Formální definice logického uvažování: Logický systém

Logický systém matematicky přesně definuje

* co je logických výrok: ***syntaxe***,
* jaký je jeho význam: ***sémantika***,
* co je logická argumentace: ***dokazovací systém***.

* ***Korektní***: dokazatelné platí
* ***Sémanticky úplný***: vše platné je dokazatelné

Syntaxe a sémantika PL

* ***Signatura*** – dvojice $\langle \mathcal{F}, \mathcal{P} \rangle$ mn. predikátových a funkčních symbolů s aritami
* ***Term*** – $t ::= x \mid f(t_1, \ldots, t_n)$ pro n-ární f
* ***Formule*** – $\varphi ::= p(t_1, \ldots, t_n) \mid \neg(\varphi) \mid \varphi \wedge \varphi \mid \exists x(\varphi)$ pro n-ární p
  Věta = uzavřená formule (= nemá volné proměnné)

* ***Interpretace/realizace*** I jazyka L – funkce α_I přiřadí prvky z domény D_I proměnným, relace pred. symbolům, funkce funkčním symbolům. Mluvíme o platnosti formule v interpretaci, $\boldsymbol{I} \models \varphi$.

* $\alpha_I(f(t_1, \ldots, t_n)) = \alpha_I(f)(\alpha_I(t_1), \ldots, \alpha_I(t_n))$ pro n-ární f
* $I \models p(t_1, \ldots, t_n) \Leftrightarrow (\alpha_I(t_1), \ldots, \alpha_I(t_n)) \in \alpha_I(p)$ pro n-ární p
* $I \models \varphi_1 \wedge \varphi_2 \Leftrightarrow I \models \varphi_1$ a $I \models \varphi_2$
* $I \models \neg\varphi \Leftrightarrow I \not\models \varphi$
* $I \models \exists x \varphi \Leftrightarrow I[x/v] \models \varphi$ pro nějaké $v \in D_I$, kde $I[x/v]$ je jako I, jen $\alpha_{I[x/v]}(x) = v$.
  (předp. že x je volná v φ)

Důkazový systém predikátové logiky

* ***Schémata výrokových axiomů***

$$\begin{array}{ll} \text{(A1)} & \varphi \to (\psi \to \varphi) \\ \text{(A2)} & (\varphi \to (\psi \to \eta)) \to ((\varphi \to \psi) \to (\varphi \to \eta)) \\ \text{(A3)} & (\neg\psi \to \neg\varphi) \to ((\neg\psi \to \varphi) \to \psi) \end{array}$$

kde φ, ψ, η jsou formule PL.

* ***Schéma axiomů kvantifikátoru***:
Není-li x volné ve φ, pak

$$(\forall x(\varphi \to \psi)) \to (\varphi \to (\forall x \psi))$$

* ***Schéma axiomů substituce***:

$$(\forall x\, \varphi) \to \varphi[x/t]$$

kde t je term substituovatelný za x do φ.

* ***Axiomy rovnosti***:
Pro libovolné funkční a predikátové symboly f/n a p/n a proměnné $x, x_1, \ldots, x_n, y_1, \ldots, y_n$

$$\begin{array}{c} x = x \\ x_1 = y_1 \to (\ldots x_n = y_n \to f(x_1, \ldots, x_n) = f(y_1, \ldots, y_n) \ldots) \\ x_1 = y_1 \to (\ldots x_n = y_n \to p(x_1, \ldots, x_n) \to p(y_1, \ldots, y_n) \ldots) \end{array}$$

* ***Pravidlo Modus ponens***:

Z předpokladů φ a $(\varphi \to \psi)$ odvodíme závěr ψ.

* ***Pravidlo zobecnění (generalizace)***:

Z předpokladu φ odvodíme závěr $(\forall x \varphi)$.

Důkaz formule φ (z množiny předpokladů P),
kde T je množina formulí,
je sekvencí formulí $\varphi_1, \ldots, \varphi_n$, kde $\varphi_n = \varphi$ a pro každé $i : 1 \leq i \leq n$,
formule φ_i je axiomem (nebo prvkem P)
nebo vznikla z $\varphi_1, \ldots \varphi_{i-1}$ aplikací odvozovacích pravidel. Píšeme $\vdash \boldsymbol{\varphi}$ ($\boldsymbol{P} \vdash \boldsymbol{\varphi}$).

Teorie

- ***Teorie*** s jazykem L je množina vět z L (spec. axiomů, definičních bodů,...).
- ***Model*** teorie: interpretace $\mathcal{M}$, kde $\mathcal{M} \models \varphi$ pro všechny spec. axiomy $\varphi \in T$.
- ***Logický důsledek*** teorie. $T \models \varphi$: φ je platná ve všech modelech T.
- ***Dokazatelnost*** v teorii. $T \vdash \varphi$: Existuje důkaz φ z předpokladů T.

