

# Šestá přednáška

NAIL062 Výroková a predikátová logika

---

Jakub Bulín (KTIML MFF UK)

Zimní semestr 2023

## Program

- úvod do predikátové logiky
- syntaxe a sémantika predikátové logiky
- vlastnosti teorií

## Materiály

**Zápisky z přednášky**, Sekce 6.1-6.5 z Kapitoly 6

# ČÁST II – PREDIKÁTOVÁ LOGIKA

---

# KAPITOLA 6: SYNTAXE A SÉMANTIKA PREDIKÁTOVÉ LOGIKY

---

## 6.1 Úvod

---

**Výroková logika:** popis světa pomocí **výroků** složených z **prvovýroků** (**výrokových proměnných**) – bitů informace

**Predikátová logika [prvního řádu]:**

- základní stavební kámen jsou **proměnné** reprezentující **individa** – nedělitelné objekty z nějaké množiny (např. přirozená čísla, vrcholy grafu, stavy mikroprocesoru)
- tato individua mají určité vlastnosti a vzájemné vztahy (**relace**), kterým říkáme **predikáty**
  - $\text{Leaf}(x)$  nebo  $\text{Edge}(x, y)$  mluvíme-li o grafu
  - $x \leq y$  v přirozených číslech
- a mohou vstupovat do **funkcí**
  - $\text{lowest\_common\_ancestor}(x, y)$  v zakořeněném stromu
  - $\text{succ}(x)$  nebo  $x + y$  v přirozených číslech
- a mohou být **konstantami** se speciálním významem, např. **root** v zakořeněném stromu, **0** v tělese.

# Syntaxe neformálně

- **atomické formule**: predikát (včetně **rovnosti**  $=$ ) o proměnných nebo o **termech** ('výrazy' složené z funkcí popř. konstant)
- **formule** jsou složené z atomických formulí pomocí logických spojek, a dvou **kvantifikátorů**:

$\forall x$  "pro všechna individua (reprezentovaná proměnnou  $x$ )"

$\exists x$  "existuje individuum (reprezentované proměnnou  $x$ )"

Např. "*Každý, kdo má dítě, je rodič.*" lze formalizovat takto:

$$(\forall x)((\exists y)\text{child\_of}(y, x) \rightarrow \text{is\_parent}(x))$$

- **child\_of**( $y, x$ ) je binární predikát vyjadřující, že individuum reprezentované proměnnou  $y$  je dítětem individua reprezentovaného proměnnou  $x$
- **is\_parent**( $x$ ) je unární predikát vyjadřující, že individuum reprezentované  $x$  je rodič

$$(\forall x)((\exists y)\text{child\_of}(y, x) \rightarrow \text{is\_parent}(x))$$

Platnost? Záleží na **modelu** světa/systému, který nás zajímá:

**Model** je...

- (neprázdná) množina individuí, spolu
- s binární relací **interpretující** binární relační symbol **child\_of**, a
- s unární relací (tj. podmnožinou) interpretující unární relační symbol **is\_parent**

Obecně mohou být relace jakékoliv, snadno sestojíme model, ve kterém formule neplatí, např.

$$\mathcal{A} = \langle \{0, 1\}, \{(0, 0), (0, 1), (1, 0), (1, 1)\}, \emptyset \rangle$$



## Příklad s funkcemi a konstantami

“Je-li  $x_1 \leq y_1$  a  $x_2 \leq y_2$ , potom platí  $(y_1 \cdot y_2) - (x_1 \cdot x_2) \geq 0$ .”

$$\varphi = (x_1 \leq y_1) \wedge (x_2 \leq y_2) \rightarrow ((y_1 \cdot y_2) + (-(x_1 \cdot x_2))) \geq 0$$

- dva binární relační symboly ( $\leq, \geq$ ), binární funkční symbol  $+$ , unární funkční symbol  $-$ , a konstantní symbol  $0$
- **model, ve kterém  $\varphi$  platí:**  $\mathbb{N}$  s binárními relacemi  $\leq^{\mathbb{N}}, \geq^{\mathbb{N}}$ , bin. funkcemi  $+^{\mathbb{N}}, \cdot^{\mathbb{N}}$ , unární funkcí  $-^{\mathbb{N}}$ , a konstantou  $0^{\mathbb{N}} = 0$
- vezmeme-li ale podobně množinu  $\mathbb{Z}$ ,  $\varphi$  už platit nebude

Poznámky:

- mohli bychom chápat ‘ $-$ ’ jako binární, obvykle ale bývá unární
- pro **konstantní symbol**  $0$  používáme (jak je zvykem) stejný symbol, jako pro přirozené číslo  $0$ . Ale pozor, v našem modelu může být **symbol**  $0$  interpretován jako **jiné číslo**, nebo náš model vůbec nemusí sestávat z čísel!

$$\varphi = (x_1 \leq y_1) \wedge (x_2 \leq y_2) \rightarrow ((y_1 \cdot y_2) + (-(x_1 \cdot x_2)) \geq 0)$$

- $\varphi$  nemá žádné kvantifikátory, tj. je **otevřená**
- $x_1, x_2, y_1, y_2$  jsou **volné proměnné** této formule (nejsou **vázané** žádným kvantifikátorem), píšeme  $\varphi(x_1, x_2, y_1, y_2)$
- sémantiku  $\varphi$  chápeme stejně jako  $(\forall x_1)(\forall x_2)(\forall y_1)(\forall y_2)\varphi$
- používáme **konvence** (infixový zápis, vynechání závorek), jinak:

$$\varphi = (((\leq(x_1, y_1) \wedge \leq(x_2, y_2)) \rightarrow \leq(+(\cdot(y_1, y_2), -(\cdot(x_1, x_2)))), 0))$$

- cvičení: definujte **strom formule**, nakreslete ho pro  $\varphi$

# Termy vs. atomické formule

$$\varphi = (x_1 \leq y_1) \wedge (x_2 \leq y_2) \rightarrow ((y_1 \cdot y_2) + (-(x_1 \cdot x_2)) \geq 0)$$

