4. Logika – nerozhodnutelnost *(MP leden 2010)*

Definovatelné množiny

Nechť $\mathbf{A}$ je L-struktura a $\varphi(x_1, \dots, x_n)$ jsou L-formule a

$$D = \{\langle a_1, \dots, a_n \rangle \in A^n \mid \mathbf{A} \models \varphi[a_1, \dots, a_n]\}.$$

Pak D je *množina definovaná v* $\mathbf{A}$ *formulí* $\varphi(x_1, \dots, x_n)$ *bez parametrů*. D značíme $\varphi(\mathbf{A})$.

$\Sigma_{n,L}$ a $\Pi_{n,L}$-formule

$\Sigma_{n,L}$ a $\Pi_{n,L}$-formule definujeme induktivně:

- $\Sigma_{0,L}$-formule a $\Pi_{0,L}$-formule jsou právě omezené formule jazyka L.
- $\Sigma_{n+1,L}$-formule jsou právě tvaru $(\exists \overline{x})\varphi$, kde φ je nějaká $\Pi_{n,L}$-formule.
- $\Pi_{n+1,L}$-formule jsou právě tvaru $(\forall \overline{x})\varphi$, kde φ je nějaká $\Sigma_{n,L}$-formule.

$\Delta_{n,L}$-formule logicky ekvivalentní jak nějaké $\Sigma_{n,L}$-formuli, tak nějaké $\Pi_{n,L}$-formuli.

Kolekce

Nechť jazyk L obsahuje binární predikátový symbol $\leq$. *Axiom kolekce* pro L-formuli φ dle různých proměnných $x, \overline{y}$ je formule

$$(\forall x \leq u)(\exists \overline{y})\varphi \rightarrow (\exists v)(\forall x \leq u)(\exists \overline{y} \leq v)\varphi,$$

kde u, v se nevyskytují ve φ a jsou různé od všech $x, \overline{y}$. Značíme ji $B_\varphi^{x,\overline{y}}$, či B_φ.

Numerický jazyk

Numerický jazyk je jazyk obsahující $\langle S, 0 \rangle$, kde S je unární funkční symbol *operace následníka* a 0 je konstantní symbol. Teorie v numerickém jazyce je *numerická teorie*. Konstantní term $S \cdots S0$, S aplikováno n-krát značíme $\underline{n}$ a nazýváme *n-tý numerál*.

Pak zavádíme pojem *aritmetika*, což je numerická teorie s jazykem

$$L^A = \langle S, +, \cdot, 0, \leq \rangle,$$

kde $+$ a $\cdot$ jsou binární funkční symboly a $\leq$ je binární relační symbol.

Robinsonova aritmetika

Robinsonova aritmetika Q je L^A-teorie [1] s axiomy:

(Q1)	$0 \neq Sx$	(Q2)	$Sx = Sy \ \rightarrow\ x = y$
(Q3)	$x + 0 = x$	(Q4)	$x + Sy = S(y + y)$
(Q5)	$x \cdot 0 = x$	(Q6)	$y \cdot Sy = x \cdot y + x$
(Q7)	$x \neq 0 \ \rightarrow\ (\exists y)(x = Sy)$	(Q8)	$x \leq y \ \leftrightarrow\ (\exists z)(z + x = y)$

Standardní model Robinsonovy aritmetiky je model $\mathbf{N} = \langle N, S, +, \cdot, 0, \leq \rangle$.

[1] L^A-teorie je teorie jazyka $\langle S, +, \cdot, 0, \leq \rangle$, kde S je operace následníka a $\underline{n}$ značí n-tý numerál, tedy S aplikováno n-krát na konstantní term 0.

Peanova aritmetika

Peanova aritmetika P je rozšíření Q o *schema indukce* I, tvořené *axiomy indukce* I^x_φ, které mají tvar

$$(\varphi(0) \mathbin{\&} (\forall x)(\varphi(x) \;\rightarrow\; \varphi(Sx))) \;\rightarrow\; (\forall x)\varphi(x).$$

Aritmetiky $I\Sigma$

Aritmetika $I\Sigma_n$ je rozšíření Q o schema indukce I_{Σ_n}, tvořené všemi axiomy indukce I^x_φ, kde φ je Σ_n-formule.

