

Vlastnosti a vzťahy výrokovologických formúl

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

Ján Klúka, Jozef Šiška

Letný semester 2020/2021

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

Vlastnosti a vzťahy výrokovologických formúl

Tautológie, splniteľné, falzifikovateľné a nesplniteľné formuly

Ekvivalencia

Vzťah tautológií, vyplývania a ekvivalencie

Ekvivalentné úpravy a CNF

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 vztahy výrokovologických formúl

Vlastnosti a vztáhy 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.

Rozpoznatelné logické pravdy

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

- $c \doteq c$ aj $(A \vee \neg A)$ sú pravdivé v každej štruktúre.
- Výrokovologické ohodnotenia sa nezaoberajú rovnostnými atómami. Pomocou nich nezistíme, že $c \doteq c$ je nutne pravda. Ale zistíme, že $(A \vee \neg A)$ 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 $\mathcal{C}_{\mathcal{L}} = \{\text{Pacient348}\}$, $\mathcal{P}_{\mathcal{L}} = \{\text{očkovaný}^1, \text{chorý}^1\}$. Je formula $X = (\neg(\neg\text{očkovaný}(\text{Pacient348}) \vee \text{chorý}(\text{Pacient348})) \rightarrow (\text{očkovaný}(\text{Pacient348}) \vee \neg\text{chorý}(\text{Pacient348})))$ tautológiou?

Označme $O = \text{očkovaný}(\text{Pacient348})$ a $C = \text{chorý}(\text{Pacient348})$, teda $X = (\neg(\neg O \vee C) \rightarrow (O \vee \neg C))$ a preskúmajme všetky výrokovologické ohodnotenia týchto atómov:

	v_i		$\neg O$	$(\neg O \vee C)$	$\neg(\neg O \vee C)$	$\neg C$	$(O \vee \neg C)$	X
	O	C						
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.

Definícia 4.2

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

Nech X je výrokovologická formula.

Formulu X nazveme **tautológiou** (skrátene $\models_{\mathcal{L}} X$) vtt

X je **pravdivá** v **každom** výrokovologickom ohodnotení v pre \mathcal{L}
(teda **pre každé** výrokovologické ohodnotenie v pre \mathcal{L} platí $v \models_{\mathcal{L}} X$).

Definícia vyžaduje preveriť všetky možné ohodnotenia pre \mathcal{L} , teda ohodnotenia **všetkých predikátových atómov jazyka \mathcal{L}** .

Ale...

	v_i			
	A_1	A_2	\dots	X
v_0	f	f	\dots	$\models_{\mathcal{L}}$
v_1	f	f	\dots	$\models_{\mathcal{L}}$
		\dots		
v_k	t	f	\dots	$\models_{\mathcal{L}}$
		\dots		

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 $\text{atoms}(X)$, platí $v_1 \models_p X$ vtt $v_2 \models_p X$.

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 $v : \text{atoms}(X) \rightarrow \{f, t\}$.

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 $\text{atoms}(X)$, 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 $\text{atoms}(\neg X)$. Pretože $\text{atoms}(\neg X) = \text{atoms}(X)$, v_1 a v_2 sa zhodujú na $\text{atoms}(X)$, 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 $(X \wedge Y)$. Zoberme ľubovoľné ohodnotenia v_1 a v_2 , ktoré sa zhodujú na $\text{atoms}((X \wedge Y))$. Pretože $\text{atoms}((X \wedge Y)) = \text{atoms}(X) \cup \text{atoms}(Y)$, v_1 a v_2 sa zhodujú na $\text{atoms}(X)$, a teda podľa IP $v_1 \models_p X$ vtt $v_2 \models_p X$; tiež sa zhodujú na $\text{atoms}(Y)$, a teda podľa IP $v_1 \models_p Y$ vtt $v_2 \models_p Y$. Preto $v_1 \models_p (X \wedge Y)$ 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) $v_2 \models_p (X \wedge Y)$.

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	\dots	X
v_0	f	f	\dots	$\not\models_p$
v_1	f	f	\dots	$\not\models_p$
		\dots		
v_k	t	f	\dots	\models_p
		\dots		

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 $v \models_p X$).

Falzifikovateľnosť

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

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

Definícia 4.6

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

Nech X je výrokovologická formula.

