

# Prednášky z Matematiky (4) — Logiky pre informatikov

Ján Kľuka, Jozef Šiška

Letný semester 2017/2018

## Obsah

<b>I. O logike a tomto kurze</b>	
Syntax výrokovej logiky	<b>4</b>
<b>1. Úvod</b>	<b>4</b>
1.1. O logike . . . . .	4
1.2. O kurze . . . . .	11
<b>2. Výroková logika</b>	<b>11</b>
2.1. Opakovanie: Výroková logika v prirodzenom jazyku . . . . .	11
2.2. Syntax . . . . .	13
<b>II. Sémantika výrokovej logiky</b>	<b>18</b>
2.3. Sémantika . . . . .	24
2.4. Tautológia, (ne)splniteľnosť, falzifikovateľnosť . . . . .	28
<b>III. Vyplyvanie, ekvivalentné úpravy</b>	<b>34</b>
2.5. Vyplyvanie . . . . .	35

2.6. Ekvivalencia . . . . .	38
2.6.1. Ekvivalentné úpravy . . . . .	40
2.6.2. Konjunktívna a disjunktívna normálna forma . . . . .	43
<b>IV. CNF. Tablový kalkul</b>	<b>46</b>
2.7. Kalkuly . . . . .	49
2.8. Tablový kalkul . . . . .	51
2.8.1. Korektnosť . . . . .	57
<b>V. Korektnosť a úplnosť tablového kalkulu</b>	<b>58</b>
2.8.2. Tablový dôkaz splniteľnosti . . . . .	60
2.8.3. Hintikkova lema . . . . .	62
2.8.4. Úplnosť . . . . .	63
<b>VI. Korektné pravidlá. Rezolvenca</b>	<b>64</b>
2.8.5. Nové korektné pravidlá . . . . .	64
2.9. Výroková rezolvenca . . . . .	66
2.10. Späť k dôkazom o vyplývaní . . . . .	70
<b>VII. SAT solver a algoritmus DPLL. Syntax relačnej logiky prvého rádu</b>	<b>77</b>
2.11. Problém výrokovologickej splniteľnosti (SAT) . . . . .	77
2.11.1. Naivný backtracking . . . . .	78
2.11.2. Optimalizácia backtrackingu . . . . .	80
2.11.3. DPLL . . . . .	85
<b>3. Logika prvého rádu</b>	<b>86</b>
3.1. Syntax relačnej logiky prvého rádu . . . . .	86
3.2. Formalizácia . . . . .	93
3.2.1. Jednoduchá formalizácia . . . . .	93
3.2.2. Základné idiómy . . . . .	94
3.2.3. Nutné a postačujúce podmienky . . . . .	96

3.2.4. Idiómy s rovnosťou . . . . .	97
<b>VIII. Definície predikátov. Sémantika relačnej logiky prvého rádu</b>	<b>99</b>
3.2.5. Definície predikátov . . . . .	100
3.3. Sémantika . . . . .	102

## 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* pravidiel zápisu tvrdení
    - Sémantika* význam tvrdení
  - Usudzovanie (inferencia)** ododenie 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

## I.5 Usudzovacie pravidlá, korektnosť, dedukcia

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

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

- **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.

A čo: Atmosféra  
Zeme je dýchateľná?

Na Venuši sa prejavuje skleníkový efekt.

- **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**

- **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

- 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 výrokovkej logiky
- Príklad 1.5.* Sformalizujme náš párty 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.



- 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

- 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*

- 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 výrokovkej a predikátovej logiky, ich syntaxou a sémantikou

- Korektnosťou usudzovacích pravidiel
- Korektnosťou a úplnosťou logických kalkulov
- Automatizovateľnými kalkulmi

**Prakticky** • Vyjadrovaním problémov v jazyku logiky

- Automatizovaním riešenia problémov použitím SAT-solverov
- Manipuláciou symbolických stromových štruktúr (výrazov — for-  
múl a termov)
- Programovaním vlastných jednoduchých automatických dokazo-  
vačov

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

- Obmedzeniami vyjadrovania a usudzovania

I.15 Organizácia kurzu — rozvrh, kontakty, pravidlá

---

[https://dai.fmph.uniba.sk/w/Course:Mathematics\\_4](https://dai.fmph.uniba.sk/w/Course:Mathematics_4)

## 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.

- Stredoškolský prístup príliš **neoddeľuje** samotný *jazyk* výrokovkej 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 výrokovkej 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 výrokovkej logiky

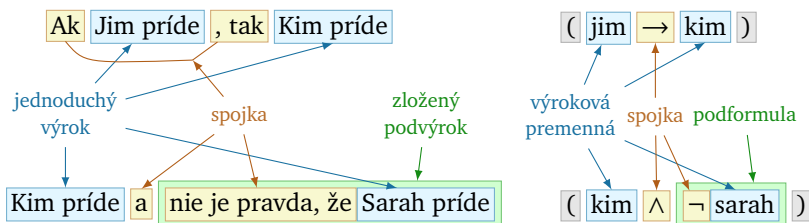
- Syntax sú pravidlá budovania viet v jazyku
- Pri formálnych jazykoch sú popísané matematicky
- Nedajte sa tým odradiť, nie je to oveľa iné ako programovanie
- Viac sa budete formálnymi jazykmi zaoberať na Úvode do teoretickej informatiky
- Naše definície vychádzajú prevažne z kníh [Smullyan, 1979]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

Aké tvrdenia chceme zapisovať vo výrokovkej 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.