- výraz  $(y_1 \cdot y_2) + (-(x_1 \cdot x_2))$  je **term**
- výrazy  $(x_1 \leq y_1)$ ,  $(x_2 \leq y_2)$  a  $((y_1 \cdot y_2) + (-(x_1 \cdot x_2)) \geq 0)$  jsou (všechny) **atomické (pod)formule**  $\varphi$

V čem je rozdíl? Máme-li konkrétní model, a konkrétní **ohodnocení proměnných** individui (prvky) tohoto modelu:

- výsledkem termu (při daném ohodnocení proměnných) je konkrétní **individuum z modelu**, zatímco
- atomickým formulí lze přiřadit **pravdivostní hodnotu** (a tedy kombinovat je logickými spojkami)

## 6.2 Struktury

---

- specifikuje jakého **typu** bude daná struktura, tj. jaké má relace, funkce (jakých arit) a konstanty, a symboly pro ně
- **konstanty** lze chápat jako funkce arity 0, tj. funkce bez vstupů

**Signatura** je dvojice  $\langle \mathcal{R}, \mathcal{F} \rangle$ , kde  $\mathcal{R}, \mathcal{F}$  jsou disjunktní množiny symbolů (**relační** a **funkční**, ty zahrnují **konstantní**) spolu s danými aritami (tj. danými funkcí  $ar: \mathcal{R} \cup \mathcal{F} \rightarrow \mathbb{N}$ ) a neobsahující symbol '=' (ten je rezervovaný pro **rovnost**).

- často zapíšeme jen výčet symbolů, jsou-li arity a zda jsou relační nebo funkční zřejmé
- kromě běžně používaných symbolů typicky používáme:
  - pro relační symboly  $P, Q, R, \dots$
  - pro funkční (nekonstantní) symboly  $f, g, h, \dots$
  - pro konstantní symboly  $c, d, a, b, \dots$

## Příklady signatur

- $\langle E \rangle$  signatura **grafů**:  $E$  je binární relační symbol (strukтуры jsou uspořádané grafy)
- $\langle \leq \rangle$  signatura **částečných uspořádání**: stejná jako signatura grafů, jen jiný symbol (ne každá struktura v této signatuře je částečné uspořádání! k tomu musí splňovat příslušné **axiomy**)
- $\langle +, -, 0 \rangle$  signatura **grup**:  $+$  je binární funkční,  $-$  unární funkční,  $0$  konstantní symbol
- $\langle +, -, 0, \cdot, 1 \rangle$  signatura **těles**:  $\cdot$  je binární funkční,  $1$  konstantní symbol
- $\langle +, -, 0, \cdot, 1, \leq \rangle$  signatura **uspořádaných těles**:  $\leq$  je binární relační symbol
- $\langle -, \wedge, \vee, \perp, \top \rangle$  signatura **Booleových algeber**:  $\wedge, \vee$  jsou binární funkční,  $\perp, \top$  jsou konstantní symboly
- $\langle S, +, \cdot, 0, \leq \rangle$  signatura **aritmetiky**:  $S$  je unární funkční symbol

Strukturu dané signatury získáme tak, že:

- zvolíme neprázdnou **doménu**, a na ní
- zvolíme **realizace** (také říkáme **interpretace**) všech relačních a funkčních symbolů (a konstant)
- to znamená **konkrétní** relace resp. funkce příslušných arit
- realizací konstantního symbolu je zvolený prvek z domény
- na tom, jaké konkrétní symboly jsou v signatuře nezáleží (např.  $+$  neznamená, že realizace musí souviset se sčítáním)

- Struktura v **prázdné signatuře**  $\langle \rangle$  je libovolná neprázdna množina. (Nemusí být konečná, ani spočetná! Formálně to bude trojice  $\langle A, \emptyset, \emptyset \rangle$ , ale rozdíl zanedbáme.)
- Struktura v **signatuře grafů** je  $\mathcal{G} = \langle V, E \rangle$ , kde  $V \neq \emptyset$  a  $E \subseteq V^2$ , říkáme jí **orientovaný graf**.
  - je-li  $E$  ireflexivní a symetrická, je to **jednoduchý graf**
  - je-li  $E$  reflexivní, tranzitivní, a antisymetrická, jde o **částečné uspořádání**
  - je-li  $E$  reflexivní, tranzitivní, a symetrická, je to **ekvivalence**
- Struktury v **signatuře částečných uspořádání** jsou tytéž, jako v signatuře grafů, signatury se liší jen symbolem. (Ne každá struktura v signatuře částečných uspořádání je č. uspořádání!)



Struktury v signatuře grup jsou například následující grupy:

- $\underline{\mathbb{Z}}_n = \langle \mathbb{Z}_n, +, -, 0 \rangle$ , aditivní grupa celých čísel modulo  $n$  (operace jsou modulo  $n$ ).

**Poznámka:**  $\underline{\mathbb{Z}}_n$  znamená strukturu, zatímco  $\mathbb{Z}_n$  jen její doménu. Často se to ale nerozlišuje a  $\mathbb{Z}_n$  se používá i pro strukturu. Podobně  $+$ ,  $-$ ,  $0$  jsou jak symboly, tak interpretace.

- $\mathcal{S}_n = \langle \text{Sym}_n, \circ, {}^{-1}, \text{id} \rangle$  je symetrická grupa (grupa všech permutací) na  $n$  prvcích.
- $\underline{\mathbb{Q}}^* = \langle \mathbb{Q} \setminus \{0\}, \cdot, {}^{-1}, 1 \rangle$  je multiplikativní grupa (nenulových) racionálních čísel. (Interpretací symbolu  $0$  je číslo  $1!$ )

Všechny tyto struktury splňují axiomy teorie grup, snadno ale najdeme jiné, které axiomy nesplňují, nejsou tedy grupami.

- Struktury  $\underline{\mathbb{Q}} = \langle \mathbb{Q}, +, -, 0, \cdot, 1, \leq \rangle$  a  $\underline{\mathbb{Z}} = \langle \mathbb{Z}, +, -, 0, \cdot, 1, \leq \rangle$  (se standardními operacemi a uspořádáním) jsou v signatuře uspořádaných těles (ale jen první z nich je uspořádané těleso).
- $\underline{\mathcal{P}(X)} = \langle \mathcal{P}(X), \neg, \cap, \cup, \emptyset, X \rangle$ , tzv. potenční algebra nad množinou  $X$ , je struktura v signatuře Booleových algeber. (Booleova algebra je to pokud  $X \neq \emptyset$ .)
- $\underline{\mathbb{N}} = \langle \mathbb{N}, S, +, \cdot, 0, \leq \rangle$ , kde  $S(x) = x + 1$ , a ostatní symboly jsou realizovány standardně, je standardní model aritmetiky.

