ÚLOHY Z PREDIKÁTOVÉ LOGIKY

Instance, varianty.

UF.1.1. Substituovatelnost.

1. Buď φ formule

$$(\exists z)(x = z) \,\&\, y < x$$

a dále x, y, z různé proměnné, F unární funkční symbol, c konstantní symbol.

Uveďte, zda je term t substituovatelný do φ za proměnnou v v následujících případech:

a) t je $F(z)$, v je x. Řešení: Ne.
b) t je $F(z)$, v je y. Řešení: Ano.
c) t je $F(x)$, v je x. Řešení: Ano.
d) t je $F(c)$, v je y. Řešení: Ano.

2. Buď φ formule

$$(\forall x)((\exists z)(z < x \,\&\, y = z) \vee z \neq x)$$

a dále x, y, z různé proměnné, G binární funkční symbol, c konstantní symbol.

Uveďte, zda je term t substituovatelný do φ za proměnnou v v následujících případech:

a) t je $G(c, x)$, v je y Řešení: Ne.
b) t je $G(c, y)$, v je y Řešení: Ano.
c) t je $G(c, c)$, v je z Řešení: Ano.
d) t je $G(z, x)$, v je z Řešení: Ne.

UF.1.2. Instance. Varianty.

1. Nechť y není volná ve φ a je substituovatelná za x do φ, φ' je $\varphi(x/y)$. Zjistěte, zda $\varphi'(y/x)$ je φ. Zdůvodněte odpověď.

Řešení: Oba předpoklady dohromady zaručují, že volný výskyt y ve φ' je právě tam, kde je volný výskyt x v φ. Tedy x je substituovatelné za y do φ' a také rovnost obou uvažovaných formulí platí.

2. Buďte x, y, z, u různé proměnné, Q kvantifikátor. Odpovězte a zdůvodněte, zda v následujících případech platí:

$$\psi \text{ je varianta } \varphi.$$

a) φ je $(Qx)(x < y \vee (\exists z)(z = y \,\&\, z \neq x))$
ψ je $(Qz)(z < y \vee (\exists z)(z = y \,\&\, z \neq z))$
Řešení: Ne. z není substituovatelné za x do $x < y \vee (\exists z)(z = y \,\&\, z \neq x)$.

b) φ je $(Qx)(x < y \vee (\forall z)(z = y \,\&\, z \neq x))$
ψ je $(Qy)(y < y \vee (\forall z)(z = y \,\&\, z \neq y))$
Řešení: Ne. y je volná ve φ.

c) φ je $(Qx)(x < y \vee (\exists z)(z = y \,\&\, z \neq x))$
ψ je $(Qu)(u < y \vee (\exists z)(z = y \,\&\, z \neq u))$
Řešení: Ano. u není volná ve φ a je substituovatelná za x do $x < y \vee (\exists z)(z = y \,\&\, z \neq x)$.

3. Buď P unární predikátový symbol,

φ formule $(\exists y)(y = x) \,\&\, P(x)$, φ' formule $(\exists y)(y = y) \,\&\, P(y)$.

a) Je $(\forall x)\varphi'$ varianta $(\forall x)\varphi$?
Řešení: Ne.

b) Je x substituovatelné do φ' za y?
Řešení: Ano.

c) Je φ rovno $\varphi'(y/x)$?
Řešení: Ne. $\varphi'(y/x)$ je $(\exists y)(y = y) \,\&\, P(x)$.

d) Je $\vdash \varphi \leftrightarrow \varphi'(y/x)$?
Řešení: Ano. Je $\vdash (\exists y)(y = x) \leftrightarrow (\exists y)(y = y)$, protože obě formule z ekvivalence jsou dokazatelné. Odtud $\vdash (\exists y)(y = x) \,\&\, P(x) \leftrightarrow (\exists y)(y = y) \,\&\, P(x)$.

Pojem modelu a splňování. Axiomatizovatelnost.

UF.1.3. Platnost formule v modelu.

1. Buď φ formule $P(x) \to (\forall x)P(x)$, kde P je unární relační symbol. V právě kterých strukturách $\langle A, P^A\rangle$ neplatí φ ani $\neg\varphi$?

Řešení: Právě když $\emptyset \neq P^A \neq A$.

2. Buď φ formule $x = c$, kde c je konstantní symbol. V právě kterých strukturách $\langle A, c^A\rangle$ neplatí φ ani $\neg\varphi$?

Řešení: Právě když $|A| \geq 2$.

3. Buď φ formule $P(x) \to (\forall x)R(x)$, kde P, R jsou různé unární predikátové symboly. V právě kterých strukturách $\mathcal{A} = \langle A, P^A, R^A\rangle$ neplatí φ ani $\neg\varphi$?

Řešení: Právě když $\emptyset \neq P^A \neq A \neq R^A$.

Zřejmě totiž:
$\mathcal{A} \not\models \varphi \Leftrightarrow P^A \neq \emptyset$ a $R^A \neq A$, $\quad \mathcal{A} \not\models \neg\varphi \Leftrightarrow P^A \neq A$ nebo $R^A = A$.

UF.1.4. Korektnost substituce.

Buď φ formule $(\exists y)(x \neq y)$ s různými proměnnými x, y. Buď φ' výsledek „nekorektní substituce“ y do φ za volný výskyt x. Buď $\mathcal{A}$ struktura. Uvažujme tvrzení:

$$\text{Pro každé } e : \mathrm{Var} \to A \text{ je } \mathcal{A} \models \varphi'[e] \Leftrightarrow \mathcal{A} \models \varphi[e(x/y[e])]. \qquad (*)$$

a) Uveďte, zda $(*)$ platí pro $\mathcal{A} = \langle \mathbb{N}, +\rangle$, kde $+$ je sčítání přirozených čísel.

Řešení: Ne.

b) Uveďte, zda $(*)$ platí pro $\mathcal{A} = \langle \{0\}, R\rangle$, kde $R = \{\langle 0, 0\rangle\}$.

Řešení: Ano.

c) Právě pro které modely $\mathcal{A} = \langle A\rangle$ (teorie čisté rovnosti) platí $(*)$?

Řešení: Právě pro $\mathcal{A}$ s A jednoprvkovým.

UF.1.5. Axiomatizovatelnost.

1. Buď $\mathsf{K} = \{\langle A\rangle$; velikost A je sudá nebo nekonečná$\}$ třída modelů jazyka L čisté rovnosti. Zjistěte, zda je K axiomatizovatelná, případně najděte její axiomatiku.

Řešení: $T = \{\neg$„existuje právě $2k + 1$ prvků“; $k \in \mathbb{N}\}$ axiomatizuje K.

2. Nechť T je teorie v jazyce L s rovností taková, že T má model a každý její model je nekonečný. Buď $0 < n \in \mathbb{N}$. Najděte L-teorii T' tak, aby $\mathsf{M}^\infty(T') = \mathsf{M}^\infty(T)$ a T' měla nějaké konečné modely, a to všechny:

a) právě n-prvkové,

b) právě n-prvkové nebo $2n$-prvkové.

Řešení: Buď $T' = \{\varphi \vee \psi;\ \varphi \in T\}$ s vhodným ψ.

3. Buď $0 < n \in \mathbb{N}$. Najděte teorii T v nějakém jazyce s rovností, která má nekonečné modely, nemá spočetný model, má konečné modely, všechny kardinality nejvýše n.