## I.22 Symboly, výrokové premenné

---

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

Je o čosi všeobecnejší ako pojem znak.

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

### Dohoda

Výrokové premenné budeme *označovať* písmenami  $p, q, \dots$ , podľa potreby aj s dolnými indexmi.

Výrokové premenné formalizujú jednoduché výroky.

## I.23 Výrokové formuly

---

- 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.  $\neg\text{sarah}$ .
  - 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.

#### I.24 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  $\mathcal{E}$  (*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.

#### I.25 Výrokové formuly

---

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

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



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

#### I.26 Vytvárajúca postupnosť

---

**Definícia 2.8.** *Vytvárajúcou postupnosťou nad množinou výrokových premenných  $\mathcal{V}$  je ľubovoľná konečná postupnosť postupností symbolov, ktorej každý člen je výroková premenná z  $\mathcal{V}$ , alebo má tvar  $\neg A$ , pričom  $A$  je nejaký predchádzajúci člen postupnosti, alebo má jeden z tvarov  $(A \wedge B)$ ,  $(A \vee B)$ ,  $(A \rightarrow B)$ , 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  $A$ .*

#### I.27 Vytvárajúca postupnosť

---

**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  $X = (A \ b \ B)$ .

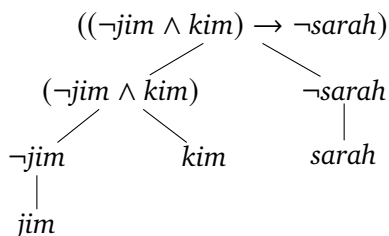
#### II.5 Vytvárajúca postupnosť a vytvárajúci strom

---

- 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  $(A \ b \ B)$ , 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.

- 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 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 splňajúca:

- 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 forém 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.

## II.10 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:

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

**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:

- i. priame podformuly,
- ii. podformuly,
- iii. 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, zobral 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 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:

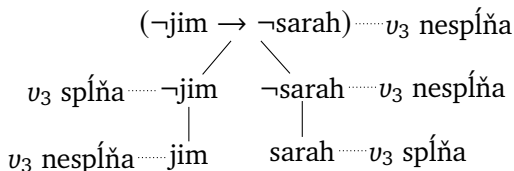
Formulu	jim	sarah	$\neg \text{jim}$	$\neg \text{sarah}$	$(\neg \text{jim} \rightarrow \neg \text{sarah})$
ohodnotenie $v_3$	nesplňa	spĺňa	spĺňa	nesplňa	nesplňa

## 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.

**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

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

Zistíme, 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.

$\deg(X)$	$v_3$ spĺňa $X$	$v_3$ nespĺňa $X$
0	kim, sarah	jim
1	$\neg$ jim, $(\text{kim} \vee \text{jim})$ , $(\text{jim} \rightarrow \text{kim})$	$\neg$ 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 Splňanie z hľadiska formuly

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

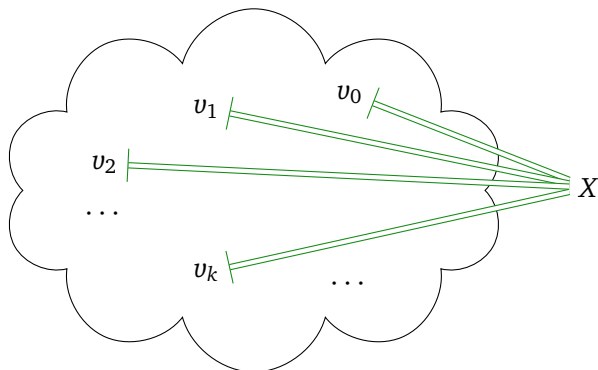
### Dohoda

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

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

*Ohodnotením* rozumieme ohodnotenie množiny výrok. prem.  $\mathcal{V}$ .