Formulu X nazveme **falseifikovateľnou**

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	\dots	X
v_0	f	f	\dots	$\not\models_p$
v_1	f	f	\dots	$\not\models_p$
		\dots		
v_k	t	f	\dots	$\not\models_p$
		\dots		

Definícia 4.7

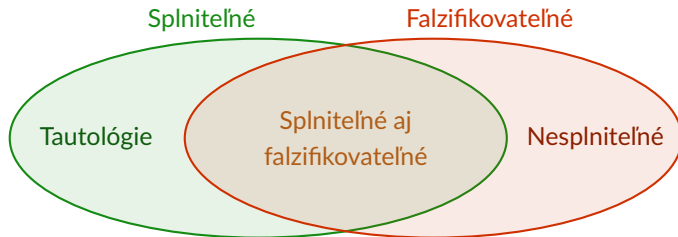
Nech \mathcal{L} je jazyk výrokovologickej časti logiky prvého rádu.

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 vztahy výrokovologických formúl

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 výrokovologicke ekvivalentných formúl

Príklad 4.8

V jazyku \mathcal{L} z príkladu 4.1 označme $O = \text{očkovaný(Pacient348)}$ a $C = \text{chorý(Pacient348)}$. Sú formuly $X = \neg(O \rightarrow \neg C)$ a $Y = (O \wedge C)$ výrokovologicke ekvivalentné?

Preskúmame všetky výrokovologické ohodnotenia atómov O a C :

	v_i				X	Y
	O	C	$\neg C$	$(O \rightarrow \neg C)$	$\neg(O \rightarrow \neg C)$	$(C \wedge O)$
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 výrokovologicke ekvivalentné.

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 $X \Leftrightarrow_p Y$ vtt pre **každé** výrokovologické ohodnotenie v pre jazyk \mathcal{L} platí, že X je pravdivá vo v vtt Y je pravdivá vo v .

 **Pozor!** Nemýľte si zápis $X \Leftrightarrow_p Y$ s formulou $(X \leftrightarrow Y)$.

- $X \Leftrightarrow_p Y$ je skrátené vyjadrenie vzťahu dvoch formúl podľa práve uvedenej definície. Keď napíšeme $X \Leftrightarrow_p Y$, 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, nespĺniteľná, môže vyplývať, či byť nezávislá od nejakej teórie, alebo môže byť výrokovologicky ekvivalentná s inou formulou.

Medzi $X \Leftrightarrow_p Y$ a $(X \leftrightarrow Y)$ je vzťah, ktorý si ozrejníme neskôr.

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:

$$(A \rightarrow B) \Leftrightarrow_p (\neg A \vee B)$$

nahradenie \rightarrow

$$(A \wedge (B \wedge C)) \Leftrightarrow_p ((A \wedge B) \wedge C)$$

asociatívnosť \wedge

$$(A \vee (B \vee C)) \Leftrightarrow_p ((A \vee B) \vee C)$$

asociatívnosť \vee

$$(A \wedge B) \Leftrightarrow_p (B \wedge A)$$

komutatívnosť \wedge

$$(A \vee B) \Leftrightarrow_p (B \vee A)$$

komutatívnosť \vee

$$(A \wedge (B \vee C)) \Leftrightarrow_p ((A \wedge B) \vee (A \wedge C))$$

distributívnosť \wedge cez \vee

$$(A \vee (B \wedge C)) \Leftrightarrow_p ((A \vee B) \wedge (A \vee C))$$

distributívnosť \vee cez \wedge

Veta 4.10 (pokračovanie)

$$\neg(A \wedge B) \Leftrightarrow_p (\neg A \vee \neg B) \quad \text{de Morganove}$$

$$\neg(A \vee B) \Leftrightarrow_p (\neg A \wedge \neg B) \quad \text{zákony}$$

$$\neg\neg A \Leftrightarrow_p A \quad \text{zákon dvojitej negácie}$$

$$(A \wedge A) \Leftrightarrow_p A \quad \text{idempotencia pre } \wedge$$

$$(A \vee A) \Leftrightarrow_p A \quad \text{idempotencia pre } \vee$$

$$(A \wedge \top) \Leftrightarrow_p A \quad \text{identita pre } \wedge$$

$$(A \vee \perp) \Leftrightarrow_p A \quad \text{identita pre } \vee$$

$$(A \vee (A \wedge B)) \Leftrightarrow_p A \quad \text{absorpcia}$$

$$(A \wedge (A \vee B)) \Leftrightarrow_p A$$

$$(A \vee \neg A) \Leftrightarrow_p \top \quad \text{vylúčenie tretieho (tertium non datur)}$$

$$(A \wedge \neg A) \Leftrightarrow_p \perp \quad \text{spor,}$$

kde \top je ľubovoľná tautológia a \perp je ľubovoľná nespĺniteľná 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 $(A \rightarrow B)$ a $(\neg A \vee B)$ pre **ľubovoľné** formuly A a B vyžaduje **opatrnejší** postup.

