Úvod do matematickej logiky

1 Syntax a sémantika výrokovej logiky prvého rádu

Definícia 4.20

Literál je atóm
alebo negácia atómu.

Klauzula (tiež „klauza“, angl. *clause*)
je *disjunkcia* postupnosti literálov.

Formula v konjunktívnom normálnom tvare
(angl. conjunctive normal form, *CNF*)
je *konjunkcia* postupnosti klauzúl.

Definícia 10.2

Symbolmi jazyka logiky prvého rádu $\mathcal{L}$ sú:

indivíduové premenné z nejakej nekonečnej spočítateľnej množiny $\mathcal{V}_\mathcal{L}$;

mimologické symboly:

indivíduové konštanty z nejakej spočítateľnej množiny $\mathcal{C}_\mathcal{L}$,
funkčné symboly z nejakej spočítateľnej množiny $\mathcal{F}_\mathcal{L}$,
predikátové symboly z nejakej spočít. množiny $\mathcal{P}_\mathcal{L}$;

logické symboly: *logické spojky* — unárna $\neg$ a binárne $\land$, $\lor$ a $\to$,
symbol rovnosti $\doteq$ a *kvantifikátory* — *existenčný* $\exists$ a *všeobecný* $\forall$;

pomocné symboly: (,) a , (ľavá zátvorka, pravá zátvorka a čiarka).

Množiny $\mathcal{V}_\mathcal{L}, \mathcal{C}_\mathcal{L}, \mathcal{F}_\mathcal{L}, \mathcal{P}_\mathcal{L}$ sú vzájomne disjunktné. Logické ani pomocné symboly sa nevyskytujú v symboloch z $\mathcal{V}_\mathcal{L}, \mathcal{C}_\mathcal{L}, \mathcal{F}_\mathcal{L}, \mathcal{P}_\mathcal{L}$.

Každému symbolu $s \in \mathcal{P}_\mathcal{L} \cup \mathcal{F}_\mathcal{L}$ je priradená *arita* $\operatorname{ar}(s) \in \mathbb{N}^+$.

Definícia 6.4 (Atomické formuly)

Nech $\mathcal{L}$ je jazyk relačnej logiky prvého rádu.

Rovnostný atóm jazyka $\mathcal{L}$ je každá postupnosť symbolov $t_1 \doteq t_2$, kde t_1 a t_2 sú termy jazyka $\mathcal{L}$.

Predikátový atóm jazyka $\mathcal{L}$ je každá postupnosť symbolov $P(t_1, \dots, t_n)$, kde P je predikátový symbol s aritou n a $t_1, \dots, t_n$ sú termy jazyka $\mathcal{L}$.

Atomickými formulami (skrátene *atómami*) jazyka $\mathcal{L}$ súhrnne nazývame všetky rovnostné a predikátové atómy jazyka $\mathcal{L}$.

Množinu všetkých atómov jazyka $\mathcal{L}$ označujeme $\mathcal{A}_{\mathcal{L}}$.

Definícia 6.3 (Term)

Nech $\mathcal{L}$ je jazyk relačnej logiky prvého rádu. Indivíduové premenné z $\mathcal{V}_{\mathcal{L}}$ a konštanty z $\mathcal{C}_{\mathcal{L}}$ súhrnne nazývame *termy* jazyka $\mathcal{L}$.

Definícia 10.4

Množina $\mathcal{T}_{\mathcal{L}}$ *termov* jazyka logiky prvého rádu $\mathcal{L}$ je najmenšia množina postupností symbolov jazyka $\mathcal{L}$, pre ktorú platí:

i. každá indivíduová premenná $x \in \mathcal{V}_{\mathcal{L}}$ patrí do $\mathcal{T}_{\mathcal{L}}$ (teda $\mathcal{V}_{\mathcal{L}} \subseteq \mathcal{T}_{\mathcal{L}}$);
ii. každá indivíduová konštanta $c \in \mathcal{C}_{\mathcal{L}}$ patrí do $\mathcal{T}_{\mathcal{L}}$ (teda $\mathcal{C}_{\mathcal{L}} \subseteq \mathcal{T}_{\mathcal{L}}$);
iii. ak f je funkčný symbol s aritou n a $t_1, \dots, t_n$ patria do $\mathcal{T}_{\mathcal{L}}$, tak aj postupnosť symbolov $f(t_1, \dots, t_n)$ patrí do $\mathcal{T}_{\mathcal{L}}$.

