Výroková a **pred**ikátová **log**ika
Výpisky z cvičení Martina Piláta

Jan Štětina

1. prosince 2009

Cvičení 29.9.2009

Pojem: *Sekvence* je konečná posloupnost, značíme ji predikátem $seq(x)$.

- $lh(x)$ je délka sekvence x
- $(x)y$ je y-tý prvek x
- $x \sqcup y$ je konkatenace (zřetězení)
- $\bigsqcup(X)$ je konkatenace více sekvencí (z množiny X)
- $\emptyset$ je prázdná sekvence
- $< x_0, ..., x_{n-1} >$ je uspořádaná n-tice
  (pozn., definováno přes množiny: $\{x\}, \{x, y\}$ je uspořádaná dvojice, $\{\{x\}, \{x, y\}\}, \{x, y, z\}$ je uspořádaná trojice, etc; převod zajišťuje funkce $'$: $\emptyset' \to \emptyset, \{x\}' \to \{x\}, s \sqcup < t >' \to \{s, t\}$)
- z^n je množina všech n-tic nad množinou z
- $dom(f)$ pro funkci $f : x \to y$ je n-tice $\Leftrightarrow$ funkce je n-ární
- Relace $r \subseteq z^n$ je n-ární

Poznámka: $f(< a_0, ..., a_{n-1})$ píšeme jako $f(a_0, ..., a_{n-1})$,
$< x_0, ..., x_{n-1} >\in r$ píšeme jako $r(x_0, ..., x_{n-1})$.

Příklad: Relace $<$ na $\mathbb{N}$: $<\subseteq \mathbb{N}^2$, $\quad (1, 2) \in< \equiv < (1, 2) \equiv \underbrace{1 < 2}_{\text{„jako normální lidi“}}$

Pojem: *Obecná notace* je dvojice $\underline{S} =< S, Ar_S >$, kde $\emptyset \notin S$ a $Ar_S : S \to \mathbb{N}$ udává počet argumentů pro $s \in S$.

- $s \in S$ je symbol $\underline{S}$
- $Ar_S(s)$ je četnost (arita) s
- $Ar_S[S]$ je množina četností $\underline{S}$
- Pokud $Ar_S(s) = 0$, je s konstantní symbol

Notace je obecná notace, která má alespoň jeden konstantní symbol, tedy $0 \in Ar_S[S]$

Příklad: $\underline{S} =< S = \{+, \cdot, ^{-1}, 0, <\}, Ar_S >$, pak
$Ar_S(+) = 2, Ar_S(\cdot) = 2, Ar_S(^{-1}) = 1, Ar_S(0) = 0, Ar_S(<) = 2, Ar_S[S] = \{0, 1, 2\}$.

Pojem: *Signatura* je $< \underline{R}, \underline{F} >$, kde $\underline{R}$ je obecná notace (s $0 \in Ar_R[R]$), $\underline{F}$ je obecná notace a $R \cap F = \emptyset$.

- $R = F = \emptyset \Rightarrow$ *prázdná signatura*
- Prvky R se nazývají *relační symboly*
- Prvky F se nazývají *funkční symboly*
- $R = \emptyset \Rightarrow < \underline{R}, \underline{F} >$ je *funkční*
- $F = \emptyset \Rightarrow < \underline{R}, \underline{F} >$ je *relační*

Pojem:z *Struktura* je $\mathcal{A} =< A, R, F >$, kde $A \neq \emptyset, R$ je soubor relací konečných kladných četností a F je soubor operací konečných kladných četností.

- A je *univerzum* v $\mathcal{A}$
- Nulární funkce v A je $\{< \emptyset, c >\}, c \in A$

Cvičení 6.10.2009

Opakování: Vysvětlení přednášky.

Pojem: *Podstruktura*. Mějme $\underline{A} =< A, R, F >, \underline{B} =< B, R', F' >$. $\underline{B}$ je podstruktura $\underline{A}$, pokud platí následující:

1. $B \subseteq A$
2. $R' = \{r \cap B^m; \quad r \in R, Ar_R(r) = m\}$
3. $F' = \{f \cap B^m \times B; \quad f \in F, Ar_F(f) = m\}$
4. B je uzavřeno na $f \quad (f \in F)$.

Pojem: Mějme $\underline{A} =< A, R, F >$, množinu X. *Množina generovaná v $\underline{A}$ z X* je nejmenší podmnožina A obsahující X a uzavřená na operace z $\overline{X}^A$.

Příklad: $X = \emptyset \quad \rightsquigarrow \quad \overline{X}^A = \{\text{konstanty a vše, co tyto generují}\}$
$X = \emptyset, F = \emptyset \quad \rightsquigarrow \quad \overline{X}^A = \emptyset$
$\overline{X}^A \neq \emptyset \Rightarrow$ univerzum nejmenší podstruktury A, $A < X >$ je podstuktura generovaná X.

Téma: *Booleovy algebry*.

Příklad: Zde nejasný zápis.
$\underline{2} =< 2 = \{0, 1\}, -_1, \vee_1, \wedge_1, 0, 1 >, 0, 1$ je nulární, $-_1$ je unární, $\vee_1, \wedge_1$ je binární.
$-_1 : 2 \to 2 \qquad -_1(0) = 1, -_1(1) = 0$
$\vee_1 : 2 \times 2 \to 2 \quad \vee_1(x, y) = \max\{x, y\}$
$\wedge_1 : 2 \times 2 \to 2 \quad \wedge_1(x, y) = \min\{x, y\}$

Pojem: *L-struktura* je $L =< -, \vee, \wedge, 0, 1 >$
$\underline{{}^I 2} =<^I 2, -_I, \vee_I, \wedge_I, 0_I, 1_I >; \qquad -_I :^I 2 \to^I 2; \qquad -_I(x) = -_1(f(x))$
Umožňuje užití operací na výrazy složitější než 0, 1.
Musí splňovat následující ($\diamond$ znamená $\vee$ nebo $\wedge$, $\diamond'$ je opačné než $\diamond$):