Nemôžeme predpokladať, že A a B sú atomické a ohodnotenia im **priamo** priradujú pravdivostné hodnoty f a t (ak napr. $A = (\text{oč}(p) \wedge \neg \text{ch}(p))$), tak $v(A)$ nie je definované, definované sú iba $v(\text{oč}(p))$ a $v(\text{ch}(p))$.

Môžeme však:

1. zobrať **ľubovoľné** ohodnotenie v ,
2. rozobrať všetky prípady, akými môžu byť A a B pravdivé alebo nepravdivé v tomto ohodnotení (teda $v \models_p A$ a $v \models_p B$,
 $v \models_p A$ a $v \not\models_p B$, $v \not\models_p A$ a $v \models_p B$, $v \not\models_p A$ a $v \not\models_p B$)
3. a ukázať, že v každom prípade
je $(A \rightarrow B)$ pravdivá vo v vtt je $(\neg A \vee B)$ 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:

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

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 $v \models_p (A \rightarrow B)$ **vtt** $v \models_p (\neg A \vee B)$. Preto môžeme konštatovať, že bez ohľadu na to, ktorý prípad nastáva, v ohodnotení v platí, že $v \models_p (A \rightarrow B)$ vtt $v \models_p (\neg A \vee B)$.

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. \square

Dôkazy rozborom prípadov

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

	A	B	$(A \rightarrow B)$	$(\neg A \vee B)$
\vee	$\not\vdash_p$	$\not\vdash_p$	$\not\vdash_p$	$\not\vdash_p$
\vee	$\not\vdash_p$	\vdash_p	\vdash_p	\vdash_p
\vee	\vdash_p	$\not\vdash_p$	$\not\vdash_p$	$\not\vdash_p$
\vee	\vdash_p	\vdash_p	\vdash_p	\vdash_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 $((A_1 \wedge A_2) \rightarrow B)$ tautológia?

Vtedy, keď je pravdivá v každom ohodnotení,

teda keď v každom ohodnotení v máme $v \not\models_p (A_1 \wedge A_2)$ alebo $v \models_p B$,

čiže keď v každom ohodnotení v ,

v ktorom $v \models_p (A_1 \wedge A_2)$, 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 výrokovologickeho vyplývania a tautológií

Tvrdenie 4.11

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

Nech S a T sú výrokovologicke teórie a A je výrokovologická formula v \mathcal{L} , pričom $S \subseteq T$.

Ak $S \models_p A$, tak $T \models_p A$.

Tvrdenie 4.12

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

Nech T je výrokovologická teória, nech $A, B, A_1, A_2, \dots, A_n$ sú výrokovologické formuly v \mathcal{L} . Potom:

a) A vyplýva z prázdnej teórie \emptyset vtt A je tautológia.

(Skrátene: $\emptyset \models_p A$ vtt $\models_p A$.)

b) $T \cup \{A\} \models_p B$ vtt $T \models_p (A \rightarrow B)$.

c) $\models_p (((\dots (A_1 \wedge A_2) \wedge \dots) \wedge A_n) \rightarrow B)$ vtt $\{A_1, A_2, \dots, A_n\} \models_p B$.

Dôkaz vzťahu vyplývania a tautológií (\Rightarrow)

Dôkaz tvrdenia 4.12c).

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

(\Rightarrow) Predpokladajme, že $X = (((\dots (A_1 \wedge A_2) \wedge \dots) \wedge A_n) \rightarrow B)$ je tautológia a dokážme, že potom z $\{A_1, A_2, \dots, A_n\}$ vyplýva B .

Zoberme ľubovoľné výrokovologické ohodnotenie v pre \mathcal{L} . Musíme preň dokázať, že ak $v \models_p \{A_1, A_2, \dots, A_n\}$, tak $v \models_p B$. Predpokladajme teda, že $v \models_p \{A_1, A_2, \dots, A_n\}$. Potom je vo v pravdivá každá z formúl A_1 až A_n , a teda aj o konjunkciách $(A_1 \wedge A_2)$, $((A_1 \wedge A_2) \wedge A_3)$, \dots , $((\dots (A_1 \wedge A_2) \wedge \dots) \wedge A_n)$ 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 $v \models_p \{A_1, A_2, \dots, A_n\}$, tak $v \models_p B$. Pretože v bolo ľubovoľné, môžeme toto zistenie zovšeobecniť na všetky ohodnotenia a podľa definície vyplývania potom $\{A_1, A_2, \dots, A_n\} \models_p B$. □

Dôkaz vzťahu vyplývania a tautológií (\Leftrightarrow)

Dôkaz tvrdenia 4.12c) (pokračovanie).