**Struktura v signatuře**  $\langle \mathcal{R}, \mathcal{F} \rangle$  je trojice  $\mathcal{A} = \langle A, \mathcal{R}^{\mathcal{A}}, \mathcal{F}^{\mathcal{A}} \rangle$ , kde

- $A$  je neprázdná množina, říkáme jí **doména** (také **univerzum**),
- $\mathcal{R}^{\mathcal{A}} = \{R^{\mathcal{A}} \mid R \in \mathcal{R}\}$  kde  $R^{\mathcal{A}} \subseteq A^{\text{ar}(R)}$  je **interpretace** relačního symbolu  $R$ ,
- $\mathcal{F}^{\mathcal{A}} = \{f^{\mathcal{A}} \mid f \in \mathcal{F}\}$  kde  $f^{\mathcal{A}}: A^{\text{ar}(f)} \rightarrow A$  je **interpretace** funkčního symbolu  $f$  (speciálně pro konstantní symbol  $c \in \mathcal{F}$  máme  $c^{\mathcal{A}} \in A$ ).

**Příklad:** rozmyslete si, jak vypadají struktury v **signatuře**  $n$  konstant  $\langle c_1, c_2, \dots, c_n \rangle$ ? Popište všechny 5-prvkové v signatuře 3 konstant.

## 6.3 Syntaxe

---

Jazyk je daný **signaturou** a informací, zda je **s rovností** nebo ne.

Tj. specifikujeme 'typ' modelů a zda můžeme používat symbol '=' interpretovaný jako **identita** prvků z domény; většinou to dovolíme. (Je-li jazyk bez rovnosti, musí mít signatura relační symbol. Proč?)

Do jazyka patří:

- spočetně mnoho **proměnných**  $x_0, x_1, x_2, \dots$  (píšeme také  $x, y, z, \dots$ ; množinu všech proměnných označíme **Var**)
- **relační, funkční a konstantní symboly** ze signatury, symbol = jde-li o jazyk s rovností (to jsou '**mimologické**' symboly)
- **univerzální a existenční kvantifikátory**  $(\forall x), (\exists x)$  pro každou proměnnou  $x \in \text{Var}$  (kvantifikátor ' $(\forall x)$ ' chápeme jako jediný symbol, tj. **neobsahuje** proměnnou  $x$ )
- symboly pro log. spojky  $\neg, \wedge, \vee, \rightarrow, \leftrightarrow$ , závorky  $(, )$ , a čárka ','

- Jazyk  $L = \langle \rangle$  s rovností je jazyk **čisté rovnosti**
- jazyk  $L = \langle c_0, c_1, c_2, \dots \rangle$  s rovností je jazyk **spočetně mnoha konstant**
- jazyk **uspořádání** je  $\langle \leq \rangle$  s rovností
- jazyk **teorie grafů** je  $\langle E \rangle$  s rovností
- jazyky **teorie grup, teorie těles, teorie uspořádaných těles, Booleových algeber, aritmetiky** jsou jazyky s rovností odpovídající daným signaturám

čistě syntaktické 'výrazy' z proměnných, konstantních symbolů, funkčních symbolů, závorek a čárek

**Termy** jazyka  $L$  jsou konečné nápisy definované induktivně:

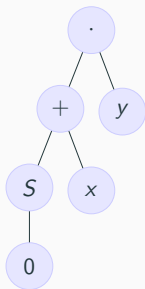
- každá proměnná a každý konstantní symbol z  $L$  je term,
- je-li  $f$  funkční symbol z  $L$  arity  $n$  a jsou-li  $t_1, \dots, t_n$  termy, potom nápis  $f(t_1, t_2, \dots, t_n)$  je také term.

Množinu všech **termů** jazyka  $L$  označíme  $\text{Term}_L$ .

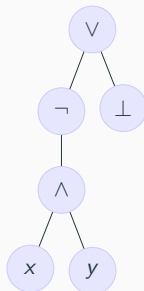
- **podterm** je podřetězec, který je sám termem
- term bez proměnných je **konstantní (ground)**, např.  $((S(0) + S(0)) \cdot S(S(0)))$  v jazyce aritmetiky
- **termy nesmí obsahovat prvky struktury, jen symboly z jazyka**
- $(1 + 1) \cdot 2$  **není** term, ledaže rozšíříme jazyk o **symboly** 1 a 2
- jako lidé můžeme použít **infixový** zápis, např.  $(t_1 + t_2)$  místo  $+(t_1, t_2)$ , vynechat závorky je-li struktura termu zřejmá

# Strom termu

**Strom termu**  $t$ ,  $\text{Tree}(t)$ : v listech proměnné nebo konst. symboly, ve vnitřních vrcholech funkční symboly (arita je rovna počtu synů)



(a)  $(S(0) + x) \cdot y$  v jazyce aritmetiky



(b)  $\neg(x \wedge y) \vee \perp$  v jazyce Booleových algeber

- symboly  $\neg, \wedge, \vee$  nejsou logické, ale mimologické ze signatury
- **sémantika**: proměnné ohodnotíme prvky, konst. a funkční symboly nahradíme interpretacemi, výsledek je prvek z domény



# Atomické formule

Termům nelze přiřadit **pravdivostní hodnotu**, potřebujeme **predikát** (relační symbol nebo  $=$ ), který mluví o **'vztahu' termů**: v dané struktuře při ohodnocení proměnných prvky je buď splněn, nebo ne.

**Formule** ('tvrzení o strukturách') skládáme z **atomických formulí** pomocí logických spojek a kvantifikátorů:

**Atomická formule** jazyka  $L$  je nápis  $R(t_1, \dots, t_n)$ , kde  $R$  je  $n$ -ární relační symbol z  $L$  (včetně  $=$  jde-li o jazyk s rovností) a  $t_i \in \text{Term}_L$ .

