Kapitola 1

(draft) Nerozhodnutelnost a neúplnost

[TODO]

1.1 (draft) Rozhodnutelnost

[TODO]

Rekurzivní axiomatizace a rozhodnutelnost

- Intuitivní pojem *"algoritmus"* lze přesně formalizovat (např. pomocí TS).
- Teorie T je *rekurzivně axiomatizovaná*, pokud existuje algoritmus, který pro každou vstupní formuli φ skončí a oznámí, zda $\varphi \in T$.
- Teorie T je *rozhodnutelná*, pokud existuje algoritmus, který pro každou vstupní formuli φ skončí a oznámí, zda $\varphi \in Thm(T)$.
- Teorie T je *částečně rozhodnutelná*, pokud existuje algoritmus, který pro každou vstupní formuli φ skončí, právě když $\varphi \in Thm(T)$.

Tvrzení *Pro každou rekurzivně axiomatizovanou teorii T,*

(i) T je částečně rozhodnutelná,

(ii) je-li navíc T kompletní, je T rozhodnutelná.

Důkaz Konstrukce systematického tabla z T s $F\varphi$ v kořeni poskytuje algoritmus, který rozpoznává $T \vdash \varphi$. Je-li navíc T kompletní, paralelní konstrukce pro $F\varphi$ resp. $T\varphi$ v kořeni rozhoduje, zda $T \vdash \varphi$ či $T \vdash \neg\varphi$. $\square$

Rekurzivně spočetná kompletace

Co když efektivně popíšeme všechny jednoduché kompletní extenze?

Řekneme, že množina všech (až na ekvivalenci) jednoduchých kompletních extenzí teorie T je *rekurzivně spočetná*, existuje-li algoritmus $\alpha(i, j)$, který generuje i-tý axiom j-té extenze (při nějakém očíslování), případně oznámí, že (takový axiom či extenze) neexistuje.

Tvrzení *Je-li teorie T rekurzivně axiomatizovaná a množina všech (až na ekvivalenci) jejích jednoduchých kompletních extenzí je rekurzivně spočetná, je T rozhodnutelná.*

Důkaz Díky rek. axiomatizaci poskytuje konstrukce systematického tabla z T s $F\varphi$ v kořeni algoritmus pro rozpoznání $T \vdash \varphi$. Pokud ale $T \nvdash \varphi$, pak $T' \vdash \neg\varphi$ v nějaké jednoduché kompletní extenzi T' teorie T. To lze rozpoznat paralelní postupnou konstrukcí systematických tabel pro $T\varphi$ z jednotlivých extenzí. V i-tém stupni se sestrojí tabla do i kroků pro prvních i extenzí. $\square$

1.1.1 (draft) Rozhodnutelné teorie

[TODO]

Příklady rozhodnutelných teorií

Následující teorie jsou rozhodnutelné, ačkoliv jsou nekompletní.

- teorie čisté rovnosti; bez axiomů v jazyce $L = \langle\rangle$ s rovností,
- teorie unárního predikátu; bez axiomů v jazyce $L = \langle U \rangle$ s rovností, kde U je unární relační symbol,
- teorie hustých lineárních uspořádání $DeLO^*$,
- teorie algebraicky uzavřených těles v jazyce $L = \langle +, -, \cdot, 0, 1\rangle$ s rovností, s axiomy teorie těles a navíc axiomy pro každé $n \geq 1$,

  $$(\forall x_{n-1}) \dots (\forall x_0)(\exists y)(y^n + x_{n-1} \cdot y^{n-1} + \dots + x_1 \cdot y + x_0 = 0),$$

  kde y^k je zkratka za term $y \cdot y \cdot \ \cdots \ \cdot y$ ($\cdot$ aplikováno $(k-1)$-krát).
- teorie komutativních grup,
- teorie Booleových algeber.

1.1.2 (draft) Rekurzivní axiomatizovatelnost

[TODO]

Rekurzivní axiomatizovatelnost

Dají se matematické struktury "efektivně" popsat?