### II.23 Tautológia



**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.24 Tautológia — testovanie

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

**Tvrdenie 2.25.** *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?

#### II.25 Tautológia — testovanie

**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  $v_2 \models p$ .

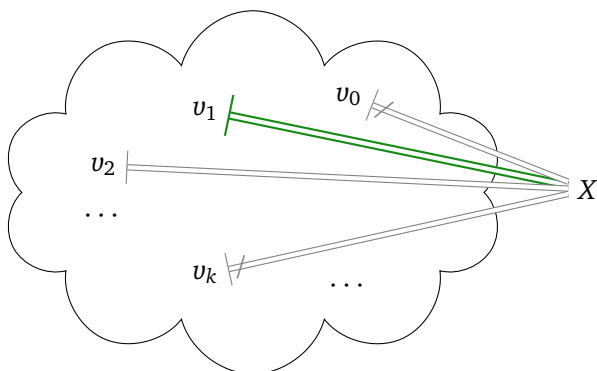
**Krok:** Nech  $X$  je stupňa  $n > 0$  a tvrdenie platí pre všetky formuly stupňa nižšieho ako  $n$  (indukčný predpoklad). Zoberme ľubovoľné ohodnotenia  $v_1$  a  $v_2$ , ktoré sa zhodujú na premenných v  $X$ . Podľa definície stupňa a jednoznačnosti rozkladu nastáva práve jeden z prípadov:

- $X = \neg A$  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.

□

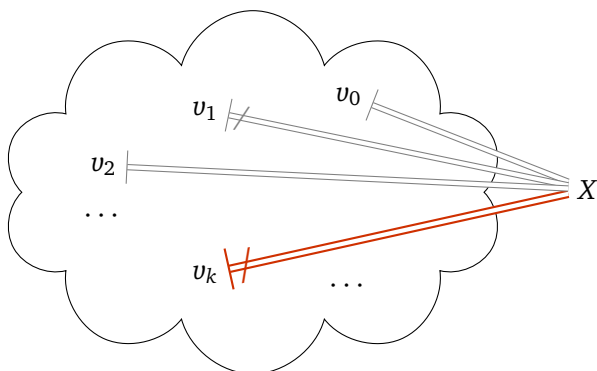
## II.27 Splniteľnosť

---



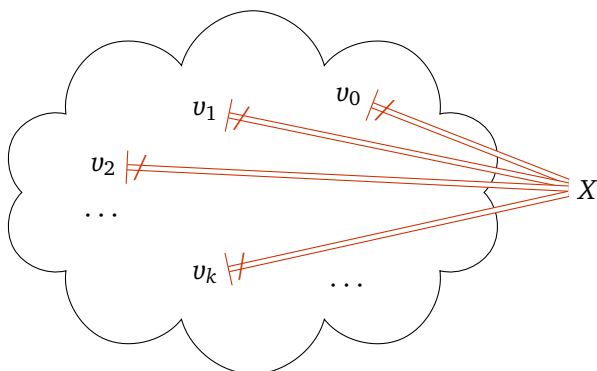
**Definícia 2.27.** Formulu  $X$  nazveme *splniteľnou* vtt **nejaké** ohodnotenie výrokových premenných **spĺňa**  $X$  (teda **existuje** také ohodnotenie výrokových premenných  $v$ , že  $v \models X$ ).

## II.28 Falzifikovateľnosť



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

## II.29 Nesplniteľnosť



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

#### II.30 „Geografia“ výrokových formúl podľa spĺňania



- 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 for-  
múl.

#### 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)  $T_{\text{party}}$ ?

**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.

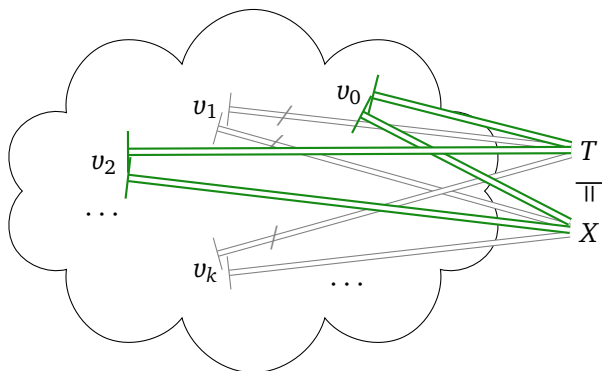
- Aký je účel teórií? Kedy je teória užitočná?
  - Keď z nej dokážeme *odvodiť* (uvažovaním alebo počítaním) *doteraz neznáme skutočnosti* (teda nezapísané v teórii), ktoré platia vo všetkých stavoch sveta spĺňajúcich teóriu.

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

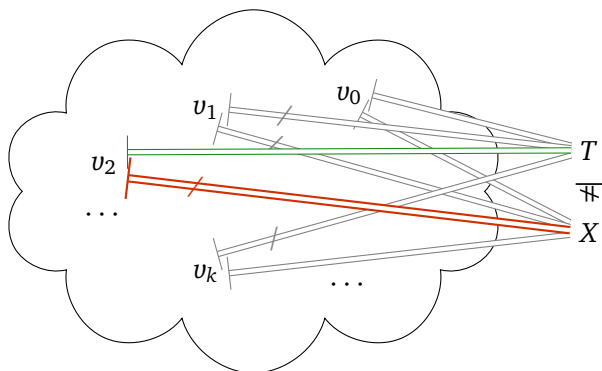
### III.6 Výrokovologické vyplývanie



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

(tiež  $X$  je výrokovologickým dôsledkom  $T$ , skrátene  $T \models X$ ) 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  $X$  výrokovologicky 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  $X$ . □

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

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

**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.  $\models (((\dots(A_1 \wedge A_2) \wedge \dots) \wedge A_n) \rightarrow B)$

### Spomeňte si III.1

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

Pravda alebo nepravda?