- $R(f(f(x)), c, f(d))$  kde  $R$  je ternární relační,  $f$  unární funkční,  $c, d$  konstantní symboly
- **infixový zápis**  $\leq(x, y), = (t_1, t_2)$  píšeme jako  $x \leq y, t_1 = t_2$
- $(x \cdot x) + (y \cdot y) \leq (x + y) \cdot (x + y)$  v jazyce uspořádaných těles
- $x \cdot y \leq (S(0) + x) \cdot y$  v jazyce aritmetiky
- $\neg(x \wedge y) \vee \perp = \perp$  v jazyce Booleových algeber

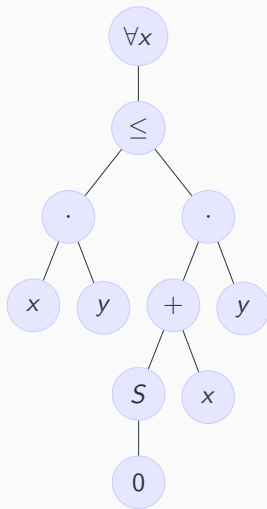
**Formule** jazyka  $L$  jsou konečné nápisy definované induktivně:

- každá **atomická formule** jazyka  $L$  je formule,
  - je-li  $\varphi$  formule, potom  $(\neg\varphi)$  je také formule
  - jsou-li  $\varphi, \psi$  formule, potom  $(\varphi \square \psi)$  pro  $\square \in \{\wedge, \vee, \rightarrow, \leftrightarrow\}$  jsou také formule
  - je-li  $\varphi$  formule a  $x$  proměnná, potom  $((Qx)\varphi)$  pro  $Q \in \{\forall, \exists\}$  jsou také formule
- 
- **podformule** je podřetězec, který je sám formulí
  - při zápisu formulí jako lidé používáme obvyklé konvence
  - kvantifikátory mají stejnou prioritu jako  $\neg$ , vyšší než ostatní logické spojky! místo  $((\forall x)\varphi)$  píšeme  $(\forall x)\varphi$
  - **pozor,  $(\forall x)\varphi \wedge \psi$  neznamená totéž, co  $(\forall x)(\varphi \wedge \psi)$ !**
  - někde uvidíte  $\forall x\varphi$  nebo  $\forall_x\varphi$ , my ale budeme psát jen  $(\forall x)\varphi$

Příklad:  $(\forall x)(x \cdot y \leq (S(0) + x) \cdot y)$

Strom formule,  $\text{Tree}(\varphi)$ :

- strom atomické formule  $R(t_1, \dots, t_n)$ :  
v kořeni  $R$ , připojíme stromy  $\text{Tree}(t_i)$
- pro složené formule podobně jako ve  
výrokové logice
- kvantifikátory mají jediného syna



# Volné a vázané proměnné

Význam formule (**pravdivostní hodnota**) může/nemusí záviset na proměnných v ní:  $x \leq 0$  vs.  $(\exists x)(x \leq 0)$  vs.  $x \leq 0 \vee (\exists x)(x \leq 0)$

- **výskyt  $x$  ve  $\varphi$** : list  $\text{Tree}(\varphi)$  označený  $x$  [ $\vee (Qx)$  nemá výskyt!]
- **vázaný**: součástí podformule začínající  $(Qx)$ , jinak **volný**
- $x$  je **volná** ve  $\varphi$  má-li volný výskyt, **vázaná** má-li vázaný výskyt
- zápis  $\varphi(x_1, \dots, x_n)$  znamená, že  $x_1, \dots, x_n$  jsou všechny volné proměnné ve formuli  $\varphi$

Proměnná může být **volná i vázaná**, např.:

$$\varphi = (\forall x)(\exists y)(x \leq y) \vee x \leq z$$

- první výskyt  $x$  je vázaný a druhý volný (nakreslete si strom!)
- $y$  je vázaná a  $z$  je volná, můžeme tedy psát  $\varphi(x, z)$

# Otevřené a uzavřené formule

**otevřená formule:** nemá žádný kvantifikátor

**uzavřená formule (sentence):** nemá žádnou volnou proměnnou

- $x + y \leq 0$  je otevřená formule
- $(\forall x)(\forall y)(x + y \leq 0)$  je uzavřená formule neboli sentence
- $(\forall x)(x + y \leq 0)$  není ani otevřená, ani uzavřená
- $(0 + 1 = 1) \wedge (1 + 1 = 0)$  je otevřená i uzavřená
- atomické formule je otevřená, otevřené formule jsou kombinace atomických pomocí logických spojek
- je-li formule otevřená i uzavřená potom nemá žádné proměnné (všechny termy v ní jsou konstantní)
- formule bez vázané proměnné není nutně otevřená!  $(\forall x)0 = 1$

Uvidíme, že **pravdivostní hodnota** závisí jen na ohodnocení volných proměnných; **sentence** mají ve struktuře pravdiv. hodnotu 0 nebo 1

## Instance a varianty: neformálně

- proměnná může hrát různé 'role' ('lokální' vs. 'globální')
- **instance**: 'dosazení' do 'globální' proměnné (lépe 'nahrazení' proměnné nějakým termem, který ji počítá, čistě syntaktické!)
- **varianta**: 'přejmenování' 'lokální' proměnné

$$P(x) \wedge (\forall x)(Q(x) \wedge (\exists x)R(x))$$

- první výskyt  $x$  je volný, 2. je vázaný ( $\forall x$ ), 3. je vázaný ( $\exists x$ )
- pokud **substituujeme** za proměnnou  $x$  term  $t = 1 + 1$ , dostáváme **instanci** formule  $\varphi$ , kterou označíme  $\varphi(x/t)$ :

$$P(1 + 1) \wedge (\forall x)(Q(x) \wedge (\exists x)R(x))$$

- přejmenujeme-li kvantifikátory, získáme **variantu** formule  $\varphi$ :

$$P(x) \wedge (\forall y)(Q(y) \wedge (\exists z)R(z))$$

Kdy a jak to lze, aby instance byla **důsledek** a varianta **ekvivalentní**?