- Třída $K \subseteq M(L)$ je *rekurzivně axiomatizovatelná*, pokud existuje rekurzivně axiomatizovaná teorie T jazyka L s $M(T) = K$.
- Teorie T je rekurzivně axiomatizovatelná, pokud $M(T)$ je rekurzivně axiomatizovatelná.

Tvrzení *Pro každou konečnou strukturu $\mathcal{A}$ v konečném jazyce s rovností je* $\mathrm{Th}(\mathcal{A})$ *rekurzivně axiomatizovatelná. Tedy,* $\mathrm{Th}(\mathcal{A})$ *je rozhodnutelná.*

Důkaz Nechť $A = \{a_1, \ldots, a_n\}$. Teorii $\mathrm{Th}(\mathcal{A})$ axiomatizujeme jednou sentencí (tedy rekurzivně) kompletně popisující $\mathcal{A}$. Bude tvaru *"existuje právě n prvků $a_1, \ldots, a_n$ splňujících právě ty základní vztahy o funkčních hodnotách a relacích, které platí ve struktuře $\mathcal{A}$."* $\square$

Příklady rekurzivní axiomatizovatelnosti

Následující struktury $\mathcal{A}$ mají rekurzivně axiomatizovatelnou teorii $\mathrm{Th}(\mathcal{A})$.

- $\langle \mathbb{Z}, \leq \rangle$, teorií diskrétních lineárních uspořádání,
- $\langle \mathbb{Q}, \leq \rangle$, teorií hustých lineárních uspořádání bez konců (*DeLO*),
- $\langle \mathbb{N}, S, 0 \rangle$, teorií následníka s nulou,
- $\langle \mathbb{N}, S, +, 0 \rangle$, tzv. Presburgerovou aritmetikou,
- $\langle \mathbb{R}, +, -, \cdot, 0, 1 \rangle$, teorií reálně uzavřených těles,
- $\langle \mathbb{C}, +, -, \cdot, 0, 1 \rangle$, teorií algebraicky uzavřených těles charakteristiky 0.

Důsledek *Pro uvedené struktury je* $\mathrm{Th}(\mathcal{A})$ *rozhodnutelná.*

Poznámka Uvidíme, že ale $\underline{\mathbb{N}} = \langle \mathbb{N}, S, +, \cdot, 0, \leq \rangle$ *rekurzivně axiomatizovat* nelze. *(Vyplývá to z první Gödelovy věty o neúplnosti).*

1.2 (draft) Aritmetika

[TODO]

1.2.1 (draft) Robinsonova a Peanova aritmetika

[TODO]

Robinsonova aritmetika

Jak efektivně a přitom co nejúplněji axiomatizovat $\underline{\mathbb{N}} = \langle \mathbb{N}, S, +, \cdot, 0, \leq \rangle$*?*

Jazyk aritmetiky je $L = \langle S, +, \cdot, 0, \leq \rangle$ s rovností.

Robinsonova aritmetika Q má axiomy (konečně mnoho)

$$\begin{array}{ll} S(x) \neq 0 & x \cdot 0 = 0 \\ S(x) = S(y) \rightarrow x = y & x \cdot S(y) = x \cdot y + x \\ x + 0 = x & x \neq 0 \rightarrow (\exists y)(x = S(y)) \\ x + S(y) = S(x + y) & x \leq y \leftrightarrow (\exists z)(z + x = y) \end{array}$$

Poznámka Q *je velmi slabá, např. nedokazuje komutativitu či asociativitu operací* $+$, $\cdot$ *ani tranzitivitu* $\leq$. *Nicméně postačuje například k důkazu existenčních tvrzení o numerálech, která jsou pravdivá v* $\underline{\mathbb{N}}$.

