Prednášky z Matematiky (4) — Logiky pre informatikov

Ján Kľuka, Jozef Šiška

Letný semester 2017/2018

Obsah

l.	O logike a tomto kurze Syntax výrokovej logiky	3
1.	Úvod	3
	1.1. O logike	. 3
	1.2. O kurze	. 9
2.	Výroková logika	10
	2.1. Opakovanie: Výroková logika v prirodzenom jazyku	. 10
	2.2. Syntax	. 12
II.	Sémantika výrokovej logiky	16
	2.3. Sémantika	. 17
	2.4. Tautológie, (ne)splniteľnosť, falzifikovateľnosť	. 20
III.	l. Vyplývanie, ekvivalentné úpravy	26
	2.5. Vyplývanie	. 27
	2.6. Ekvivalencia	. 30
	2.6.1. Ekvivalentné úpravy	. 32

	2.6.2. Konjunktívna a disjunktívna normálna forma	35
IV.	. CNF. Tablový kalkul	37
	2.7. Kalkuly	40
	2.8. Tablový kalkul	
	2.8.1. Korektnosť	
V.	Korektnosť a úplnosť tablového kalkulu	48
	2.8.2. Tablový dôkaz splniteľnosti	50
	2.8.3. Hintikkova lema	51
	2.8.4. Úplnosť	
VI	. Korektné pravidlá. Rezolvencia	54
	2.8.5. Nové korektné pravidlá	54
	2.9. Výroková rezolvencia	56
	2.10.Späť k dôkazom o vyplývaní	59

I. prednáška

O logike a tomto kurze Syntax výrokovej logiky

19. februára 2018

1. Úvod

1.1. O logike

I.1	Čo je logika	

- Logika je vedná disciplína, ktorá študuje formy usudzovania
 - filozofická, matematická, informatická, výpočtová
- Tri dôležité predmety záujmu:

Jazyk zápis pozorovaní, definície pojmov, formulovanie teórií *Syntax* pravidlá zápisu tvrdení *Sémantika* význam tvrdení

Usudzovanie (inferencia) odvodenie nových dôsledkov z doterajších poznatkov

Dôkaz presvedčenie ostatných o správnosti záverov usudzovania

I.2 Poznatky a teórie	
-----------------------	--

- V logike slúži jazyk na zápis tvrdení, ktoré vyjadrujú informácie poznatky o svete
- Súbor poznatkov, ktoré považujeme za pravdivé, tvorí teóriu

Príklad 1.1 (Party time!). Máme troch nových známych – Kim, Jima a Sarah.Organizujeme párty a chceme na ňu pozvať niektorých z nich.Od spoločných kamarátov sme sa ale dozvedeli o ich požiadavkách:

- P1: Sarah nepôjde na párty, ak pôjde Kim.
- P2: Jim pôjde na párty, len ak pôjde Kim.
- P3: Sarah nepôjde bez Jima.
- I.3 Možné svety a logické dôsledky
 - Tvrdenie rozdeľuje množinu možných stavov sveta na tie stavy, v ktorých je pravdivé (modely), a tie stavy, v ktorých je nepravdivé
 - Teória môže mať viacero modelov (ale aj žiaden)
 Príklad 1.2. Vymenujme možné stavy prítomnosti Kim, Jima a Sarah na párty a zistime, v ktorých sú pravdivé jednotlivé tvrdenia našej teórie a celá teória.
 - **Logickými dôsledkami** teórie sú tvrdenia, ktoré sú pravdivé vo *všetkých* modeloch teórie (svetoch, v ktorých je pravdivá)

Príklad 1.3. Logickým dôsledkom teórie (P1), (P2), (P3) je napríklad: Sarah nepôjde na párty.

1.4	Logické usudzovanie	

- Vymenovanie všetkých svetov je často nepraktické až nemožné
- Logické dôsledky môžeme odvodzovať **usudzovaním** (inferovať)
- Pri odvodení vychádzame z premís (predpokladov) a postupnosťou úsudkov dospievame k záverom

Príklad 1.4. Vieme, že ak na párty pôjde Kim, tak nepôjde Sarah (P1), a že ak pôjde Jim, tak pôjde Kim (P2).

Predpokladajme, že na párty pôjde Jim.

Potom podľa (P2) pôjde aj Kim.

Potom podľa (P1) nepôjde Sarah.

Teda: Ak na párty pôjde Jim, nepôjde Sarah.

• Ak sú všetky úsudky v odvodení správne, záver je logickým dôsledkom premís a odvodenie je jeho **dôkazom** z premís

I.5 Usudzovacie pravidlá, korekt	tnosť, dedukcia			
 Už Aristoteles zistil, ž bez ohľadu na obsah 	-	ıdky sa	dajú rozpozna	ť podľa ich <i>formy</i> ,
Ak pôjde Jim, tak pôj	de Kim.		Ak je dilítium o tak antihmot	dekryštalizované, ta neprúdi.
Pôjde Jim.			Dilítium je dek	ryštalizované.
Pôjde Kim.		_	Antihmota nep	rúdi.
Usudzovacie (infere dení, s ktorými pracu	-	dlo je າ	vzor úsudkov d	laný formou tvr-
	Ak <i>A</i> , tak <i>B</i> . <i>A</i> .	} vzoi	ry premís	
	<i>B</i> .	VZO1	záveru	
 Korektné pravidlo od Dôkaz je teda postují (najlepšie samozrejm) Dedukcia — usudzov 	pnosť použit ých pre čitate	í korek eľa dôka	at ných usudzo azu)	vacích pravidiel
I.6 Nededuktívne pravidlá _	d======	-: 41		- X- 4.
Niektoré nie korektné usud Indukcia – zovšeobecneni	_	/idia su	ргакиску изи	ocne:
Videl som tisíc havrar Žiaden nebol inej far		_	Platí aj	pre červené Fabie?
Všetky havrany sú čie	erne.			
Abdukcia — odvodzovanie	možných prí	čin z na	ásledkov:	
Ak je batéria vybitá, a Ak je nádrž prázdna, Nádrž nie je prázdna Auto nenaštartovalo.	auto nenaštar			Čo ak nám kuna prehrýzla káble?
Batéria je vybitá.				

Usudzovanie na základe analógie (podobnosti)

Venuša má atmosféru, podobne ako Zem.	A čo: Atmosféra
Na Zemi sa prejavuje skleníkový efekt.	Zeme je dýchateľná
Na Venuši sa prejavuje skleníkový efekt.	Zeme je dychatema.

1.7	Nededuktívne pravidlá		

- Závery nededuktívnych pravidiel treba považovať za hypotézy plauzibilné, ale neoverené tvrdenia
- Hypotézy je nutné preverovať!
- Niektoré špeciálne prípady sú správne, napríklad matematická indukcia
- Usudzovanie s nededuktívnymi pravidlami je teda hypotetické
- Hypotetické usudzovanie je dôležité pre umelú inteligenciu
 - Reprezentácia znalostí a inferencia (magisterský predmet)
- V tomto kurze sa budeme zaoberať iba dedukciou

1.8	Formálny jazyk			
-----	----------------	--	--	--

- Prirodzený jazyk je problematický tvrdenia môžu byť viacznačné, ťažko zrozumiteľné, používať obraty a ustálené výrazy so špeciálnym významom
 - Mišo je myš.
 - Videl som dievča v sále s ďalekohľadom.
 - Vlastníci bytov a nebytových priestorov v dome prijímajú rozhodnutia na schôdzi vlastníkov dvojtretinovou väčšinou hlasov všetkých vlastníkov bytov a nebytových priestorov v dome, ak hlasujú o zmluve o úvere a o každom dodatku k nej, o zmluve o zabezpečení úveru a o každom dodatku k nej, o zmluve o nájme a kúpe veci, ktorú vlastníci bytov a nebytových priestorov v dome užívajú s právom jej kúpy po uplynutí dojednaného času užívania a o každom dodatku k nej, o zmluve o vstavbe alebo nadstavbe a o každom dodatku k nim, o zmene účelu užívania spoločných častí domu a spoločných zariadení domu a o zmene formy výkonu správy; ak sa rozhoduje o nadstavbe alebo o vstavbe v podkroví alebo povale, vyžaduje sa zároveň súhlas všetkých vlastníkov bytov a nebytových priestorov v dome na najvyššom poschodí. Zákon č. 182/1993 Z. z. SR v zmení neskorších predpisov

- Nikto nie je dokonalý.
- Tieto ťažkosti sa obchádzajú použitím formálneho jazyka
 - Presne definovaná, zjednodušená syntax (pravidlá zápisu tvrdení) a sémantika (význam) – podobne ako programovací jazyk
- Problémy z reálneho sveta opísané v prirodzenom jazyku musíme najprv formalizovať, a potom naň môžeme použiť logický aparát

• S formalizáciou ste sa už stretli pri riešení slovných úloh

```
Karol je trikrát starší ako Mária. k=3\cdot m
Súčet Karolovho a Máriinho veku je 12 rokov. \longleftrightarrow k+m=12
```

- Stretli ste sa už aj s formálnym jazykom výrokovej logiky
 Príklad 1.5. Sformalizujme náš párty príklad:
 - PO: Niekto z trojice Kim, Jim, Sarah pôjde na párty.
 - P1: Sarah nepôjde na párty, ak pôjde Kim.
 - P2: Jim pôjde na párty, len ak pôjde Kim.
 - рз: Sarah nepôjde bez Jima.

I.10 Kalkuly – formalizácia usudzovania

- Pre mnohé logiky sú známe kalkuly množiny usudzovacích pravidiel, ktoré sú
 - korektné odvodzujú iba logické dôsledky
 - **úplné** umožňujú odvodiť všetky logické dôsledky
- Kalkuly existujú aj v iných častiach matematiky
 - na počítanie s číslami, zlomkami (aritmetický kalkul),

- riešenie lineárnych rovníc (kalkul lineárnej algebry),
- derivovanie, integrovanie, riešenie diferenciálnych rovníc (kalkul matematickej analýzy)

. . .

Nie vždy sú úplné

I.11 Výpočtová logika – automatizácia usudzovania ______

- Základná idea výpočtovej logiky:
 - Napíšeme program,
 ktorý systematicky aplikuje pravidlá logického kalkulu,
 kým neodvodí želaný dôsledok,
 alebo nevyčerpá všetky možnosti (nie vždy je ich konečne veľa!)
- Skutočnosť je komplikovanejšia, ale existuje množstvo automatických usudzovacích systémov
- Jeden z prienikov informatiky a logiky

I.12 Výpočtová logika — aplikácie _____

- Overovanie, dopĺňanie, hľadanie dôkazov matematických viet
- Špecifikácia a verifikácia hardvérových obvodov, programov, komunikačných protokolov
 - Špecifikácia a verifikácia programov (3. ročník)
 - Formálne metódy tvorby softvéru (magisterský)
- Logické programovanie
 - Programovacie paradigmy (3. ročník)
 - Výpočtová logika (magisterský)
 - Logické programovanie ASP (magisterský)
- Databázy pohľady, integritné obmedzenia, optimalizácia dopytov

- Deduktívne databázy (3. ročník)
- Sémantický web a integrácia dát z rôznych zdrojov
 - Reprezentácia znalostí a inferencia (magisterský)
 - Ontológie a znalostné inžinierstvo (magisterský)
- Analýza zákonov, regulácií, zmlúv

1.13

Spomeňte si I.1

Tvrdenie, ktoré je pravdivé vo všetkých svetoch, v ktorých je pravdivá teória, je jej

A. premisou,

C. záverom,

B. logickým dôsledkom,

D. implikáciou.

Spomeňte si I.2

Účelom dôkazu je presvedčiť ostatných o správnosti nášho úsudku. Preto musí pozostávať z

Spomeňte si I.3

Usudzovanie, pri ktorom používame iba také pravidlá, ktoré z pravdivých premís vždy odvodia pravdivé závery, sa nazýva:

A. abdukcia,

C. formalizácia,

E. indukcia,

B. interpretácia,

D. dedukcia,

F. inferencia.

1.2. O tomto kurze

I.14 Čím sa budeme zaoberať v tomto kurze

Teoreticky • Jazykmi výrokovej a predikátovej logiky, ich syntaxou a sémantikou

• Korektnosťou usudzovacích pravidiel

- Korektnosťou a úplnosťou logických kalkulov
- Automatizovateľnými kalkulmi

Prakticky

- Vyjadrovaním problémov v jazyku logiky
- Automatizovaním riešenia problémov použitím SAT-solverov
- Manipuláciou symbolických stromových štruktúr (výrazov formúl a termov)
- Programovaním vlastných jednoduchých automatických dokazovačov

Filozoficky

- Zamýšľanými a nezamýšľanými okolnosťami platnosti tvrdení
- Obmedzeniami vyjadrovania a usudzovania

I.15 Organizácia kurzu — rozvrh, kontakty, pravidlá

https://dai.fmph.uniba.sk/w/Course:Mathematics_4

2. Výroková logika

2.1. Opakovanie: Výroková logika v prirodzenom jazyku

I.16 Opakovanie: Výroková logika v prirodzenom jazyku
 Výrok – veta, o pravdivosti ktorej má zmysel uvažovať (zväčša oznamovacia).
 Príklady 2.1.

- Miro je v posluchárni F1.
- Slnečná sústava má deviatu planétu.
- Mama upiekla koláč, ale Editka dostala z matematiky štvorku.
- · Niekto zhasol.

Negatívne príklady

- Toto je čudné.
- Píšte všetci modrým perom!

• Prečo je obloha modrá?

