

Prednášky z Matematiky (4) – Logiky pre informatikov

Ján Kľuka, Jozef Šiška

Letný semester 2017/2018

Obsah

I. 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	22
2.4. Tautológia, (ne)splniteľnosť, falzifikovateľnosť	25
III. Vyplyvanie, ekvivalentné úpravy	31
2.5. Vyplyvanie	32
2.6. Ekvivalencia	35
2.7. Ekvivalentné úpravy	37

2.8. Konjunktívna a disjunktívna normálna forma	40
---	----

I. prednáška

O logike a tomto kurze Syntax výrokovkej 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 zistíme, 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.

I.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

- Už Aristoteles zistil, že správne úsudky sa dajú rozpoznať podľa ich *formy*, bez ohľadu na obsah

Ak pôjde Jim, tak pôjde Kim.

Ak je diltium dekryštalizované,
tak antihmota neprúdi.

Pôjde Jim.

Diltium je dekryštalizované.

Pôjde Kim.

Antihmota neprúdi.

- Usudzovacie (inferenčné) pravidlo** je *vzor* úsudkov daný formou tvrdení, s ktorými pracuje

Ak A, tak B. <u>A.</u> B.	}	vzory premís vzor záveru
---------------------------------	---	---------------------------------

- Korektné** pravidlo odvodí z pravdivých premís pravdivý záver
- Dôkaz** je teda **postupnosť použitia korektných usudzovacích pravidiel** (najlepšie *samozrejmych* pre čitateľa dôkazu)
- Dedukcia** — usudzovanie iba pomocou korektných pravidiel

Niektoré **nie korektné** usudzovacie pravidlá sú prakticky užitočné:

Indukcia — zovšeobecnenie:

Videl som tisíc havranov.

Žiaden nebol inej farby ako čiernej.

Platí aj pre červené Fabie?

Všetky havrany sú čierne.

Abdukcia — odvodzovanie možných príčin z následkov:

Ak je batéria vybitá, auto nenašartuje.

Ak je nádrž prázdna, auto nenašartuje.

Nádrž nie je prázdna.

Auto nenašartovalo.

Čo ak nám kuna
prehrýzla káble?

Batéria je vybitá.

Usudzovanie na základe analógie (podobnosti)

Venuša má atmosféru, podobne ako Zem.

Na Zemi sa prejavuje skleníkový efekt.

Na Venuši sa prejavuje skleníkový efekt.

A čo: Atmosféra

Zeme je dýchatelná?

I.7 Nededuktívne pravidlá

- **Záver** 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**

I.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 dvojtrietinovou 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 vecí, 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 znení 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

I.9 Formalizácia poznatkov

- S formalizáciou ste sa už stretli pri riešení slovných úloh

Karol je trikrát starší ako Mária.
 Súčet Karolovho a Máriinho veku je 12 rokov. \rightsquigarrow $k = 3 \cdot m$
 Koľko rokov majú Karol a Mária? $k + m = 12$

- Stretli ste sa už aj s formálnym jazykom výrokovej logiky

Príklad 1.5. Sformalizujme náš pártý príklad:

- P0: Nieкто 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.
 P3: 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

I.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 odvodí 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 kalkulo
- 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.
- Slnčná sústava má deviatu planétu.
- Mama upiekla koláč, ale Editka dostala z matematiky štvorku.
- Nieкто zhasol.

Negatívne príklady

- Toto je čudné.
- Píšte všetci modrým perom!

- Prečo je obloha modrá?

Výrokom priradujeme *pravdivostné hodnoty*

I.17 Opakovanie: Výroková logika v prirodzenom jazyku

Operácie s výrokmami – *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 *logickú* 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 *redefinuje 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 Syntax výrokovej 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]

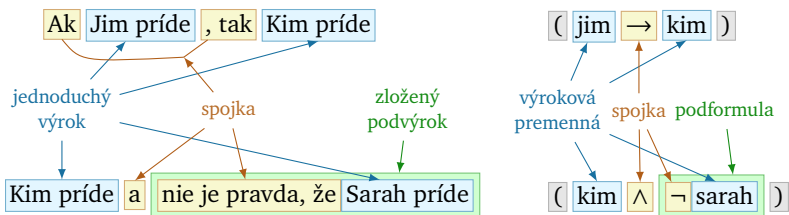
I.20 Syntax výrokovej logiky

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 **symbols**

I.21 Symbols jazyka výrokovej logiky

Definícia 2.3. *Symbolmi jazyka výrokovej logiky sú:*

- *výrokové premenné* z nejakej spočítateľnej množiny $\mathcal{V} = \{p_1, p_2, \dots, p_n, \dots\}$, ktorej prvkami nie sú symbols $\neg, \wedge, \vee, \rightarrow, (,)$, ani jej prvky tieto symbols neobsahujú;
- *logické symbols (logické spojky)*: $\neg, \wedge, \vee, \rightarrow$
(nazývané, v uvedenom poradí, *symbol negácie*, *symbol konjunkcie*, *symbol disjunkcie*, *symbol implikácie* a čítané „nie“, „a“, „alebo“, „ak ..., tak ...“);
- *pomocné symbols*: $(,)$ (ľavá zátvorka a pravá zátvorka).