Řešení: Buď $L = \langle c_i;\ i \in \mathbb{R}\rangle$ s konstantními symboly c_i a T_0 buď L-teorie $\{c_i \neq c_j;\ i, j \in \mathbb{R}, i \neq j\}$; hledaná T je L-teorie

$$\{\varphi \vee \text{„existuje nejvýše } n \text{ prvků“};\ \varphi \in T_0\}.$$

4. Buď $L = \langle U\rangle$ s rovností, přičemž U je unární relační symbol, $0 < n \in \mathbb{N}$ a

$$\mathsf{K} = \{\langle A, U^A\rangle;\ U^A \text{ je nekonečná nebo nejvýše } n\text{-prvková}\}$$

je třída L-struktur. Zjistěte, zda je K axiomatizovatelná, případně najděte její axiomatiku.

Řešení: Nechť T_0 je teorie L-teorie

$$\{(\exists x_0, \dots, x_{m-1})(\textstyle\bigwedge_{i<j<m} x_i \neq x_j \ \&\ \bigwedge_{i<m} U(x_i));\ 0 < m \in \mathbb{N}\}.$$

Pro L-strukturu $\mathcal{A}$ platí: $\mathcal{A} \models T_0 \Leftrightarrow |U^A| \geq \omega$. Buď χ sentence „existuje nejvýše n prvků x s $U(x)$“. Pak $T = \{\varphi \vee \chi;\ \varphi \in T_0\}$, axiomatizuje K.

Izomorfní spektra.

UF.1.6. Izomorfní spektra v jazyce $\langle U, c\rangle$.

Buď $L = \langle U, c\rangle$, kde U je unární relační a c konstantní symbol.

1. Popište izomorfní spektrum L-teorie $T = \{U(c)\}$.

Řešení: $\mathrm{I}(\kappa, T) = |\mathbf{Cn} \cap \kappa|$. Modely $\langle \kappa, U', c'\rangle$, $\langle \kappa, U'', c''\rangle$ teorie T jsou izomorfní, právě když $\langle |U'|, |\kappa - U'|\rangle = \langle |U''|, |\kappa - U''|\rangle$, přičemž $|U'| \geq 1$. Všech různých dvojic $\langle |U'|, |\kappa - U'|\rangle$ s $|U'| \geq 1$, $U' \subseteq \kappa$ je právě $|\mathbf{Cn} \cap \kappa|$. Pro $\kappa < \omega$ je totiž $|\mathbf{Cn} \cap \kappa| = \kappa$. Pro $\kappa \geq \omega$ je buď $|U'|$ jakékoli kardinality $< \kappa$, nebo $|U'| = \kappa$ a pak může být $|\kappa - U'|$ jakékoli kardinality $\leq \kappa$; takových možností je $|\mathbf{Cn} \cap \kappa| + |\mathbf{Cn} \cap \kappa| = |\mathbf{Cn} \cap \kappa|$.

2. Popište izomorfní spektrum L-teorie $T = \{(\exists!x)U(x)\}$.

Řešení: $\mathrm{I}(\kappa, T) = 1$ pro $\kappa = 1$ a 2 pro $\kappa > 1$.

UF.1.7. Izomorfní spektrum jazyka spočetně konstant.

Buď $L = \langle c_i\rangle_{i\in\omega}$, kde c_i jsou konstantní symboly.

1. Pro L-strukturu $\mathcal{A}$ definujeme ekvivalenci E^A na ω:

$$i\ E^A j \quad \Leftrightarrow \quad c_i^A = c_j^A.$$

Buďte $\mathcal{A}, \mathcal{B}$ dvě L-struktury téže velikosti.

a) Platí:

$$\mathcal{A} \cong \mathcal{B} \quad \Leftrightarrow \quad E^A = E^B \text{ a } |A - \{c_i^A;\, i < \omega\}| = |B - \{c_i^B;\, i < \omega\}|. \tag{1}$$

Speciálně je nejvýše kontinuum neizomorfních L-struktur dané kardinality.

b) Jsou-li $\mathcal{A}$, $\mathcal{B}$ konečné nebo nespočetné, platí:

$$\mathcal{A} \cong \mathcal{B} \quad \Leftrightarrow \quad E^A = E^B. \tag{2}$$

c) Najděte spočetné $\mathcal{A}$, $\mathcal{B}$, pro které (2) neplatí.

2. Pro $\kappa \geq 2$ je $\mathrm{I}(\kappa, L) = 2^\omega$.

Návod: Užijte toho, že na ω je kontinuum různých ekvivalencí s λ třídami, když $2 \leq \lambda \leq \omega$.

Řešení: Buď E ekvivalence na ω, $\lambda(E)$ počet tříd E. Pro $\kappa \geq \lambda(E)$ definujme L-strukturu $\kappa^E = \langle \kappa, c_i^E\rangle_{i<\omega}$ tak, aby platilo: $c_i^E = c_j^E \Leftrightarrow i\,E\,j$. Pak:

$$\text{Jsou-li } E, E' \text{ ekvivalence na } \omega \text{ tak } \kappa^E \cong \kappa^{E'} \Leftrightarrow E = E'.$$

Tedy: jelikož je na ω kontinuum různých ekvivalencí s λ třídami, jakmile $2 \leq \lambda \leq \omega$, existuje alespoň kontinuum neizomorfních L-struktur kardinality $\kappa\,(\geq 2)$ a dle (1) jich není více.

UF.1.8.

Teorie DiLO diskrétního lineárního uspořádání má pro každé $\kappa \geq \omega$ právě 2^κ neizomorfních modelů kardinality κ.

Návod: Užijte toho, že pro každé $\kappa \geq \omega$ je právě 2^κ neizomorfních lineárních uspořádání s univerzem kardinality κ.

Řešení: Pro ostré lineární uspořádání $\mathcal{A} = \langle A, <^A\rangle$ buď $\mathcal{A}(\mathbb{Z}) = \langle A \times \mathbb{Z}, <_{Le}\rangle$ lexikografické uspořádání. Je diskrétní a kardinality $\max(|A|, \omega)$. Nechť $\mathcal{B} = \langle B, <^B\rangle$ je lineární uspořádání. Pak platí $\mathcal{A}(\mathbb{Z}) \cong \mathcal{B}(\mathbb{Z}) \Rightarrow \mathcal{A} \cong \mathcal{B}$. Buď totiž h isomorfizmus $\mathcal{A}(\mathbb{Z})$ a $\mathcal{B}(\mathbb{Z})$; definujme $H : A \to B$ takto:

$$H(a) = b_a \Leftrightarrow \text{existuje } j_a \in \mathbb{Z} \text{ s } h(\langle a, 0\rangle) = \langle b_a, j_a\rangle.$$

Pak to je jasně zobrazení na B a

$$\begin{aligned} a <^A a' \quad &\Leftrightarrow \quad h(\langle a, 0\rangle) <^{\mathcal{B}(\mathbb{Z})} h(\langle a', 0\rangle) \text{ a mezi } h(\langle a, 0\rangle),\ h(\langle a', 0\rangle) \text{ je nekonečně prvků} \\ &\Leftrightarrow \quad b_a <^B b_{a'} \quad \Leftrightarrow \quad H(a) <^B H(b). \end{aligned}$$

Jelikož na $\kappa \geq \omega$ je 2^κ neizomorfních lineárních uspořádání $\mathcal{A}$, máme 2^κ neizomorfních lineárních uspořádání $\mathcal{A}(\mathbb{Z})$ na $\kappa \times \mathbb{Z}$, tedy 2^κ neizomorfních diskrétních lineárních uspořádání, majících každé velikost univerza κ.

Základy dedukce.

UF.1.9. Syntaktický důkaz bezespornosti teorie rovnosti v L.