Výrokom priraďujeme pravdivostné hodnoty

I.17 Opakovanie: Výroková logika v prirodzenom jazyku

Operácie s výrokmi – *logické spojky*

- Vytvárajú nové výroky, zložené (súvetia).
- Majú povahu funkcií na pravdivostných hodnotách spájaných výrokov (boolovských funkcií), teda pravdivostná hodnota zloženého výroku závisí iba od pravdivostných hodnôt podvýrokov.

Príklad 2.2. Negácia, konjunkcia, disjunkcia, implikácia, ekvivalencia, ...

Negatívny príklad

Spojku "pretože" nepovažujeme za $logick\acute{u}$ spojku.

Pravdivostná hodnota výroku "Emka ochorela, pretože zjedla babôčku" sa nedá určiť funkciou na pravdivostných hodnotách spájaných výrokov.

I.18	(Meta) matematika výrokovej logiky	
------	------------------------------------	--

- Stredoškolský prístup príliš neoddeľuje samotný jazyk výrokovej logiky od jeho významu a vlastne ani jednu stránku nedefinuje jasne
- V tomto kurze sa budeme snažiť byť **presní**
 - ► Zdanlivo budeme o jednoduchých veciach hovoriť zložito
- Pojmy z výrokovej logiky budeme definovať matematicky
 - ▶ ako množiny, postupnosti, funkcie, atď. ← Matematika (1), (3)
- Na praktických cvičeniach veľa pojmov zadefinujete programátorsky
 - ▶ ako reťazce, slovníky, triedy a ich metódy
 ←-- Programovanie
 (1), (2)
- Budeme sa pokúšať dokazovať ich vlastnosti

- Budeme teda hovoriť o formálnej logike pomocou matematiky, ktorá je ale sama postavená na logike v prirodzenom jazyku
- Matematickej logike sa preto hovorí aj *meta* matematika, matematika *o* logike (a v konečnom dôsledku aj o matematike)

2.2. Syntax výrokovej logiky

I.19 Svntax výrokovei logiky

- Syntax sú pravidlá budovania viet v jazyku
- Pri formálnych jazykoch sú popísané matematicky
- · Nedajte sa tým odradiť, nie je to oveľa iné ako programovanie
- Viac sa budete formálnymi jazykmi zaoberať na Úvode do teoretickej informatiky
- Naše definície vychádzajú prevažne z kníh [Smullyan, 1979] a [Švejdar, 2002]

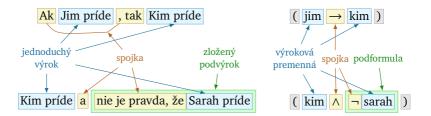
I.20 Svntax výrokovei logiky

Aké tvrdenia chceme zapisovať vo výrokovej logike?

- Jednoduché výroky, ktorých štruktúra nás nebude zaujímať
 - ▶ "Miro sa nachádza v F1", "Kim príde"

Ich formálnu verziu nazveme výrokové premenné

• Zložené výroky, tvorené podvýrokmi a spojkou:



Ich formálnu verziu nazveme formuly

- Čo sú základné stavebné kamene týchto výrokov?
 - ▶ jednoduché výroky a spojky

Tieto základné prvky nazveme symboly

I.21 Symboly jazyka výrokovej logiky

Definícia 2.3. Symbolmi jazyka výrokovej logiky sú:

- *výrokové premenné* z nejakej spočítateľnej množiny $\mathcal{V} = \{p_1, p_2, \ldots, p_n, \ldots\}$, ktorej prvkami nie sú symboly ¬, ∧, ∨, →, (a), ani jej prvky tieto symboly neobsahujú;
- logické symboly (logické spojky): ¬, ∧, ∨, →
 (nazývané, v uvedenom poradí, symbol negácie, symbol konjunkcie, symbol disjunkcie, symbol implikácie a čítané "nie", "a", "alebo", "ak ..., tak ...");
- pomocné symboly: (a) (ľavá zátvorka a pravá zátvorka).

Spojka ¬ je *unárna* (má jeden argument).

Spojky \land , \lor , \rightarrow sú *binárne* (spájajú dve formuly).

Poznámka 2.4. Definícia je záväzná dohoda o význame pojmov.

I.22 Symboly, výrokové premenné

Symbol je základný pojem, ktorý matematicky nedefinujeme (netvrdíme, že je to množina alebo podobne).

Je o čosi všeobecnejší ako pojem znak.

Príklad 2.5. Ako množinu výrokových premenných $\mathcal V$ môžeme zobrať všetky slová (teda konečné postupnosti) nad slovenskou abecedou a číslicami. Výrokovými premennými potom sú aj Jim, Kim, Sarah.

Dohoda

Výrokové premenné budeme označovať písmenami p, q, ..., podľa potreby aj s dolnými indexmi.

Výrokové premenné formalizujú jednoduché výroky.

- Povedzme, že máme množinu výrokových premenných $\mathcal{V} = \{\text{kim, jim, sarah}\}$
- Ako môžu vyzerať formuly vybudované nad touto množinou?
 - Samotné premenné, napr. sarah.
 - Negácie premenných, napr. ¬sarah.
 - Premenné alebo aj ich negácie spojené spojkou, napr. (¬kim∨sarah).
 - Ale negovať a spájať spojkami môžeme aj zložitejšie formuly, napr.
 (¬(kim ∧ sarah) → (¬kim ∨ ¬sarah)).
- Ako presne popíšeme, čo je formula?

Induktívnou definíciou:

- 1. Povieme, čo sú základné formuly, ktoré sa nedajú rozdeliť na menšie formuly.
- 2. Opíšeme, ako sa z jednoduchších formúl skladajú zložitejšie.

1.24	Výrokové formuly	У
------	------------------	---

Definícia 2.6. Množina $\mathcal E$ všetkých *výrokových formúl* nad množinou výrokových premenných $\mathcal V$ je najmenšia množina postupností symbolov, pre ktorú platí:

- i. každá výroková premenná $p \in \mathcal{V}$ je výrokovou formulou z \mathcal{E} (hovoríme jej *atomická formula* alebo iba *atóm*);
- ii. ak A je výroková formula z \mathcal{E} , tak aj postupnosť symbolov $\neg A$ je výrokovou formulou z \mathcal{E} (*negácia* formuly A);
- iii. ak A a B sú výrokové formuly z \mathcal{E} , tak aj $(A \wedge B)$, $(A \vee B)$ a $(A \to B)$ sú výrokovými formulami z \mathcal{E} (konjunkcia, disjunkcia, implikácia formúl A a B).

Dohoda

Výrokové formuly skrátene nazývame iba *formuly* a označujeme ich veľkými písmenami A, B, C, X, Y, Z, podľa potreby aj s dolnými indexmi.

Príklad 2.7. Nech $\mathcal{V} = \{\text{kim, jim, sarah}\}.$

Ako vyzerá množina ${\mathcal E}$ všetkých výrokových formúl nad ${\mathcal V}$?

```
\mathcal{E} = \{\text{kim, jim, sarah,}\}
                                                                                          podľa (i)
         ¬kim, ¬iim, ¬sarah.
                                                                                          podľa (ii)
         (kim \wedge kim), (kim \wedge jim), (kim \wedge sarah),
                                                                                          podľa (iii) pre ∧
         (\text{kim} \land \neg \text{kim}), (\text{kim} \land \neg \text{jim}), (\text{kim} \land \neg \text{sarah}),
         (jim \land kim), (jim \land jim), (jim \land sarah),
         (jim \land \neg kim), (jim \land \neg jim), (jim \land \neg sarah),
         (\neg kim \land kim), (\neg kim \land jim), (\neg kim \land sarah), \dots,
         (\neg jim \land \neg sarah), \ldots,
                                                                                          podľa (iii) pre \rightarrow
         (sarah \lor (kim \rightarrow jim)), \ldots,
                                                                                          a potom pre V
         (\neg(kim \land sarah) \lor (\neg jim \rightarrow \neg sarah)), \ldots)
                                                                                          podľa (iii) pre \wedge,
                                                                                          \rightarrow, \vee
```

I.26 Vytvárajúca postupnosť

Definícia 2.8. *Vytvárajúcou postupnosťou* nad množinou výrokových premenných $\mathcal V$ je ľubovoľná konečná postupnosť postupností symbolov, ktorej každý člen je výroková premenná z $\mathcal V$, alebo má tvar $\neg A$, pričom A je nejaký predchádzajúci člen postupnosti, alebo má jeden z tvarov $(A \land B)$, $(A \lor B)$, $(A \to B)$, kde A a B sú nejaké predchádzajúce členy postupnosti.

Vytvárajúcou postupnosťou pre X je ľubovoľná vytvárajúca postupnosť, ktorej posledným prvkom je X.

Tvrdenie 2.9. Postupnosť symbolov A je formulou vtedy a len vtedy, keď existuje vytvárajúca postupnosť pre A.

I.27 Vytvárajúca postupnosť _____

Príklad 2.10. Nájdime vytvárajúcu postupnosť pre formulu (¬kim → (jim \lor sarah)).

II. prednáška

Sémantika výrokovej logiky

26. februára 2018

2.3. Sémantika výrokovej logiky

II.1 Sémantika výrokovej logiky

- Syntax jazyka výrokovej logiky hovorí iba tom, ako sa zapisujú formuly ako postupnosti symbolov.
- Samé o sebe tieto postupnosti nemajú žiaden ďalší význam.
- Ten im dáva sémantika jazyka výrokovej logiky.
- Za význam výrokov považujeme ich pravdivostnú hodnotu.

II.2 Ohodnotenie výrokových premenných

- Výrokové premenné predstavujú jednoduché výroky.
- Ich význam (pravdivosť) nie je pevne daný.
- Môže závisieť od situácie, stavu sveta (Sára ide na párty, svieti slnko, zobral som si čiapku, ...).
- Ako vieme *programátorsky* popísať pravdivosť výrokových premenných v nejakom stave sveta? A *matematicky*?

Definícia 2.11. Nech (t, f) je usporiadaná dvojica pravdivostných hodnôt, $t \neq f$, pričom hodnota t predstavuje pravdu a f nepravdu.

Ohodnotením množiny výrokových premenných $\mathcal V$ nazveme každé zobrazenie v množiny $\mathcal V$ do množiny $\{t,f\}$ (teda každú funkciu $v\colon \mathcal V\to \{t,f\}$).

Výroková premenná p je pravdivá pri ohodnotení v, ak v(p) = t.

Výroková premenná p je nepravdivá pri ohodnotení v, ak v(p) = f.

II.3 Ohodnotenie výrokových premenných

Príklad 2.12. Zoberme $t \neq f$ (napr. t = 1, f = 0), $\mathcal{V} = \{a, \acute{a}, \ddot{a}, \dots, \check{z}, 0, \dots, 9, _\}^+$. Dnešné ráno by popísalo ohodnotenie v_1 množiny \mathcal{V} , kde (okrem iného):

$$v_1(\text{svieti_slnko}) = t$$
 $v_1(\text{zobral_som_si_čiapku}) = f$

Pondelkové ráno pred týždňom opisuje ohodnotenie v_2 , kde okrem iného

$$v_2$$
(svieti slnko) = f v_2 (zobral som si čiapku) = f

Jednu zo situácií v probléme pozývania kamarátov na párty by popísalo ohodnotenie, v ktorom (okrem iného):

$$v_3(\text{sarah}) = t$$
 $v_3(\text{kim}) = f$ $v_3(\text{jim}) = t$

Prečo "okrem iného"?

Kde v informatickej praxi **nie je** f = 0 a t = 1?

II.4 Spĺňanie výrokových formúl

- Na formulu sa dá pozerať ako na podmienku, ktorú stav sveta buď spĺňa (je v tomto stave pravdivá) alebo nespĺňa (je v ňom nepravdivá).
- Z pravdivostného ohodnotenia výrokových premenných v nejakom stave sveta, vieme *jednoznačne* povedať, ktoré formuly sú v tomto stave splnené.

Príklad 2.13. Nech v_3 je ohodnotenie množiny $\mathcal{V} = \{a, \dots, z\}^+$, také že

$$v_3(\text{kim}) = t$$
 $v_3(\text{jim}) = f$ $v_3(\text{sarah}) = t$.

Spĺňa svet s týmto ohodnotením formulu (¬jim → ¬sarah)? Zoberieme vytvárajúcu postupnosť, prejdeme ju zľava doprava:

Formulu	jim	sarah	¬jim	¬sarah	$(\neg jim \rightarrow \neg sarah)$
ohodnotenie v_3	nespĺňa	spĺňa	spĺňa	nespĺňa	nespĺňa

II.5 Spĺňanie výrokových formúl – vytvárajúci strom

Príklad 2.13 (pokračovanie).

$$v_3(\text{kim}) = t$$
 $v_3(\text{jim}) = f$ $v_3(\text{sarah}) = t$.

Iná možnosť je použiť vytvárajúci strom:

$$(\neg \text{jim} \to \neg \text{sarah}) - v_3 \text{ nespĺňa}$$
 $v_3 \text{ spĺňa} - \neg \text{jim} - \neg \text{sarah} - v_3 \text{ nespĺňa}$
 $v_3 \text{ nespĺňa} - \neg \text{jim} - \neg \text{sarah} - v_3 \text{ spĺňa}$

- II.6 Spĺňanie výrokových formúl program
 - Proces zisťovania, či ohodnotenie spĺňa formulu, vieme naprogramovať:

```
def satisfies(v, A):
```

• Veľmi podobne vieme zadefinovať splnenie matematicky.

