

# Prednášky z Matematiky (4) — Logiky pre informatikov

Ján Kľuka, Jozef Šiška

Letný semester 2018/2019

## Obsah

<b>I. O logike a tomto kurze</b>	
Syntax výrokovej logiky	<b>3</b>
<b>1. Úvod</b>	<b>3</b>
1.1. O logike . . . . .	3
1.2. O kurze . . . . .	11
<b>2. Výroková logika</b>	<b>12</b>
2.1. Opakovanie: Výroková logika v prirodzenom jazyku . . . . .	12
2.2. Syntax . . . . .	13
<b>II. Sémantika výrokovej logiky</b>	<b>19</b>
2.3. Sémantika . . . . .	25
2.4. Tautológia, (ne)splniteľnosť, falzifikovateľnosť . . . . .	30
<b>III. Vyplyvanie a ekvivalencia</b>	<b>36</b>
2.5. Vyplyvanie . . . . .	37

2.6. Ekvivalencia . . . . .	41
2.6.1. Ekvivalentné úpravy . . . . .	43
2.6.2. Konjunktívna a disjunktívna normálna forma . . . . .	47

#### IV. CNF

<b>Hilbertovský kalkul</b>	<b>49</b>
2.7. Logické kalkuly . . . . .	54
2.8. Hilbertovský kalkul . . . . .	56

#### V. Tablový kalkul a jeho korektnosť

2.9. Tablový kalkul . . . . .	62
2.9.1. Korektnosť . . . . .	70

## I. prednáška

# O logike a tomto kurze

## Syntax výrokovkej logiky

18. februára 2019

## 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 stavy sveta a modely

Tvrdenie (teória) rozdeľuje triedu **možných stavov sveta** (interpretácií) na dve podtriedy:

|= stavy, v ktorých je pravdivé — **modely** tvrdenia (teórie),

≠ stavy, v ktorých je nepravdivé.

Tvrdenie aj teória môžu mať viacero modelov, ale aj žiaden.

*Príklad 1.2.* Vymenujme možné stavy prítomnosti Kim, Jima a Sarah na párty.

Zistíme, v ktorých sú pravdivé jednotlivé tvrdenia našej teórie a celá teória.

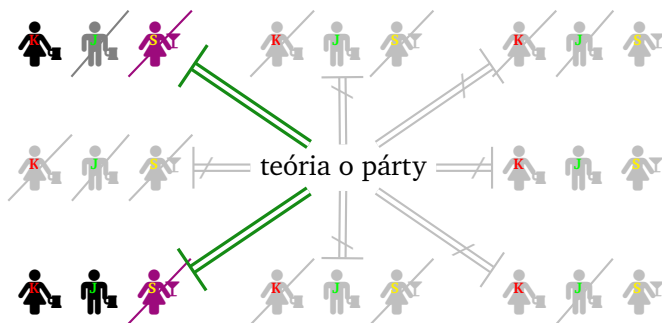


### I.4 Logické dôsledky

**Logickými dôsledkami** teórie sú tvrdenia, ktoré sú pravdivé vo **všetkých modeloch** teórie

*Príklad 1.3.* Logickým dôsledkom teórie (P1), (P2), (P3) je napríklad:

**Sarah nepôjde na párty.**



## I.5 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 (P1) ak na párty pôjde Kim, tak nepôjde Sarah, a že (P2) ak pôjde Jim, tak pôjde Kim.

Predpokladajme, že na párty pôjde Jim.

Teda podľa (P2) pôjde aj Kim.

Teda podľa (P1) nepôjde Sarah.

Teda podľa uvedenej úvahy: Ak na párty pôjde Jim, tak nepôjde Sarah.

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

## I.6 Usudzovacie pravidlá

Už Aristoteles zistil, že niektoré **správne úsudky sa dajú rozpoznať podľa svojej formy**, bez ohľadu na konkrétny obsah

Ak pôjde Jim, tak pôjde Kim.

Pôjde Jim.

---

Pôjde Kim.

Ak je dilítium dekryštalizované,  
tak antihmota neprúdi.

Dilítium je dekryštalizované.

---

Antihmota neprúdi.

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

$$\left. \begin{array}{l} \text{Ak } A, \text{ tak } B. \\ A. \\ \hline B. \end{array} \right\} \begin{array}{l} \text{vzory premís} \\ \text{vzor záveru} \end{array}$$

### I.7 Korektné usudzovacie pravidlá a dedukcia

**Korektné** pravidlo odvodí z pravdivých premís pravdivý záver

*Príklad 1.5. Pravidlo modus ponens*

Ak  $A$ , tak  $B$ .

$A$ .

---

$B$ .

je korektné.

**Dôkaz** je teda **postupnosť použití korektných usudzovacích pravidiel** (najlepšie *samozrejmych* pre čitateľa dôkazu)

**Dedukcia** je usudzovanie, pri ktorom sa používajú iba korektné pravidlá

### I.8 Nededuktívne pravidlá

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

**Indukcia** — zovšeobecnenie:

Videl som tisíc havranov.

Žiaden nebol inej farby ako čiernej.

---

Všetky havrany sú čierne.

Platí aj pre biele bicykle?

**Abdukcia** — odvodzovanie možných príčin z následkov:

Ak je batéria vybitá, auto nenašartuje.  
Ak je nádrž prázdna, auto nenašartuje.  
Nádrž nie je prázdna.  
Auto nenašartovalo.

---

Batéria je vybitá.

Čo ak nám kuna  
prehrýzla káble?

## 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 dýchateľná?

### I.9 Nededuktívne pravidlá

---

- **Závery nededuktívnych pravidiel** treba považovať za **hypotézy** — plauzibilné, ale **neoverené** tvrdenia
- Hypotézy je **nutné preverovať!**
- Niektoré špeciálne prípady nededuktívnych pravidiel sú korektné, 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.10 Ťažkosti s prirodzeným jazykom

---

**Prirodzený jazyk** je problematický:

- Viacznačné slová: Miro *je* v posluchárni F1.
- Viacznačné tvrdenia: Videl som dievča v sále *s ďalekohľadom*.
- Ťažko syntakticky analyzovateľné tvrdenia:

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 znení neskorších predpisov*

- Výnimky a obraty so špeciálnym ustáleným významom: Nikto *nie* je dokonalý.

### I.11 Formálne jazyky

Problémy prirodzených jazykov sa obchádzajú použitím **formálnych** jazykov

- Presne definovaná, zjednodušená syntax (pravidlá zápisu tvrdení) a sémantika (význam)
- Niekoľko formálnych jazykov už poznáte: aritmetika, jazyky fyzikálnych a chemických vzorcov, programovacie jazyky, ...
- Problémy z reálneho sveta opísané v prirodzenom jazyku musíme najprv **formalizovať**, a potom naň môžeme použiť logický aparát

### I.12 Formalizácia poznatkov

- S formalizáciou ste sa už stretli — napríklad pri riešení slovných úloh

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

- Stretli ste sa už aj s formálnym jazykom výrokovej logiky



*Príklad 1.6.* 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.13 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 (násobilka, aritmetika),
  - riešenie lineárnych rovníc (kalkul lineárnej algebry),
  - derivovanie, integrovanie, riešenie diferenciálnych rovníc (kalkul matematickej analýzy)

...

Poznáte už aj jeden logický kalkul — ekvivalentné úpravy

Sú korektné, ale nie vždy úplné

#### I.14 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.15 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 — odvodzovanie neuložených faktov, 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.16

---

##### ***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.17 Čím sa budeme zaoberať v tomto kurze

---

**Teoreticky** • Jazykmi výrokovkej 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 — for-  
múl a termov)
- Programovaním vlastných jednoduchých automatických dokazo-  
vačov

**Filozoficky** • Zamýšľanými a nezamýšľanými okolnosťami platnosti tvr-  
dení

- Obmedzeniami vyjadrovania a usudzovania

## 2. Výroková logika

### 2.1. Opakovanie: Výroková logika v prirodzenom jazyku

*Výrok* – veta, o pravdivosti ktorej má zmysel uvažovať (zväčša oznamovania).

*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*

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 *logickú* spojku.

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

#### I.21 (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.22 Syntax výrokovej logiky

---

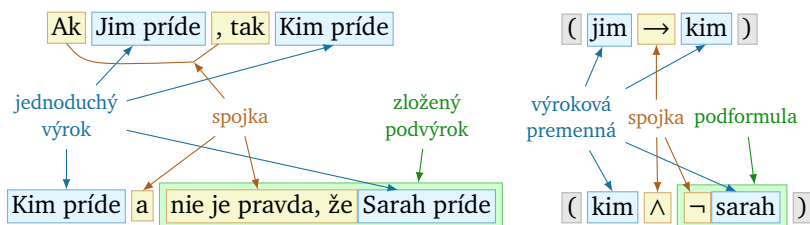
- Syntax sú pravidlá budovania viet v jazyku

- 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.23 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**

**Definícia 2.3.** Symbolmi jazyka výrokovkej logiky sú:

- *výrokové premenné* z nejakej spočítateľnej množiny  $\mathcal{V} = \{p_1, p_2, \dots, p_n, \dots\}$ , ktorej prvkami nie sú symboly  $\neg, \wedge, \vee, \rightarrow, (, )$ , ani jej prvky tieto symboly neobsahujú;
- *logické symboly (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 symboly*:  $(, )$  (*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.

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 vyzeráť formuly vybudované nad touto množinou?