Aritmetika $I\Sigma_{n,L}$⟨2⟩ je rozšíření Q o schema indukce $I_{\Sigma_{n,L}}$, tvořené všemi axiomy indukce I^x_φ, kde φ je $\Sigma_{n,L}$-formule.

Aritmetizace – idea via $^\Delta$N a 4.2.11

IS-teorie je teorie S, která obsahuje axiomy $I\Sigma_{1,L(S)}$.

Δ_1*-extenze* teorie S je teorie S' získaná z S postupně prováděnou extenzí o symbol definovaný $\Delta_{1,L(S)}$-formulí právě extendované teorie S_0. Značíme ji $\mathbf{A}^{S'}$. Každý model $\mathbf{A} \models S$ lze jednoznačně expandovat do modelu S'.

Buď S nějaká IS-teroie. *Teorie* S^Δ se získá tak, že k ní přidáme pro každou Δ_1-formuli jazyka aritmetiky φ (relační) symbol $\mathcal{O}_\varphi$ a jeho definici formulí φ, přičemž splňuje-li φ podmínku existence a jednoznačnosti, přidáme ještě i funkční symbol $\mathcal{O}_\varphi$. Když $\mathbf{A} \models S^\Delta$, značíme ji $\mathbf{A}^{S^\Delta}$ či $\mathbf{A}^\Delta$ a interpretaci symbolu $\mathcal{O}$ teorie $\mathbf{A}^{S^\Delta}$ značíme $\mathcal{O}^\Delta$.

Snaha aritmetizace je převést vše na přirozená čísla. Každou formuli tedy potřebujeme zakódovat nějakým přirozeným číslem. Je několik možností, jak formule kódovat. Začněme kódováním dvojic – např. použijme Cantorovo diagonální uspořádání.

$a\backslash b$	0	1	2
0	0	1	3
1	2	4	.
2	5	.	.

Toto kódování dvojici (a, b) přiřadí číslo

$$\langle a, b\rangle = \frac{(a+b)(a+b+1)}{2} + a.$$

Když už umíme zakódovat dvojice, n-tice můžeme kódovat následovně:

$$\langle x_1, \ldots, x_{n+1}\rangle_{n+1} = \langle x_1, \langle x_2, \ldots, x_{n+1}\rangle_n\rangle,$$

⟨2⟩ L je extenze jazyka L^A aritmetiky.

kde index n u pravé závorky značí kód n-tice. Závorky bez indexu značí kód dvojice, jak jsme ho zavedli. Jelikož formule jsou konečné n-sekvence, můžeme již kódovat formule.

Teorie BAS se získá jako Δ_1-extenze teorie $I\Sigma_1$. Definuje se binární funkční symbol

$$(x, y) = z \;\leftrightarrow\; \underline{2}z = (x + y + \underline{1})(x + y) + \underline{2}x,$$

kde (x, y) se nazývá *kód uspořádané dvojice*. Dále se definuje unární funkční symbol 2^x, který se nazývá *exponenciální dvojka*. Platí základní vlastnosti. Dále definujeme mnoho funkčních a relačních symbolů.

Řekneme-li, že A *je* Σ_n*-množina*, znamená to, že A je množina definovaná bez parametrů v $\mathbf{N}$ nějakou Σ_n-formulí. Obdobně pro Π_n a Δ_n.

Platí, že $A \subseteq \mathbf{N}^k$ je Δ_n, právě když A i $\mathbf{N}^k \setminus A$ je Σ_n.