Např. pro $\varphi(x, y)$ *tvaru* $(\exists z)(x + z = y)$ *je*

$$Q \vdash \varphi(\underline{1}, \underline{2}), \quad \textit{kde } \underline{1} = S(0) \textit{ a } \underline{2} = S(S(0)).$$

Peanova aritmetika

Peanova aritmetika PA má axiomy

(a) Robinsonovy aritmetiky Q,

(b) schéma indukce, tj. pro každou formuli $\varphi(x, \overline{y})$ jazyka L axiom

$$(\varphi(0, \overline{y}) \wedge (\forall x)(\varphi(x, \overline{y}) \rightarrow \varphi(S(x), \overline{y}))) \rightarrow (\forall x)\varphi(x, \overline{y}).$$

Poznámka PA *je poměrně dobrou aproximací* $\mathrm{Th}(\underline{\mathbb{N}})$, *dokazuje všechny základní vlastnosti platné v* $\underline{\mathbb{N}}$ *(např. komutativitu* $+$*). Na druhou stranu existují sentence pravdivé v* $\underline{\mathbb{N}}$ *ale nezávislé v* PA.

Poznámka V jazyce 2. řádu lze axiomatizovat $\underline{\mathbb{N}}$ *(až na izomorfismus), vezmeme-li místo schéma indukce přímo axiom indukce (2. řádu)*

$$(\forall X)\ ((X(0) \wedge (\forall x)(X(x) \rightarrow X(S(x)))) \rightarrow (\forall x)\ X(x)).$$

1.2.2 (draft) Hilbertův desátý problém

[TODO]

Hilbertův 10. problém

- Nechť $p(x_1, \ldots, x_n)$ je polynom s celočíselnými koeficienty.

  Má *Diofantická rovnice* $p(x_1, \ldots, x_n) = 0$ celočíselné řešení?

- Hilbert (1900) *"Nalezněte algoritmus, který po konečně mnoha krocích určí, zda daná Diofantická rovnice s libovolným počtem proměnných a celočíselnými koeficienty má celočíselné řešení."*

Poznámka Ekvivalentně lze požadovat algoritmus rozhodující, zda existuje řešení v přirozených číslech.

Věta (DPRM, 1970) *Problém existence celočíselného řešení dané Diofantické rovnice s celočíselnými koeficienty je alg. nerozhodnutelný.*

Důsledek *Neexistuje algoritmus rozhodující pro dané polynomy $p(x_1, \ldots, x_n)$, $q(x_1, \ldots, x_n)$ s přirozenými koeficienty, zda*

$$\underline{\mathbb{N}} \models (\exists x_1) \ldots (\exists x_n)(p(x_1, \ldots, x_n) = q(x_1, \ldots, x_n)).$$

1.3 (draft) Nerozhodnutelnost predikátové logiky

[TODO]

Nerozhodutelnost predikátové logiky

Existuje algoritmus, rozhodující o dané sentenci, zda je logicky pravdivá?

- Víme, že Robinsonova aritmetika Q má konečně axiomů, má za model $\underline{\mathbb{N}}$ a stačí k důkazu existenčních tvrzení o numerálech, která platí v $\underline{\mathbb{N}}$.

- Přesněji, pro každou existenční formuli $\varphi(x_1, \ldots, x_n)$ jazyka aritmetiky

  $$Q \vdash \varphi(x_1/\underline{a_1}, \ldots, x_n/\underline{a_n}) \quad \Leftrightarrow \quad \underline{\mathbb{N}} \models \varphi[e(x_1/a_1, \ldots, x_n/a_n)]$$

  pro každé $a_1, \ldots, a_n \in \mathbb{N}$, kde $\underline{a_i}$ značí a_i-tý numerál.

- Speciálně, pro φ tvaru $(\exists x_1)\dots(\exists x_n)(p(x_1,\dots,x_n) = q(x_1,\dots,x_n))$, kde p, q jsou polynomy s přirozenými koeficienty (numerály), platí

$$\underline{\mathbb{N}} \models \varphi \quad \Leftrightarrow \quad Q \vdash \varphi \quad \Leftrightarrow \quad \vdash \psi \to \varphi \quad \Leftrightarrow \quad \models \psi \to \varphi,$$

  kde ψ je konjunkce (uzávěrů) všech axiomů Q.

- Tedy, pokud by existoval algoritmus rozhodující logickou pravdivost, existoval by i algoritmus rozhodující, zda $\underline{\mathbb{N}} \models \varphi$, což není možné.

