Logika a počítání

* Souvislost počítání a logického uvažování, jejich limitů.
* Gödel: aritmetika nemůže být úplná (matematické dokazování není všemocné),
  Turing: zastavení se nedá rozhodnout (počítání není všemocné).

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***.

Část I

Výroková logika (VL)

Syntaxe a sémantika výrokové logiky

* Pro danou množinu výrokových proměnných $\mathbb{X}$, ***syntaxe*** formulí je dána gramatikou

$$\varphi \to X \mid \neg(\varphi) \mid (\varphi \wedge \varphi) \quad \text{kde } X \in \mathbb{X}$$

* Další logické spojky a zkratky mohou být definovaný jako syntaktický cukr:
$\varphi \vee \psi = \neg(\neg\varphi \wedge \neg\psi)$, $\varphi \to \psi = \varphi \vee \neg\psi$, $\varphi \leftrightarrow \psi = (\varphi \to \psi) \wedge (\psi \to \varphi)$,
φ XOR $\psi = \neg(\varphi \leftrightarrow \psi)$, φ NAND $\psi = \neg(\varphi \wedge \psi)$, $0 = X \wedge \neg X$, $1 = X \vee \neg X$
* ***Ohodnocení*** $I : \mathbb{X} \to \{0, 1\}$ přiřazuje Booleovské hodnoty proměnným.
* ***Sémantika*** formulí je dána relací ***splňování***, $I \models \varphi$:

$I \models X$	právě tehdy, když	$I(X) = 1$
$I \models \neg(\varphi)$	právě tehdy, když	$I \not\models \varphi$
$I \models (\varphi \wedge \varphi')$	právě tehdy, když	$I \models \varphi$ a zároveň $I \models \varphi'$

Platnost a splnitelnost, důsledek, ekvivalence

* φ je ***platná*** (***tautologie***, $\models \varphi$) právě když $I \models \varphi$ pro všechna ohodnocení I
* φ je ***nesplnitelná*** (***kontradikce***) právě když $I \models \varphi$ pro žádné ohodnocení I
  - φ je ***platná*** právě když $\neg\varphi$ je ***nesplnitelná***
  - φ je ***splnitelná*** právě když $\neg\varphi$ je ***neplatná***
* φ a ψ jsou ***logicky ekvivalentní*** ($\varphi \Leftrightarrow \psi$) pokud je $\varphi \leftrightarrow \psi$ tautologie
* ψ je ***logickým důsledkem*** ($\varphi \Rightarrow \psi$) φ pokud je $\varphi \rightarrow \psi$ tautologie

Hilbertovský dokazovací systém VL

* ***Schémata výrokových axiomů***

$$\begin{array}{ll} \text{(A1)} & A \to (B \to A) \\ \text{(A2)} & (A \to (B \to C)) \to ((A \to B) \to (A \to C)) \\ \text{(A3)} & (\neg B \to \neg A) \to ((\neg B \to A) \to B) \end{array}$$

kde A, B, C jsou libovolné výrokové formule.

* ***Odvozovací pravidlo modus ponens (pravidlo odloučení)***

(MP) Z *předpokladů* A a $(A \to B)$ odvodíme *závěr* B.

* (A1): Pokud A určitě platí a dovím se B, tak A bude pořád platit.
* (A2): V podstatě tranzitivita implikace.
* (A3): Pokud z výroku $(\neg B)$ plyne spor, pak neplatí. Tedy platí opak, B.
* (MP): Z (*prší* $\to$ *nemám deštník*) a *prší* odvodím, že *nemám deštník*.

Důkaz

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 $\vdash \boldsymbol{\varphi}$ ($\boldsymbol{P} \vdash \boldsymbol{\varphi}$).