## 2.6. 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.*

### III.13 Ekvivalencia a vyplývanie

---

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.  $\square$

### III.14 Tranzitivita ekvivalencie

---

**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.  $\square$

### 2.6.1. Ekvivalentné úpravy

#### III.15 Ekvivalentné úpravy

---

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

*Príklad 2.50.*

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

$$\Downarrow$$

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

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

#### III.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)

$$\text{Príklad 2.51. } C = \neg\neg p \quad D = p$$

$$\Downarrow \quad \Downarrow$$

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



- 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  $X$

nech  $\ell$  je dĺžka  $A$

**kým** nie si na konci  $X$ :

**ak** sa nasledujúcich  $\ell$  symbolov zhoduje s  $A$ :

nahraď ich za  $B$

pokračuj za posledným nahradeným symbolom

**inak:**

pokračuj ďalším symbolom

alebo ako rekurzívne definovanú operáciu:

(cv02)

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

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

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

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

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

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

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

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

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:*

$(A \wedge (B \wedge C)) \text{ a } ((A \wedge B) \wedge C)$	<i>asociatívnosť</i>
$(A \vee (B \vee C)) \text{ a } ((A \vee B) \vee C)$	
$(A \wedge B) \text{ a } (B \wedge A)$	<i>komutatívnosť</i>
$(A \vee B) \text{ a } (B \vee A)$	
$(A \wedge (B \vee C)) \text{ a } ((A \wedge B) \vee (A \wedge C))$	<i>distributívnosť</i>
$(A \vee (B \wedge C)) \text{ a } ((A \vee B) \wedge (A \vee C))$	
$\neg(A \wedge B) \text{ a } (\neg A \vee \neg B)$	<i>de Morganove</i>
$\neg(A \vee B) \text{ a } (\neg A \wedge \neg B)$	<i>pravidlá</i>
$\neg\neg A \text{ a } A$	<i>dvojitá negácia</i>

### III.22 Ekvivalencie pre ekvivalentné úpravy

---

#### Veta 2.56 (Pokračovanie).

$(A \wedge A) \text{ a } A$	<i>idempotencia</i>
$(A \vee A) \text{ a } A$	
$(A \wedge \top) \text{ a } A$	<i>identita</i>
$(A \vee \perp) \text{ a } A$	
$(A \vee (A \wedge B)) \text{ a } A$	<i>absorpcia</i>
$(A \wedge (A \vee B)) \text{ a } A$	
$(A \vee \neg A) \text{ a } \top$	<i>vylúčenie tretieho</i>
$(A \wedge \neg A) \text{ a } \perp$	<i>spor</i>
$(A \rightarrow B) \text{ a } (\neg A \vee B)$	<i>nahradenie <math>\rightarrow</math></i>

### 2.6.2. Konjunktívna a disjunktívna normálna forma

#### III.23 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 nespĺniteľnú 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.24 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.

### III.25 Konjunktívny a disjunktívny normálny tvar

---

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

$$A_1 = p$$

$$A_2 = \neg q$$

$$A_3 = \square$$

$$A_4 = (p \vee \neg q)$$

$$A_5 = (p \wedge \neg q)$$

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

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

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

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

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

## IV. prednáška

# CNF. Tablový kalkul

12. 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 CNF<sub>1</sub>

1. Nahradíme implikáciu disjunkciou:

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

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

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

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

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

4. Prezátvorkujeme na požadovaný tvar pomocou asociatívnych pravidiel.

**Tvrdenie 2.60.** Výsledná formula alg. CNF<sub>1</sub> je ekvivalentná s pôvodnou a je v CNF.

#### IV.4 CNF — trochu lepší prístup

---

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.  $((\neg a \wedge \neg b) \vee \neg(c \vee (d \wedge \neg e)))$  [2 – deMorganovo pravidlo]
4.  $((\neg a \wedge b) \vee \neg(c \vee (d \wedge \neg e)))$  [2 – dvojitá implikácia]
5.  $((\neg a \wedge b) \vee (\neg c \wedge \neg(d \wedge \neg e)))$  [2 – deMorganovo pravidlo]
6.  $((\neg a \wedge b) \vee (\neg c \wedge (\neg d \vee \neg e)))$  [2 – deMorganovo pravidlo]
7.  $((\neg a \wedge b) \vee (\neg c \wedge (\neg d \vee e)))$  [2 – dvojitá implikácia]
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 CNF – prečo iba trochu lepší prístup