1. Asociativita: $x \diamond (y \diamond y) = (x \diamond y) \diamond z$
2. Komutativita: $x \diamond y = y \diamond x$
3. Distributivita: $x \diamond (y \diamond' z) = (x \diamond y) \diamond' (x \diamond z)$
4. Absorpce: $x \vee (x \wedge y) = x = x \wedge (x \vee y)$

5. Komplementace $x \vee (-x) = 1; \quad x \wedge (-x) = 0$

Příklad: $< P(I), \setminus, \cup, \cap, \emptyset, I >$ je booleova algebra. Definováno $\leq^B$: $\quad a \leq^B b \quad \Leftrightarrow a = a \wedge b$.
Operace:

- Rozdíl: $a - b = a \wedge (-b)$
- Symetrická diference: $a \dot{-} b = (a - b) \wedge (b - a)$
- Implikace: $a \rightarrow b = -a \vee b; \qquad a \leftrightarrow b = (a \rightarrow b) \wedge (b \rightarrow a)$

Pojem: Mějme $\mathcal{F}$ množinu funkcí konečné četnosti, X množinu, F n-ární funkci. F-*konkluze* x je $F\lceil x^n \rceil = \{F(x_1, ..., x_n) | < x_1, ..., x_n > \in x^n\}$.
$F : x^n \rightarrow x; \qquad F\lceil x \rceil = rng(F)$

Příklad: $X = \{0, 1, 2\}; \quad F(x) = min\{2, x + 1\}; \qquad \rightsquigarrow F\lceil x \rceil = \{1, 2\}$

$\mathcal{F}$-*konkluze* x je $\mathcal{F}\lceil x \rceil = \bigcup\{F\lceil x \rceil | F \in \mathcal{F}\}$
X je $\mathcal{F}$-*uzavřená*, když $\mathcal{F}\lceil x \rceil \subseteq X$
$\mathcal{F}$-*uzávěr* X je nejmenší nadmnožina X, která je $\mathcal{F}$-uzavřená. Značíme $\mathcal{F} < X >$.
$\mathcal{F}$-*odvození z* X je sekvence s taková, že pro $i \in lh(s)$ je $(s)_i \in X$ nebo $\exists i_0, ..., i_n$ a n-ární $F \in \mathcal{F}$ taková, že $(s)_i = F((s)_{i_0}, ..., (s)_{i_n})$.
s je odvozené $y = (s)_{lh(s)-1}$.
Prvek je $\mathcal{F}$-*odvozený z* $X \equiv$ je posledním členem $\mathcal{F}$-odvození.

Cvičení 13.10.2009

Opakování: Induktivní definice množiny Y.

1. $x \in X \Rightarrow x \in Y$
2. n-ární $g \in \mathcal{F}, < y_1, ..., y_2 > \in Y^n, f(y_1, ..., y_n) \in Y$

Pojem: Realizace signatury $< R, F >$ je struktura $< A, \mathcal{R}^A, \mathcal{F}^A >$:
$\mathcal{R}^A =< R_R : R \in \mathcal{R} >: R_R \subseteq A^{Ar(R)}$
$\mathcal{F}^A =< F_F : F \in \mathcal{F} >: F_F \subseteq A^{Ar(F)}$

Příklad: $< T = \{0, 1, 2\}, +, *, 0, 1, \leq>$
$\leq^T = \{(0, 1), (0, 2), (1, 2)\}; \qquad +^T = \quad 0 + 0 = 0, x + y = (x + y) mod 3$

Pojem: Izomorfismus struktur.
Mějme $\mathcal{A} =< A, R^A, F^A >, \mathcal{B} =< B, R^B, F^B >$. $h : A \rightarrow B$ je isomorfismus $\mathcal{A}$ a $\mathcal{B}$, pokud:

1. h je bijekce.
2. $R \in \mathcal{R}, < a_1, ..., a_n > \in A^n, n = Ar(R) : \quad R^A(a_1, ..., a_n) \Leftrightarrow R^B(h(a_1), ..., h(a_n))$
3. $F \in \mathcal{F}, < a_1, ..., a_n > \in A^n, n = Ar(F) : \quad h(F^A(a_1, ..., a_n)) = F^B(h(a_1), ..., h(a_n))$

Pojem: Aplikační doména.
Mějme $< S, Ar_S >, X$ množinu sekvencí. Pak aplikační doména je $Ad(S, X) = \bigcup_{\mathfrak{s} \in S}\{\{\mathfrak{s}\} \times X^{Ar_S(\mathfrak{s})}\}, \quad < \mathfrak{s}, s >, \mathfrak{s} \in S, s \in X^{Ar_S(\mathfrak{s})}$

Příklad: $S =< +, \cdot, 0, 1 >, X = \{0, 1, 2\}$
$Ad(S, X) = \{(+, < 0, 0 >), (+, < 0, 1 >), (+, < 0, 2 >), ..., (\cdot, < 0, 0 >), ..., (O, \emptyset), ...\}$
Aplikace $< S, Ar_S >$ na $X : Ap_{S,X}(\mathfrak{s}, s) =< \mathfrak{s} > \sqcup s; \qquad Ap_S := Ap_{S,S^*}$

Pojem: Obor výrazů $< S, Ar_S >$ je struktura $\underline{D}^*(S)$ tvaru $< S^*, \mathfrak{s}^0 >$, kde $\mathfrak{s}^0$ je $< \mathfrak{s} | \mathfrak{s} \in S >$.
$\mathfrak{s}^0 : S^{*\,Ar_S(\mathfrak{s})} \to S^*$; $\quad \mathfrak{s}^0(s) = Ap_S(s, s)$ pro $s \in S^{*\,Ar_S(\mathfrak{s})}$

Pojem: Obor designátorů $\underline{D}(S)$ notace $< S, Ar_S >$ je podstruktura $D^A(S)$ generovaná $\emptyset$.