Příklad důkazu: $\vdash A \to A$

(1)	$A \to ((A \to A) \to A)$	(A1)
(2)	$(A \to ((A \to A) \to A)) \to ((A \to (A \to A)) \to (A \to A))$	(A2)
(3)	$(A \to (A \to A)) \to (A \to A)$	(1),(2) MP
(4)	$A \to (A \to A)$	(A1)
(5)	$A \to A$	(3),(4) MP

Pozn.:
(1) je (A1) pro volbu A, $A \to A$ za A, B
(2) je (A2) pro volbu A, $A \to A$, A za A, B, C
(3) je závěr MP z předpokladů $(1), (2)$

Normální formy

* ***Literál*** je buď proměnná (X) nebo negace proměnné ($\neg X$).
* ***Negační normální forma*** (NNF)
  - pouze $\wedge$, $\vee$ a $\neg$, $\neg$ pouze v literálech.
  - převod do NNF odstraněním ostatních spojek a aplikacích De Morganových zákonů.
* ***Disjunktivní normální forma*** (DNF) je **d**isjunkce konjunkcí literálů.
  Konjunktivní normální forma (CNF) je **k**onjunkce disjunkcí literálů.
  - převod do [C,D]NF převodem do NNF a použitím distributivních zákonů.

SAT – Splnitelnost formulí výrokové logiky

* SAT $= \{$formule VL $\varphi \mid \varphi$ je splnitelná$\}$ je rozhodnutelný problém.
* Složitost známých algoritmů v nejhorším případě více než $2^{|\mathbb{X}|}$. NP-úplný problém ... (Vyzkoušej všechna možná ohodnocení)
* SAT solvery rychlé v praktických případech (zvládají stovky tisíc proměnných).
  - pracují s DNF
  - základ backtracking, 30+ let heuristik a chytrosti (SAT competition)
* Aplikace v průmyslu:
  Plánování, kombinatorická optimalizace, lámání šifer, analýza software a hardware, generování testů, automatický design, optimalizace kompilace, zpracování přirozeného jazyka, herní AI, biologie, zdravotnictví, ...

SAT a normální formy

* Převod do ekvivalentní CNF je exponenciální.
* SAT solver může pracovat s CNF díky Tseitynově transformaci do CNF, která není ekvivalentní, ale ekvisplnitelná:
  - Induktivně ke struktuře formule nahrazuj všechny podform. φ za nové proměnné x_φ a přidávej nové konjunkty $(x_\varphi \leftrightarrow \varphi)$.
  - Pro poslední podformuli ψ přidej konjunkt x_ψ.
  - Převeď nové konjunkty do *CNF* (NNF a distributivní zákony).
* Co by znamenala existence efektivního polynomiálního překladu do DNF?

Část II

Predikátová logika (PL)

Syntaxe predikátové logiky

* ***Signatura*** jazyka PL dvojice $\langle \mathcal{F}, \mathcal{P} \rangle$ množin ***funkčních a predikátových symbolů***, každý asociovaný a ***aritou*** z $\mathbb{N}$. Píšeme $f_{/n} \in \mathcal{F}$, $p_{/n} \in \mathcal{P}$ ve smyslu symbol s ar. n. (sig. je tedy vlastně trojice $\langle \mathcal{F}, \mathcal{P}, ar \rangle$ kde $ar : \mathcal{F} \cup \mathcal{P} \to \mathbb{N}$ je arita)
* ***Jazyk formulí PL*** se signaturou $\langle \mathcal{F}, \mathcal{P} \rangle$ a množinou proměnných $\mathbb{X}$ je dán gramatikou

$$\varphi \to p(\overbrace{t, \ldots, t}^{n}) \mid \neg(\varphi) \mid (\varphi \wedge \varphi) \mid (\exists x \varphi) \qquad p_{/n} \in \mathcal{P}$$

$$t \to f(\underbrace{t, \ldots, t}_{m}) \mid x \qquad x \in \mathbb{X}, f_{/m} \in \mathcal{F}$$

* t je ***term***
* $p(t, \ldots, t)$ je ***atomická formule***
* Další spojky a 0 a 1 jsou syntaktický cukr jako ve VL, plus $(\forall x \varphi) = \neg(\exists x \neg \varphi)$.
* ***Volný/vázaný výskyt proměnné*** ..., ***věta*** = uzavřená formule (bez volných prom.)