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

- $A_2 = ((p_1 \wedge q_1) \vee (p_2 \wedge q_2))$   
 $C_2 = ((p_1 \vee p_2) \wedge (p_1 \vee q_2) \wedge (q_1 \vee p_2) \wedge (q_1 \vee p_2))$   
 $A_2 \Leftrightarrow C_2, \quad \deg(A_2) = 3, \quad \deg(B_2) = 7$
- $A_3 = ((p_1 \wedge q_1) \vee (p_2 \wedge q_2) \vee (p_3 \wedge q_3))$   
 $C_3 = ((p_1 \vee p_2 \vee p_3) \wedge (p_1 \vee q_2 \vee p_3) \wedge (q_1 \vee p_2 \vee p_3) \wedge (q_1 \vee p_2 \vee p_3) \wedge (p_1 \vee p_2 \vee q_3) \wedge (p_1 \vee q_2 \vee q_3) \wedge (q_1 \vee p_2 \vee q_3) \wedge (q_1 \vee p_2 \vee q_3))$   
 $A_3 \Leftrightarrow C_3, \quad \deg(A_3) = 5, \quad \deg(C_3) = 23$
- $A_n = ((p_1 \wedge q_1) \vee \dots \vee (p_n \wedge q_n))$   
 Koľko klauzúl bude obsahovať  $C_n$ ?  
 Akého bude stupňa?



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. Vyjadrime, že  $r_i$  je ekvivalentným zástupcom konjunkcie  $(p_i \wedge q_i)$ :  
 $(r_i \leftrightarrow (p_i \wedge q_i))$
3. Použime  $r_i$  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  $((s \leftrightarrow (r_1 \vee \dots \vee r_n)) \wedge (r_1 \leftrightarrow (p_1 \wedge q_1)) \wedge \dots \wedge (r_n \leftrightarrow (p_n \wedge q_n)) \wedge s)$

Ekvivalentnými úpravami

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

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

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

## 2.7. Kalkuly

- 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.9 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.10 Kalkuly — dokazovanie vyplývania syntakticky

---

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

- Ukážeme si dva kalkuly:  
*tablový* — stromový, prirodzenejší  
*rezolvenciu* — lineárny, strojový

## 2.8. Tablový kalkul

### IV.11 Dôkaz vyplývania sporom v slovenčine

*Príklad 2.62.* Dokážme, že z  $T'_{\text{party}} = \{ (kim \rightarrow (jim \wedge \neg sarah)), (eva \rightarrow kim) \}$  vyplýva  $(sarah \rightarrow \neg eva)$ . Poďme na to sporom:

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

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

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

### IV.12 Tablová notácia pre dôkazy

Dôkaz stručne zapíšeme v tablovej notácii:

- **T**  $X$  označuje fakt, že  $v$  spĺňa  $X$ .
- **F**  $X$  označuje fakt, že  $v$  nespĺňa  $X$ .
- Ak z niektorého predchádzajúceho faktu o formule  $X$  priamo z *definície splňania* **vyplýva (ne)splnenie** niektorej *priamej podformuly*  $X$ , zapíšeme ho do *ďalšieho* riadka.  
 Poznačíme si k nemu písmeno  $\alpha$  a číslo zdrojového faktu.

- Ak z niektorého faktu o formule  $X$  **vyplýva** o jej *priamych podformulách* fakt  $F_1$  **alebo** fakt  $F_2$ , **rozdelíme** úvahu na dve nezávislé vetvy, pričom prvá začne faktom  $F_1$  a druhá faktom  $F_2$ . K oboj si poznačíme písmeno  $\beta$  a číslo zdrojového faktu.
- Ak nastane **spor** medzi splnením a nesplnením *tej istej* formuly, pridáme riadok so symbolom  $*$  a poznačíme si čísla faktov, ktoré sú v spore.

#### IV.13 Dôkaz vyplývania sporom v tablovej notácii

Príklad 2.63.

(1)	$\mathbf{T}(kim \rightarrow (jim \wedge \neg sarah))$	$z\ T'_{party}$
(2)	$\mathbf{T}(eva \rightarrow kim)$	$z\ T'_{party}$
(3)	$\mathbf{F}(sarah \rightarrow \neg eva)$	dôkaz sporom
(4)	$\mathbf{T}\ sarah$	$\alpha(3)$
(5)	$\mathbf{F}\ \neg eva$	$\alpha(3)$
(6)	$\mathbf{T}\ eva$	$\alpha(5)$
(7)	$\mathbf{F}\ eva$	$\beta(2)$
	$*$ (6) a (7)	
(8)	$\mathbf{T}\ kim$	$\beta(2)$
(9)	$\mathbf{F}\ kim$	$\beta(1)$
	$*$ (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)	$\mathbf{F}\ sarah$	$\alpha(12)$
	$*$	(4) a (13)

#### IV.14 Spĺňanie a priame podformuly

**Pozorovanie 2.64.** *Nech  $v$  je ľubovoľné ohodnotenie výrokových premenných. Nech  $X$  a  $Y$  sú ľubovoľné formuly.*

1.  $T)$  Ak  $v$  spĺňa  $\neg X$ , tak  $v$  nespĺňa  $X$ .  
 $F)$  Ak  $v$  nespĺňa  $\neg X$ , tak  $v$  spĺňa  $X$ .
2.  $T)$  Ak  $v$  spĺňa  $(X \wedge Y)$ , tak  $v$  spĺňa  $X$  a  $v$  spĺňa  $Y$ .