- ***Bezespornost***: není možné $T \vdash \varphi$ a $T \vdash \neg\varphi$.
- ***Efektivnost***: množina axiomů je rozhodnutelná.
- ***Syntaktická úplnost***: pro větu, buď $T \vdash \varphi$ nebo $T \vdash \neg\varphi$.

- PL je ***korektní***: Pokud $T \vdash \varphi$, potom $T \models \varphi$.
- PL je ***sémanticky úplná***: Pokud $T \models \varphi$, potom $T \vdash \varphi$. (Gödel)
- PL je ***efektivní***: Množina důkazů (v efektivní teorii) je rozhodnutelná.

Rozhodnutelnost, úplnost

Teorie je (částečně) rozhodnutelná, pokud $\{\varphi \mid T \models \varphi\}$ je (částečně) rozhodnutelná.

Pro efektivní, bezespornou a úplnou teorii je $\{\varphi \mid T \vdash \varphi\} = \{\varphi \mid T \models \varphi\}$ rozhodnutelná.

Generuj řetězce v lex. pořadí, dokud nenajdeš důkaz φ nebo $\neg\varphi$.

* z korektnosti: důkaz znamená platnost
* z efektivnosti: důkaz je zkontrolovatelný
* ze syntaktické úplnosti: důkaz jedné varianty se časem najde (terminace)

Rozhodnutelnost neimplikuje úplnost! Ale

Rozhodnutelná bezesporná teorie má úplné, efektivní a bezesporné rozšíření.

Rozšíření teorie T je teorie $T' \supseteq T$.

Dokazování o „zajímavých“ matematických strukturách?

- Mat. struktura je definována úplnou (a bezespornou a efektivní) teorií $\Rightarrow$ všechno se dá dokázat nebo vyvrátit, a existuje mechanický matematik.
- Je to možné pro zajímavé matematické struktury?
  Např. aritmetika přir. čísel, množiny, relace, algebry, grafy, . . . ?
- Dokázali bychom v principu automaticky dokazovat teorémy, včetně řady nevyřešených / neřešitelných problémů, jako
  - *Je každé sudé číslo je součtem dvou prvočísel? (Goldbachova doměnka)*
  - *Dají se reálná čísla dobře uspořádat?*

Pro připomenutí: Peanova aritmetika T_{PA}

Počítání, $+$ a $*$ v $\mathbb{N}$.

1. $\forall x \neg(S(x) = 0)$ (nula je první)
2. $\forall xy(S(x) = S(y) \to x = y)$ (každý má jiného následníka)
3. pro formule φ jazyka T_{PA} s jednou volnou proměnou:

$$\left[\varphi(0) \wedge (\forall x(\varphi(x) \to \varphi(S(x))))\right] \to \forall x\,(\varphi(x)) \qquad \text{(ax. indukce)}$$

4. $\forall x(x + 0 = x)$ (0 je neutrální k $+$)
5. $\forall xy(x + S(y) = S(x + y))$ (def sčítání)
6. $\forall x(x \cdot 0 = 0)$ (0 je nulová k $\cdot$)
7. $\forall xy(x \cdot S(y) = x \cdot y + x)$ (def násobení)

$$0, \overset{1}{S}(0), S(\overset{2}{S}(0)), S(S(\overset{3}{S}(0))), S(S(S(\overset{4}{S}(0)))), S(S(S(S(\overset{5}{S}(0))))), \ldots$$

$$T_{PA} \models \overset{1}{S}(0) + \overset{1}{S}(0) = S(\overset{2}{S}(0)) \quad \text{a} \quad T_{PA} \vdash \overset{1}{S}(0) + \overset{1}{S}(0) = S(\overset{2}{S}(0))$$

Gödelovy věty o neúplnosti

První Gödelova věta o neúplnosti:
Žádná efektivní bezesporná teorie PL zahrnující Peanovu aritm. nemůže být úplná.

* V T_{PA} nemůžeme dokázat všechny platné teorémy přirozených číslech. T_{PA} nedefinuje přirozená čísla úplně přesně.
* Nejde to opravit, v PL ani a v žádném jiném efektivním bezesporném systému.
* Logické odvozování má své limity, stejně jako počítání.
* Aritmetika přirozených čísel je nerozhodnutelná.

Gödelovy věty o neúplnosti

Druhá Gödelova věta o neúplnosti:
V žádném bezesporném a efektivním logickém systému zahrnujícím Peanovu aritmetiku není možné dokázat jeho vlastní bezespornost.