Příklad: $D_1 = \{0, 1\}$; $\quad D_2 = \{+(0, 0), +(0, 1), +(1, 0), +(1, 1), ..., *(0, 0)\}$

$\lightning$: Doplnit!

Téma: Teorie.
Teorie $T \subseteq VF_P$ (prvky T jsou axiomy, $P(T)$ jsou prvovýroky T)

$$\begin{array}{lll} \& : & a\&b & \equiv \neg(a \to \neg b) \\ \vee : & a \vee b & \equiv \neg a \to b \\ \leftrightarrow : & a \leftrightarrow b & \equiv (a \to b) \wedge (b \to a) \\ \dot{-} : & a \dot{-} b & \equiv (a \wedge \neg b) \vee (b \wedge \neg a) \end{array}$$

$\lightning$: Doplnit!

Cvičení 20.10.2009

Téma: Výroková logika.
Ohodnocení je funkce, která vrací 0 nebo 1: $v \in_2^p \varphi \in VF_{\mathbb{P}} = D(\mathbb{P} \cup \{\to, \neg\})$
$v(\varphi) = 1$ ... v je model φ
$T \subseteq VF_{\mathbb{P}}$ ... teorie
$M^{\mathbb{P}}(\varphi) = \{v \in_2^{\mathbb{P}} | v(\varphi) = 1\}$
$M^{\mathbb{P}}(T) = \bigcap_{\varphi \in T} M^{\mathbb{P}}(\varphi)$
$-M^{\mathbb{P}}(T) :=_2^{\mathbb{P}} \setminus M^{\mathbb{P}}(T)$

$\varphi \leftrightarrow \psi \Leftrightarrow M^{\mathbb{P}}(\varphi) = M^{\mathbb{P}}(\psi)$
$\varphi \to \psi \Leftrightarrow M^{\mathbb{P}}(\varphi) \subseteq M^{\mathbb{P}}(\psi)$
$M^{\mathbb{P}}(\varphi \vee \psi) = M^{\mathbb{P}}(\varphi) \cup M^{\mathbb{P}}(\psi)$
$M^{\mathbb{P}}(\varphi \& \psi) = M^{\mathbb{P}}(\varphi) \cap M^{\mathbb{P}}(\psi)$
$M^{\mathbb{P}}(\neg\varphi) = -M^{\mathbb{P}}(\varphi)$

Věta: (2.1.4) Mějme $\mathbb{P}$ konečný, $K \subseteq_2^{\mathbb{P}}$, $M^{\mathbb{P}}(\vee_{\omega \in K} \cdot \wedge_{p \in \mathbb{P}} p^{\omega(p)}) = K$
$p^0 = \neg p$; $\quad p^1 = p$
$K = M^{\mathbb{P}}(\{(p \to q) \vee r\})$

p	q	r	$(p \to q) \vee r$
0	0	0	1
0	0	1	1
0	1	0	1
0	1	1	1
1	0	0	0
1	0	1	1
1	1	0	1
1	1	1	1

$\rightsquigarrow ... \vee (p^0 \wedge q^0 \wedge r^1) \vee (p^0 \wedge q^0 \wedge r^0) \quad \sim \quad ...(\neg p \wedge \neg q \wedge r) \vee (\neg p \wedge \neg q \wedge \neg r)$

$M^{\mathbb{P}}(T, \varphi) = M^{\mathbb{P}}(T, \psi)$ ... T-sémanticky ekvivalentní $\varphi \sim_T \psi$.

Tvrzení: Nechť φ' vznikne z φ nahrazením výskydu podle ψ funkcí ψ'. Pak $\psi \sim \psi' \Rightarrow \varphi \sim \varphi'$.

$\varphi = p$
$\psi \sim \psi' \Rightarrow \varphi \sim \varphi'$

$\varphi = \psi; \qquad \varphi' = \psi'$
$\varphi = \neg\sigma$
σ' vznikla z σ nahrazením ψ za ψ'.
$\sigma \sim \sigma'$ (IP)
$M^{\mathbb{P}}(\neg\sigma) = -M^{\mathbb{P}}(\sigma) = -M^{\mathbb{P}}(\sigma') = M^{\mathbb{P}}(\neg\sigma')$

$\varphi = \sigma \to \xi$
$M^{\mathbb{P}}(\varphi) = -M^{\mathbb{P}}(\sigma) \cup M^{\mathbb{P}}(\xi)$
$\sigma \to \xi \quad \equiv \quad \neg\sigma \vee \xi$
σ' vznikla ...(předpoklad)
$M^{\mathbb{P}}(\sigma') = M^{\mathbb{P}}(\sigma)$ (IP)
ξ' vznikla ... (předpoklad)
$M^{\mathbb{P}}(\xi') = M^{\mathbb{P}}(\xi)$
$M^{\mathbb{P}}(\varphi') = -M^{\mathbb{P}}(\sigma') \cup M^{\mathbb{P}}(\xi')$

Úloha: Mějme teorie $T \subseteq T'$. Jaký je vztah $M(T) \circ M(T')$?

Řešení: $M(T) \supseteq M(T')$
$T' = T \sup S$
$M(T') = M(T \cup S) = M(T) \cap M(S)$

Definice: φ je *pravdivá* v T, když v každém modelu T platí $T \neq \varphi$,
lživá v T, když v každém modelu T platí $T \neq \neg\varphi$.
$\Phi_{\mathbb{P}}(T)$ je množina všech pravdivých výroků v T,
$\Phi'_{\mathbb{P}}(T)$ je množina všech lživých výroků v T.