Sémantika predikátové logiky

* ***Interpretace/realizace*** jazyka se sig. $\langle \mathcal{F}, \mathcal{P} \rangle$ a proměnnými $\mathbb{X}$ je pár $I = (D_I, \alpha_I)$, kde
  - D_I je ***doména***, libovolná neprázdná množina
  - α_I přiřazuje prvky D_I a relace/funkce nad D_I proměnným a pred./fun. symbolům.
* Termy jsou interpretovány jako hodnoty z domény:

$$\alpha_I(f(x_1, \ldots, x_n)) = \alpha_I(f)(\alpha_I(x_1), \ldots, \alpha_I(x_n)) \quad f_{/n} \in \mathcal{F}$$

* Sémantika formulí je dána relací splnění v interpretaci, $I \models \varphi$:

$$\begin{array}{lll} I \models p(t_1, \ldots, t_n) & \text{právě když} & (\alpha_I(t_1), \ldots, \alpha_I(t_n)) \in \alpha_I(p) \quad p_{/n} \in \mathcal{P} \\ I \models \varphi_1 \wedge \varphi_2 & \text{právě když} & I \models \varphi_1 \text{ a zároveň } I \models \varphi_2 \\ I \models \neg\varphi & \text{právě když} & I \not\models \varphi \\ I \models \exists x \varphi & \text{právě když} & I[x/v]^* \models \varphi \text{ pro nějaké } v \in D_I \end{array}$$

Pokud $I \models \varphi$, potom I je ***modelem*** φ.

*$f[x/v]$ vznikne z f přesměrováním funkční hodnoty $f(x)$ na v.

Důkazový systém PL

* Axiomy VL a modus ponens.
* ***Schéma axiomů kvantifikátoru***: Není-li x volné ve φ, pak

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

* ***Schéma axiomů substituce***: pokud t je term substituovatelný[a] za x do φ

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

* ***Axiomy rovnosti***: Pro $f_{/n} \in \mathcal{F}$, $p_{/n} \in \mathcal{P}$ a proměnné $x, x_i, y_i, 1 \leq i \leq n$

$$x = x, \qquad x_1 = y_1 \to (x_2 = y_2 \to (\ldots (x_n = y_n \to f(x_1, \ldots, x_n) = f(y_1, \ldots, y_n)) \ldots))$$

$$x_1 = y_1 \to (x_2 = y_2 \to (\ldots (x_n = y_n \to p(x_1, \ldots, x_n) \to p(y_1, \ldots, y_n)) \ldots))$$

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

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

[a] t neobsahuje volné proměnné φ

Příklady axiomů PL

* axiom kvantifikátoru: $(\forall x(\varphi \to \psi)) \to (\varphi \to (\forall x \psi))$

$$(\forall \textit{Brňák}\ (\textit{je hezky} \to \textit{Brňák je na přehradě})) \to (\textit{je hezky} \to (\forall \textit{Brňák}(\textit{Brňák je na přehradě})))$$

* axiom substituce: $(\forall x\, \varphi) \to \varphi[x/t]$

$$(\forall \check{c}\ \textit{zaslouží\_soucit}(\check{c})) \to \textit{zaslouží\_soucit}(\textit{matka}(\textit{manželka}(x)))$$

* ax. rovnosti: $x_1 = y_1 \to (\ldots (x_n = y_n \to p(x_1, \ldots, x_n) \to p(y_1, \ldots, y_n)) \ldots)$

$$(\textit{pivo} = \textit{chleba} \to (\textit{snídaně}(\textit{chleba}, \textit{máslo}) \to \textit{snídaně}(\textit{pivo}, \textit{máslo}))$$

Příklad důkazu v PL: $p(x, y) \vdash p(y, x)$

(1)	$p(x, y)$	(předpoklad)
(2)	$\forall y\, p(x, y)$	(pravidlo zobecnění)
(3)	$\forall x \forall y\, p(x, y)$	(pravidlo zobecnění)
(4)	$(\forall x \forall y\, p(x, y)) \rightarrow (\forall y\, p(z, y))$	(axiom substituce, x za z)
(5)	$\forall y\, p(z, y)$	(MP)
(6)	$(\forall y\, p(z,y)) \rightarrow p(z,x)$	(axiom substituce, y za x)
(7)	$p(z, x)$	(MP)
(8)	$(\forall z\, p(z, x))$	(pravidlo zobecnění)
(9)	$(\forall z\, p(z, x)) \rightarrow p(y, x)$	(axiom substituce, z za y)
(10)	$p(y, x)$	(MP)