Nechť T je teorie rovnosti v L, tj. L-teorie s rovností bez mimologických axiomů. Buď d nový konstantní symbol. Pro L-formuli φ buď φ^* formule, která se získá z φ odstraněním všech kvantifikací a nahrazením každého termu konstantním symbolem d. Pak φ^* je výrok nad prvovýroky $d = d$, $R(d, \dots, d)$, kde R je relační symbol z L.

a) Je-li φ logický axiom nebo axiom rovnosti, kromě axiomu $x = x$, je φ^* tautologie.

Řešení: Pro logický axiom φ, který není axiomem rovnosti, to je jasné. Axiomy rovnosti φ kromě $x = x$ přejdou na φ^* tvaru

$$d = d \to d = d \to \cdots \to (R(d, \dots, d) \to R(d, \dots, d))$$

nebo

$$d = d \to d = d \to \cdots \to d = d$$

a pak ovšem $\overline{v}(\varphi^*) = 1$.

b) $T \vdash \varphi \Rightarrow \overline{v}(\varphi^*) = 1$, jakmile v je ohodnocení uvedených prvovýroků takové, že platí $v(d = d) = 1$. Speciálně je T bezesporná.

Návod: Užijte indukci na teorémech T.

Řešení: Indukcí na teorémech T. Pro axiom φ to platí, neboť $(x = x)^*$ je $d = d$. Buď $v(d = d) = 1$. Nechť pro ψ, $\psi \to \varphi$ to platí. Pak $1 = \overline{v}((\psi \to \varphi)^*) = \overline{v}(\psi^* \to \varphi^*)$ a $\overline{v}(\psi^*) = 1$, tedy $\overline{v}(\varphi^*) = 1$. Platí-li to pro φ, tak $\overline{v}(((\forall x)\varphi)^*) = \overline{v}(\varphi^*) = 1$.

UF.1.10. Dokazatelné, vyvratitelné, nezávislé a bezesporné formule.

1. Buďte P, R různé unární predikátové symboly. Zdůvodněte, zda formule φ je dokazatelná, vyvratitelná či nezávislá v logice, kde φ je

a) $P(x)$ b) $P(x) \to R(x)$
c) $(\forall x, y)(P(x) \to (R(x) \to P(x)))$ d) $(\exists x)P(x)$

Řešení: a) Nezávislá. $\langle 1, \emptyset\rangle \models \neg\varphi$, $\langle 1, 1\rangle \models \varphi$. b) Nezávislá. $\langle 2, \emptyset, 2\rangle \models \varphi$, $\langle 2, 2, \emptyset\rangle \models \neg\varphi$. c) Dokazatelná, neboť $P(x) \to (R(x) \to P(x))$ je tautologie. d) Nezávislá. $\langle 1, \emptyset\rangle \models \neg\varphi$, $\langle 1, 1\rangle \models \varphi$.

2. Najděte nějaké nezávislé sentence teorie čisté rovnosti, teorie lineárního uspořádání, teorie grup, teorie těles.

3. Nechť $T \vdash (\exists x)\varphi(x)$. Co lze říci o dokazatelnosti, vyvratitelnosti, nezávislosti, konzistenci φ, $\neg\varphi$ vzhledem k T?

UF.1.11. Vlastnosti kvantifikátorů.

1. $\vdash (\forall x)(\varphi \to \psi) \to ((Qx)\varphi \to (Qx)\psi)$, kde Q značí kvantifikátor.

Návod: Užijte větu o konstantách.

Řešení: Buďte T logické axiomy v jazyce rozšířeném o nové konstantní symboly c_i; $\varphi(x, x_1/c_1, \cdots)$ resp. $\psi(x, x_1/c_1, \cdots)$ označme $\varphi'(x)$ resp. $\psi'(x)$ (konstanty substituujeme za všechny volné proměnné, kromě x). Pak $T, (\forall x)(\varphi' \to \psi') \vdash \varphi' \to \psi'$, dle pravidla distribuce kvantifikátoru i $T, (\forall x)(\varphi' \to \psi') \vdash (Qx)\varphi' \to (Qx)\psi'$ a zbytek dá věta o dedukci a konstantách.

2.

a) $\vdash (\forall x)\varphi \to (\exists x)\varphi$.

Řešení: Je $\vdash (\forall x)\varphi \to \varphi$, $\vdash \varphi(x) \to (\exists x)\varphi$; odtud pomocí pravidla tranzitivity implikace plyne dokazované.

b) $\vdash \varphi \to (\forall x)\varphi \quad \Leftrightarrow \quad \vdash (\exists x)\varphi \to (\forall x)\varphi \quad \Leftrightarrow \quad \vdash (\forall x)\neg\varphi \vee (\forall x)\varphi$.

Řešení: Prvá ekvivalence. Implikace $\Rightarrow$: $\vdash \varphi \to (\forall x)\varphi \Leftrightarrow \vdash (\forall x)(\varphi \to (\forall x)\varphi) \Rightarrow \vdash (\exists x)\varphi \to (\forall x)\varphi$. Implikace $\Leftarrow$: $\vdash (\exists x)\varphi \to (\forall x)\varphi \Rightarrow \vdash (\forall x)(\varphi \to (\forall x)\varphi) \Rightarrow \vdash \varphi \to (\forall x)\varphi$. Užitím de Morganových vztahů plyne druhá ekvivalence.

3.

a) $\vdash (\forall x)(\forall x)\varphi \leftrightarrow (\forall x)\varphi$.

Řešení: i) $\vdash (\forall x)(\forall x)\varphi \to (\forall x)\varphi$ dává axiom substituce.

ii) $\vdash (\forall x)\varphi \to (\forall x)(\forall x)\varphi$ plyne z $\vdash (\forall x)\varphi \to (\forall x)\varphi$ pravidlem $\forall$-zavedení. Z i), ii) plyne ihned dokazované.

b) $\vdash (\exists x)(\forall x)\varphi \leftrightarrow (\forall x)\varphi$.

Řešení: i) $(\exists x)(\forall x)\varphi \to (\forall x)\varphi$ dává pravidlo $\exists$-zavedení.

ii) $(\forall x)\varphi \to (\exists x)(\forall x)\varphi$ plyne z platného vztahu $\vdash \psi \to (\exists x)\psi$. Z i), ii) plyne ihned dokazované.

UF.1.12. Vytýkání kvantifikátorů - protipříklady.

1. $\nvdash (\forall x)(\varphi \to \psi) \to (\varphi \to (\forall x)\psi)$.

Řešení: Buď $\mathcal{A} = \langle A, P^A, R^A\rangle$, kde P, R jsou unární predikátové symboly, $a \in P^A \subseteq R^A \subsetneq A$. Pak

$$\mathcal{A} \models (\forall x)(P(x) \to R(x)), \qquad \mathcal{A} \not\models (P(x) \to (\forall x)R(x))[a].$$

Tedy $\mathcal{A} \not\models (\forall x)(P(x) \to R(x)) \to (P(x) \to (\forall x)R(x))$.

2. $\nvdash (\varphi \to (\forall x)\psi) \to (\forall x)(\varphi \to \psi)$.

Řešení: Buď $\mathcal{A} = \langle A, P^A, R^A\rangle$, kde P, R jsou unární predikátové symboly, $a \in A - P^A$, $\emptyset \neq P^A \not\subseteq R^A$. Pak

$$\mathcal{A} \models (P(x) \to (\forall x)R(x))[a], \qquad \mathcal{A} \not\models (\forall x)(P(x) \to R(x)).$$

Tedy $\mathcal{A} \not\models (P(x) \to (\forall x)R(x)) \to (\forall x)(P(x) \to R(x))$.

3. $\nvdash (\exists x)(\varphi \to \psi) \to (\varphi \to (\exists x)\psi)$.