- Samotné premenné, napr. sarah.
  - Negácie premenných, napr.  $\neg$ 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.
  - Podobne ako 0 pri matematickej indukcii
2. Opíšeme, ako sa z jednoduchších formúl skladajú zložitejšie.
  - Podobne ako indukčný krok pri matematickej indukcii

## I.27 Výrokové formuly

---

**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  $\mathcal{E}$  (nazývanými *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 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 niektorý predchádzajúci člen postupnosti, alebo
- má jeden z tvarov  $(A \wedge B)$ ,  $(A \vee B)$ ,  $(A \rightarrow B)$ , kde  $A$  a  $B$  sú niektoré 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 výrokovkej logiky

25. februára 2019

### 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 výrokovkej logiky

---

Čo keby sme zadefinovali „formuly“ takto?

#### Definícia „formúl“



Množina  $\mathcal{E}$  všetkých výrokových „formúl“ nad množinou výrokových premenných  $\mathcal{V}$  je najmenšia množina postupností symbolov, kde platí:

- každá výroková premenná  $p \in \mathcal{V}$  je „formulou“ z  $\mathcal{E}$ ;
- ak  $A$  je „formula“ z  $\mathcal{E}$ , tak aj postupnosť symbolov  $\neg A$  je „formulou“ z  $\mathcal{E}$ ;
- 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 Problémy s vytvárajúcou postupnosťou

Vytvárajúca postupnosť popisuje konštrukciu formuly podľa definície formúl:

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

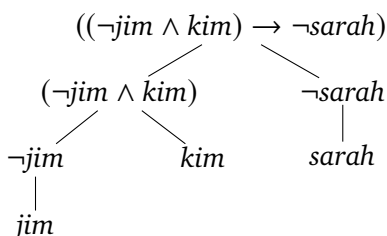
ale

- môže obsahovať „zbytočné“ prvky;
- nie je jasné *ktoré* z predchádzajúcich formúl sa *bezprostredne* použijú na vytvorenie nasledujúcej formuly.

Akou „dátovou štruktúrou“ vieme vyjadriť konštrukciu formuly bez týchto problémov?

## II.6 Vytvárajúci strom

Konštrukciu si ale vieme predstaviť ako *strom*:



Takéto stromy voláme *vytvárajúce*.

Ako ich *presne* a *všeobecne* popíšeme — zadefinujeme?

## II.7 Vytvárajúci strom formuly

**Definícia 2.12.** *Vytvárajúci strom*  $T$  pre formulu  $X$  je binárny strom 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  $(A \text{ } b \text{ } B)$ , kde  $b$  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.

Uvažujme formulu:

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

- Ako nazveme formuly, z ktorých vznikla?

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

- Ako nazveme formuly, z ktorých *bezprostredne/priamo* vznikla?

$$(\neg jim \wedge kim) \quad \text{a} \quad \neg sarah$$

- Ako tieto pojmy presne zadefinujeme?

**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  $Z$ .

## II.10 Meranie syntaktickej zložitosti formúl

---

Miera zložitosti/veľkosti formuly:

- Jednoduchá: dĺžka, teda počet symbolov
  - Počíta aj pomocné symboly
  - Atóm má mieru 1, nič nemá mieru 0
- Lepšia: počet netriviálnych krokov pri konštrukcii formuly
  - pridanie negácie,
  - spojenie formúl spojkou

Lepšiu mieru nazývame *stupeň formuly*

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

## II.11 Meranie syntaktickej zložitosti formúl

---

Ako stupeň zadefinujeme?

Podobne ako sme zadefinovali formuly — induktívne:

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

## II.12 Stupeň 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:*

$$\deg(p) = 0,$$

$$\deg(\neg A) = \deg(A) + 1,$$

$$\deg((A \wedge B)) = \deg((A \vee B)) = \deg((A \rightarrow B)) = \deg(A) + \deg(B) + 1.$$

## II.13 Indukcia na stupeň formuly

---

**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  $P$  ( $P = \mathcal{E}$ ).*

## II.14 Množina výrokových premenných formuly

---

**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 výrokových premenných formúl  $(A \wedge B)$ ,  $(A \vee B)$  a  $(A \rightarrow B)$ .



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

- 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:

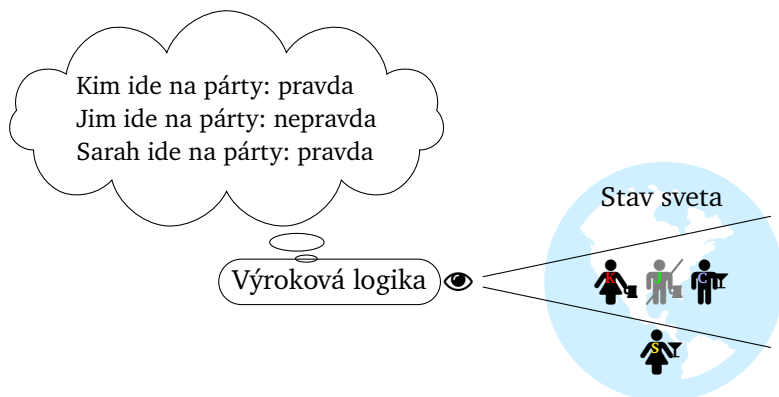
- priame podformuly,
- podformuly,
- vytvárajúci strom.

### 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

- Syntax jazyka výrokovej logiky hovorí iba o tom, ako sa zapisujú formuly ako postupnosti symbolov.
- Nehovorí nič o význame týchto postupností.
- Ten im dáva *sémantika* jazyka výrokovej logiky.



## II.18 Predstava výrokovej logiky o svete

Výroková logika vníma svet *veľmi zjednodušene*.

Zaujíma ju iba

- obmedzené množstvo jednoduchých výrokov,
- ich pravdivosť alebo nepravdivosť v danom stave sveta.

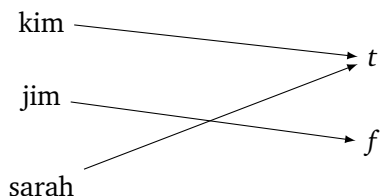
## II.19 Formalizácia výrokového pohľadu na svet

- V matematickej výrokovej logike jednoduché výroky predstavujú výrokové premenné
- Ako vieme *programátorsky* popísať pravdivosť výrokových premenných v nejakom stave sveta?
- A *matematicky*?

## II.20 Ohodnotenie výrokových premenných

**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.21 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.22 Splňanie 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  $(\neg \text{jim} \rightarrow \neg \text{sarah})$ ?

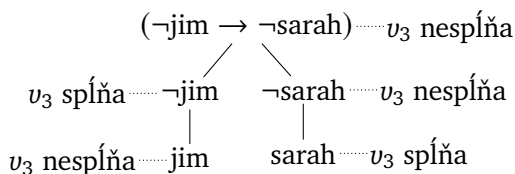
Zoberieme vytvárajúcu postupnosť, prejdeme ju zľava doprava:

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

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:



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

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

- Veľmi podobne vieme zadať splnenie matematicky.

**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  $X$*  skratene 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  $v$ .

**Definícia 2.22** (symbolicky). 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:

$$\begin{array}{ll}
 v \models p & \text{vtt} \quad v(p) = t; \\
 v \models \neg A & \text{vtt} \quad v \not\models A; \\
 v \models (A \wedge B) & \text{vtt} \quad v \models A \text{ a } v \models B; \\
 v \models (A \vee B) & \text{vtt} \quad v \models A \text{ alebo } v \models B; \\
 v \models (A \rightarrow B) & \text{vtt} \quad v \not\models A \text{ alebo } v \models B.
 \end{array}$$

Vzťah  $\models$  je súčasťou programovacích jazykov – vyhodnocovanie boolovských výrazov

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

$$((\text{kim} \vee \text{jim}) \vee \text{sarah})$$

$$(\text{kim} \rightarrow \neg \text{sarah}) \quad (\text{jim} \rightarrow \text{kim}) \quad (\neg \text{jim} \rightarrow \neg \text{sarah})$$

ohodnotenie  $v_3$  spĺňa a ktoré nespĺňa.

$\text{deg}(X)$	$v_3 \models X$	$v_3 \not\models X$
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

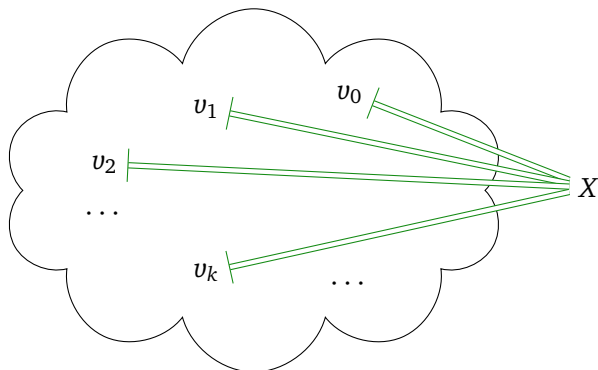
- Predchádzajúca definícia a príklad:  
spĺňanie **mnohých formúl jedným ohodnotením** (stavom sveta)
- Obráťme perspektívu:  
spĺňanie **jednej formuly mnohými ohodnoteniami**
- Ktoré stavy sveta vyhovujú podmienke vyjadrenej formulou?

### Dohoda

V 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  $v \models X$ ).