Část I

Kostra důkazu první Gödelovy věty

Sebereference

* Athéňané nikdy nelžou, Kréťané vždy lžou. Kdo může říct „Právě lžu.“?
* „Tato věta není pravdivá.“ Je to pravdivá věta?
* „Tato věta není dokazatelná.“ Je to pravdivá věta? Je dokazatelná?
* M je množina množin, které nejsou prvkem sama sebe. Je M prvkem sama sebe?
* Stroj T zastaví na kódu stroje T' právě tehdy, když T' nezastaví na vlastním kódu. Zastaví T na vlastním kódu?

Princip důkazu na příkladu

* Stroj tisknoucí řetězce nad abecedou $\{\neg, N, P, (,), \}^*$.
* Řetězce formy $P(X)$, $\neg P(X)$, $PN(X)$ a $\neg PN(X)$ jsou výroky (kde X je řetězec).
* Výroky mají význam:
  - $P(X)$: X je tisknutelný.
  - $PN(X)$: norma X je tisknutelná. Norma řetězce X je řetězec $X(X)$.
  - $\neg V$: není pravda, že V.
* Systém je korektní. Tiskne pouze pravdivé výroky.

Může systém být úplný? Být schopen vytisknout všechny pravdivé výroky?

* Výrok, který implikuje netisknutelnost sebe sama?

$$\neg PN(\neg PN) \begin{cases} \text{Nepravdivý, tedy tisknutelný. Spor s korektností.} \\ \text{Pravdivý, tedy netisknutelný. Spor s úplností.} \end{cases}$$

Základní pozorování: Jména čísel a čísla slov

* Formální zápisy jako formule, důkazy, popisy Turingových strojů ... jsou slova nad konečnou abecedou.
* Slova se dají uspořádat, třeba abecedně, a číslovat.
* Např. číslo slova je hodnota jeho ASCI zápisu interpretovaného jako binární číslo.
* Můžeme mluvit o čísle slova a číslovce (slově/jméně čísla).

Sebereference, abstraktní systém

Abstraktní formální systém

* $\mathcal{E}$ je množina ***výrazů***, slov nad nějakou konečnou abecedou. Expressions
* $\mathcal{S} \subseteq \mathcal{E}$ je množina ***vět***. Sentences
* $\mathcal{T} \subseteq \mathcal{S}$ je množina ***pravdivých vět***. True sent.
* $\mathcal{P} \subseteq \mathcal{S}$ je množina ***dokazatelných vět***. Proovable
* $\mathcal{R} \subseteq \mathcal{S}$ je množina ***vyvratitelných vět***. Refutable
* $\mathcal{H} \subseteq \mathcal{E}$ je množina ***predikátů***, kde pro každé $H \in \mathcal{H}$ a $n \in \mathbb{N}$, $H(n)$ je věta.
* Korektnost: $\mathcal{P} \subseteq \mathcal{T}$, $\mathcal{R} \subseteq \mathcal{E} \setminus \mathcal{T}$.
* Syntaktická úplnost: $\mathcal{S} \subseteq \mathcal{P} \cup \mathcal{R}$.

Sebereference, notace

* Očíslujeme výrazy: Nechť každý výraz e má ***Gödelovo číslo*** $G(e)$.
* E_n značí výraz s G. číslem n.
* Výraz $E_n(n)$ nazýváme ***diagonalizací*** n.
* Predikát H ***vyjadřuje*** množinu $A = \{n \in \mathbb{N} \mid H(n) \in \mathcal{T}\}$.
* $\tilde{A}$ značíme komplement $\mathbb{N} \setminus A$ množiny A.
* Pro $A \subseteq \mathbb{N}$, $A^* = \{n \in \mathbb{N} \mid G(E_n(n)) \in A\}$.

Tarski: V systému se sebereferencí nevyjádříme pravdivost

Dostatečně expresivní systém nemůže vyjádřit pravdivost vlastních vět, t.j. množinu
$$T = \{G(e) \mid e \in \mathcal{T}\}.$$
Stačí, když

G1 A^* je vyjádřitelná pro každou vyjádřitelnou A, a

G2 $\tilde{A}$ je vyjádřitelná pro každou vyjádřitelnou A.