Řešení: Buď $\mathcal{A} = \langle A, P^A, R^A\rangle$, kde P, R jsou unární predikátové symboly, $a \in P^A \subsetneq A$, $R^A = \emptyset$. Pak

$$\mathcal{A} \models (\exists x)(P(x) \to R(x)) \qquad \text{(protože existuje } b \in A - P^A\text{)},$$
$$\mathcal{A} \not\models (P(x) \to (\exists x)R(x))[a] \quad \text{(protože je } a \in P^A\text{)}.$$

Tedy $\mathcal{A} \not\models (\exists x)(P(x) \to R(x)) \to (P(x) \to (\exists x)R(x))$.

Rozšíření o funkční symbol a definovaný funkční symbol.

UF.1.13.

Teorie těles má axiomatiku $T = T_0 \cup \{(\exists y)\varphi\}$, kde T_0 je jistá množina otevřených formulí jazyka $L = \langle +, -, \cdot, 0, 1\rangle$ těles a φ je $x \neq 0 \to x \cdot y = 1$.

- Buď F nový unární funkční symbol a
$$T^\varphi = T_0 \cup \{\varphi(y/F(x))\}.$$
- Buď ψ formule $x \cdot y = 1 \vee (x = 0 \;\&\; y = 1)$; je $T \vdash (\forall x)(\exists!y)\psi$. Buď
$$T^\psi = T_0 \cup \{\psi(y/F(x))\}.$$

Platí:

1. T^φ je konzervativní otevřená extenze teorie T (a $(\forall x)\varphi(y/F(x))$ je Skolemova varianta $(\forall x)(\exists y)\varphi$.)

Řešení: $S = T \cup \{\varphi(y/F(x))\}$ je rozšíření T o funkční symbol F, tedy to je konzervativní rozšíření. Protože $\vdash \varphi(y/F(x)) \to (\exists y)\varphi$, je $T^\varphi = S - \{(\exists y)\varphi\}$ ekvivalentní s S a tedy to je konzervativní rozšíření T, které je ovšem tvořeno jen otevřenými axiomy. (Evidentně je $(\forall x)\varphi(y/F(x))$ Skolemova varianta $(\forall x)(\exists y)\varphi$.)

2. Neexistuje L-formule $\chi(x, y)$ taková, že $T^\varphi \vdash F(x) = y \leftrightarrow \chi(x, y)$.

Řešení: Sporem. Nechť χ existuje. Pak speciálně, díky tomu, že T^φ je konzervativní rozšíření T, máme $T \vdash (\exists!y)\chi(0, y)$. Pro těleso racionálních čísel $\underline{\mathbb{Q}}$ buď $a \in \mathbb{Q}$ takové, že $\underline{\mathbb{Q}} \models \chi[0, a]$; takové a je jediné. Interpretujme F tak, že $F^{\mathbb{Q}}(0) \neq a$ a $F^{\mathbb{Q}}(q) = q^{-1}$ pro $q \neq 0$; to ovšem můžeme, neboť $\vdash \varphi(0, y) \leftrightarrow y = y$. Pak $\langle \underline{\mathbb{Q}}, F^{\mathbb{Q}}\rangle \models T^\varphi \cup \{\neg\chi(0, F(0))\}$. To je spor s $T^\varphi \vdash \chi(0, F(0))$.

3. T^ψ je konzervativní otevřená extenze teorie T v jazyce teorie T^φ. Rozšiřuje T^φ a není ekvivalentní s T^φ.

Řešení: $S = T \cup \{\psi(y/F(x))\}$ je rozšíření T o funkční symbol F, tedy to je konzervativní rozšíření. Z $T_0 \vdash \psi(x,y) \to \varphi(x,y)$ plyne

$$T_0, \psi(y/F(x)) \vdash (\exists y)\varphi, \qquad (*)$$

tudíž $T^\psi = S - \{(\exists y)\varphi\}$ je ekvivalentní s S a tedy to je konzervativní rozšíření T, které je ovšem tvořeno jen otevřenými axiomy. Dále $T^\psi \vdash \varphi(y/F(x))$ dává (*). Tudíž je T^ψ silnější, než T^φ. Konečně $T^\psi \vdash F(0) = 1$, ale $T^\varphi \nvdash F(0) = 1$; o tom svědčí např. $\langle \underline{\mathbb{Q}}, F^{\mathbb{Q}} \rangle \models T^\varphi$ s $F^{\mathbb{Q}}(0) = 0$.

Otevřené teorie.

Teorie je *otevřená*, je-li množina jejích mimologických axiomů tvořená otevřenými formulemi. Teorie T je *axiomatizovatelná otevřenými formulemi* čili *otevřeně axiomatizovatelná*, existuje-li otevřená teorie ekvivalentní s T.

UF.1.14.

1. Buď T teorie čisté rovnosti, tj. teorie v jazyce L_0 s rovností bez mimologických symbolů, která nemá mimologické axiomy. Pro nenulové $n \in \mathbb{N}$ buď teorie

T_n /$T_{\leq n}$ /$T_{\geq n}$ s jediným axiomem „existuje právě /nejvýše /alespoň n prvků“.

a) Je T_n axiomatizovatelná otevřenými formulemi? Odpověď zdůvodněte.
b) Je $T_{\leq n}$ axiomatizovatelná otevřenými formulemi? Odpověď zdůvodněte.
c) Je $T_{\geq n}$ axiomatizovatelná otevřenými formulemi? Odpověď zdůvodněte.
d) Která kompletní rozšíření teorie T v jazyce L_0 jsou otevřeně axiomatizovatelná?

Návod: Užijte tvrzení, že podstruktura modelu otevřené teorie je její model.

Řešení: Budeme užívat tvrzení:

podstruktura modelu otevřené teorie je model této teorie. (*)

a) Pro $n = 1$ je, a to jediným axiomem $x = y$. Pro $n > 1$ není. Je-li totiž $\langle A\rangle \models T_n$, pro $\emptyset \neq A' \subsetneq A$ je $\langle A'\rangle$ podstruktura $\langle A\rangle$ a není to model T_n.
b) Každá $T_{\leq n}$ je, neboť je ekvivalentní s teorií $\bigvee\{x_i = x_j;\ i \neq j, i, j \leq n\}$.
c) Pro $n = 1$ je, neboť T_1 je ekvivalentní s T. Pro $n > 1$ není. Je-li totiž $\langle A\rangle \models T_{\geq n}$, jednoprvková podstruktura modelu $\langle A\rangle$ není model $T_{\geq n}$.
d) Kompletní rozšíření teorie T v jazyce L_0 jsou T_n s $0 < n \in \mathbb{N}$ a $T_\infty = \bigcup_{0<n\in\mathbb{N}} T_{\geq n}$. Axiomatizovatelná otevřenými formulemi je jen T_1. To plyne z a) a díky tomu, že T_∞ není otevřeně axiomatizovatelná podle (*), protože její model má konečnou podstrukturu, která ovšem není modelem T_∞.

2. Teorie těles (v jazyce $\langle +, -, \cdot, 0, 1\rangle$ těles) není otevřeně axiomatizovatelná.

Návod: Užijte tvrzení, že podstruktura modelu otevřené teorie je její model.

Řešení: Užijeme tvrzení, že podstruktura modelu otevřené teorie je model této teorie. Buď $\underline{\mathbb{Z}}$ podstruktura tělesa $\underline{\mathbb{Q}}$ racionálních čísel, jejíž univerzum jsou celá čísla; $\underline{\mathbb{Z}}$ není těleso.

3. Buď T otevřená axiomatika teorie lineárního uspořádání v jazyce $L = \langle\leq\rangle$ uspořádání. Označme pro $0 < n \in \mathbb{N}$ jako $T_{\leq n}$ rozšíření T o axiom „existuje nejvýše n prvků“.