## II.31 Tautológia — testovanie

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

## II.32 Tautológia — testovanie

**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.

**Dôkaz.** Indukciou na stupeň formuly  $X$ .

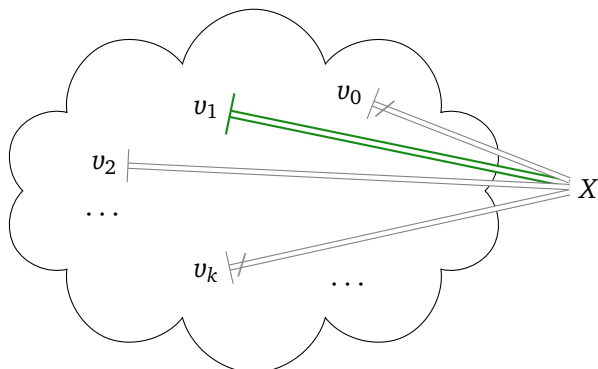
**Báza:** Nech  $X$  je stupňa 0. Podľa vety o jednoznačnosti rozkladu a definície stupňa musí byť  $X = p$  pre nejakú výrokovú premennú. Zoberme ľubovoľné ohodnotenia  $v_1$  a  $v_2$ , ktoré sa zhodujú na premenných v  $X$ , teda aj na  $p$ . Podľa definície spĺňania  $v_1 \models p$  vtt  $v_1(p)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

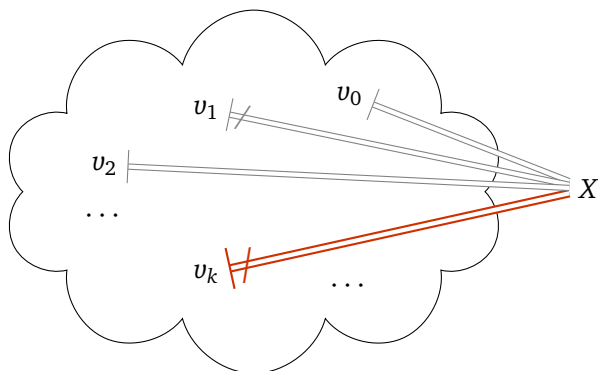
- $X = \neg A$  pre práve jednu formulu  $A$ . Pretože  $\deg(X) = \deg(A) + 1 > \deg(A)$ , podľa ind. predpokladu tvrdenie platí pre  $A$ . Ohodnotenia  $v_1$  a  $v_2$  sa zhodujú na premenných v  $A$  (rovnaké ako v  $X$ ). Preto  $v_1 \models A$  vtt  $v_2 \models A$ , a teda  $v_1 \models \neg A$  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.

□

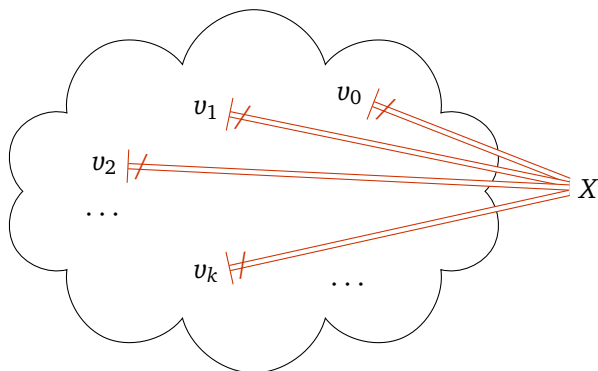




**Definícia 2.27.** Formulu  $X$  nazveme *splniteľnou* vtt **nejaké** ohodnotenie výrokových premenných **spĺňa**  $X$  (teda **existuje** také ohodnotenie výrokových premenných  $v$ , že  $v \models X$ ).



**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 **nesplňa**  $X$  (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 a ekvivalencia

4. marca 2019

#### III.1 Tautológie a (ne)splniteľnosť

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

*Dôkaz.*  $(\Rightarrow)$  Nech  $X$  je tautológia, teda je splnená pri každom ohodnotení výrokových premenných. To znamená, že  $\neg X$  je nespĺnená pri každom ohodnotení (podľa definície splnenia formuly ohodnotením), a teda  $\neg X$  je nespĺniteľná.

$(\Leftarrow)$  Opačne, nech  $\neg X$  je nespĺniteľná. To znamená, že pri každom ohodnotení výrokových premenných je  $\neg X$  nespĺnená. 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 výrokových 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, nech  $v$  je ohodnotenie výrokových premených. 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)  $T_{\text{party}}$ ?

**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.*  $T_{\text{party}}$  je súčasne splniteľná množina formúl.

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

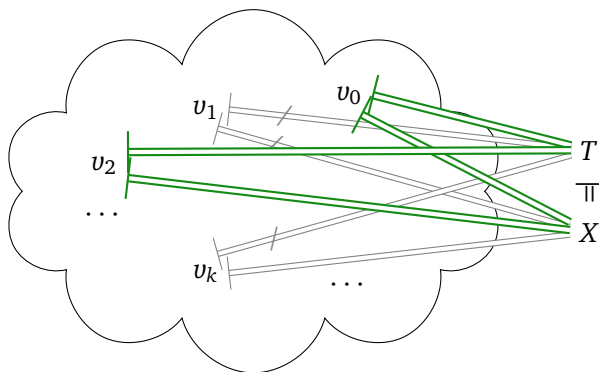
- Aký je účel teórií? Kedy je teória užitočná?
  - Keď z nej dokážeme *odvodiť* (uvažovaním alebo počítaním) *doteraz neznáme skutočnosti* (teda nezapísané v teórii), ktoré platia vo všetkých stavoch sveta spĺňajúcich teóriu.

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

*Príklad 2.38.* Všimnime si, že v každom ohodnotení, ktoré spĺňa  $T_{\text{party}}$ , je splnená aj premenná  $\text{kim}$ .

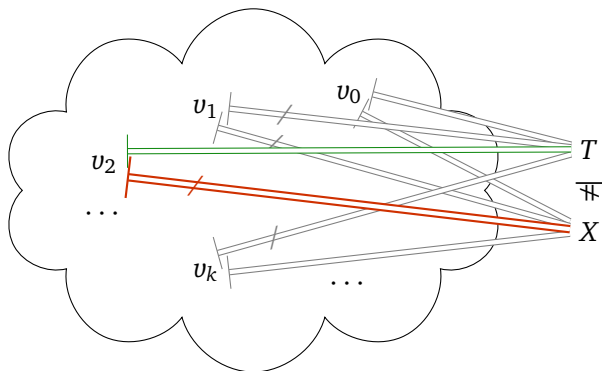
Ktorá ďalšia formula vyplýva z  $T_{\text{party}}$ ?

### III.6 Výrokovologické vyplývanie



**Definícia 2.39** (Výrokovologické vyplývanie). Z teórie  $T$  výrokovologicky vyplýva formula  $X$  (tiež  $X$  je výrokovologickým dôsledkom  $T$ , skrátené  $T \models X$ ) vtt každé ohodnotenie výrokových premenných, ktoré spĺňa  $T$ , spĺňa aj  $X$ .

### III.7 Nevyplyvanie



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

Vyplýva z  $T_{\text{party}}$  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  $T \cup \{\neg X\}$  je nespĺniteľná.*

Prečo je to tak?

### III.9 Vyplývanie a (ne)splniteľnosť – dôkaz

---

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

( $\Rightarrow$ ) Predpokladajme, že  $X$  vyplýva z množiny  $T$ . Nech  $v$  je ľubovoľné ohodnotenie  $\mathcal{V}$ . Potrebujeme ukázať, že  $v$  nespĺňa  $T \cup \{\neg X\}$ . Máme dve možnosti:

- Ak  $v$  nespĺňa  $T$ , tak nespĺňa niektorú formulu  $X_i$  z  $T$ . Formula  $X_i$  patrí aj do  $T \cup \{\neg X\}$ , preto  $v$  nespĺňa ani  $T \cup \{\neg X\}$ .
- Ak  $v$  spĺňa  $T$ , tak  $v$  musí spĺňať aj  $X$  (definícia vyplývania). Potom ale  $v$  nespĺňa  $\neg X$ , a teda  $v$  nespĺňa ani  $T \cup \{\neg X\}$ .

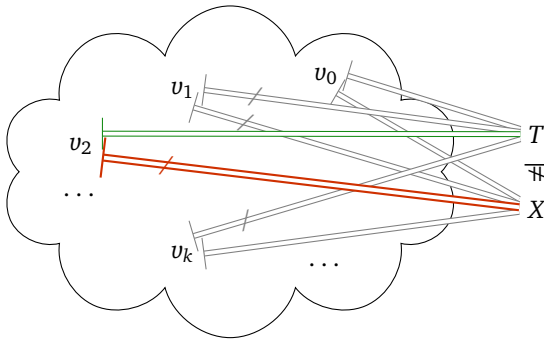
V oboch prípadoch  $v$  nespĺňa  $T \cup \{\neg X\}$ . Pretože  $v$  bolo ľubovoľné, môžeme zovšeobecniť, že žiadne  $v$  nespĺňa  $T \cup \{\neg X\}$ , teda  $T \cup \{\neg X\}$  je nespĺniteľná.

( $\Leftarrow$ ) Opačne, nech  $T \cup \{\neg X\}$  je nespĺniteľná a nech  $v$  je ľubovoľné ohodnotenie  $\mathcal{V}$ . Potrebujeme ukázať, že ak  $v$  spĺňa  $T$ , tak potom  $v$  spĺňa aj  $X$ . Ak  $v$  spĺňa  $T$ , potom spĺňa každé  $X_i$ . Keďže ale  $T \cup \{\neg X\}$  je nespĺniteľná,  $v$  nespĺňa  $T \cup \{\neg X\}$ , preto  $v$  musí nespĺňať  $\neg X$  (jediná zostávajúca formula z  $T \cup \{\neg X\}$ ), čo znamená, že  $v$  spĺňa  $X$ . Pretože  $v$  bolo ľubovoľné, môžeme zovšeobecniť, že pre každé  $v$  platí, že ak  $v$  spĺňa  $T$ , tak  $v$  spĺňa aj  $X$ , teda  $X$  vyplýva z  $T$ .  $\square$

**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  $T_{\text{party}}$ ?

Je aj jej negácia nezávislá od  $T_{\text{party}}$ ?



