TÉMATICKÉ PROBLÉMY

Jde o okruhy tvrzení, dokazatelných s využitím poznatků z přednášky.

Booleovské univerzum množin a booleovsky izomorfní struktury.

Pracuje se v teorii ZFC; jejím jazykem je $\in$-jazyk $\langle \in \rangle$. Formule (jazyka s $\in$) je *omezená*, jsou-li v ní jen omezené kvantifikace (tvaru $(Qx \in y)$) a je Σ_1, je-li sestavena jen z atomických a negací atomických formulí pomocí $\vee, \wedge, (\forall x \in y), (\exists x)$. V ZFC je každá Σ_1-formule ekvivalentní formuli tvaru $(\exists \overline{z})\varphi$ s jistou omezenou formulí φ.

• Buď B kompletní Booleova algebra. *B-booleovské univerzum* $\mathrm{V}^{(B)}$ je třída $\bigcup_{\alpha \in \mathsf{On}} \mathrm{V}_\alpha^{(B)}$, kde $\mathrm{V}_\alpha^{(B)} = \{u;\ u$ je funkce & $\mathrm{rng}(u) \subseteq B$ & $(\exists \beta < \alpha)(\mathrm{dom}(u) \subseteq \mathrm{V}_\beta^{(B)})\}$. (Je $\mathrm{V}_0^{(B)} = \emptyset$). *Kanonické vnoření* $\check{}: \mathrm{V} \to \mathrm{V}^{(B)}$ definujeme $\in$-rekurzí: $\check{x} = \{\langle \check{y}, 1\rangle;\ y \in x\}$. *$B$-formule* jsou formule $\in$-jazyka, rozšířeného o jména c_a prvků $a \in \mathrm{V}^{(B)}$; pišme jen a místo c_a. Jde tedy o formule tvaru $\varphi(x_0/a_0, \ldots, x_{n-1}/a_{n-1})$, kde φ je $\in$-formule, a_i jsou z $\mathrm{V}^{(B)}$.

• Pro $\in$-formuli $\varphi(\overline{x})$ definujeme třídové zobrazení $\|\varphi(\overline{x})\| : (\mathrm{V}^{(B)})^{\mathrm{l}(\overline{x})} \to B$ následovně indukcí dle složitosti φ, přičemž $\|\varphi(\overline{x})\|(\overline{a})$ značíme $\|\varphi(\overline{a})\|$, obšírněji $\|\varphi(\overline{a})\|^B$ a říkáme, že to je *booleovská hodnota* B-sentence $\varphi(\overline{a})$. Pro atomické formule $x \in y$, $x = y$ definujme $\|x \in y\| : (\mathrm{V}^{(B)})^2 \to B$ a $\|x = y\| : (\mathrm{V}^{(B)})^2 \to B$: (B1) $\|a \in b\| = \bigvee_{d \in \mathrm{dom}(b)} b(d) \wedge \|d = a\|$,
(B2) $\|a = b\| = \bigwedge_{c \in \mathrm{dom}(a)} (a(c) \to \|c \in b\|)\ \wedge \bigwedge_{d \in \mathrm{dom}(b)} (b(d) \to \|d \in a\|)$.
Definici je fundovanou rekurzí na základě relace R: $\langle c, d\rangle\, R\, \langle a, b\rangle \leftrightarrow c \in \mathrm{dom}(a)$ & $d \in \mathrm{dom}(b)$.
Dále definici rozšíříme níže uvedenými rovnostmi (B3), (B4), kde $\diamond$ je logická spojka (unární $\neg$, binární $\vee, \wedge, \to, \leftrightarrow$), $\diamond^B$ odpovídající operace v B a $\Diamond$ je $\exists\,[\forall]$, $\Diamond^B$ je $\bigvee [\bigwedge]$ algebry B:
(B3) $\|([\varphi] \diamond \psi)(\overline{a})\| = [\|\varphi(\overline{a})\|] \diamond^B \|\psi(\overline{a})\|$, (B4) $\|(\Diamond x)\varphi(x, \overline{a})\| = \Diamond^B \{\|\varphi(b, \overline{a})\|;\ b \in \mathrm{V}^{(B)}\}$.

• B-formule φ *je pravdivá* ve $\mathrm{V}^{(B)}$, když $\|\forall$-uzávěr $\varphi\| = 1$; pokud φ je B-sentence, píšeme $\mathrm{V}^{(B)} \models \varphi$. Pravidlo odvozování je *validní* ve $\mathrm{V}^{(B)}$, zachovává-li pravdivost formulí ve $\mathrm{V}^{(B)}$.

