Vlastnosti a vzťahy výrokovologických formúl

4. prednáška · Matematika (4): Logika pre informatikov

Ján Kľuka, Jozef Šiška

Letný semester 2019/2020

Univerzita Komenského v Bratislave
Fakulta matematiky, fyziky a informatiky
Katedra aplikovanej informatiky

Obsah 4. prednášky

Vlastnosti a vzťahy výrokovologických formúl

- Tautológie, splniteľné, falzifikovateľné a nesplniteľné formuly
- Ekvivalencia
- Vzťah tautológií, vyplývania a ekvivalencie
- Ekvivalentné úpravy a CNF

Rekapitulácia

Minulý týždeň sme:

- zjednodušili pohľad na možné stavy sveta zo štruktúr na výrokovologické ohodnotenia,
- zistili sme, že na zistenie vyplývania/logických dôsledkov stačí pre konečné teórie skúmať konečne veľa ohodnotení, ktoré zastúpia nekonečne veľa štruktúr,
- presne sme zadefinovali vzťahy medzi teóriou a formulou z hľadiska ohodnotení:
    - výrokovologické vyplývanie,
    - výrokovologickú nezávislosť.

Vlastnosti a vzťahy výrokovologických formúl

Vlastnosti a vzťahy výrokovologických 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 $(A \vee \neg A)$.

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

Majme jazyk $\mathcal{L}$ s $\mathcal{C}_{\mathcal{L}} = \{\texttt{Pacient348}\}$, $\mathcal{P}_{\mathcal{L}} = \{\texttt{očkovaný}^1, \texttt{chorý}^1\}$. Je formula $X = \big(\neg(\neg\texttt{očkovaný}(\texttt{Pacient348}) \lor \texttt{chorý}(\texttt{Pacient348})) \to (\texttt{očkovaný}(\texttt{Pacient348}) \lor \neg\texttt{chorý}(\texttt{Pacient348}))\big)$ tautológiou?

Označme $O = \texttt{očkovaný}(\texttt{Pacient348})$ a $C = \texttt{chorý}(\texttt{Pacient348})$, teda $X = \big(\neg(\neg O \lor C) \to (O \lor \neg C)\big)$ a preskúmajme všetky výrokovologické ohodnotenia týchto atómov:

	v_i							
	O	C	$\neg O$	$(\neg O \lor C)$	$\neg(\neg O \lor C)$	$\neg C$	$(O \lor \neg C)$	X
v_0	f	f	$\models_p$	$\models_p$	$\not\models_p$	$\models_p$	$\models_p$	$\models_p$
v_1	t	f	$\not\models_p$	$\not\models_p$	$\models_p$	$\models_p$	$\models_p$	$\models_p$
v_2	f	t	$\models_p$	$\models_p$	$\not\models_p$	$\not\models_p$	$\not\models_p$	$\models_p$
v_3	t	t	$\not\models_p$	$\models_p$	$\not\models_p$	$\not\models_p$	$\models_p$	$\models_p$

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 pre $\mathcal{L}$, teda ohodnotenia **všetkých predikátových atómov jazyka $\mathcal{L}$**.
Ale…

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

Postačujúca podmienka pre tautológiu

Na minulej prednáške sme spomenuli, že platí:

Tvrdenie 4.3

Nech $\mathcal{L}$ je jazyk výrokovologickej časti logiky prvého rádu a nech X je výrokovologická formula jazyka $\mathcal{L}$.
Pre všetky ohodnotenia v_1 a v_2, ktoré zhodujú na množine $\mathrm{atoms}(X)$, platí $v_1 \models_{\mathrm{p}} X$ vtt $v_2 \models_{\mathrm{p}} X$.

Stačí teda preverovať ohodnotenia atómov vyskytujúcich sa vo formule:

Dôsledok 4.4

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 $v : \ \mathrm{atoms}(X) \to \{f, t\}$.

Dôkaz zhody ohodnotení na formule

O pravdivosti týchto tvrdení sa vieme ľahko presvedčiť:

Dôkaz tvrdenia 4.3.

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. □

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.

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

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
$v \models_{\mathrm{p}} X$).

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**.

	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	$\cdots$	$\not\models_p$
		$\cdots$		

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
$v \not\models_p X$).

Nesplniteľnosť

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

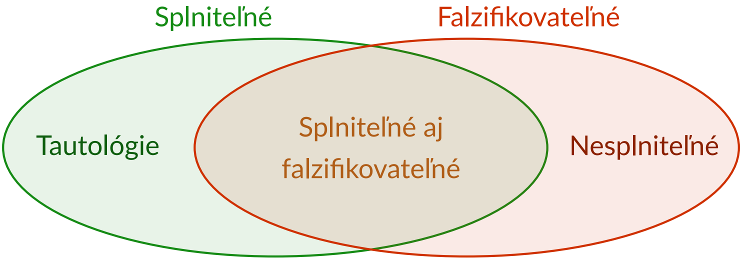
Nazývame ich nesplniteľné.