Pozn.:
(1): předpoklad; (2): p. zobec. pro $\varphi = (1)$, x = y; (3): p. zobec. pro $\varphi = (2)$;
(4): ax. subst. pro $\varphi = (3)$ a $t = z$; (5): MP pro $\varphi = (3)$ a $\varphi \rightarrow \psi = (4)$;
(6): ax. subst. pro $\varphi = (5)$, $x = y$ a $t = x$; (7): MP pro $\varphi = (5)$ a $\varphi \rightarrow \psi = (6)$;
(8): ax. subst. pro $\varphi = (7)$, $x = z$; (9): ax. subst. pro $\varphi = (8)$, $x = z$ a $t = y$;
(10): MP pro $\varphi = (8)$ a $\varphi \rightarrow \psi = (9)$;

Část III

Vlastnosti logických systémů

Efektivnost

Logický systém je efektivní, pokud můžeme efektivně ověřit korektnost logického argumentu, důkazu. TS ověří, že daný řetězec symbolů je důkaz.

Výroková i predikátová logika je efektivní.

* Protože můžeme algoritmicky ověřit
  1. co je dobře formulovaná formule,
  2. co je axiom,
  3. že formule v důkazu byla odvozena odvozovacími pravidly z předchozích.

Dokazatelnost versus Platnost

$\vdash \varphi$	$\models \varphi$
Dokazatelná (z axiomů pomocí odvoz. prav.). Čistě syntaktická manipulace.	Platná ve všech interpretacích. Rozhoduje sémantika, význam. Ve VL ověříme pravď. tabulkou, SAT, ... V PL problém s nekon. dom. a $\forall\psi$

$\vdash \varphi$ je ověřením $\models \varphi$
Důkaz je ověřením platnosti.

Mělo byt tedy platit, že
$\vdash \varphi \iff \models \varphi.$

Korektnost a sémantická úplnost

Systém je ***korektní*** pokud

$$\vdash \varphi \implies \models \varphi$$

Co je dokazatelné, to je platné.
Nemůžeme dokázat nesmysly.

Systém je sémanticy ***úplný*** pokud

$$\models \varphi \implies \vdash \varphi$$

Vše platné můžeme dokázat.

Korektnost a sémantická úplnost Hilbertovského systému pro VL a PL

Výroková i predikátová logika je korektní a sémanticky úplná. (Post, Gödel)
Pro libovolnou formuli VL nebo PL platí $\models \varphi \iff \vdash \varphi$.

Pro PL je to Gödelova věta o úplnosti.

Kurt Gödel

Brno, 1906 - 1978

Část IV

Teorie v PL

Platnost a dokazování ve vybraných strukturách

$$\not\models 1 + 1 = 2$$

Chceme vyjádřit a dokázat, že $1 + 1 = 2$ je platná v přirozených číslech, jak je známe (t.j. když 1, 2, a + jsou interpretovány, jak jsme zvyklí)

K tomu slouží logické teorie:

$$[\text{Teorie celých čísel}] \models 1 + 1 = 2$$

Teorie

- ***Teorie*** s jazykem L je množina T ***speciálních axiomů***, vět z jazyka L.
- ***Model*** T je interpretace $\mathcal{M}$ jazyka L, kde $\mathcal{M} \models \psi$ pro všechny $\psi \in T$. $\boldsymbol{\mathcal{M} \models T}$.
- ***Důsledek teorie*** je formule φ platná ve všech jejích modelech. $\boldsymbol{T \models \varphi}$.
- ***Dokazatelnost v teorii*** T je dokazatelnost z předpokladů T. $\boldsymbol{T \vdash \varphi}$

- T-splnitelnost – formuli splňuje nějaký model teorie T
- T-ekvivalence – formule mají stejné modely teorie T,
- T-důsledek ...