Dále si zavedeme formuli $\varphi_{Ax}^{Prf}(x, y)$ jazyka $L(S^\Delta)$ vyjadřující, že y je důkazem x ⟨3⟩ a teorii extendujeme o symboly

$\mathrm{Prf}_{Ax}(x, y) \leftrightarrow \varphi_{Ax}^{Prf}(x, y)$	y je důkazem x
$\mathrm{Th}_{Ax}(x) \leftrightarrow (\exists y)(\mathrm{Prf}_{Ax}(x, y)\ \&\ \ \mathrm{Sent}(x))$	$x \in \mathrm{Th(Ax)}$, tzn. dokazatelná sentence
$\mathrm{nTh}_{Ax}(x) \leftrightarrow \mathrm{Th}_{Ax}(\langle\neg, x\rangle)$.	$x \notin \mathrm{Th(Ax)}$

Zavedeme strukturu ${}^\Delta\mathbf{N}$ jako model teorie SA^Δ, kde $\mathrm{SA} = Th(\mathbf{N})$, tedy tzv. standardní aritmetika.

$${}^\Delta\mathbf{N} \models SA^\Delta$$

To znamená, že teorii SA rozšíříme o symboly definované Δ_1-formulemi. Pro každý takový symbol $\mathcal{O}$ teorie SA^Δ je $\mathcal{O}^\Delta$ jeho interpretace v ${}^\Delta\mathbf{N}$.

Pro jazyk L ve struktuře ${}^\Delta\mathbf{N}$ je L*-axiomatika* množina $Ax \subseteq {}^\Delta Fm_L$. Teorie je nad ${}^\Delta\mathbf{N}$ je jazyk L v ${}^\Delta\mathbf{N}$ a nějaká L-axiomatika.

Buď T teorie nad ${}^\Delta\mathbf{N}$. Označme expanzi $\langle {}^\Delta\mathbf{N}, Ax_T\rangle$ do modelu $\mathrm{SA}^\Delta(Ax)$ jako ${}^\Delta\mathbf{N}(T)$.

Říkáme, že T je Δ_1*-axiomatizovaná*, je-li její axiomatika Δ_1. Dále T je Δ_1*-axiomatizovatelná*, je-li T ekvivalentní nějaké Δ_1-axiomatizované teorii. Obdobně pro Σ_1.

Jde nám tedy o to, že opět vše převádíme na čísla. To, že je jazyk z ${}^\Delta\mathbf{N}$ a teorie nad ${}^\Delta\mathbf{N}$ znamená, že je vše kódováno přirozenými čísly. Daná axiomatika jsou pak zakódované axiomy teorie.

Místo $\mathrm{Prf}_{Ax}(x, y)$ píšeme $\mathrm{Prf}_T = \{\langle a, b\rangle \in \mathbf{N}^2 \mid \langle {}^\Delta\mathbf{N}, Ax_T\rangle \models \varphi_{Ax}^{Prf}[a, b]\}$.

⟨3⟩ $Ax(x)$ je unární relační symbol vyjadřující, že x je mimologickým axiomem T.

Rozhodnutelnost

Teorie T je *rozhodnutelná*, když Th_T je Δ_1. Jinak je *nerozhodnutelná.*

TVRZENÍ 4.2.13

1) *Když teorie T je $\Delta_1[\Sigma_1]$-axiomatizovaná, Prf_T je $\Delta_1[\Sigma_1]$ a Th_T i nTh_T jsou Σ_1.*
2) *Kompletní Σ_1-axiomatizovaná teorie T je rozhodnutelná.*

Důkaz: První plyne z definic Prf_T a Th_T a nTh_T.

Druhé je již důsledek prvního, neboť pokud je T Σ_1-axiomatizovaná, tak Th_T je Σ_1 a jelikož je kompletní, tak se dokáže, že $\mathbf{N}\setminus \mathrm{Th}_T$ je Σ_1. Neboť x není z Th_T právě tehdy, když je z nTh_T (což je Σ_1), nebo to není sentence (což je asi definováno Δ_1 formulí). Tedy Th_T je Δ_1, tedy T je rozhodnutelná. ♡

Relace $R \subseteq \mathbf{N}^2$ je Σ_1-*kompletace* L-teorie T, jestliže

1) R je Σ_1 (množina).
2) Pro každé $a \in \mathrm{dom}(R)$ je $R[a]$ L-axiomatika kompletní extenze teorie T.
3) Každá kompletní L-extenze teorie T je ekvivalentní L-teorii s axiomatikou tvaru $R[a]$.

TVRZENÍ 4.2.15 (Kompletační kriterium rozhodnutelnosti)

Když teorie T je Σ_1-axiomatizovaná a má Σ_1-kompletaci, je rozhodnutelná.