	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	$\cdots$	$\not\models_p$
		$\cdots$		

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
$v \not\models_p X$).

„Geografia“ formúl podľa pravdivosti vo všetkých ohodnoteniach



Obrázok podľa Papadimitriou [1994]

Vlastnosti a vzťahy výrokovologických 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 $O = \texttt{očkovaný}(\texttt{Pacient348})$ a $C = \texttt{chorý}(\texttt{Pacient348})$. Sú formuly $X = \neg(O \to \neg C)$ a $Y = (O \land C)$ výrokovologicky ekvivalentné?

Preskúmajme všetky výrokovologické ohodnotenia atómov O a C:

	v_i				X	Y
	O	C	$\neg C$	$(O \to \neg C)$	$\neg(O \to \neg C)$	$(C \land O)$
v_0	f	f	$\models_p$	$\models_p$	$\not\models_p$	$\not\models_p$
v_1	t	f	$\models_p$	$\models_p$	$\not\models_p$	$\not\models_p$
v_2	f	t	$\not\models_p$	$\models_p$	$\not\models_p$	$\not\models_p$
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 práve uvedenej definície. 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.

Známe ekvivalencie

Veta 4.10

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

$$(A \to B) \Leftrightarrow_{\mathrm{p}} (\neg A \lor B) \qquad \text{nahradenie } \to$$

$$(A \land (B \land C)) \Leftrightarrow_{\mathrm{p}} ((A \land B) \land C) \qquad \text{asociatívnosť } \land$$

$$(A \lor (B \lor C)) \Leftrightarrow_{\mathrm{p}} ((A \lor B) \lor C) \qquad \text{asociatívnosť } \lor$$

$$(A \land B) \Leftrightarrow_{\mathrm{p}} (B \land A) \qquad \text{komutatívnosť } \land$$

$$(A \lor B) \Leftrightarrow_{\mathrm{p}} (B \lor A) \qquad \text{komutatívnosť } \lor$$

$$(A \land (B \lor C)) \Leftrightarrow_{\mathrm{p}} ((A \land B) \lor (A \land C)) \qquad \text{distributívnosť } \land \text{ cez } \lor$$

$$(A \lor (B \land C)) \Leftrightarrow_{\mathrm{p}} ((A \lor B) \land (A \lor C)) \qquad \text{distributívnosť } \lor \text{ cez } \land$$

Známe ekvivalencie

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*

Všeobecné dôkazy známych ekvivalencií

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

Ak chceme dokázať napríklad ekvivalenciu $(A \to B)$ a $(\neg A \lor B)$ skutočne pre **ľubovoľné** formuly A a B, musíme postupovať **opatrnejšie**.

Nemôžeme predpokladať, že A a B sú atomické a ohodnotenia im **priamo** priraďujú pravdivostné hodnoty f a t.

Môžeme však zobrať **ľubovoľné** ohodnotenie v a uvažovať o všetkých možnostiach, akými môžu byť A a B pravdivé alebo nepravdivé v tomto ohodnotení a ukázať, že v každom prípade bude $(A \to B)$ pravdivá vo v vtt bude $(\neg A \lor B)$ pravdivá vo v.

Príklad dôkazu známej ekvivalencie

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:

- $v \not\models_p A$ a $v \not\models_p B$, vtedy $v \models_p (A \to B)$ a $v \models_p (\neg A \lor B)$;
- $v \not\models_p A$ a $v \models_p B$, vtedy $v \models_p (A \to B)$ a $v \models_p (\neg A \lor B)$;
- $v \models_p A$ a $v \not\models_p B$, vtedy $v \not\models_p (A \to B)$ a $v \not\models_p (\neg A \lor B)$;
- $v \models_p A$ a $v \models_p B$, vtedy $v \models_p (A \to B)$ a $v \models_p (\neg A \lor B)$.

Rozobrali sme všetky prípady pravdivosti A a B v ohodnotení v a aj keď sa prípady od seba líšia pravdivosťou $(A \to B)$ a $(\neg A \lor B)$, v každom prípade platí, že $v \models_p (A \to B)$ vtt $v \models_p (\neg A \lor B)$. Preto môžeme konštatovať, že bez ohľadu na to, ktorý prípad nastáva, v ohodnotení v platí, že $v \models_p (A \to B)$ vtt $v \models_p (\neg A \lor B)$.