**Otázka.** Ak z  $T$  nevyplýva formula  $X$ , je pravda, že z  $T$  vyplýva formula  $\neg X$ ?

**Nie!** Na to, aby z  $T$  nevyplývala formula  $X$ , stačí, keď *existuje jediné* ohodnotenie, ktoré spĺňa  $T$ , ale nespĺňa  $X$ .

Na to, aby z  $T$  vyplývala formula  $\neg X$ , je nutné, aby všetky ohodnotenia, ktoré spĺňajú  $T$ , nespĺňali  $X$  (a teda spĺňali  $\neg X$ ).

**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.13 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.14 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  $Y$ .

### III.15 Ekvivalencia formúl a skratka $\leftrightarrow$

---

Ako súvisí 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.

*Skráteno:* Pre všetky formuly  $X$  a  $Y$  platí, že  $X \Leftrightarrow Y$  vtt  $\models (X \leftrightarrow Y)$ .

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  $Z$ .*

sémantická ekvivalencia formúl  
(„ $X$  a  $Y$  sú výrokovologicky ekvivalentné“,  
teda „pre každé ohodnotenie  $v$  platí,  
že  $v \models X$  vtt  $v \models Y$ “)

ekvivalencia  
slovenských  
výrokov  
(„vtedy a len  
vtedy, keď“)

syntaktická  
ekvivalencia  
(postup. symbolov  
( $(X \rightarrow Y) \wedge$   
 $(Y \rightarrow X)$ ))

*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.  $\square$

## 2.6.1. Ekvivalentné úpravy

### III.18 Ekvivalentné úpravy

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

*Príklad 2.50* (Nahradenie podformuly ekvivalentnou).

$$A = \neg\neg(r \wedge q) \quad B = (r \wedge q) \quad X = (p \rightarrow \neg\neg(r \wedge q))$$

$$\Downarrow$$

$$Y = (p \rightarrow \neg(r \wedge q))$$

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

### III.19 Pravidlá ekvivalentných úprav

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

*Príklad 2.51* (Dosadenie za premennú v ekvivalentných  
formulách).  $C = \neg\neg p$        $D = p$

$$\Downarrow \qquad \Downarrow$$

$$A = \neg\neg(r \wedge q) \quad B = (r \wedge q)$$

- 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  $X$ :

### Substitúcia ako cyklus

```
def X[A|B]:  
    Y = ""  
    i = 0  
    while i < len(X):  
        if X[i : i + len(A)] == A:  
            Y += B  
            i += len(A)  
        else:  
            Y += X[i]  
            i += 1  
    return Y
```

Substitúciu si vieme predstaviť aj ako rekurzívne definovanú operáciu: (pu02)

### Substitúcia rekurzívne

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

$$\begin{array}{ll} X[A|B] = B, & \text{ak } A = X \\ p[A|B] = p, & \text{ak } A \neq p \\ (\neg X)[A|B] = \neg(X[A|B]), & \text{ak } A \neq \neg X \\ (X \ b \ Y)[A|B] = ((X[A|B]) \ b \ (Y[A|B])), & \text{ak } A \neq (X \ b \ Y). \end{array}$$

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).

$$(A \wedge A) \text{ a } A \quad \text{idempotencia}$$

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

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

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

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

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

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

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

$$(A \rightarrow B) \text{ a } (\neg A \vee B) \quad \text{nahradenie } \rightarrow$$

## 2.6.2. Konjunktívna a disjunktívna normálna forma

### III.28 Konjunkcia a disjunkcia postupnosti formúl

---

#### Dohoda

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

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

### III.29 Konjunktívny a disjunktívny normálny tvar

---

#### Definícia 2.57.

*Literál* je výroková premenná alebo negácia výrokovej premennej.

*Klauzula* (tiež „klauza“) je *disjunkcia* literálov.

*Formula v disjunktívnom normálnom tvare* (DNF) je *disjunkcia* formúl, z ktorých každá je konjunkciou literálov.

*Formula v konjunktívnom normálnom tvare* (CNF) je *konjunkcia* klauzúl.

*Príklad 2.58.* Ktoré z nasledujúcich formúl sú literálmi, klauzulami, sú v CNF, v DNF?

$$A_1 = p \qquad A_6 = ((p \wedge \neg q) \vee (\neg p \wedge r) \vee (\neg p \wedge q \wedge \neg r))$$

$$A_2 = \neg q \qquad A_7 = ((\neg p \vee q \vee \neg r) \wedge (q \rightarrow r))$$

$$A_3 = \square \qquad A_8 = ((\neg p \vee \neg q) \wedge (p \vee r) \wedge (p \vee q \vee \neg r))$$

$$A_4 = (p \vee \neg q) \qquad A_9 = ((\neg p \vee (p \wedge r)) \wedge (p \vee q \vee \neg r))$$

$$A_5 = (p \wedge \neg q) \qquad A_{10} = ((\neg p \vee p \vee r) \wedge (\neg(p \vee q) \vee \neg r))$$



## IV. prednáška

### CNF

### Hilbertovský kalkul

11. marca 2018

#### IV.1 Existencia DNF a CNF

---

**Veta 2.59.** 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.

*Dôkaz.* 1. Zoberme všetky ohodnotenia  $v_1, \dots, v_n$  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  $X$ .  $\square$

#### 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.  $\neg(A \vee B)$ )?
- **Disjunkcie** sa nachádzajú iba **vnútri konjunkcií** — ako presunieme „vonkajšie“ disjunkcie „dovnútra“ konjunkcií (napr.  $(A \vee (B \wedge C))$ )?

#### IV.3 CNF — trochu lepší prístup — algoritmus

---

##### Algoritmus CNF

1. Nahradíme implikáciu disjunkciou:

$$\bullet (A \rightarrow B) \Leftrightarrow (\neg A \vee B).$$

2. Presunieme  $\neg$  dovnútra pomocou de Morganových pravidiel a pravidla dvojitej negácie.

3. „Roznásobíme“  $\wedge$  s  $\vee$  podľa distributívnosti a komutatívnosti:

$$\bullet (A \vee (B \wedge C)) \Leftrightarrow ((A \vee B) \wedge (A \vee C))$$

$$\bullet ((B \wedge C) \vee A) \Leftrightarrow (A \vee (B \wedge C)) \Leftrightarrow ((A \vee B) \wedge (A \vee C)) \Leftrightarrow ((B \vee A) \wedge (C \vee A))$$

4. Prezátvorkujeme na požadovaný tvar pomocou asociatívnych pravidiel.

**Tvrdenie 2.60.** Výsledná formula alg. CNF je ekvivalentná s pôvodnou a je v CNF.

## Príklad 2.61.

1.  $((a \vee \neg b) \rightarrow \neg(c \vee (d \wedge \neg e)))$
2.  $(\neg(a \vee \neg b) \vee \neg(c \vee (d \wedge \neg e)))$  [1 – nahradenie implikácie]
3.  $((\neg a \wedge \neg \neg b) \vee \neg(c \vee (d \wedge \neg e)))$  [2 – de Morganovo pravidlo]
4.  $((\neg a \wedge b) \vee \neg(c \vee (d \wedge \neg e)))$  [2 – dvojitá negácia]
5.  $((\neg a \wedge b) \vee (\neg c \wedge \neg(d \wedge \neg e)))$  [2 – de Morganovo pravidlo]
6.  $((\neg a \wedge b) \vee (\neg c \wedge (\neg d \vee \neg \neg e)))$  [2 – de Morganovo pravidlo]
7.  $((\neg a \wedge b) \vee (\neg c \wedge (\neg d \vee e)))$  [2 – dvojitá negácia]
8.  $((\neg a \wedge b) \vee \neg c) \wedge ((\neg a \wedge b) \vee (\neg d \vee e))$  [3 – distributívnosť]
9.  $((\neg a \vee \neg c) \wedge (b \vee \neg c)) \wedge ((\neg a \vee (\neg d \vee e)) \wedge (b \vee (\neg d \vee e)))$  [3]
10.  $((\neg a \vee \neg c) \wedge (b \vee \neg c) \wedge (\neg a \vee (\neg d \vee e)) \wedge (b \vee (\neg d \vee e)))$  [4]
11.  $((\neg a \vee \neg c) \wedge (b \vee \neg c) \wedge (\neg a \vee \neg d \vee e) \wedge (b \vee \neg d \vee e))$  [4 – asoc.]

## IV.5 Prečo iba trochu lepší prístup?

Distribúcia  $\vee$  cez  $\wedge$  spôsobuje nárast formuly:

- $A_2 = ((p_1 \wedge q_1) \vee (p_2 \wedge q_2))$   
 $C_2 = ((p_1 \vee p_2) \wedge (p_1 \vee q_2) \wedge (q_1 \vee p_2) \wedge (q_1 \vee q_2))$   
 $A_2 \Leftrightarrow C_2, \quad \deg(A_2) = 3, \quad \deg(C_2) = 7$
- $A_3 = ((p_1 \wedge q_1) \vee (p_2 \wedge q_2) \vee (p_3 \wedge q_3))$   
 $C_3 = ((p_1 \vee p_2 \vee p_3) \wedge (p_1 \vee p_2 \vee q_3)$   
 $\quad \wedge (p_1 \vee q_2 \vee p_3) \wedge (p_1 \vee q_2 \vee q_3)$   
 $\quad \wedge (q_1 \vee p_2 \vee p_3) \wedge (q_1 \vee p_2 \vee q_3)$   
 $\quad \wedge (q_1 \vee p_2 \vee p_3) \wedge (q_1 \vee p_2 \vee q_3)),$   
 $A_3 \Leftrightarrow C_3, \quad \deg(A_3) = 5, \quad \deg(C_3) = 23$

- $A_n = ((p_1 \wedge q_1) \vee \dots \vee (p_n \wedge q_n))$   
 Koľko klauzúl bude obsahovať  $C_n$ ?  $2^n$   
 Akého bude stupňa?  $(n-1) \cdot 2^n + (2^n - 1) = n \cdot 2^n - 1$

#### IV.6 Obmedzenie exponenciálneho rastu CNF

---

*Otázka.* Dá sa vyhnúť exponenciálnemu nárastu formuly  $A_n = ((p_1 \wedge q_1) \vee \dots \vee (p_n \wedge q_n))$  kvôli distributívnosti?