Pak L-teorie T' rozšiřující T je axiomatizovatelná otevřenými formulemi právě když

T' je ekvivalentní $T_{\leq n}$ nebo T' je ekvivalentní T.

Návod: Užijte tvrzení, že podstruktura modelu otevřené teorie je její model.

Řešení: Stačí dokázat implikaci $\Rightarrow$, neboť opačná platí proto, že $T_{\leq n}$, T jsou axiomatizovatelné otevřenými formulemi. Buď dále T' otevřená teorie. Užijeme tvrzení:

Podstruktura modelu otevřené teorie je její model. (*)

i) Nechť T' má jen konečné modely. Existuje největší $n \in \mathbb{N}$ takové, že existuje model $\mathcal{A} \models T'$, A velikosti n. Platí pak $\mathcal{B} \models T' \Rightarrow \mathcal{B} \models T_{\leq n}$; tudíž T' je silnější, než $T_{\leq n}$. Dále $\mathcal{B} \models T_{\leq n} \Rightarrow \mathcal{B} \models T'$, neboť ze $\mathcal{B} \models T_{\leq n}$ plyne, že až na izomorfizmus, převádějící i-tý prvek uspořádání $\leq^B$ na i-tý prvek uspořádání $\leq^A$, je $\mathcal{B}$ podstruktura $\mathcal{A}$, a tedy $\mathcal{B} \models T'$. Tudíž $T_{\leq n}$ je silnější než T'.

ii) Nechť T' má i nekonečné modely. Pak dle (*) má model každé konečné nenulové velikosti. Dokážeme, že libovolný model $\mathcal{A} \models T$ je až na izomorfizmus podstrukturou nějakého modelu teorie T' a tedy to je model T'. Odtud plyne, že T' je ekvivalentní T.

Definujme jazyk $L_A = \langle\leq, c_a\rangle_{a\in A}$, kde c_a jsou nové konstantní symboly. Buď $\mathcal{A}_A$ expanze $\mathcal{A}$ do L_A-struktury, přičemž c_a interpretujeme jako a (c_a je tzv. jméno

prvku a). Buď $\Delta(\mathcal{A})$ množina všech uzavřených formulí χ jazyka L_A takových, že χ je literál (tj. atomická nebo negace atomické formule) a $\mathcal{A} \models \chi$. ($\Delta(\mathcal{A})$ je tzv. diagram $\mathcal{A}$.) Buď $T_A = T' \cup \Delta(\mathcal{A})$. T_A je bezesporná, neboť pro $S \subseteq \Delta(\mathcal{A})$ konečnou je jistá konečná podstruktura $\mathcal{B} \subseteq \mathcal{A}$ taková, že $\mathcal{B}_B \models S$. (B nechť obsahuje všechny prvky $a \in A$ takové, že c_a má výskyt v S.) Díky konečnosti B je $\mathcal{B} \models T'$ a tedy $\mathcal{B}_B \models T' \cup S$. Buď $\langle \mathcal{B}, c_a^B \rangle_{a \in A} \models T_A$ (je $\mathcal{B} \models T'$). Pak zobrazení $h : A \to B$, kde $h(a) = c_a^B$ je vnoření $\mathcal{A}$ do $\mathcal{B}$, tj. h je prosté a pro každé $a, b \in A$ je $a \leq^A b \Leftrightarrow h(a) \leq^B h(b)$. Máme totiž $a \leq^A b \Leftrightarrow c_a \leq c_b \in \Delta(\mathcal{A}) \Leftrightarrow c_a^B \leq^B c_b^B \Leftrightarrow h(a) \leq^B h(b)$ a stejně pro $=$ místo $\leq$. Podstruktura $\mathcal{A}^h$ struktury $\mathcal{B}$ s univerzem $\{h(a);\, a \in A\}$ je jednak model T' díky (*), jednak je $\mathcal{A}$ izomorfní s $\mathcal{A}^h$ prostřednictvím h; to jsme měli dokázat.

Robinsonova aritmetika Q

Robinsonova aritmetika Q je teorie v jazyce $L^A = \langle \mathrm{S}, +, \cdot, 0, \leq \rangle$ aritmetiky. Její axiomy jsou:

(Q1) $0 \neq \mathrm{S}x$	(Q2) $\mathrm{S}x = \mathrm{S}y \to x = y$
(Q3) $x + 0 = x$	(Q4) $x + \mathrm{S}y = \mathrm{S}(x + y)$
(Q5) $x \cdot 0 = 0$	(Q6) $x \cdot \mathrm{S}y = x \cdot y + x$
(Q7) $x \neq 0 \to (\exists y)(x = \mathrm{S}y)$	(Q8) $x \leq y \leftrightarrow (\exists z)(z + x = y)$.

UF.1.15. Dokazatelné formule Robinsonovy aritmetiky Q.

1. $\mathrm{Q} \vdash 0 \leq x$.

Řešení: $\mathrm{Q} \vdash x + 0 = x$, tedy dle věty o rovnosti $\mathrm{Q} \vdash x = y \to y + 0 = x$ (první výskyt termu x v $x + 0 = x$ je nahrazen termem y). Pak $\mathrm{Q} \vdash (\exists y)(x = y) \to (\exists y)(y + 0 = x)$ pomocí pravidla distribuce $\exists$. Jelikož $\vdash (\exists y)(y = x)$, dostáváme $\mathrm{Q} \vdash (\exists y)(y + 0 = x)$ pomocí MP a nakonec $\mathrm{Q} \vdash 0 \leq x$ pomocí Q8.

2. a) $\mathrm{Q} \vdash x \leq y \leftrightarrow \mathrm{S}x \leq \mathrm{S}y$, b) $\mathrm{Q} \vdash \mathrm{S}x + \underline{n} = \mathrm{S}(x + \underline{n})$ pro $n \in \mathbb{N}$.

Řešení: a) V Q máme: $x \leq y \leftrightarrow (\exists z)(z + x = y) \leftrightarrow (\exists z)(\mathrm{S}(z + x) = \mathrm{S}y) \leftrightarrow (\exists z)(z + \mathrm{S}x = \mathrm{S}y) \leftrightarrow \mathrm{S}x \leq \mathrm{S}y$. 2. $\leftrightarrow$ plyne z Q2, 3. z Q4, 1. a 4. z Q8.
b) Matematickou indukcí přes n. $\mathrm{Q} \vdash \mathrm{S}x + \underline{0} = \mathrm{S}x = \mathrm{S}(x + \underline{0})$ užitím Q3. Indukční krok. Nechť $\mathrm{Q} \vdash \mathrm{S}x + \underline{n} = \mathrm{S}(x + \underline{n})$. Pak v Q máme: $\mathrm{S}x + \mathrm{S}\underline{n} = \mathrm{S}(\mathrm{S}x + \underline{n}) = \mathrm{SS}(x + \underline{n}) = \mathrm{S}(x + \mathrm{S}\underline{n})$; užili jsme Q4 a v 2. rovnosti indukční předpoklad.

3. a) $\mathrm{Q} \vdash z + x = 0 \to x = 0$, b) $\mathrm{Q} \vdash x \leq 0 \to x = 0$.

Řešení: a) Dokazujeme v Q logický ekvivalent $x \neq 0 \to z + x \neq 0$. V Q máme $x \neq 0 \to (\exists y)(x = \mathrm{S}y \;\&\; z + x = \mathrm{S}(z + y) \neq 0)$; užili jsme Q7, Q4, Q7, tautologie $A \;\&\; (A \to B) \leftrightarrow A \;\&\; B$. Tedy $x \neq 0 \to (\exists y)(z + x \neq 0)$, tedy i $x \neq 0 \to z + x \neq 0$, protože y nemá výskyt v $z + x \neq 0$.
b) je důsledek a), neboť v Q je:

$$x \leq 0 \leftrightarrow (\exists z)(z + x = 0) \to (\exists z)(x = 0) \to x = 0.$$

4. a) $m = 0 \Leftrightarrow \mathrm{Q} \vdash \underline{m} = 0$, b) $m = n \Leftrightarrow \mathrm{Q} \vdash \underline{m} = \underline{n}$, jakmile $m, n \in \mathbb{N}$.