Reprezentovatelnost

Funkce $F : \mathbf{N}^n \to \mathbf{N}$ a relace $R \subseteq \mathbf{N}^n$ reprezentujeme v T nějakou formulí.

TVRZENÍ 4.3.2 (O reprezentaci funkcí a relací z Δ_1 v Robinsonově aritmetice Q)

1) *Každá totální funkce ze Σ_1 je reprezentována v Q nějakou Σ_1-formulí.*
2) *Každá relace z Δ_1 je reprezentována v Q nějakou Σ_1 formulí.*

Nerozhodnutelnost

VĚTA 4.3.3 (O Δ_1-neoddělitelnosti)

Buď T bezesporná numerická L-teorie a nechť každá Δ_1-podmnožina $\mathbf{N}$ je reprezentovaná v T.

1) *Když $P \subseteq \mathbf{N}$ odděluje Th_T a nTh_T (tedy obsahuje jednu a je disjunktní s druhou), tak platí nějaký ošklivý štrúdl pro nějakou ještě ošklivější relaci.*
2) *Th_T a nTh_T nelze oddělit Δ_1-množinou $A \subseteq \mathbf{N}$ a speciálně je tedy T nerozhodnutelná.*
3) *Když T je navíc Σ_1-axiomatizovaná a A je Δ_1 nadmnožina $Th_T \cup nTh_T$, tak $A \setminus (Th_T \cup nTh_T)$ není Σ_1.*

VĚTA 4.3.4 (O nerozhodnutelnosti)

Bezesporná teorie rozšiřující Robinsonovu aritmetiku Q je nerozhodnutelná. Je-li navíc Σ_1-axiomatizovaná, není kompletní.

Bezesporná teorie T rozšiřující Robinsonovu aritmetiku Q je bezesporná numerická teorie a platí, že každá Δ_1 množina lze v Q reprezentovat. Proto je T nerozhodnutelná (dle 4.3.3.2)). Je-li Σ_1-axiomatizovaná, tak není kompletní, jinak bychom se dostali do sporu s 4.2.13.2).

TVRZENÍ 4.3.6

1) *Buď T' extenze T o konečně definic nebo jednoduchá extenze T o konečně axiomů. Pak je-li T' nerozhodnutelná, je i T nerozhodnutelná.*
2) *Buď T' konzervativní extenze T. Pak je-li T nerozhodnutelná, je T' nerozhondutelná.*

TVRZENÍ 4.3.7

Teorie T v jazyce aritmetiky, která nemá žádné mimologické axiomy, je nerozhodnutelná a nekompletní.

Aritmetika Q je nerozhodnutelná (dle 4.3.4 (O nerozhodnutelnosti)) a je to jednoduchá extenze T o konečně axiomů (o 8), tedy podle 4.3.6 je i T nerozhodnutelná. A jelikož má Δ_1-axiomatiku (prázdnou?), což je i Σ_1-axiomatika, tak je nekompletní (dle 4.3.12.2)).

Struktura $\mathbf{A}$ je *silně nerozhodnutelná*, je-li nerozhodnutelná každá teorie, která ji má za model.

Buď $\mathbf{A}$ struktura s jazykem konečné signatury. Struktura $\mathbf{A}$ je *definovatelná* ve struktuře $\mathbf{B}$, jestliže $A \subseteq B$ je definovaná bez parametrů v $\mathbf{B}$ a každá relace nebo funkce z $\mathbf{A}$ je restrikcí na A nějaké relace nebo funkce definované bez parametrů v $\mathbf{B}$.

TVRZENÍ 4.3.9

Standardní model $\mathbf{B}$ přirozených čísel je silně nerozhodnutelná struktura.

Důkaz: Buď $\mathbf{N} \models T$. Pak $T \cup Q$ je bezesporné rozšíření Q, tedy dle 4.3.4 to je nerozhodnutelná teorie. A jelikož je to jednoduché rozšíření T o konečně axiomů, tak je i T dle 4.3.6 nerozhodnutelná.

VĚTA 4.3.10 (O silně nerozhodnutelné struktuře)

Je-li $\mathbf{A}$ silně nerozhodnutelná struktura definovatelná ve struktuře $\mathbf{B}$, je i $\mathbf{B}$ silně nerozhodnutelná struktura.