Důkaz:

- Nechť je T vyjádřitelná.
- Z G2 je $\tilde{T}$ vyjádřitelná (čísla neodpovídající pravdivým větám).
- Z G1 je $\tilde{T}^*$ vyjádřitelná. (čísla n predikatů takových, že $E_n(n)$ není pravdivá věta)
- Nechť Z vyjadřuje $\tilde{T}^*$ a nechť $G(Z) = z$ (tj. $Z = E_z$).
  $Z(n)$ vyjadřuje, že $E_n(n)$ není pravdivá věta.
- $Z(z)$ je věta „Jsem nepravdivá.“ ($Z(z)$ znamená, že $E_z(z)$ není pravdivá věta, a $E_z = Z$)
- $Z(z) \in \mathcal{T} \overset{\text{def. } Z}{\Leftrightarrow} z \in \tilde{T}^* \overset{\text{def. } ^*}{\Leftrightarrow} G(Z(z)) \in \tilde{T} \overset{\text{def. } \tilde{}}{\Leftrightarrow} G(Z(z)) \notin T \overset{\text{def. } T}{\Leftrightarrow} Z(z) \notin \mathcal{T}$ Spor.

Varianta 2: Pokud platí G1, $\tilde{T}$ není vyjádřitelná.

Sebereference a neúplnost

Nechť $P = \{G(e) \mid e \in \mathcal{P}\}$ jsou čísla dokazatelných vět.

Pokud je $\tilde{P}^*$ vyjádřitelná a systém je korektní, potom není úplný.

Důkaz:

* Nechť H vyjadřuje $\tilde{P}^*$ a $h = G(H)$.
  $H(n)$ vyjadřuje, že $E_n(n)$ není dokazatelná věta.
* $H(h)$ říká „Nejsem dokazatelná.“ ($E_h(h)$ není dokazatelná věta a $E_h = H$)
* $H(h) \notin \mathcal{T} \overset{\text{def. } H(h)}{\Rightarrow} H(h) \in \mathcal{P}$. Spor s korektností. Musí platit opak.
  $H(h) \in \mathcal{T} \overset{\text{def. } H(h)}{\Rightarrow} H(h) \notin \mathcal{P}$. $H(h)$ je pravdivá nedokazatelná formule.

Dostatečně expresivní systém nemůže být úplný. Stačí, když

G1 A^* je vyjádřitelná pro každou vyjádřitelnou A,

G2 $\tilde{A}$ je vyjádřitelná pro každou vyjádřitelnou A,

G3 P je vyjádřitelná.

Kostra Gödelova důkazu: Číslování formulí

Gödel dokázal, že systém T_{PA} je dostatečně expresivní, aby nemohl být úplný, protože splňuje

- G1 A^* je vyjádřitelná pro každou vyjádřitelnou A.
- G2 $\tilde{A}$ je vyjádřitelná pro každou vyjádřitelnou A.
- G3 P (čísla dokazatelných vět) je vyjádřitelná.

G2 je super snadná, v PL máme negaci. G1 je poměrně snadná. G3 je velmi komplikovaná.

Číslování formulí je třeba zvolit tak, aby se G1 a G3 dokazovaly dobře (Gödel použil jiné).

- Každý používaný symbol a má číslo $G(a)$:

$'$	0	(	)	f	,	v	$\neg$	$\rightarrow$	$\forall$	$=$	$\leq$	$\sharp$
0	1	2	3	4	5	6	7	8	9	10	11	12

- Číslovky $0, 0', 0'', 0''', \ldots$,
- $+$, $*$ a exponent: f', f'', f''',
- jména proměnných $v, v', v'', v''', \ldots$,
- $\sharp$ je oddělovač formulí v důkazech.

Slovo $w = a_0 \cdots a_n \in \mathbb{N}^*$, je zápisem ***Gödelova čísla*** ve třináctkové soustavě:

$$G(w) = (a_0 * 13^n) + (a_1 * 13^{n-1}) + \cdots + (a_n * 13^0)$$

Kostra Gödelova důkazu: G1

Pro vyjádřitelnou $A \subseteq \mathbb{N}$ je $A^* = \{n \in \mathbb{N} \mid G(E_n(n)) \in A\}$ také vyjádřitelná:

* Konkatenace je vyjádřitelná. $G(u.v) = G(u) * 13^{|v|} + G(v)$. Značíme $G(u) \circ G(v)$.
  Musíme jen vyjádřit $|v|$ jako funkci $G(v)$ ...
* Kód číslovky $\bar{n}$ s hodnotou n? $\bar{n}$ je $0\overbrace{'''\ldots'''}^{n}$. Protože $G(0) = 1$ a $G(') = 0$, máme $G(\bar{n}) = 13^n$.
* $G(E_e(n))$ je vyjádřitelné na základě e a n:
  Pokud E_e má volnou proměnnou v, $E_e(n)$ je ekvivalentní $\forall v(v = \bar{n} \to E_e)$.
* $G(E_e(n)) = k \circ 13^n \circ 8 \circ e \circ 3$

$$\overbrace{\forall v(v =}^{k}\ \overbrace{\bar{n}}^{13^n}\ \overbrace{\to}^{8}\ \overbrace{E_e}^{e}\ \overbrace{)}^{3}$$

* Pro predikát F vyjadřující A, pak A^* je vyjádřena predikátem F^* definovaným takto
  (víme, že $F^*(n) \Leftrightarrow G(E_n(n)) \in A \Leftrightarrow \exists v(v = G(E_n(n)) \wedge F(v))$):

$$F^*(n) \;=\; \exists v(v = k \circ 13^n \circ 8 \circ n \circ 3 \wedge F(v))$$

Zbytek Gödelova důkazu

Zbývá „jen“ formulemi aritmetiky

- vyjádřit $|w|$ jako funkci $G(w)$,
- vyjádřit x^y v T_{PA} (pomocí násobení a sčítání),
- vyjádřit P.