Řešení: a) Implikace $\Rightarrow$ plyne z $\underline{0} = 0$. Implikace $\Leftarrow$. Pro $m \neq 0$ buď $m = n + 1$. Pak $\mathrm{Q} \vdash \underline{m} = \mathrm{S}\underline{n} \neq 0$ dle Q1.

b) Implikace $\Rightarrow$ plyne z $m = n \Rightarrow \underline{m} = \underline{n}$. Implikace $\Leftarrow$. Buď $m < n$. Pak $\mathrm{Q} \vdash 0 \neq \underline{n - m}$ dle a). Odtud $\mathrm{Q} \vdash \underline{m} \neq \underline{n}$ plyne užitím Q2.

5. a) $\mathrm{Q} \vdash \underline{m + n} = \underline{m} + \underline{n}$, b) $m \leq n \Leftrightarrow \mathrm{Q} \vdash \underline{m} \leq \underline{n}$, jakmile $m, n \in \mathbb{N}$.

Řešení: a) Matematickou indukcí podle n. V Q: $\underline{m + 0} = \underline{m} = \underline{m} + 0 = \underline{m} + \underline{0}$. Indukční krok. V Q: $\underline{m + (n + 1)} = \underline{(m + n) + 1} = \mathrm{S}(\underline{m + n}) = \mathrm{S}(\underline{m} + \underline{n}) = (\underline{m} + \mathrm{S}\underline{n}) = (\underline{m} + \underline{n + 1})$. V 2. $=$ užito $\mathrm{Q} \vdash \underline{k + 1} = \mathrm{S}\underline{k}$, ve 3. indukční předpoklad, ve 4. Q4, v 5. definice numerálu.

b) Implikace $\Rightarrow$. $m \leq n \Leftrightarrow$ existuje k s $k + m = n$; pak $\mathrm{Q} \vdash \underline{k} + \underline{m} = \underline{n}$, tedy i $\mathrm{Q} \vdash (\exists z)(z + \underline{m} = \underline{n})$.

Implikace $\Leftarrow$. Nechť $\mathrm{Q} \vdash \underline{m} \leq \underline{n}$; pak $\mathrm{Q} \vdash (\exists x)(x + \underline{m} = \underline{n})$. Když $n \leq m$, tak také $\mathrm{Q} \vdash (\exists x)(x + \underline{m - n} = 0)$ dle Q2, Q4. Díky $\mathrm{Q} \vdash x + y = 0 \to y = 0$ máme $m = n$ (neboť $k \neq 0 \Rightarrow \mathrm{Q} \vdash \underline{k} \neq 0$ dle Q1). Tedy nutně $m \leq n$.

6. $\mathrm{Q} \vdash \underline{m \cdot n} = \underline{m} \cdot \underline{n}$, jakmile $m, n \in \mathbb{N}$.

Návod: Lze užít $\mathrm{Q} \vdash \underline{k + l} = \underline{k} + \underline{l}$ pro k, l z $\mathbb{N}$

Řešení: Matematickou indukcí podle n. V Q: $\underline{m \cdot 0} = 0 = \underline{m} \cdot 0 = \underline{m} \cdot \underline{0}$. Indukční krok. V Q: $\underline{m \cdot (n + 1)} = \underline{(m \cdot n) + n} = \underline{m \cdot n} + \underline{n} = \underline{m} \cdot \underline{n} + \underline{n} = \underline{m} \cdot \mathrm{S}\underline{n} = \underline{m} \cdot \underline{(n + 1)}$. V 2. $=$ užito $\mathrm{Q} \vdash \underline{k + l} = \underline{k} + \underline{l}$, v 3. indukční předpoklad, ve 4. Q6, v 5. $\mathrm{Q} \vdash \underline{k + 1} = \mathrm{S}\underline{k}$.

7. $\mathrm{Q} \vdash x \leq \underline{n} \vee \underline{n} \leq x$ pro $n \in \mathbb{N}$.

Návod: Lze užít $\mathrm{Q} \vdash 0 \leq x$, $m \leq n \Rightarrow \mathrm{Q} \vdash \underline{m} \leq \underline{n}$.

Řešení: Předpokládáme, že máme již dokázáno (s $m, n \in \mathbb{N}$)

$$\mathrm{Q} \vdash 0 \le x, \qquad m \le n \Rightarrow \mathrm{Q} \vdash \underline{m} \le \underline{n}. \tag{*}$$

Matematickou indukcí dle n. Pro $n = 0$ máme $\mathrm{Q} \vdash \underline{n} \le x$ dle (*). Indukční krok. Nechť platí $\mathrm{Q} \vdash x \le \underline{n} \vee \underline{n} \le x$. V Q máme užitím (*):

$$x \le \underline{n} \to x \le \mathrm{S}\underline{n}. \tag{**}$$

Dále také $\underline{n} \le x \to ((\underline{n} = x \;\&\; x \le \mathrm{S}\underline{n}) \vee (\underline{n} \ne x \;\&\; (\exists y)(\mathrm{S}y + \underline{n} = x)))$ a $\mathrm{S}y + \underline{n} = \mathrm{S}(y + \underline{n}) = y + \mathrm{S}\underline{n}$ užitím (*); odtud a pomocí Q8:

$$\underline{n} \le x \to ((\underline{n} = x \;\&\; x \le \mathrm{S}\underline{n}) \vee (\underline{n} \ne x \;\&\; \mathrm{S}\underline{n} \le x)). \tag{***}$$

Pomocí (**), (***) tedy máme žádané $\mathrm{Q} \vdash (x \le \underline{n} \vee \underline{n} \le x) \to (x \le \mathrm{S}\underline{n} \vee \mathrm{S}\underline{n} \le x)$.

8. $\mathrm{Q} \vdash x \le \mathrm{S}\underline{n} \leftrightarrow x \le \underline{n} \vee x = \mathrm{S}\underline{n}$ pro každé $n \in \mathbb{N}$.

Návod: Užijte $\mathrm{Q} \vdash x \le 0 \to x = 0$, $\mathrm{Q} \vdash x \le y \to \mathrm{S}x \le \mathrm{S}y$, $m \le n \Rightarrow \mathrm{Q} \vdash \underline{m} \le \underline{n}$.

Řešení: Předpokládáme, že máme již dokázáno (s $m, n \in \mathbb{N}$)

$$\mathrm{Q} \vdash x \le 0 \to x = 0, \quad \mathrm{Q} \vdash x \le y \to \mathrm{S}x \le \mathrm{S}y, \quad m \le n \Rightarrow \mathrm{Q} \vdash \underline{m} \le \underline{n}. \tag{*}$$

Implikace $\to$. Užijeme matematickou indukcí dle n. Pro $n = 0$: $\mathrm{Q} \vdash x \le \mathrm{S}\underline{0} \to x = 0 \vee x = \mathrm{S}\underline{0}$ plyne užitím (*). Indukční krok: nechť dokazované platí pro n. Pak máme v Q

$$x \le \mathrm{S}(\underline{n+1}) \to (x = 0 \vee (x \ne 0 \;\&\; A)),$$

kde A je $(\exists y)(x = Sy \;\&\; y \le \mathrm{S}\underline{n} \;\&\; (y \le \underline{n} \vee y = \mathrm{S}\underline{n}) \;\&\; (x \le \underline{n+1} \vee x = \mathrm{S}(\underline{n+1})))$; užili jsme (*), Q7. Jelikož také $x = 0 \to x \le \underline{n+1} \vee x = \mathrm{S}(\underline{n+1})$, máme i požadované $x \le \mathrm{S}(\underline{n+1}) \to x \le \underline{n+1} \vee x = \mathrm{S}(\underline{n+1})$.