II.7 Spĺňanie výrokových formúl – definícia

Definícia 2.14. Nech $\mathcal V$ je množina výrokových premenných. Nech v je ohodnotenie množiny $\mathcal V$. Pre všetky výrokové premenné p z $\mathcal V$ a všetky formuly A, B nad $\mathcal V$ definujeme:

- v spĺňa atomickú formulu p vtt v(p) = t;
- v spĺňa formulu $\neg A$ vtt v nespĺňa A;
- v spĺňa formulu $(A \wedge B)$ vtt v spĺňa A a v spĺňa B;
- v spĺňa formulu $(A \lor B)$ vtt v spĺňa A alebo v spĺňa B;
- v spĺňa formulu $(A \rightarrow B)$ vtt v nespĺňa A alebo v spĺňa B.

Dohoda

- Skratka vtt znamená vtedy a len vtedy, keď.
- Vzťah ohodnotenie v spĺňa formulu X skrátene zapisujeme $v \models X$, ohodnotenie v nespĺňa formulu X zapisujeme $v \not\models X$.
- Namiesto v (ne)spĺňa X hovoríme aj X je (ne)pravdivá pri v.

Príklad 2.15. Nech v_3 je ohodnotenie množiny $\mathcal{V} = \{a, \dots, z\}^+$, také že

$$v_3(\text{kim}) = t$$
 $v_3(\text{jim}) = f$ $v_3(\text{sarah}) = t$.

Zistime, ktoré z formúl

$$((kim \lor jim) \lor sarah)$$

$$(kim \to \neg sarah) \qquad (jim \to kim) \qquad (\neg jim \to \neg sarah)$$

ohodnotenie v_3 spĺňa a ktoré nespĺňa.

deg(X)	v_3 spĺňa X	v_3 nespĺňa X
0	kim, sarah	jim
1	\neg jim, (kim \vee jim), (jim \rightarrow kim)	¬sarah
2	$((kim \lor jim) \lor sarah)$	$(kim \rightarrow \neg sarah)$
3		$(\neg jim \rightarrow \neg sarah)$

2.4. Tautológie, (ne)splniteľnosť, falzifikovateľnosť

II.9 Spĺňanie z hľadiska formuly

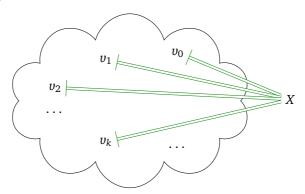
- Doteraz sme sa na spĺňanie pozerali z hľadiska **jedného ohodnotenia** (stavu sveta) a zisťovali sme, **ktoré formuly** sú v ňom splnené
- Obráťme teraz perspektívu: vyberme si jednu formulu a zisťujme, ktoré ohodnotenia ju spĺňajú, teda ktoré stavy sveta vyhovujú podmienke vyjadrenej formulou

Dohoda

V ďalších definíciách a tvrdeniach predpokladáme, že sme si *pevne zvolili* nejakú množinu výrokových premenných $\mathcal V$ a hodnoty t,f.

Formulou rozumieme formulu nad množinou výrok. prem. ${\mathcal V}.$

Ohodnotením rozumieme ohodnotenie množiny výrok. prem. $\mathcal V$.



Definícia 2.16. Formulu X nazveme tautológiou (skrátene $\models X$) vtt **každé** ohodnotenie výrokových premenných spĺňa X (teda **pre každé** ohodnotenie výrokových premenných v platí $v \models X$).

II.11 Tautológia — testovanie

- Ak máme nekonečne veľa výrokových premenných, máme aj nekonečne veľa ohodnotení
- Musíme skúmať **všetky**, aby sme zistili, či je formula *X* tautológiou?
- Platí

Tvrdenie 2.17. Splnenie výrokovej formuly pri ohodnotení výrokových premenných závisí iba od ohodnotenia (konečného počtu) výrokových premenných, ktoré sa v nej vyskytujú.

Presnejšie: Pre každú formulu X a všetky ohodnotenia v_1 a v_2 , ktoré zhodujú na množine v_1 výrokových premenných vyskytujúcich sa v X, platí $v_1 \models X$ vtt $v_2 \models X$.

- Takže stačí skúmať ohodnotenia, ktoré sa líšia na výrokových premenných vyskytujúcich sa v X, ktorých je iba konečne veľa
- Koľko je takých ohodnotení?

II.12 Tautológia — testovanie

Príklad 2.18. Zistime, či je $X = (\neg(p \land q) \rightarrow (\neg p \lor \neg q))$ tautológiou.

Preskúmame všetky rôzne ohodnotenia výrokových premenných, ktoré sa vyskytujú v X:

ι	,						
p	q	$(p \wedge q)$	$\neg(p \land q)$	$\neg p$	$\neg q$	$(\neg p \vee \neg q)$	$(\neg(p \land q) \to (\neg p \lor \neg q))$
t f	f	≠ ≠ ≠ =	= = = #	⊭ ⊨	 - - - -	= = = #	= = = =

Pretože všetky skúmané ohodnotenia spĺňajú *X*, je *X* tautológiou.

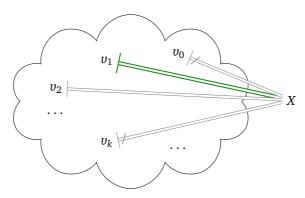
II.13 Ohodnotenia zhodujúce sa na premenných formuly

 $D\hat{o}kaz$. Indukciou na stupeň formuly X.

Báza: Nech X je stupňa 0. Podľa vety o jednoznačnosti rozkladu a definície stupňa musí byť X=p pre nejakú výrokovú premennú. Zoberme ľubovoľné ohodnotenia v_1 a v_2 , ktoré sa zhodujú na premenných v X, teda aj na p. Podľa definície spĺňania $v_1 \models p$ vtt $v_1(p) = t$ vtt $v_2(p) = t$ vtt $v_2 \models p$.

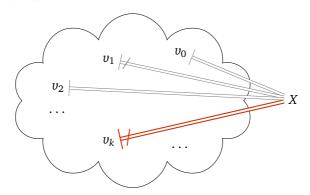
Krok: Nech X je stupňa n>0 a tvrdenie platí pre všetky formuly stupňa nižšieho ako n (indukčný predpoklad). Zoberme ľubovoľné ohodnotenia v_1 a v_2 , ktoré sa zhodujú na premenných v X. Podľa definície stupňa a jednoznačnosti rozkladu nastáva práve jeden z prípadov:

- *X* = ¬*A* pre práve jednu formulu *A*. Pretože deg(*X*) = deg(*A*) + 1 > deg(*A*), podľa ind. predpokladu tvrdenie platí pre *A*. Ohodnotenia *v*₁ a *v*₂ sa zhodujú na premenných v *A* (rovnaké ako v *X*). Preto *v*₁ |= *A* vtt *v*₂ |= *A*, a teda *v*₁ |= ¬*A* vtt *v*₁ |≠ *A* vtt *v*₂ |≠ *A* vtt *v*₂ |= ¬*A*.
- $X = (A \wedge B)$ pre práve jednu dvojicu formúl A, B. Pretože $\deg(X) = \deg(A) + \deg(B) + 1 > \deg(A)$ aj $\deg(B)$, podľa ind. predpokladu pre A aj B tvrdenie platí. Podobne pre ďalšie binárne spojky.

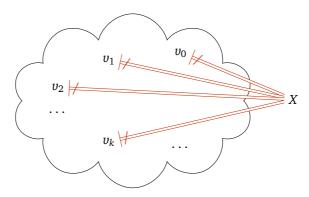


Definícia 2.19. Formulu X nazveme *splniteľnou* vtt **nejaké** ohodnotenie výrokových premenných **spĺňa** X (teda **existuje** také ohodnotenie výrokových premenných v, že $v \models X$).

II.15 Falzifikovateľnosť



Definícia 2.20. Formulu X nazveme falzifikovateľnou vtt **nejaké** ohodnotenie výrokových premenných **nespĺňa** X (teda **existuje** také ohodnotenie výrokových premenných v, že $v \not\models X$).



Definícia 2.21. Formulu X nazveme *nesplniteľnou* vtt **každé** ohodnotenie výrokových premenných **nespĺňa** X (teda **pre každé** ohodnotenie výrokových premenných v platí $v \not\models X$).

Splniteľné

Splniteľné

Splniteľné

Splniteľné aj falzifikovateľné

Nesplniteľné

- Tautológie sú výrokovologické pravdy. Sú zaujímavé najmä pre klasický pohľad na logiku ako skúmanie správneho usudzovania.
- Vo výpočtovej logike je zaujímavá splniteľnosť a konkrétne spĺňajúce ohodnotenia.

Obrázok podľa [Papadimitriou, 1994]

Zamyslite sa II.1

Ak formula nie je falzifikovateľná, je:

- A. splniteľná, B. nesplniteľná, C. tautológia.

III. prednáška

Vyplývanie, ekvivalentné úpravy

5. marca 2018

III.1 Tautológie a (ne)splniteľnosť

Tvrdenie 2.22. Formula X je tautológia vtt keď $\neg X$ je nesplniteľná.

 $D\hat{o}kaz$. (\Longrightarrow) Nech X je tautológia, teda je splnená pri každom ohodnotení výrokových premenných. To znamená, že $\neg X$ je nesplnená pri každom ohodnotení (podľa definície splnenia formuly ohodnotením), a teda $\neg X$ je nesplniteľná.

(\Leftarrow) Opačne, nech ¬X je nesplniteľná. To znamená, že pri každom ohodnotení výrokových premenných je ¬X nesplnená. Podľa definície spĺňania je teda X pri každom ohodnotení splnená, a teda je tautológia. □

III.2 Teórie

Neformálne slovom *teória* označujeme nejaký súbor presvedčení o fungovaní sveta alebo jeho časti.

Definícia 2.23. (Výrokovologickou) teóriou nazývame každú množinu formúl.

Dohoda

Teórie budeme označovať písmenami T, S, podľa potreby s indexmi.

Príklad 2.24. Formalizácia problému pozývania známych na párty je teóriou:

$$T_{\mathrm{party}} = \{ ((\mathrm{kim} \lor \mathrm{jim}) \lor \mathrm{sara}), \qquad (\mathrm{kim} \to \neg \mathrm{sara}),$$

$$(\mathrm{jim} \to \mathrm{kim}), \qquad (\neg \mathrm{jim} \to \neg \mathrm{sara}) \}$$

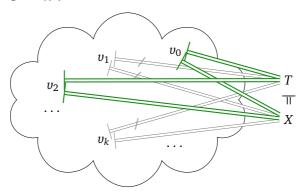
III.3 Splnenie teórie, model
III.3 Splnenie teórie, modelPojem spĺňania sa jednoducho rozšíri na teórie.
Definícia 2.25. Nech T je teória. Ohodnotenie v spĺňa teóriu T (skrátene $v \models T$) vtt v spĺňa každú formulu X z množiny T . Spĺňajúce ohodnotenie nazývame <i>modelom</i> teórie T .
Príklad 2.26. Aké ohodnotenie spĺňa (teda je modelom) T_{party} ?
Tvrdenie 2.27. Splnenie teórie T pri ohodnotení výrokových premenných závisí iba od ohodnotenia výrokových premenných, ktoré sa vyskytujú vo formulách v T.
Presná formulácia je podobná ako pri spĺňaní formúl. Dôkaz sporom, lebo množina formúl môže byť nekonečná.
2.5. Výrokovologické vyplývanie
III.4 Splniteľnosť teórie
• Kedy je teória "zlá"?
• Keď nepopisuje žiaden svet (stav sveta).
• "Dobrá" je teda taká teória, ktorá má aspoň jeden model.
Definícia 2.28. Teória T je súčasne výrokovologicky splniteľná (skrátene splniteľná) vtt existuje aspoň jeden model T . Teória je nesplniteľná vtt nie je splniteľná.
Príklad 2.29. T_{party} je súčasne splniteľná množina formúl. $T_{\text{party}} \cup \{\text{sara}\}$ je súčasne nesplniteľná množina formúl.
III.5 Logické dôsledky a vyplývanie
 Aký je účel teórií? Kedy je teória užitočná?
 Keď z nej dokážeme odvodiť (uvažovaním alebo počítaním) presentation> doteraz neznáme skutočnosti (teda nezapísané v teórii),
ktoré platia vo všetkých stavoch sveta spĺňajúcich teóriu.

• Takéto skutočnosti nazývame **logickými dôsledkami teórie** a hovoríme, že z nej *vyplývajú*.

Príklad 2.30. Všimnime si, že v každom ohodnotení, ktoré spĺňa T_{party} , je splnená aj premenná kim.

Ktorá ďalšia formula vyplýva z T_{party} ?

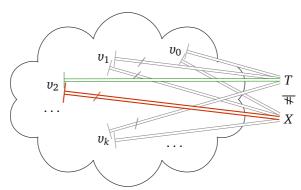
III.6 Výrokovologické vyplývanie



Definícia 2.31 (Výrokovologické vyplývanie). Z teórie T výrokovologicky vyplýva formula X

(tiež X je *výrokovologickým dôsledkom T*, skrátene $T \models X$) vtt každé ohodnotenie výrokových premenných, ktoré spĺňa T, spĺňa aj X.

III.7 Nevyplývanie



Príklad 2.32.	Ktoré atomické for	muly a ich	negácie i	nevyplývajú	z T_{party} ?
Vyplýva z 7	T _{party} formula (<i>kim</i> -	$\rightarrow jim)$?			

III.8 Vyplývanie a (ne)splniteľnosť

Použitie SAT solvera na rozhodovanie vyplývania je založené na:

Tvrdenie 2.33. Formula X výrokovologicky vyplýva z teórie T vtt množina $T_1 = T \cup \{\neg X\}$ je nesplniteľná.