Každý prvok $\mathcal{T}_{\mathcal{L}}$ je *term* jazyka $\mathcal{L}$ a nič iné nie je termom jazyka $\mathcal{L}$.

Definícia 10.8

Množina $\mathcal{E}_\mathcal{L}$ všetkých *formúl* jazyka logiky prvého rádu $\mathcal{L}$
je najmenšia množina postupností symbolov jazyka $\mathcal{L}$, ktorá spĺňa všetky nasledujúce podmienky:

i. Každý atóm z $\mathcal{A}_\mathcal{L}$ patrí do $\mathcal{E}_\mathcal{L}$. Inak povedané, $\mathcal{A}_\mathcal{L} \subseteq \mathcal{E}_\mathcal{L}$.

ii. Ak A patrí do $\mathcal{E}_\mathcal{L}$, tak aj postupnosť symbolov $\neg A$ patrí do $\mathcal{E}_\mathcal{L}$ a nazývame ju *negácia* formuly A.

iii. Ak A a B sú v $\mathcal{E}_\mathcal{L}$, tak aj postupnosti symbolov $(A \wedge B)$, $(A \vee B)$ a $(A \rightarrow B)$ patria do $\mathcal{E}_\mathcal{L}$ a nazývame ich postupne *konjunkcia*, *disjunkcia* a *implikácia* formúl A a B.

iv. Ak x je indivíduová premenná a A patrí do $\mathcal{E}_\mathcal{L}$, tak aj postupnosti symbolov $\exists x\, A$ a $\forall x\, A$ patria do $\mathcal{E}_\mathcal{L}$ a nazývame ich postupne *existenčná* a *všeobecná kvantifikácia* formuly A vzhľadom na x.

Každý prvok A množiny $\mathcal{E}_\mathcal{L}$ nazývame *formulou* jazyka $\mathcal{L}$.

Definícia 6.10 (Oblasť platnosti kvantifikátora)

Nech A je postupnosť symbolov, nech B je formula,
nech $Q \in \{\forall, \exists\}$, nech x je premenná.
V postupnosti $A = \ldots Q\, x\, B \ldots$ sa výskyt formuly $Q\, x\, B$ nazýva *oblasť platnosti kvantifikátora $Q\, x$ v A*.

Definícia 6.12 (Voľné a viazané výskyty premenných)

Nech A je postupnosť symbolov, nech x je premenná.

Výskyt premennej x v A je *viazaný* vtt
sa *nachádza v niektorej* oblasti platnosti kvantifikátora $\forall x$ alebo $\exists x$ v A.

Výskyt premennej x A je *voľný* vtt
sa *nenachádza v žiadnej* oblasti platnosti kvantifikátora $\forall x$ ani $\exists x$ v A.

Definícia 6.14 (Voľné a viazané premenné)

Nech A je formula alebo term, nech x je premenná.

Premenná x je *viazaná* v A vtt

x sa vyskytuje v A a *všetky* výskyty x v A sú viazané.

Premenná x je *voľná* v A vtt x má v A *aspoň jeden voľný výskyt*.

Množinu voľných premenných formuly A označíme $\mathrm{free}(A)$.

Definícia 6.17 (Uzavretá formula, teória)

Formula A jazyka $\mathcal{L}$ je *uzavretá* vtt

žiadna premenná nie je voľná v A

(teda $\mathrm{free}(A) = \emptyset$).

Teóriou v jazyku $\mathcal{L}$ je každá

spočítateľná množinu uzavretých formúl jazyka $\mathcal{L}$.

Definícia 10.12

Nech $\mathcal{L}$ je jazyk logiky prvého rádu.

Štruktúrou pre jazyk $\mathcal{L}$ nazývame dvojicu $\mathcal{M} = (D, i)$, kde

doména D štruktúry $\mathcal{M}$ je ľubovoľná neprázdna množina;

interpretačná funkcia i štruktúry $\mathcal{M}$ je zobrazenie, ktoré

- každému symbolu konštanty c jazyka $\mathcal{L}$ priraďuje prvok $i(c) \in D$;
- každému funkčnému symbolu f jazyka $\mathcal{L}$ s aritou n priraďuje funkciu $i(f): D^n \to D$;
- každému predikátovému symbolu P jazyka $\mathcal{L}$ s aritou n priraďuje množinu $i(P) \subseteq D^n$.