Technicky velmi komplikované, zvlášť vyjádřit P.
Je třeba definovat predikát D takový,
že $D(m, n)$ právě když m je G. číslem důkazu formule s G. číslem n.
P je potom vyjádřena predikátem $\exists m\, D(m, n)$.

Část II

Neúplnost a nerozhodnutelnost

Neúplnost a nerozhodnutelnost

Gödel:
Bezesporná teorie zahrnující Peanovu aritmetiku nemůže být syntakticky úplná.
(Existují pravdivé formálně nedokazatelné věty o artimetice přirozených čísel.)

Turing:
Problém zastavení je nerozhodnutelný.
(Existují algoritmicky neřešitelné problémy.)

Důkaz a výpočet

* ***Důkaz*** */* ***výpočet*** jsou velmi podobné věci:
  - Je to sekvence ***formulí*** / ***konfigurací***,
  - které jsou buď ***axiomy*** / ***iniciální konfigurace***
  - nebo jsou odvozeny z předchozích pomocí jednoduchých mechanických ***odvozovacích pravidel*** / ***pravidel daných přechodovou funkcí***.

Nerozhodnutelnost HP jako instance abstraktní Tarského věty

Varianta 2 T.v.: Pokud platí G1, potom $\tilde{T}$ není vyjádřitelná.

(G1: Pro vyjádřitelnou $A \subseteq \mathbb{N}$ je $A^* = \{n \in \mathbb{N} \mid G(E_n(n)) \in A\}$ také vyjádřitelná)

Abstraktní formální systém, instanciovaný pro Turingovy stroje

* $\mathcal{E}$ je množina výrazů – řetězců.
* $\mathcal{S} \subseteq \mathcal{E}$ je množina vět – formy $M(n)$ kde M je zápis TS.
* $\mathcal{T} \subseteq \mathcal{S}$ je množina pravdivých vět – vět $M(n)$ kde M zastaví na n.
* $\mathcal{H} \subseteq \mathcal{E}$ je množina predikátů – kódů TS. Pro $M \in \mathcal{H}$ a $n \in \mathbb{N}$ je $M(n)$ věta.

G1: pro vyjádřitelnou A je také A^* vyjádřitelná:

* Nechť stroj M vyjadřuje A (zastaví právě pro elementy A).
* Potom A^* je vyjádřena strojem M^*, který pro vstup n simuluje M na $G(M_n(n))$. (konstrukce M_n na základě n je možná, viz kódování TS).

Rozhodnutelnost problému zastavení strojem K by ale implikovala vyjádřitelnost $\tilde{T}$. Spor. (simuluj K, ale cykli, pokud K přijímá)

Podobnost Gödelova a Turingova důkazu

Gödel: Nemůžeme dokázat nebo vyvrátit každou formuli.
Sporem. Formule $\psi(x) : \neg\exists y\ D(y, x)$ říká, že formule s G. číslem x nemá důkaz.

* $\psi(G(\psi))$ je dokazatelná. Pak, podle definice ψ, neexistuje důkaz $\psi(G(\psi))$.
* $\neg\psi(G(\psi))$ je dokazatelná. Pak, podle definice ψ, existuje důkaz $\psi(G(\psi))$.

Turing: Zastavení je nerozh. (neexistuje TS, který zastaví přijme nebo zastaví a zamítne).
Sporem. TS M, který zastaví $\Leftrightarrow$ jeho vstup je kódem TS, který nezastaví na vlastním kódu.

* $M(\langle M\rangle)$ zastaví. Pak, podle definice M, M nezastaví s vlastním kódem na vstupu.
* $M(\langle M\rangle)$ nezastaví. Pak, podle definice M, M zastaví s vlastním kódem na vstupu.

Redukce problému zastavení na problém platnosti aritm. formule

Mějme DTS M který, pro jednoduchost, nikdy neskončí abnormálně.

Sestrojíme aritm. formuli φ_w^M platnou právě tehdy, když M zastaví na slově $w = a_1 \cdots a_n$.