Platí:

Buď B' kompletní podalgebra kompletní algebry B. Pak

0) *Axiomy predikátové logiky s rovností jsou pravdivé a deduktivní pravidla jsou validní ve* $\mathrm{V}^{(B)}$.

1) a) $\mathrm{V}^{(B')} \subseteq \mathrm{V}^{(B)}$. b) *Pro každou* omezenou *B'-sentenci σ platí* $\|\sigma\|^{B'} = \|\sigma\|^B$.

2) *Zobrazení $x \mapsto \check{x}$ je izomorfizmus struktur* V *a* $\mathrm{V}^{(2)}$.

3) *Pro $\in$-formuli $\varphi(\overline{x})$ platí:* $\varphi(\overline{x}) \leftrightarrow \mathrm{V}^{(2)} \models \varphi(\check{\overline{x}})$.
Když φ je Σ_1 resp. omezená, platí: $\varphi(\overline{x}) \leftrightarrow \mathrm{V}^{(B)} \models \varphi(\check{\overline{x}})$ *resp.* $\varphi(\overline{x}) \to \mathrm{V}^{(B)} \models \varphi(\check{\overline{x}})$.

4) (Princip maxima.) *Pro každou B-formuli $\varphi(x)$ existuje $a \in \mathrm{V}^{(B)}$ s* $\|(\exists x)\varphi\| = \|\varphi(a)\|$.

5) *Axiomy* ZFC *jsou pravdivé ve* $\mathrm{V}^{(B)}$.

• Základní booleovské operace jsou $0, 1$ nulární, $-$ unární, $\vee, \wedge$ binární. Buď $A \neq \emptyset$ množina. *Extraktor (v A)* je operace $o : \mathcal{P}(A) \to \mathcal{P}(A)$ taková, že $o(o(X)) = o(X)$ pro $X \subseteq A, o(\emptyset) = \emptyset, o(A) = A$. Je *booleovský*, když navíc pro každé X, Y z $\mathrm{rng}(o)$ platí $o(X \cap Y) = o(X) \cap o(Y)$, $o(X \cup o(A - X)) = A$, $o(A - X) \subseteq A - X$. Symbol $\mathrm{B}(o)$ značí strukturu s univerzem $\mathrm{rng}(o)$ a základními booleovskými operacemi $\diamond$, kde $[X] \diamond Y = o([X] \diamond^{\mathcal{P}(A)} Y)$.

• Dvě struktury $\mathcal{A}, \mathcal{B}$ téže signatury jsou *D-izomorfní*, kde D je nějaká kompletní Booleova algebra, platí-li $\mathrm{V}^{(D)} \models \check{\mathcal{A}} \cong \check{\mathcal{B}}$; píšeme $\mathcal{A} \cong_D \mathcal{B}$. Dále $\mathcal{A}, \mathcal{B}$ jsou *Booleovsky izomorfní*, píšeme $\mathcal{A} \cong_{Bool} \mathcal{B}$, existuje-li D s $\mathcal{A} \cong_D \mathcal{B}$.

Problémy.

a) Pro booleovský extraktor o je $\mathrm{B}(o)$ kompletní Booleova algebra. Její průsek je $\cap$, kanonické uspořádání je $\subseteq$ a pro $\emptyset \neq S \subseteq \mathrm{B}(o)$ je $\inf_{\mathrm{B}(o)} S = o(\bigcap S)$ a $\sup_{\mathrm{B}(o)} S = o(\bigcup S)$.

b) Buď $\langle P, \leq\rangle$ neprázdné uspořádání. Pro $X \subseteq P$ buď $o(X) = \{x \in P;\ y \leq x \to \hat{y} \cap X \neq \emptyset\}$. Pak o je booleovský extraktor v P. Algebru $\mathrm{B}(o)$ značíme $\mathrm{B}(P)$ či $\mathrm{B}(P, \leq)$. ($\hat{y} = \{x \in P;\ x \leq y\}$.)

