Výrokovologické vyplývanie, sémantické vlastnosti formúl a ekvivalencia

3. prednáška
Logika pre informatikov a Úvod do matematickej logiky

Ján Kľuka, Ján Mazák, Jozef Šiška

Letný semester 2024/2025

Univerzita Komenského v Bratislave
Fakulta matematiky, fyziky a informatiky

Obsah 3. prednášky

- Výrokovologické vyplývanie
  - Výrokovologické teórie a modely
  - Vyplývanie, nezávislosť a nesplniteľnosť
- Sémantické vlastnosti a vzťahy formúl
  - Tautológie, splniteľné, falzifikovateľné a nesplniteľné formuly
  - Hľadanie ohodnotení
  - Ekvivalencia
  - Vzťah tautológií, vyplývania a ekvivalencie
  - Ekvivalentné úpravy a CNF
  - CNF vs. XOR

Rekapitulácia

Minulý týždeň sme hovorili o tom,

- čo sú výrokovologické spojky,
- ako zodpovedajú slovenským spojkám,
- čo sú symboly jazyka výrokovologickej časti logiky prvého rádu,
- čo sú formuly tohto jazyka,
- kedy sú formuly pravdivé v danej štruktúre.
- čo je výrokovologická teória a jej model,
- ako zjednodušíme štruktúry na výrokovologické ohodnotenia.

Výrokovologické vyplývanie

Logické dôsledky

Na 1. prednáške:

- Hovorili sme o tom, že logiku zaujíma,
  čo a prečo sú zákonitosti správneho usudzovania.
- Správne úsudky odvodzujú z predpokladov (teórií) závery,
  ktoré sú ich logickými dôsledkami.
- ***Logickými dôsledkami*** teórie sú tvrdenia,
  ktoré sú pravdivé vo **všetkých modeloch** teórie.

Minulý týždeň sme začali pracovať s **výrokovologickou** časťou logiky prvého rádu.

Už vieme, čo sú v nej teórie a modely.

Čo sú logické dôsledky?

Výrokovologické vyplývanie

Výrokovologické teórie a modely

Výrokovologické teórie

Vráťme sa naspäť k teóriám, modelom a vyplývaniu.

Definícia 3.1

Nech $\mathcal{L}$ je jazyk výrokovologickej časti logiky prvého rádu.
Každú množinu výrokovologických formúl jazyka $\mathcal{L}$ budeme nazývať ***výrokovologickou teóriou*** v jazyku $\mathcal{L}$.

Príklad 3.2

Výrokovologickou teóriou je

$$\begin{aligned} T_{\text{party}} = \{ & ((\texttt{príde}(\texttt{Kim}) \lor \texttt{príde}(\texttt{Jim})) \lor \texttt{príde}(\texttt{Sarah})), \\ & (\texttt{príde}(\texttt{Kim}) \to \neg\texttt{príde}(\texttt{Sarah})), \\ & (\texttt{príde}(\texttt{Jim}) \to \texttt{príde}(\texttt{Kim})), \\ & (\texttt{príde}(\texttt{Sarah}) \to \texttt{príde}(\texttt{Jim}))\}, \end{aligned}$$

ale nie

$$T_{\text{party}} \cup \{\texttt{Kim} \doteq \texttt{Sarah}\}.$$

Príklad výrokovologického modelu

Príklad 3.3 (Výrokovologický model teórie o party)

$$v = \{\texttt{príde(Kim)} \mapsto t, \texttt{príde(Jim)} \mapsto t, \texttt{príde(Sarah)} \mapsto f\}$$

$$\left.\begin{aligned}
&v \models_p ((\texttt{príde(Kim)} \lor \texttt{príde(Jim)}) \lor \texttt{príde(Sarah)})\\
&v \models_p (\texttt{príde(Kim)} \to \neg\texttt{príde(Sarah)})\\
&v \models_p (\texttt{príde(Jim)} \to \texttt{príde(Kim)})\\
&v \models_p (\texttt{príde(Sarah)} \to \texttt{príde(Jim)})
\end{aligned}\right\} v \models_p T_{\text{party}}$$

Výrokovologický model

Definícia 3.4 (Výrokovologický model)

Nech $\mathcal{L}$ je jazyk výrokovologickej časti logiky prvého rádu a nech T je teória v jazyku $\mathcal{L}$ a v je výrokovologické ohodnotenie pre jazyk $\mathcal{L}$.

Teória T je ***pravdivá*** v ohodnotení v, skrátene $v \models_{\mathrm{p}} T$, vtt **každá** formula X z T je pravdivá vo v (teda $v \models_{\mathrm{p}} X$ pre každú $X \in T$).

Hovoríme tiež, že v je ***výrokovologickým modelom*** T.

Teória T je ***nepravdivá*** vo v, skrátene $v \not\models_{\mathrm{p}} T$, vtt T nie je pravdivá vo v.

Zrejme $v \not\models_{\mathrm{p}} T$ vtt $v \not\models_{\mathrm{p}} X$ pre **nejakú** $X \in T$.

Model teórie, splniteľnosť a nesplniteľnosť

Definícia 3.5 (Splniteľnosť a nesplniteľnosť)

Teória je *výrokovologicky splniteľná* vtt
má aspoň jeden výrokovologický model.

Teória je *výrokovologicky nesplniteľná* vtt
nemá žiaden výrokovologický model.

Zrejme teória nie je splniteľná vtt keď je nesplniteľná.

Príklad 3.6

T_{party} je evidentne splniteľná.

Výrokovologické vyplývanie

Vyplývanie, nezávislosť a nesplniteľnosť

Výrokovologické vyplývanie

Ak sú množiny konštánt a predikátových symbolov jazyka konečné, jazyk má konečne veľa predikátových atómov a teda aj **konečne veľa** ohodnotení.

Uvažovať o všetkých ohodnoteniach a modeloch teórie nie je také odstrašujúce. Napríklad si ľahšie predstavíme logický dôsledok:

Definícia 3.7

Nech $\mathcal{L}$ je jazyk výrokovologickej časti logiky prvého rádu a nech T je výrokovologická teória a X je výrokovologická formula, obe v jazyku $\mathcal{L}$.

Formula X je ***výrokovologickým dôsledkom*** teórie T vtt
pre každé ohodnotenie v pre jazyk $\mathcal{L}$ platí, že ak $v \models_{\mathrm{p}} T$, tak $v \models_{\mathrm{p}} X$.

Hovoríme tiež, že X ***vyplýva*** z T a píšeme $T \models_{\mathrm{p}} X$.

Ak X **ne**vyplýva z T, píšeme $T \not\models_{\mathrm{p}} X$.

Príklad výrokovologického vyplývania

Príklad 3.8

Vyplýva `príde(Kim)` výrokovologicky z T_{party}?
Pretože vieme vymenovať všetky ohodnotenia pre $\mathcal{L}_{\text{party}}$, zistíme to ľahko:

	v_i			$((\mathtt{p(K)} \lor \mathtt{p(J)})$	$(\mathtt{p(K)} \to$	$(\mathtt{p(J)} \to$	$(\mathtt{p(S)} \to$		
	$\mathtt{p(K)}$	$\mathtt{p(J)}$	$\mathtt{p(S)}$	$\lor\, \mathtt{p(S)})$	$\neg\mathtt{p(S)})$	$\mathtt{p(K)})$	$\mathtt{p(J)})$	T_{party}	$\mathtt{p(K)}$
v_0	f	f	f	$\not\models_p$				$\not\models_p$	
v_1	f	f	t	$\models_p$	$\models_p$	$\models_p$	$\not\models_p$	$\not\models_p$	
v_2	f	t	f	$\models_p$	$\models_p$	$\not\models_p$		$\not\models_p$	
v_3	f	t	t	$\models_p$	$\models_p$	$\not\models_p$		$\not\models_p$	
v_4	t	f	f	$\models_p$	$\models_p$	$\models_p$	$\models_p$	$\models_p$	$\models_p$
v_5	t	f	t	$\models_p$	$\not\models_p$			$\not\models_p$	
v_6	t	t	f	$\models_p$	$\models_p$	$\models_p$	$\models_p$	$\models_p$	$\models_p$
v_7	t	t	t	$\models_p$	$\not\models_p$			$\not\models_p$	

Skrátili sme `príde` na `p`, `Kim` na `K`, `Jim` na `J`, `Sarah` na `S`.

Logický záver: Formula `príde(Kim)` výrokovologicky vyplýva z T_{party}.

Praktický záver: Aby boli všetky požiadavky splnené, Kim **musí** prísť na párty.

Príklad nezávislosti

Príklad 3.9

Vyplýva $\texttt{príde(Jim)}$ výrokovologicky z T_{party}?

	v_i			$((\mathrm{p(K)} \lor \mathrm{p(J)}) \lor \mathrm{p(S)})$	$(\mathrm{p(K)} \to \neg\mathrm{p(S)})$	$(\mathrm{p(J)} \to \mathrm{p(K)})$	$(\mathrm{p(S)} \to \mathrm{p(J)})$	T_{party}	$\mathrm{p(J)}$
	p(K)	p(J)	p(S)						
v_0	f	f	f	$\not\models_{\mathrm{p}}$				$\not\models_{\mathrm{p}}$	
v_1	f	f	t	$\models_{\mathrm{p}}$	$\models_{\mathrm{p}}$	$\models_{\mathrm{p}}$	$\not\models_{\mathrm{p}}$	$\not\models_{\mathrm{p}}$	
v_2	f	t	f	$\models_{\mathrm{p}}$	$\models_{\mathrm{p}}$	$\not\models_{\mathrm{p}}$		$\not\models_{\mathrm{p}}$	
v_3	f	t	t	$\models_{\mathrm{p}}$	$\models_{\mathrm{p}}$	$\not\models_{\mathrm{p}}$		$\not\models_{\mathrm{p}}$	
v_4	t	f	f	$\models_{\mathrm{p}}$	$\models_{\mathrm{p}}$	$\models_{\mathrm{p}}$	$\models_{\mathrm{p}}$	$\models_{\mathrm{p}}$	$\not\models_{\mathrm{p}}$
v_5	t	f	t	$\models_{\mathrm{p}}$	$\not\models_{\mathrm{p}}$			$\not\models_{\mathrm{p}}$	
v_6	t	t	f	$\models_{\mathrm{p}}$	$\models_{\mathrm{p}}$	$\models_{\mathrm{p}}$	$\models_{\mathrm{p}}$	$\models_{\mathrm{p}}$	$\models_{\mathrm{p}}$
v_7	t	t	t	$\models_{\mathrm{p}}$	$\not\models_{\mathrm{p}}$			$\not\models_{\mathrm{p}}$	

Logický záver: Formula $\texttt{príde(Jim)}$ **nevyplýva** z T_{party}.