Substituujeme-li do  $\varphi$  za  $x$  term  $t$ , chceme aby výsledná formule 'říkala o  $t$  totéž, co  $\varphi$  o  $x$ '. Např.  $\varphi(x) = (\exists y)(x + y = 1)$

- říká o  $x$ , že 'existuje  $x - 1$ '
- term  $t = 1$  lze:  $\varphi(x/t) = (\exists y)(1 + y = 1)$  říká 'existuje 1-1'
- term  $t = y$  nelze:  $(\exists y)(y + y = 1)$  říká '1 je dělitelné 2'

**problém:** obsahuje  $y$ , po nahrazení bude nově vázané  $(\exists y)$

Term  $t$  je **substituovatelný** za proměnnou  $x$  ve formuli  $\varphi$ , pokud po simultánním nahrazení všech volných výskytů  $x$  za  $t$  nevznikne žádný vázaný výskyt proměnné  $z$   $t$ . Potom je vzniklá formule **instance**  $\varphi$  vzniklá substitucí  $t$  za  $x$ ,  $\varphi(x/t)$ .

- $t$  **není** substituovatelný za  $x$  do  $\varphi$ , právě když  $x$  má volný výskyt v nějaké podformuli  $\varphi$  tvaru  $(Qy)\psi$  a  $y$  se vyskytuje v  $t$
- speciálně: konstantní termy jsou vždy substituovatelné

## Varianta

Substituovat  $t$  můžeme vždy do **varianty**  $\varphi$ , ve které přejmenujeme všechny kvantifikované proměnné na nové (které nejsou v  $t$  ani  $\varphi$ )

Má-li formule  $\varphi$  podformuli tvaru  $(Qx)\psi$  a je-li  $y$  proměnná, že

- (i)  $y$  je substituovatelná za  $x$  do  $\psi$ , a
- (ii)  $y$  nemá volný výskyt v  $\psi$ .

**Varianta**  $\varphi$  vznikne nahrazením  $(Qx)\psi$  formulí  $(Qy)\psi(x/y)$ , říkáme tak i výsledku postupné variace ve více podformulích.

Mějme  $\varphi = (\exists x)(\forall y)(x \leq y)$ :

- $(\exists u)(\forall v)(u \leq v)$  je varianta  $\varphi$
- $(\exists y)(\forall y)(y \leq y)$  není varianta kvůli (i):  $y$  není substituovatelná za  $x$  do  $\psi = (\forall y)(y \leq y)$
- $(\exists x)(\forall x)(x \leq x)$  není varianta kvůli (ii):  $x$  má volný výskyt v  $\psi = (x \leq y)$



## 6.4 Sémantika

---

- **modely jsou struktury** dané signatury,
- formule **platí** ve struktuře, pokud platí při každém ohodnocení volných proměnných prvky z domény,
- **hodnoty termů** (jsou to prvky z domény) se vyhodnocují podle jejich stromů, kde symboly nahradíme jejich interpretacemi (relacemi, funkcemi, a konstantami z domény),
- z hodnot termů získáme **pravdivostní hodnoty atomických formulí**: je výsledná  $n$ -tice v relaci?
- hodnoty složených formulí vyhodnocujeme také podle jejich stromu, přičemž  $(\forall x)$  hraje roli 'konjunkce přes všechny prvky' a  $(\exists y)$  hraje roli 'disjunkce přes všechny prvky' z domény struktury

# Modely jazyka

**Model jazyka**  $L$ , nebo také  **$L$ -struktura**, je libovolná struktura v signatuře jazyka  $L$ . **Třidu** všech modelů jazyka označíme  $M_L$ .

- zda je jazyk s rovností nebo bez nehraje roli
- proč **třída** a ne **množina** všech modelů  $M_L$ ? doména je libovolná neprázdná množina, 'množina všech množin' neexistuje; třída je '**soubor**' všech množin splňujících danou vlastnost (popsatelnou v **jazyce teorie množin**)

Mezi **modely jazyka uspořádání**  $L = \langle \leq \rangle$  patří:

- částečně uspořádané množiny  $\langle \mathbb{N}, \leq \rangle$ ,  $\langle \mathbb{Q}, > \rangle$ ,  $\langle \mathcal{P}(X), \subseteq \rangle$
- libovolný orientovaný graf  $G = \langle V, E \rangle$ , typicky není částečné uspořádání, tj. nesplňuje axiomy **teorie uspořádání**
- $\langle \mathbb{C}, R^{\mathbb{C}} \rangle$  kde  $(z_1, z_2) \in R^{\mathbb{C}}$  právě když  $|z_1| = |z_2|$  (není č. usp.)

# Hodnota termu

Mějme term  $t$  jazyka  $L = \langle \mathcal{R}, \mathcal{F} \rangle$  a  $L$ -strukturu  $\mathcal{A} = \langle A, \mathcal{R}^{\mathcal{A}}, F^{\mathcal{A}} \rangle$ .

**Ohodnocení proměnných** v množině  $A$  je lib. funkce  $e : \text{Var} \rightarrow A$ .

**Hodnota termu  $t$  ve struktuře  $\mathcal{A}$  při ohodnocení  $e$** , značíme  $t^{\mathcal{A}}[e]$ , je definovaná induktivně:

- $x^{\mathcal{A}}[e] = e(x)$  pro proměnnou  $x \in \text{Var}$ ,
- $c^{\mathcal{A}}[e] = c^{\mathcal{A}}$  pro konstantní symbol  $c \in \mathcal{F}$ , a
- je-li  $t = f(t_1, \dots, t_n)$  složený term, kde  $f \in \mathcal{F}$ , potom:

$$t^{\mathcal{A}}[e] = f^{\mathcal{A}}(t_1^{\mathcal{A}}[e], \dots, t_n^{\mathcal{A}}[e])$$

- závisí pouze na ohodnocení proměnných vyskytujících se v  $t$
- obecně, term  $t$  reprezentuje **termovou funkci**  $f_t^{\mathcal{A}}: A^k \rightarrow A$ , kde  $k$  je počet proměnných v  $t$
- speciálně, hodnota konstantního termu na ohodnocení nezávisí, konstantní termy reprezentují konstantní funkce

## Hodnota termu: příklady

1. Hodnota termu  $t = -(x \vee \perp) \wedge y$  v Booleově algebře

$\mathcal{A} = \mathcal{P}(\{0, 1, 2\})$  při ohodnocení  $e$  ve kterém:

- $e(x) = \{0, 1\}$
- $e(y) = \{1, 2\}$

$$t^{\mathcal{A}}[e] = \{2\}$$

2. Hodnota termu  $x + 1$  ve struktuře  $\mathcal{N} = \langle \mathbb{N}, \cdot, 3 \rangle$  jazyka

$L = \langle +, 1 \rangle$  při ohodnocení  $e$  ve kterém  $e(x) = 2$

$$(x + 1)^{\mathcal{N}}[e] = 6$$

# Pravdivostní hodnota formule

Bud'  $\varphi$  v jazyce  $L$ ,  $\mathcal{A} \in M_L$ ,  $e : \text{Var} \rightarrow A$  ohodnocení proměnných.