1. Zoberme nové výrokové premenné  $r_1, \dots, r_n, s$
2. Vyjadrieme, že  $r_i$  je ekvivalentným zástupcom konjunkcie  $(p_i \wedge q_i)$ :  
 $(r_i \leftrightarrow (p_i \wedge q_i))$
3. Použijeme  $r_i$  na vyjadrenie, že  $s$  je ekvivalentným zástupcom disjunkcie  $A_n$ :  $(s \leftrightarrow (r_1 \vee \dots \vee r_n))$
4.  $A_n$  teda môžeme nahradiť formulou  $(s \wedge (s \leftrightarrow (r_1 \vee \dots \vee r_n))) \wedge (r_1 \leftrightarrow (p_1 \wedge q_1)) \wedge \dots \wedge (r_n \leftrightarrow (p_n \wedge q_n))$

Ekvivalentnými úpravami

- druhý konjunkt upravíme na  $n + 1$  klauzúl,
  - ďalších  $n$  na 3 klauzuly každý
- } spolu iba  $4 \cdot n + 2$  klauzúl!

#### IV.7 Cejtinova transformácia do CNF

---

**Cejtinova transformácia** (angl. Tseytin transformation)

- algoritmus nájdenia CNF použitím tohto princípu na všetky podformuly
- výsledok Cejtinovej transformácie **nie je ekvivalentný** s  $X$ , iba **ekvisplniteľný**

**Definícia 2.62.** Formuly  $X$  a  $Y$  sú rovnako splniteľné (ekvisplniteľné, equisatisfiable) práve vtedy, keď  $X$  je splniteľná vtt  $Y$  je splniteľná.

**Tvrdenie 2.63.** Ak  $X$  a  $Y$  sú ekvivalentné, sú aj rovnako splniteľné.

*Príklad 2.64* (Ekvivalentnosť vs. ekvisplniteľnosť). Sú  $(p \rightarrow q)$  a  $(p \wedge r)$  rovnako splniteľné? Sú ekvivalentné?

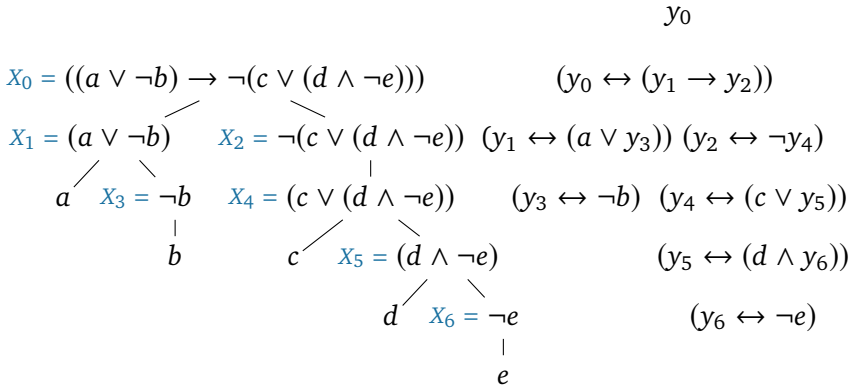
Pri úprave formuly do CNF pre SAT solver

- nepotrebuje zachovať ekvivalenciu
- stačí ekvisplniteľnosť

### Cejtinova transformácia

1. Zostrojíme vytvárajúci strom pre formulu  $X$  a označíme formuly v ňom  $X_0, X_1, X_2, \dots$  tak, aby  $X_0 = X$ .
2. Pre každú formulu  $X_i$ , ak  $X_i = p$  pre nejakú  $p \in \mathcal{V}$ , označíme  $y_i = p$ , inak označíme ako  $y_i$  novú výrokovú premennú, ktorá bude „reprezentovať“ formulu  $X_i$ .
3. Vytvoríme formuly, ktoré popisujú vzťah medzi  $X_i$  a jej priamymi podformulami prostredníctvom „reprezentačných“ premenných:
  - ak  $X_i$  je tvaru  $\neg X_j$  pre nejaké  $X_j$ , pridáme  $(y_i \leftrightarrow \neg y_j)$ ,
  - ak  $X_i$  je tvaru  $(X_j \wedge X_k)$ , pridáme  $(y_i \leftrightarrow (y_j \wedge y_k))$ ,
  - ak  $X_i$  je tvaru  $(X_j \vee X_k)$ , pridáme  $(y_i \leftrightarrow (y_j \vee y_k))$ ,
  - ak  $X_i$  je tvaru  $(X_j \rightarrow X_k)$  pridáme  $(y_i \leftrightarrow (y_j \rightarrow y_k))$ ,
4. Pridáme formulu  $y_0$  (chceme aby formula  $X$  bola pravdivá).
5. Všetky nové formuly z krokov 3 a 4 prevedieme do CNF (je to jednoduché) a spojíme konjunkciou.

## Príklad 2.65.



$$\begin{aligned}
 & (y_0 \wedge (y_0 \leftrightarrow (y_1 \rightarrow y_2)) \wedge \cdots \wedge (y_6 \leftrightarrow \neg e)) \Leftrightarrow \\
 & (y_0 \wedge (\neg y_0 \vee \neg y_1 \vee y_2) \wedge (y_1 \vee y_0) \wedge (\neg y_2 \vee y_0) \wedge \cdots \wedge (\neg y_6 \vee \neg e) \wedge (e \vee y_6))
 \end{aligned}$$

**Tvrdenie 2.66.** Pre výslednú formulu  $Y$  algoritmu Cejtinovej transformácie formuly  $X$  platí:

- $Y$  je v CNF,
- stupeň  $Y$  je lineárny vzhľadom na stupeň  $X$ ,
- $Y$  je ekvisplniteľná s  $X$ .

**Lema 2.67.** Nech  $X = (AcB)$  je formula, kde  $c \in \{\wedge, \vee, \rightarrow\}$ . Nech  $p, q, r \in \mathcal{V}$  sa nevyskytujú v  $X$ . Potom  $X$  a  $Y = (p \wedge (p \leftrightarrow (q \ c \ r)) \wedge (q \leftrightarrow A) \wedge (r \leftrightarrow B))$  sú ekvisplniteľné.

## 2.7. Logické kalkuly

- 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  $X = ((a \vee \neg b) \rightarrow \neg(c \vee (d \wedge \neg e)))$  sme upravili do CNF  $Y = ((\neg a \vee \neg c) \wedge (b \vee \neg c) \wedge (\neg a \vee \neg d \vee e) \wedge (b \vee \neg d \vee e))$  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.

#### IV.13 Ekvivalencia syntakticky vs. sémanticky

---

- 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.14 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 tri kalkuly:  
*hilbertovský* — klasický, lineárny, pomerne ťažkopádny  
*tablový* — stromový, prirodzenejší  
*rezolvenciu* — lineárny, strojový

## 2.8. Hilbertovský kalkul

### IV.15 Hilbertovský kalkul — axiómy a pravidlo

**Definícia 2.68.** *Hilbertovský kalkul* sa skladá z axióm vytvorených podľa nasledujúcich schém axióm pre všetky formuly  $A, B, C$ :

$$(A1) \quad (A \rightarrow (B \rightarrow A))$$

$$(A2) \quad ((A \rightarrow (B \rightarrow C)) \rightarrow ((A \rightarrow B) \rightarrow (A \rightarrow C)))$$

$$(A3) \quad ((\neg A \rightarrow \neg B) \rightarrow (B \rightarrow A))$$

$$(A4) \quad ((A \wedge B) \rightarrow A), \quad ((A \wedge B) \rightarrow B)$$

$$(A5) \quad (A \rightarrow (B \rightarrow (A \wedge B)))$$

$$(A6) \quad (A \rightarrow (A \vee B)), \quad (B \rightarrow (A \vee B))$$

$$(A7) \quad ((A \rightarrow C) \rightarrow ((B \rightarrow C) \rightarrow ((A \vee B) \rightarrow C)))$$

a pravidla *modus ponens*:

$$(MP) \quad \frac{A \quad (A \rightarrow B)}{B}$$

pre všetky formuly  $A$  a  $B$ .

[Švejdar, 2002, §1.3]



**Definícia 2.69.** (*Formálnym hilbertovským*) *dôkazom* z množiny predpokladov  $S$  je postupnosť formúl  $Y_1, Y_2, \dots, Y_n$ , v ktorej každá formula  $Y_i$  je

- predpoklad z množiny  $S$ , alebo
- záver odvodzovacieho pravidla, ktorého premisy sa nachádzajú v postupnosti pred  $Y_i$ , teda špeciálne
  - $Y_i$  je axióma, inštancia jednej zo schém (A1)–(A7), alebo
  - existujú  $j < i$  a  $k < i$  také, že  $Y_i$  je záver pravidla (MP) pre formuly  $Y_j$  a  $Y_k = (Y_j \rightarrow Y_i)$ .

*Dôkazom formuly  $X$  z  $S$*  je taký dôkaz z  $S$ , ktorého posledným členom je  $X$ .

Formula  $X$  je *dokázateľná* z množiny predpokladov  $S$  (skrátene  $S \vdash X$ ) vtt existuje dôkaz  $X$  z  $S$ .