Výrokovologická nezávislosť

Vzťahu medzi $\texttt{príde}(\texttt{Jim})$ a T_{party} hovoríme nezávislosť.

Definícia 3.10

Nech $\mathcal{L}$ je jazyk výrokovologickej časti logiky prvého rádu a nech T je výrokovologická teória a X je výrokovologická formula, obe v jazyku $\mathcal{L}$.

Formula X je ***výrokovologicky nezávislá*** od teórie T vtt existujú také ohodnotenia v_0 a v_1 pre jazyk $\mathcal{L}$, že $v_0 \models_{\mathrm{p}} T$ aj $v_1 \models_{\mathrm{p}} T$, ale $v_0 \not\models_{\mathrm{p}} X$ a $v_1 \models_{\mathrm{p}} X$.

Príklad 3.11 (pokračovanie príkladu 3.9)

Logický záver: Formula $\texttt{príde}(\texttt{Jim})$ je nezávislá od T_{party}.

Praktický záver: Všetky požiadavky budú naplnené bez ohľadu na to, či Jim príde alebo nepríde na párty. Nie je nutné, aby bol prítomný ani aby bol neprítomný. Môže, ale nemusí prísť. Jeho prítomnosť od požiadaviek nezávisí.

Príklad vyplývania negácie

Príklad 3.12

Je $\texttt{príde}(\texttt{Sarah})$ výrokovologickým dôsledkom T_{party} alebo nezávislá od T_{party}?

	v_i			$((\texttt{p(K)} \lor \texttt{p(J)}) \lor \texttt{p(S)})$	$(\texttt{p(K)} \to \neg\texttt{p(S)})$	$(\texttt{p(J)} \to \texttt{p(K)})$	$(\texttt{p(S)} \to \texttt{p(J)})$	T_{party}	$\texttt{p(S)}$
	$\texttt{p(K)}$	$\texttt{p(J)}$	$\texttt{p(S)}$						
v_0	f	f	f	$\not\models_p$				$\not\models_p$	
v_1	f	f	t	$\models_p$	$\models_p$	$\models_p$	$\not\models_p$	$\not\models_p$	
v_2	f	t	f	$\models_p$	$\models_p$	$\not\models_p$		$\not\models_p$	
v_3	f	t	t	$\models_p$	$\models_p$	$\not\models_p$		$\not\models_p$	
v_4	t	f	f	$\models_p$	$\models_p$	$\models_p$	$\models_p$	$\models_p$	$\not\models_p$
v_5	t	f	t	$\models_p$	$\not\models_p$			$\not\models_p$	
v_6	t	t	f	$\models_p$	$\models_p$	$\models_p$	$\models_p$	$\models_p$	$\not\models_p$
v_7	t	t	t	$\models_p$	$\not\models_p$			$\not\models_p$	

Logický záver: Formula $\texttt{príde}(\texttt{Sarah})$ **nevyplýva** z T_{party}, ale ani **nie je nezávislá** od T_{party}.

Vyplývanie negácie

Tvrdenie 3.13

Nech $\mathcal{L}$ je jazyk výrokovologickej časti logiky prvého rádu a nech T je splniteľná výrokovologická teória a X je výrokovologická formula, obe v jazyku $\mathcal{L}$.

Formula X nevyplýva z teórie T a nie je výrokovologicky nezávislá od T vtt $\neg X$ vyplýva z T.

Príklad 3.14 (pokračovanie príkladu 3.12)

Logický záver: Z T_{party} vyplýva $\neg\mathtt{príde}(\mathtt{Sarah})$.

Praktický záver: Aby boli všetky požiadavky naplnené, Sarah **nesmie** prísť na party.

Vzťahy teórií a formúl

Medzi ohodnotením a formulou sú iba dva vzájomne výlučné vzťahy:

$$\text{Buď } v \models_p X, \text{ alebo } v \not\models_p X.$$

Medzi teóriou a formulou je viac možných vzťahov:

	existuje v také, že $v \models_p T$ a $v \models_p X$	pre všetky v, ak $v \models_p T$, tak $v \not\models_p X$
existuje v také, že $v \models_p T$ a $v \not\models_p X$	X je nezávislá od T $T \not\models_p X$ a $T \not\models_p \neg X$	$T \models_p \neg X$
pre všetky v, ak $v \models_p T$, tak $v \models_p X$	$T \models_p X$	

Vzťahy teórií a formúl

Medzi **ohodnotením a formulou** sú iba **dva vzájomne výlučné** vzťahy:

Buď $v \models_{p} X$, alebo $v \not\models_{p} X$.

Medzi **teóriou a formulou** je **viac** možných vzťahov:

	existuje v také, že $v \models_{p} T$ a $v \models_{p} X$	pre všetky v, ak $v \models_{p} T$, tak $v \not\models_{p} X$
existuje v také, že $v \models_{p} T$ a $v \not\models_{p} X$	X je nezávislá od T $T \not\models_{p} X$ a $T \not\models_{p} \neg X$	$T \models_{p} \neg X$ a $T \not\models_{p} X$
pre všetky v, ak $v \models_{p} T$, tak $v \models_{p} X$	$T \models_{p} X$	

Vzťahy teórií a formúl

Medzi ohodnotením a formulou sú iba dva vzájomne výlučné vzťahy:

Buď $v \models_p X$, alebo $v \not\models_p X$.

Medzi teóriou a formulou je viac možných vzťahov:

	existuje v také, že $v \models_p T$ a $v \models_p X$	pre všetky v, ak $v \models_p T$, tak $v \not\models_p X$
existuje v také, že $v \models_p T$ a $v \not\models_p X$	X je nezávislá od T $T \not\models_p X$ a $T \not\models_p \neg X$	$T \models_p \neg X$ a $T \not\models_p X$
pre všetky v, ak $v \models_p T$, tak $v \models_p X$	$T \models_p X$ a $T \not\models_p \neg X$	

Vzťahy teórií a formúl

Medzi **ohodnotením a formulou** sú iba **dva vzájomne výlučné** vzťahy:

$$\text{Buď } v \models_p X, \text{ alebo } v \not\models_p X.$$

Medzi **teóriou a formulou** je **viac** možných vzťahov:

	existuje v také, že $v \models_p T$ a $v \models_p X$	pre všetky v, ak $v \models_p T$, tak $v \not\models_p X$
existuje v také, že $v \models_p T$ a $v \not\models_p X$	X je nezávislá od T $T \not\models_p X$ a $T \not\models_p \neg X$	$T \models_p \neg X$ a $T \not\models_p X$
pre všetky v, ak $v \models_p T$, tak $v \models_p X$	$T \models_p X$ a $T \not\models_p \neg X$	T je **nesplniteľná** $T \models_p X$ aj $T \models_p \neg X$

Nesplniteľná teória

Príklad 3.15

Je teória $T'_{\text{party}} = T_{\text{party}} \cup \{(\neg\mathtt{príde(Sarah)} \to \neg\mathtt{príde(Kim)})\}$ splniteľná?

	v_i			$((\mathtt{p(K)} \lor \mathtt{p(J)}) \lor \mathtt{p(S)})$	$(\mathtt{p(K)} \to \neg\mathtt{p(S)})$	$(\mathtt{p(J)} \to \mathtt{p(K)})$	$(\mathtt{p(S)} \to \mathtt{p(J)})$	$(\neg\mathtt{p(S)} \to \neg\mathtt{p(K)})$	T'_{party}
	$\mathtt{p(K)}$	$\mathtt{p(J)}$	$\mathtt{p(S)}$						
v_0	f	f	f	$\not\models_{\mathrm{p}}$					$\not\models_{\mathrm{p}}$
v_1	f	f	t	$\models_{\mathrm{p}}$	$\models_{\mathrm{p}}$	$\models_{\mathrm{p}}$	$\not\models_{\mathrm{p}}$		$\not\models_{\mathrm{p}}$
v_2	f	t	f	$\models_{\mathrm{p}}$	$\models_{\mathrm{p}}$	$\not\models_{\mathrm{p}}$			$\not\models_{\mathrm{p}}$
v_3	f	t	t	$\models_{\mathrm{p}}$	$\models_{\mathrm{p}}$	$\not\models_{\mathrm{p}}$			$\not\models_{\mathrm{p}}$
v_4	t	f	f	$\models_{\mathrm{p}}$	$\models_{\mathrm{p}}$	$\models_{\mathrm{p}}$	$\models_{\mathrm{p}}$	$\not\models_{\mathrm{p}}$	$\not\models_{\mathrm{p}}$
v_5	t	f	t	$\models_{\mathrm{p}}$	$\not\models_{\mathrm{p}}$				$\not\models_{\mathrm{p}}$
v_6	t	t	f	$\models_{\mathrm{p}}$	$\models_{\mathrm{p}}$	$\models_{\mathrm{p}}$	$\models_{\mathrm{p}}$	$\not\models_{\mathrm{p}}$	$\not\models_{\mathrm{p}}$
v_7	t	t	t	$\models_{\mathrm{p}}$	$\not\models_{\mathrm{p}}$				$\not\models_{\mathrm{p}}$

Logický záver: T'_{party} je nesplniteľná, vyplýva z nej každá formula.

Praktický záver: T'_{party} **nemá** praktické dôsledky, lebo **nevypovedá o žiadnom stave sveta**. Na jej základe **nevieme rozhodnúť**, kto musí alebo nesmie prísť na párty.

Vyplývanie a nesplniteľnosť

Nesplniteľnosť ale nie je neužitočná vlastnosť.