Spojka \neg je *unárna* (má jeden argument).

Spojky $\wedge, \vee, \rightarrow$ sú *binárne* (spájajú dve formuly).

Poznámka 2.4. Definícia je **záväzná** dohoda o význame pojmov.

I.22 Symbols, 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, \dots , 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 vyzerat' formuly vybudované nad touto množinou?
 - Samotné premenné, napr. sarah.
 - Negácie premenných, napr. $\neg\text{sarah}$.
 - Premenné alebo aj ich negácie spojené spojkou, napr. $(\neg\text{kim} \vee \text{sarah})$.
 - Ale negovať a spájať spojkami môžeme aj zložitejšie formuly, napr. $(\neg(\text{kim} \wedge \text{sarah}) \rightarrow (\neg\text{kim} \vee \neg\text{sarah}))$.
- 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.

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 $(A \rightarrow B)$ 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 $\mathcal{V} = \{\text{kim}, \text{jim}, \text{sarah}\}$.

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

$\mathcal{E} = \{\text{kim}, \text{jim}, \text{sarah},$	podľa (i)
$\neg\text{kim}, \neg\text{jim}, \neg\text{sarah},$	podľa (ii)
$(\text{kim} \wedge \text{kim}), (\text{kim} \wedge \text{jim}), (\text{kim} \wedge \text{sarah}),$	podľa (iii) pre \wedge
$(\text{kim} \wedge \neg\text{kim}), (\text{kim} \wedge \neg\text{jim}), (\text{kim} \wedge \neg\text{sarah}),$	
$(\text{jim} \wedge \text{kim}), (\text{jim} \wedge \text{jim}), (\text{jim} \wedge \text{sarah}),$	
$(\text{jim} \wedge \neg\text{kim}), (\text{jim} \wedge \neg\text{jim}), (\text{jim} \wedge \neg\text{sarah}),$	
$(\neg\text{kim} \wedge \text{kim}), (\neg\text{kim} \wedge \text{jim}), (\neg\text{kim} \wedge \text{sarah}), \dots,$	
$(\neg\text{jim} \wedge \neg\text{sarah}), \dots,$	podľa (iii) pre \rightarrow
$(\text{sarah} \vee (\text{kim} \rightarrow \text{jim})), \dots,$	a potom pre \vee
$(\neg(\text{kim} \wedge \text{sarah}) \vee (\neg\text{jim} \rightarrow \neg\text{sarah})), \dots\}$	podľa (iii) pre $\wedge,$ \rightarrow, \vee

Definícia 2.8. *Vytvárajúcou postupnosťou* nad množinou výrokových premených \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 $(A \wedge B)$, $(A \vee B)$, $(A \rightarrow B)$, 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 .*

Príklad 2.10. Nájdime vytvárajúcu postupnosť pre formulu $(\neg\text{kim} \rightarrow (\text{jim} \vee \text{sarah}))$.

II. prednáška

Sémantika výrokovej logiky

26. februára 2018

II.1

Spomeňte si II.1

Ktoré z nasledujúcich postupností symbolov sú formulami nad množinou výrokových premenných $\mathcal{V} = \{p, q, r, \dots\}$?

A. $(p \vee \neg q \vee \neg r)$,

C. $\neg(\neg(\neg p))$,

B. $(p \wedge \neg(q \rightarrow r))$,

D. $(p \leftrightarrow \neg q)$.

II.2 Ekvivalencia

Dohoda

Pre každú dvojicu formúl $A, B \in \mathcal{E}$ je zápis $(A \leftrightarrow B)$ skratka za formulu $((A \rightarrow B) \wedge (B \rightarrow A))$.

II.3 Jednoznačnosť rozkladu formúl výrokovej logiky

- Predpokladajme, že by sme zadefinovali „formuly“ takto:

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 „formulou“ z \mathcal{E} ;
- ii. ak A je „formula“ z \mathcal{E} , tak aj postupnosť symbolov $\neg A$ je „formulou“ z \mathcal{E} ;
- iii. ak A a B sú „formuly“ z \mathcal{E} , tak aj $A \wedge B$, $A \vee B$ a $A \rightarrow B$ sú „formulami“ z \mathcal{E} ;

iv. ak A je „formula“ z \mathcal{E} , tak aj postupnosť symbolov (A) je „formulou“ z \mathcal{E} .

- Bola by potom $(jim \rightarrow kim \rightarrow \neg sarah)$ „formulou“?
- Aký by bol jej význam?

Formulu by sme mohli čítať ako $A = (jim \rightarrow (kim \rightarrow \neg sarah))$ alebo ako $B = ((jim \rightarrow kim) \rightarrow \neg sarah)$.

Čítanie A hovorí, že Sarah nepríde, ak prídu Jim a Kim súčasne. To neplatí v práve jednej situácii: keď všetci prídu.