Tvrzení: $T \subseteq T'$, pak $\Phi_{\mathbb{P}}(T) \subseteq \Phi_{\mathbb{P}}(T')$.
$\varphi \in \Phi_{\mathbb{P}}(T) ... v \models \varphi, v \in M(T) \Rightarrow v \models \varphi, v \in M(T') \Rightarrow \varphi \in \Phi_{\mathbb{P}}(T')$

Tvrzení: $T \subset \Phi_{\mathbb{P}}(T)$
$\Phi_{\mathbb{P}}(T) = \Phi_{\mathbb{P}}(\Phi_{\mathbb{P}}(T))$
$\subseteq$ je triviální, zbývá $\supseteq$:
$\varphi \in \Phi_{\mathbb{P}}(\Phi_{\mathbb{P}}(T))$
$v \neq \varphi, v \in M(\Phi_{\mathbb{P}}(T))$
Odbočka, chceme zjistit vztah $M(T) \circ M(\Phi_{\mathbb{P}}(T))$. $T \models \varphi \Rightarrow M(T) \subseteq M(\varphi)$
$M(T \cup \{\varphi\}) = M(T) \cap M(\varphi) = M(T)$.
Tedy $M(T) = M(\Phi_{\mathbb{P}}(T))$, konec odbočky.
$v \models \varphi, \quad v \in M(T)$
$\varphi \in \Phi_{\mathbb{P}}(T)$

Poznámky: $\top = (p \to p)$ je vždy platný výrok,
$\bot = \neg(p \to p)$ je vždy lživý výrok.
Žádný model ... sporná množina
$M(T, T) = M(T)$
$M(T, \bot) = \emptyset$
$M(\bot) = \emptyset$
$\Phi_{\mathbb{P}}(\bot) = VF_{\mathbb{P}}$
$M(VF_{\mathbb{P}}) = \emptyset$

$(\varphi \to \psi) \to (\neg\psi \to\neq \varphi)$
$T \models \varphi \to \psi \Leftrightarrow T \models \neg\psi \to\neq \varphi$

$T \models P(x) \Rightarrow T \models (\forall x)P(x)$
$T \models P(x) \rightarrow (\forall x)P(x)$

Nezávislá formule: ani pravdivá ani lživá.
$\emptyset\neg \models p$; $\quad \emptyset\neg \models\neq p$
$\Phi_{\mathbb{P}}(\emptyset)$ je tautologie.
$\Phi_{\mathbb{P}}(VF_{\mathbb{P}}) = VF_{\mathbb{P}}$
Konzistentní (splnitelná) formule: není lživá.

Úloha: SAT: Máme formuli v CNF, je splnitelná?
A co v DNF (disjunktivní normální formě), $(a \wedge b \wedge c \wedge \neg d) \vee (a \wedge \neg b \wedge \neq c \wedge \neg d) \vee ... \vee (a \wedge \neg a \wedge b \wedge \neg c)$ - lineární, stačí nalézt jednu splnitelnou klauzuli (závorku).
FALS: Je formule v DNF falzifikovatelná?
CNF splnitelná: NP-úplný problém, DNF splnitelná: $O(n)$. Potíž je ale ve složitosti převodu.

Cvičení 27.10.2009

Úvod: $r \in^{\mathbb{P}} 2 \quad \rightarrow \overline{r} \in^{VF_{\mathbb{P}}} 2$
$\overline{r}(p) = v(p) \quad p \in \mathbb{P}$
$\overline{r}(\neg\varphi) = 1 - \overline{r}(\varphi) \quad \varphi \in VF_{\mathbb{P}}$
$\overline{r}(\varphi \rightarrow \psi) = 1(\quad \overline{r}(\varphi) = 0 \vee \overline{r}(\psi) = 1), 0$ jinak.
$VF_{\mathbb{P}} = D(< \{\neg, \rightarrow\} \cup \mathbb{P}, >); \quad W = 2, U = \emptyset$

Tvrzení: Nechť $< S, Ar_S >$ je notace, U, V množiny, $s \in S$, $n = Ar_S(s)$, $G_s(z_1, ..., z_n, u) : \mathcal{P}(W)^n \times U \rightarrow W$, $G_{s,1}(u), ..., G_{s,n}(u) : U \rightarrow \mathcal{P}(U)$. Potom $\exists! H : D(S) \times U \rightarrow W$ taková, že $H(< s > \sqcup \eta_1 \sqcup ... \sqcup \eta_n, u) = G_s(H[\{\eta_1\} \times G_{s,1}(u)], ..., H[\{\eta_n\} \times G_{s,n}(u)], u)$
$\exists! H : D(S) \rightarrow W; \quad s \in S : G_s(z_1, ..., z_n) : W^n \rightarrow W$
$H(< s > \sqcup \eta_1 \sqcup ... \sqcup \eta_n) = G_s(H(\eta_1), ..., H(\eta_n))$

Téma: Dedukce, axiomy výrokové logiky (množina LAx).

(PL1) $\varphi \rightarrow (\psi \rightarrow \varphi)$

(PL2) $(\varphi \rightarrow (\psi \rightarrow \chi)) \rightarrow ((\varphi \rightarrow \psi) \rightarrow (\varphi \rightarrow \chi))$

(PL3) $(\neg\varphi \rightarrow \neg\psi) \rightarrow (\psi \rightarrow \varphi)$

Pojem: *Modus ponens* aneb pravidlo odloučení, jediné pravidlo výrokové logiky: $MP(\varphi, \varphi \rightarrow \psi) = \psi$ pro $\varphi \in T$

Poznámka: Důkaz $\equiv$ $\{MP\}$-odvození φ z $LAx \cup T$.
$T \vdash \varphi \quad \equiv$ existuje důkaz φ z $LAx \cup T$.

Úloha: Ověřit $\vdash \varphi \rightarrow \varphi$.