Tvrdenie 3.16

Nech $\mathcal{L}$ je jazyk výrokovologickej časti logiky prvého rádu a nech T je splniteľná výrokovologická teória a X je výrokovologická formula, obe v jazyku $\mathcal{L}$.

Formula X výrokovologicky vyplýva z teórie T vtt $T \cup \{\neg X\}$ je výrokovologicky nesplniteľná.

Podľa tohto tvrdenia sa rozhodnutie vyplývania dá zredukovať na rozhodnutie splniteľnosti.

Výrokovologickú splniteľnosť rozhoduje SAT solver.

Množina atómov formuly a teórie

Definícia 3.17

Množinu atómov $\mathrm{atoms}(X)$ formuly $X \in \mathcal{E}_{\mathcal{L}}$ definujeme pre všetky formuly $A, B \in \mathcal{E}_{\mathcal{L}}$ nasledovne:

- $\mathrm{atoms}(A) = \{A\}$, ak A je atóm,
- $\mathrm{atoms}(\neg A) = \mathrm{atoms}(A)$,
- $\mathrm{atoms}((A \land B)) = \mathrm{atoms}((A \lor B)) = \mathrm{atoms}((A \to B)) = \mathrm{atoms}(A) \cup \mathrm{atoms}(B)$.

Množinou atómov teórie T je

$$\mathrm{atoms}(T) = \bigcup_{X \in T} \mathrm{atoms}(X).$$

Ohodnotenia zhodné na atómoch teórie

Definícia 3.18

Nech $\mathcal{L}$ je jazyk výrokovologickej časti logiky prvého rádu, nech $M \subseteq \mathcal{PA}_{\mathcal{L}}$. Ohodnotenia v_1 a v_2 sa ***zhodujú*** na množine M vtt $v_1(A) = v_2(A)$ pre každý atóm $A \in M$.

Tvrdenie 3.19

Nech $\mathcal{L}$ je jazyk výrokovologickej časti logiky prvého rádu.
Pre každú výrokovologickú teóriu T a formulu X jazyka $\mathcal{L}$ a všetky ohodnotenia v_1 a v_2, ktoré zhodujú na množine $\mathrm{atoms}(T) \cup \mathrm{atoms}(X)$ platí

- $v_1 \models_{\mathrm{p}} T$ *vtt* $v_2 \models_{\mathrm{p}} T$,
- $v_1 \models_{\mathrm{p}} X$ *vtt* $v_2 \models_{\mathrm{p}} X$.

Ohodnotenia postačujúce na skúmanie teórií

Inak povedané: Pravdivosť formuly/teórie v ohodnotení závisí iba od pravdivostných hodnôt tých atómov, ktoré sa v nej vyskytujú.

Takže na zistenie vyplývania, nezávislosti, splniteľnosti stačí preskúmať všetky ohodnotenia, ktoré sa líšia na atómoch vyskytujúcich sa vo formule a teórii.

Pokiaľ je teória je konečná, stačí skúmať konečne veľa ohodnotení, aj keby bol jazyk nekonečný.
(A podľa vety o kompaktnosti ak máme nejaký spor v nekonečnej teórii, nájde sa sporná konečná podmnožina.)

Dôkaz indukciou na konštrukciu formuly

(1)	X je výrokovologická formula jazyka $\mathcal{L}$
(2)	v_1 a v_2 sú ohodnotenia zhodné na $\operatorname{atoms}(X)$

$$\Downarrow$$

$$v_1 \models_{\mathrm{p}} X \text{ vtt } v_2 \models_{\mathrm{p}} X$$

Báza: X je atóm.

(3)	X predikátový atóm	podľa 1
(4)	$v_1 \models_{\mathrm{p}} X$ vtt $v_1(X) = t$	def. pravdivosti
(5)	$v_2 \models_{\mathrm{p}} X$ vtt $v_2(X) = t$	def. pravdivosti
(6)	$v_1(X) = v_2(X)$	podľa 2
	$v_1 \models_{\mathrm{p}} X$ vtt $v_2 \models_{\mathrm{p}} X$	podľa 4, 5, 6

Dôkaz indukciou na konštrukciu formuly

(1) Z je výrokovologická formula jazyka $\mathcal{L}$

(2) v_1 a v_2 sú ohodnotenia zhodné na $\mathrm{atoms}(Z)$

$$\Downarrow$$

$$v_1 \models_{\mathrm{p}} Z \text{ vtt } v_2 \models_{\mathrm{p}} Z$$

Ind. krok pre $\neg$: Formula v tvare $Z = \neg X$.

(IP)	Tvrdenie platí pre X	
(3)	v_1, v_2 sa zhodujú na $\mathrm{atoms}(X)$	2, $\mathrm{atoms}(\neg X) = \mathrm{atoms}(X)$
(4)	$v_1 \models_{\mathrm{p}} X$ vtt $v_2 \models_{\mathrm{p}} X$	3, IP pre Z = X
(5)	$v_1 \models_{\mathrm{p}} \neg X$ vtt $v_1 \not\models_{\mathrm{p}} X$	def. $\models_{\mathrm{p}}$
(6)	$v_2 \models_{\mathrm{p}} \neg X$ vtt $v_2 \not\models_{\mathrm{p}} X$	def. $\models_{\mathrm{p}}$
(7)	$v_1 \not\models_{\mathrm{p}} X$ vtt $v_2 \not\models_{\mathrm{p}} X$	4, def. $\not\models_{\mathrm{p}}$
	$v_1 \models_{\mathrm{p}} \neg X$ vtt $v_2 \models_{\mathrm{p}} \neg X$	5, 6, 7

Dôkaz indukciou na konštrukciu formuly

(1) Z je výrokovologická formula jazyka $\mathcal{L}$

(2) v_1 a v_2 sú ohodnotenia zhodné na $\mathrm{atoms}(Z)$

$$\Downarrow$$

$$v_1 \models_p Z \text{ vtt } v_2 \models_p Z$$

Ind. krok pre $\land$: Formula v tvare $Z = (X \land Y)$.

(IP)	Tvrdenie platí pre X aj pre Y	
(3)	$\mathrm{atoms}((X \land Y)) = \mathrm{atoms}(X) \cup \mathrm{atoms}(Y)$	def. atoms
(4)	v_1, v_2 sa zhodujú na $\mathrm{atoms}(X)$	2, 3
(5)	$v_1 \models_p X$ vtt $v_2 \models_p X$	4, IP pre Z = X
(6)	v_1, v_2 sa zhodujú na $\mathrm{atoms}(Y)$	2, 3
(7)	$v_1 \models_p Y$ vtt $v_2 \models_p Y$	6, IP pre Z = Y
(8)	$v_1 \models_p (X \land Y)$ vtt $v_1 \models_p X$ a $v_1 \models_p Y$	def. $\models_p$
(9)	$v_2 \models_p (X \land Y)$ vtt $v_2 \models_p X$ a $v_2 \models_p Y$	def. $\models_p$
	$v_1 \models_p (X \land Y)$ vtt $v_2 \models_p (X \land Y)$	5, 7, 8, 9

Dôkaz tvrdenia 3.19 (ešte raz, vo vetách).

Tvrdenie dokážeme indukciou na konštrukciu formuly:

1.1. Ak X je rovnostný atóm, nie je výrokovologickou formulou a tvrdenie preň platí triviálne.

1.2. Nech X je predikátový atóm. Zoberme ľubovoľné ohodnotenia v_1 a v_2, ktoré sa zhodujú na $\mathrm{atoms}(X)$, teda na samotnom X. Podľa definície pravdivosti platí $v_1 \models_p X$ vtt $v_1(X) = t$ vtt $v_2(X) = t$ vtt $v_2 \models_p X$.

2.1 Indukčný predpoklad (IP): Predpokladajme, že tvrdenie platí pre formulu X. Dokážme ho pre $\neg X$. Zoberme ľubovoľné ohodnotenia v_1 a v_2, ktoré sa zhodujú na $\mathrm{atoms}(\neg X)$. Pretože $\mathrm{atoms}(\neg X) = \mathrm{atoms}(X)$, v_1 a v_2 sa zhodujú na $\mathrm{atoms}(X)$, a teda podľa IP $v_1 \models_p X$ vtt $v_2 \models_p X$. Preto $v_1 \models_p \neg X$ vtt (def. $\models_p$) $v_1 \not\models_p X$ vtt (IP) $v_2 \not\models_p X$ vtt (def. $\models_p$) $v_2 \models_p \neg X$.

2.2 Indukčný predpoklad (IP): Predpokladajme, že tvrdenie platí pre formuly X a Y. Dokážme ho pre $(X \land Y)$. Zoberme ľubovoľné ohodnotenia v_1 a v_2, ktoré sa zhodujú na $\mathrm{atoms}((X \land Y))$. Pretože $\mathrm{atoms}((X \land Y)) = \mathrm{atoms}(X) \cup \mathrm{atoms}(Y)$, v_1 a v_2 sa zhodujú na $\mathrm{atoms}(X)$, a teda podľa IP $v_1 \models_p X$ vtt $v_2 \models_p X$; tiež sa zhodujú na $\mathrm{atoms}(Y)$, a teda podľa IP $v_1 \models_p Y$ vtt $v_2 \models_p Y$. Preto $v_1 \models_p (X \land Y)$ vtt (def. $\models_p$) $v_1 \models_p X$ a $v_1 \models_p Y$ vtt (IP) $v_2 \models_p X$ a $v_2 \models_p Y$ vtt (def. $\models_p$) $v_2 \models_p (X \land Y)$.

Podobne postupujeme pre ďalšie binárne spojky. $\square$

Sémantické vlastnosti a vzťahy formúl

Sémantické vlastnosti a vzťahy formúl

Tautológie, splniteľné, falzifikovateľné a nesplniteľné formuly

Logické dôsledky prázdnej teórie

Tvrdenie vyplýva z nejakej teórie (je jej logickým dôsledkom),
keď je pravdivé v každom modeli teórie, teda v každom stave sveta,
v ktorom sú pravdivé všetky tvrdenia teórie.

Čo keď je teória **prázdna**?