Čítanie B hovorí, že Sarah nepríde, ak alebo nepríde Jim alebo príde Kim. To však neplatí v *aspoň dvoch* rôznych situáciách: keď prídu všetci a keď príde Sarah a Kim, ale nie Jim.

II.4 Jednoznačnosť rozkladu formúl výrokovej logiky

Pre našu definíciu formúl platí:

Tvrdenie 2.11 (o jednoznačnosti rozkladu). *Pre každú formulu $X \in \mathcal{E}$ nad množinou výrokových premenných \mathcal{V} platí práve jedna z nasledujúcich možností:*

- X je výroková premenná z \mathcal{V} .
- Existuje práve jedna formula $A \in \mathcal{E}$ taká, že $X = \neg A$.
- Existujú práve jedna dvojica formúl $A, B \in \mathcal{E}$ a jedna spojka $b \in \{\wedge, \vee, \rightarrow\}$ také, že $X = (A \ b \ B)$.

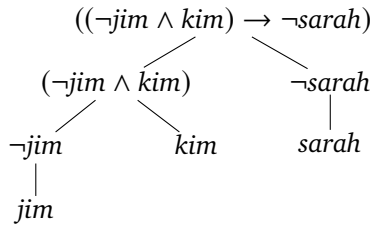
II.5 Vytvárajúca postupnosť a vytvárajúci strom

- Konštrukciu formuly podľa definície si vieme predstaviť pomocou vytvárajúcej postupnosti:

$jim, sarah, \neg jim, kim, \neg sarah, (\neg jim \wedge kim), ((\neg jim \wedge kim) \rightarrow \neg sarah)$

- Postupnosť ale jasne nevyjadruje, ktoré z predchádzajúcich formúl sa *bezprostredne* použijú na vytvorenie nasledujúcej formuly.

- Konštrukciu formuly si ale vieme predstaviť ako *strom*:



- Takéto stromy voláme vytvárajúce.
- Ako ich *presne* a *všeobecne* popíšeme — zdefinujeme?

II.6 Vytvárajúci strom formuly

Definícia 2.12. Vytvárajúci strom pre formulu X je binárny strom T obsahujúci v každom vrchole formulu, pričom platí:

- v koreni T je formula X ,
- ak vrchol obsahuje formulu $\neg A$, tak má práve jedno dieťa, ktoré obsahuje formulu A ,
- ak vrchol obsahuje formulu $(A \mathbin{\&B} B)$, kde $\mathbin{\&B}$ je jedna z binárnych spojok, tak má dve deti, pričom ľavé dieťa obsahuje formulu A a pravé formulu B ,
- vrcholy obsahujúce výrokové premenné sú listami.

II.7 Podformuly

- Ako by ste nazvali formuly, z ktorých daná formula vznikla?

Napríklad formuly $sarah$, $\neg jim$, $(\neg jim \wedge kim)$ pre

$$((\neg jim \wedge kim) \rightarrow \neg sarah).$$

- Ako by ste nazvali formuly, z ktorých daná formula *bezprostredne/priamo* vznikla?

V príklade vyššie sú to $(\neg jim \wedge kim)$ a $\neg sarah$.

- Ako tieto pojmy presne zdefinujeme?

Definícia 2.13 (Priama podformula).

- Priamou podformulou $\neg A$ je formula A .
- Priamymi podformulami $(A \wedge B)$, $(A \vee B)$ a $(A \rightarrow B)$ sú formuly A (ľavá priama podformula) a B (pravá priama podformula).

Definícia 2.14 (Podformula). Vzťah *byť podformulou* je najmenšia relácia na formulách spĺňajúca:

- Ak X je priamou podformulou Y , tak X je podformulou Y .
- Ak X je podformulou Y a Y je podformulou Z , tak X je podformulou Z .

- Zložitosť formúl by sa mohla merať napríklad jej dĺžkou (počtom symbolov)
- Prirodzenejšie je ale merať zložitosť počtom netriviálnych krokov potrebných na konštrukciu formuly:
 - pridanie negácie pred formulu,
 - spojenie formúl spojkou

- Tejto miere hovoríme *stupeň formuly*

Príklad 2.15. Aký je stupeň formuly $((p \vee \neg q) \wedge \neg(q \rightarrow p))$?

- Ako stupeň zadefinujeme?

Induktívne, podobne ako sme zadefinovali formuly:

1. určíme hodnotu stupňa pre atomické formuly,
2. určíme, ako zo stupňa priamych podformúl vypočítame stupeň z nich zloženej formuly.

Definícia 2.16 (Stupeň formuly).

- Výroková premenná je stupňa 0.
- Ak A je formula stupňa n , tak $\neg A$ je stupňa $n + 1$.
- Ak A je formula stupňa n_1 a B je formula stupňa n_2 , tak $(A \wedge B)$, $(A \vee B)$ a $(A \rightarrow B)$ sú stupňa $n_1 + n_2 + 1$.