*F) Ak v nespĺňa  $(X \wedge Y)$ , tak v nespĺňa  $X$  alebo v nespĺňa  $Y$ .*

3. *T) Ak v spĺňa  $(X \vee Y)$ , tak v spĺňa  $X$  alebo v spĺňa  $Y$ .*

*F) Ak v nespĺňa  $(X \vee Y)$ , tak v nespĺňa  $X$  a v nespĺňa  $Y$ .*

4. *T) Ak v spĺňa  $(X \rightarrow Y)$ , tak v nespĺňa  $X$  alebo v spĺňa  $Y$ .*

*F) Ak v nespĺňa  $(X \rightarrow Y)$ , tak v spĺňa  $X$  a v nespĺňa  $Y$ .*

#### IV.15 Označené formuly a ich sémantika

---

**Definícia 2.65.** Nech  $X$  je formula výrokovej logiky.

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

**Definícia 2.66.** 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.  $S^+$ ,  $T_3^+$ .

#### IV.16 Tablové pravidlá

---

Podľa pozorovania 2.64 a definície 2.66 môžeme sformulovať pravidlá pre označené formuly:

$\alpha$	$\beta$	
$\alpha_1$	$\beta_1$	$\beta_2$
$\alpha_2$		
$\frac{\mathbf{T}(X \wedge Y)}{\mathbf{T} X}$	$\frac{\mathbf{F}(X \wedge Y)}{\mathbf{F} X \mid \mathbf{F} Y}$	$\frac{\mathbf{T} \neg X}{\mathbf{F} X}$
$\mathbf{T} Y$		
$\frac{\mathbf{F}(X \vee Y)}{\mathbf{F} X}$	$\frac{\mathbf{T}(X \vee Y)}{\mathbf{T} X \mid \mathbf{T} Y}$	$\frac{\mathbf{F} \neg X}{\mathbf{T} X}$
$\mathbf{F} Y$		
$\frac{\mathbf{F}(X \rightarrow Y)}{\mathbf{T} X}$	$\frac{\mathbf{T}(X \rightarrow Y)}{\mathbf{F} X \mid \mathbf{T} Y}$	
$\mathbf{F} Y$		

#### IV.17 Jednotný zápis označených formúl typu $\alpha$

**Definícia 2.67** (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 2.68** (Stručne vďaka jednotnému zápisu). *Nech  $v$  je ľubovoľné ohodnotenie výrokových premenných.*

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

#### IV.18 Jednotný zápis označených formúl typu $\beta$

**Definícia 2.69** (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 2.70** (Stručne vďaka jednotnému zápisu). *Nech  $v$  je ľubovoľné ohodnotenie výrokových premenných. Potom  $v$  spĺňa  $\beta$  vtt  $v$  spĺňa  $\beta_1$  alebo  $v$  spĺňa  $\beta_2$ .*

#### IV.19 Tablo pre množinu označených formúl

**Definícia 2.71.** *Analytické tablo pre množinu označených formúl  $S^+$  (skrátene tablo pre  $S^+$ ) je binárny strom, ktorého vrcholy obsahujú označené formuly*

*a ktorý je skonštruovaný podľa nasledovných rekurzívnych pravidiel:*

- Strom s jediným vrcholom (koreňom) obsahujúcim niektorú označenú formulu  $A^+$  z  $S^+$  je tablom pre  $S^+$ .
- Nech  $\mathcal{T}$  je tablo pre  $S^+$  a  $y$  je nejaký jeho list. Potom tablom pre  $S^+$  je aj každé *priame rozšírenie*  $\mathcal{T}$  ktoroukoľvek z operácií:

A: Ak sa na vetve  $\pi_y$  (ceste z koreňa do  $y$ ) vyskytuje nejaká označená formula  $\alpha$ , tak ako jediné dieťa  $y$  pripojíme nový vrchol obsahujúci  $\alpha_1$  alebo  $\alpha_2$ .

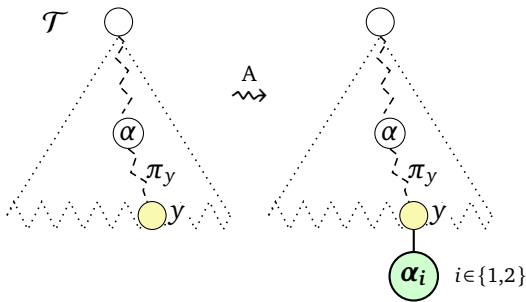
B: Ak sa na vetve  $\pi_y$  vyskytuje nejaká označená formula  $\beta$ , tak ako deti  $y$  pripojíme dva nové vrcholy, pričom ľavé dieťa bude obsahovať  $\beta_1$  a pravé  $\beta_2$ .