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

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	$\not\models_{\mathrm{p}}$	$\not\models_{\mathrm{p}}$	$\models_{\mathrm{p}}$	$\models_{\mathrm{p}}$
v	$\not\models_{\mathrm{p}}$	$\models_{\mathrm{p}}$	$\models_{\mathrm{p}}$	$\models_{\mathrm{p}}$
v	$\models_{\mathrm{p}}$	$\not\models_{\mathrm{p}}$	$\not\models_{\mathrm{p}}$	$\not\models_{\mathrm{p}}$
v	$\models_{\mathrm{p}}$	$\models_{\mathrm{p}}$	$\models_{\mathrm{p}}$	$\models_{\mathrm{p}}$

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, či dokonca vyplývaní.

Vlastnosti a vzťahy výrokovologických 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 $v \not\models_{\mathrm{p}} (A_1 \land A_2)$ alebo $v \models_{\mathrm{p}} B$,
čiže keď v každom ohodnotení v,
v ktorom $v \models_{\mathrm{p}} (A_1 \land A_2)$, máme aj $v \models_{\mathrm{p}} B$
teda keď v každom ohodnotení v,
v ktorom $v \models_{\mathrm{p}} A_1$ a $v \models_{\mathrm{p}} A_2$, máme aj $v \models_{\mathrm{p}} B$,
teda keď z $\{A_1, A_2\}$ výrokovologicky **vyplýva** B.

Vzťahy výrokovologického vyplývania a tautológií

Tvrdenie 4.11

Nech $\mathcal{L}$ je jazyk výrokovologickej časti logiky prvého rádu.
Nech S a T sú výrokovologické teórie a A je výrokovologická formula v $\mathcal{L}$, pričom $S \subseteq T$.
Ak $S \vDash_{\mathrm{p}} A$, tak $T \vDash_{\mathrm{p}} A$.

Tvrdenie 4.12

Nech $\mathcal{L}$ je jazyk výrokovologickej časti logiky prvého rádu.
Nech T je výrokovologická teória, nech A, B, A_1, A_2, $\ldots$, A_n sú výrokovologické formuly v $\mathcal{L}$. Potom:

a) *A vyplýva z prázdnej teórie $\emptyset$ vtt A je tautológia.*
   (Skrátene: $\emptyset \vDash_{\mathrm{p}} A$ vtt $\vDash_{\mathrm{p}} A$.)
b) *$T \cup \{A\} \vDash_{\mathrm{p}} B$ vtt $T \vDash_{\mathrm{p}} (A \to B)$.*
c) *$\vDash_{\mathrm{p}} (((\cdots(A_1 \land A_2) \land \cdots) \land A_n) \to B)$ vtt $\{A_1, A_2, \ldots, A_n\} \vDash_{\mathrm{p}} B$.*

Dôkaz vzťahu vyplývania a tautológií (⇒)

Dôkaz tvrdenia 4.12c).

Dôkaz tohto tvrdenia sme už naznačili, ale spravme ho podrobnejšie: Nech A_1, A_2, $\ldots$, A_n, B sú výrokovologické formuly v ľubovoľnom jazyku $\mathcal{L}$.

(⇒) Predpokladajme, že $X = (((\cdots(A_1 \land A_2) \land \cdots) \land A_n) \to B)$ je tautológia a dokážme, že potom z $\{A_1, A_2, \ldots, A_n\}$ vyplýva B.

Zoberme ľubovoľné výrokovologické ohodnotenie v pre $\mathcal{L}$. Musíme preň dokázať, že ak $v \models_p \{A_1, A_2, \ldots, A_n\}$, tak $v \models_p B$. Predpokladajme teda, že $v \models_p \{A_1, A_2, \ldots, A_n\}$. Potom je vo v pravdivá každá z formúl A_1 až A_n, a teda aj o konjunkciách $(A_1 \land A_2)$, $((A_1 \land A_2) \land A_3)$, $\ldots$, $(((\cdots(A_1 \land A_2) \land \cdots) \land A_n)$ postupne zistíme, že sú pravdivé vo v. Pretože X je tautológia, je pravdivá aj v ohodnotení v, a teda podľa definície pravdivosti a predchádzajúceho zistenia, musí byť pravdivý jej konzekvent B.

Zistili sme teda, že pre v platí, že ak $v \models_p \{A_1, A_2, \ldots, A_n\}$, tak $v \models_p B$. Pretože v bolo ľubovoľné, môžeme toto zistenie zovšebecniť na všetky ohodnotenia a podľa definície vyplývania potom $\{A_1, A_2, \ldots, A_n\} \models_p B$. □

Dôkaz vzťahu vyplývania a tautológií ($\Leftarrow$)

Dôkaz tvrdenia 4.12c) (pokračovanie).

($\Leftarrow$) Predpokladajme, že ($*$) z $\{A_1, A_2, \ldots, A_n\}$ vyplýva B a dokážme, že $X = (((\cdots(A_1 \land A_2) \land \cdots) \land A_n) \to B)$ je tautológia.