Definícia 2.16 (Stupeň formuly stručne, symbolicky). *Stupeň* $\deg(X)$ formuly $X \in \mathcal{E}$ definujeme pre každú výrokovú premennú $p \in \mathcal{V}$ a pre všetky formuly A , $B \in \mathcal{E}$ nasledovne:

- $\deg(p) = 0$,
- $\deg(\neg A) = \deg(A) + 1$,
- $\deg((A \wedge B)) = \deg((A \vee B)) = \deg((A \rightarrow B)) = \deg(A) + \deg(B) + 1$.

Veta 2.17 (Princíp indukcie na stupeň formuly). *Nech P je ľubovoľná vlastnosť formúl ($P \subseteq \mathcal{E}$). Ak platí súčasne*

báza indukcie: každá formula stupňa 0 má vlastnosť P ,

indukčný krok: pre každú formulu X z predpokladu, že všetky formuly menšieho stupňa ako $\deg(X)$ majú vlastnosť P , vyplýva, že aj X má vlastnosť P ,

tak všetky formuly majú vlastnosť P ($P = \mathcal{E}$).

Definícia 2.18 (Množina výrok. prem. formuly $\text{vars}(X)$)).

- Ak p je výroková premenná, množinou výrokových premenných atomickej formuly p je $\{p\}$.
- Ak V je množina výrokových premenných formuly A , tak V je tiež množinou výrok. prem. formuly $\neg A$.
- Ak V_1 je množina výrok. prem. formuly A a V_2 je množina výrok. prem. formuly B , tak $V_1 \cup V_2$ je množinou výrok. prem. formúl $(A \wedge B)$, $(A \vee B)$ a $(A \rightarrow B)$.

Definícia 2.18 ($\text{vars}(X)$ stručnejšie).

- Ak p je výroková premenná, tak $\text{vars}(p) = \{p\}$.
- Ak A a B sú formuly, tak $\text{vars}(\neg A) = \text{vars}(A)$ a $\text{vars}((A \wedge B)) = \text{vars}((A \vee B)) = \text{vars}((A \rightarrow B)) = \text{vars}(A) \cup \text{vars}(B)$.

Spomeňte si II.2

Je nasledujúce tvrdenie pravdivé? Odpovedzte áno/nie.

Vďaka jednoznačnosti rozkladu má každá formula práve jednu priamu podformulu.

Spomeňte si II.3

Určte pre formulu $((p \vee \neg q) \wedge \neg(q \rightarrow p))$ jej:

- priame podformuly,
- podformuly,
- vytvárajúci strom.

Spomeňte si II.4

Stupeň formuly $((\neg p \leftrightarrow q) \wedge q)$ je
 $\text{vars}(((\neg p \leftrightarrow q) \wedge q)) = \dots\dots\dots$

2.3. Sémantika výrokovej logiky

II.14 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.15 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, zobrať som si čiapku, ...).
- Ako vieme *programátorsky* popísať pravdivosť výrokových premenných v nejakom stave sveta? A *matematicky*?

Definícia 2.19. 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 $v: \mathcal{V} \rightarrow \{t, f\}$).

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.16 Ohodnotenie výrokových premenných

Príklad 2.20. Zoberme $t \neq f$ (napr. $t = 1, f = 0$), $\mathcal{V} = \{a, á, ä, \dots, ž, 0, \dots, 9, _\}^+$.

Dnešné ráno by popísalo ohodnotenie v_1 množiny \mathcal{V} , kde (okrem iného):

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

Pondelkové ráno pred týždňom opisuje ohodnotenie v_2 , kde okrem iného

$$v_2(\text{svieti_slnko}) = f \quad v_2(\text{zobral_som_si_čiapku}) = f$$

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

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

Prečo „okrem iného“?

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

II.17 Spĺňanie výrokových formúl

- Na formulu sa dá pozeráť 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 2.21. Nech v_3 je ohodnotenie množiny $\mathcal{V} = \{a, \dots, z\}^+$, také že

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

Spĺňa svet s týmto ohodnotením formulu $(\neg \text{jim} \rightarrow \neg \text{sarah})$?

Zoberieme vytvárajúcu postupnosť, prejdeme ju zľava doprava:

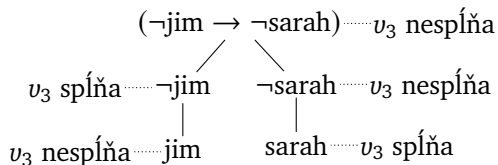
Formulu	jim	sarah	$\neg \text{jim}$	$\neg \text{sarah}$	$(\neg \text{jim} \rightarrow \neg \text{sarah})$
ohodnotenie v_3	nespĺňa	spĺňa	spĺňa	nespĺňa	nespĺňa

II.18 Spĺňanie výrokových formúl – vytvárajúci strom

Príklad 2.21 (pokračovanie).

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

Iná možnosť je použiť vytvárajúci strom:



II.19 Spĺňanie výrokových formúl — program

- Proces zisťovania, či ohodnotenie spĺňa formulu, vieme naprogramovať:

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

- Veľmi podobne vieme zdefinovať splnenie matematicky.