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

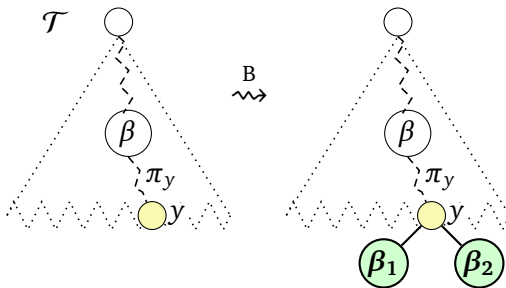
Nič iné nie je tablom pre  $S^+$ .

## Operácia priameho rozšírenia

## Pravidlá a označené formuly v nich



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



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

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

**Definícia 2.72.** 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  $X^+ \in \text{formulas}(\pi)$ .

**Definícia 2.73.** Vetva  $\pi$  tabla  $\mathcal{T}$  je uzavretá vtt na  $\pi$  sa súčasne vyskytujú označené formuly  $\mathbf{FX}$  a  $\mathbf{TX}$  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.



### 2.8.1. Korektnosť

#### IV.22 Korektnosť tablového kalkulu

---

*Korektnosť* (angl. *soundness*) kalkulu neformálne:

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

**Veta 2.74** (Korektnosť tablového kalkulu). *Nech  $S^+$  je množina označených formúl a  $\mathcal{T}$  je uzavreté tablo pre  $S^+$ .*

*Potom je množina  $S^+$  nesplniteľná.*

**Dôsledok 2.75.** *Nech  $S$  je množina formúl a  $X$  je formula.*

*Ak existuje uzavreté tablo pre  $\{\mathbf{T} A \mid A \in S\} \cup \{\mathbf{F} X\}$  (skr.  $S \vdash X$ ),*

*tak z  $S$  vyplýva  $X$  ( $S \models X$ ).*

**Dôsledok 2.76.** *Nech  $X$  je formula.*

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

## V. prednáška

# Korektnosť a úplnosť tablového kalkulu

19. marca 2018

### V.1 Korektnosť — splnenie priameho rozšírenia tabla

Na dôkaz korektnosti potrebujeme pomocnú definíciu a dve lemy.

**Definícia 2.77.** 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 2.78 (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.2 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  $\mathcal{T}$  operáciou A, pridaním nového dieťaťa z nejakému listu  $y$  v  $\mathcal{T}$ , pričom  $y$  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  $\mathcal{T}$  operáciou B, 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  $\mathcal{T}$  operáciou Ax, pridaním nového dieťaťa  $z$  nejakému listu  $y$  v  $\mathcal{T}$ , pričom  $z$  obsahuje formulu  $X^+ \in S^+$ . Ak  $\pi \neq \pi_y$ , tak  $\mathcal{T}_1$  obsahuje  $\pi$  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.3 Korektnosť — splnenie množiny a tabla pre ňu

**Lema 2.79** (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.4 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.  $\square$

### 2.8.2. Tablový dôkaz splniteľnosti

#### V.5 Úplná vetva a tablo

---

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

**Definícia 2.80** (Úplná vetva a úplné tablo). Nech  $S^+$  je množina označených formúl a  $\mathcal{T}$  je tablo pre  $S^+$ .

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

- pre každú označenú formulu  $\alpha$ , ktorá sa vyskytuje na  $\pi$ , sa *obidve* označené formuly  $\alpha_1$  a  $\alpha_2$  vyskytujú na  $\pi$ ;
- pre každú označenú formulu  $\beta$ , ktorá sa vyskytuje na  $\pi$ , sa *aspoň jedna* z označených formúl  $\beta_1, \beta_2$  vyskytuje na  $\pi$ ;
- každá  $X^+ \in S^+$  sa vyskytuje na  $\pi$ .

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

**Príklad 2.81.** Vybudujme úplné tablo pre  $\mathbf{F}X$ , kde  $X = (((p \vee q) \wedge (r \vee p)) \rightarrow (p \wedge (q \vee r)))$ .

#### V.6 Otvorené tablo a splniteľnosť

---

Nech tablové pravidlá v príklade použijeme v akomkoľvek,

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

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

1. nájdeme otvorenú vetvu  $\pi$ ,
2. pre každú výrokovú premennú  $p$ 
  - ak sa v  $\pi$  nachádza  $\mathbf{T}p$ , definujeme  $v(p) = t$ ;
  - ak sa v  $\pi$  nachádza  $\mathbf{F}p$ , definujeme  $v(p) = f$ ;
  - inak definujeme  $v(p)$  ľubovoľne.