**Pravdivostní hodnota**  $\varphi$  v  $\mathcal{A}$  při ohodnocení  $e$ ,  $\text{PH}^{\mathcal{A}}(\varphi)[e]$ :

- pro atomickou formuli  $R(t_1, \dots, t_n)$ :

$$\text{PH}^{\mathcal{A}}(R(t_1, \dots, t_n))[e] = \begin{cases} 1 & \text{pokud } (t_1^{\mathcal{A}}[e], \dots, t_n^{\mathcal{A}}[e]) \in R^{\mathcal{A}} \\ 0 & \text{jinak} \end{cases}$$

- pro formuli tvaru  $(\neg\varphi)$ :

$$\text{PH}^{\mathcal{A}}(\neg\varphi)[e] = f_{\neg}(\text{PH}^{\mathcal{A}}(\varphi)[e]) = 1 - \text{PH}^{\mathcal{A}}(\varphi)[e]$$

- pro formuli tvaru  $(\varphi \square \psi)$  kde  $\square \in \{\wedge, \vee, \rightarrow, \leftrightarrow\}$ :

$$\text{PH}^{\mathcal{A}}(\varphi \square \psi)[e] = f_{\square}(\text{PH}^{\mathcal{A}}(\varphi)[e], \text{PH}^{\mathcal{A}}(\psi)[e])$$

## Pravdivostní hodnota formule: zbytek definice a poznámky

- pro formuli tvaru  $(Qx)\varphi$  kde  $Q \in \{\forall, \exists\}$ :

$$\text{PH}^A((\forall x)\varphi)[e] = \min_{a \in A}(\text{PH}^A(\varphi)[e(x/a)])$$

$$\text{PH}^A((\exists x)\varphi)[e] = \max_{a \in A}(\text{PH}^A(\varphi)[e(x/a)])$$

kde  $e(x/a)$  je ohodnocení získané z  $e$  změnou  $e(x)$  na  $a$

**Pozorování:** Závisí pouze na ohodnocení volných proměnných. Speciálně, pro sentenci nezávisí na ohodnocení.

- Tedy v ohodnocení  $e$  nastavíme hodnotu proměnné  $x$  postupně na všechny prvky  $a \in A$  a požadujeme, aby PH byla rovna 1 vždy (v případě  $\forall$ ) nebo alespoň jednou (v případě  $\exists$ ).<sup>1</sup>
- speciálně,  $\text{PH}^A(t_1 = t_2)[e] = 1 \Leftrightarrow (t_1^A[e], t_2^A[e]) \in =^A$  (**identita** na  $A$ ), tj.  $t_1^A[e] = t_2^A[e]$  (obě strany jsou stejné)

Vezměme si uspořádané těleso  $\underline{\mathbb{Q}}$ . Potom:

- $\text{PH}^{\underline{\mathbb{Q}}}(x \leq 1 \wedge \neg(x \leq 0))[e] = 1$  právě když  $e(x) \in (0, 1]$
- $\text{PH}^{\underline{\mathbb{Q}}}((\forall x)(x \cdot y = y))[e] = 1$  právě když  $e(y) = 0$
- $\text{PH}^{\underline{\mathbb{Q}}}((\exists x)(x \leq 0 \wedge \neg x = 0))[e] = 1$  pro každé ohodnocení  $e$  (je to sentence)

Ale pro strukturu  $\mathcal{A} = \langle \mathbb{N}, +, -, 0, \cdot, 1, \leq \rangle$  máme:

- $\text{PH}^{\mathcal{A}}((\exists x)(x \leq 0 \wedge \neg x = 0))[e] = 0$



Mějme formuli  $\varphi$ , strukturu  $\mathcal{A}$  (ve stejném jazyce), a ohodnocení  $e$ .

- je-li  $\text{PH}^{\mathcal{A}}(\varphi)[e] = 1$ ,  $\varphi$  **platí** v  $\mathcal{A}$  **při ohodnocení**  $e$ ,  $\mathcal{A} \models \varphi[e]$
- je-li  $\text{PH}^{\mathcal{A}}(\varphi)[e] = 0$ ,  $\varphi$  **neplatí** v  $\mathcal{A}$  **při ohodnoc.**  $e$ ,  $\mathcal{A} \not\models \varphi[e]$
- $\varphi$  je **pravdivá** (**platí**) v  $\mathcal{A}$ ,  $\mathcal{A} \models \varphi$ , pokud platí při každém ohodnocení  $e : \text{Var} \rightarrow A$
- $\varphi$  je **lživá** v  $\mathcal{A}$ , pokud neplatí při žádném ohodnocení (v tom případě  $\mathcal{A} \models \neg\varphi$ )
- pozor, **lživá** není totéž, co **není pravdivá** (**neplatí**)! (Platí to ale pro sentence.)
- **platnost** je klíčový pojem sémantiky a celé logiky