- Je pravdivá v **každom** stave sveta.
- Jej logické dôsledky sú teda **tiež** pravdivé v každom stave sveta.

Navyše:

- Každý model hocijakej neprázdnej teórie T
  je aj modelom prázdnej teórie.
- Logické dôsledky prázdnej teórie sú v ňom pravdivé.
- Preto sú aj logickými dôsledkami T.

Logické dôsledky prázdnej teórie sú teda dôsledkami **všetkých** teórií.

Príklady logických dôsledkov prázdnej teórie

Existujú vôbec logické dôsledky prázdnej teórie?

Áno, napríklad:

- pre každú konštantu c je pravdivé tvrdenie $c \doteq c$;
- pre každý atóm A je pravdivé $(A \lor \neg A)$.

Pretože sú pravdivé bez ohľadu na teóriu a sú pravdivé v každom stave sveta, sú logickými pravdami a sú nutne pravdivé.

Rozpoznateľné logické pravdy

Jazyk a spôsob pohľadu na stavy sveta ovplyvňuje, ktoré logické pravdy dokážeme rozpoznať:

- $c \doteq c$ aj $(A \lor \neg A)$ sú pravdivé v každej štruktúre.
- Výrokovologické ohodnotenia sa nezaoberajú rovnostnými atómami. Pomocou nich nezistíme, že $c \doteq c$ je nutne pravda. Ale zistíme, že $(A \lor \neg A)$ pre každý **predikátový** atóm A je pravdivé v každom ohodnotení, a teda je nutne pravdou.

Logickým pravdám, ktorých nutnú pravdivosť dokážeme určiť rozborom všetkých výrokovologických ohodnotení, hovoríme **tautológie**.

Príklad tautológie

Príklad 4.1 (Peirceov zákon)

Majme jazyk $\mathcal{L}$ s $\mathcal{C}_{\mathcal{L}} = \{\mathrm{a}, \mathrm{b}\}$, $\mathcal{P}_{\mathcal{L}} = \{\mathrm{p}^1\}$.
Je formula $X = \big(((\mathrm{p(a)} \to \mathrm{p(b)}) \to \mathrm{p(a)}\big) \to \mathrm{p(a)}\big)$ tautológiou?

Označme $A = \mathrm{p(a)}$ a $B = \mathrm{p(b)}$, teda $X = \big(((A \to B) \to A\big) \to A\big)$
a preskúmajme všetky výrokovologické ohodnotenia týchto atómov:

	v_i				X
	A	B	$(A \to B)$	$((A \to B) \to A)$	$(((A \to B) \to A) \to A)$
v_0	f	f	$\models_{\mathrm{p}}$	$\not\models_{\mathrm{p}}$	$\models_{\mathrm{p}}$
v_1	f	t	$\models_{\mathrm{p}}$	$\not\models_{\mathrm{p}}$	$\models_{\mathrm{p}}$
v_2	t	f	$\not\models_{\mathrm{p}}$	$\models_{\mathrm{p}}$	$\models_{\mathrm{p}}$
v_3	t	t	$\models_{\mathrm{p}}$	$\models_{\mathrm{p}}$	$\models_{\mathrm{p}}$

Pretože X je pravdivá vo všetkých ohodnoteniach pre $\mathcal{L}$, X je tautológiou.

Tautológia

Definícia 4.2

Nech $\mathcal{L}$ je jazyk výrokovologickej časti logiky prvého rádu.
Nech X je výrokovologická formula.
Formulu X nazveme ***tautológiou*** (skrátene $\models_p X$) vtt
X je **pravdivá** v **každom** výrokovologickom ohodnotení v pre $\mathcal{L}$
(teda **pre každé** výrokovologické ohodnotenie v pre $\mathcal{L}$ platí $v \models_p X$).

Definícia vyžaduje preveriť **všetky možné** ohodnotenia, ale podľa 3.19 stačí preverovať **ohodnotenia atómov vyskytujúcich sa vo formule**:

Dôsledok 4.3

Nech $\mathcal{L}$ je jazyk výrokovologickej časti logiky prvého rádu a nech X je výrokovologická formula jazyka $\mathcal{L}$.
Formula X je tautológiou vtt X je pravdivá v každom výrokovologickom ohodnotení $v : \ \mathrm{atoms}(X) \to \{f, t\}$.

	v_i			
	A_1	A_2	$\cdots$	X
v_0	f	f	$\cdots$	$\models_p$
v_1	f	f	$\cdots$	$\models_p$
		$\cdots$		
v_k	t	f	$\cdots$	$\models_p$
		$\cdots$		

Tvrdenie 4.4 (Tautológie, vyplývanie a jeho monotónnosť)

Nech $\mathcal{L}$ je jazyk výrokovologickej časti logiky prvého rádu.
Nech A je výrokovologická formula v $\mathcal{L}$.
Nech T_1 a T_2 sú výrokovologické teórie v $\mathcal{L}$. Potom:

a) $\vDash_{\mathrm{p}} A$ *(A je tautológia) vtt* $\emptyset \vDash_{\mathrm{p}} A$ *(A vyplýva z prázdnej teórie).*

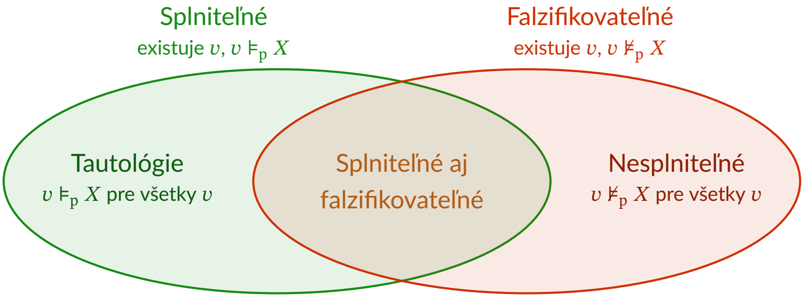
b) $T_1 \vDash_{\mathrm{p}} A$ *a* $T_1 \subseteq T_2$*, tak* $T_2 \vDash_{\mathrm{p}} A$.

c) $\vDash_{\mathrm{p}} A$ *vtt pre každú teóriu* T *v* $\mathcal{L}$*,* $T \vDash_{\mathrm{p}} A$.

Vlastnosti b) hovoríme *monotónnosť*: pridávaním ďalších formúl do teórie nemožno zrušiť platnosť jej dôsledkov.

„Geografia“ formúl podľa pravdivosti vo všetkých ohodnoteniach

Tautológie (vždy pravdivé) a kontradikcie (vždy nepravdivé) sú „výnimočné“ formuly. Väčšina formúl je kdesi medzi týmito extrémami.



Obrázok podľa **?**

Splniteľnosť

Kým tautológie sú nutne pravdivé,
teda pravdivé vo všetkých ohodnoteniach,
mnohé formuly iba môžu byť pravdivé,
teda sú pravdivé v niektorých ohodnoteniach.
Nazývame ich splniteľné.

Definícia 4.5

Nech $\mathcal{L}$ je jazyk výrokovologickej časti logiky prvého rádu.
Nech X je výrokovologická formula.
Formulu X nazveme ***splniteľnou***
vtt X je pravdivá v nejakom výrokovologickom ohodnotení pre $\mathcal{L}$
(teda existuje také výrokovologické ohodnotenie v pre $\mathcal{L}$, že $v \models_p X$).

	v_i			
	A_1	A_2	$\cdots$	X
v_0	f	f	$\cdots$	$\not\models_p$
v_1	f	f	$\cdots$	$\not\models_p$
		$\cdots$		
v_k	t	f	$\cdots$	$\models_p$
		$\cdots$		

Falzifikovateľnosť

Na rozdiel od tautológií, ktoré sú **nutne** pravdivé,
a teda **nemôžu** byť **ne**pravdivé,
mnohé formuly **môžu** byť **ne**pravdivé,
teda sú **ne**pravdivé v **niektorých** ohodnoteniach.
Nazývame ich **falzifikovateľné**.

Definícia 4.6

Nech $\mathcal{L}$ je jazyk výrokovologickej časti logiky prvého rádu.
Nech X je výrokovologická formula.
Formulu X nazveme ***falzifikovateľnou***
vtt X je **nepravdivá** v **nejakom** výrokovologickom ohodnotení pre $\mathcal{L}$
(teda **existuje** také výrokovologické ohodnotenie v pre $\mathcal{L}$, že $v \not\models_{\mathrm{p}} X$).

	v_i			
	A_1	A_2	$\cdots$	X
v_0	f	f	$\cdots$	$\models_{\mathrm{p}}$
v_1	f	f	$\cdots$	$\models_{\mathrm{p}}$
		$\cdots$		
v_k	t	f	$\cdots$	$\not\models_{\mathrm{p}}$
		$\cdots$		

Nesplniteľnosť

Nakoniec, mnohé formuly sú nutne nepravdivé,
teda sú nepravdivé vo všetkých ohodnoteniach.
Nazývame ich nesplniteľné.

Definícia 4.7

Nech $\mathcal{L}$ je jazyk výrokovologickej časti logiky prvého rádu.
Nech X je výrokovologická formula.
Formulu X nazveme *nesplniteľnou*
vtt X je nepravdivá v každom výrokovologickom ohodnotení pre $\mathcal{L}$
(teda pre každé výrokovologické ohodnotenie v pre $\mathcal{L}$, platí $v \not\models_p X$).

	v_i			
	A_1	A_2	$\cdots$	X
v_0	f	f	$\cdots$	$\not\models_p$
v_1	f	f	$\cdots$	$\not\models_p$
		$\cdots$		
v_k	t	f	$\cdots$	$\not\models_p$
		$\cdots$		

Sémantické vlastnosti a vzťahy formúl

Hľadanie ohodnotení

Ohodnotenia pre danú formulu

Ak máme dané ohodnotenie atómov, pravdivosť formuly zistíme indukciou podľa jej štruktúry. Čo však spraviť, ak naopak máme danú formulu a hľadáme ohodnotenia, v ktorých je pravdivá či nepravdivá?