Řešení: **(PL1):** $\vdash \varphi \rightarrow (\varphi \rightarrow \varphi)$
(PL2): $\vdash (\varphi \rightarrow ((\varphi \rightarrow \varphi) \rightarrow \varphi)) \rightarrow ((\varphi \rightarrow (\varphi \rightarrow \varphi)) \rightarrow (\varphi \rightarrow \varphi))$
(PL1): $\vdash \varphi \rightarrow ((\varphi \rightarrow \varphi) \rightarrow \varphi)$
(MP): $\vdash (\varphi \rightarrow (\varphi \rightarrow \varphi)) \rightarrow (\varphi \rightarrow \varphi)$
(PL1): $\vdash \varphi \rightarrow (\varphi \rightarrow \varphi)$

(MP): $\vdash \varphi \to \varphi$

Věta: *O dedukci.* Mějme T teorii, φ, ψ funkce, $T \vdash \varphi \to \psi \quad \Leftrightarrow \quad T, \varphi \vdash \psi$

Důkaz: $\Rightarrow \quad T \vdash \varphi \to \psi$

- Mám důkaz z $T: \quad \varphi \to \psi$.
- Přidám kroky φ a MP $\rightsquigarrow \psi$:
- $T \vdash \varphi \to \psi$
  $T, \varphi \vdash \varphi \to \psi$
  $T, \varphi \vdash \varphi$
  $T, \varphi \vdash \psi$

$\square$

$\Leftarrow \quad T, \varphi \vdash \psi$

- $\psi \in T$ je vidět, $\psi = X \to X$ dokázáno dříve.
- Mějme $\varphi_1, ..., \varphi_n$.
- $\varphi_i \in T, \varphi: \quad \varphi = \psi ... T \vdash \psi \to \psi$
- $\psi \in T, \varphi \wedge \psi \neq \varphi:$
  $T \vdash \psi \to (\varphi \to \psi)$
  $T \vdash \psi$
  $T \vdash \varphi \to \psi$
- ψ odvozeno MP z $\chi, \chi \to \psi$
  $T, \varphi \vdash \chi; \qquad T, \varphi \vdash \chi \to \psi$

(IP) $T \vdash \varphi \to \chi, \varphi \to (\chi \to \psi)$

Důkaz úporným tvrzením: platí, platí, platí, platí, platí, platí, platí!

(PL2) $T \vdash (\varphi \to (\chi \to \psi)) \to ((\varphi \to \chi) \to (\varphi \to \psi))$

(2× **MP**) $T \vdash \varphi \to \psi$

$\square$

Úloha: $\vdash \neg\neg\varphi \to \varphi$

Řešení: **[2** :] $\vdash \neg\neg\varphi \to (\neg\varphi \to \neg\neg\neg\varphi)$

(VD): $\neg\neg\varphi \vdash \quad \neg\varphi \to \neg\neg\neg\varphi$

- $(\neg\varphi \to \neg\neg\neg\varphi) \to (\neg\neg\varphi \to \varphi)$

(PL3), MD: $\neg\neg\varphi \vdash \quad \neg\neg\varphi \to \varphi$

ZXVD (?): $\vdash \neg\neg\varphi \to \varphi$

$\square$

Úloha: $\vdash \varphi \to \neg\neg\varphi$

Řešení: ?

Úloha: $\vdash \neg\varphi \to (\varphi \to \psi)$

Řešení: ?

Úloha: $\vdash \varphi \to \varphi$

Řešení: ?

Pojem: *Extenze teorie.*
Mějme teorie S, T. S je extenze T, pokud $\mathbb{P}(T) \subseteq \mathbb{P}(S), \Theta(T) \subseteq \Theta(S)$.

- *Jednoduchá extenze* je, když navíc platí $\mathbb{P}(T) = \mathbb{P}(S)$.
- T je *kompletní*, jestliže má model a pro každou $\varphi : T \models \varphi$ nebo $T \models \neg\varphi$.

Tvrzení: T je kompletní $\Leftrightarrow$ má právě jeden model.

Důkaz: $\Rightarrow$: $v, w \in M(T), v \neq w \quad \exists p \in \mathbb{P} : v(p) \neq w(p)$
- $T \neg \models p$ ani $T \neg \models \neg p$.

Tvrzení: Teorie má model $\Leftrightarrow$ každá její konečná část má model.

Důkaz: $\Rightarrow$: triviální.

$\Leftarrow$: Použijeme princip maximality, máme-li strukturu $< A, \leq >$, jejíž každá lineárně uspořádaná podmnožina má maximum (majorantu), potom v A existuje největší prvek. OBRÁZEK.

- Vezměme T konečně splnitelnou (každá konečná podmnožina má model), strukturu $< \{T'; T'$ konečně splnite $T'\}, \subseteq >$
- $\Rightarrow$ (PM) existuje S maximální konečně splnitelná.
- Má S model? Potřebujeme dokázat následující:

(a): $(\varphi \in S, \varphi \to \psi \in S) \Rightarrow \psi \in S$
Vezmeme $v \in M(\varphi, \varphi \to \psi) \quad \Rightarrow \quad v(\psi) = 1 \quad \Rightarrow \quad v \in M(\varphi, \varphi \to \psi, S', \psi) \quad \Rightarrow \quad S \cup \{\psi\}$ je konečně splnitelná $\Rightarrow \psi \in S$, jinak spor s maximalitou S.

(b): $\varphi \in S \Leftrightarrow \neg\varphi \notin S$
$\Rightarrow$: $\{\varphi, \neg\varphi\}$ nemá model $\Rightarrow$ spor s konečnou splnitelností.