c) Buďte $\mathcal{A} = \langle A, R\rangle$, $\mathcal{B} = \langle B, S\rangle$ struktury, R, S binární a D buď kompletní Booleova algebra. Pak $\mathcal{A}$ a $\mathcal{B}$ jsou D-izomorfní, právě když existují $u_{ab} \in D$ s $a \in A, b \in B$ tak, že pro každé $a, a' \in A$, $b, b' \in B$ platí

$$\textstyle\bigvee_{b\in B} u_{ab} = 1, \quad u_{ab} \wedge u_{ab'} = 0 \text{ pro } b \neq b', \quad \bigvee_{a\in A} u_{ab} = 1, \quad u_{ab} \wedge u_{a'b} = 0 \text{ pro } a \neq a', \tag{1}$$

$$u_{ab} \wedge u_{a'b'} = 0, \text{ jakmile } R(a, a') \not\leftrightarrow S(b, b'). \tag{2}$$

Návod. Nedokazujte.

d) Buďte $\mathcal{A} = \langle A, R\rangle$, $\mathcal{B} = \langle B, S\rangle$ struktury, R, S binární. Pak platí

$$\mathcal{A} \equiv_{L_{\infty\omega}} \mathcal{B} \;\Leftrightarrow\; \mathcal{A} \cong_{Bool} \mathcal{B}.$$

Návod. Užijte c). Pro $\Rightarrow$ buď $\mathcal{A} \hookrightarrow_s \mathcal{B}$ via $\langle \mathcal{H}\rangle$; užijte $\langle \mathcal{H}, \supseteq\rangle$. Pro $\Leftarrow$ buď $\mathcal{A} \cong_D \mathcal{B}$, $\mathcal{H} = \{h_u;\, 0 \neq u \in D\}$, kde $h_u = \{\langle a, b\rangle \in A \times B;\, u \leq u_{ab}\}$.

O P-teoriích.

P-*teorie* je extenze Peanovy aritmetiky v konečném jazyce, obsahující všechny axiomy indukce

$$\varphi(x/0) \;\&\; (\forall x)(\varphi \to \varphi(x/\mathrm{S}x)) \to \varphi.$$

Je to IS-teorie a tedy poskytuje aritmetizaci. Její extenze o definice je zřejmě opět P-teorie. Když $\overline{u}$ je n-tice $u_0, \dots, u_{n-1}$ proměnných, formuli $\bigwedge_{i<n} u_i < x$ zapisujeme stručně jako $\overline{u} < x$.

Problémy.

a) Nechť T je konzistentní P-teorie. Pak v nějaké extenzi T' teorie T o definice existuje binární funkční symbol G takový, že pro každý $L(T)$-term $t(\overline{u})$ obsahující nejvýše n funkčních symbolů platí

$$T' \vdash \overline{u} < x \to t(\overline{u}) < G(x, \underline{n}), \qquad T' \vdash y < y' \to G(x, y) < G(x, y').$$

Návod. Ukažte, že v jisté extenzi T_0 teorie T o definice je unární funkční symbol H takový, že pro každý funkční symbol f z $L(T)$ platí $T_0 \vdash \overline{u} < y \to f(\overline{u}) < H(y)$. V T_0 definujte G rekurzí; zdůvodněte, proč to lze.

b) Neexistuje otevřená konzistentní P-teorie. *Návod.* Buď T otevřená konzistentní P-teorie, $\mathcal{A} \models T$ s „nekonečným“ $a \in A - \{(\underline{n})^{\mathcal{A}};\, n \in \mathbb{N}\}$ a $\mathcal{A}_0$ podstruktura $\mathcal{A}$, generovaná prvkem a. Pomocí a) odvoďte spor.

c) Existuje-li konečně axiomatizovaná konzistentní P-teorie, existuje i otevřená konečně axiomatizovaná konzistentní P-teorie. *Návod.* Nechť $\{(\exists y)\varphi(\overline{x}, y)\}$ je axiomatika konzistentní P-teorie T. Ukažte, že pak existuje konzistentní P-teorie T' v jazyce $L(T) \cup \{f\}$ s axiomatikou $\{\varphi(\overline{x}, y/f(\overline{x}))\}$.

Parciálně rekurzivní funkce.