- Ak by sme hľadali všetky štruktúry, nemáme šancu, je ich nekonečne veľa.
- Všetkých vyhovujúcich ohodnotení môže byť exponenciálne veľa (nemôže teda existovať rýchly všeobecný algoritmus).
- Ohodnotenia možno hľadať rozborom všetkých možností pomocou tabuľky, ktorá má v záhlaví vytvárajúcu postupnosť danej formuly a v riadkoch jednotlivé ohodnotenia.
- Mohli by sme lepšie využiť znalosť štruktúry formuly na urýchlenie postupu? Azda áno: $A \land \neg A \land B_1 \land B_2 \land \cdots \land B_{100}$.

Ohodnotenia pre danú formulu

Pre formulu so známou pravdivostnou hodnotou vieme určiť
pravdivosť priamych podformúl.
Napr. ak $A \vee B$ je nepravda, tak A aj B musia byť nepravdivé.

Možností môže byť viac, čo zodpovedá vetveniu.
Napr. pre pravdivú implikáciu $A \to B$ osobitne skúmame situácie,
kde A je nepravdivá, a kde B je pravdivá.

Pri takejto postupnej analýze dostávame čoraz jednoduchšie formuly.
Končíme, keď sa dostaneme k atómom:
ich ohodnotenie presne popisuje, ako má model vyzerať.

Hľadanie ohodnotení

$A \to (\neg A \wedge B) \quad t$

$A \quad f$

$B \quad$ **ľub.**

$\neg A \wedge B \quad t$

$\neg A \quad t$

$B \quad t$

$A \quad f$

Ľavá vetva zodpovedá dvom ohodnoteniam,
pravá jednému (avšak už obsiahnutému v ľavej vetve).

Hľadanie ohodnotení

Môže sa stať, že v niektorej vetve vznikne **spor**
(atóm A má byť zároveň pravdivý aj nepravdivý).
Taká vetva neobsahuje žiadne vyhovujúce ohodnotenie
a netreba sa ňou ďalej zapodievať.

$$A \land B \land (\neg A \lor \neg B) \quad t$$

$$A \quad t$$

$$B \quad t$$

$$\neg A \lor \neg B \quad t$$

$$\neg A \quad t \qquad\qquad \neg B \quad t$$

$$A \quad f \qquad\qquad B \quad f$$

$$* \qquad\qquad *$$

Spor v každej vetve: formula nie je pravdivá v žiadnom ohodnotení.

Hľadanie ohodnotení

$$
\begin{array}{c}
A \wedge \neg A \wedge B_1 \wedge B_2 \wedge \cdots \wedge B_n \quad t \\
| \\
A \quad t \\
\neg A \quad t \\
B_1 \quad t \\
\cdots \\
B_n \quad t \\
| \\
A \quad f \\
*
\end{array}
$$

Tabuľka všetkých možných ohodnotení by mala 2^{n+1} riadkov, pritom táto úvaha je $O(n)$.

Sémantické vlastnosti a vzťahy formúl

Ekvivalencia

Logická ekvivalencia

Dve tvrdenia sú **ekvivalentné**, ak sú v každom stave sveta buď obe pravdivé alebo obe nepravdivé.

Ekvivalentné tvrdenia sú navzájom nahraditeľné. To je výhodné vtedy, keď potrebujeme, aby tvrdenie malo nejaký požadovaný tvar, alebo používalo iba niektoré spojky. Napríklad vstupom pre SAT solver je teória zložená iba z disjunkcií literálov.

Podobne ako pri tautológiách môžeme pomocou skúmania všetkých ohodnotení rozpoznať **niektoré** ekvivalentné tvrdenia zapísané formulami (ale nie všetky, pretože ohodnotenia napríklad nedávajú význam rovnostným atómom).

Príklad výrokovologicky ekvivalentných formúl

Príklad 4.8

V jazyku $\mathcal{L}$ z príkladu 4.1 označme $A = \mathrm{p}(\mathrm{a})$ a $B = \mathrm{p}(\mathrm{b})$.
Sú formuly $X = \neg(A \to \neg B)$ a $Y = (A \land B)$ výrokovologicky ekvivalentné?

Preskúmajme všetky výrokovologické ohodnotenia atómov A a B:

	v_i				X	Y
	A	B	$\neg B$	$(A \to \neg B)$	$\neg(A \to \neg B)$	$(A \land B)$
v_0	f	f	$\models_p$	$\models_p$	$\not\models_p$	$\not\models_p$
v_1	f	t	$\not\models_p$	$\models_p$	$\not\models_p$	$\not\models_p$
v_2	t	f	$\models_p$	$\models_p$	$\not\models_p$	$\not\models_p$
v_3	t	t	$\not\models_p$	$\not\models_p$	$\models_p$	$\models_p$

X je pravdivá **v práve tých** ohodnoteniach pre $\mathcal{L}$, v ktorých je pravdivá Y, preto X a Y sú výrokovologicky ekvivalentné.

Výrokovogická ekvivalencia

Definícia 4.9

Nech $\mathcal{L}$ je jazyk výrokovologickej časti logiky prvého rádu.
Nech X a Y sú výrokovologické formuly jazyka $\mathcal{L}$.
Formuly X a Y sú ***výrokovologicky ekvivalentné***, skrátene $X \Leftrightarrow_{\mathrm{p}} Y$ vtt pre **každé** výrokovologické ohodnotenie v pre jazyk $\mathcal{L}$ platí, že X je pravdivá vo v vtt Y je pravdivá vo v.

$\Leftrightarrow_{\mathrm{p}}$ verzus $\leftrightarrow$

Pozor! Nemýľte si zápis $X \Leftrightarrow_{\mathrm{p}} Y$ s formulou $(X \leftrightarrow Y)$.

- $X \Leftrightarrow_{\mathrm{p}} Y$ je skrátené vyjadrenie vzťahu dvoch formúl podľa definície 4.9. Keď napíšeme $X \Leftrightarrow_{\mathrm{p}} Y$, tvrdíme tým, že X a Y sú výrokovologicky ekvivalentné formuly (alebo sa pýtame, či to tak je).
- $(X \leftrightarrow Y)$ je formula, postupnosť symbolov, ktorá môže byť pravdivá v nejakom ohodnotení a nepravdivá v inom, môže byť splniteľná, tautológia, falzifikovateľná, nesplniteľná, môže vyplývať, či byť nezávislá od nejakej teórie, alebo môže byť výrokovologicky ekvivalentná s inou formulou.

Medzi $X \Leftrightarrow_{\mathrm{p}} Y$ a $(X \leftrightarrow Y)$ je vzťah, ktorý si ozrejmíme neskôr.

Známe ekvivalencie

O mnohých dvojiciach formúl už viete, že sú vzájomne ekvivalentné. Zhrnuli sme ich do nasledujúcej vety.

Veta 4.10

Nech $\mathcal{L}$ je jazyk výrokovologickej časti logiky prvého rádu.
Nech A, B a C sú ľubovoľné výrokovologické formuly jazyka $\mathcal{L}$. Potom:

$(A \to B) \Leftrightarrow_{\mathrm{p}} (\neg A \lor B)$	*nahradenie* $\to$
$(A \land (B \land C)) \Leftrightarrow_{\mathrm{p}} ((A \land B) \land C)$	*asociatívnosť* $\land$
$(A \lor (B \lor C)) \Leftrightarrow_{\mathrm{p}} ((A \lor B) \lor C)$	*asociatívnosť* $\lor$
$(A \land B) \Leftrightarrow_{\mathrm{p}} (B \land A)$	*komutatívnosť* $\land$
$(A \lor B) \Leftrightarrow_{\mathrm{p}} (B \lor A)$	*komutatívnosť* $\lor$
$(A \land (B \lor C)) \Leftrightarrow_{\mathrm{p}} ((A \land B) \lor (A \land C))$	*distributívnosť* $\land$ *cez* $\lor$
$(A \lor (B \land C)) \Leftrightarrow_{\mathrm{p}} ((A \lor B) \land (A \lor C))$	*distributívnosť* $\lor$ *cez* $\land$

Veta 4.10 (pokračovanie)

$\neg(A \land B) \Leftrightarrow_{\mathrm{p}} (\neg A \lor \neg B)$	*de Morganove*
$\neg(A \lor B) \Leftrightarrow_{\mathrm{p}} (\neg A \land \neg B)$	*zákony*
$\neg\neg A \Leftrightarrow_{\mathrm{p}} A$	*zákon dvojitej negácie*
$(A \land A) \Leftrightarrow_{\mathrm{p}} A$	*idempotencia pre* $\land$
$(A \lor A) \Leftrightarrow_{\mathrm{p}} A$	*idempotencia pre* $\lor$
$(A \land \top) \Leftrightarrow_{\mathrm{p}} A$	*identita pre* $\land$
$(A \lor \bot) \Leftrightarrow_{\mathrm{p}} A$	*identita pre* $\lor$
$(A \lor (A \land B)) \Leftrightarrow_{\mathrm{p}} A$	*absorpcia*
$(A \land (A \lor B)) \Leftrightarrow_{\mathrm{p}} A$	
$(A \lor \neg A) \Leftrightarrow_{\mathrm{p}} \top$	*vylúčenie tretieho (tertium non datur)*
$(A \land \neg A) \Leftrightarrow_{\mathrm{p}} \bot$	*spor,*

kde $\top$ je ľubovoľná tautológia a $\bot$ je ľubovoľná nesplniteľná formula.

Všeobecné dôkazy známych ekvivalencií

Pre konkrétne dvojice formúl v konkrétnom jazyku sa ekvivalencia dá dokázať rozborom všetkých ohodnotení ako v príklade 4.8.

Dôkaz ekvivalencie $(A \to B)$ a $(\neg A \lor B)$ pre ľubovoľné formuly A a B vyžaduje opatrnejší postup.

Nemôžeme predpokladať, že A a B sú atomické a ohodnotenia im priamo priraďujú pravdivostné hodnoty f a t (ak napr. $A = (\mathrm{p}(\mathrm{a}) \land \neg \mathrm{p}(\mathrm{a}))$, tak $v(A)$ nie je definované, definované sú iba $v(\mathrm{p}(\mathrm{a}))$ a $v(\mathrm{p}(\mathrm{b}))$).