$\Leftarrow$: $\neg\varphi \notin S \quad \rightsquigarrow$? $S \cup \{\varphi\}$ je konečně splnitelná.
- S_0 konečná $\subseteq S$ tž. $S_0 \cup \{\neg\varphi\}$ nemá model.
- S' konečná $\subseteq S \quad \exists v \models S_0 \cup S'$.
- $v(\varphi) = 1$

(c): $(\varphi \to \psi \in S) \Leftrightarrow (\neg\varphi \in S \vee \psi \in S)$
$\Rightarrow$: $\neg\varphi \notin S \quad \Rightarrow \quad \varphi \in S$ a $\psi \in S$ podle (a).
$\Leftarrow$: $\neg\varphi \in S$ pro $S' \subseteq S$ konečnou $\exists$ model $v \models S' \cup \{\neg\varphi\}, \quad v \models S' \cup \{\neq \varphi\} \cup \{\varphi \to \psi\}$

- Vezmeme ohodnocení v: $v(p) = 1 \Leftrightarrow p \in S$
$\square$

Pojem: *Axiomatizovatelnost.*
$K \subseteq^{\mathbb{P}} 2$ je axiomatizovatelná $\equiv \quad \exists$ teorie $T : K = M(T)$
Funkce $\sigma \subseteq \mathbb{P} \times 2 \quad ...\tilde{\sigma} = \{v \in^{\mathbb{P}} 2 | \sigma \subseteq v\}$
$\epsilon_\sigma := \bigwedge_{p \in dom(\sigma)} p^{\sigma(p)} \qquad \tilde{\sigma} = M(\epsilon_\sigma)$

Pro $K \subseteq^{\mathbb{P}} 2$:

1. v je *oddělená od* K, když existuje $\sigma \subseteq v$ konečné, $\tilde{\sigma} \cap K = 0$

2. K je *uzavřená*, když obsahuje každé v, které není oddělené od K
3. K je *otevřená*, když ${}^{\mathbb{P}}2 \setminus K$ je uzavřená
4. K je *obojetná*, když K i její $-K$ jsou uzavřené

Z toho plyne následující:

(K1) **(a)** Průnik uzavřených je uzavřený.
(b) Sjednocení konečně uzavřených je uzavřené.

(K2) **(a)** $v \in^{\mathbb{P}} 2 \setminus K$ je oddělená $\Leftrightarrow$ $\exists \psi$ takové, že $v \in M(\psi) \wedge M(\psi) \cap K = \emptyset$
(b) K je uzavřená $\Leftrightarrow$ $\forall v \in^{\mathbb{P}} 2 \setminus K \quad \exists \psi$ s $v \in M(\psi) \wedge M(\psi) \cap K = \emptyset$.

Věta: $K \subseteq^{\mathbb{P}} 2$ je konečně axiomatizovatelná $\Leftrightarrow$ ona i komplement jsou axiomatizovatelné.

Důkaz: $\Rightarrow$**:** i σ_ϵ triviální.
$\Leftarrow$**:** $K = M(T) = -M(S)({}^{\mathbb{P}}3 \setminus K = M(S))$, potom $M(T \cup S) = M(T) \cap M(S) = \emptyset$,
(o kompaktnosti): $\exists$ konečná $T' \subseteq T$ a $S' \subseteq S$ tž. $M(T' \cup S') = M(T') \cap M(S') = \emptyset$.

- Chceme $M(T) = M(T')$, $M(T') \supseteq M(T)$ víme ($T' \subseteq T$).
- $M(T') \subseteq -M(S') \subseteq -M(S) = M(T) \quad \Rightarrow M(T') = M(T) = K$

□

Věta: $K \subseteq^{\mathbb{P}} 2$ je axiomatizovatelná $\Leftrightarrow$ je uzavřená.

Důkaz: $\Leftarrow$**:** Podle (K2b) je $-K = \bigcup_{\varphi \in S} M(\varphi)$ pro jistou S.

- Potom $K = \bigcap_{\varphi \in S} M(\neg\varphi)$ a tedy $K = M(T)$, kde $T = \{\neg\varphi, \varphi \in S\}$.

$\Rightarrow$**:**
Lemma: Pro funkci φ : $M(\varphi)$ je uzavřená (pro $v \in^{\mathbb{P}} 3 \setminus M(\varphi)$)
je $v \in M(\neg\psi_i)$, přičemž $\varphi \equiv \bigvee_i \psi_i$ (DNF + (K2b)) ($v \in M(\neg\varphi)$)

- $K = M(T) = \bigcap_{\varphi \in T} M(\varphi)$+ (K1a)

□

Věta: K je konečně axiomatizovatelná $\Leftrightarrow$ je obojetná

Důkaz: Vyplývá z předchozích dvou vět. □

Cvičení 10.11.2009

Věta: Mějme φ, ψ funkce, T teorii. Pak platí následující:

(1.a) T je sporná $\Leftrightarrow$ v T je dokazatelný spor.

(1.b) $T, \neg\varphi$ sporná $\Leftrightarrow T \models \varphi$

Důkaz:

(1.a) „$\Rightarrow$“ zřejmé.
„$\Leftarrow$“: $T \models \varphi, \neg\varphi \models\neq \varphi \to (\varphi \to \psi)$ dle (2.2.5.a)
$\models \varphi \to \psi$ (MP)
$T \models \psi$ (MP)

(1.b) „$\Rightarrow$“ $T, \neq \varphi \models \varphi$ (spornost)
$T \models \neq \varphi \to \varphi$
$\models (\neq \varphi \to \varphi) \to \varphi$ dle (2.2.5.e)
$T \models \varphi$
„$\Leftarrow$“ $T \models \varpi \to (\neg\varphi \to \psi)$ dle (2.2.5.a)
$T \models \varphi$ (předpis)
$T \models \neq \varphi \to \psi$ (MP)
$T, \neq \varphi \models \psi$ (VD)

(2) T je maximální bezesporná teorie

(2.a) $T \models \varphi \Leftrightarrow \varphi \in T \Leftrightarrow T, \varphi$ je bezesporná.