Dôkaz. Nech $T = \{X_1, X_2, ..., X_n, ...\}.$

- (\Rightarrow) Predpokladajme, že X vyplýva z množiny T. Nech v je nejaké ohodnotenie \mathcal{V} . Potrebujeme ukázať, že v nespĺňa T_1 . Máme dve možnosti:
 - Ak v nespĺňa T, tak nespĺňa ani T_1 .
 - Ak *v* spĺňa *T*, tak *v* musí spĺňať aj *X* (definícia vyplývania). To znamená, že ¬*X* je nesplnená pri *v*, a teda *v* nespĺňa *T*₁.
- (⇐) Opačne, nech T_1 je nesplniteľná a nech v je nejaké ohodnotenie $\mathcal{V}.v$ teda nespĺňa T_1 . Potrebujeme ukázať, že ak v spĺňa T, tak potom v spĺňa aj X. Ak v spĺňa T, potom spĺňa každé X_i . Keďže ale v nespĺňa T_1 , v musí nespĺňať $\neg X$ (jediná zostávajúca formula z T_1), čo znamená, že v spĺňa X.

III.9 Nezávislosť

Definícia 2.34. Formula X je $nez ext{\'a}visl ext{\'a}$ od teórie T, ak existuje dvojica ohodnotení v_1, v_2 spĺňajúcich T, pričom v_1 spĺňa X, ale v_2 nespĺňa X.

Príklad 2.35. Ktorá atomická formula je nezávislá od T_{party} ? Je aj jej negácia nezávislá od T_{party} ?

III.10 Vzťahy vyplývania, implikácií a tautológií ______

Tvrdenie 2.36. Nech S a T sú teórie, $S \subseteq T$, A je formula. $Ak S \models A$, $tak T \models A$.

Tvrdenie 2.37. Nech T je teória, nech A, B, A_1 , A_2 , ..., A_n sú formuly.

- a) $T \cup \{A\} \models B \text{ vtt } T \models (A \rightarrow B)$.
- b) $\{\} \models A \text{ vtt } A \text{ je tautológia } (\models A).$
- c) Nasledujúce tvrdenia sú ekvivalentné:

i.
$$\{A_1, A_2, ..., A_n\} \models B$$

ii.
$$\{((\cdots (A_1 \wedge A_2) \wedge \cdots) \wedge A_n)\} \models B$$

iii.
$$\{\} \models ((\cdots (A_1 \land A_2) \land \cdots) \land A_n) \rightarrow B)$$

iv.
$$\models (((\cdots (A_1 \land A_2) \land \cdots) \land A_n) \rightarrow B)$$

III.11 Hlasujte

Spomeňte si III.1

Formula X vyplýva z teórie T vtt každý model T spĺňa X.

Pravda alebo nepravda?

2.6. Ekvivalencia formúl

III.12 Ekvivalencia formúl

Ako vieme pomocou doterajších **sémantických** pojmov vyjadriť, že dve formuly sú ekvivalentné?

Definícia 2.38. Dve formuly X a Y sú $(v\acute{y}rokovologicky)$ $ekvivalentné <math>(X \Leftrightarrow Y)$ vtt

pre každé ohodnotenie v výrokových premenných platí, že v spĺňa X vtt v spĺňa Y.

Ako súvisí takto sémanticky zadefinovaná ekvivalencia formúl so skratkou \leftrightarrow ? Podľa dohody z 2. prednášky je $(X \leftrightarrow Y)$ je skráteným zápisom $((X \to Y) \land (Y \to X))$.

Tvrdenie 2.39. Formuly X a Y sú výrokovologicky ekvivalentné vtt formula $(X \leftrightarrow Y)$ je tautológia.

III.13	Fkviva	lencia a	wh	ívanie
III.TO	EKVIVA	itiilla a	i vypi	/vallle

Ako súvisí ekvivalencia formúl s vyplývaním?

Tvrdenie 2.40. Formuly X a Y sú ekvivalentné vtt $\{X\} \models Y$ a $\{Y\} \models X$.

 $D\hat{o}kaz$. (\Longrightarrow) Nech X a Y sú ekvivalentné formuly. Chceme dokázať, že $\{X\} \models Y$, teda že (podľa definície vyplývania) pre každé ohodnotenie v platí, že ak $v \models \{X\}$, tak $v \models Y$.

Nech v je ľubovoľné ohodnotenie, nech $v \models \{X\}$. Potom $v \models X$ (podľa definície splnenia teórie), a teda $v \models Y$ (z predpokladu a podľa definície ekvivalencie). Teda platí, že ak $v \models \{X\}$, tak $v \models Y$. Pretože v bolo ľubovoľné, môžeme túto vlastnosť zovšeobecniť na všetky ohodnotenia, a teda $\{X\} \models Y$.

Dôkaz $\{Y\} \models X$ je podobný.

(⇐) Nech X a Y sú formuly a nech $\{X\} \models Y$ a $\{Y\} \models X$. Chceme dokázať, že X a Y sú ekvivalentné.

Nech v je ľubovoľné ohodnotenie. Ak $v \models X$, tak $v \models \{X\}$ a podľa prvého predpokladu $v \models Y$. Ak $v \models Y$, tak $v \models \{Y\}$ a podľa druhého predpokladu $v \models X$. Teda $v \models X$ vtt $v \models Y$. Pretože v bolo ľubovoľné, môžeme túto vlastnosť zovšeobecniť na všetky ohodnotenia, a teda X a Y sú ekvivalentné. \Box

III.14	Tranzitivita ekvivalencie	
--------	---------------------------	--

Tvrdenie 2.41 (Tranzitivita ekvivalencie). *Nech X, Y a Z sú formuly.* Ak X je ekvivalentná s Y a Y je ekvivalentná so Z, tak X je ekvivalentná so Z.

 $D\hat{o}kaz$. Nech X, Y a Z sú formuly. Nech X je ekvivalentná sY a Y je ekvivalentná so Z. Nech v je ľubovoľné ohodnotenie.

Ak $v \models X$, tak $v \models Y$ podľa prvého predpokladu, a teda $v \models Z$ podľa druhého predpokladu.

Nezávisle od toho, ak $v \models Z$, tak $v \models Y$ podľa druhého predpokladu, a teda $v \models X$ podľa prvého predpokladu.

Preto $v \models X$ vtt $v \models Z$. Zovšeobecnením na všetky ohodnotenia dostávame, že X a Z sú ekvivalentné.

2.6.1. Ekvivalentné úpravy

III.15 Ekvivalentné úpravy

- Už ste určite ekvivalente upravovali formuly
- Aké kroky ste pri tom robili?

Príklad 2.42.
$$A = \neg \neg (r \land q)$$
 $B = (r \land q)$ $X = (p \rightarrow \neg \neg \neg (r \land q))$
$$\cline{} \cline{} \$$

Nahradenie podformuly A vo formule X formulou B, ktorá je ekvivalentná s A

III.16 Pravidlá ekvivalentných úprav

- Ako vieme, že *A* a *B* sú ekvivalentné?
 - Môžeme odvodiť sémanticky
 - Naozaj ste dosadili $(r \land q)$ za pv známej ekvivalencii medzi $\neg \neg p$ a p (princíp dvojitej negácie)

III.17 Korektnosť ekvivalentných úprav

- Prečo sú tieto úpravy korektné (správne)?
- Teda:
 Prečo, ak je C ekvivalentné s D,
 tak je aj A ekvivalentné s B a X ekvivalentné s Y?



Oba druhy dosadení pri ekvivalentných úpravách sú substitúcie

Definícia 2.44 (Substitúcia). Nech *X*, *A*, *B* sú formuly.

Substitúciou B za A v X (skrátene X[A|B])) nazývame formulu, ktorá vznikne nahradením každého výskytu A v X formulou B.

Substitúciu si vieme predstaviť ako cyklus prechádzajúci cez X

```
nech \ell je dĺžka A kým nie si na konci X:

ak sa nasledujúcich \ell symbolov zhoduje s A:

nahraď ich za B

pokračuj za posledným nahradeným symbolom

inak:

pokračuj ďalším symbolom
```

alebo ako rekurzívne definovanú operáciu:

(cv02)

Pre všetky formuly A, B, X, Y, všetky výrokové premenné p a všetky binárne spojky $b \in \{\land, \lor, \rightarrow\}$:

$$A[A|B] = B$$

$$p[A|B] = p$$

$$(\neg X)[A|B] = \neg (X[A|B])$$

$$(X b Y)[A|B] = ((X[A|B]) b (Y[A|B]))$$

$$ak A \neq \neg X$$

$$ak A \neq (X b Y)$$

III.19 Korektnosť ekvivalentných úprav

Korektnosť ekvivalentných úprav vyjadrujú nasledujúce tvrdenia:

Tvrdenie 2.45 (Dosadenie do ekvivalentných formúl). *Nech A a B sú navzájom ekvivalentné formuly, p je výroková premenná a Y je formula. Potom formuly A[p|Y] a B[p|Y] sú ekvivalentné.*

Veta 2.46 (Ekvivalentné úpravy). *Nech X je formula, A a B sú ekvivalentné formuly.*

Potom formuly X a X[A|B] sú tiež ekvivalentné.

Obe tvrdenia o korektnosti sú dôsledkami nasledujúcej lemy:

Lema 2.47. Nech X je výroková formula, p je výroková premenná, A je formula a v je ohodnotenie výrokových premenných.

Potom $v \models X[p|A]$ vtt $v_{p|A} \models X$, kde $v_{p|A}$ je ohodnotenie, pre ktoré platí:

- $v_{p|A}(r) = v(r)$, ak r je výroková premenná a $p \neq r$;
- $v_{p|A}(p) = t$, $ak \ v \models A$;
- $v_{p|A}(p) = f$, $ak \ v \not\models A$.

O jej platnosti sa môžeme presvedčiť indukciou na stupeň formuly *X*.

III.21 Ekvivalencie pre ekvivalentné úpravy

Veta 2.48. Nech A, B a C sú ľubovoľné formuly, \top je ľubovoľná tautológia a \bot je ľubovoľná nesplniteľná formula.

Nasledujúce dvojice formúl sú ekvivalentné:

$$(A \land (B \land C)) \ a \ ((A \land B) \land C) \qquad asociatívnosť \\ (A \lor (B \lor C)) \ a \ ((A \lor B) \lor C) \qquad komutatívnosť \\ (A \land B) \ a \ (B \land A) \qquad komutatívnosť \\ (A \lor B) \ a \ (B \lor A) \qquad distributívnosť \\ (A \land (B \lor C)) \ a \ ((A \land B) \lor (A \land C)) \qquad distributívnosť \\ (A \lor (B \land C)) \ a \ ((A \lor B) \land (A \lor C)) \qquad de \ Morganove \\ \neg (A \land B) \ a \ (\neg A \lor \neg B) \qquad pravidlá \\ \neg \neg A \ a \ A \qquad dvojitá negácia$$

III.22 Ekvivalencie pre ekvivalentné úpravy

Veta 2.48 (Pokračovanie).

$$(A \land A) \ a \ A \qquad idempotencia$$

$$(A \lor A) \ a \ A \qquad identita$$

$$(A \lor \bot) \ a \ A \qquad identita$$

$$(A \lor \bot) \ a \ A \qquad absorpcia$$

$$(A \lor (A \lor B)) \ a \ A \qquad absorpcia$$

$$(A \lor \neg A) \ a \ \top \qquad vylúčenie \ tretieho$$

$$(A \land \neg A) \ a \ \bot \qquad spor$$

$$(A \to B) \ a \ (\neg A \lor B) \qquad nahradenie \to$$

2.6.2. Konjunktívna a disjunktívna normálna forma

III.23 Konjunkcia a disjunkcia postupnosti formúl

Dohoda

Nech $A_1, A_2, ..., A_n$ je konečná postupnosť formúl.

- Konjunkciu postupnosti formúl A_1, \ldots, A_n , teda $(((A_1 \wedge A_2) \wedge A_3) \wedge \cdots \wedge A_n)$, skrátene zapisujeme $(A_1 \wedge A_2 \wedge A_3 \wedge \cdots \wedge A_n)$, prípadne $\bigwedge_{i=1}^n A_i$.
 - Konjunkciu *prázdnej* postupnosti formúl (n=0) označujeme \top . Chápeme ju ako ľubovoľnú tautológiu, napríklad ($p_1 \lor \neg p_1$).
- Disjunkciu postupnosti formúl A₁, ..., A_n, teda (((A₁ ∨ A₂) ∨ A₃) ∨ ··· ∨ A_n), skrátene zapisujeme (A₁ ∨ A₂ ∨ A₃ ∨ ··· ∨ A_n), prípadne ∨ⁿ_{i=1} A_i.
 - Disjunkciu *prázdnej* postupnosti formúl označujeme \bot alebo \Box . Chápeme ju ako ľubovoľnú nesplniteľnú formulu, napríklad $(p_1 \land \neg p_1)$.
- Pre n = 1 chápeme samotnú formulu A_1 ako konjunkciu aj ako disjunkciu jednoprvkovej postupnosti formúl A_1 .

- **Definícia 2.49.** Výrokovú premennú alebo negáciou premennej nazývame *literál*.
 - Disjunkciu literálov nazývame klauzula (tiež "klauza").
 - Hovoríme, že formula *X* je v *konjunktívnom normálnom tvare* (CNF), ak *X* je *konjunkciou* klauzúl.
 - Hovoríme, že formula *X* je v *disjunktívnom normálnom tvare* (DNF), ak *X* je *disjunkciou* formúl, z ktorých každá je konjunkciou literálov.