1.4 (draft) Gödelovy věty

[TODO]

1.4.1 (draft) První věta o neúplnosti

[TODO]

Gödelova 1. věta o neúplnosti

Věta (Gödel) *Pro každou bezespornou rekurzivně axiomatizovanou extenzi T Robinsonovy aritmetiky existuje sentence pravdivá v $\underline{\mathbb{N}}$ a nedokazatelná v T.*

Poznámky

- *"Rekurzivně axiomatizovaná" znamená, že je* "efektivně zadaná"*.*
- *"Extenze R. aritmetiky" znamená, že je* "základní aritmetické síly"*.*
- *Je-li navíc $\underline{\mathbb{N}} \models T$, je teorie T nekompletní.*
- *V důkazu sestrojená sentence vyjadřuje* "nejsem dokazatelná v T"*.*
- *Důkaz je založen na dvou principech:*

  (*a*) *aritmetizaci syntaxe,*

  (*b*) *self-referenci.*

1.4.2 Aritmetizace dokazatelnosti

Aritmetizace - predikát dokazatelnosti

- Konečné objekty syntaxe (symboly jazyka, termy, formule, konečná tabla, tablo důkazy) lze vhodně zakódovat přirozenými čísly.

- Nechť $\ulcorner\varphi\urcorner$ značí kód formule φ a nechť $\underline{\varphi}$ značí numerál (term jazyka aritmetiky) reprezentující $\ulcorner\varphi\urcorner$.
- Je-li T rekurzivně axiomatizovaná, je relace $\mathrm{Prf}_T \subseteq \mathbb{N}^2$ rekurzivní.

$$\mathrm{Prf}_T(x, y) \quad \Leftrightarrow \quad \textit{(tablo) } y \textit{ je důkazem (sentence) } x \textit{ v } T.$$

- Je-li T navíc extenze Robinsonovy aritmetiky Q, dá se dokázat, že Prf_T je reprezentovatelná nějakou formulí $Prf_T(x, y)$ tak, že pro každé $x, y \in \mathbb{N}$

$$\begin{array}{lll} Q \vdash Prf_T(\underline{x}, \underline{y}), & \textit{je-li} & \mathrm{Prf}_T(x, y), \\ Q \vdash \neg Prf_T(\underline{x}, \underline{y}), & \textit{jinak.} & \end{array}$$

- $Prf_T(x, y)$ vyjadřuje *"y je důkaz x v T"*.
- $(\exists y)Prf_T(x, y)$ vyjadřuje *"x je dokazatelná v T"*.
- Je-li $T \vdash \varphi$, pak $\underline{\mathbb{N}} \models (\exists y)Prf_T(\underline{\varphi}, y)$ a navíc $T \vdash (\exists y)Prf_T(\underline{\varphi}, y)$.

1.4.3 Self-reference

Princip self-reference

- *Tato věta má 16 písmen.*

  Self-reference ve formálních systémech většinou není přímo k dispozici.

- *Následující věta má 24 písmen "Následující věta má 24 písmen".*

  Přímá reference obvykle je k dispozici, stačí, když umíme "mluvit" o posloupnostech symbolů. Uvedená věta ale není self-referenční.

- *Následující věta zapsaná jednou a ještě jednou v uvozovkách má 116 písmen "Následující věta zapsaná jednou a ještě jednou v uvozovkách má 116 písmen".*