Definícia 6.21

Nech $\mathcal{M} = (D, i)$ je štruktúra pre jazyk $\mathcal{L}$.
Ohodnotenie indivíduových premenných je ľubovoľná funkcia $e : \mathcal{V}_{\mathcal{L}} \to D$ (priraďuje premenným prvky domény).

Nech ďalej x je indivíduová premenná z $\mathcal{L}$ a d je prvok D.
Zápisom $e(x/d)$ označíme ohodnotenie indivíduových premenných, ktoré premennej x priraďuje hodnotu d
a všetkým ostatným premenným rovnakú hodnotu ako im priraďuje e, čiže

$$e(x/d)(y) = \begin{cases} d, & \text{ak } y = x, \\ e(y), & \text{ak } y \neq x, \end{cases}$$

alebo množinovo zapísané $e(x/d) = e \setminus \{x \mapsto e(x)\} \cup \{x \mapsto d\}$.

Definícia 6.22

Nech $\mathcal{M} = (D, i)$ je štruktúra, e je ohodnotenie premenných.
Hodnotou termu t v štruktúre $\mathcal{M}$ pri ohodnotení premenných e je prvok $t^{\mathcal{M}}[e]$ z D určený nasledovne:

- $t^{\mathcal{M}}[e] = e(x)$, ak t je premenná $x \in \mathcal{V}_{\mathcal{L}}$,
- $t^{\mathcal{M}}[e] = i(a)$, ak t je konštanta $a \in \mathcal{C}_{\mathcal{L}}$.

Definícia 10.15

Nech $\mathcal{M} = (D, i)$ je štruktúra pre jazyk logiky prvého rádu $\mathcal{L}$, nech e je ohodnotenie premenných.
Hodnotou termu t v štruktúre $\mathcal{M}$ pri ohodnotení premenných e je prvok z D označovaný $t^{\mathcal{M}}[e]$ a zadefinovaný induktívne pre všetky premenné x, konštanty a, každú aritu n, všetky funkčné symboly f s aritou n, a všetky termy $t_1, \ldots, t_n$ nasledovne:

$$\begin{aligned} x^{\mathcal{M}}[e] &= e(x), \\ a^{\mathcal{M}}[e] &= i(a), \\ \big(f(t_1, \dots, t_n)\big)^{\mathcal{M}}[e] &= i(f)\big(t_1^{\mathcal{M}}[e], \dots, t_n^{\mathcal{M}}[e]\big). \end{aligned}$$

Definícia 6.25

Nech X je uzavretá formula jazyka $\mathcal{L}$, nech T je teória v jazyku $\mathcal{L}$ a nech $\mathcal{M}$ je štruktúra pre $\mathcal{L}$.

Formula X je *pravdivá* v štruktúre $\mathcal{M}$ (skrátene $\mathcal{M} \models X$) vtt $\mathcal{M}$ spĺňa formulu X pri každom ohodnotení e.
Vtedy tiež hovoríme, že $\mathcal{M}$ je *modelom* formuly X.

Teória T je *pravdivá* v štruktúre $\mathcal{M}$ (skrátene $\mathcal{M} \models T$) vtt každá formula X z T je pravdivá v $\mathcal{M}$.
Vtedy tiež hovoríme, že $\mathcal{M}$ je *modelom* teórie T.

2 Tablový kalkul pre výrokovú logiku, korektnosť a úplnosť tablového kalkulu

Pre mnohé logické jazyky sú známe **kalkuly** — množiny usudzovacích pravidiel, ktoré sú

korektné — odvodzujú iba logické dôsledky,
úplné — umožňujú odvodiť všetky logické dôsledky.

Definícia 5.4

Nech $\mathcal{L}$ je jazyk výrokovologickej časti logiky prvého rádu.
Nech X je výrokovologická formula jazyka $\mathcal{L}$.
Postupnosti symbolov $\mathbf{T}\,X$ a $\mathbf{F}\,X$ nazývame *označené formuly*.