[Švejdar, 2002, §1.3]

#### IV.17 Príklad dôkazu v hilbertovskom kalkule

*Príklad 2.70.* Nájdime dôkaz formuly  $Z = (X \rightarrow X)$  z množiny predpokladov  $\{\}$

(pre ľubovoľnú formulu  $X$ ):

$Y_1 = (X \rightarrow (X \rightarrow X))$  inštancia (A1) pre  $A = B = X$

$Y_2 = (X \rightarrow ((X \rightarrow X) \rightarrow X))$  inšt. (A1) pre  $A = X, B = (X \rightarrow X)$

$Y_3 = ((X \rightarrow ((X \rightarrow X) \rightarrow X)) \rightarrow ((X \rightarrow (X \rightarrow X)) \rightarrow (X \rightarrow X)))$   
inšt. (A2) pre  $A = C = X, B = (X \rightarrow X)$

$Y_4 = ((X \rightarrow (X \rightarrow X)) \rightarrow (X \rightarrow X))$  záver (MP) pre  $Y_2$  a  $Y_3$

$Y_5 = (X \rightarrow X)$  záver (MP) pre  $Y_1$  a  $Y_4$

**Veta 2.71** (o dedukcii).  $S \cup \{X\} \vdash Y$  vtt  $S \vdash (X \rightarrow Y)$

*Dôkaz.* ( $\Leftarrow$ ) Nech  $Y_1, \dots, Y_n$  je dôkaz  $(X \rightarrow Y)$  z  $S$ . Potom  $Y_1, \dots, Y_n, X, Y$  je dôkaz  $Y$  z  $S \cup \{X\}$ .

( $\Rightarrow$ ) Nech  $Y_1, \dots, Y_n$  je dôkaz  $Y$  z  $S \cup \{X\}$ . Úplnou indukciou na  $k$  dokážeme, že  $S \vdash (X \rightarrow Y_k)$ .

*Báza:* Nech  $k = 1$ .  $Y_1$  nemohla byť odvodená pravidlom (MP), takže je buď axióma, alebo patrí do  $S$ , alebo je  $X$ . V treťom prípade použijeme dôkaz  $(X \rightarrow X)$  z predchádzajúceho príkladu 2.70. V prvých dvoch prípadoch je postupnosť  $Y_1, (Y_1 \rightarrow (X \rightarrow Y_1)), (X \rightarrow Y_1)$  dôkazom  $(X \rightarrow Y_1)$ .

*Ind. krok:* Nech  $k > 1$  a platí IP: pre všetky  $j < k$  máme  $S \vdash (X \rightarrow Y_j)$ .

Ak  $Y_k$  je axióma, patrí do  $S$ , alebo je  $X$ , postupujeme ako pre  $k = 1$ .

Ak je  $Y_k$  záverom pravidla (MP) pre  $Y_i$  a  $Y_j = (Y_i \rightarrow Y_k)$ , tak  $i, j < k$  a platí pre ne IP. Teda existuje dôkaz  $A_1, \dots, A_a$  formuly  $A_a = (X \rightarrow Y_i)$  z  $S$  a dôkaz  $B_1, \dots, B_b$  formuly  $B_b = (X \rightarrow (Y_i \rightarrow Y_k))$  z  $S$ . Dôkazom formuly  $(X \rightarrow Y_k)$  potom je:  $A_1, \dots, A_a, B_1, \dots, B_b, ((X \rightarrow (Y_i \rightarrow Y_k)) \rightarrow ((X \rightarrow Y_i) \rightarrow (X \rightarrow Y_k))), ((X \rightarrow Y_i) \rightarrow (X \rightarrow Y_k)), (X \rightarrow Y_k)$ .  $\square$

#### IV.19 Dokazovanie s vetou o dedukcii

**Príklad 2.72.** Ukážme  $\{ \} \vdash ((A \rightarrow B) \rightarrow ((B \rightarrow C) \rightarrow (A \rightarrow C)))$

(pre ľubovoľné formuly  $A, B$  a  $C$ ).

Podľa vety o dedukcii máme  $\{ \} \vdash ((A \rightarrow B) \rightarrow ((B \rightarrow C) \rightarrow (A \rightarrow C)))$  vtt  $\{(A \rightarrow B)\} \vdash ((B \rightarrow C) \rightarrow (A \rightarrow C))$  vtt  $\{(A \rightarrow B), (B \rightarrow C)\} \vdash (A \rightarrow C)$  vtt  $\{(A \rightarrow B), (B \rightarrow C), A\} \vdash C$ .

Posledný dôkaz nájdeme veľmi ľahko:

$Y_1 = A$  predpoklad

$Y_2 = (A \rightarrow B)$  predpoklad

$Y_3 = B$  (MP) pre  $Y_1$  a  $Y_2$

$Y_4 = (B \rightarrow C)$  predpoklad

$$Y_5 = C$$

(MP) pre  $Y_3, Y_4$

Podľa úvodnej úvahy teda  $\{\} \vdash ((A \rightarrow B) \rightarrow ((B \rightarrow C) \rightarrow (A \rightarrow C)))$   
(ale nevieme, ako tento dôkaz presne vyzerá).

#### IV.20 Dokazovanie s vetou o dedukcii

**Príklad 2.73.** Ukážme  $\{\} \vdash (\neg X \rightarrow (X \rightarrow Y))$  (pre ľubovoľné formuly  $X$  a  $Y$ ).

$$Y_1 = (\neg X \rightarrow (\neg Y \rightarrow \neg X))$$

(A1) pre  $A = \neg X, B = \neg Y$

$$Y_2 = ((\neg Y \rightarrow \neg X) \rightarrow (X \rightarrow Y))$$

(A3) pre  $A = Y, B = X$

$\vdots$

dôkaz z príkladu 2.72

$$Y_3 = Y_n = ((\neg X \rightarrow (\neg Y \rightarrow \neg X)) \rightarrow (((\neg Y \rightarrow \neg X) \rightarrow (X \rightarrow Y)) \rightarrow (\neg X \rightarrow (X \rightarrow Y))))$$

$$Y_{n+1} = (((\neg Y \rightarrow \neg X) \rightarrow (X \rightarrow Y)) \rightarrow (\neg X \rightarrow (X \rightarrow Y)))$$

(MP) pre  $Y_1$  a  $Y_n$

$$Y_{n+2} = (\neg X \rightarrow (X \rightarrow Y))$$

(MP) pre  $Y_2$  a  $Y_{n+1}$

#### IV.21 Korektnosť a úplnosť hilbertovského kalkulu

**Veta 2.74.** Pre každú množinu formúl  $S$  a každú formulu  $X$  platí:

(korektnosť) ak je  $X$  dokázateľná z  $S$  ( $S \vdash X$ ),  
tak  $X$  výrokologicky vyplýva z  $S$  ( $S \models X$ );

(úplnosť) ak  $X$  výrokologicky vyplýva z  $S$  ( $S \models X$ ),  
tak  $X$  je dokázateľná z  $S$  ( $S \vdash X$ ).

Korektnosť (angl. soundness) hilbertovského kalkulu vyplýva matematickou indukciou na dĺžku dôkazu z korektnosti pravidiel:

Ak  $S$  je množina výrokových formúl a ak

$$\frac{A_1 \quad \cdots \quad A_n}{A}$$

je pravidlo (axióma alebo (MP)), potom ak  $A_1, \dots, A_n$  súčasne vyplývajú z  $S$ , tak aj  $A$  vyplýva z  $S$ .

Úplnosť (angl. completeness) je komplikovanejšia.

**Vyskúšajte si IV.1**

Ukážte  $\{\} \vdash (\neg\neg X \rightarrow X)$ .

## V. prednáška

# Tablový kalkul a jeho korektnosť

18. marca 2019

### Logické kalkuly (opakovanie)

#### V.1 Logické kalkuly — vyplývanie syntakticky

*Logický kalkul* je *formálny/syntaktický* systém na dokazovanie vyplývania

- Manipulácia postupnosťami symbolov
- Pri používaní sa netreba odvolávať na sémantiku (ohodnotenia)

Zvyčajne má dve zložky:

**Axiómy alebo ich schémy** — „základné pravdy“

Napríklad hilbertovské schémy axióm:

- $(A \rightarrow (B \rightarrow A))$
- $((A \rightarrow (B \rightarrow C)) \rightarrow ((A \rightarrow B) \rightarrow (A \rightarrow C)))$
- $((\neg A \rightarrow \neg B) \rightarrow (B \rightarrow A))$
- $((A \wedge B) \rightarrow A), ((A \wedge B) \rightarrow B)$
- $(A \rightarrow (B \rightarrow (A \wedge B)))$
- $(A \rightarrow (A \vee B)), (B \rightarrow (A \vee B))$
- $((A \rightarrow C) \rightarrow ((B \rightarrow C) \rightarrow ((A \vee B) \rightarrow C)))$

**Pravidlá** — „formy správnych úsudkov“, odvodzujú „nové pravdy“ zo základných, obsiahnutých v teórii, už odvodených

Napríklad jediné pravidlo hilbertovského kalkulu:

$$(MP) \frac{A \quad (A \rightarrow B)}{B}$$

Kalkul je najužitočnejší, keď je súčasne

**korektný** (angl. sound):

**dovoľuje** odvodiť **iba** skutočne vyplývajúce formuly,

**úplný** (angl. complete):

**umožňuje** odvodiť **všetky** vyplývajúce formuly.

Hilbertovský kalkul je korektný aj úplný

**Veta 2.74.** *Pre každú množinu formul  $S$  a každú formulu  $X$  platí:*

(korektnosť) *ak je  $X$  dokázateľná z  $S$  ( $S \vdash X$ ),*

*tak  $X$  výrokologicky vyplýva z  $S$  ( $S \models X$ );*

(úplnosť) *ak  $X$  výrokologicky vyplýva z  $S$  ( $S \models X$ ),*

*tak  $X$  je dokázateľná z  $S$  ( $S \vdash X$ ).*

- Jednoduchá definícia a dôkazy jeho vlastností
- Nie úplne jednoduché použitie

## 2.9. Tablový kalkul

**Príklad 2.75.** Dokážme, že z  $T'_{\text{party}} = \{ (kim \rightarrow (jim \wedge \neg sarah)), (eva \rightarrow kim) \}$  vyplýva  $(sarah \rightarrow \neg eva)$ .