  Pomocí přímé reference lze dosáhnout self-reference. Namísto *"má x písmen"* může být jiná vlastnost.

- ```
  main(){char *c="main(){char *c=%c%s%c; printf(c,34,
  c,34);}"; printf(c,34,c,34);}
  ```
  ```

Věta o pevném bodě

Věta *Nechť T je bezesporné rozšíření Robinsonovy aritmetiky. Pro každou formuli $\varphi(x)$ jazyka teorie T existuje sentence ψ taková, že $T \vdash \psi \leftrightarrow \varphi(\underline{\psi})$.*

Poznámka Sentence ψ je self-referenční, říká "splňuji podmínku φ".

Důkaz (idea) Uvažme *zdvojující* funkci d takovou, že pro každou formuli $\chi(x)$

$$d(\ulcorner\chi(x)\urcorner) = \ulcorner\chi(\underline{\chi(x)})\urcorner$$

- Platí, že d je reprezentovatelná v T. Předpokládejme *(pro jednoduchost)*, že nějakým termem, který si označme d, stejně jako funkci d.
- Pak pro každou formuli $\chi(x)$ jazyka teorie T platí

$$T \vdash d(\underline{\chi(x)}) = \underline{\chi(\underline{\chi(x)})} \tag{1.1}$$

- Za ψ vezměme sentenci $\varphi(d(\underline{\varphi(d(x))}))$. Stačí ověřit $T \vdash d(\underline{\varphi(d(x))}) = \underline{\psi}$.
- To plyne z (1.1) pro $\chi(x)$ tvaru $\varphi(d(x))$, neboť v tom případě

$$T \vdash d(\underline{\varphi(d(x))}) = \underline{\varphi(d(\underline{\varphi(d(x))}))} \quad \square$$

1.4.4 Nedefinovatelnost pravdy

Nedefinovatelnost pravdy

Řekneme, že formule $\tau(x)$ *definuje pravdu* v aritmetické teorii T, pokud pro každou sentenci φ platí $T \vdash \varphi \leftrightarrow \tau(\underline{\varphi})$.

Věta *V žádném bezesporném rozšíření Robinsonovy aritmetiky neexistuje definice pravdy.*

Důkaz Dle věty o pevném bodě pro $\neg\tau(x)$ existuje sentence φ taková, že

$$T \vdash \varphi \leftrightarrow \neg\tau(\underline{\varphi}).$$

Kdyby formule $\tau(x)$ definovala pravdu v T, bylo by

$$T \vdash \varphi \leftrightarrow \neg\varphi,$$

což v bezesporné teorii není možné. $\square$

Poznámka Důkaz je založen na paradoxu lháře, sentence φ by vyjadřovala "nejsem pravdivá v T".

1.4.5 1. věta o neúplnosti

Důkaz 1. věty o neúplnosti

Věta (Gödel) *Pro každou bezespornou rekurzivně axiomatizovanou extenzi T Robinsonovy aritmetiky existuje sentence pravdivá v $\underline{\mathbb{N}}$ a nedokazatelná v T.*

Důkaz Nechť $\varphi(x)$ je $\neg(\exists y)Prf_T(x, y)$, vyjadřuje *"$x$ není dokazatelná v T"*.

- Dle věty o pevném bodě pro $\varphi(x)$ existuje sentence ψ_T taková, že

$$T \vdash \psi_T \leftrightarrow \neg(\exists y)Prf_T(\underline{\psi_T}, y). \tag{1.2}$$

  ψ_T říká *"nejsem dokazatelná v T"*. Přesněji, ψ_T je ekvivalentní sentenci vyjadřující, že ψ_T není dokazatelná v T. (Ekvivalence platí v $\underline{\mathbb{N}}$ i v T).

- Nejprve ukážeme, že ψ_T *není dokazatelná v T*. Kdyby $T \vdash \psi_T$, tj. ψ_T je lživá v $\underline{\mathbb{N}}$, pak $\underline{\mathbb{N}} \models (\exists y)Prf_T(\underline{\psi_T}, y)$ a navíc $T \vdash (\exists y)Prf_T(\underline{\psi_T}, y)$. Tedy z (1.2) plyne $T \vdash \neg\psi_T$, což ale není možné, neboť T je bezesporná.