Formule φ_w^M definuje vztah mezi stavem $S(k)$ v kroce k výpočtu M, pozicí hlavy $H(k)$ v kroce k, a znakem $Z(k, p)$ v kroce k na poli pásky p:

Konkrétněji, φ_w^M specifikuje, 1) co platí na začátku běhu, 2) jak následující konfigurace závisí na předchozí, a 3) že stroj někdy zastaví:

$$\varphi_w^M \equiv \varphi_{init} \wedge \varphi_\Delta \wedge \varphi_{stop}$$

Na začátku jsme ve stavu 0, hlava je na začátku, a páska je formy $\Delta w \Delta\Delta \ldots$.

$$\varphi_{init} \equiv S(0) = q_0 \wedge H(0) = 1 \wedge Z(0,1) = \Delta \wedge (\bigwedge_{p=2}^{n+1} Z(0,p) = a_p) \wedge (\forall p > n+1 : Z(0,p) = \Delta)$$

Stroj zastaví, když se někdy dostane do koncového stavu.

$$\varphi_{stop} \equiv \exists k : S(k) = q_f$$

Pro každou k-tou konfiguraci výpočtu, s jakoukoliv pozicí hlavy p, $k+1$-tá konfigurace bude výsledkem kroku výpočtu, který závisí na momentálním stavu q a symbolu pod hlavou a.

$$\varphi_\Delta \equiv \forall k \forall p \bigwedge_{q \in Q, a \in \Gamma} \varphi_{(q,a)}, \quad \text{kde, pokud } \delta(q,a) = \{(q', X)\}, X \in \{L, R\} \cup \Sigma, \text{ potom}$$

$$\varphi_{(q,a)} \equiv (S(k) = q \wedge H(k) = p \wedge Z(k,p) = a) \rightarrow (S(k+1) = q') \wedge H(k+1) = p' \wedge Z(k+1,p) = a' \wedge \forall \bar{p} \neq p : Z(k+1,\bar{p}) = Z(k,\bar{p}))$$

$$\text{kde } p' = \begin{cases} p & \text{pokud } X \in \Sigma \\ p+1 & \text{pokud } X = R \\ p-1 & \text{pokud } X = L \end{cases}, \qquad a' = \begin{cases} X & \text{pokud } X \in \Sigma \\ a & \text{pokud } X \in \{L, R\} \end{cases}.$$

Důkaz (skoro) první Gödely věty redukcí z nezorhodnutelnosti HP

φ_w^M je platná právě tehdy, když T zastaví na w.

Tedy, platnost aritmetických formulí nemůže být rozhodnutelná,
protože potom by byl rozhodnutelný problém zastavení.

!!Nepoužili jsme T_{PA}, ale podobnou logiku.
Použili jsme Presburgerovu aritmetiku (T_{PA} bez násobení) obohacenou o neinterpretované funkční symboly (S, H, Z), pro která platí axiomy rovnosti. Označme ji T_{Presb+}.
Neinterpretované funkce umí kódovat násobení: $\forall xy\, f(0, x) = 0 \wedge f(y + 1, x) = x + f(y, x)$. Bez (S, H, Z), čistě s T_{PA} (jen pomocí $+$ a $*$), by to nebylo na slajd ...

T_{Presb+} nemůže být úplná, protože pak by platnost aritm. formulí byla rozhodnutelná.

Stejně ani žádné rozšíření T_{Presb+} (efektivní a bezesporné), ani jakýkoliv jiný efektivní a korektní systém charakterizující sčítání přirozených čísel a neinterpretované funkce přesněji, nemůže být úplný.

O čem přemýšlejí vrány na elektrickém vedení

V žádném jednom efektivním rozumném systému nemůžeme formálně dokázat všechno, co je pravda (např. o přirozených číslech).
Můžeme ale dokazovací systémy dál vyvíjet,
například objevovat nové axiomy, které umožní dokázat více.
Můžeme tak časem dokázat cokoliv, co je pravda?
Dvě možnosti:

1. Proces vymýšlení nových axiomů a systémů je také výpočtem stroje s Turingovskou silou.
   Pak je to jen komplikovaný TS generující teorémy.
   Aplikují se tedy věty o neúplnosti a nerozhodnutelnosti:
   Nemůžeme dokázat každou platnou formuli. Existují „nedokazatelné pravdy“.
2. Pokud můžeme každou formuli někdy nějak logicky zdůvodnit, dokázat, pak je lidské přemýšlení procesem s větší než Turingovskou silou, nedá se formalizovat jako efektivní a korektní systém.