Zoberme ľubovoľné výrokovologické ohodnotenie v pre $\mathcal{L}$. Musíme preň dokázať, že $v \models_p X$. Môžeme to napríklad urobiť rozborom týchto prípadov:

- Ak $v \models_p A_i$ pre všetky $i = 1, \ldots, n$, tak $v \models_p \{A_1, A_2, \ldots, A_n\}$. Podľa predpokladu ($*$) a definície vyplývania potom musí $v \models_p B$, a teda platí, že $v \not\models_p (((\cdots(A_1 \land A_2) \land \cdots) \land A_n)$ alebo $v \models_p B$, a teda $v \models_p X$.
- Ak $v \not\models_p A_i$ pre niektoré $i \in \{1, \ldots, n\}$, tak $v \not\models_p (((\cdots(A_1 \land A_2) \land \cdots) \land A_i)$ a postupným pridávaním ďalších konjunktov dostaneme, že $v \not\models_p ((\cdots((\cdots(A_1 \land A_2) \land \cdots) \land A_i) \cdots) \land A_n)$. Aj v tomto prípade teda platí, že $v \not\models_p (((\cdots(A_1 \land A_2) \land \cdots) \land A_n)$ alebo $v \models_p B$, a teda $v \models_p X$.

V oboch prípadoch, z ktorých jeden musí vždy nastať, sme dospeli k rovnakému záveru: $v \models_p X$. Pretože v bolo ľubovoľné, môžeme toto zistenie zovšeobecniť na všetky ohodnotenia a podľa definície tautológie je X tautológiou. $\square$

Tautológie a ekvivalencia

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

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

Vzťah výrokovologickej ekvivalencie a tautológií

Tvrdenie 4.13

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: $\models_{\mathrm{p}} (X \leftrightarrow Y)$ vtt $X \Leftrightarrow_{\mathrm{p}} Y$.)

Dôkaz je podobný dôkazu tvrdenia 4.12.

Vlastnosti a vzťahy výrokovologických formúl

Ekvivalentné úpravy a CNF

Reťazenie ekvivalentných úprav

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

$$\neg(O \to \neg C) \Leftrightarrow_{\mathrm{p}} \neg(\neg O \vee \neg C) \Leftrightarrow_{\mathrm{p}} (\neg\neg O \wedge \neg\neg C) \Leftrightarrow_{\mathrm{p}} (O \vee C)$$

a nakoniec ste prehlásili, že prvá $\neg(O \to \neg C)$ a posledná formula $(O \wedge C)$ 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 4.14

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 $v \models_p X$ vtt $v \models_p Y$.

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

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

Preto $v \models_p X$ vtt $v \models_p Z$.

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

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* $X \Leftrightarrow_{\mathrm{p}} Z$.

Substitúcia pri ekvivalentných úpravách

V reťazci ekvivalentných úprav

$$\neg(O \to \neg C) \Leftrightarrow_{\mathrm{p}} \neg(\neg O \lor \neg C) \Leftrightarrow_{\mathrm{p}} (\neg\neg O \land \neg\neg C) \Leftrightarrow_{\mathrm{p}} (O \lor C)$$

v prvom a poslednom 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 $b \in \{\land, \lor, \to\}$:

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

Korektnosť substitúcie ekvivalentnej formuly

Substitúciou ekvivalentnej podformuly, napríklad

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

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 ekvivalentné formuly jazyka $\mathcal{L}$.
Potom formuly X a $X[A|B]$ sú tiež ekvivalentné.

Toto tvrdenie môžeme dokázať indukciou na konštrukciu formuly.

Ekvivalentné úpravy a vstup pre SAT solver

Častým použitím ekvivalentných úprav je transformácia teórie (napríklad o nejakom Sudoku) do tvaru vhodného pre SAT solver.

Aby sme tento tvar 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: P, $\neg O$, $\square$,
$(\neg P \lor O \lor \neg C)$

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

ak $P = \mathtt{pacient}(\mathtt{Edo})$,
$O = \mathtt{očkovaný}(\mathtt{Edo})$,
$C = \mathtt{chorý}(\mathtt{Edo})$.

Existencia ekvivalentnej formuly v CNF

Veta 4.21

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

Dôkaz.

Zoberme všetky ohodnotenia $v_1, \ldots, v_n$ také, že $v_i \models_p \neg X$ 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 $D = (C_1 \vee \ldots \vee C_2)$ 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 **praktické cvičenie**.

Konverzia formuly do ekvivalentnej v CNF

Algoritmus konverzie do CNF má dve fázy:

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

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

Literatúra

Christos H. Papadimitriou. *Computational complexity*. Addison-Wesley, 1994. ISBN 978-0-201-53082-7.