Stále platí Gödelova věta o úplnosti PL:

$$\boldsymbol{T \models \varphi \iff T \vdash \varphi}$$

Příklady teorií

Teorie uspořádání $T_\leq$ má speciální axiomy

$$\begin{array}{rr} \forall x(x \leq x) & \text{(reflexivita)} \\ \forall x \forall y \forall z((x \leq y \wedge y \leq z) \rightarrow x \leq z) & \text{(tranzitivita)} \\ \forall x \forall y \forall z((x \leq y \wedge y \leq x) \rightarrow x = y) & \text{(antisymtetrie)} \end{array}$$

Příklad modelu: $D_\mathcal{M} = \{1, 2, 3\}$, $\mathcal{M}(\leq) = \{(1, 2), (1, 1), (2, 2), (3, 3)\}$, $\mathcal{M} \models T_\leq$
$T_\leq \models x \not\leq y \vee y \not\leq x \vee x = y$ a také $T_\leq \vdash x \not\leq y \vee y \not\leq x \vee x = y$

Teorie grup T_G má speciální axiomy

$$\begin{array}{rr} \forall x \forall y \forall z(x \cdot (y \cdot z) = (x \cdot y) \cdot z) & \text{(asociativita)} \\ \forall x(x \cdot e = x \wedge e \cdot x = x) & \text{(neutrální prvek)} \\ \forall x \exists y(x \cdot y = e \wedge y \cdot x = e) & \text{(inverzní prvky)} \end{array}$$

$D_\mathcal{M} = \{0, 1\}$, $\mathcal{M}(e) = 1$, $\mathcal{M}(\cdot) =$ násobení ve zbytkové třídě 2
$T_G \models x = e \rightarrow x \cdot x = x$ a také $T_G \vdash x = e \rightarrow x \cdot x = x$.

Příklady teorií: Peanova aritmetika T_{PA}

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:

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

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)

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

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

Teorie racionálních čísel se sčítáním

1. $\forall x \forall y \big((x \leq y \wedge y \leq x) \rightarrow x = y \big)$ (antisymmetry)
2. $\forall x \forall y \forall z \big((x \leq y \wedge y \leq z) \rightarrow x \leq z \big)$ (transitivity)
3. $\forall x \forall y (x \leq y \vee y \leq x)$ (totality)
4. $\forall x \forall y \forall z \big((x + y) + z = x + (y + z) \big)$ ($+$ associativity)
5. $\forall x (x + 0 = x)$ ($+$ identity)
6. $\forall x (x + (-x) = 0)$ ($+$ inverse)
7. $\forall x \forall y (x + y = y + x)$ ($+$ commutativity)
8. $\forall x \forall y \forall z (x \leq y \rightarrow x + z \leq y + z)$ ($+$ ordered)
9. for each positive integer n,
   $\forall x (nx = 0 \rightarrow x = 0)$ (torsion-free)
   $\forall x \exists y (x = ny)$ (divisible)

*where nx denotes $\overbrace{x + \cdots + x}^{n}$

Bezespornost

Teorie T je ***bezesporná***, pokud neexistuje formule φ taková, že $T \vdash \varphi$ a $T \vdash \neg\varphi$.

* Bezespornost je základ smysluplnosti. Axiomy si nesmí protiřečit.
* Ve sporné teorii je možné dokázat cokoliv.
  Pokud $T \vdash \varphi$ a $T \vdash \neg\varphi$, pak i $T \vdash \varphi \wedge \neg\varphi$. Nepravda, 0, je tedy dokazatelná.
  Z nepravdy pak plyne cokoliv (protože $0 \to \psi$ vždy platí).
* Sporná teorie nemá žádný model, protože 0 nemůže platit v žádné interpretaci.

Teorie je bezesporná právě tehdy, když má model.