II.20 Spĺňanie výrokových formúl — definícia

Definícia 2.22. 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 $(A \vee B)$ 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* skráteno 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 2.23. Nech v_3 je ohodnotenie množiny $\mathcal{V} = \{a, \dots, z\}^+$, také že

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

Zistime, ktoré z formúl

$$\begin{aligned} & ((\text{kim} \vee \text{jim}) \vee \text{sarah}) \\ & (\text{kim} \rightarrow \neg \text{sarah}) \quad (\text{jim} \rightarrow \text{kim}) \quad (\neg \text{jim} \rightarrow \neg \text{sarah}) \end{aligned}$$

ohodnotenie v_3 spĺňa a ktoré nespĺňa.

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

2.4. Tautológie, (ne)splniteľnosť, falzifikovateľnosť

II.22 Spĺňanie z hľadiska formuly

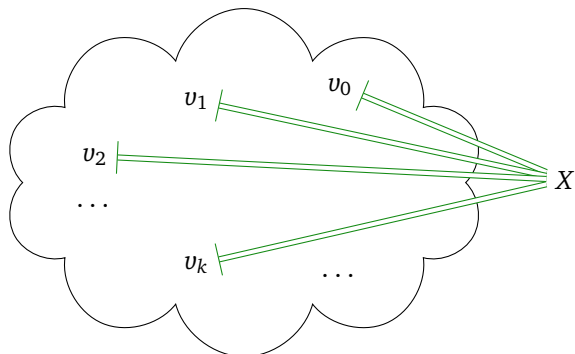
- Doteraz sme sa na spĺňanie pozerali z hľadiska **jedného ohodnotenia** (stavu sveta) a zisťovali sme, **ktoré formuly** sú v ňom splnené
- Obráťme teraz perspektívu:
vyberme si **jednu formulu** a zisťujeme, **ktoré ohodnotenia** ju spĺňajú, teda ktoré stavy sveta vyhovujú podmienke vyjadrenej formulou

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

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

Tvrdenie 2.25. *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 $\text{vars}(X)$ 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?

Príklad 2.26. Zistíme, či je $X = (\neg(p \wedge q) \rightarrow (\neg p \vee \neg q))$ tautológiou.

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

v							
p	q	$(p \wedge q)$	$\neg(p \wedge q)$	$\neg p$	$\neg q$	$(\neg p \vee \neg q)$	$(\neg(p \wedge q) \rightarrow (\neg p \vee \neg q))$
f	f	\neq	\models	\models	\models	\models	\models
t	f	\neq	\models	\neq	\models	\models	\models
f	t	\neq	\models	\models	\neq	\models	\models
t	t	\models	\neq	\neq	\neq	\neq	\models

Pretože všetky skúmané ohodnotenia spĺňajú X , je X tautológiou.

II.26 Ohodnotenia zhodujúce sa na premenných formuly

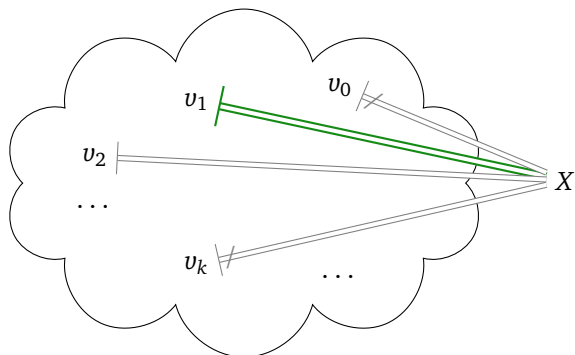
Dôkaz. Indukciou na stupeň formuly X .

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 $v_2 \models p$.

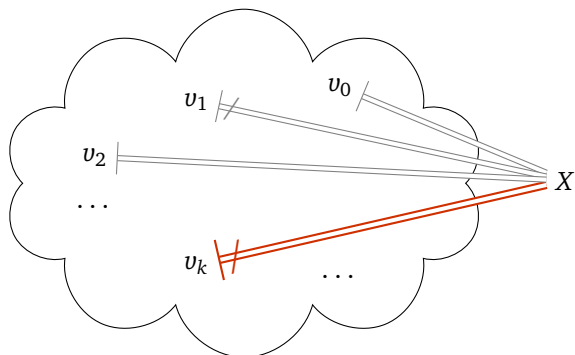
Krok: Nech X je stupňa $n > 0$ a tvrdenie platí pre všetky formuly stupňa nižšieho ako n (indukčný predpoklad). Zoberme ľubovoľné ohodnotenia v_1 a v_2 , ktoré sa zhodujú na premenných v X . Podľa definície stupňa a jednoznačnosti rozkladu nastáva práve jeden z prípadov:

- $X = \neg A$ 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 $v_1 \models A$ vtt $v_2 \models A$, a teda $v_1 \models \neg A$ vtt $v_1 \not\models A$ vtt $v_2 \not\models A$ vtt $v_2 \models \neg A$.
- $X = (A \wedge B)$ 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.