(2.b) $\varphi \in T \Leftrightarrow \neq \varphi \notin T; \quad \varphi \to \psi \in T \Leftrightarrow \neq \varphi \in T \vee \psi \in T$

(2.c) Ohodnocení $v : v(p) = 1$ pro p prvovýrok, $p \in T$ je jediný model T.

Důkaz:

(2.a) triviální.

(2.b) $\neg\varphi \notin T \Leftrightarrow T, \neq \varphi$ je sporná $\Leftrightarrow T \models \varphi \Leftrightarrow \varphi \in T$

(2.b.1) „$\Rightarrow$“ $\varphi \to \psi \in T; \quad \neg\varphi \notin T \Leftrightarrow \varphi \in T \Leftrightarrow T \models \varphi \Rightarrow T \models \psi$ (MP) $\Rightarrow \psi \in T$
„$\Leftarrow$“ $\neg\varphi \in T \Rightarrow \models \neg\varphi \to (\varphi \to \psi)$(2.2.5.?) $\Rightarrow T \models \varphi \to \psi$ (MP) $\Rightarrow \varphi \to \psi \in T$
$\psi \in T \Rightarrow T, \varphi \models \psi \Rightarrow T \models \varphi \to \psi$ (VD)

(2.c) Vezmeme $w \in^{\mathbb{P}} 3 : w \models T; \quad w \models p \ldots \omega = v$
Kdyby $w \models q$ prvovýrok $q \notin T$, $T \cup \{q\}$ byla bezesporná.

(3) Bezesporná teorie T má maximální bezesporné rozšíření.

Důkaz: Princip maximality.
$< \{S \supseteq T | S$ bezesporná$\}, \subseteq >$
Podle (PM) existuje maximální prvek.

(4) T má model $\Leftrightarrow$ je bezesporná.

Důkaz: „$\Rightarrow$“ má model v $T + \varphi \quad \rightsquigarrow v(\varphi) = 1 \Rightarrow v(\neg\varphi) = 0 \Rightarrow T\neg \models \neg\varphi$
„$\Leftarrow$“ Bezesporná $\Rightarrow$ existuje maximální bezesporné rozšíření $S \supseteq T \Rightarrow$ (2.a) S má model $\Rightarrow T$ má model.

(5) Teorie T má model $\Leftrightarrow$ každá konečná podteorie má model.

Důkaz: T má model $\Leftrightarrow T$ je bezesporná $\Leftrightarrow$ každá konečná podteorie je bezesporná $\Leftrightarrow$ každá konečná podteorie má model.

(6) $T \models \varphi \Leftrightarrow T \models \varphi$

Důkaz: „$\Rightarrow$“ víme (korektnost)
„$\Leftarrow$“ $T \models \varphi$ ... $T, \neq \varphi$ je sporná === $M(T) \subseteq M(\varphi)$...$M(T, \neq \varphi) = M(T) \cap M(\neq \varphi) = \emptyset$ $T, \neq \varphi$ je sporná$\Rightarrow T \models \varphi$

Úloha: Kolik existuje neekvivalentních teorií nad $\mathbb{P} : |\mathbb{P}| = l$?

Řešení: 2^l je počet ohodnocení ${}^{\mathbb{P}}2$
$T \sim S \Leftrightarrow M(T) = M(S)$
$|\mathcal{P}({}^{\mathbb{P}}2)| = 2^{2^l}$

Kolik je kompletních neekvivalentních teorií?

Řešení: T kompletní $\Leftrightarrow$ má jeden model $\rightsquigarrow 2^l$

Kolik je neekvivalentních pravdivých výroků T?

Řešení: Počet ohodnocení $|{}^{\mathbb{P}}2|$. $(T \models \varphi, \quad M(T) \subseteq M(\varphi))$ $2^{|{}^{\mathbb{P}}2|-|M(T)|}$

Kolik je neekvivalentních nezávislých výroků teorie T?

Řešení: Všechny − pravdivé a lživé (pravdivé negované)
$2^{2^l} - 2 \cdot 2^{2^l - M(T)} = 2^{2^l - M(T)} \cdot (-2 + 2^{|M(T)|})$

Téma: Predikátová logika.

Definice: Jazyk je tvořen

- logickými symboly $(\underbrace{\neg, \rightarrow,}_{\text{spojky}} \underbrace{\quad\forall\quad}_{\text{kvantifikátory}})$
- mimologické symboly $(< \mathcal{R}, \mathcal{F})$
- proměnné (Var)
- symbol $=$

Definice: Term

1. $x \in Var$ je term
2. t_i, x je term a $f \in \mathcal{F}$ arity $n \Rightarrow f(t_1, ..., t_n)$ je term

Definice: Atomická formule.
$t_1, ..., t_n$ termy, $P \in \mathcal{R} \Rightarrow P(t_1, ..., t_n)$ je atomická preformule $A^P Fm_L$

Definice: Formule.

1. Preformule je formule.
2. φ, ψ jsou formule, x je proměnná. Potom $\varphi \rightarrow \psi; \neq \varphi, (\forall x)\varphi$ jsou formule.
   $D(A^P Fm_L \cup \{\rightarrow, \neg\} \cup \{(\forall x) | x \in Var\})$

Cvičení 24.11.2009

Definice: Nechť $L =< R, F >$, pak velikost množiny L-termů je $max\{\omega, |F|\}$.

Poznámka: ω odpovídá mohutnosti Var (tedy i $\mathbb{N}$).
$|\omega \times \omega| = |\omega|, |\mathbb{Q}| = |\mathbb{N}|, |\mathbb{R}| > |\mathbb{N}|, |\mathbb{R} \times \mathbb{N}| = |\mathbb{R}|, |[0, 1]| = |[0, 1] \times [0, 1]|$

Cvičení 1.12.2009

Příklad: Jazyk $L =< \mathcal{R}, \mathcal{F} >$,
termy například $x_1, x_2, x_3, f(x_1, x_2), f(F(x_1, x_2), x_2)$,
atomická formule $A^p Fm_L$, například $P(x_1, f(x_1, x_2), x_3)$,

Definice: Přehled základních pojmů.