Bezespornost, příklad

Teorie T:

$$\forall x \forall y \, (x < y)$$
$$\neg \forall x \forall y \, (x < y)$$
$$\forall x \, (x \not< x)$$

Teorie T':

$$\forall x \forall y \forall z \, (x.(y.z)) = ((x.y).z)$$
$$\forall x \, (x.e = e.x = x)$$
$$\exists z \, (z \neq e \wedge \forall x \, (x.z = z.x = x))$$

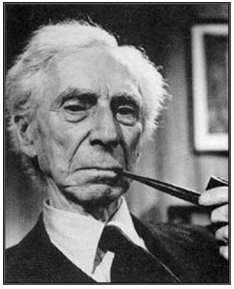
Teorie T'':

$$\exists x \, (f(x) = 0)$$
$$\forall x \forall y \, (f(x) = f(y))$$
$$\neg \exists x \, (f(x) = x)$$

Russelův paradox ve Fregeho naivní teorii množin

Gottlob Frege

Bertrand Russel



Mějme množinu M, obsahující všechny množiny, které nejsou svým vlastním prvkem.
Je M svým vlastním prvkem?
Jestli je M vlastním prvkem, pak, podle definice, není vlastním prvkem.
Jestli M není vlastním prvkem, pak, podle definice, je vlastním prvkem.
Zatr sakr ...

Syntaktická úplnost teorií, intuitivně

* Úplnost teorie formalizuje „přesnost“, nebo „jednoznačnost“ definice.
* Definice je přesná, jednoznačná, pokud definuje přesně jednu věc, jednu mat strukturu. Nevyhovuje jí hned několik různých mat. struktur.

Syntaktická úplnost teorií

Teorie T je ***úplná***, pokud pro každou větu φ jazyka T platí
$T \vdash \varphi$, nebo $T \vdash \neg\varphi$.
(Každou uzav. formuli jazyka je v T možno dokázat nebo vyvrátit.)

* Nechť T má právě jeden model $\mathcal{M}$ (až na izomorfismus).
* Pro každou formuli jazyka T máme $\mathcal{M} \models \varphi$, nebo $\mathcal{M} \models \neg\varphi$ (z def. $\mathcal{M} \models$).
* Protože $\mathcal{M}$ je jediný, tak $T \models \varphi$, nebo $T \models \neg\varphi$.
* Z věty o úplnosti PL ($T \models \psi \Leftrightarrow T \vdash \psi$) plyne, že $T \vdash \varphi$, nebo $T \vdash \neg\varphi$.

Teorie má jediný model $\Rightarrow$ je úplná.

Je úplná $\Leftrightarrow$ nemá dva modely rozlišitelné formulemi jazyka
(t.j., neexistují $\mathcal{M}, \mathcal{M}', \varphi$ tak, že $\mathcal{M} \models \varphi$ a $\mathcal{M}' \models \neg\varphi$)

Syntaktická úplnost teorií, příklady

Teorie relací ekvivalence:

$$\forall x\,(x \sim x)$$
$$\forall x \forall y\,(x \sim y \to y \sim x)$$
$$\forall x \forall y \forall z\,((x \sim y \wedge y \sim z) \to x \sim z)$$

* $\mathcal{M}$: $D_{\mathcal{M}} = \{1\}$, $\mathcal{M}(\sim) = \{(1,1)\}$
* $\mathcal{M}'$: $D_{\mathcal{M}'} = \{1,2\}$, $\mathcal{M}'(\sim) = \{(1,1),(2,2)\}$
* $\varphi : \forall x \forall y\,(x \sim y)$, $\mathcal{M} \models \varphi$ a $\mathcal{M}' \models \neg\varphi$, tedy není úplná.

Chceme definovat dvouprvkový svaz s maximem 1 a minimem 0.

$$0 \leq 1 \wedge 0 \leq 0 \wedge 1 \leq 1 \wedge 1 \not\leq 0$$
$$\forall x\,(x = 0 \vee x = 1)$$

$$\mathcal{M} : D_{\mathcal{M}} = \{a,b\},\ \mathcal{M}(0) = a,\ \mathcal{M}(1) = b,\ \mathcal{M}(\leq) = \{(a,b),(a,a),(b,b)\}$$

Jediný model $\Rightarrow$ je úplná.