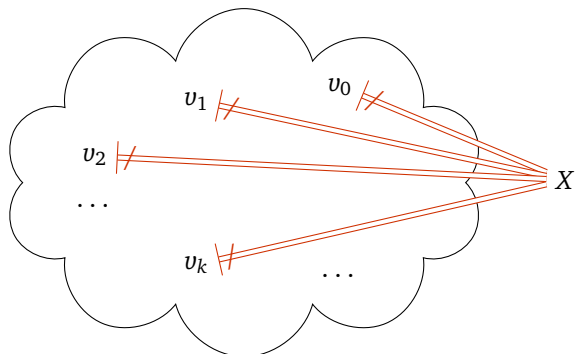
□



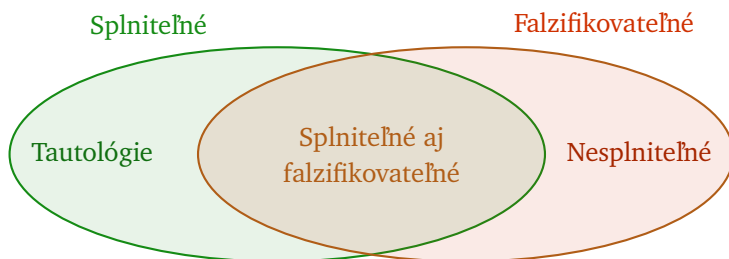
Definícia 2.27. Formulu X nazveme *splniteľnou* vtt **nejaké** ohodnotenie výrokových premenných **spĺňa** X (teda **existuje** také ohodnotenie výrokových premenných v , že $v \models X$).



Definícia 2.28. Formulu X nazveme *falzifikovateľnou* vtt **nejaké** ohodnotenie výrokových premenných **nespĺňa** X (teda **existuje** také ohodnotenie výrokových premenných v , že $v \not\models X$).



Definícia 2.29. Formulu X nazveme *nesplniteľnou* vtt **každé** ohodnotenie výrokových premenných **nesplní** X (teda **pre každé** ohodnotenie výrokových premenných v platí $v \not\models X$).



- 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.5

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 2.30. *Formula X je tautológia vtt keď $\neg X$ je nesplniteľná.*

Dôkaz. (\Rightarrow) 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 $\neg X$ je nesplniteľná. To znamená, že pri každom ohodnotení výrokových premenných je $\neg X$ nesplnená. Podľa definície spĺňania je teda X pri každom ohodnotení splnená, a teda je tautológia. \square

III.2 Teórie

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

Definícia 2.31. *(Výrokovologickou) teóriou nazývame každú množinu formúl.*

Dohoda

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

Príklad 2.32. Formalizácia problému pozývania známych na párty je teóriou:

$$T_{\text{party}} = \{ ((\text{kim} \vee \text{jim}) \vee \text{sara}), \quad (\text{kim} \rightarrow \neg \text{sara}), \\ (\text{jim} \rightarrow \text{kim}), \quad (\neg \text{jim} \rightarrow \neg \text{sara}) \}$$

Pojem splňania sa jednoducho rozšíri na teórie.

Definícia 2.33. 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 *modelom* teórie T .

Príklad 2.34. Aké ohodnotenie spĺňa (teda je modelom) T_{party} ?

Tvrdenie 2.35. *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 splňaní formúl. Dôkaz sporom, lebo množina formúl môže byť nekonečná.

2.5. Výrokovologické vyplývanie

- Kedy je teória „zlá“?
- Keď nepopisuje žiaden svet (stav sveta).
- „Dobrá“ je teda taká teória, ktorá má aspoň jeden model.

Definícia 2.36. Teória T je *súčasne výrokovologicky splniteľná* (skrátene *splniteľná*) vtt existuje aspoň jeden model T .

Teória je *nesplniteľná* vtt nie je splniteľná.

Príklad 2.37. T_{party} je súčasne splniteľná množina formúl.

$T_{\text{party}} \cup \{\text{sara}\}$ je súčasne nesplniteľná množina formúl.

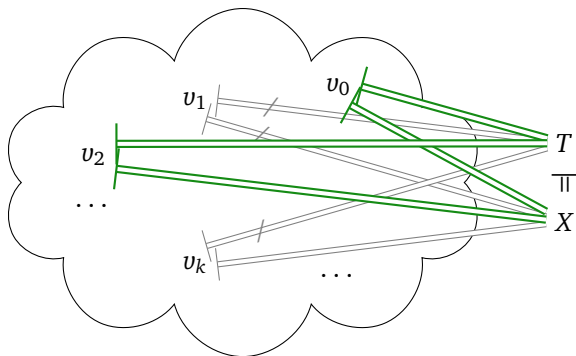
- Aký je účel teórií? Kedy je teória užitočná?
 - Keď z nej dokážeme *odvodiť* (uvažovaním alebo počítaním) $\langle \text{presentation} \rangle$ *doteraz neznáme skutočnosti* (teda nezapísané v teórii),
ktoré platia vo všetkých stavoch sveta spĺňajúcich teóriu.