Formule: $D(A^p Fm_L \cup \{\to, \neq\} \cup \} \forall x : x \in Var\})$.

Jazyk L s = je teorie rovností.

Teorie v L s = bez mimologických axiomů.

Výskyt x je vázaný v φ: výskyt v podformuli $(\forall x)\psi ... \varphi$

Volné ≡ nevázané.

Proměnná je volná ≡ má volný výskyt, vázaná ≡ má vázaný výskyt.

Např: $(\forall x)P(x) \to x = 1$.

Uzavřená formule nemá volné proměnné (sekvence), otevřená formule nemá vázané proměnné (bez kvantifikátorů).

Substituce formule φ, dosazení t za volnou proměnnou x: $\varphi(x/t) \dots \varphi(t)$.

Formule, na níž jsou aplikovány substituce, je instance.

Varianta formule: nahrazení vázané proměnné $(\forall x)\varphi \dots (\forall y)\varphi(x/y)$, kde y není volné ve φ.

Definice: Realizace (model) jazyka.

Mějme jazyk $L =< \mathcal{R}, \mathcal{F} >$, jeho realizace je L-struktura $< A, \mathcal{R}^A, \mathcal{F}^A >$. Pokud L je s =, pak $=^A$ je =.

Definice: Jazyky $L \subseteq L'$, A' je L'-struktura.

Pak redukce A' na $L(A'|L)$ je struktura s vynechanými symboly, které nejsou v L.

Definice: Mějme jazyk $L =< \mathcal{R}, \mathcal{F} >, \mathcal{A} =< A, R^A, F^A >$ jeho realizaci pak ohodnocení je $e : Var \to \mathcal{A}$.

$e(x/a)$ je stejné jako e, akorát $e(x) = a$.

Definice: Hodnota termu v A při ohodnocení e je $H^A_{tm}(x, e) = e(x)$, kde x je proměnná, $H^A_{tm}(t, e) = F^A(H^A_{tm}(t_1, e), \dots, H^A_{tm}(t_n$

pro $F \in \mathcal{F}$ a četnosti n, $t = F(t_1, \dots, t_n)$.

Příklad : $< \mathbb{N}, + >, e(x) = 0, e(y) = 1$. Termy: $H^{\mathbb{N}}_{tm}(x) = 0, H^{\mathbb{N}}_{tm}(y) = 1,\ x + y = +^{\mathbb{N}}(H^{\mathbb{N}}_{tm}(x, e), H^{\mathbb{N}}_{tm}(y, e)) =$
$+^{\mathbb{N}}(0, 1) = 1$

Definice: Hodnota atomické formule $R(t_1, \dots, t_n)$ jazyka L v ohodnocení e je $H^A_{at}(\varphi, e) = 1$, když $R^A(t_1[e], \dots, t_n[e])$ platí (tedy $(t_1[e], \dots, t_n[e]) \in R^A$), 0 jinak.

Definice: Hodnota $H^A(\varphi, e)$ formule φ v A při e je

- $H^A_{At}(\varphi, e)$ pro φ atomickou.
- $-_1 H^A(\varphi_0)$ pokud φ_0 je $\neq \varphi$.
- $H^A(\varphi_0) \to_1 H^A(\varphi_1)$, pokud φ je $\varphi_0 \to \varphi_1$.
- $min(\{H^A(\varphi_0, e(x/a)), a \in A\})$ pro $\varphi = (\forall x)\varphi_0$.

Definice: Formule φ platí v A při e, když $H^A(\varphi, e) = 1$; $\quad A \models \varphi[e]$.

Formule φ platí v A, když platí v každém ohodnocení e, $A \models \varphi$.

Definice: Nechť T je teorie v jazyce L, $A \models \varphi$ pro každou $\varphi \in T$, pak A je model T, $A \models T$.

Příklad: $(\forall x)(x \leq y) \to (f(x) = 0)$.

Jazyk $L =< f, \leq >$ (f unární funkce, $\leq$ je binární relace), realizace $\mathcal{A} =< A, f^A, \leq^A >$:

$A = \{0, 1, 2\},\ f^A = \{(0, 0), (1, 0), (2, 1)\},\ \leq^A = \{(0, 0), (0, 1), (1, 1), (1, 2), (0, 2), (2, 2)\}$

$e(x) = 1,\ e(y) = 2$.

$H^A(\varphi, e) =$

- $(\forall x)(x \leq y) \rightarrow (f(x) = 0)$
- $(\forall x)(x \leq 2) \rightarrow \underbrace{(f(1) = 0)}_{1}$
- $min(0 \leq 2, 1 \leq 2, 2 \leq 2) = 1$
- $1 \rightarrow_1 1$
- 1

Platí v A, pokud platí pro všechna ohodnocení e.

Věta: Nechť A je L-struktura, t, s termy, φ formule jazyka L, e ohodnocení proměnných v A. Potom:

- $t(x/s)[e] = t[e(x/s[e])]$.
  Příklad, $f(x)(x/f(y))[e] = f(f(y))[e] = f(f(y)[e]) = f(x)[e(x/f(y)[e])] = f(f(y)[e])$.
- $A \models \varphi(x/s)[e] \Leftrightarrow A \models \varphi[e(x/s[e])]$.
-

Lemma: ...
Mějme $L \subseteq L', A' \models L', A$ redukt A na L, e ohodnocení v A, resp. v A'. Potom platí:

1. Pro L-term t je $t^A[e] = t^{A'}[e]$.
2. Pro formule je $A \models \varphi[e] \Leftrightarrow A' \models \varphi[e]$.