Môžeme však:

1. zobrať ľubovoľné ohodnotenie v,
2. rozobrať všetky prípady, akými môžu byť A a B pravdivé alebo nepravdivé v tomto ohodnotení (teda $v \models_{\mathrm{p}} A$ a $v \models_{\mathrm{p}} B$, $v \models_{\mathrm{p}} A$ a $v \not\models_{\mathrm{p}} B$, $v \not\models_{\mathrm{p}} A$ a $v \models_{\mathrm{p}} B$, $v \not\models_{\mathrm{p}} A$ a $v \not\models_{\mathrm{p}} B$)
3. a ukázať, že v každom prípade je $(A \to B)$ pravdivá vo v vtt je $(\neg A \lor B)$ pravdivá vo v.

Príklad 4.11 (Dôkaz prvej ekvivalentnej dvojice z vety 4.10)

Nech A a B sú ľubovoľné výrokovologické formuly v ľubovoľnom jazyku $\mathcal{L}$.

Nech v je ľubovoľné ohodnotenie pre $\mathcal{L}$. V tomto ohodnotení môže byť každá z formúl A a B buď pravdivá alebo nepravdivá, a teda môžu nastať nasledovné prípady:

- $v \not\models_{\mathrm{p}} A$ a $v \not\models_{\mathrm{p}} B$, vtedy $v \models_{\mathrm{p}} (A \rightarrow B)$ a $v \models_{\mathrm{p}} (\neg A \vee B)$;
- $v \not\models_{\mathrm{p}} A$ a $v \models_{\mathrm{p}} B$, vtedy $v \models_{\mathrm{p}} (A \rightarrow B)$ a $v \models_{\mathrm{p}} (\neg A \vee B)$;
- $v \models_{\mathrm{p}} A$ a $v \not\models_{\mathrm{p}} B$, vtedy $v \not\models_{\mathrm{p}} (A \rightarrow B)$ a $v \not\models_{\mathrm{p}} (\neg A \vee B)$;
- $v \models_{\mathrm{p}} A$ a $v \models_{\mathrm{p}} B$, vtedy $v \models_{\mathrm{p}} (A \rightarrow B)$ a $v \models_{\mathrm{p}} (\neg A \vee B)$.

Rozobrali sme **všetky prípady** pravdivosti A a B v ohodnotení v a aj keď sa prípady od seba líšia pravdivosťou $(A \rightarrow B)$ a $(\neg A \vee B)$, v **každom prípade** platí, že $v \models_{\mathrm{p}} (A \rightarrow B)$ **vtt** $v \models_{\mathrm{p}} (\neg A \vee B)$. Preto môžeme konštatovať, že bez ohľadu na to, ktorý prípad nastáva, v ohodnotení v platí, že $v \models_{\mathrm{p}} (A \rightarrow B)$ vtt $v \models_{\mathrm{p}} (\neg A \vee B)$.

Pretože ohodnotenie v bolo **ľubovoľné**, môžeme toto konštatovanie **zovšeobecniť** na všetky ohodnotenia pre $\mathcal{L}$ a podľa definície 4.9 sú $(A \rightarrow B)$ a $(\neg A \vee B)$ výrokovologicky ekvivalentné.

Dôkazy rozborom prípadov

Rozbor prípadov z odrážkového zoznamu v predchádzajúcom dôkaze môžeme zapísať do **podobnej** tabuľky ako v príklade 4.8:

	A	B	$(A \to B)$	$(\neg A \lor B)$
v	$\not\models_p$	$\not\models_p$	$\models_p$	$\models_p$
v	$\not\models_p$	$\models_p$	$\models_p$	$\models_p$
v	$\models_p$	$\not\models_p$	$\not\models_p$	$\not\models_p$
v	$\models_p$	$\models_p$	$\models_p$	$\models_p$

Vždy ju však treba doplniť

1. úvodom o ľubovoľnom ohodnotení,
2. úvodom k rozboru prípadov,
3. záverom o všetkých prípadoch,
4. záverom o všetkých ohodnoteniach.

Podobne môžeme uvažovať o tautológiách, nesplniteľnosti, aj vyplývaní.

Sémantické vlastnosti a vzťahy formúl

Vzťah tautológií, vyplývania a ekvivalencie

Tautológie a vyplývanie

Tautológie nie sú zaujímavé iba preto, že sú logickými pravdami.

Kedy je formula $((A_1 \land A_2) \to B)$ tautológia?

Vtedy, keď je pravdivá v každom ohodnotení,
teda keď v každom ohodnotení v máme $v \not\models_p (A_1 \land A_2)$ alebo $v \models_p B$,
čiže keď v každom ohodnotení v,
v ktorom $v \models_p (A_1 \land A_2)$, máme aj $v \models_p B$
teda keď v každom ohodnotení v,
v ktorom $v \models_p A_1$ a $v \models_p A_2$, máme aj $v \models_p B$,
teda keď z $\{A_1, A_2\}$ výrokovologicky **vyplýva** B.

Vzťahy výrokovologického vyplývania a tautológií

Pripomeňme, že podľa tvrdenia 4.4: $\emptyset \models_{\mathrm{p}} A$ vtt $\models_{\mathrm{p}} A$.

Tvrdenie 4.12 (Sémantická verzia vety o dedukcii)

Nech $\mathcal{L}$ je jazyk výrokovologickej časti logiky prvého rádu.
Nech T je výrokovologická teória, nech A, B, C sú výrokovologické formuly v $\mathcal{L}$. Potom:

a) $T \cup \{A\} \models_{\mathrm{p}} C$ vtt $T \models_{\mathrm{p}} (A \to C)$.
b) $T \cup \{A, B\} \models_{\mathrm{p}} C$ vtt $T \cup \{(A \land B)\} \models_{\mathrm{p}} C$.

Dôsledok 4.13 (Redukcia vyplývania na tautológiu)

Nech $\mathcal{L}$ je jazyk výrokovologickej časti logiky prvého rádu.
Nech $A_1, A_2, \ldots, A_n$ a C sú výrokovologické formuly v jazyku $\mathcal{L}$.
Potom $\{A_1, \ldots, A_n\} \models_{\mathrm{p}} C$ vtt $\models_{\mathrm{p}} \big(((\cdots(A_1 \land A_2) \land \cdots) \land A_n\big) \to C\big)$.

Dôkaz tvrdenia 4.12.

a) Nech T je teória a A a C sú výrokovologické formuly v ľubovoľnom jazyku $\mathcal{L}$.

($\Leftarrow$) Predpokladajme, že $T \models_{\mathrm{p}} (A \to C)$ a dokážme **priamo**, že z $T \cup \{A\}$ vyplýva C.

Zoberme ľubovoľné výrokovologické ohodnotenie v pre $\mathcal{L}$, ktoré je modelom $T \cup \{A\}$. Vo v sú teda pravdivé všetky formuly z $T \cup \{A\}$. Preto $v \models_{\mathrm{p}} T$ a tiež $v \models_{\mathrm{p}} A$.

Dôkaz tvrdenia 4.12.

a) Nech T je teória a A a C sú výrokovologické formuly v ľubovoľnom jazyku $\mathcal{L}$.

($\Leftarrow$) Predpokladajme, že $T \models_p (A \to C)$ a dokážme **priamo**, že z $T \cup \{A\}$ vyplýva C.

Zoberme ľubovoľné výrokovologické ohodnotenie v pre $\mathcal{L}$, ktoré je modelom $T \cup \{A\}$. Vo v sú teda pravdivé všetky formuly z $T \cup \{A\}$. Preto $v \models_p T$ a tiež $v \models_p A$.

Z $v \models_p T$ na základe predpokladu $T \models_p (A \to C)$ dostávame, že vo v je pravdivá implikácia $(A \to C)$, teda podľa definície pravdivosti $v \not\models_p A$ alebo $v \models_p C$. Pretože ale vieme, že $v \models_p A$, musí $v \models_p C$.

Keďže v bol ľubovoľný model $T \cup \{A\}$, môžeme toto zistenie zovšeobecniť na všetky ohodnotenia a podľa definície vyplývania potom $T \cup \{A\} \models_p C$.

Dôkaz tvrdenia 4.12.

a) Nech T je teória a A a C sú výrokovologické formuly v ľubovoľnom jazyku $\mathcal{L}$.

(⇐) Predpokladajme, že $T \models_p (A \to C)$ a dokážme **priamo**, že z $T \cup \{A\}$ vyplýva C.

Zoberme ľubovoľné výrokovologické ohodnotenie v pre $\mathcal{L}$, ktoré je modelom $T \cup \{A\}$. Vo v sú teda pravdivé všetky formuly z $T \cup \{A\}$. Preto $v \models_p T$ a tiež $v \models_p A$.

Z $v \models_p T$ na základe predpokladu $T \models_p (A \to C)$ dostávame, že vo v je pravdivá implikácia $(A \to C)$, teda podľa definície pravdivosti $v \not\models_p A$ alebo $v \models_p C$. Pretože ale vieme, že $v \models_p A$, musí $v \models_p C$.

Keďže v bol ľubovoľný model $T \cup \{A\}$, môžeme toto zistenie zovšeobecniť na všetky ohodnotenia a podľa definície vyplývania potom $T \cup \{A\} \models_p C$.

(⇒) Predpokladajme, že z $T \cup \{A\}$ vyplýva C a dokážme **sporom**, že z T vyplýva $(A \to C)$.

Dôkaz tvrdenia 4.12.

a) Nech T je teória a A a C sú výrokovologické formuly v ľubovoľnom jazyku $\mathcal{L}$.

($\Leftarrow$) Predpokladajme, že $T \vDash_p (A \to C)$ a dokážme **priamo**, že z $T \cup \{A\}$ vyplýva C.

Zoberme ľubovoľné výrokovologické ohodnotenie v pre $\mathcal{L}$, ktoré je modelom $T \cup \{A\}$. Vo v sú teda pravdivé všetky formuly z $T \cup \{A\}$. Preto $v \vDash_p T$ a tiež $v \vDash_p A$.