VĚTA 4.3.11

1) *Struktura $\mathbf{B} = \langle \mathbf{Z}, +, -, ., 0, 1 \rangle$ celých čísel je silně nerozhodnutelná.*
   Důsledek: Teorie okruhů, komutativních okruhů a oborů integrity jsou nerozhodnutelné.
2) *Struktura $\langle \mathbf{Q}, +, -, ., 0, 1 \rangle$ racionálních čísel je silně nerozhodnutelná.*
   Důsledek: Teorie těles a teorie těles charakteristiky 0 jsou nerozhodnutelné.

Stačí jen ukázat, že standardní model je definovatelný ve struktuře $\mathbf{B}$ tak, že $\mathbf{N}$ definujeme v $\mathbf{Z}$ pomocí formule $\varphi(x)$ v jazyce struktury $\mathbf{B}$

$$(\exists a, b, c, d)(a \cdot a + b \cdot b + c \cdot c + d \cdot d = x).$$

Že tato formule definuje právě přirozená čísla nám dává Lagrangeova věta o 4 čtvercích. Dále stačí jen definovat následníka jako $S(a) = a + 1$ a $\leq$ jako

$$a \leq b \leftrightarrow (\exists c \in \mathbf{N})(a + c = b).$$

(První Gödelova věta)

LEMMA 4.3.12 (Diagonální lemma) *Buď T rozšíření teorie Q. Pak pro formuli $\varphi(v_0)$ teorie T existuje její sentence $\varphi*$ tak, že $T \vdash \varphi* \leftrightarrow \varphi(\underline{\varphi*})$.*

Formule $\tau(x)$ numerické teorie T je *definice pravdy v T*, jestliže pro každou sentenci φ teorie T platí $T \vdash \varphi \leftrightarrow \tau(\underline{\varphi})$.

TVRZENÍ 4.3.14

1) V bezesporném rozšíření teorie Q neexistuje definice pravdy.
2) Th($\mathbf{N}$) není aritmetická množina.

VĚTA 4.3.15 (První Gödlova věta) *Buď T bezesporná Δ_1-axiomatizované rozšíření Q. Pak existuje Π_1-sentence pravdivá v $\mathbf{N}$ a nedokazatelná v T.*

Speciálně když $\mathbf{N} \models T$, tak existuje sentence nezávislá v T.

Rekurze a Δ_1-definované funkce a relace

Rekurzivní funkce definujeme induktivně následujícími pravidly:

RF1. Funkce $S(x) = x + 1$ (následník), $I_i^n(x_1, \ldots, x_n) = x_i$ pro $0 < i \leq n$ a $0 < n$ (i-tá projekce), $x + y$, $x \cdot y$ a $K_<$ jsou základní rekurzivní funkce.

RF2. Je-li H k-ární rekurzivní funkce a $G_1, \ldots G_k$ jsou m-ární rekurzivní funkce, je složená funkce $F(\overline{a}) = H(G_1(\overline{a}), \ldots, G_n(\overline{a}))$ rekurzivní.

RF3. Je-li G speciální⟨4⟩ rekurzivní $(m + 1)$-ární funkce, pak je $\mu x(G(\overline{a}, x) = 0)$⟨5⟩ rekurzivní m-ární funkce.

TVRZENÍ 4.4.7

1) Totální číselná funkce, resp. relace je rekurzivní, právě když je z Δ_1.
2) Číselná relace je rekurzivně spočetná, právě když je ze Σ_1.

Silně nerozhodnutelné struktury

Expanze L-struktury $\mathbf{A}$ je *nepodstatná*, je-li její jazyk extenzí L pouze o konstantní symboly.

LEMMA 4.5.2 (O nepodstatné expanzi)

Je-li nepodstatná expanze $\mathbf{A}'$ struktury $\mathbf{A}$ silně nerozhodnutelná, je $\mathbf{A}$ silně nerozhodnutelná.

TVRZENÍ 4.5.3

Grupa $\langle Perm(\mathbf{Z}), \cdot, Id\rangle$ je silně nerozhodnutelná.