Příklad (beze)sporné a (ne)úplné teorie

$$\varphi_1 : \forall y(1.y = y) \qquad \varphi_2 : \forall y(1.y = 1) \qquad \varphi_3 : \neg\exists x(x.x = x)$$

* $T_1 = \{\varphi_1\}$
  - bezesporná, má model $\mathcal{M}$ s $D_{\mathcal{M}} = \{a\}$, $\mathcal{M}(1) = a$, a $\mathcal{M}(.) = \{((a, a), a)\}$
  - není úplná, má model $\mathcal{M}'$ s $D_{\mathcal{M}'} = \{a, b\}$, $\mathcal{M}'(1) = a$, $\mathcal{M}'(.) = \{((a, a), a), ((a, b), b)), ((b, a), a), ((b, b), a)\}$ a pro $\psi = \exists x(x.x \neq x)$ je $\mathcal{M} \not\models \neg\psi$ ale $\mathcal{M}' \models \psi$.
* $T_2 = \{\varphi_1, \varphi_2\}$
  - stále bezesporná ($\mathcal{M}$)
  - úplná, $\mathcal{M}$ je jediný (každá φ v $\mathcal{M}$ platí pozitivní nebo negovaná, a tedy platí pro všechny modely, což se pak z Gö. v. o ú. dá dokázat)
* $T_3 = \{\varphi_1, \varphi_3\}$
  - sporná, obojí nemůže platit zároveň v žádné interpretaci, nemá model
  - každá sporná teorie je i úplná, protože ze sporu je dokazatelné vše

Efektivnost + korektnost + synt. úplnost $\Rightarrow$ rozhodování důsledků teorie

Pro efekt. úplnou teorii T ex. program/TS ***Rozhodovač důsledků T/platnosti v T***.
Pro danou φ pracuje takto:

foreach *slovo w z abecedy jazyka T* `// slova v lexikografickém pořadí`
do
  if *w je důkaz φ v T* **then** φ je důsledkem T
  if *w je důkaz $\neg\varphi$* **then** φ není důsledkem T

* Efektivnost zaručuje, že jsme shopni ověřit, co je důkaz.
* Korektnost zaručuje, že odpověď je správná.
* Synt. úplnost zaručuje, že program skončí nalezením důkazu nebo vyvrácení φ (jeden z nich existuje).

Příklad běhu Mecha. matematika: Je $T_{PA} \models S(0) + S(0) = S(S(0))$?

a	
b	$xyp =\!\!\rightarrow$
c	$\ldots$
$\ldots$	$x = y \rightarrow p$
$\wedge$	$\ldots$
$\neg$	$xy =\!\!\rightarrow (((, ((\wedge\neg\neg x, , \exists$
$\exists$	$\ldots$
aa	$p\rightarrow((p\rightarrow p)\rightarrow p)$, $(p\rightarrow(p\rightarrow p)\rightarrow(p\rightarrow p))$, $\forall x \forall y\, x{=}y$
ab	$\ldots$
ac	Psal jsem si se slepýšem, ale už si nepíšem. (Plíhal)
$\ldots$	$\ldots$
aab	$\boldsymbol{p\rightarrow((p\rightarrow p)\rightarrow p)}$, $\boldsymbol{(p\rightarrow((p\rightarrow p)\rightarrow p)\rightarrow((p\rightarrow(p\rightarrow p))\rightarrow(p\rightarrow p))}$, $\underline{\boldsymbol{(p\rightarrow(p\rightarrow p)\rightarrow(p\rightarrow p))}}$
$\ldots$	$\ldots$
$ab\exists$	$\ldots$
$\ldots$	$\ldots$
$a \vee b\neg($	$\boldsymbol{\forall\neg(S(x){=}0)}$**.....důkaz.....**, $\underline{\boldsymbol{S(0){+}S(0){=}S(S(0))}}$
$\ldots$	

Rozhodnutelnost, úplnost, SAT

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 (generátor časem vygeneruje důkaz φ nebo $\neg\varphi$)

Efektivní, bezesporná a úplná teorie je rozhodnutelná.
Efektivní a bezesporná teorie je částečně rozhodnutelná.

* Sporná teorie je rozhodnutelná triviálně, protože každá formule je jejím důsledkem.
* Rozhodnutelnost neimplikuje úplnost!
* Formule φ s volnými proměnnými $x_1, \ldots, x_n$ je T-splnitelná $\Leftrightarrow$ $T \models \exists x_1 \ldots \exists x_n \varphi$.
* Věta φ je T-splnitelná $\Leftrightarrow$ $T \models \varphi$.