Z $v \vDash_p T$ na základe predpokladu $T \vDash_p (A \to C)$ dostávame, že vo v je pravdivá implikácia $(A \to C)$, teda podľa definície pravdivosti $v \nvDash_p A$ alebo $v \vDash_p C$. Pretože ale vieme, že $v \vDash_p A$, musí $v \vDash_p C$.

Keďže v bol ľubovoľný model $T \cup \{A\}$, môžeme toto zistenie zovšeobecniť na všetky ohodnotenia a podľa definície vyplývania potom $T \cup \{A\} \vDash_p C$.

($\Rightarrow$) Predpokladajme, že z $T \cup \{A\}$ vyplýva C a dokážme **sporom**, že z T vyplýva $(A \to C)$.

Nech by existovalo ohodnotenie v, ktoré je modelom T, ale nie formuly $(A \to C)$, teda podľa definície pravdivosti $v \vDash_p A$ a $v \nvDash_p C$. Z $v \vDash_p T$ a $v \vDash_p A$ máme $v \vDash_p T \cup \{A\}$ a z predpokladu $T \cup \{A\} \vDash_p C$ dostávame $v \vDash_p C$, čo je spor.

b) Dôkaz je podobný ako v časti a). $\square$

Dôkaz dôsledku 4.13.

Nech $\mathcal{L}$ je jazyk výrokovologickej časti logiky prvého rádu. Nech $A_1, A_2, \ldots, A_n$ a C sú výrokovologické formuly v jazyku $\mathcal{L}$.

Opakovaným použitím tvrdenia 4.12 a pomocou 4.4 dostávame:

$$
\begin{aligned}
\{A_1, A_2, \ldots, A_n\} \vDash_{\mathrm{p}} C \quad & \text{vtt} \quad \{(A_1 \wedge A_2), \ldots, A_n\} \vDash_{\mathrm{p}} C \\
& \text{vtt} \quad \cdots \\
& \text{vtt} \quad \emptyset \cup \{((\cdots(A_1 \wedge A_2) \wedge \cdots) \wedge A_n)\} \vDash_{\mathrm{p}} C \\
& \text{vtt} \quad \emptyset \vDash_{\mathrm{p}} (((\cdots(A_1 \wedge A_2) \wedge \cdots) \wedge A_n) \to C) \\
& \text{vtt} \quad \vDash_{\mathrm{p}} (((\cdots(A_1 \wedge A_2) \wedge \cdots) \wedge A_n) \to C) \qquad \square
\end{aligned}
$$

Tautológie a ekvivalencia

Kedy je formula $(X \leftrightarrow Y)$, teda $((X \to Y) \land (Y \to X))$ tautológia?

Vtedy a len vtedy, keď je pravdivá v každom ohodnotení, teda
vtt v každom ohodnotení v máme $v \models_p (X \to Y)$ a $v \models_p (Y \to X)$,
vtt v každom ohodnotení v máme buď $v \not\models_p X$ alebo $v \models Y$ a zároveň
buď $v \not\models_p Y$ alebo $v \models X$,
vtt v každom ohodnotení v platí,
že ak $v \models_p X$, tak $v \models_p Y$, a ak $v \models_p Y$, tak $v \models_p X$,
vtt v každom ohodnotení v máme $v \models_p X$ vtt $v \models_p Y$,
vtt X je výrokovologicky **ekvivalentná** s Y.

Tvrdenie 4.14

Nech $\mathcal{L}$ je jazyk výrokovologickej časti logiky prvého rádu.
Nech X a Y sú výrokovologické formuly v $\mathcal{L}$.
Potom $(X \leftrightarrow Y)$ je tautológia vtt X a Y sú výrokologicky ekvivalentné.
(Skrátene: $\models_p (X \leftrightarrow Y)$ vtt $X \Leftrightarrow_p Y$.)

Sémantické vlastnosti a vzťahy formúl

Ekvivalentné úpravy a CNF

Reťazenie ekvivalentných úprav

Určite ste už robili ekvivalentné úpravy formúl,
pri ktorých ste **reťazili dvojice** vzájomne ekvivalentných formúl:

$$\neg(A \to \neg B) \Leftrightarrow_{\mathrm{p}} \neg(\neg A \lor \neg B) \Leftrightarrow_{\mathrm{p}} (\neg\neg A \land \neg\neg B) \Leftrightarrow_{\mathrm{p}} (A \land B)$$

a nakoniec ste prehlásili, že prvá $\neg(A \to \neg B)$ a posledná formula $(A \land B)$ sú ekvivalentné.

Mohli ste to urobiť, lebo $\Leftrightarrow_{\mathrm{p}}$ je **tranzitívna** relácia na formulách, dokonca viac než iba tranzitívna.

Výrokovologická ekvivalencia ako relácia ekvivalencie

Tvrdenie 4.15

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

*Vzťah výrokovologickej ekvivalencie $\Leftrightarrow_{\mathrm{p}}$ je **reláciou ekvivalencie** na výrokovologických formulách jazyka $\mathcal{L}$, teda pre všetky výrokovologické formuly X, Y, Z jazyka $\mathcal{L}$ platí:*

- *Reflexivita:* $X \Leftrightarrow_{\mathrm{p}} X$.
- *Symetria: Ak* $X \Leftrightarrow_{\mathrm{p}} Y$, *tak* $Y \Leftrightarrow_{\mathrm{p}} X$.
- *Tranzitivita: Ak* $X \Leftrightarrow_{\mathrm{p}} Y$ *a* $Y \Leftrightarrow_{\mathrm{p}} Z$, *tak* $X \Leftrightarrow_{\mathrm{p}} Z$.

Dôkaz.

Priamym dôkazom dokážeme tranzitivitu. Ostatné vlastnosti sa dajú dokázať podobne.

Nech X, Y a Z sú výrokovologické formuly jazyka $\mathcal{L}$.
Nech (1) X je výrokovologicky ekvivalentná s Y a (2) Y je ekvivalentná so Z.

Aby sme dokázali, že X je výrokovologicky ekvivalentná so Z, musíme ukázať, že pre každé ohodnotenie pre jazyk $\mathcal{L}$ platí, že $v \models_{\mathrm{p}} X$ vtt $v \models_{\mathrm{p}} Z$.

Nech teda v je ľubovoľné ohodnotenie pre $\mathcal{L}$.

- Ak $v \models_{\mathrm{p}} X$, tak podľa predpokladu (1) a definície výrokovologickej ekvivalencie 4.9 musí platiť $v \models_{\mathrm{p}} Y$, a teda podľa predpokladu (2) a definície ekvivalencie máme $v \models_{\mathrm{p}} Z$.
- Nezávisle od toho, ak $v \models_{\mathrm{p}} Z$, tak $v \models_{\mathrm{p}} Y$ podľa (2) a def. 4.9, a teda $v \models_{\mathrm{p}} X$ podľa (1) a def. 4.9.

Preto $v \models_{\mathrm{p}} X$ vtt $v \models_{\mathrm{p}} Z$.

Pretože v bolo ľubovoľné, môžeme náš záver zovšeobecniť na všetky ohodnotenia, a teda podľa definície ekvivalencie 4.9 sú X a Z výrokovologicky ekvivalentné. $\square$

Substitúcia pri ekvivalentných úpravách

V reťazci ekvivalentných úprav

$$\neg(A \to \neg B) \Leftrightarrow_{\mathrm{p}} \neg(\neg A \lor \neg B) \Leftrightarrow_{\mathrm{p}} (\neg\neg A \land \neg\neg B)$$
$$\Leftrightarrow_{\mathrm{p}} (A \land \neg\neg B) \Leftrightarrow_{\mathrm{p}} (A \land B)$$

v prvom, treťom a štvrtom kroku **nezodpovedá celá** formula niektorej zo známych ekvivalencií z vety 4.10.

Podľa známej ekvivalencie sme **nahrádzali podformuly** — **substituovali** sme ich.

Definícia 4.16 (Substitúcia)

Nech $\mathcal{L}$ je jazyk výrokovologickej časti logiky prvého rádu a nech X, A, B sú formuly jazyka $\mathcal{L}$.
Substitúciou B za A v X (skrátene $X[A|B]$) nazývame formulu, ktorá vznikne nahradením každého výskytu A v X formulou B.

Substitúcia rekurzívne

Substitúciu si vieme predstaviť aj ako induktívne definovanú (rekurzívnu) operáciu:

Substitúcia rekurzívne

Nech $\mathcal{L}$ je jazyk výrokovologickej časti logiky prvého rádu. Pre všetky formuly A, B, X, Y jazyka $\mathcal{L}$ a všetky binárne spojky $b \in \{\wedge, \vee, \rightarrow\}$:

$$\begin{aligned} X[A|B] &= B, && \text{ak } A = X \\ X[A|B] &= X, && \text{ak } X \text{ je atóm a } A \neq X \\ (\neg X)[A|B] &= \neg(X[A|B]), && \text{ak } A \neq \neg X \\ (X\ b\ Y)[A|B] &= ((X[A|B])\ b\ (Y[A|B])), && \text{ak } A \neq (X\ b\ Y). \end{aligned}$$

Korektnosť substitúcie ekvivalentnej formuly

Substitúciou ekvivalentnej podformuly, napríklad

$$(\neg\neg O \land \neg\neg C)[\neg\neg O|O] = (O \land \neg\neg C),$$

skutočne dostávame formulu ekvivalentnú s pôvodnou:

Veta 4.17 (Ekvivalentné úpravy substitúciou)

Nech $\mathcal{L}$ je jazyk výrokovologickej časti logiky prvého rádu a nech X je formula, A a B sú výrokovologicky ekvivalentné formuly jazyka $\mathcal{L}$. Potom formuly X a $X[A|B]$ sú tiež výrokovologicky ekvivalentné.

Toto tvrdenie môžeme dokázať indukciou na konštrukciu formuly.

Ekvivalentné úpravy a vstup pre SAT solver

Mnoho teoretických i praktických problémov možno formulovať ako otázku splniteľnosti výrokovologickej formuly — SAT (napr. riešiteľnosť sudoku, existenciu cesty či farbenia v grafe, ekvivalenciu logických hardvérových obvodov).