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

Príklad 2.38. 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

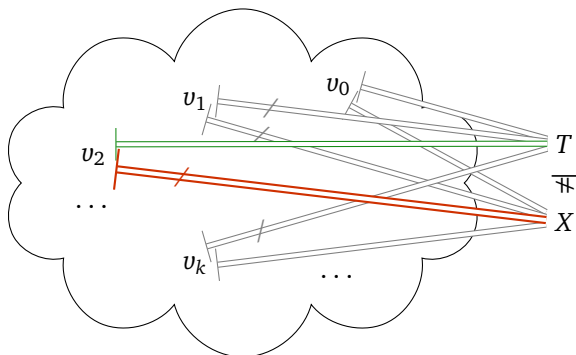


Definícia 2.39 (Výrokovologické vyplývanie). Z teórie T výrokovologicky vyplýva formula X

(tiež X je výrokovologickým dôsledkom T , skráteno $T \models X$) vtt

každé ohodnotenie výrokových premenných, ktoré spĺňa T , spĺňa aj X .

III.7 Nevyplývanie



Príklad 2.40. Ktoré atomické formuly a ich negácie nevyplývajú z T_{party} ?

Vyšplýva z T_{party} formula ($\text{kim} \rightarrow \text{jim}$)?

III.8 Vyplývanie a (ne)splniteľnosť

Použitie SAT solvera na rozhodovanie vyplývania je založené na:

Tvrdenie 2.41. Formula X výrokologicky vyplýva z teórie T vtt množina $T_1 = T \cup \{\neg X\}$ je nesplniteľná.

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

(\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 $\neg X$ je nesplnená pri v , a teda v nespĺňa T_1 .

(\Leftarrow) 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 . \square

III.9 Nezávislosť

Definícia 2.42. Formula X je nezávislá od teórie T , ak existuje dvojica ohodnotení v_1, v_2 spĺňajúcich T , pričom v_1 spĺňa X , ale v_2 nespĺňa X .

Príklad 2.43. Ktorá atomická formula je nezávislá od T_{party} ?

Je aj jej negácia nezávislá od T_{party} ?

III.10 Vzťahy vyplývania, implikácií a tautológií

Tvrdenie 2.44. Nech S a T sú teórie, $S \subseteq T$, A je formula.

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

Tvrdenie 2.45. Nech T je teória, nech $A, B, A_1, A_2, \dots, A_n$ sú formuly.

- a) $T \cup \{A\} \models B$ vtt $T \models (A \rightarrow B)$.
- b) $\{\}$ $\models A$ vtt A je tautológia ($\models A$).
- c) Nasledujúce tvrdenia sú ekvivalentné:
- i. $\{A_1, A_2, \dots, A_n\} \models B$
 - ii. $\{((\dots(A_1 \wedge A_2) \wedge \dots) \wedge A_n)\} \models B$
 - iii. $\{\} \models ((\dots(A_1 \wedge A_2) \wedge \dots) \wedge A_n \rightarrow B)$
 - iv. $\models (((\dots(A_1 \wedge A_2) \wedge \dots) \wedge A_n) \rightarrow B)$

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 2.46. Dve formuly X a Y sú (výrokovologicky) ekvivalentné ($X \Leftrightarrow Y$) 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 $((X \rightarrow Y) \wedge (Y \rightarrow X))$.

Tvrdenie 2.47. Formuly X a Y sú výrokovologicky ekvivalentné vtt formula $(X \leftrightarrow Y)$ je tautológia.

Ako súvisí ekvivalencia formúl s vyplývaním?

Tvrdenie 2.48. *Formuly X a Y sú ekvivalentné vtt $\{X\} \models Y$ a $\{Y\} \models X$.*

Dôkaz. (\Rightarrow) 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.

(\Leftarrow) 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. \square

Tvrdenie 2.49 (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 .*

Dôkaz. Nech X , Y a Z sú formuly. Nech X je ekvivalentná s Y 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. \square

2.7. Ekvivalentné úpravy

III.15 Ekvivalentné úpravy

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

$$\begin{array}{lcl} \text{Príklad 2.50. } A = \neg\neg(r \wedge q) & B = (r \wedge q) & X = (p \rightarrow \neg\neg(r \wedge q)) \\ & & \Downarrow \\ & & Y = (p \rightarrow (r \wedge q)) \end{array}$$

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 $(r \wedge q)$ za p
v známej ekvivalencii medzi $\neg\neg p$ a p (princíp dvojitej negácie)

$$\begin{array}{lcl} \text{Príklad 2.51. } C = \neg\neg p & D = p & \\ & \Downarrow & \Downarrow \\ A = \neg\neg(r \wedge q) & B = (r \wedge q) & \end{array}$$

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 2.52 (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 ℓ je dĺžka A

kým nie si na konci X :

ak sa nasledujúcich ℓ 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 $b \in \{\wedge, \vee, \rightarrow\}$:

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

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

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

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

$$\text{ak } A \neq p$$

$$\text{ak } A \neq \neg X$$

$$\text{ak } A \neq (X \ b \ Y)$$

Korektnosť ekvivalentných úprav vyjadrujú nasledujúce tvrdenia:

Tvrdenie 2.53 (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 2.54 (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 2.55. *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 .