Funkce resp. relace je nadále nějaká n-ární parciální funkce $F : \mathbb{N}^n \nrightarrow \mathbb{N}$ resp. relace $R \subseteq \mathbb{N}^n$; F je totální, je-li $\mathrm{dom}(F) = \mathbb{N}^n$. Graf $\mathcal{G}_F$ funkce F je $(n+1)$-ární relace $\{\langle \overline{a}, F(\overline{a})\rangle;\, \overline{a} \in \mathrm{dom}(F)\}$ (což je ovšem množinová prezentace funkce F). Je-li F' funkce, místo (množinové rovnosti) $F = F'$ se píše také $F(\overline{x}) \simeq F'(\overline{x})$. Charakteristická funkce relace R je $\mathrm{K}_R(\overline{a}) = 0$ resp. 1, je-li $R(\overline{a})$ resp. $\neg R(\overline{a})$. Je-li $G : \mathbb{N}^{n+1} \nrightarrow \mathbb{N}$, $k \in \mathbb{N}$, tak $F(\overline{a}) \simeq \mu x(G(\overline{a}, x) = k$ značí, že

$$F(\overline{a}) = x \leftrightarrow G(\overline{a}, x) = k \;\&\; (\forall x' < x)(\exists y)(y \neq k \;\&\; G(\overline{a}, x') = y);$$

říkáme, že F je definováno μ-operací (funkčního vztahu) $G(\overline{a}, x) = k$. Dále μ-operace relace $R(\subseteq N^{n+1})$ je n-ární parciální funkci $G = \{\langle \overline{a}, x\rangle;\, R(\overline{a}, x) \;\&\; (\forall y < x)\neg R(\overline{a}, y)\}$; píšeme pak také $G(\overline{a}) \simeq \mu x R(\overline{a}, x)$. Platí $\mu x R(\overline{a}, x) \simeq \mu x(\mathrm{K}_R(\overline{a}, x) = 0)$ a $F(\overline{a}) \simeq \mu x \mathcal{G}_F(\overline{a}, x)$. Když G resp. R je $(n+1)$-ární funkce resp. relace, řekneme, že jsou *speciální*, platí-li $(\forall \overline{a})(\exists x)G(\overline{a}, x) = 0$ resp. $(\forall \overline{a})(\exists x)R(\overline{a}, x)$. Zřejmě: Je-li $G(\overline{a}, x)$ speciální funkce, je $G(\overline{a}, x) = 0$ speciální relace. Je-li G resp. R speciální $n+1$-ární, je $\mu x(G(\overline{a}, x) = 0)$ resp. $\mu x R(\overline{a}, x)$ totální n-ární funkce.

Obor rekurzivních funkcí je nejmenší množina obsahující základní rekurzivní funkce $\mathrm{S}(x)$, $\mathrm{I}_i^n(x_1, \dots, x_n)$, $x + y$, $x \cdot y$, $\mathrm{K}_<$, která je uzavřena na skládání a μ-operaci speciálních funkcí; rekurzivní funkce jsou totální. Relace je rekurzivní, má-li rekurzivní charakteristickou funkci a je rekurzivně spočetná, je-li definičním oborem rekurzivní relace. Předpokládáme dále znalost základních vlastností rekurzivních funkcí a relací a rekurzivně spočetných relací.

Problémy. *Parciálně* neboli *částečně rekurzivní funkce* jsou takové parciální funkce, jejichž graf je rekurzivně spočetná relace. Zřejmě je každá rekurzivní funkce také parciálně rekurzivní funkcí, neboť její graf je rekurzivní.

a) (O grafu funkce.) Buď F částečná funkce, P relace. Pak platí
$$(\forall y)(\mathcal{G}_F(\overline{a}, y) \leftrightarrow (\exists x)P(\overline{a}, y, x)) \;\Rightarrow\; F(\overline{a}) \simeq (\mu z P(\overline{a}, (z)_0, (z)_1))_0.$$

b) Definujte rekurzivní funkce Sb_n takové, že $Sb_n(\ulcorner\varphi\urcorner, a_1, \ldots, a_n) = \ulcorner\varphi(v_1/\underline{a_1}, \ldots, v_n/\underline{a_n})\urcorner$ platí pro každou formuli φ aritmetiky a $\langle a_1, \ldots, a_n\rangle \in \mathbb{N}^n$.