- Zbývá dokázat, že ψ_T je pravdivá v $\underline{\mathbb{N}}$. Kdyby ne, tj. $\underline{\mathbb{N}} \models \neg\psi_T$, pak $\underline{\mathbb{N}} \models (\exists y)Prf_T(\underline{\psi_T}, y)$. Tedy $T \vdash \psi_T$, což jsme již dokázali, že neplatí. □

1.4.6 (draft) Důsledky první věty

[TODO]

Důsledky a zesílení 1. věty

Důsledek *Je-li navíc $\underline{\mathbb{N}} \models T$, je teorie T nekompletní.*

Důkaz Kdyby byla T kompletní, pak $T \vdash \neg\psi_T$ a tedy $\underline{\mathbb{N}} \models \neg\psi_T$, což je ve sporu s $\underline{\mathbb{N}} \models \psi_T$. □

Důsledek $\mathrm{Th}(\underline{\mathbb{N}})$ *není rekurzivně axiomatizovatelná.*

Důkaz $\mathrm{Th}(\underline{\mathbb{N}})$ je bezesporná extenze Robinsonovy aritmetiky a má model $\underline{\mathbb{N}}$. Kdyby byla rekurzivně axiomatizovatelná, dle předchozího důsledku by byla nekompletní, ale $\mathrm{Th}(\underline{\mathbb{N}})$ je kompletní. □

Gödelovu 1. větu o neúplnosti lze následovně zesílit.

Věta (Rosser) *Pro každou bezespornou rekurzivně axiomatizovanou extenzi T Robinsonovy aritmetiky existuje nezávislá sentence. Tedy T je nekompletní.*
Poznámka Tedy předpoklad, že $\underline{\mathbb{N}} \models T$, je v prvním důsledku nadbytečný.

1.4.7 (draft) Druhá věta o neúplnosti

[TODO]

Gödelova 2. věta o neúplnosti

Označme Con_T sentenci $\neg(\exists y)Prf_T(\underline{0=1}, y)$. Platí $\underline{\mathbb{N}} \models Con_T \Leftrightarrow T \nvdash 0 = \underline{1}$. Tedy Con_T vyjadřuje, že *"T je bezesporná"*.

Věta (Gödel) *Pro každou bezespornou rekurzivně axiomatizovanou extenzi T Peanovy aritmetiky platí, že Con_T není dokazatelná v T.*

Důkaz (náznak) Nechť ψ_T je Gödelova sentence *"nejsem dokazatelná v T"*.

- V první části důkazu 1. věty o neúplnosti jsme ukázali, že

$$\text{"Je-li } T \text{ bezesporná, pak } \psi_T \text{ není dokazatelná v } T.\text{"} \tag{1.3}$$

  Jinak vyjádřeno, platí $Con_T \to \psi_T$.

- Je-li T extenze Peanovy aritmetiky, důkaz tvrzení (1.3) lze formalizovat v rámci T. Tedy $T \vdash Con_T \to \psi_T$.
- Jelikož T je bezesporná dle předpokladu věty, podle (1.3) je $T \nvdash \psi_T$.
- Z předchozích dvou bodů vyplývá, že $T \nvdash Con_T$. $\square$

Poznámka Taková teorie T tedy neumí dokázat vlastní bezespornost.

1.4.8 (draft) Důsledky druhé věty

[TODO]

Důsledky 2. věty

Důsledek *Existuje model $\mathcal{A}$ Peanovy aritmetiky t.ž. $\mathcal{A} \models (\exists y)Prf_{PA}(\underline{0=1}, y)$.*

Poznámka $\mathcal{A}$ musí být nestandardní model PA, svědkem musí být nestandardní prvek (jiný než hodnoty numerálů).

Důsledek *Existuje bezesporná rekurzivně axiomatizovaná extenze T Peanovy aritmetiky taková, že $T \vdash \neg Con_T$.*

Důkaz Nechť $T = PA \cup \{\neg Con_{PA}\}$. Pak T je bezesporná, neboť $PA \nvdash Con_{PA}$. Navíc $T \vdash \neg Con_{PA}$, tj. T dokazuje spornost $PA \subseteq T$, tedy i $T \vdash \neg Con_T$. $\square$

Poznámka $\underline{\mathbb{N}}$ nemůže být modelem teorie T.

Důsledek *Je-li teorie množin ZFC bezesporná, není Con_{ZFC} dokazatelná v ZFC.*