(\Leftarrow) Predpokladajme, že $(*)$ z $\{A_1, A_2, \dots, A_n\}$ vyplýva B a dokážme, že $X = (((\dots (A_1 \wedge A_2) \wedge \dots) \wedge A_n) \rightarrow B)$ 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 $i = 1, \dots, n$, tak $v \models_p \{A_1, A_2, \dots, A_n\}$. Podľa predpokladu $(*)$ a definície vyplývania potom musí $v \models_p B$, a teda platí, že $v \models_p (((\dots (A_1 \wedge A_2) \wedge \dots) \wedge A_n) \rightarrow B)$ alebo $v \models_p B$, a teda $v \models_p X$.
- Ak $v \not\models_p A_i$ pre niektoré $i \in \{1, \dots, n\}$, tak $v \not\models_p (((\dots (A_1 \wedge A_2) \wedge \dots) \wedge A_i)$ a postupným pridávaním ďalších konjunktov dostaneme, že $v \not\models_p (((\dots (((\dots (A_1 \wedge A_2) \wedge \dots) \wedge A_i) \dots) \wedge A_n))$. Aj v tomto prípade teda platí, že $v \models_p (((\dots (A_1 \wedge A_2) \wedge \dots) \wedge A_n) \rightarrow B)$ 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 $((X \rightarrow Y) \wedge (Y \rightarrow X))$ 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 $v \models_p Y$, tak $v \models_p X$,

teda keď v každom ohodnotení v máme $v \models_p X$ vtt $v \models_p Y$,

teda keď X výrokovologicky **ekvivalentná** s Y .

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: $\models_p (X \leftrightarrow Y)$ vtt $X \Leftrightarrow_p Y$.)

Dôkaz je podobný dôkazu tvrdenia 4.12.

Vlastnosti a vztahy výrokovologických formúl

Ekvivalentné úpravy a CNF

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

$$\neg(O \rightarrow \neg C) \Leftrightarrow_p \neg(\neg O \vee \neg C) \Leftrightarrow_p (\neg\neg O \wedge \neg\neg C) \Leftrightarrow_p (O \wedge C)$$

a nakoniec ste prehlásili, že prvá $\neg(O \rightarrow \neg C)$ a posledná formula $(O \wedge C)$ sú ekvivalentné.

Mohli ste to urobiť, lebo \Leftrightarrow_p je **tranzitívna** relácia na formulách,
dokonca viac než iba tranzitívna.

Tvrdenie 4.14

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

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

- Reflexivita: $X \Leftrightarrow_p X$.
- Symetria: Ak $X \Leftrightarrow_p Y$, tak $Y \Leftrightarrow_p X$.
- Tranzitivita: Ak $X \Leftrightarrow_p Y$ a $Y \Leftrightarrow_p Z$, tak $X \Leftrightarrow_p Z$.

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

Substitúcia pri ekvivalentných úpravách

V reťazci ekvivalentných úprav

$$\begin{aligned}\neg(O \rightarrow \neg C) &\Leftrightarrow_p \neg(\neg O \vee \neg C) \Leftrightarrow_p (\neg\neg O \wedge \neg\neg C) \\ &\Leftrightarrow_p (O \wedge \neg\neg C) \Leftrightarrow_p (O \wedge C)\end{aligned}$$

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 4.15 (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 indukzívne 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 $b \in \{\wedge, \vee, \rightarrow\}$:

$$X[A|B] = B, \quad \text{ak } A = X$$

$$X[A|B] = X, \quad \text{ak } X \text{ je atóm a } A \neq X$$

$$(\neg X)[A|B] = \neg(X[A|B]), \quad \text{ak } A \neq \neg X$$

$$(X \ b \ Y)[A|B] = ((X[A|B]) \ b \ (Y[A|B])), \quad \text{ak } A \neq (X \ b \ Y).$$

Korektnosť substitúcie ekvivalentnej formuly

Substitúciou ekvivalentnej podformuly, napríklad

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

skutočne dostávame formulu ekvivalentnú s pôvodnou:

Veta 4.16 (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.

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 4.17

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

Nech A_1, A_2, \dots, A_n je konečná postupnosť formúl jazyka \mathcal{L} .