Definícia 5.5

Nech $\mathcal{L}$ je jazyk výrokovologickej časti logiky prvého rádu, v je ohodnotenie pre $\mathcal{L}$ a X je výrokovologická formula v $\mathcal{L}$. Potom

- *vo v je pravdivá $\mathbf{T}\,X$* (skrátene $v \models_p \mathbf{T}\,X$) vtt vo v je pravdivá X;
- *vo v je pravdivá $\mathbf{F}\,X$* (skr. $v \models_p \mathbf{F}\,X$) vtt vo v nie je pravdivá X.

Definícia (Jednotný zápis označených formúl typu α)

Označená formula je *typu α* vtt má jeden z tvarov v ľavom stĺpci tabuľky pre nejaké formuly A a B.
Takéto formuly označujeme písmenom α; α_1 označuje príslušnú formulu zo stredného stĺpca a α_2 príslušnú formulu z pravého stĺpca.

α	α_1	α_2
$\mathbf{T}(A \wedge B)$	$\mathbf{T}A$	$\mathbf{T}B$
$\mathbf{F}(A \vee B)$	$\mathbf{F}A$	$\mathbf{F}B$
$\mathbf{F}(A \rightarrow B)$	$\mathbf{T}A$	$\mathbf{F}B$
$\mathbf{T}\neg A$	$\mathbf{F}A$	$\mathbf{F}A$
$\mathbf{F}\neg A$	$\mathbf{T}A$	$\mathbf{T}A$

Definícia (Jednotný zápis označených formúl typu β)

Označená formula je *typu β* vtt má jeden z tvarov v ľavom stĺpci tabuľky pre nejaké formuly A a B.
Takéto formuly označujeme písmenom β; β_1 označuje príslušnú formulu zo stredného stĺpca a β_2 príslušnú formulu z pravého stĺpca.

β	β_1	β_2
$\mathbf{F}(A \land B)$	$\mathbf{F}A$	$\mathbf{F}B$
$\mathbf{T}(A \lor B)$	$\mathbf{T}A$	$\mathbf{T}B$
$\mathbf{T}(A \to B)$	$\mathbf{F}A$	$\mathbf{T}B$

Definícia (Jednotný zápis označených formúl typu γ)

Označená formula je *typu γ* vtt má jeden z tvarov v ľavom stĺpci tabuľky pre nejakú formulu A a indivíduovú premennú x.
Takéto formuly označujeme $\gamma(x)$ a pre ľubovoľný term t substituovateľný za x v A príslušnú formulu z pravého stĺpca označujeme $\gamma_1(t)$.

$\gamma(x)$	$\gamma_1(t)$
$\mathbf{F}\,\exists x\, A$	$\mathbf{F}A\{x \mapsto t\}$
$\mathbf{T}\,\forall x\, A$	$\mathbf{T}A\{x \mapsto t\}$

Definícia (Jednotný zápis označených formúl typu δ)

Označená formula je *typu δ* vtt má jeden z tvarov v ľavom stĺpci tabuľky pre nejakú formulu A a indivíduovú premennú x.
Takéto formuly označujeme $\delta(x)$ a pre ľubovoľnú premennú y substituovateľnú za x v A príslušnú formulu z pravého stĺpca označujeme $\delta_1(y)$.

$\delta(x)$	$\delta_1(y)$
$\mathbf{T}\,\exists x\, A$	$\mathbf{T}A\{x \mapsto y\}$
$\mathbf{F}\,\forall x\, A$	$\mathbf{F}A\{x \mapsto y\}$

Pravidlá rovnosti: Leibnitzovo pravidlo

Definícia 11.2

Analytické tablo pre množinu označených formúl S^+ (skr. *tablo pre S^+*) je binárny strom, ktorého vrcholy obsahujú označené formuly a je skonštruovaný induktívne podľa nasledovných pravidiel:

- Strom s jediným vrcholom (koreňom) obsahujúcim niektorú označenú formulu A^+ z S^+ je tablom pre S^+.
- Nech $\mathcal{T}$ je tablo pre S^+ a ℓ je nejaký jeho list. Potom tablom pre S^+ je aj každé *priame rozšírenie* $\mathcal{T}$ ktorýmkoľvek z pravidiel:

  S^+: Ako jediné dieťa ℓ pripojíme nový vrchol obsahujúci ľubovoľnú označenú formulu $A^+ \in S^+$.