Implikace $\leftarrow$. Máme $\mathrm{Q} \vdash \underline{n} \le \mathrm{S}\underline{n}$ dle (*) a odtud plyne ihned dokazované.

9. $\mathrm{Q} \vdash x \le \underline{n} \leftrightarrow \bigvee_{i \le n} x = \underline{i}$ pro každé $n \in \mathbb{N}$.

Návod: Užijte $x \le \mathrm{S}\underline{n} \to x \le \underline{n} \vee x = \mathrm{S}\underline{n}$, $m \le n \Rightarrow \mathrm{Q} \vdash \underline{m} \le \underline{n}$.

Řešení: Předpokládáme, že máme již dokázáno (s $m, n \in \mathbb{N}$)

$$\mathrm{Q} \vdash x \le \mathrm{S}\underline{n} \to x \le \underline{n} \vee x = \mathrm{S}\underline{n}, \quad m \le n \Rightarrow \mathrm{Q} \vdash \underline{m} \le \underline{n}. \tag{*}$$

Implikace $\to$. Matematickou indukcí dle n pomocí (*). Pro $n = 0$ to platí. Indukční krok: když to platí pro n, tak v Q máme:

$$x \le \underline{n+1} \to x \le \underline{n} \vee x = \underline{n+1} \to \textstyle\bigvee_{i \le n} x = \underline{i} \vee x = \underline{n+1}.$$

Implikace $\leftarrow$. Pro $i \le n$ dle (*) máme $\mathrm{Q} \vdash \underline{i} \le \underline{n}$ a odtud plyne dokazovaná implikace.

UF.1.16. Modely Robinsonovy aritmetiky Q.

1. Buď $\mathcal{A} \models \mathrm{Q}$. Pak zobrazení $h : \mathbb{N} \to A$, kde $h(n) = \underline{n}^A$, splňuje

$$h(m \diamond n) = h(m) \diamond^A h(n) \text{ pro } \diamond \text{ roven } + \text{ nebo } \cdot, \quad h(\mathrm{S}m) = \mathrm{S}^A h(m)$$
$$h(0) = 0^A,\ m \le n \Leftrightarrow h(m) \le^A h(n).$$

Říkáme, že h je *přirozené vnoření* standardního modelu do modelu $\mathcal{A}$.

Řešení: Je to bezprostřední důsledek následujících vlastností Q:

$$\mathrm{Q} \vdash \underline{m \diamond n} = \underline{m} \diamond \underline{n}, \quad \mathrm{Q} \vdash \underline{n+1} = \mathrm{S}\underline{n}, \quad \underline{0} = 0, \quad m \le n \Leftrightarrow \mathrm{Q} \vdash \underline{m} \le \underline{n}.$$

2. Buď $\mathcal{A} = \langle A, S^A, +^A, \cdot^A, 0^A, \le^A \rangle$ struktura pro jazyk aritmetiky, definovaná takto:

A je množina všech polynomů $p(X, Y)$ dvou proměnných X, Y s celočíselnými koeficienty a $p(X, Y)$ má buď koeficienty u nejvyšších mocnin kladné nebo jde o polynom nulový. (Speciálně konstantní polynom z A je právě tvaru $p(X, Y) = aX^0Y^0$ s $a \in \mathbb{N}$; ztotožňujeme jej s a.) $\mathrm{S}^A p = p + 1$, $+^A$ a $\cdot^A$ je sčítání a násobení polynomů, 0^A je polynom 0, $p \le q \Leftrightarrow$ existuje $r \in A$ s $r +^A p = q$.

Pak

a) $\mathcal{A}$ je nestandardní model Q, b) $\mathcal{A} \not\models x \le y \vee y \le x$.

Řešení: a) $\mathcal{A} \models \mathrm{Q}$ plyne ihned z vlastností sčítání a násobení a toho, že definice $\le^A$ zaručuje platnost Q8. Dále $\underline{n}^A = n$, tedy X je nestandardní prvek modelu $\mathcal{A}$. b) Jasně není $X \le^A Y$ a není $Y \le^A X$, neboť polynomy $X - Y$ a $Y - X$ nepatří do A. Tedy $\mathcal{A} \models \neg(x \le y \vee y \le x)[X, Y]$.

Aritmetika IO**.**

Aritmetika IO je extenze Robinsonovy aritmetiky o schema indukce

$$\mathrm{I}_{\mathrm{OFm}_{L^A}} = \{\mathrm{I}_\varphi;\ \varphi \in \mathrm{OFm}_{L^A}\}.$$

pro otevřené formule jazyka jazyka L^A aritmetiky. (OFm_{L^A} značí obor otevřených formulí jazyka L^A aritmetiky.)

UF.1.17. Dokazatelné formule v IO.

1. $\mathrm{IO} \vdash \mathrm{S}x + y = \mathrm{S}(x + y)$.

Řešení: Indukcí podle y. $\mathrm{S}x + 0 = \mathrm{S}x = \mathrm{S}(x + 0)$ dle Q3. Indukční krok: v Q máme

$$\mathrm{S}x + \mathrm{S}y = \mathrm{S}(\mathrm{S}x + y) = \mathrm{SS}(x + y) = \mathrm{S}(x + Sy).$$

1. rovnost plyne z Q4, 2. je indukční předpoklad, 3. dle Q4.

2. $\mathrm{IO} \vdash 0 + x = x + 0$.

Řešení: Indukcí dle x. $0 + 0 = 0 + 0$. Indukční krok: máme

$$0 + \mathrm{S}x = \mathrm{S}(0 + x) = \mathrm{S}(x + 0) = \mathrm{S}x = \mathrm{S}x + 0.$$

1. rovnost plyne z Q4, 2. dle indukčního předpokladu, 3. dle Q3, 4. dle Q3.

3. $\mathrm{IO} \vdash x + y = y + x$.

Návod: Lze předpokládat, že $0 + x = x$, $\mathrm{S}x + y = \mathrm{S}(x + y)$.

Řešení: Předpokládáme, že v IO již máme dokázáno

$$0 + x = x, \quad \mathrm{S}x + y = \mathrm{S}(x + y). \tag{*}$$

Dále indukcí dle x. $0 + y = y + 0$ platí díky (*) a užitím Q3. Indukční krok:

$$\mathrm{S}x + y = \mathrm{S}(x + y) = \mathrm{S}(y + \mathrm{S}x);$$

1. rovnost plyne z (*), 2. je indukční předpoklad, 3. plyne z Q4.

4. $\mathrm{IO} \vdash (x + y) + z = x + (y + z)$.

Návod: Lze užít $0 + x = x$, $\mathrm{S}(x + y) = \mathrm{S}x + y$.

Řešení: Předpokládáme, že v IO již máme dokázáno

$$0 + x = x, \quad \mathrm{S}x + y = \mathrm{S}(x + y). \tag{*}$$

Dále indukcí dle x. Pro $x = 0$ to platí: $(0 + y) + z = y + z = 0 + (y + z)$ užitím (*). Indukční krok:

$$(\mathrm{S}x + y) + z = \mathrm{S}(x + y) + z = \mathrm{S}((x + y) + z) = \mathrm{S}(x + (y + z)).$$

1. a 2. rovnost plyne z (*), 3. z indukčního předpokladu.