⟨4⟩ Funkce F s aritou $(n + 1)$ je *speciální*, platí-li $(\forall \overline{a})(\exists x)F(\overline{a}, x) = 0$.
⟨5⟩ Vrací minimální x, pro které platí $G(\overline{a}, x) = 0$.

TVRZENÍ 4.5.4

Buď $\mathbf{D_4} = \langle \mathbf{N}, R_4^D \rangle$, *kde*

$$R_4^D = \{\langle 1, m, n, m+n \rangle \ \mid m, n, \in \mathbf{N}\} \cup \{\langle 0, m, n, m \cdot n \rangle \ \mid m, n, \in \mathbf{N}\}.$$

Struktura $\mathbf{D_4}$ *je silně nerozhodnutelná.*

Důsledek: Každý jazyk $\langle R \rangle$ *(prázdná teorie s tímto jazykem), kde* R *je kvartérní relační symbol, je nerozhodnutelný.*

Standardní model je definovatelný ve struktuře $\langle \mathbf{N}, +, -, \cdot, 0, 1 \rangle$, která je zase definovatelná v $\mathbf{D_4}$ (stačí jen definovat konstanty 0 a 1 a binární funkční symboly $\cdot$ a $+$ pomocí formulí v $\mathbf{D_4}$). Jelikož standardní model je silně nerozhodnutelný, tak i $\langle \mathbf{N}, +, -, \cdot, 0, 1 \rangle$ a $\mathbf{D_4}$ jsou silně nerozhodnutelné.

TVRZENÍ 4.5.5

Buď $\mathbf{D_2} = \langle \mathbf{N} \cup \mathbf{N}^2 \cup \{\infty\}, R_2^D \rangle$, *kde* R_2^D *je*

$$\{\langle \langle m, n \rangle, \langle m', n' \rangle \rangle \mid R_4^D(m, n, m', n'))\} \cup$$

$$\cup \{\langle m, \langle m, n \rangle \rangle \mid m, n \in \mathbf{N}\} \cup$$

$$\cup \{\langle \langle m, n \rangle, n \rangle \mid m, n \in \mathbf{N}\} \cup$$

$$\cup \{\langle \infty, m \rangle \mid m \in \mathbf{N}\} \cup$$

$$\cup \{\langle \langle m, n \rangle, \infty \rangle \mid m, n \in \mathbf{N}\} \cup$$

Struktura $\mathbf{D_2}$ *je silně nerozhodnutelná.*

Důsledek: Každý jazyk $\langle R \rangle$ *(prázdná teorie s tímto jazykem), kde* R *je binární relační symbol, je nerozhodnutelný.*

Definujme $\mathbf{D_4}$ v nepodstatné expanzi $\mathbf{D_2}$, kterou rozšíříme o konstantní symbol e^D značící ∞. Pak relační symbol $R_4^D(x, y, x', y')$ definujeme formulí $\varphi(x, y, x', y')$ tvaru

$$R_2(e, x) \ \& \ R_2(e, y) \ \& \ R_2(e, x') \ \& \ R_2(e, y') \ \&$$

$$(\exists u, u')(\ \ R_2(u, e) \ \& \ R_2(u', e) \ \& \ R_2(u, u') \ \&$$

$$\& \ R_2(x, u) \ \& \ R_2(u, y) \ \& \ R_2(x', u') \ \& \ R_2(u', y') \ \ ).$$

TVRZENÍ 4.5.6

Existuje silně nerozhodnutelný (obyčejný) graf.

Definujme $\mathbf{D_2}$ v nepodstatné expanzi $\mathbf{A}'$ struktury $\langle A, P^A \rangle$.

TVRZENÍ 4.5.7

1) *Existuje silně nerozhodnutelný svaz.*
2) *Existuje silně nerozhodnutelná struktura* $\langle B, F^B, G^B \rangle$, *kde* F^B, G^B *jsou unární funkce.*

Najdeme strukturu izomorfní s $\mathbf{A}$ definovatelnou v $\mathbf{B} = \langle B, \leq^B \rangle$.

Definujme $\mathbf{A}$ v $\mathbf{B}$.