  α: Ak sa na vetve π_ℓ (ceste z koreňa do ℓ) vyskytuje nejaká označená formula α, tak ako jediné dieťa ℓ pripojíme nový vrchol obsahujúci α_1 alebo α_2.

  β: Ak sa na vetve π_ℓ vyskytuje nejaká označená formula β, tak ako deti ℓ pripojíme dva nové vrcholy, pričom ľavé dieťa bude obsahovať β_1 a pravé β_2.

Definícia 11.2 (pokračovanie)

γ: Ak sa na vetve π_ℓ vyskytuje nejaká označená formula $\gamma(x)$, tak ako jediné dieťa ℓ pripojíme nový vrchol obsahujúci $\gamma_1(t)$ pre ľubovoľný term t substituovateľný za x v $\gamma_1(x)$.

δ: Ak sa na vetve π_ℓ vyskytuje nejaká označená formula $\delta(x)$, tak ako jediné dieťa ℓ pripojíme nový vrchol obsahujúci $\delta_1(y)$ pre ľubovoľnú premennú y, ktorá je substitovateľná za x v $\delta_1(x)$ a nemá voľný výskyt v žiadnej formule na vetve π_ℓ.

L: Ak sa na vetve π_ℓ vyskytuje $\mathbf{T}\, t_1 \doteq t_2$ pre nejaké termy t_1 a t_2 a označená formula $A^+\{x \mapsto t_1\}$ pre nejakú A^+, v ktorej sú t_1 a t_2 substituovateľné za x, tak ako jediné dieťa ℓ pripojíme nový vrchol obsahujúci $A^+\{x \mapsto t_2\}$.

R: Ako jediné dieťa ℓ pripojíme nový vrchol obsahujúci označenú formulu $\mathbf{T}\, t \doteq t$ pre ľubovoľný term t.

Definícia 5.14

Vetvou tabla $\mathcal{T}$ je každá cesta od koreňa $\mathcal{T}$ k niektorému listu $\mathcal{T}$.

Označená formula X^+ sa *vyskytuje na vetve* π v $\mathcal{T}$
vtt X^+ sa nachádza v niektorom vrchole na π.
Skrátene to budeme zapisovať $X^+ \in \mathrm{formulas}(\pi)$.

Definícia 5.15

Vetva π tabla $\mathcal{T}$ je *uzavretá* vtt na π sa súčasne vyskytujú označené formuly $\mathbf{F}X$ a $\mathbf{T}X$ pre nejakú formulu X.
Inak je π *otvorená*.

Tablo $\mathcal{T}$ je uzavreté vtt *každá* jeho vetva je uzavretá.
Naopak, $\mathcal{T}$ je *otvorené* vtt *aspoň jedna* jeho vetva je otvorená.

Veta 5.17 (Korektnosť tablového kalkulu)

Nech S^+ je množina označených formúl a $\mathcal{T}$ je uzavreté tablo pre S^+.
Potom je množina S^+ nesplniteľná.

Veta 11.3 (Korektnosť tablového kalkulu)

Nech S^+ je množina označených formúl.
Ak existuje uzavreté tablo $\mathcal{T}$ pre S^+, tak je množina S^+ nesplniteľná.

Dôkaz vety o korektnosti 5.16.

Nech S^+ je množina označených formúl a $\mathcal{T}$ je uzavreté tablo pre S^+.
Sporom: Predpokladajme, že existuje ohodnotenie, v ktorom je S^+ pravdivá. Označme ho v.
Potom podľa lemy K2 je vo v pravdivé tablo $\mathcal{T}$, teda vo v je pravdivá niektorá vetva π v $\mathcal{T}$.
Pretože $\mathcal{T}$ je uzavreté, aj vetva π je uzavretá. Na π sa teda nachádzajú označené formuly $\mathbf{T}\,X$ a $\mathbf{F}\,X$ pre nejakú formulu X.
Pretože π je pravdivá vo v, musia byť vo v pravdivé všetky formuly na nej. Ale $v \models_{\mathrm{p}} \mathbf{T}\,X$ vtt $v \models_{\mathrm{p}} X$ a $v \models_{\mathrm{p}} \mathbf{F}\,X$ vtt $v \not\models_{\mathrm{p}} X$.
Teda $\mathbf{T}\,X$ a $\mathbf{F}\,X$ nemôžu byť obe pravdivé, čo je spor. □