Príklad 2.50. Ktoré z nasledujúcich formúl sú literálmi, klauzulami, sú v CNF, v DNF:

$$A_{1} = p \qquad \qquad A_{6} = ((p \land \neg q) \lor (\neg p \land r) \lor (\neg p \land q \land \neg r))$$

$$A_{2} = \neg q \qquad \qquad A_{7} = ((\neg p \lor q \lor \neg r) \land (q \to r))$$

$$A_{3} = \square \qquad \qquad A_{8} = ((\neg p \lor \neg q) \land (p \lor r) \land (p \lor q \lor \neg r))$$

$$A_{4} = (p \lor \neg q) \qquad \qquad A_{9} = ((\neg p \lor (p \land r)) \land (p \lor q \lor \neg r))$$

$$A_{5} = (p \land \neg q) \qquad \qquad A_{10} = ((\neg p \lor p \lor r) \land (\neg (p \lor q) \lor \neg r))$$

IV. prednáška

CNF. Tablový kalkul

12. marca 2018

IV.1	Existencia DNF a CNF
Veta	2.51. 1. Ku každej formule X existuje ekvivalentná formula D v disjunktívnom normálnom tvare.
2.	. Ku každej formule X existuje ekvivalentná formula C v konjunktívnom normálnom tvare.
Dôko	v_i z. 1. Zoberme všetky ohodnotenia v_1, \ldots, v_n také, že $v_i \models X$ a $v_i(q) = f$ pre všetky premenné $q \notin \text{vars}(X)$. Pre každé v_i zostrojme formulu C_i ako konjunkciu obsahujúcu p , ak $v_i(p) = t$, alebo $\neg p$, ak $v_i(p) = f$, pre každú $p \in \text{vars}(X)$. Očividne formula $D = \bigvee_{1 \leq i \leq n} C_i$ je v DNF a je ekvivalentná s X (vymenúva všetky možnosti, kedy je X splnená).
2	. K $\neg X$ teda existuje ekvivalentná formula D v DNF. Znegovaním D a aplikáciou de Morganových pravidiel dostaneme formulu C v CNF, ktorá je ekvivalentná s X .
IV.2	CNF — trochu lepší prístup
•	Skúmanie všetkých ohodnotení nie je ideálny spôsob ako upraviť formulu do CNF — najmä keď má veľa premenných a jej splniteľnosť chceme rozhodnúť SAT solverom.
•	Je nejaký lepší systematický postup?
•	Všimnime si:
	CNF je konjunkcia disjunkcií literálov – výrokových premenných alebo ich negácií
	Teda:

- CNF neobsahuje implikácie ako sa ich zbavíme?
- Negácia sa vyskytuje iba pri výrokových premenných ako ju tam dostaneme, ak to tak nie je (napr. \neg (*A* ∨ *B*))?
- Disjunkcie sa nachádzajú iba vnútri konjunkcií ako presunieme "vonkajšie" disjunkcie "dovnútra" konjunkcií (napr. (A ∨ (B ∧ C)))?

IV.3 CNF — trochu lepší prístup

Algoritmus CNF₁

- 1. Nahradíme implikáciu disjunkciou:
 - $(A \to B) \Leftrightarrow (\neg A \lor B)$.
- 2. Presunieme dovnútra pomocou de Morganových pravidiel a dvojitej negácie.
- 3. "Roznásobíme" ∧ s ∨ podľa distributívnosti a komutatívnosti:
 - $(A \lor (B \land C)) \Leftrightarrow ((A \lor B) \land (A \lor C))$
- 4. Prezátvorkujeme na požadovaný tvar pomocou asociatívnych pravidiel.

Tvrdenie 2.52. *Výsledná formula alg. CNF*₁ *je ekvivalentná s pôvodnou a je v CNF.*

IV.4 CNF – trochu lepší prístup

Príklad 2.53. 1.
$$((a \lor \neg b) \rightarrow \neg (c \lor (d \land \neg e)))$$

- 2. $(\neg (a \lor \neg b) \lor \neg (c \lor (d \land \neg e)))$ [1 nahradenie implikácie]
- 3. $((\neg a \land \neg \neg b) \lor \neg (c \lor (d \land \neg e)))$ [2 deMorganovo pravidlo]
- 4. $((\neg a \land b) \lor \neg (c \lor (d \land \neg e)))$ [2 dvojitá implikácia]
- 5. $((\neg a \land b) \lor (\neg c \land \neg (d \land \neg e)))$ [2 deMorganovo pravidlo]

6. $((\neg a \land b) \lor (\neg c \land (\neg d \lor \neg \neg e)))$

[2 — deMorganovo pravidlo]

7. $((\neg a \land b) \lor (\neg c \land (\neg d \lor e)))$

- [2 dvojitá implikácia]
- 8. $(((\neg a \land b) \lor \neg c) \land ((\neg a \land b) \lor (\neg d \lor e)))$
- [3 distributívnosť]

[3]

9.
$$(((\neg a \lor \neg c) \land (b \lor \neg c)) \land ((\neg a \lor (\neg d \lor e)) \land (b \lor (\neg d \lor e))))$$

10.
$$((\neg a \lor \neg c) \land (b \lor \neg c) \land (\neg a \lor (\neg d \lor e)) \land (b \lor (\neg d \lor e)))$$
 [4]

11.
$$((\neg a \lor \neg c) \land (b \lor \neg c) \land (\neg a \lor \neg d \lor e) \land (b \lor \neg d \lor e))$$
 [4 – asoc.]

IV.5 CNF – prečo iba trochu lepší prístup

Distribúcia ∨ cez ∧ spôsobuje nárast formuly:

- $A_2 = ((p_1 \land q_1) \lor (p_2 \land q_2))$ $C_2 = ((p_1 \lor p_2) \land (p_1 \lor q_2) \land (q_1 \lor p_2) \land (q_1 \lor p_2))$ $A_2 \Leftrightarrow C_2, \deg(A_2) = 3, \deg(B_2) = 7$
- $A_3 = ((p_1 \land q_1) \lor (p_2 \land q_2) \lor (p_3 \land q_3))$ $C_3 = ((p_1 \lor p_2 \lor p_3) \land (p_1 \lor q_2 \lor p_3) \land (q_1 \lor p_2 \lor p_3) \land (q_1 \lor p_2 \lor p_3) \land$ $(p_1 \lor p_2 \lor q_3) \land (p_1 \lor q_2 \lor q_3) \land (q_1 \lor p_2 \lor q_3) \land (q_1 \lor p_2 \lor q_3)) \land A_3 \Leftrightarrow C_3,$ $\deg(A_3) = 5, \qquad \deg(C_3) = 23$
- A_n = ((p₁ ∧ q₁) ∨ · · · ∨ (p_n ∧ q_n))
 Koľko klauzúl bude obsahovať C_n?
 Akého bude stupňa?

IV.6 CNF — obmedzenie exponenciálneho rastu __

Otázka. Dá sa vyhnúť exponenciálnemu nárastu formuly $A_n = ((p_1 \land q_1) \lor \cdots \lor (p_n \land q_n))$ kvôli distributívnosti?

- 1. Zoberme nové výrokové premenné r_1, \ldots, r_n, s
- 2. Vyjadrime, že r_i je ekvivalentným zástupcom konjunkcie $(p_i \land q_i)$: $(r_i \leftrightarrow (p_i \land q_i))$

- 3. Použime r_i na vyjadrenie, že s je ekvivalentným zástupcom disjunkcie A_n : $(s \leftrightarrow (r_1 \lor \cdots \lor r_n))$
- 4. A_n teda môžeme nahradiť formulou $((s \leftrightarrow (r_1 \lor \cdots \lor r_n)) \land (r_1 \leftrightarrow (p_1 \land q_1)) \land \cdots \land (r_n \leftrightarrow (p_n \land q_n)) \land s)$

Ekvivalentnými úpravami \circ prvý konjunkt upravíme na n+1 klauzúl, \circ spolu iba 4 dalších n na 3 klauzuly každý

IV.7 CNF — Cejtinova transformácia

Cejtinova transformácia (angl. Tseytin transformation)

- algoritmus nájdenia CNF použitím tohto princípu na všetky podformuly
- výsledok Cejtinovej transformácia T(X) nie je ekvivalentný s X,
 iba ekvisplniteľný: formula T(X) je splniteľná vtt X je splniteľná

2.7. Kalkuly

IV.8 Dokazovanie ekvivalencie syntakticky vs. sémanticky

- Pomocou substitúcie ekvivalentných formúl vieme dokázať, že dve formuly sú ekvivalentné bez toho, aby sme vyšetrovali všetky ohodnotenia ich výrokových premenných.
- Výhodné pri formulách s veľkým počtom premenných.
- Formulu $X = ((a \lor \neg b) \to \neg(c \lor (d \land \neg e)))$ sme upravili do CNF $Y = ((\neg a \lor \neg c) \land (b \lor \neg c) \land (\neg a \lor \neg d \lor e) \land (b \lor \neg d \lor e))$ pomocou 12 substitúcií ekvivalentných podformúl.
- Zároveň sme dokázali, že *X* a *Y* sú ekvivalentné.
- Na dôkaz ich ekvivalencie tabuľkovou metódou by sme potrebovali vyšetriť 32 prípadov.

- Tabuľková metóda je sémantická
 - využíva ohodnotenia výrokových premenných a spĺňanie formúl ohodnoteniami
- Substitúcie ekvivalentných formúl sú syntaktickou metódou
 - pracujú iba s postupnosťami symbolov, nie s ohodnoteniami
- Navyše sú deduktívnou metódou
 - odvodíme iba formuly ekvivalentné s pôvodnou

iv.10 Kaikuly — dokazovanie vyplyvania syntakticky	IV.10	Kalkuly – dokazovanie vyplývania syntakticky	
--	-------	--	--

- Ak začneme nejakou formulou a budeme substituovať ekvivalentné podformuly, dostávame postupne rôzne formuly, ktoré sú ale stále ekvivalentné s pôvodnou formulou.
- Čo keby sme začali s tautológiou?
 - Dostávame stále tautológie.
- Logiku viac zaujíma vyplývanie ako ekvivalencia a tautológie
- Vyplývanie dôsledkov z teórií sme doteraz dokazovali sémanticky vyšetrovaním všetkých ohodnotení.
- Na tento účel ale existujú aj syntaktické metódy kalkuly.
- Ukážeme si dva kalkuly:
 tablový stromový, prirodzenejší
 rezolvenciu lineárny, strojový

2.8. Tablový kalkul

IV.11 Dôkaz vyplývania sporom v slovenčine

Príklad 2.54. Dokážme, že z $T'_{party} = \{ (kim \rightarrow (jim \land \neg sarah)), (eva \rightarrow kim) \}$ vyplýva (sarah $\rightarrow \neg eva$). Poďme na to sporom:

Predpokladajme, že existuje také ohodnotenie v,

že $v \models T'_{\text{party}}$, teda (1) $v \models (kim \rightarrow (jim \land \neg sarah))$ a (2) $v \models (eva \rightarrow kim)$, ale pritom (3) $v \not\models (sarah \rightarrow \neg eva)$.

Podľa definície splnenia implikácie z faktu (3) vyplýva, že (4) $v \models sarah$ a zároveň (5) $v \not\models \neg eva$. Z (5) dostávame, že (6) $v \models eva$.

Podľa (2) máme dve možnosti: (7) $v \not\models eva$ alebo (8) $v \models kim$. Možnosť (7) je v spore s (6).

Platí teda (8) a podľa (1) ďalej môžu nastať dva prípady: (9) $v \not\models kim$, ktorý je však v spore s (8), alebo (10) $v \models (jim \land \neg sarah)$. V tom prípade (11) $v \models jim$ a (12) $v \models \neg sarah$, čiže (13) $v \not\models sarah$, čo je zase v spore s (4).

Vo všetkých prípadoch sme prišli k sporu, predpoklad je teda neplatný a každé ohodnotenie, ktoré spĺňa T'_{party} , spĺňa aj $(sarah \rightarrow \neg eva)$.

IV.12 Tablová notácia pre dôkazy

Dôkaz stručne zapíšeme v tablovej notácii:

- TX označuje fakt, že v spĺňa X.
- **F** *X* označuje fakt, že *v* nespĺňa *X*.
- Ak z niektorého predchádzajúceho faktu o formule X priamo z definície spĺňania vyplýva (ne)splnenie niektorej priamej podformuly X, zapíšeme ho do ďalšieho riadka.

Poznačíme si k nemu písmeno α a číslo zdrojového faktu.

Ak z niektorého faktu o formule *X* vyplýva
o jej *priamych podformulách* fakt *F*₁ alebo fakt *F*₂,
rozdelíme úvahu na dve nezávislé vetvy,
pričom prvá začne faktom *F*₁ a druhá faktom *F*₂.
K obom si poznačíme písmeno β a číslo zdrojového faktu.

 Ak nastane spor medzi splnením a nesplnením tej istej formuly, pridáme riadok so symbolom *
 a poznačíme si čísla faktov, ktoré sú v spore.

IV.13 Dôkaz vyplývania sporom v tablovej notácii								
Príklad	Príklad 2.55.							
(1)	T(kim → (jim	. ∧ ¬s	arah))				z T' _{party}
(2)		T(eva —	→ kim))				z T' _{party}
(3)		F(sarah -	$\rightarrow \neg ev$	a)				dôkaz
(4)		Т	. ~ l.					sporom
(4)		T sar	an					$\alpha(3)$
(5)		$\mathbf{F} \neg e$	va					$\alpha(3)$
(6)		T ev	a					$\alpha(5)$
(7)	F eva	β(2)	(8)		T <i>k</i>	im		β(2)
	*	(6) a (7)	(9)	F kim	β(1)	(10)	$T(jim \land \neg sarah)$	β(1)
				*	(8) a (9)	(11)	T jim	$\alpha(10)$
						(12)	T ¬sarah	$\alpha(10)$
						(13)	F sarah	$\alpha(12)$
							*	(4) a (13)
						-		

IV.14 Spĺňanie a priame podformuly __

Pozorovanie 2.56. Nech v je ľubovoľné ohodnotenie výrokových premenných. Nech X a Y sú ľubovoľné formuly.