5. $\mathrm{IO} \vdash 0 \cdot x = 0$.

Řešení: Indukcí podle x. Platí $0 \cdot 0 = 0$ dle Q5. Indukční krok: $0 \cdot \mathrm{S}x = 0 \cdot x + 0 = 0$ užitím Q6 a Q5.

6. $\mathrm{IO} \vdash \mathrm{S}x \cdot y = xy + y$.

Návod: Lze užít $\mathrm{S}x + y = \mathrm{S}(x + y)$ a komutativitu a asociativitu $+$.

Řešení: Předpokládáme, že v IO již máme dokázáno

$$\mathrm{S}x + y = \mathrm{S}(x + y), \quad \text{komutativita a asociativita } +. \tag{*}$$

Indukcí dle y. Je $\mathrm{S}x \cdot 0 = 0 = x \cdot 0 + 0$ užitím Q5, Q6. Indukční krok: $\mathrm{S}x \cdot \mathrm{S}y = \mathrm{S}(\mathrm{S}x \cdot y + x) = \mathrm{S}((xy + y) + x) = \mathrm{S}((xy + x) + y) = \mathrm{S}(x \cdot \mathrm{S}y + y) = x \cdot \mathrm{S}y + \mathrm{S}y$. 1. rovnost dává Q6, Q4, 2. plyne z indukčního předpokladu, 3. a 4. plyne užitím (*).

7. $\mathrm{IO} \vdash xy = yx$.

Návod: Lze užít $0 \cdot x = 0$, $\mathrm{S}x \cdot y = xy + y$.

Řešení: Předpokládáme, že v IO již máme dokázáno

$$0 \cdot x = 0, \quad \mathrm{S}x + y = \mathrm{S}(x + y). \tag{*}$$

Indukcí dle x. Je $0 \cdot y = 0 = y \cdot 0$ užitím (*) a Q5. Indukční krok: $\mathrm{S}x \cdot y = xy + y = yx + y = y \cdot \mathrm{S}x$. 1. rovnost platí dle (*), 2. plyne z indukčního předpokladu.

8. $\mathrm{IO} \vdash (x \neq 0 \vee y \neq 0) \to x + y \neq 0$.

Návod: Lze užít $\mathrm{S}x + y = \mathrm{S}(x + y)$.

Řešení: Předpokládáme, že v IO již máme dokázáno

$$\mathrm{S}x + y = \mathrm{S}(x + y). \qquad (*)$$

Máme $x \neq 0 \to (\exists z)(\mathrm{S}z = x)$ dle Q7. Dále $(\exists z)(\mathrm{S}z = x) \to x + y \neq 0$ dle (*) a Q1. Užitím tranzitivity implikace pak máme $\mathrm{IO} \vdash x \neq 0 \to x + y \neq 0$. Stejně dokážeme $\mathrm{IO} \vdash y \neq 0 \to x + y \neq 0$, přičemž místo (*) užijeme Q4. Pravidlo rozbor případů dá výsledek.

9. $\mathrm{IO} \vdash x \neq 0 \to y \neq x + y$.

Řešení: Indukcí podle y. Platí $x \neq 0 \to 0 \neq x + 0$ užitím Q3. Indukční krok platí, neboť to je formule

$$(x \neq 0 \to y \neq x + y) \to (x \neq 0 \to \mathrm{S}y \neq x + \mathrm{S}y).$$

Má totiž tvar $(\varphi \to \psi) \to (\varphi \to \psi')$, kde φ je $x \neq 0$, ψ je $y \neq x+y$, ψ' je $\mathrm{S}y \neq x+\mathrm{S}y$. Přitom $(\varphi \to \psi)$ & $(\psi \to \psi') \to (\varphi \to \psi')$ je tautologie a $\mathrm{Q} \vdash \psi \to \psi'$ díky Q2, Q4, tedy $\mathrm{Q} \vdash (\varphi \to \psi) \to (\varphi \to \psi')$.

10. $\mathrm{IO} \vdash x \leq x \ \&\ (x \leq y \,\&\, y \leq x \to x = y) \ \&\ (x \leq y \,\&\, y \leq z \to x \leq z)$.

Návod: Lze užít komutativitu a asociativitu $+$, $x + y = 0 \to x = 0 = y$, $x + y = y \to x = 0$.

Řešení: Předpokládáme, že v IO již je dokázána

$$\text{komutativita a asociativita } +, \quad x + y = 0 \to x = 0 = y, \quad x + y = y \to x = 0. \qquad (*)$$

a) $x \leq x$ plyne z $0 + x = x$, Q8 a komutativity $+$.
b) Dokážeme (v IO), že $(x \leq y \,\&\, y \leq x) \to x = y$. Máme $(x \leq y \,\&\, y \leq x) \to (\exists z, z')(z + x = y \,\&\, z' + y = x)$, tedy i $(x \leq y \,\&\, y \leq x) \to (\exists z, z')(z' + z + x = x \,\&\, (z + x = y \,\&\, z' + y = x))$ užitím (*). Opětovným užitím (*) získáme $(x \leq y \,\&\, y \leq x) \to (\exists z, z')(z' = 0 = z \,\&\, (z + x = y \,\&\, z' + y = x))$, tj. i $x \leq y \,\&\, y \leq x \to x = y$.
c) Dokážeme $(x \leq y \,\&\, y \leq z \to x \leq z)$. Máme (v IO) $(x \leq y \,\&\, y \leq z) \to (\exists u, u')(u + x = y \,\&\, u' + y = z \,\&\, u' + u + x = z) \to (\exists v)(v + x = z) \to x \leq z$ užitím Q8 a (*) (a vět o rovnosti).

11. $\mathrm{IO} \vdash x \leq y \vee y \leq x$.

Návod: Lze užít $\mathrm{S}x + y = x + \mathrm{S}y$.

Řešení: Předpokládáme, že v IO je již dokázané

$$\mathrm{S}x + y = x + \mathrm{S}y. \qquad (*)$$

Indukcí dle x. Pro $x = 0$ máme (v Q) $0 \leq y$, tedy i $0 \leq y \vee y \leq 0$. Dokážeme indukční krok. Předpoklad je $(\exists z)(z + x = y) \vee y \leq x$. Platí (v IO):
a) $(\exists z)(z + x = y) \to x = y \vee (\exists z')(\mathrm{S}z' + x = y) \to x = y \vee \mathrm{S}x \leq y$. Užili jsme Q7, Q8, (*).
b) $y \leq x \to y \leq \mathrm{S}x$ (díky $z + y = x \to \mathrm{S}z + y = \mathrm{S}x$; užili jsme (*)).
Z a), b) tedy dostaneme požadovanou implikaci:

$$(x \leq y \vee y \leq x) \ \to\ (x = y \vee \mathrm{S}x \leq y \vee y \leq \mathrm{S}x) \ \to\ (\mathrm{S}x \leq y \vee y \leq \mathrm{S}x). \qquad (**)$$

Použili jsme $T \vdash \varphi \to \varphi'$, $T \vdash \psi \to \psi' \Rightarrow T \vdash (\varphi \vee \psi) \to (\varphi' \vee \psi')$, což plyne z tautologie $(\varphi \to \varphi')$ & $(\psi \to \psi') \to ((\varphi \vee \psi) \to (\varphi' \vee \psi'))$; odtud jsme dostali prvou implikaci. Druhá plyne díky implikaci $x = y \vee y \leq \mathrm{S}x \ \to\ y \leq \mathrm{S}x$, jejíž platnost plyne z $x = y \to y \leq \mathrm{S}x$ a to z $\mathrm{S}0 + y = \mathrm{S}0 + x = \mathrm{S}x$.