Na riešenie SAT existujú dlhoročne vyvíjané solvery. Ukázalo sa, že najvýhodnejšie je mať vstup v špecifickom tvare: v konjunktívnej normálnej forme (CNF). Transformácia formuly do tejto formy je tak jedným z najčastejších využití ekvivalentných úprav.

Aby sme CNF mohli popísať, potrebujeme pomenovať viacnásobne vnorené konjunkcie a viacnásobne vnorené disjunkcie a dohodneme sa na skracovaní ich zápisu vynechaním vnútorných zátvoriek.

Konjunkcia a disjunkcia postupnosti formúl

Definícia 4.18

Nech $\mathcal{L}$ je jazyk výrokovologickej časti logiky prvého rádu.
Nech $A_1, A_2, \ldots, A_n$ je konečná postupnosť formúl jazyka $\mathcal{L}$.

- *Konjunkciou postupnosti* $A_1, \ldots, A_n$ je formula $(((A_1 \land A_2) \land A_3) \land \cdots \land A_n)$, skrátene $(A_1 \land A_2 \land A_3 \land \cdots \land A_n)$.
  - Konjunkciu *prázdnej* postupnosti formúl ($n = 0$) označujeme $\top$. Chápeme ju ako ľubovoľnú *tautológiu*, napríklad $(P(c) \lor \neg P(c))$ pre nejaký unárny predikát P a nejakú konštantu c jazyka $\mathcal{L}$.
- *Disjunkciou postupnosti* $A_1, \ldots, A_n$ je formula $(((A_1 \lor A_2) \lor A_3) \lor \cdots \lor A_n)$, skrátene $(A_1 \lor A_2 \lor A_3 \lor \cdots \lor A_n)$.
  - Disjunkciu *prázdnej* postupnosti formúl označujeme $\bot$ alebo $\square$. Chápeme ju ako ľubovoľnú *nesplniteľnú* formulu, napríklad $(P(c) \land \neg P(c))$.
- Pre $n = 1$ chápeme samotnú formulu A_1 ako konjunkciu aj ako disjunkciu jednoprvkovej postupnosti formúl A_1.

Literál, klauzula, konjunktívny normálny tvar

Vstup do SAT solvera je formula v konjunktívnom normálnom tvare.

Definícia 4.19

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.

Príklad 4.20

Literály: P, C,
$\neg C$, $\neg O$

Klauzuly: $(\neg P \lor O \lor \neg C)$,
ale aj P, $\neg O$, $\square$,

CNF: $((P \lor O) \land \square)$, $((\neg P \lor O) \land (O \lor C))$, ale
aj P, $\neg O$, $\top$, $(P \lor \neg O)$ $(P \land \neg O \land C)$, $\square$,

kde P, O, C sú ľubovoľné atómy.

Existencia ekvivalentnej formuly v CNF

Veta 4.21

Ku každej výrokovologickej formule X existuje ekvivalentná formula C v konjunktívnom normálnom tvare.

Dôkaz.

Zoberme všetky ohodnotenia $v_1, \ldots, v_n$ také, že $v_i \models_\mathrm{p} \neg X$ a $v_i(A) = f$ pre všetky atómy $A \notin \mathrm{atoms}(\neg X)$.
Pre každé v_i zostrojme formulu C_i ako konjunkciu obsahujúcu A, ak $v_i(A) = t$, alebo $\neg A$, ak $v_i(A) = f$, pre každý atóm $A \in \mathrm{atoms}(\neg X)$.
Očividne formula $D = (C_1 \lor \cdots \lor C_n)$ je ekvivalentná s $\neg X$ (vymenúva všetky možnosti, kedy je $\neg X$ pravdivá).

Znegovaním D a aplikáciou de Morganových pravidiel dostaneme formulu C v CNF, ktorá je ekvivalentná s X. $\square$

Konverzia formuly do ekvivalentnej v CNF

Skúmanie všetkých ohodnotení podľa dôkazu vety 4.21 nie je ideálny spôsob ako upraviť formulu do CNF — najmä keď má veľa premenných a jej splniteľnosť chceme rozhodnúť SAT solverom.

Jednoduchý algoritmus na konverziu formuly do ekvivalentnej formuly v CNF založený na ekvivalentných úpravách si naprogramujete ako **4. praktické cvičenie**.

Konverzia formuly do ekvivalentnej v CNF

Základný algoritmus konverzie do CNF má dve fázy:

1. Upravíme formulu na *negačný normálny tvar* (NNF) —
   nevyskytuje sa v ňom implikácia a negované sú iba atómy:
   - Nahradíme implikácie disjunkciami: $(A \to B) \Leftrightarrow_{\mathrm{p}} (\neg A \lor B)$
   - Presunieme $\neg$ k atómom opakovaným použitím de Morganových zákonov a zákona dvojitej negácie.
2. Odstránime konjunkcie vnorené v disjunkciách „roznásobením“ podľa distributívnosti a komutatívnosti:

$$(A \lor (B \land C)) \Leftrightarrow_{\mathrm{p}} ((A \lor B) \land (A \lor C))$$

$$\begin{aligned}((B \land C) \lor A) &\Leftrightarrow_{\mathrm{p}} (A \lor (B \land C)) \Leftrightarrow_{\mathrm{p}} ((A \lor B) \land (A \lor C))\\ &\Leftrightarrow_{\mathrm{p}} ((B \lor A) \land (A \lor C))\\ &\Leftrightarrow_{\mathrm{p}} ((B \lor A) \land (C \lor A))\end{aligned}$$

Príklad 4.22

Úprava formuly do NNF:

$$
\begin{aligned}
((\neg S \land P) \to \neg(Z \lor \neg O)) &\Leftrightarrow_{\mathrm{p}} (\neg(\neg S \land P) \lor \neg(Z \lor \neg O)) && \text{(nahr. } \to\text{)}\\
&\Leftrightarrow_{\mathrm{p}} ((\neg\neg S \lor \neg P) \lor (\neg Z \land \neg\neg O)) && \text{(2} \times \text{de Morgan)}\\
&\Leftrightarrow_{\mathrm{p}} ((S \lor \neg P) \lor (\neg Z \land O)) && \text{(2} \times \text{dvoj. neg.)}
\end{aligned}
$$

Úprava formuly v NNF do CNF:

$$
\begin{aligned}
&((S \lor \neg P) \lor (\neg Z \land O))\\
&\qquad \Leftrightarrow_{\mathrm{p}} (((S \lor \neg P) \lor \neg Z) \land ((S \lor \neg P) \lor O)) && \text{(distr. } \land \text{ cez } \lor\text{)}
\end{aligned}
$$

Podľa dohody v def. 4.18 výslednú formulu v CNF skrátene zapíšeme:

$$((S \lor \neg P \lor \neg Z) \land (S \lor \neg P \lor O))$$

Sémantické vlastnosti a vzťahy formúl

CNF vs. XOR

XOR

Logická spojka exlusive or (XOR):

a	b	$a \oplus b$
0	0	0
0	1	1
1	0	1
1	1	0

- zodpovedá sčítaniu v poli $\mathbb{Z}_2$
- komutatívna a asociatívna
- rýchlo vypočítateľná, aj na úrovni hardvéru
- dôležitá v kryptológii

XOR

Ideálna šifra: všetky zašifrované texty sú rovnako pravdepodobné. Napr. vezmeme náhodný reťazec (kľúč) rovnako dlhý ako správa a spravíme XOR bit po bite. Použitý kľúč zahodíme a nikdy viac nepoužijeme.

Reálne šifry: kľúč je krátky (napr. 1024 B). Ak by sme ho nakopírovali veľakrát za sebou, bity správy šifrované tým istým bitom kľúča vytvoria slabinu (možno dešifrovať aj bez znalosti kľúča, stačí uhádnuť jeho dĺžku). Preto napr. použijeme kľúč ako seed do pseudonáhodného generátora a vygenerujeme reťazec potrebnej dĺžky.

Útoky na šifry: o.i. pomocou SAT solvera, ktorý vie pracovať s XOR (aktívna oblasť výskumu).

XOR

Ku XOR existuje prepis do CNF, napr. z $a \oplus b \oplus c$ sa stane

$(a \vee b \vee c) \wedge (a \vee \neg b \vee \neg c) \wedge (b \vee \neg a \vee \neg c) \wedge (c \vee \neg a \vee \neg b)$

XOR

Ku XOR existuje prepis do CNF, napr. z $a \oplus b \oplus c$ sa stane

$(a \vee b \vee c) \wedge (a \vee \neg b \vee \neg c) \wedge (b \vee \neg a \vee \neg c) \wedge (c \vee \neg a \vee \neg b)$

Ale s počtom premenných rastie dĺžka ekvivalentnej CNF formuly exponenciálne. Preto sa oplatí predspracovanie: XOR formuly vnímame ako súčty nad $\mathbb{Z}_2$ a použijeme Gaussovu elimináciu.

$$a_1 \oplus a_2 \oplus a_3 = 0$$

$$a_1 \oplus a_3 \oplus a_4 = 0$$

$$\begin{pmatrix} 1 & 1 & 1 & 0 & | & 0 \\ 1 & 0 & 1 & 1 & | & 0 \end{pmatrix}$$

$$\begin{pmatrix} 1 & 0 & 1 & 1 & | & 0 \\ 0 & 1 & 0 & 1 & | & 0 \end{pmatrix}$$

Sémantické vlastnosti a vzťahy formúl

Rekapitulácia

Rekapitulácia

Dnes sme prebrali:

- Logické vyplývanie z teórie a logický dôsledok teórie
- Nezávislosť formuly od teórie
- Štyri situácie vo vzťahoch teórií a formúl a ich praktické dôsledky
- Splniteľné a nesplniteľné teórie
- Vzťah nesplniteľnosti a vyplývania
- Význačné sémantické vlastnosti formúl: tautologickosť, splniteľnosť, nesplniteľnosť, falzifikovateľnosť
- Ekvivalencia — sémantický vzťah formúl
- Syntaktické odvodenie ekvivalencie pomocou substitúcií podľa známych ekvivalencií
- NNF a CNF
- Vzťah tautológií s vyplývaním a ekvivalenciou