## Zřejmé vlastnosti platnosti ve struktuře při ohodnocení

- $\mathcal{A} \models \neg\varphi[e]$  právě když  $\mathcal{A} \not\models \varphi[e]$
- $\mathcal{A} \models (\varphi \wedge \psi)[e]$  právě když  $\mathcal{A} \models \varphi[e]$  a  $\mathcal{A} \models \psi[e]$
- $\mathcal{A} \models (\varphi \vee \psi)[e]$  právě když  $\mathcal{A} \models \varphi[e]$  nebo  $\mathcal{A} \models \psi[e]$
- $\mathcal{A} \models (\varphi \rightarrow \psi)[e]$  právě když platí: jestliže  $\mathcal{A} \models \varphi[e]$  potom  $\mathcal{A} \models \psi[e]$
- $\mathcal{A} \models (\varphi \leftrightarrow \psi)[e]$  právě když platí:  $\mathcal{A} \models \varphi[e]$  právě když  $\mathcal{A} \models \psi[e]$
- $\mathcal{A} \models (\forall x)\varphi[e]$  právě když  $\mathcal{A} \models \varphi[e(x/a)]$  pro každé  $a \in A$
- $\mathcal{A} \models (\exists x)\varphi[e]$  právě když  $\mathcal{A} \models \varphi[e(x/a)]$  pro nějaké  $a \in A$
- je-li term  $t$  substituovatelný za proměnnou  $x$  do  $\varphi$ , potom:  
 $\mathcal{A} \models \varphi(x/t)[e]$  právě když  $\mathcal{A} \models \varphi[e(x/a)]$  pro  $a = t^{\mathcal{A}}[e]$
- je-li  $\psi$  varianta  $\varphi$ , potom  $\mathcal{A} \models \varphi[e]$  právě když  $\mathcal{A} \models \psi[e]$

(dokažte si snadno z definic, najděte protipříklady)

- pokud  $\mathcal{A} \models \varphi$ , potom  $\mathcal{A} \not\models \neg\varphi$ ; je-li  $\varphi$  sentence, platí i opačná implikace
- $\mathcal{A} \models \varphi \wedge \psi$  právě když  $\mathcal{A} \models \varphi$  a  $\mathcal{A} \models \psi$
- pokud  $\mathcal{A} \models \varphi$  nebo  $\mathcal{A} \models \psi$ , potom  $\mathcal{A} \models \varphi \vee \psi$ ; je-li  $\varphi$  sentence, platí i opačná implikace.
- $\mathcal{A} \models \varphi$  právě když  $\mathcal{A} \models (\forall x)\varphi$
- speciálně,  $\varphi(x_1, \dots, x_n)$  platí ve struktuře  $\mathcal{A}$ , právě když v  $\mathcal{A}$  platí její **generální uzávěr**, tj. sentence  $(\forall x_1) \cdots (\forall x_n)\varphi$

(dokažte si snadno z definic, najděte protipříklady)

## 6.5 Vlastnosti teorií

---

- **teorie** jazyka  $L$  je množina  $L$ -formulí, její prvky jsou **axiomy**
- **model** teorie  $T$  je  $L$ -struktura, ve které platí všechny axiomy  $T$ , tj.  $\mathcal{A} \models \varphi$  pro všechna  $\varphi \in T$ , značíme  $\mathcal{A} \models T$
- **třída modelů** teorie  $T$  je:

$$M_L(T) = \{\mathcal{A} \in M_L \mid \mathcal{A} \models T\}$$

Je-li  $T$  teorie v jazyce  $L$  a  $\varphi$   $L$ -formule, potom  $\varphi$  je:

- **pravdivá (platí) v  $T$** , značíme  $T \models \varphi$ , pokud  $\mathcal{A} \models \varphi$  pro všechna  $\mathcal{A} \in M(T)$  (neboli:  $M(T) \subseteq M(\varphi)$ )
- **lživá v  $T$** , pokud  $T \models \neg\varphi$ , tj. pokud je lživá v každém modelu  $T$  (neboli:  $M(T) \cap M(\varphi) = \emptyset$ )
- **nezávislá v  $T$** , pokud není pravdivá v  $T$  ani lživá v  $T$
- je-li  $T = \emptyset$  (tj.  $M(T) = M_L$ ), píšeme jen  $\models \varphi$ , a říkáme, že  $\varphi$  je pravdivá (v logice), (logicky) platí, je tautologie, apod.

- $T$  je **sporná**, pokud v ní platí **spor**  $\perp$  (definujeme jako  $R(x_1, \dots, x_n) \wedge \neg R(x_1, \dots, x_n)$ , kde  $R$  je lib. relační symbol)
- $T$  je sporná, právě když v ní platí každá formule (ekvivalentně, nemá žádný model), jinak je **bezesporná** (neplatí-li v ní spor, má-li alespoň jeden model)
- **důsledky**  $T$  jsou **sentence** pravdivé v  $T$ , množina všech důsledků  $T$  v jazyce  $L$  je

$$\text{Csq}_L(T) = \{\varphi \mid \varphi \text{ je sentence a } T \models \varphi\}$$

# Kompletnost v predikátové logice

- $T$  je **kompletní**, je-li bezesporná a každá **sentence** je v ní buď pravdivá, nebo lživá. **Pozor: neplatí, že má jediný model!**
- máme-li jeden model, máme i nekonečně mnoho **izomorfních** modelů (liší se jen pojmenováním prvků, definujeme později)
- uvažovat jediný model **až na izomorfismus** ale také **nestačí!**

Struktury  $\mathcal{A}, \mathcal{B}$  (v témž jazyce) jsou **elementárně ekvivalentní**, píšeme  $\mathcal{A} \equiv \mathcal{B}$ , pokud v nich platí tytéž sentence.

**Pozorování:** Teorie je kompletní, právě když má právě jeden model **až na elementární ekvivalenci**.

Příklad: uspořádané množiny  $\mathcal{A} = \langle \mathbb{Q}, \leq \rangle$  a  $\mathcal{B} = \langle \mathbb{R}, \leq \rangle$ .

- **nejsou izomorfní**,  $\mathbb{Q}$  je spočetná a  $\mathbb{R}$  nespočetná množina, neexistuje dokonce žádná **bijekce** mezi doménami
- **ale  $\mathcal{A} \equiv \mathcal{B}$** : indukcí dle struktury sentence  $\varphi$  lze ukázat  $\mathcal{A} \models \varphi \Leftrightarrow \mathcal{B} \models \varphi$ ; netriviální případ je  $\exists$ , klíčová je **hustota**

# Platnost pomocí nesplnitelnosti

Otázku platnosti v teorii lze převést na problém existence modelu:

**Tvrzení (O nesplnitelnosti a pravdivosti):** Je-li  $T$  teorie a  $\varphi$  sentence (v témž jazyce), potom:  $T \models \varphi \Leftrightarrow T \cup \{\neg\varphi\}$  nemá model.