- 1. T) $Ak v spĺňa \neg X$, tak v nespĺňa X.
 - F) Ak v nespĺňa $\neg X$, tak v spĺňa X.
- 2. T) Ak v spĺňa $(X \wedge Y)$, tak v spĺňa X a v spĺňa Y.
 - F) Ak v nespĺňa $(X \wedge Y)$, tak v nespĺňa X alebo v nespĺňa Y.
- 3. T) Ak v spĺňa $(X \vee Y)$, tak v spĺňa X alebo v spĺňa Y.
 - F) Ak v nespĺňa $(X \vee Y)$, tak v nespĺňa X a v nespĺňa Y.
- 4. T) Ak v spĺňa $(X \rightarrow Y)$, tak v nespĺňa X alebo v spĺňa Y.
 - F) Ak v nespĺňa $(X \to Y)$, tak v spĺňa X a v nespĺňa Y.

Definícia 2.57. Nech X je formula výrokovej logiky. Postupnosti symbolov **T**X a **F**X nazývame *označené formuly*.

Definícia 2.58. Nech v je ohodnotenie výrokových premenných a X je formula. Potom

- v spĺňa TX vtt v spĺňa X;
- v spĺňa F X vtt v nespĺňa X.

Dohoda

Pre označené formuly budeme používať veľké písmená zo začiatku a konca abecedy s horným indexom + a prípadne s dolnými indexmi, napr. A^+ , X_7^+ .

Pre množiny označených formúl budeme používať písmená S, T s horným indexom + a prípadne s dolnými indexmi, napr. S^+ , T_3^+ .

IV.16 Tablové pravidlá

Podľa pozorovania 2.56 a definície 2.58 môžeme sformulovať pravidlá pre označené formuly:

Definícia 2.59 (Jednotný zápis označených formúl typu α).

Označená formula A^+ je typu α vtt má jeden z tvarov v ľavom stĺpci tabuľky pre nejaké formuly X a Y. Takéto formuly budeme označovať písmenom α ; α_1 bude označovať príslušnú označenú formulu zo stredného stĺpca, α_2 príslušnú formulu z pravého stĺpca.

_	α	α_1	α_2
	$\mathbf{T}(X \wedge Y)$	$\mathbf{T}X$	$\mathbf{T}Y$
	$\mathbf{F}(X \vee Y)$	$\mathbf{F}X$	$\mathbf{F} Y$
	$\mathbf{F}(X \to Y)$	$\mathbf{T}X$	$\mathbf{F}Y$
	$\mathbf{T} \neg X$	$\mathbf{F}X$	$\mathbf{F}X$
	$\mathbf{F} \neg X$	$\mathbf{T}X$	$\mathbf{T}X$

Pozorovanie 2.60 (Stručne vďaka jednotnému zápisu). *Nech v je ľubovoľné ohodnotenie výrokových premenných.* Potom v spĺňa α vtt v spĺňa α_1 a v spĺňa α_2 .

IV.18 Jednotný zápis označených formúl typu β

Definícia 2.61 (Jednotný zápis označených formúl typu β).

Označená formula B^+ je $typu\ \beta$ vtt má jeden z tvarov v ľavom stĺpci tabuľky pre nejaké formuly X a Y. Takéto formuly budeme označovať písmenom β ; β_1 bude označovať príslušnú označenú formulu zo stredného stĺpca, β_2 príslušnú formulu z pravého stĺpca.

β	eta_1	eta_2
$\mathbf{F}(X \wedge Y)$	$\mathbf{F}X$	$\mathbf{F} Y$
$\mathbf{T}(X \vee Y)$	$\mathbf{T}X$	$\mathbf{T}Y$
$\mathbf{T}(X \to Y)$	$\mathbf{F}X$	$\mathbf{T}Y$

Pozorovanie 2.62 (Stručne vďaka jednotnému zápisu). Nech v je ľubovoľné ohodnotenie výrokových premenných. Potom v spĺňa β vtt v spĺňa β_1 alebo v spĺňa β_2 .

IV.19 Tablo pre množinu označených formúl

D-C-/--- 0.60 A 1.11/.11

Definícia 2.63. *Analytické tablo pre množinu označených formúl* S^+ (skrátene *tablo pre* S^+) je binárny strom, ktorého vrcholy obsahujú označené formuly a ktorý je skonštruovaný podľa nasledovných rekurzívnych pravidiel:

• Strom s jediným vrcholom (koreňom) obsahujúcim niektorú označenú formulu A^+ z S^+ je tablom pre S^+ .

- Nech \mathcal{T} je tablo pre S^+ a y je nejaký jeho list. Potom tablom pre S^+ je aj každé *priame rozšírenie* \mathcal{T} ktoroukoľvek z operácií:
 - A: Ak sa na vetve π_y (ceste z koreňa do y) vyskytuje nejaká označená formula α , tak ako jediné dieťa y pripojíme nový vrchol obsahujúci α_1 alebo α_2 .
 - B: Ak sa na vetve π_y vyskytuje nejaká označená formula β , tak ako deti y pripojíme dva nové vrcholy, pričom ľavé dieťa bude obsahovať β_1 a pravé β_2 .
 - S^+ : Ako jediné dieťa y pripojíme nový vrchol obsahujúci ľubovoľnú označenú formulu $A^+ \in S^+$.

Nič iné nie je tablom pre S^+ .

IV.20 Tablá, tablové pravidlá, operácie rozšírenia

Pravidlá a označené formuly v nich Operácia priameho rozšírenia α α_1 α_2 $\mathbf{T}(X \wedge Y)$ $\mathbf{T}X$ $\mathbf{T}Y$ $\mathbf{F}(X \vee Y)$ $\mathbf{F}X$ $\mathbf{F}Y$ $\mathbf{F}(X \to Y)$ $\mathbf{T}X$ $\mathbf{F}Y$ $\mathbf{T} \neg X$ $\mathbf{F}X$ $\mathbf{F}X$ $\mathbf{F} \neg X$ $\mathbf{T}X$ $\mathbf{T}X$ $i \in \{1,2\}$ \mathcal{T} $\mathbf{F}Y$ $\mathbf{T}(X \vee Y)$ $\mathbf{T}Y$

 $T(X \rightarrow Y)$

 $\mathbf{F}X$

 $\mathbf{T}Y$

Legenda: y je list v table \mathcal{T} , π_v je cesta od koreňa k y

IV.21 Uzavretosť a otvorenosť vetvy a tabla

Definícia 2.64. *Vetvou* tabla \mathcal{T} je každá cesta od koreňa \mathcal{T} k niektorému listu \mathcal{T} .

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

Definícia 2.65. Vetva π tabla $\mathcal T$ je uzavretá vtt

na π sa súčasne vyskytujú označené formuly **F** X a **T** X pre nejakú formulu X. Inak je π otvorená.

Tablo \mathcal{T} je uzavreté vtt každá jeho vetva je uzavretá.

Naopak, \mathcal{T} je otvorené vtt aspoň jedna jeho vetva je otvorená.

2.8.1. Korektnosť

V.22	Korektnosť tablového kalkulu
Korek	tnosť (angl. soundness) kalkulu neformálne:

Ak v kalkule dokážeme nejaké tvrdenie, tak to tvrdenie je naozaj pravdivé.

Veta 2.66 (Korektnosť tablového kalkulu). Nech S^+ je množina označených formúl a $\mathcal T$ je uzavreté tablo pre S^+ .

Potom je množina S^+ nesplniteľná.

Dôsledok 2.67. Nech S je množina formúl a X je formula. Ak existuje uzavreté tablo pre $\{TA \mid A \in S\} \cup \{FX\}$ (skr. $S \vdash X$), tak z S vyplýva X $(S \models X)$.

Dôsledok 2.69. *Nech X je formula.*

Ak existuje uzavreté tablo pre $\{FX\}$ (skr. $\vdash X$), tak X je tautológia $(\models X)$.

V. prednáška

Korektnosť a úplnosť tablového kalkulu

19. marca 2018

V.1	Korektnosť — splnenie priameho rozšírenia tabla
Na o	lôkaz korektnosti potrebujeme pomocnú definíciu a dve lemy.

Definícia 2.70. Nech S^+ je množina označených formúl, nech \mathcal{T} je tablo pre S^+ a nech v je ohodnotenie množiny výrokových premenných. Potom:

- υ spĺňa vetvu π v table T vtt
 υ spĺňa všetky označené formuly vyskytujúce sa na na vetve π.
- v spĺňa tablo \mathcal{T} vtt v spĺňa niektorú vetvu v table \mathcal{T} .

Lema 2.71 (K1). Nech S^+ je množina označených formúl, nech \mathcal{T} je tablo pre S^+ a nech v je ohodnotenie množiny výrokových premenných. Ak v spĺňa S^+ a v spĺňa \mathcal{T} , tak v spĺňa aj každé priame rozšírenie \mathcal{T} .

v.z Korektnost — spinenie priameno rozsirenia tabia	V.2	Korektnosť – splnenie priameho rozšírenia tabla	
---	-----	---	--

 $D\hat{o}kaz\ lemy\ K1$. Nech S^+ je množina označených formúl, nech $\mathcal T$ je tablo pre S^+ a v je ohodnotenie množiny výrokových premenných. Nech $v \models S^+$. Nech v spĺňa $\mathcal T$ a v ňom vetvu π . Nech $\mathcal T_1$ je rozšírenie $\mathcal T$. Nastáva jeden z prípadov:

T₁ vzniklo z T operáciou A, pridaním nového dieťaťa z nejakému listu y v T, pričom z obsahuje α₁ alebo α₂ pre nejakú formulu α na vetve π_y. Ak π ≠ π_y, tak T₁ obsahuje π a teda je splnené. Ak π = π_y, tak v spĺňa aj α, pretože spĺňa π. Potom v musí spĺňať aj α₁ a α₂. Spĺňa teda vetvu π_z v table T₁, ktorá rozširuje splnenú vetvu π o vrchol z obsahujúci splnenú ozn. formulu α₁ alebo α₂. Preto v spĺňa tablo T₁.

- T₁ vzniklo z T operáciou B, pridaním detí z₁ a z₂ nejakému listu y v T, pričom z₁ obsahuje β₁ a z₂ obsahuje β₂ pre nejakú formulu β na vetve π_y. Ak π ≠ π_y, tak T₁ obsahuje π a teda je splnené. Ak π = π_y, tak v spĺňa aj β, pretože spĺňa π. Potom ale v musí spĺňať aj β₁ alebo β₂. Ak v spĺňa β₁, tak spĺňa aj vetvu π_{z1} v table T₁, a preto v spĺňa tablo T₁. Ak v spĺňa β₂, spĺňa aj π_{z2}, a teda aj T₁.
- \mathcal{T}_1 vzniklo z \mathcal{T} operáciou Ax, pridaním nového dieťaťa z nejakému listu y v \mathcal{T} , pričom z obsahuje formulu $X^+ \in S^+$. Ak $\pi \neq \pi_y$, tak \mathcal{T}_1 obsahuje π a teda je splnené.

Ak $\pi = \pi_y$, tak v spĺňa vetvu π_z v table \mathcal{T}_1 , pretože je rozšírením splnenej vetvy π o vrchol z obsahujúci splnenú formulu X (pretože $v \models S^+$). Preto v spĺňa tablo \mathcal{T}_1 .

V.3 Korektnosť — splnenie množiny a tabla pre ňu

Lema 2.72 (K2). Nech S^+ je množina označených formúl, nech $\mathcal T$ je tablo pre S^+ a nech v je ohodnotenie.

Ak v spĺňa S^+ , tak v spĺňa \mathcal{T} .

 $D\hat{o}kaz\ lemy\ K2$. Nech S^+ je množina označených formúl, nech v je ohodnotenie a nech $v \models S^+$. Úplnou indukciou na počet vrcholov tabla $\mathcal T$ dokážeme, že v spĺňa každé tablo $\mathcal T$ pre S^+ .

Ak má \mathcal{T} jediný vrchol, tento vrchol obsahuje formulu $X^+ \in S^+$, ktorá je splnená pri v. Preto je splnená jediná vetva v \mathcal{T} , teda aj \mathcal{T} .

Ak \mathcal{T} má viac ako jeden vrchol, je priamym rozšírením nejakého tabla \mathcal{T}_0 , ktoré má o 1 alebo o 2 vrcholy menej ako \mathcal{T} . Podľa indukčného predpokladu teda v spĺňa \mathcal{T}_0 . Podľa predchádzajúcej lemy potom v spĺňa aj \mathcal{T} .

V.4 Korektnosť – dôkaz

 $D\hat{o}kaz$ vety o korektnosti. Nech S^+ je množina označených formúl a $\mathcal T$ je uzavreté tablo pre $S^+.$

Sporom: Predpokladajme, že existuje ohodnotenie, ktoré spĺňa S^+ . Označme ho v.

Potom podľa lemy K2 v spĺňa tablo \mathcal{T} , teda v spĺňa niektorú vetvu π v \mathcal{T} .

Pretože $\mathcal T$ je uzavreté, aj vetva π je uzavretá, teda π obsahuje označené formuly $\mathbf T X$ a $\mathbf F X$ pre nejakú formulu X. Ale $v \models \mathbf T X$ vtt $v \models X$ a $v \models \mathbf F X$ vtt $v \not\models X$, čo je spor.

2.8.2. Tablový dôkaz splniteľnosti

V.5 Úplná vetva a tablo

Čo ak nevieme nájsť uzavreté tablo pre nejakú množinu ozn. formúl?

Definícia 2.73 (Úplná vetva a úplné tablo). Nech S^+ je množina označených formúl a \mathcal{T} je tablo pre S^+ .