c) (O univerzálních parciálně rekurzivních funkcích.) Pro každé $n > 0$ existuje $(n+2)$-ární rekurzivní relace T_n tak, že platí:
   1) Částečná $(n+1)$-ární funkce $\phi^n(x, \overline{a}) \simeq (\mu z \mathrm{T}_n(x, \overline{a}, z))_0$ je univerzální pro množinu n-árních parciálně rekurzivních funkcí a funkce ϕ^n je parciálně rekurzivní.
   2) $(n+1)$-ární relace $(\exists z)\mathrm{T}_n(x, \overline{a}, z)$, značená $\mathrm{W}^n(x, \overline{a})$, je univerzální pro množinu n-árních rekurzivně spočetných relací.
   3) Platí $\mathrm{W}^n = \mathrm{dom}(\phi^n)$. Pro pevné x buď $\phi^n_x(\overline{a}) \simeq \phi^n(x, \overline{a})$, $\mathrm{W}^n_x(\overline{a}) \leftrightarrow \mathrm{W}^n(x, \overline{a})$. Pak $\mathrm{W}^n_x = \mathrm{dom}(\phi^n_x)$. Každá n-ární parciálně rekurzivní funkce resp. rekurzivně spočetná relace je právě nějaké ϕ^n_x resp. W^n_x s jistým $x \in \mathbb{N}$; říká se, že x je její index.

   Návod. Buď F nějaká n-ární parciálně rekurzivní funkce; existuje rekurzivní relace R tak, že $\mathcal{G}_F(\overline{a}, y) \leftrightarrow (\exists v)R(y, v, \overline{a})$. Užijte formuli φ s $v_1, \ldots, v_{n+2}$ reprezentující R v Q a tvrzení a) o grafu funkce.

d) $\mathrm{dom}(\phi^n)$, čili W^n, není rekurzivní a neexistuje n-ární rekurzivní funkce rozšiřující ϕ^n. *Návod.* Je-li W^n rekurzivní, je i $R = \{\overline{a} \in \mathbb{N}^n;\ \overline{a}_0 \smile \overline{a} \in \mathrm{W}^n\}$, tedy i $\mathbb{N}^n - R$. Buď e její index a uvažujte o $\overline{e} = \langle e, e, \ldots, e\rangle \in \mathbb{N}^n$.

e) i) Pro $n > 0, k \geq 0$ existuje $(k+1)$-ární rekurzivní funkce s^n_k taková, že
$$\mathrm{T}_{n+k}(f, \overline{a}, \overline{b}, x) \leftrightarrow \mathrm{T}_n(s^n_k(f, \overline{b}), \overline{a}, x).$$
   ii) Pro $n > 0, k \geq 0$ je $\phi^{n+k}(f, \overline{a}, \overline{b}) \simeq \phi^n(s^n_k(f, \overline{b}), \overline{a})$, $\mathrm{W}^{n+k}(f, \overline{a}, \overline{b}) \leftrightarrow \mathrm{W}^n(s^n_k(f, \overline{b}), \overline{a})$.

   Návod. Uvažujte o těchto definicích: $s^n_0(f) = f$, $s^n_1(f, a) = \mathrm{Sub}(f, \mathrm{Var}(n+3), \mathrm{Num}(a))$, $s^n_{k+1}(f, \overline{a}, a) = s^n_k(s^{n+k}_1(f, a), \overline{a})$.

f) i) Je-li $n > 0$ a G nějaká $(n+1)$-ární parciálně rekurzivní funkce, existuje n-ární parciálně rekurzivní funkce F s indexem f tak, že $F(\overline{a}) \simeq G(\overline{a}, f)$.
   ii) Buď F unární parciálně rekurzivní funkce, $n > 0$ přirozené. Pak existuje číslo e tak, že
$$\phi^n(e, \overline{x}) \simeq \phi^n(F(e), \overline{x}).$$

g) Buď $G(x, \overline{a})$ nějaká $n+1$-ární parciálně rekurzivní funkce, $n > 0$. Pak existuje parciálně rekurzivní funkci F taková, že platí „rovnice“ $F(\overline{a}) \simeq G(F(\overline{a}), \overline{a})$. *Návod.* Užijte f) i).

h) „Program vypíšící právě sám sebe“: Existuje číslo f tak, že pro každé x je $\phi^1_f(x) = f$. *Návod.* Užijte f) i).

i) (Riceova věta.) Nechť Γ je neprázdná vlastní podmnožina množiny unárních parciálně rekurzivních funkcí. Pak $\{e;\ \phi^1_e \in \Gamma\}$ není rekurzivní množina. *Návod.* Je-li $X = \{e;\ \phi^1_e \in \Gamma\}$ rekurzivní, najděte rekurzivní G s $G(x) \notin X \Leftrightarrow x \in X$ a uvažujte o e s $\phi^1_e = \phi^1_{G(e)}$ – viz f) ii).