Definícia 5.19

Nech S^+ je množina označených formúl v jazyku $\mathcal{L}$, nech $\mathcal{T}$ je tablo pre S^+, nech π je vetva tabla $\mathcal{T}$ a nech v je výrokovologické ohodnotenie pre $\mathcal{L}$. Potom:

- *vetva π je pravdivá vo v* ($v \models_{\mathrm{p}} \pi$) vtt vo v sú pravdivé **všetky** označené formuly vyskytujúce sa na vetve π.
- *tablo $\mathcal{T}$ je pravdivé vo v* ($v \models_{\mathrm{p}} \mathcal{T}$) vtt **niektorá** vetva v table $\mathcal{T}$ je pravdivá.

Definícia 5.23 (Úplná vetva a úplné tablo)

Nech S^+ je množina označených formúl a $\mathcal{T}$ je tablo pre S^+.

Vetva π v table $\mathcal{T}$ *je úplná* vtt má všetky nasledujúce vlastnosti:

- pre každú označenú formulu α, ktorá sa vyskytuje na π, sa obidve označené formuly α_1 a α_2 vyskytujú na π;
- pre každú označenú formulu β, ktorá sa vyskytuje na π, sa aspoň jedna z označených formúl β_1, β_2 vyskytuje na π;
- každá $X^+ \in S^+$ sa vyskytuje na π.

Tablo $\mathcal{T}$ je úplné vtt každá jeho vetva je buď úplná alebo uzavretá.

Lema 5.24 (o existencii úplného tabla)

Nech S^+ je konečná množina označených formúl. Potom existuje úplné tablo pre S^+.

Veta 5.28 (o úplnosti tablového kalkulu [Smullyan, 1979])

Nech S^+ je konečná nesplniteľná množina označených formúl. Potom existuje uzavreté tablo pre S^+.

Dôkaz vety o úplnosti.

Zoberme ľubovoľnú konečnú nesplniteľnú množinu označených formúl S^+.

Podľa lemy o existencii úplného tabla vieme pre S^+ nájsť úplné tablo $\mathcal{T}$, teda také, že každá vetva je buď *uzavretá* alebo *úplná*.

Ak by niektorá vetva bola otvorená, potom musí byť úplná, a teda nadol nasýtená. Podľa Hintikkovej lemy by bola splniteľná. Pretože obsahuje všetky formuly z S^+, bola by aj S^+ splniteľná, čo je spor s nesplniteľnosťou S^+.

Preto musia byť všetky vetvy tabla $\mathcal{T}$ uzavreté. $\square$

Definícia 5.33 (Vzor tablového pravidla)

Nech $n \geq 0$ a $k > 0$ sú prirodzené čísla, nech $P_1^+, \ldots, P_n^+$, $C_1^+, \ldots, C_k^+$ sú označené formuly.

Dvojicu tvorenú n-ticou $(P_1^+, \ldots, P_n^+)$ a k-ticou $(C_1^+, \ldots, C_k^+)$ a zapisovanú

$$\frac{P_1^+ \quad \cdots \quad P_n^+}{C_1^+ \;\middle|\; \cdots \;\middle|\; C_k^+}$$

nazývame *vzorom tablového pravidla*.

Označené formuly $P_1^+, \ldots, P_n^+$ nazývame *vzory premís*, označené formuly $C_1^+, \ldots, C_k^+$ nazývame *vzory záverov*.

Definícia 5.35 (Tablové pravidlo a jeho korektnosť)

Tablové pravidlo R je *korektné* vtt
pre každú inštanciu pravidla R

$$\frac{P_1^+ \quad \cdots \quad P_n^+}{C_1^+ \;\middle|\; \cdots \;\middle|\; C_k^+}$$

a pre každé ohodnotenie v platí, že
ak sú vo v pravdivé všetky premisy $P_1^+, \ldots, P_n^+$,
tak je vo v pravdivý niektorý záver $C_1^+, \ldots, C_k^+$.

3 Tablový kalkul pre logiku prvého rádu a jeho korektnosť

Aký je rozdiel od otázky 2?