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

- pre každú označenú formulu α, ktorá sa vyskytuje na π, sa *obidve* označené formuly α₁ a α₂ vyskytujú na π;
- pre každú označenú formulu β , ktorá sa vyskytuje na π , sa *aspoň jedna* z označených formúl β_1 , β_2 vyskytuje na π ;
- $ka\check{z}d\acute{a}X^+ \in S^+$ sa vyskytuje na π .

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

Príklad 2.74. Vybudujme úplné tablo pre $\mathbf{F}X$, kde $X = (((p \lor q) \land (r \lor p)) \rightarrow (p \land (q \lor r))).$

V.6 Otvorené tablo a splniteľnosť

Nech tablové pravidlá v príklade použijeme v akomkoľvek,

- nenájdeme uzavreté tablo, ale
- vyrobíme úplné otvorené tablo.

Z úplného otvoreného tabla pre S^+ vieme vytvoriť ohodnotenie v:

- 1. nájdeme otvorenú vetvu π ,
- 2. pre každú výrokovú premennú p
 - ak sa v π nachádza **T** p, definujeme v(p) = t;

- ak sa v π nachádza **F** p, definujeme v(p) = f;
- inak definujeme v(p) ľubovoľne.

Toto v spĺňa π , a preto v spĺňa S^+ (všetky formuly z S^+ sa vyskytujú na π).

Otázka. • Dá sa vždy nájsť úplné tablo?

• Naozaj sa z úplného otvoreného tabla dá vytvoriť spĺňajúce ohodnotenie?

Lema 2.75 (o existencii úplného tabla). Nech S^+ je konečná množina označených formúl.

Potom existuje úplné tablo pre S^+ .

 $D\hat{o}kaz$. Vybudujme tablo \mathcal{T}_0 pre S^+ tak, že do koreňa vložíme niektorú formulu z S^+ a opakovaním operácie Ax postupne doplníme ostatné.

Potom tablo postupne rozširujeme tak, že vyberieme ľubovoľný list y tabla \mathcal{T}_i , ktorého vetva π_y je otvorená a nie je úplná. Potom nastane aspoň jedna z možností:

- Na π_y sa nachádza nejaká formula α, ale nenachádza sa niektorá z formúl α₁ a α₂.
- Na π_y sa nachádza nejaká formula β , ale nenachádza sa ani jedna z formúl β_1 a β_2 .

Ak platí prvá alebo obe možnosti, aplikujeme operáciu A. Ak platí druhá možnosť, aplikujeme operáciu B. Získame tablo \mathcal{T}_{i+1} , s ktorým proces opakujeme.

Tento proces po konečnom počte krokov (prečo?) vytvorí nejaké tablo \mathcal{T}_n , v ktorom už neexistuje vetva, ktorá by bola otvorená a nebola úplná. Teda každá vetva v \mathcal{T}_n je buď uzavretá alebo úplná, čiže \mathcal{T}_n je úplné.

2.8.3. Hintikkova lema

V.8 Nadol nasýtené množiny a Hintikkova lemma

Definícia 2.76. Množina označených formúl S^+ sa nazýva *nadol nasýtená* vtt platí:

 $H_0 \ v S^+$ sa nevyskytujú naraz $\mathbf{T} p$ a $\mathbf{F} p$ pre žiadnu výrokovú premennú p;

$$H_1$$
 ak $\alpha \in S^+$, tak $\alpha_1 \in S^+$ a $\alpha_2 \in S^+$;

$$H_2$$
 ak $\beta \in S^+$, tak $\beta_1 \in S^+$ alebo $\beta_2 \in S^+$.

Pozorovanie 2.77. Nech π je úplná otvorená vetva nejakého tabla \mathcal{T} . Potom množina všetkých formúl na π je nadol nasýtená.

Lema 2.78 (Hintikkova). Každá nadol nasýtená množina S^+ je splniteľná.

 $D\hat{o}kaz$ Hintikkovej lemy. Chceme vytvoriť ohodnotenie v, ktoré splní všetky formuly z S^+ . Definujme v pre každú výrokovú premennú p takto:

- ak **T** $p \in S^+$: v(p) = t,
- ak **F** $p \in S^+$: v(p) = f,
- ak ani **T** p ani **F** p nie sú v S^+ , tak v(p) = t.

v je korektne definované vďaka H_0 .

Indukciou na stupeň formuly dokážeme, že v spĺňa všetky formuly z S^+ :

- v očividne spĺňa všetky označené výrokové premenné z S^+ .
- $X^+ \in S^+$ je buď α alebo β :
 - Ak X^+ je α , potom obidve α_1 , $\alpha_2 \in S^+$ (H₁), sú nižšieho stupňa X^+ , a teda podľa indukčného predpokladu sú splnené pri v, preto v spĺňa aj α (podľa pozorovania 2.60).
 - Ak X^+ je β , potom aspoň jedna z β_1 , β_2 je v S^+ (H₂). Nech je to ktorákoľvek, je nižšieho stupňa ako X^+ , teda podľa IP ju v spĺňa, a preto v spĺňa β (podľa pozorovania 2.62).

2.8.4. Úplnosť

V.10 Úplnosť _____

Úplnosť kalkulu neformálne:

Ak je nejaké tvrdenie pravdivé, tak existuje jeho dôkaz v kalkule.

Veta 2.79 (o úplnosti). Nech S^+ je konečná nesplniteľná množina označených formúl.

Potom existuje uzavreté tablo pre S^+ .

Dôsledok 2.80. Nech S je konečná teória a X je formula. $Ak S \models X$, tak $S \vdash X$.

Dôsledok 2.81. *Nech X je formula. Ak* \models *X, tak* \vdash *X.*

Úplnosť platí aj pre nekonečné množiny, ale dôkaz je ťažší.

V.11	Úplnosť — dôkaz	

 $D\hat{o}kaz$ vety o úplnosti. Zoberme ľubovoľnú konečnú nesplniteľnú množinu označených formúl $S^+.$

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

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

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

VI. prednáška

Korektné pravidlá. Rezolvencia

26. marca 2018

2.8.5. Nové korektné pravidlá

VI.1 Ingrediencie korektnosti a úplnosti tabiel

Všimnite si:

- Na dokázanie korektnosti tablového kalkulu stačilo, aby mali pravidlá vlastnosť:
 - Nech v je ohodnotenie. Ak v spĺňa premisu (a množinu S^+), tak spĺňa oba (α) závery/aspoň jeden (β) záver.
 - Vďaka tejto vlastnosti zo splniteľnej množiny S^+ skonštruujeme iba splniteľné tablá.
 - Netreba opačnú implikáciu (ak v spĺňa oba/jeden záver, tak spĺňa premisu).
- Na dôkaz *úplnosti* stačili pravidlá (S^+), α , β , pretože stačia na vybudovanie úplného tabla.

VI.2 Nové pravidlo _____

Čo sa stane, ak pridáme nové pravidlo, napríklad disjunktívny sylogizmus:

$$\frac{\mathbf{T}(A \vee B) \quad \mathbf{F}A}{\mathbf{T}B} \qquad ? \tag{DS}_1)$$

Upravíme definíciu priameho rozšírenia:

Úprava definície 2.63

(...) Nech \mathcal{T} je tablo pre S^+ a y je nejaký jeho list. Potom tablom pre S^+ je aj každé *priame rozšírenie* \mathcal{T} ktoroukoľvek z operácií:

 $A\ \cdots$

:

DS₁: Ak sa na vetve π_y nachádzajú *obe* formuly $\mathbf{T}(A \vee B)$ a $\mathbf{F}A$, tak ako jediné dieťa y pripojíme nový vrchol obsahujúci $\mathbf{T}B$.

VI.3 Nové pravidlo vs. korektnosť a úplnosť

• Pravidlo (DS₁) je *korektné*:

Nech v je ľubovoľné ohodnotenie.

Ak v spĺňa $\mathbf{T}(A \vee B)$ a $\mathbf{F} A$, tak v spĺňa $\mathbf{T} B$.

Keďže $v \models \mathbf{T}(A \lor B)$, tak $v \models (A \lor B)$, teda $v \models A$ alebo $v \models B$. Pretože ale $v \models \mathbf{F} A$, tak $v \not\models A$. Takže $v \models B$.

• Preto stále dokážeme lemu K1 (2.71):

Nech S^+ je množina označených formúl, nech $\mathcal T$ je tablo pre S^+ a v je ohodnotenie množiny výrokových premenných.

Ak v spĺňa S^+ a v spĺňa \mathcal{T} ,

tak v spĺňa aj každé priame rozšírenie \mathcal{T} .

Z nej dokážeme K2 a vetu o korektnosti

 Pridanie pravidla neohrozuje úplnosť (doterajšími pravidlami stále vybudujeme úplné tablo).

VI.4 Nové pravidlá vo všeobecnosti

Definícia 2.82 (Tablové pravidlo a jeho korektnosť). Nech n a k sú prirodzené čísla, $n \geq 0$, k > 0, nech $P_1^+, \ldots, P_n^+, C_1^+, \ldots, C_k^+$ sú označené formuly nad výrokovými premennými $\{q_1, \ldots, q_m\}$.

Tablové pravidlo R je množina dvojíc n-tíc a k-tic označených formúl

$$R = \left\{ \begin{array}{c|cc} P_1^+|_{[q_1|X_1,\dots,q_m|X_m]} & \cdots & P_n^+|_{[q_1|X_1,\dots,q_m|X_m]} \\ \hline C_1^+|_{[q_1|X_1,\dots,q_m|X_m]} & \dots & C_k^+|_{[q_1|X_1,\dots,q_m|X_m]} \end{array} \middle| X_1,\dots,X_m \in \mathcal{E} \right\},$$

ktoré vzniknú súčasnou substitúciou formúl X_1, \ldots, X_m za premenné q_1, \ldots, q_m v označených formulách $P_1^+, \ldots, P_n^+, C_1^+, \ldots, C_k^+$.

Prvky hornej *n*-tice nazývame *premisy*, prvky dolnej *k*-tice nazývame *závery*. Každý prvok *R* nazývame *inštancia* pravidla *R*.

Tablové pravidlo R je korektné (tiež zdravé z angl. sound) vtt pre každé ohodnotenie výrokových premenných v platí, že ak v spĺňa všetky premisy P_1^+, \ldots, P_n^+ , tak v spĺňa niektorý záver C_1^+, \ldots, C_k^+ .

VI.5 Nové pravidlá vo všeobecnosti

Úprava definície 2.63

(...)

• . . .

• Nech \mathcal{T} je tablo pre S^+ a y je nejaký jeho list. Potom tablom pre S^+ je aj každé *priame rozšírenie* \mathcal{T} ktoroukoľvek z operácií:

:

R: Ak sa pre nejakú inštanciu pravidla *R* na vetve π_y nachádzajú *všetky* premisy P_1^+, \ldots, P_n^+ , tak k uzlu *y* pripojíme *k* nových vrcholov obsahujúcich postupne závery C_1^+, \ldots, C_k^+ .

2.9. Rezolvencia vo výrokovej logike

VI.6 Tranzitivita implikácie

Vráťme sa k neoznačeným formulám.

Je nasledujúce pravidlo korektné?

$$\frac{(A \to B) \qquad (B \to C)}{(A \to C)}$$

Nahraďme implikácie disjunkciami:

$$\frac{(\neg A \lor \mathbf{B}) \qquad (\neg \mathbf{B} \lor C)}{(\neg A \lor C)}$$

VI.7 Rezolvencia

Predchádzajúce pravidlo sa dá zovšeobecniť na ľubovoľné dvojice klauzúl:

Definícia 2.83. Rezolvenčný princíp (rezolvencia, angl. resolution principle) je pravidlo

$$\frac{(k_1 \vee \cdots \vee p \vee \cdots \vee k_m) \quad (\ell_1 \vee \cdots \vee \neg p \vee \cdots \vee \ell_n)}{(k_1 \vee \cdots \vee k_m \vee \ell_1 \vee \cdots \vee \ell_n)}$$

pre ľubovoľnú výrokovú premennú p

a ľubovoľné literály $k_1, \ldots, k_m, \ell_1, \ldots, \ell_n$.

Klauzulu $(k_1 \vee \cdots \vee k_m \vee \ell_1 \vee \cdots \vee \ell_n)$ nazývame *rezolventou* klauzúl $(k_1 \vee \cdots \vee p \vee \cdots \vee k_m)$ a $(\ell_1 \vee \cdots \vee \neg p \vee \cdots \vee \ell_n)$.

Tvrdenie 2.84. Rezolvencia je korektné pravidlo, teda rezolventa je logickým dôsledkom množiny obsahujúcej obe premisy.

VI.8 Špeciálne prípady rezolvencie

Viacero pravidiel sa dá chápať ako špeciálne prípady rezolvencie:

$$\frac{(\neg p \lor q) \quad (\neg q \lor r)}{(\neg p \lor r)} \qquad \frac{(p \to q) \quad (q \to r)}{(p \to r)} \quad \text{(tranzitivita} \to)$$

$$\frac{(\neg p \lor \ell) \quad p}{\ell} \qquad \frac{(p \to \ell) \quad p}{\ell} \quad \text{(modus ponens)}$$

$$\frac{(\neg p \lor q) \quad \neg q}{\neg p} \qquad \frac{(p \to q) \quad \neg q}{\neg p} \quad \text{(modus tolens)}$$

VI.9 Pozorovania o rezolvencii

• Rezolvencia s jednotkovou klauzulou skráti druhú klauzulu:

$$\frac{\neg q \quad (p \lor q \lor \neg r)}{(p \lor \neg r)}$$

• Nie každý logický dôsledok sa dá odvodiť rezolvenciou: $\{p,q\} \models (p \lor q)$

• Ak rezolvencia odvodí prázdnu klauzulu

$$\frac{\neg p \quad p}{\Box}$$
,

premisy nie sú súčasne splniteľné

 Niektoré dvojice klauzúl možno rezolvovať na viacerých literáloch, ale je nekorektné urobiť to naraz:

$$\frac{(\neg p \lor q) \quad (p \lor \neg q)}{(q \lor \neg q)} \quad \frac{(\neg p \lor q) \quad (p \lor \neg q)}{(\neg p \lor p)} \quad \boxed{(\neg p \lor q)}$$

Prečo?