Veta 2.56. *Nech A , B a C sú ľubovoľné formuly, \top je ľubovoľná tautológia a \perp je ľubovoľná nespĺniteľná formula.*

Nasledujúce dvojice formúl sú ekvivalentné:

$$(A \wedge (B \wedge C)) \text{ a } ((A \wedge B) \wedge C) \quad \text{asociatívnosť}$$

$$(A \vee (B \vee C)) \text{ a } ((A \vee B) \vee C)$$

$$(A \wedge B) \text{ a } (B \wedge A) \quad \text{komutatívnosť}$$

$$(A \vee B) \text{ a } (B \vee A)$$

$$(A \wedge (B \vee C)) \text{ a } ((A \wedge B) \vee (A \wedge C)) \quad \text{distributívnosť}$$

$$(A \vee (B \wedge C)) \text{ a } ((A \vee B) \wedge (A \vee C))$$

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

$$\neg(A \vee B) \text{ a } (\neg A \wedge \neg B) \quad \text{pravidlá}$$

$$\neg\neg A \text{ a } A \quad \text{dvojitá negácia}$$

Veta 2.56 (Pokračovanie).

$(A \wedge A) \alpha A$	<i>idempotencia</i>
$(A \vee A) \alpha A$	
$(A \wedge \top) \alpha A$	<i>identita</i>
$(A \vee \perp) \alpha A$	
$(A \vee (A \wedge B)) \alpha A$	<i>absorpcia</i>
$(A \wedge (A \vee B)) \alpha A$	
$(A \vee \neg A) \alpha \top$	<i>vylúčenie tretieho</i>
$(A \wedge \neg A) \alpha \perp$	<i>spor</i>
$(A \rightarrow B) \alpha (\neg A \vee B)$	<i>nahradenie \rightarrow</i>

2.8. Konjunktívna a disjunktívna normálna forma

Dohoda

Nech A_1, A_2, \dots, A_n je konečná postupnosť formúl.

- Formulu $((A_1 \wedge A_2) \wedge A_3) \wedge \dots \wedge A_n$ budeme skráteno zapisovať $(A_1 \wedge A_2 \wedge A_3 \wedge \dots \wedge A_n)$, prípadne $\bigwedge_{i=1}^n A_i$ a nazývať *konjunkcia postupnosti formúl* A_1, \dots, A_n .
- Formulu $((A_1 \vee A_2) \vee A_3) \vee \dots \vee A_n$ budeme skráteno zapisovať $(A_1 \vee A_2 \vee A_3 \vee \dots \vee A_n)$, prípadne $\bigvee_{i=1}^n A_i$ a nazývať *disjunkcia postupnosti formúl* A_1, \dots, A_n .
- Pre $n = 1$ chápeme samotnú formulu A_1 ako konjunkciu aj ako disjunkciu jednoprvkovej postupnosti formúl A_1 .
- Konjunkciu prázdnej postupnosti formúl ($n = 0$) chápeme ako ľubovoľnú tautológiu (napríklad $(p_1 \vee \neg p_1)$) a označujeme ju \top .
- Disjunkciu prázdnej postupnosti formúl chápeme ako ľubovoľnú nesplniteľnú formulu (napríklad $(p_1 \wedge \neg p_1)$) a označujeme ju \perp alebo \square .

Definícia 2.53. • Výrokovú premennú alebo negáciou premennej nazývame *literál*.

- Disjunkciu literálov nazývame *klauzula* (tiež „klaúza“).
- 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 2.54. Ktoré z nasledujúcich formúl sú literálmi, klauzulami, sú v CNF, v DNF:

$$\begin{array}{ll}
 A_1 = p & A_6 = ((p \wedge \neg q) \vee (\neg p \wedge r) \vee (\neg p \wedge q \wedge \neg r)) \\
 A_2 = \neg q & A_7 = ((\neg p \vee q \vee \neg r) \wedge (q \rightarrow r)) \\
 A_3 = \square & A_8 = ((\neg p \vee \neg q) \wedge (p \vee r) \wedge (p \vee q \vee \neg r)) \\
 A_4 = (p \vee \neg q) & A_9 = ((\neg p \vee (p \wedge r)) \wedge (p \vee q \vee \neg r)) \\
 A_5 = (p \wedge \neg q) & A_{10} = ((\neg p \vee p \vee r) \wedge (\neg(p \vee q) \vee \neg r))
 \end{array}$$

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: neúplnosť, složitost, nutnost*. Academia, 2002. Prístupné aj na <http://www1.cuni.cz/~svejdar/book/LogikaSve2002.pdf>.