**Důkaz:** Platí následující ekvivalence:

- $T \cup \{\neg\varphi\}$  nemá model,
- právě když  $\neg\varphi$  neplatí v žádném modelu  $T$ ,
- právě když  $\varphi$  platí v každém modelu  $T$  ( $\varphi$  je sentence!).  $\square$

NB: Předpoklad, že  $\varphi$  je sentence, je nutný: pro  $T = \{P(c)\}$  a formuli  $\varphi = P(x)$  je  $P(c) \not\models P(x)$  ale  $\{P(c), \neg P(x)\}$  nemá model.



Teorie grafů:  $L = \langle E \rangle$  s rovností, axiomy **ireflexivity** a **symetrie**

$$T_{\text{graph}} = \{ \neg E(x, x), E(x, y) \rightarrow E(y, x) \}$$

**Modely:**  $\mathcal{G} = \langle G, E^{\mathcal{G}} \rangle$ , kde  $E^{\mathcal{G}}$  je symetrická ireflexivní relace, tj. **jednoduché** grafy, hranu  $\{x, y\}$  reprezentuje dvojice  $(x, y), (y, x)$

- Formule  $\neg x = y \rightarrow E(x, y)$  platí v grafu, právě když je **úplný**. Je tedy nezávislá v  $T_{\text{graph}}$ .
- Formule  $(\exists y_1)(\exists y_2)(\neg y_1 = y_2 \wedge E(x, y_1) \wedge E(x, y_2) \wedge (\forall z)(E(x, z) \rightarrow z = y_1 \vee z = y_2))$  vyjadřuje, že každý vrchol má stupeň právě 2. Platí tedy právě v grafech, které jsou disjunktní sjednocení kružnic, a je nezávislá v teorii  $T_{\text{graph}}$ .

## Příklady teorií: Teorie uspořádání

Teorie uspořádání: v jazyce uspořádání  $L = \langle \leq \rangle$  s rovností, axiomy **reflexivity**, **antisymetrie**, a **tranzitivity**

$$T = \{x \leq x, x \leq y \wedge y \leq x \rightarrow x = y, x \leq y \wedge y \leq z \rightarrow x \leq z\}$$

**Modely:**  $\langle S, \leq^S \rangle$ , kde  $\leq^S$  je **částečné uspořádání**.

Příklad:  $\mathcal{A} = \langle \mathbb{N}, \leq \rangle$ ,  $\mathcal{B} = \langle \mathcal{P}(X), \subseteq \rangle$  pro  $X = \{0, 1, 2\}$ .

- Formule  $x \leq y \vee y \leq x$  (**linearita**) platí v  $\mathcal{A}$ , ale neplatí v  $\mathcal{B}$ : neplatí např. při ohodnocení kde  $e(x) = \{0\}$ ,  $e(y) = \{1\}$  (píšeme  $\mathcal{B} \not\models \varphi[e]$ ). Je tedy nezávislá v  $T$ .
- Sentence  $(\exists x)(\forall y)(y \leq x)$  (označme  $\psi$ ) je pravdivá v  $\mathcal{B}$  a lživá v  $\mathcal{A}$ , píšeme  $\mathcal{B} \models \psi$ ,  $\mathcal{A} \models \neg\psi$ . Je také nezávislá v  $T$ .
- Formule  $(x \leq y \wedge y \leq z \wedge z \leq x) \rightarrow (x = y \wedge y = z)$  (označme  $\chi$ ) je pravdivá v  $T$ , píšeme  $T \models \chi$ . Totéž platí pro její **generální uzávěr**  $(\forall x)(\forall y)(\forall z)\chi$ .

## Příklady teorií: Algebraické teorie 1/2

Teorie grup:  $L = \langle +, -, 0 \rangle$  s rovností, axiomy asociativita  $+$ , neutralita  $0$  vůči  $+$ , a  $-x$  je inverzní prvek k  $x$  (vůči  $+$  a  $0$ )

$$\begin{aligned}T_1 = \{ & x + (y + z) = (x + y) + z, \\ & 0 + x = x, \quad x + 0 = 0, \\ & x + (-x) = 0, \quad (-x) + x = 0 \}\end{aligned}$$

Teorie komutativních grup: navíc komutativita  $+$

$$T_2 = T_1 \cup \{x + y = y + x\}$$

Teorie okruhů:  $L = \langle +, -, 0, \cdot, 1 \rangle$  s rovností, navíc neutralita  $1$  vůči  $\cdot$ , asociativita  $\cdot$ , a (levá i pravá) distributivita  $\cdot$  vůči  $+$

$$\begin{aligned}T_3 = T_2 \cup \{ & 1 \cdot x = x \cdot 1, \\ & x \cdot (y \cdot z) = (x \cdot y) \cdot z, \\ & x \cdot (y + z) = x \cdot y + x \cdot z, \\ & (x + y) \cdot z = x \cdot z + y \cdot z \}\end{aligned}$$

## Příklady teorií: Algebraické teorie 2/2

Teorie komutativních okruhů: navíc axiom **komutativity**  $\cdot$ :

$$T_4 = T_3 \cup \{x \cdot y = y \cdot x\}$$

Teorie těles je ve stejném jazyce, ale má navíc axiomy **existence inverzního prvku**  $k \cdot$  a **netriviality**:

$$T_5 = T_4 \cup \{\neg x = 0 \rightarrow (\exists y)(x \cdot y = 1), \neg 0 = 1\}$$

Teorie uspořádaných těles je v jazyce  $\langle +, -, 0, \cdot, 1, \leq \rangle$  s rovností, sestává z axiomů teorie těles, teorie uspořádání spolu s axiomem linearity, a z následujících axiomů **kompatibility uspořádání**:

- $x \leq y \rightarrow (x + z \leq y + z)$
- $(0 \leq x \wedge 0 \leq y) \rightarrow 0 \leq x \cdot y$

Modely jsou tělesa s **lineárním (totálním)** uspořádáním, které je kompatibilní s tělesovými operacemi.