Část V

SMT-solving

Co a k čemu je SMT-solving?

* ***SMT - SAT Modulo Theory***. SAT solver, s nadstavbou pro prvořádové teorie.
* Omezený ale praktický mechanický matematik (nemá rád kvantifikátory, občas neví, ...).
* Rozhodne, zda je daná formule v dané teorii splnitelná, příp. vrátí model.

$$(x + 5 \leq 6 \wedge x.y = z + 2 \wedge x/5 = z) \rightarrow (z \mod y = 10) \quad \text{(aritmetika na } \mathbb{N}, \mathbb{Z}, \mathbb{Q}, \mathbb{R})$$
$$a[i]_r = e \rightarrow \forall j((a[i, e]_w)[j]_r = a[j]_r) \quad \text{(teorie polí)}$$
$$((y_4 +_8 1) \not<_8 y_3) \wedge y_2 = y_4 +_8 y_1 \quad \text{(teorie bitových vektorů)}$$
$$x \in \texttt{Name:[a} - \texttt{z]}* \wedge y \in \texttt{Year:.}* \wedge z = x.y \wedge |z| \leq 10 \quad \text{(teorie řetězců)}$$

* Vyřeš sudoku! Co naskládat do kamionu, aby to v rámci váhového limitu mělo co největší cenu? Naplánuj cestu. Navrhni rozvrh. Jak donutit program projít danými řádky? Je toto invariant cyklu? ...
* Aplikace v automatickém testování, verifikaci, v návrhu a syntéze systémů, plánování, optimalizaci, inferenci typů, AI, ...
  - Certora, Trail of Bits – verifikace block-chain kontraktů (Brno)
  - Honeywell – automatické generování testů (Brno)
  - RedHat – pokusy o formální metody (Brno)
  - Amazon – analýza konfig. Cloud služeb (N. Rungta: A Billion SMT Queries per Day)
  - Microsoft – formální metody obecně
  - AI (ChatGPT + SMT?)

Architektura SMT-solveru

Vstup:

* formule
* identifikace teorie

Komponenty:

* ***SAT-solver***. Řeší výrokové formule v CNF, zvládá řádově až 10^7 proměnných.
* ***Theory-solver***. Hledá řešení *konjunkcí* v dané teorii.
  Každá teorie potřebuje vlastní specializovaný algoritmus.

1. SAT-solverem najdi model Booleovské kostry, pokud neexistuje, vrať UNSAT.
2. Theory-solverem zkontroluj model z hlediska teorie.
   - Pokud je model splnitelný z hlediska teorie, vrať SAT,
   - jinak přidej Booleovské kostře negaci modelu jako naučenou klauzuli, goto 1.

Příklad

$$\varphi : (x < 0 \vee x \not< 2) \wedge (x < 2 \vee x = 3) \wedge (x = -1 \vee \neg x < 0),\ T_{\mathbb{Z}}$$

Bool. kostra: $(a \vee \neg b) \wedge (b \vee c) \wedge (d \vee \neg a)$

1. SAT-solver: SAT, $\{a \mapsto 1, b \mapsto 1, c \mapsto 1, d \mapsto 1\}$
   Theory-solver: $(x < 0 \wedge x < 2 \wedge x = -1 \wedge x = 3)$ je UNSAT. Learned cl. $\neg(a \wedge b \wedge c \wedge d)$
2. SAT-solver: SAT, $\{a \mapsto 0, b \mapsto 1, c \mapsto 1, d \mapsto 0\}$
   Theory-solver: $(\neg x < 0 \wedge x < 2 \wedge x = -1 \wedge \neg x = 3)$ je UNSAT. L. cl. $\neg(\neg a \wedge b \wedge c \wedge \neg d)$
3. SAT-solver: SAT, $\{a \mapsto 0, b \mapsto 0, c \mapsto 0, d \mapsto 1\}$
   Theory-solver: $(\neg x < 0 \wedge \neg x < 2 \wedge \neg x = -1 \wedge x = 3)$ je SAT, $\{x \mapsto 3\}$ je řešení.