- **Konjunkciou postupnosti A_1, \dots, A_n** je formula $((A_1 \wedge A_2) \wedge A_3) \wedge \dots \wedge A_n$, skrátene $(A_1 \wedge A_2 \wedge A_3 \wedge \dots \wedge A_n)$.
 - Konjunkciu *prázdnej* postupnosti formúl ($n = 0$) označujeme \top .
Chápeme ju ako ľubovoľnú *tautológiu*, napríklad $(P(c) \vee \neg P(c))$ pre nejaký unárny predikát P a nejakú konštantu c jazyka \mathcal{L} .
- **Disjunkciou postupnosti A_1, \dots, A_n** je formula $((A_1 \vee A_2) \vee A_3) \vee \dots \vee A_n$, skrátene $(A_1 \vee A_2 \vee A_3 \vee \dots \vee A_n)$.
 - Disjunkciu *prázdnej* postupnosti formúl označujeme \perp alebo \square .
Chápeme ju ako ľubovoľnú *nesplniteľnú* formulu, napríklad $(P(c) \wedge \neg P(c))$.
- 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 4.18

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 4.19

Literály: $P, C,$
 $\neg C, \neg O$

Klauzuly: $P, \neg O, \square,$
 $(\neg P \vee O \vee \neg C)$

CNF: $P, \neg O, \top, (P \vee \neg O)$
 $(P \wedge \neg O \wedge C), \square,$
 $((P \vee O) \wedge \square),$
 $((\neg P \vee O) \wedge (O \vee C))$

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

Veta 4.20

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

Dôkaz.

Zoberme všetky ohodnotenia v_1, \dots, v_n také, že $v_i \models_p \neg X$ a $v_i(A) = f$ pre všetky atómy $A \notin \text{atoms}(\neg X)$.

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 $A \in \text{atoms}(\neg X)$.

Očividne formula $D = (C_1 \vee \dots \vee C_n)$ 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 . □

Konverzia formuly do ekvivalentnej v CNF

Skúmanie všetkých ohodnotení podľa dôkazu vety 4.20 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: $(A \rightarrow B) \Leftrightarrow_p (\neg A \vee B)$
 - Presunieme \neg k atómom opakovaným použitím de Morganových zákonov a zákona dvojitej negácie.
2. Odstránime konjunkcie vnorené v disjunkciách „roznásobením“ podľa distributívnosti a komutatívnosti:

$$(A \vee (B \wedge C)) \Leftrightarrow_p ((A \vee B) \wedge (A \vee C))$$

$$((B \wedge C) \vee A) \Leftrightarrow_p (A \vee (B \wedge C)) \Leftrightarrow_p ((A \vee B) \wedge (A \vee C))$$

$$\Leftrightarrow_p ((B \vee A) \wedge (A \vee C))$$

$$\Leftrightarrow_p ((B \vee A) \wedge (C \vee A))$$

Príklad 4.21

Úprava formuly do NNF:

$$\begin{aligned} ((\neg S \wedge P) \rightarrow \neg(Z \vee \neg O)) &\Leftrightarrow_p (\neg(\neg S \wedge P) \vee \neg(Z \vee \neg O)) \quad (\text{nahr. } \rightarrow) \\ &\Leftrightarrow_p ((\neg\neg S \vee \neg P) \vee (\neg Z \wedge \neg\neg O)) \quad (2 \times \text{de Morgan}) \\ &\Leftrightarrow_p ((S \vee \neg P) \vee (\neg Z \wedge O)) \quad (2 \times \text{dvoj. neg.}) \end{aligned}$$

Úprava formuly v NNF do CNF:

$$\begin{aligned} &((S \vee \neg P) \vee (\neg Z \wedge O)) \\ &\Leftrightarrow_p (((S \vee \neg P) \vee \neg Z) \wedge ((S \vee \neg P) \vee O)) \quad (\text{distr. } \wedge \text{ cez } \vee) \end{aligned}$$

Podľa dohody v def. 4.17 výslednú formulu v CNF skrátené zapíšeme:

$$((S \vee \neg P \vee \neg Z) \wedge (S \vee \neg P \vee O))$$

- Význačné sémantické vlastnosti formúl:
tautologickosť, splniteľnosť, nespľniteľnosť, falzifikovateľnosť
- Ekvivalencia — sémantický vzťah formúl
- Vzťah tautológií s vyplývaním a ekvivalenciou
- Syntaktické odvodenie ekvivalencie pomocou substitúcií podľa známych ekvivalencií
- NNF a CNF

Literatúra

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