Podme na to sporom: Predpokladajme, že existuje také ohodnotenie  $v$ , že  $v \models T'_{\text{party}}$ , teda (1)  $v \models (kim \rightarrow (jim \wedge \neg sarah))$  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)  $v \not\models \text{eva}$  alebo (8)  $v \models \text{kim}$ . Možnosť (7) je v spore s (6).

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

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

## V.5 Tablová notácia pre dôkazy

Dôkaz stručne zapíšeme v tablovej (tabuľkovej) notácii:

- $\mathbf{T} X$  označuje  $v$  spĺňa  $X$ .
- $\mathbf{F} X$  označuje  $v$  nespĺňa  $X$ .
- Ak z niektorého predchádzajúceho faktu o formule  $X$  priamo z *def. spĺňania* vyplýva fakt (ne)splnenia niektorej *priamej podformuly*  $X$ , pridáme ho ako **ďalší riadok** tabla.  
Poznačíme si k nemu písmeno  $\alpha$  a číslo zdrojového faktu.
- Ak z niektorého predch. faktu o formule  $X$  **vyplýva** o jej *priamych podformulách* fakt  $F_1$  **alebo** fakt  $F_2$ , tablo **rozdelíme na dve vzájomne nezávislé vetvy** (stĺpce), pričom prvá začne faktom  $F_1$  a druhá faktom  $F_2$ .  
K oboj si poznačíme písmeno  $\beta$  a číslo zdrojového faktu.
- Ak nastane **spor** medzi splnením a nespĺnením *tej istej* formuly, pridáme riadok so symbolom  $*$   
a poznačíme si čísla faktov, ktoré sú v spore.

## V.6 Dôkaz vyplývania sporom v tablovej notácii

Príklad 2.76.

1.	$\mathbf{T}(kim \rightarrow (jim \wedge \neg sarah))$	$z\ T'_{party}{}^\dagger$
2.	$\mathbf{T}(eva \rightarrow kim)$	$z\ T'_{party}{}^\dagger$
3.	$\mathbf{F}(sarah \rightarrow \neg eva)$	dôkaz sporom <sup>†</sup>
4.	$\mathbf{T}\ sarah$	$\alpha 3$
5.	$\mathbf{F}\ \neg eva$	$\alpha 3$
6.	$\mathbf{T}\ eva$	$\alpha 5$
7.	$\mathbf{F}\ eva\ \beta 2$	
	$\ast\ 6\ a\ 7$	
8.	$\mathbf{T}\ kim$	$\beta 2$
9.	$\mathbf{F}\ kim\ \beta 1$	
	$\ast\ 8\ a\ 9$	
10.	$\mathbf{T}(jim \wedge \neg sarah)$	$\beta 1$
11.	$\mathbf{T}\ jim$	$\alpha 10$
12.	$\mathbf{T}\ \neg sarah$	$\alpha 10$
13.	$\mathbf{F}\ sarah$	$\alpha 12$
	$\ast$	$4\ a\ 13$

<sup>†</sup> Tento zápis nepoužívajte vo svojich riešeniach.

## V.7 Definícia tablového kalkulu

### Tablová notácia

- Dohoda o stručnom zápise podrobných úvah v dôkaze sporom
- Neformálna a nie veľmi presná

Tablový *kalkul* — presne matematicky zadefinovaný formálny systém  
Zadefinujeme:

- Význam značiek **T** a **F**
- Axiómy a pravidlá kalkulu
- Tablo — formálny dôkaz v tablovom kalkule
- Podmienky úspešného ukončenia dôkazu



**Definícia 2.77.** Nech  $X$  je formula výrokovej logiky.

Postupnosti symbolov  $\mathbf{T}X$  a  $\mathbf{F}X$  nazývame *označené formuly*.

**Definícia 2.78.** Nech  $v$  je ohodnotenie výrokových premenných a  $X$  je formula. Potom

- $v$  *spĺňa*  $\mathbf{T}X$  vtt  $v$  *spĺňa*  $X$ ;
- $v$  *spĺňa*  $\mathbf{F}X$  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.  $S^+$ ,  $T_3^+$ .

### V.9 Spĺňanie a priame podformuly

---

Nasledujúce fakty vyplývajú **priamo** z definície splnenia formuly ohodnotením:

**Pozorovanie 2.79.** Nech  $v$  je ľubovoľné ohodnotenie výrokových premenných. Nech  $X$  a  $Y$  sú ľubovoľné formuly.

- Ak  $v$  *spĺňa*  $\neg X$ , tak  $v$  *nespĺňa*  $X$ .
  - Ak  $v$  *nespĺňa*  $\neg X$ , tak  $v$  *spĺňa*  $X$ .
- Ak  $v$  *spĺňa*  $(X \wedge Y)$ , tak  $v$  *spĺňa*  $X$  a  $v$  *spĺňa*  $Y$ .
  - Ak  $v$  *nespĺňa*  $(X \wedge Y)$ , tak  $v$  *nespĺňa*  $X$  alebo  $v$  *nespĺňa*  $Y$ .
- Ak  $v$  *spĺňa*  $(X \vee Y)$ , tak  $v$  *spĺňa*  $X$  alebo  $v$  *spĺňa*  $Y$ .
  - Ak  $v$  *nespĺňa*  $(X \vee Y)$ , tak  $v$  *nespĺňa*  $X$  a  $v$  *nespĺňa*  $Y$ .
- Ak  $v$  *spĺňa*  $(X \rightarrow Y)$ , tak  $v$  *nespĺňa*  $X$  alebo  $v$  *spĺňa*  $Y$ .
  - Ak  $v$  *nespĺňa*  $(X \rightarrow Y)$ , tak  $v$  *spĺňa*  $X$  a  $v$  *nespĺňa*  $Y$ .

Pozorovanie 2.79 — dobrý základ pre odvodzovacie pravidlá

- Základné, ľahko overiteľné fakty
- Závery sú jednoduchšie ako premisy

Splnenie/nespĺnenie vyjadríme označenými formulami podľa def. 2.78

$\frac{T \neg X}{F X}$	$\frac{T(X \wedge Y)}{T X}$	$\frac{T(X \vee Y)}{T X \mid T Y}$	$\frac{T(X \rightarrow Y)}{F X \mid T Y}$
	$\frac{T(X \wedge Y)}{T Y}$		
$\frac{F \neg X}{T X}$	$\frac{F(X \wedge Y)}{F X \mid F Y}$	$\frac{F(X \vee Y)}{F X}$	$\frac{F(X \rightarrow Y)}{T X}$
		$\frac{F(X \vee Y)}{F Y}$	$\frac{F(X \rightarrow Y)}{F Y}$

- Nemáme žiadne axiómy
- Pravidiel je veľa
- Sú však zjavne dvoch druhov:
  - $\alpha$ : Pravidlá odvodzujúce jeden záver
  - $\beta$ : Pravidlá odvodzujúce dva závery, z ktorých platí aspoň jeden
- Zjednotíme zápis pravidiel rovnakého druhu

**Definícia 2.80** (Jednotný zápis označených formúl typu  $\alpha$ ).

Označená formula  $A^+$  je typu  $\alpha$  vtt má jeden z tvarov v ľavom stĺpci tabuľky pre nejaké formuly  $X$  a  $Y$ . Takéto formuly budeme označovať písmenom  $\alpha$ ;  $\alpha_1$  bude označovať príslušnú označenú formulu zo stredného stĺpca,  $\alpha_2$  príslušnú formulu z pravého stĺpca.

$\alpha$	$\alpha_1$	$\alpha_2$
$\mathbf{T}(X \wedge Y)$	$\mathbf{T} X$	$\mathbf{T} Y$
$\mathbf{F}(X \vee Y)$	$\mathbf{F} X$	$\mathbf{F} Y$
$\mathbf{F}(X \rightarrow Y)$	$\mathbf{T} X$	$\mathbf{F} Y$
$\mathbf{T} \neg X$	$\mathbf{F} X$	$\mathbf{F} X$
$\mathbf{F} \neg X$	$\mathbf{T} X$	$\mathbf{T} X$

**Pozorovanie 2.81** (Stručne vďaka jednotnému zápisu). *Nech  $v$  je ľubovoľné ohodnotenie výrokových premenných.*

*Potom  $v$  spĺňa  $\alpha$  vtt  $v$  spĺňa  $\alpha_1$  a  $v$  spĺňa  $\alpha_2$ .*

**Definícia 2.82** (Jednotný zápis označených formúl typu  $\beta$ ).

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  $\beta$ ;  $\beta_1$  bude označovať príslušnú označenú formulu zo stredného stĺpca,  $\beta_2$  príslušnú formulu z pravého stĺpca.