Poznámky

* ***Úplnost teorie implikuje rozhodnutelnost*** (generátorem teorémů a důkazů).
  Ne naopak. Teorie může být rozhodnutelné, tj., existuje algoritmus rozhodující platnost v teorii, a stále neúplná.
* ***Čistá prvořádová logika s rovností*** (axiomy rovnosti: reflexivita, funkční a predikátová kongruence) ***je neúplná*** (např. jednoprvkový vs. nekonečný model a formule $\forall x \forall y (x = y)$, je možné ji zúplnit přidáním axiomu specifikujícího velikost domény).
  Je ale rozhodnutelná (Leopold Löwenheim, 1915).
* Úplnost a „přesnost definice“ není přesně to stejné. Peanova aritmetika je neúplná, ale Presburgerovat aritmetika (Peanova aritmetika bez násobení) je úplná. Protože T_{PA} je neúplná, má více modelů, a protože presburgerova aritmetika je podmnožinou speciálních axiomů T_{PA}, musí mít také více modelů. Presburgerova aritmetika je ale uplná, protože ***rozdíl mezi různými modely se v ní nedá vyjádřit***.
* Úplná teorie je rozhodnutelná generátorem teorémů/důkazů, ale většinou existuje i mnohem efektivnější algoritmus. Například pro Presburgerovu aritmetiku.

Formální versus neformální dokazování/přemýšlení

Věta

"Toto je nedokazatelná věta."

musí být pravdivá, a tedy nedokazatelná, protože jinak by byla dokazatelná, a to by byl spor s korektností dokazovacího systému.

* Přirozený jazyk je také systém se syntaxí a sémantikou a pravidly odvozování.
* Právě jsme v něm formulovali a dokázali větu „Toto je nedokazatelná věta.“,
* která je nedokazatelná ...

Část III

Příklad rozhodovací procedury pro prvořádovou teorii

Eliminace kvantifikátorů

Příklad: Je formule důskedek teorie racionálních čísel $T_{\mathbb{Q}}$ se signaturou $\{0, 1, \ldots, +, \leq\}$?

$$\exists y \forall x (x \neq 5 \vee y \neq 3x)$$
$$\downarrow$$
$$\exists y \neg \exists x (x = 5 \wedge y = 3x)$$
$$\downarrow$$
$$\exists y (\neg y = 15)$$
$$\downarrow$$
$$\top$$

Eliminace kvantifikátorů obecně

Eliminace kvantifikátoru (QE) transformuje $(\exists x \varphi)$ na T-ekvivalentní ψ bez volného výskytu x. (pokud φ má množinu volných proměnných V, pak ψ má množinu volných proměnných $V \setminus \{x\}$)

Platnost věty φ pomocí QE

Eliminuj všechny kvantifikátory induktivně ke struktuře formule. Procedura $elim(\varphi)$:

- Pokud φ je bez kvantifikátorů, vrať φ, jinak
- pokud $\varphi = \exists x \psi$ kde ψ je bez kvantifikátorů, vrať $QE(\varphi)$, jinak
- pokud $\varphi = \exists x \psi$, vrať $elim(\exists x(elim(\psi)))$, jinak
- pokud $\varphi = \forall x \psi$, vrať $elim(\neg\exists\neg\psi)$, jinak
- pokud $\varphi = \neg\psi$, vrať $\neg(elim(\psi))$, jinak
- pokud $\varphi = \psi \vee \psi'$, vrať $elim(\psi) \vee elim(\psi')$.

Rozhodni platnost výsledné proměnné bez proměnných.

Teorie musí ***připouštět eliminaci kvantifikátorů***:

- Pro každou $\exists x \varphi$ musí existovat ekvivalentní ψ bez x,
- musí existovat eliminační procedura (úplný TS), která ψ vytvoří.

Platnost formulí bez proměnných musí být rozhodnutelná.

Fourier-Motzkin: QE pro $\mathbb{Q}$ se sčítáním

QE pro formuli $\exists x \varphi$ z teorie racionálních čísel $T_{\mathbb{Q}}$ se signaturou $\{0, 1, \ldots, +, \leq\}$
(např. $\exists y \forall x . x \neq 5 \vee y \neq 3x$)

Příprava:

1. převeď φ to DNF
2. přesuň $\exists$ do disjunktů

$$(\exists x\, P \vee Q) \Leftrightarrow (\exists x\, P) \vee (\exists x\, Q)$$

3. odstraň disjunkty, které nemluví o x

$$(\exists x\, P \wedge Q) \Leftrightarrow (\exists x\, P) \wedge Q \quad \text{pokud } x \text{ není volné v } Q$$

$$\exists x((3 < x \wedge x + 2y \leq 6 \wedge y < 0) \vee (3x \leq 2y))$$
$$(\exists x\, 3 < x \wedge x + 2y \leq 6 \wedge y < 0) \vee (\exists x\, 3x \leq 2y)$$
$$((\exists x\, 3 < x \wedge x + 2y \leq 6) \wedge y < 0) \vee (\exists x\, 3x \leq 2y)$$

