konečná posloupnost symbolů z této abecedy.

Příklad 1:

$$\Sigma = \{\mathtt{A}, \mathtt{B}, \mathtt{C}, \mathtt{D}, \mathtt{E}, \mathtt{F}, \mathtt{G}, \mathtt{H}, \mathtt{I}, \mathtt{J}, \mathtt{K}, \mathtt{L}, \mathtt{M}, \mathtt{N}, \mathtt{O}, \mathtt{P}, \mathtt{Q}, \mathtt{R}, \mathtt{S}, \mathtt{T}, \mathtt{U}, \mathtt{V}, \mathtt{W}, \mathtt{X}, \mathtt{Y}, \mathtt{Z}\}$$

Slova v abecedě Σ: `AHOJ` `ABRACADABRA` `ERROR`

Abeceda a slovo

Příklad 2:

$\Sigma_2 = \{\mathtt{A}, \mathtt{B}, \mathtt{C}, \mathtt{D}, \mathtt{E}, \mathtt{F}, \mathtt{G}, \mathtt{H}, \mathtt{I}, \mathtt{J}, \mathtt{K}, \mathtt{L}, \mathtt{M}, \mathtt{N}, \mathtt{O}, \mathtt{P}, \mathtt{Q}, \mathtt{R}, \mathtt{S}, \mathtt{T}, \mathtt{U}, \mathtt{V}, \mathtt{W}, \mathtt{X}, \mathtt{Y}, \mathtt{Z}, \sqcup\}$

Slovo v abecedě Σ_2: $\mathtt{HELLO}\sqcup\mathtt{WORLD}$

Příklad 3:

$\Sigma_3 = \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9\}$

Slova v abecedě Σ_3: 0, 31415926536, 65536

Příklad 4:

Slova v abecedě $\Sigma_4 = \{0, 1\}$: 011010001, 111, 1010101010101010

Příklad 5:

Slova v abecedě $\Sigma_5 = \{a, b\}$: *aababb*, *abbabbba*, *aaab*

Abeceda a slovo

Příklad 6:

Abeceda Σ_6 je množina všech ASCII znaků.

Příklad slova:

```
class HelloWorld {
    public static void main(String[] args) {
        System.out.println("Hello, world!");
    }
}
```

$\texttt{class␣HelloWorld␣\{} \hookleftarrow \texttt{␣␣␣␣public␣static␣void␣main(Str}\cdots$

Teorie formálních jazyků – motivace

Jazyk — množina (některých) slov tvořených symboly z dané abecedy

Příklady typů problémů, při jejichž řešení se využívá poznatků z teorie formálních jazyků:

- Tvorba překladačů:
  - lexikální analýza
  - syntaktická analýza
- Vyhledávání v textu:
  - hledání zadaného vzorku
  - hledání textu zadaného regulárním výrazem

Práce s formálními jazyky

Když chceme nějaký jazyk popsat, máme několik možností:

- Můžeme vyjmenovat všechna jeho slova (což je ale použitelné jen pro malé konečné jazyky).

  Příklad: $L = \{aab, babba, aaaaaa\}$

- Můžeme specifikovat nějakou vlastnost, kterou mají právě ta slova, která do tohoto jazyka patří:

  Příklad: Jazyk nad abecedou $\{0, 1\}$, obsahující všechna slova, ve kterých je počet výskytů symbolu 1 sudý.

Práce s formálními jazyky

V teorii formálních jazyků se používají především následující dva přístupy:

- Popsat (idealizovaný) stroj, zařízení, algoritmus, který rozpozná slova patřící do daného jazyka – vede k použití tzv. **automatů**.
- Popsat nějaký mechanismus umožňující generovat všechna možná slova patřící do daného jazyka – vede k tzv. **gramatikám** a **regulárním výrazům**.