$\beta$	$\beta_1$	$\beta_2$
$\mathbf{F}(X \wedge Y)$	$\mathbf{F} X$	$\mathbf{F} Y$
$\mathbf{T}(X \vee Y)$	$\mathbf{T} X$	$\mathbf{T} Y$
$\mathbf{T}(X \rightarrow Y)$	$\mathbf{F} X$	$\mathbf{T} Y$

**Pozorovanie 2.83** (Stručne vďaka jednotnému zápisu). *Nech  $v$  je ľubovoľné ohodnotenie výrokových premenných.*

*Potom  $v$  spĺňa  $\beta$  vtt  $v$  spĺňa  $\beta_1$  alebo  $v$  spĺňa  $\beta_2$ .*

Akú štruktúru má dôkaz zapísaný v tablovej notácii?

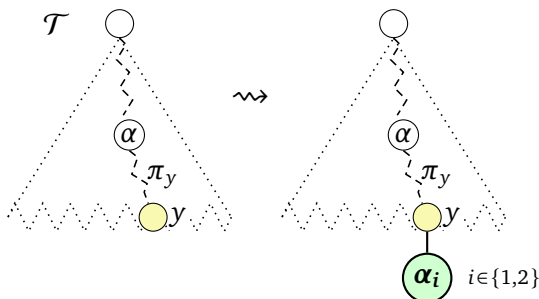


$S^+$ : Ako jediné dieťa  $y$  pripojíme nový vrchol obsahujúci ľubovoľnú označenú formulu  $A^+ \in S^+$ .

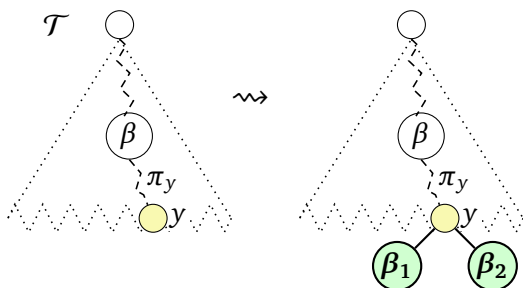
Nič iné nie je tablom pre  $S^+$ .

#### V.16 Tablá a tablové pravidlá

**Pôvodné tablo**      **Možné priame rozšírenie**      **Pravidlá a označené formuly v nich**



$\alpha$	$\alpha$	$\alpha$	$\alpha_1$	$\alpha_2$
$\alpha_1$	$\alpha_2$			
$\mathbf{T}(X \wedge Y)$	$\mathbf{T}X$	$\mathbf{T}Y$		
$\mathbf{F}(X \vee Y)$	$\mathbf{F}X$	$\mathbf{F}Y$		
$\mathbf{F}(X \rightarrow Y)$	$\mathbf{T}X$	$\mathbf{F}Y$		
$\mathbf{T}\neg X$	$\mathbf{F}X$	$\mathbf{F}X$		
$\mathbf{F}\neg X$	$\mathbf{T}X$	$\mathbf{T}X$		



$\beta$	$\beta$	$\beta_1$	$\beta_2$
$\beta_1$	$\beta_2$		
$\mathbf{F}(X \wedge Y)$	$\mathbf{F}X$	$\mathbf{F}Y$	
$\mathbf{T}(X \vee Y)$	$\mathbf{T}X$	$\mathbf{T}Y$	
$\mathbf{T}(X \rightarrow Y)$	$\mathbf{F}X$	$\mathbf{T}Y$	

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

#### V.17 Uzavretosť a otvorenosť vetvy a tabla

**Definícia 2.85.** *Vetvou* tabla  $\mathcal{T}$  je každá cesta od koreňa  $\mathcal{T}$  k niektorému listu  $\mathcal{T}$ .

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

Tablo  $\sim$  dôkaz sporom. Vetvenie  $\sim$  rozbor možných prípadov.  $\implies$  Spor musí nastať vo všetkých vetvách.

**Definícia 2.86.** Vetva  $\pi$  tabla  $\mathcal{T}$  je uzavretá vtt na  $\pi$  sa súčasne vyskytujú označené formuly  $\mathbf{F} X$  a  $\mathbf{T} X$  pre nejakú formulu  $X$ . Inak je  $\pi$  otvorená.

Tablo  $\mathcal{T}$  je uzavreté vtt každá jeho vetva je uzavretá. Naopak,  $\mathcal{T}$  je otvorené vtt aspoň jedna jeho vetva je otvorená.

V.18

---

### Spomeňte si V.1

1. Má každé tablo aspoň jedno priame rozšírenie?
2. Má každé tablo najviac jedno priame rozšírenie?

### 2.9.1. Korektnosť

V.19 Korektnosť tablového kalkulu

---

**Veta 2.87** (Korektnosť tablového kalkulu). *Nech  $S^+$  je množina označených formúl a  $\mathcal{T}$  je uzavreté tablo pre  $S^+$ . Potom je množina  $S^+$  nesplniteľná.*

**Dôsledok 2.88.** *Nech  $S$  je množina formúl a  $X$  je formula. Ak existuje uzavreté tablo pre  $\{\mathbf{T} A \mid A \in S\} \cup \{\mathbf{F} X\}$  (skrátene  $S \vdash X$ ), tak z  $S$  vyplýva  $X$  ( $S \models X$ ).*

**Dôsledok 2.89.** *Nech  $X$  je formula. Ak existuje uzavreté tablo pre  $\{\mathbf{F} X\}$  (skrátene  $\vdash X$ ), tak  $X$  je tautológia ( $\models X$ ).*

V.20 Korektnosť — idea dôkazu

---

Aby sme dokázali korektnosť tabiel, dokážeme postupne dve lemy:

- (K1) Ak máme tablo pre splniteľnú množinu  $S^+$  s aspoň jednou splniteľnou vetvou, tak každé jeho priame rozšírenie má tiež splniteľnú vetvu.

(K2) Každé tablo pre splniteľnú množinu  $S^+$  má aspoň jednu splniteľnú vetvu.

Z toho ľahko sporom dokážeme, že množina, pre ktorú sme našli uzavreté tablo je nespľniteľná.

#### V.21 Korektnosť — splnenie priameho rozšírenia tabla

Hodí sa nám pomocná definícia:

**Definícia 2.90.** Nech  $S^+$  je množina označených formúl, nech  $\mathcal{T}$  je tablo pre  $S^+$  a nech  $v$  je ohodnotenie množiny výrokových premenných. Potom:

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

**Lema 2.91** (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.22 Korektnosť — splnenie priameho rozšírenia tabla

*Dôkaz 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  $\pi$ . Nech  $\mathcal{T}_1$  je rozšírenie  $\mathcal{T}$ . Nastáva jeden z prípadov:

- $\mathcal{T}_1$  vzniklo z  $\mathcal{T}$  pravidlom  $\alpha$ , pridaním nového dieťaťa  $z$  nejakému listu  $y$  v  $\mathcal{T}$ , pričom  $z$  obsahuje  $\alpha_1$  alebo  $\alpha_2$  pre nejakú formulu  $\alpha$  na vetve  $\pi_y$ . Ak  $\pi \neq \pi_y$ , tak  $\mathcal{T}_1$  obsahuje  $\pi$  a teda je splnené.  
 Ak  $\pi = \pi_y$ , tak  $v$  spĺňa aj  $\alpha$ , pretože spĺňa  $\pi$ . Potom  $v$  musí spĺňať aj  $\alpha_1$  a  $\alpha_2$ . Spĺňa teda vetvu  $\pi_z$  v table  $\mathcal{T}_1$ , ktorá rozširuje splnenú vetvu  $\pi$  o vrchol  $z$  obsahujúci splnenú ozn. formulu  $\alpha_1$  alebo  $\alpha_2$ . Preto  $v$  spĺňa tablo  $\mathcal{T}_1$ .

- $\mathcal{T}_1$  vzniklo z  $\mathcal{T}$  pravidlom  $\beta$ , pridaním detí  $z_1$  a  $z_2$  nejakému listu  $y$  v  $\mathcal{T}$ , pričom  $z_1$  obsahuje  $\beta_1$  a  $z_2$  obsahuje  $\beta_2$  pre nejakú formulu  $\beta$  na vetve  $\pi_y$ . Ak  $\pi \neq \pi_y$ , tak  $\mathcal{T}_1$  obsahuje  $\pi$  a teda je splnené.  
Ak  $\pi = \pi_y$ , tak  $v$  spĺňa aj  $\beta$ , pretože spĺňa  $\pi$ . Potom ale  $v$  musí spĺňať aj  $\beta_1$  alebo  $\beta_2$ . Ak  $v$  spĺňa  $\beta_1$ , tak spĺňa aj vetvu  $\pi_{z_1}$  v table  $\mathcal{T}_1$ , a preto  $v$  spĺňa tablo  $\mathcal{T}_1$ . Ak  $v$  spĺňa  $\beta_2$ , spĺňa aj  $\pi_{z_2}$ , a teda aj  $\mathcal{T}_1$ .
- $\mathcal{T}_1$  vzniklo z  $\mathcal{T}$  pravidlom  $S^+$ , 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  $\pi$  a teda je splnené.  
Ak  $\pi = \pi_y$ , tak  $v$  spĺňa vetvu  $\pi_z$  v table  $\mathcal{T}_1$ , pretože je rozšírením splnenej vetvy  $\pi$  o vrchol  $z$  obsahujúci splnenú formulu  $X$  (pretože  $v \models S^+$ ). Preto  $v$  spĺňa tablo  $\mathcal{T}_1$ .  $\square$

#### V.23 Korektnosť — splnenie množiny a tabla pre ňu

**Lema 2.92** (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  $\mathcal{T}$ .*

*Dôkaz 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  $\mathcal{T}$ .  $\square$

#### V.24 Korektnosť — dôkaz

*Dôkaz 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  $\pi$  v  $\mathcal{T}$ .

Pretože  $\mathcal{T}$  je uzavreté, aj vetva  $\pi$  je uzavretá,

teda  $\pi$  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.  $\square$

## 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>.