Lebo
$$\{(\neg p \lor q), (p \lor \neg q)\}$$
 je splniteľná $(v_1 = \{p \mapsto t, q \mapsto t\}, v_2 = \{p \mapsto f, q \mapsto f\}),$ ale \square je nesplniteľná

VI.11 Problematické prípady

- Opakovaným aplikovaním rezolvencie môžeme odvodzovať ďalšie dôsledky *Príklad* 2.85. Z množiny $S = \{(\neg p \lor r), (\neg q \lor r), (p \lor q)\}$ odvodíme $(r \lor r)$:
 - (1) $(\neg p \lor r)$ predpoklad z S
 - (2) $(\neg q \lor r)$ predpoklad z *S*
 - (3) $(p \lor q)$ predpoklad z S
 - (4) $(r \lor q)$ rezolventa (1) a (3)
 - (5) $(r \lor r)$ rezolventa (2) a (4)
- Klauzula (r ∨ r) je evidentne ekvivalentná s r;
 r sa ale z množiny S iba rezolvenciou odvodiť nedá
- Preto potrebujeme ešte pravidlo idempotencie:

$$\frac{(k_1 \vee \cdots \vee \textcolor{red}{\ell} \vee \cdots \vee \textcolor{red}{\ell} \vee \cdots \vee k_n)}{(k_1 \vee \textcolor{red}{\ell} \vee \cdots \vee k_n)}$$

Definícia 2.86. Rezolvenčné odvodenie z množiny klauzúl S je každá (aj nekonečná) postupnosť klauzúl $C_1, C_2, \ldots, C_n, \ldots$, ktorej každý člen C_i je:

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

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

Definícia 2.87. Množinu klauzúl budeme nazývať aj klauzálna teória.

VI.13 Korektnosť a úplnosť rezolvencie

Veta 2.88 (Korektnosť rezolvencie). *Nech S je množina klauzúl. Ak existuje zamietnutie S, tak S je nesplniteľná.*

Veta 2.89 (Úplnosť rezolvencie). Nech S je množina klauzúl. Ak S je nesplniteľná, tak existuje zamietnutie S.

2.10. Späť k dôkazom o vyplývaní

VI.14 Konzultácie a termín pre 6. sadu úloh

- Ak chcete
 - získať spätnú väzbu na riešenie nehodnotených úloh,
 - poradiť sa o riešení aktuálnej sady úloh (teoretických aj praktických),
 - poradiť sa o obsahu prednášok,
 - dať nám spätnú väzbu na obsah alebo formu vyučovania predmetu,

využívajte konzultačné hodiny:

streda od 13:10 do 14:30 v I-7 alebo I-16

• Riešenie 6. sady úloh odovzdajte

najneskôr vo štvrtok 5. apríla 2018 o 13:00 v kancelárii I-7 alebo I-16

VI.15 Uvažovanie o vyplývaní _____

Cvičenie 2.90. sada úloh 3, úloha 3 Nech X a Y sú ľubovoľné výrokové formuly, nech T je ľubovoľná výroková teória.

Dokážte alebo vyvráťte:

- c) Ak $T \models \neg X$, tak $T \not\models X$.
- d) Ak $T \not\models X$, tak $T \models \neg X$.
- e) $T \models (X \rightarrow Y)$ vtt $T \cup \{X\} \models Y$.

VI.16 su03/3c) Ak $T \models \neg X$, tak $T \not\models X$

Riešenie 2.90 (c). Zoberme ľubovoľnú teóriu T a formulu X také, že $T \models \neg X$. *Aby* tvrdenie platilo:

- musí $T \not\models X$, teda (podľa definície vyplývania)
- nesmie byť pravda, že každé ohodnotenie spĺňajúce T spĺňa aj X, teda
- musí existovať ohodnotenie, ktoré spĺňa T a nespĺňa X, teda
- T musí byť *splniteľná*. Predpoklad $T \models \neg X$ to však nezaručuje: $T \models \neg X$ platí aj pre nesplniteľnú T (a vtedy dokonca pre ľubovoľnú X).

Tvrdenie teda neplatí a vieme ho vyvrátiť konkrétnym kontrapríkladom:

• Zoberme $T = \{(p \land \neg p)\}\$ a X = p.

- Pre ľubovoľné ohodnotenie v platí $v \not\models T$, teda platia aj implikácie: i. ak $v \models T$, tak $v \models \neg X$, ii. ak $v \models T$, tak $v \models X$, lebo ich antecedenty sú nepravdivé.
- Ich zovšeobecnením dostávame: i. $T \models \neg X$ a ii. $T \models X$.

VI.17 su03/3d) Ak $T \not\models X$, tak $T \models \neg X$

Riešenie 2.90 (d). Zoberme ľubovoľnú teóriu T a formulu X také, že $T \not\models X$.

- Aby tvrdenie platilo, musí $T \models \neg X$, teda
- $každ\acute{e}$ ohodnotenie v spĺňajúce T musí spĺňať aj $\neg X$.
- Podľa predpokladu a definície vyplývania existuje ohodnotenie v také, že v |= T a v |≠ X, teda aj v |= ¬X.
- Ale to *nestačí na to*, aby pre *ľubovoľné* ohodnotenie v', ktoré spĺňa T, tiež platilo $v' \not\models X$ a teda aj $v' \models \neg X$.

Tvrdenie teda **neplatí** a vieme ho vyvrátiť konkrétnym kontrapríkladom:

- Zoberme $T = \{p\}$ a X = q.
- Pre ohodnotenie $v = \{p \mapsto t, q \mapsto f\}$ máme $v \models T$ a $v \not\models X$, preto $T \not\models X$.
- Pre ohodnotenie $v = \{p \mapsto t, q \mapsto t\}$ máme $v \models T$ a $v \not\models \neg X$, preto $T \not\models \neg X$.
- Teda $T \not\models X$ a $T \not\models \neg X$.

VI.18 su03/3e) $T \models (X \rightarrow Y)$ vtt $T \cup \{X\} \models Y$

Riešenie 2.90 (e, smer \Rightarrow). Zoberme ľubovoľnú teóriu T a formuly X a Y také, že $T \models (X \rightarrow Y)$, teda

pre každé ohodnotenie v platí, že ak $v \models T$, tak $v \models (X \rightarrow Y)$.

Aby tvrdenie (e \Rightarrow) platilo, musí $T \cup \{X\} \models Y$, teda

pre každé ohodnotenie v musí platiť, že (*) ak $v \models T \cup \{X\}$, tak $v \models Y$.

Zoberme teda ľubovoľné ohodnotenie v.

- Ak $v \not\models T \cup \{X\}$, vlastnosť (*) platí, lebo jej antecedent je nepravdivý.
- Ak $v \models T \cup \{X\}$, tak $v \models T$ a $T \models X$ a musíme ukázať, že $v \models Y$.
 - Z $v \models T$ a predpokladu, vyplýva, že $v \models (X \rightarrow Y)$, teda
 - (a) $v \not\models X$ alebo (b) $v \models Y$ podľa definície spĺňania.
 - Podľa $T \models X$ prípad (a) nenastáva,
 - takže $v \models Y$.

Vlastnosť (*) teda platí aj v tomto prípade.

Ďalšie možnosti nie sú. Môžeme teda zovšeobecniť, že $T \cup \{X\} \models Y$, č.b.t.d.

```
VI.19 su03/3e) T \models (X \rightarrow Y) vtt T \cup \{X\} \models Y
```

Riešenie 2.90 (e, smer \Leftarrow). Zoberme ľubovoľnú teóriu T a formuly X a Y také, že $T \cup \{X\} \models Y$, teda

pre každé ohodnotenie v platí, že ak $v \models T$, tak $v \models (X \rightarrow Y)$. Aby tvrdenie (e \Leftarrow) platilo, musí $T \models (X \rightarrow Y)$, teda

pre každé ohodnotenie v musí platiť, že (*) ak $v \models T$, tak $v \models (X \rightarrow Y)$.

Zoberme teda ľubovoľné ohodnotenie v.

- Ak $v \not\models T$, vlastnosť (*) platí.
- Ak $v \models T$, musíme ukázať, že $v \models (X \rightarrow Y)$.
 - Ak $v \not\models X$, tak $v \models (X \rightarrow Y)$, a teda (*) platí.
 - Ak $v \models X$, tak $v \models T \cup \{X\}$, teda podľa predpokladu $v \models Y$. Preto $v \models (X \rightarrow Y)$. Vlastnosť (*) teda znova platí.

Ďalšie možnosti nie sú. Môžeme teda zovšeobecniť, že $T \models (X \rightarrow Y)$, č.b.t.d.

Používanie pojmov splnenie a vyplývanie

- \bigcirc ohodnotenie v spĺňa formulu X
- **⊘** formula *X* je splnená v ohodnotení *v*
- $v \models X$
- \odot ohodnotenie v spĺňa teóriu T
- teória *T* je splnená v ohodnotení *v*
- \circ $v \models T$
- c teória *T* spĺňa ohodnotenie *v*
- of formula X vyplýva z teórie T
- **⊘** formula *X* je (logickým) dôsledkom teórie *T*
- v teória T má (logický) dôsledok X
- \bigcirc $T \models X$
- z ohodnotenia v vyplýva...
- c z formuly *X* vyplýva teória *T*

VI.21 Problémy v dôkazoch (2)

Ignorovanie pojmov a ich definícií

- Niektorí úplne ignorovali, že pojmy vyplývanie a splnenie majú presný dohodnutý význam
- Hovorili o pravdivosti bez ohodnotenia alebo o vyplývaní bez teórie

Definície pojmov a ich negovanie

- Z T vyplýva X ($T \models X$) vtt
 - \bigcirc pre **všetky** ohodnotenia v, **ak** $v \models T$, **tak** $v \models X$
 - \bigcirc každý model v teórie T spĺňa X
 - \bigcirc pre **všetky** ohodnotenia $v, v \models T$ **a** $v \models X$
 - igoplusexistuje ohodnotenie v také, že $v \models T$ a $v \models X$
 - igoplus existuje ohodnotenie v také, že ak $v \models T$, tak $v \models X$
- Z T **ne**vyplýva X ($T \not\models X$) vtt
 - **existuje** ohodnotenie v také, že $v \models T$ a $v \not\models X$
 - \bigcirc existuje model v teórie T, ktorý nespĺňa X
 - **a** ...

VI.22 Problémy v dôkazoch (3)

Skríženie pojmov splnenia a vyplývania

- ⚠ Vyplývanie z teórie ($T \models X$) sa správa inak ako splnenie formuly ohodnotením ($v \models X$)
 - $v \models \neg X \text{ vtt } v \not\models X$ priamo z definície splnenia formuly ohodnotením
 - $T \models \neg X \text{ vtt } T \not\models X$ **neplatí ani v jednom smere** (videli sme pred chvíľou)
- A Symbol |= sa (žiaľ) používa pre oba pojmy

Skoky v uvažovaní veľké a nezdôvodnené

- \triangle Ak $T \models (X \rightarrow Y)$, tak $T \not\models X$ alebo $T \models Y$.
- lacktriangle Ak $T \not\models X$ alebo $T \models Y$, tak $T \models (X \rightarrow Y)$.
- \bigcirc Ak $v \not\models T$, tak T je nesplniteľná.

- Neuvedomenie si toho, čo treba dokázať Rozoberú sa možnosti vyplývajúce z predpokladov, ale nezistí sa, či platí požadovaný záver
- Uvažovanie v kruhu
 Použitie toho, čo máme dokázať, na zdôvodnenie nejakého kroku
- A Snaha uvažovať naraz o všetkých modeloch/ohodnoteniach
- Vyslovte jasne, akú vlastnosť majú mať všetky ohodnotenia
 - 2. Zoberte jedno ohodnotenie, o ktorom nič nepredpokladáte ("ľubovoľné"
 - 3. Overte, či má za každých okolností požadovanú vlastnosť
 - 4. Zovšeobecnite, že požadovanú vlastnosť majú všetky ohodnotenia
- A Snaha uvažovať súbežne o viacerých možnostiach
- Uvažujte prípady postupne a oddelene, vyčerpajte všetky možnosti

VI.24 Problémy v dôkazoch (5)

Uvažovanie o formulách a teóriách, akoby to boli výrokové premenné

- Ohodnotenie v priraďuje t alebo f iba výrokovej premennej (v(p) = t, v(p) = f, v(X) = t, v(X = Y) = t, v(T) = t)
- Formula X je v ohodnotení v splnená ($v \models X$) alebo nesplnená ($v \not\models X$)
- Teória T je v ohodnotení v splnená ($v \models T$) alebo nesplnená ($v \not\models T$)

Literatúra

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

Raymond M. Smullyan. *Logika prvého rádu*. Alfa, 1979. Z angl. orig. *First-Order Logic*, Berlin-Heidelberg: Springer-Verlag, 1968 preložil Svätoslav Mathé.

Vítězslav Švejdar. *Logika: neúplnost, složitost, nutnost*. Academia, 2002. Prístupné aj na http://www1.cuni.cz/~svejdar/book/LogikaSve2002.pdf.