Fourier-Motzkin teorém

Nad $\mathbb{R}$ or $\mathbb{Q}$ máme

$$(\exists x\, c \leq ax \wedge bx \leq d) \quad \Leftrightarrow \quad bc \leq ad$$

Intuitivněji, pokud $a, b \neq 0$: $(\exists x\, c \leq ax \wedge bx \leq d) \;\Leftrightarrow\; (\exists x\, \frac{c}{a} \leq x \wedge x \leq \frac{d}{b}) \;\Leftrightarrow\; \frac{c}{a} \leq \frac{d}{b}$

Centrální eliminační formule:

$$\exists x \left(\bigwedge_{i=1}^{m} c_i \leq a_i x \right) \quad \wedge \quad \left(\bigwedge_{j=1}^{k} b_j x \leq d_j \right) \qquad \Leftrightarrow \qquad \bigwedge_{i=1}^{m} \bigwedge_{j=1}^{k} b_j c_i \qquad \leq \qquad a_i d_j$$

(pokud φ obsahuje pouze horní/pouze dolní omezení na x, potom eliminace vrátí 1)

Příklad

* $\forall x(20 + x \leq 0 \rightarrow \exists y(3y + x \leq 10 \wedge 20 \leq y - x))$
* (přeuspořádej)
  $\Leftrightarrow \forall x(20 + x \leq 0 \rightarrow \exists y(20 - x \leq y \wedge 3y \leq 10 - x))$
* (eliminuj y)
  $\Leftrightarrow \forall x(20 + x \leq 0 \rightarrow 60 + 3x \leq 10 - x)$
* (přeuspořádej)
  $\Leftrightarrow \forall x(20 + x \leq 0 \rightarrow 4x + 50 \leq 0)$
* (převeď $\forall$ na $\exists$)
  $\Leftrightarrow \neg\exists x(20 + x \leq 0 \wedge 4x + 50 > 0)$
* (přeuspořádej)
  $\Leftrightarrow \neg\exists x(-50 < 4x \wedge x \leq -20)$
* (eliminuj x)
  $\Leftrightarrow \neg(-50 < -80) \Leftrightarrow \top$

Složitost

* Centrální eliminační formule vyrobí formuli ***kvadratické*** velikosti: má $m * k$ konjunktů, její velikost je v $O(|\varphi|^2)$.
* Transformace do DNF je ***exponenciální***.
* Tyto dva kroky jsou opakovány pro každou alternaci kvantifikátorů.

$$\exists y.\forall x.(a \wedge b) \vee (c \wedge d) \vee (e \wedge f)$$
$$\exists y.\neg\exists x.\neg((a \wedge b) \vee (c \wedge d) \vee (e \wedge f))$$
$$\exists y.\neg\exists x.(\neg a \vee \neg b) \wedge (\neg c \vee \neg d) \wedge (\neg e \vee \neg f)$$
$$\exists y.\neg\exists x.(\neg a \wedge \neg c \wedge \neg e) \vee (\neg a \wedge \neg c \wedge \neg f) \vee$$
$$(\neg a \wedge \neg d \wedge \neg e) \vee (\neg a \wedge \neg d \wedge \neg f) \vee (\neg b \wedge \neg c \wedge \neg e) \vee$$
$$(\neg b \wedge \neg c \wedge \neg f) \vee (\neg b \wedge \neg d \wedge \neg e) \vee (\neg b \wedge \neg d \wedge \neg f)$$
$$\exists y.\neg(\text{kvadraticky větší DNF})$$
$$\text{exponenciální CNF ...}$$

* Složitost je ***neelementární***, věž exponenciál s výškou lineární k počtu alternací kvantifikátorů.

Některé rozhodnutelné a nerozhodnutelné teorie

Nerozhodnutelná je

- Peanova aritmetika, $\mathbb{N}$ s $=$, $+$ a $*$,
- teorie racionálních čísel $\mathbb{Q}$ s $=$, $+$ a $*$,
- teorie s $=$ a dvěma neinterpretovanými funkčními symboly/binárním relačním symbolem,
- mnoho dalších, rozhodnutelnost je vzácná.

Rozhodnutelná je

- teorie rovnosti,
- teorie reálných čísel $\mathbb{R}$ s $=$, $+$ a $*$,
- Presburgerova aritmetika, $\mathbb{N}$ s $=$ a $+$,
- Skolemova aritmetika, $\mathbb{N}$ s $=$ a $*$,
- řada existenciálních (a jiných) fragmentů teorií (použití v SMT-solvingu).