4 SAT solvery, algoritmus CDDL, rezolvencia vo výrokovej logike

Prednáška 7

Definícia 5.1 (Problém SAT)

Problémom výrokovologickej splniteľnosti (*SAT*) je problém určenia toho, či je daná množina výrokovologických formúl splniteľná.

- Zvyčajne sa redukuje na problém splniteľnosti klauzálnej teórie (teda formuly v CNF).
- *SAT solver* je program, ktorý rieši problém SAT.

Praktické využitie:

- verifikácia hardvéru (Intel i7)
- verifikácia softvéru (Windows 7 device drivers)
- manažment softvérových závislostí (Eclipse plugins, Python Conda)
- konfigurácia produktov (Daimler)
- bioinformatika, kryptológia
- expertné systémy, letová kontrola, rozvrhovanie, …

- zložitosť algoritmu — počet krokov výpočtu ako funkcia veľkosti vstupu n (nezávisí od hardvéru)
- zložitosť problému — zložitosť optimálneho algoritmu riešiaceho daný problém; je známa len veľmi výnimočne, napr. triedenie porovnávaním je $O(n \log n)$
- zložitosť porovnávame za predpokladu n idúceho do nekonečna

DPLL:

Algoritmus 5.8 (Davis and Putnam [1960], Davis et al. [1962])

def DPLL(Φ, v)**:**
    if Φ obsahuje prázdnu klauzulu**:**
        return False
    if v ohodnocuje všetky atómy**:**
        return True
    while existuje jednotková (unit) klauzula ℓ vo Φ**:**
        $\Phi, v =$ unit-propagate(ℓ, Φ, v)
    while existuje nezmiešaný (pure) literál ℓ vo Φ**:**
        $\Phi, v =$ pure-literal-assign(ℓ, Φ, v)
    $x =$ choose-branch-atom(Φ, v)
    return DPLL($\Phi|_{x \mapsto t}, v(x \mapsto t)$) **or** DPLL($\Phi|_{x \mapsto f}, v(x \mapsto f)$)

5 Normálne formy formúl vo výrokovej logike, transformácia do CNF, veta o dedukcii, veta o kompaktnosti pre výrokovú logiku

Neviem čo je normálna forma formuly, CNF je v prednáške 12 veta o dedukcii a kompaktnosti neviem kde je

6 Normálne formy formúl v logike prvého rádu, skolemizácia, rezolvencia v prvorádovej logike

Rezolvencia:

Definícia 14.1

Rezolvenčný princíp (*rezolvencia*, angl. *resolution principle*) je pravidlo

$$\frac{(K_1 \lor \cdots \lor A \lor \cdots \lor K_m) \qquad (L_1 \lor \cdots \lor \neg A \lor \cdots \lor L_n)}{(K_1 \lor \cdots \lor K_m \lor L_1 \lor \cdots \lor L_n)}$$

pre ľubovoľný atóm A a ľub. literály $K_1, \ldots, K_m, L_1, \ldots, L_n$.

Klauzulu $(K_1 \lor \cdots \lor K_m \lor L_1 \lor \cdots \lor L_n)$ nazývame *rezolventou* klauzúl $(K_1 \lor \cdots \lor A \lor \cdots \lor K_m)$ a $(L_1 \lor \cdots \lor \neg A \lor \cdots \lor L_n)$.

Tvrdenie 14.2

Rezolvencia je korektné pravidlo. (Rezolventa je pravdivá v každom ohodnotení, v ktorom sú pravdivé pôvodné klauzuly.)

Definícia 14.4

Výrokovologické rezolvenčné odvodenie z množiny klauzúl S je každá (aj nekonečná) postupnosť klauzúl $C_1, C_2, \dots, C_n, \dots$, ktorej každý člen C_i je:

- prvkom S alebo
- rezolventou dvoch predchádzajúcich klauzúl C_j a C_k pre $j < i$ a $k < i$, alebo
- záverom pravidla idempotencie pre nejakú predchádzajúcu klauzulu C_j, $j < i$.

Zamietnutím (angl. *refutation*) množiny klauzúl S je konečné rezolvenčné odvodenie, ktorého posledným prvkom je prázdna klauzula $\square$.

Veta 14.8 (Korektnosť a úplnosť rezolvencie)

Nech S je klauzálna teória.
S je výrokovologicky nesplniteľná vtt existuje zamietnutie S.

Radšej pozrieť celú prednášku 12