Toto  $v$  splňa  $\pi$ , a preto  $v$  splňa  $S^+$  (všetky formuly z  $S^+$  sa vyskytujú na  $\pi$ ).

Otázka. • Dá sa vždy nájsť úplné tablo?

- Naozaj sa z úplného otvoreného tabla dá vytvoriť splňajúce ohodnotenie?

## V.7 Existencia úplného tabla

**Lema 2.82** (o existencii úplného tabla). *Nech  $S^+$  je konečná množina označených formúl.*

*Potom existuje úplné tablo pre  $S^+$ .*

*Dôkaz.* Vybudujeme tablo  $\mathcal{T}_0$  pre  $S^+$  tak, že do koreňa vložíme niektorú formulu z  $S^+$  a opakovaním operácie  $Ax$  postupne doplníme ostatné.

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

- Na  $\pi_y$  sa nachádza nejaká formula  $\alpha$ , ale nenachádza sa niektorá z formúl  $\alpha_1$  a  $\alpha_2$ .
- Na  $\pi_y$  sa nachádza nejaká formula  $\beta$ , ale nenachádza sa ani jedna z formúl  $\beta_1$  a  $\beta_2$ .

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

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

### 2.8.3. Hintikkova lema

#### V.8 Nadol nasýtené množiny a Hintikkova lemma

**Definícia 2.83.** Množina označených formúl  $S^+$  sa nazýva *nadol nasýtená* vtt platí:

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

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

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

**Pozorovanie 2.84.** *Nech  $\pi$  je úplná otvorená vetva nejakého tabla  $\mathcal{T}$ . Potom množina všetkých formúl na  $\pi$  je nadol nasýtená.*

**Lema 2.85** (Hintikkova). *Každá nadol nasýtená množina  $S^+$  je splniteľná.*

*Dôkaz Hintikkovej lemy.* Chceme vytvoriť ohodnotenie  $v$ , ktoré splní všetky formuly z  $S^+$ . Definujme  $v$  pre každú výrokovú premennú  $p$  takto:

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

$v$  je korektne definované vďaka  $H_0$ .

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

- $v$  očividne splňa všetky označené výrokové premenné z  $S^+$ .
- $X^+ \in S^+$  je buď  $\alpha$  alebo  $\beta$ :
  - Ak  $X^+$  je  $\alpha$ , potom obidve  $\alpha_1, \alpha_2 \in S^+$  ( $H_1$ ), sú nižšieho stupňa  $X^+$ , a teda podľa indukčného predpokladu sú splnené pri  $v$ , preto  $v$  splňa aj  $\alpha$  (podľa pozorovania 2.68).
  - Ak  $X^+$  je  $\beta$ , potom aspoň jedna z  $\beta_1, \beta_2$  je v  $S^+$  ( $H_2$ ). Nech je to ktorákoľvek, je nižšieho stupňa ako  $X^+$ , teda podľa IP ju  $v$  splňa, a preto  $v$  splňa  $\beta$  (podľa pozorovania 2.70).  $\square$

## 2.8.4. Úplnosť

### V.10 Úplnosť

---

Úplnosť kalkulu neformálne:

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

**Veta 2.86** (o úplnosti). *Nech  $S^+$  je konečná nesplniteľná množina označených formúl.*

*Potom existuje uzavreté tablo pre  $S^+$ .*

**Dôsledok 2.87.** *Nech  $S$  je konečná teória a  $X$  je formula.*

*Ak  $S \models X$ , tak  $S \vdash X$ .*

**Dôsledok 2.88.** *Nech  $X$  je formula. Ak  $\models X$ , tak  $\vdash X$ .*

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

### V.11 Úplnosť – dôkaz

---

*Dôkaz vety o úplnosti.* Zoberme ľubovoľnú konečnú nesplniteľnú množinu označených formúl  $S^+$ .

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

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

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

## VI. prednáška

# Korektné pravidlá. Rezolvenca

26. marca 2018

### 2.8.5. Nové korektné pravidlá

#### VI.1 Ingrediencie korektnosti a úplnosti tabiel

Všimnite si:

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

#### VI.2 Nové pravidlo

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

$$\frac{T(A \vee B) \quad F A}{T B} \quad ? \quad (DS_1)$$

Upravíme definíciu priameho rozšírenia:

#### Úprava definície 2.71

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



A ...

⋮

**DS<sub>1</sub>**: Ak sa na vetve  $\pi_y$  nachádzajú obe formuly  $\mathbf{T}(A \vee B)$  a  $\mathbf{F} A$ , tak ako jediné dieťa  $y$  pripojíme nový vrchol obsahujúci  $\mathbf{T} B$ .

### VI.3 Nové pravidlo vs. korektnosť a úplnosť

- Pravidlo (**DS<sub>1</sub>**) je *korektné*:

Nech  $v$  je ľubovoľné ohodnotenie.

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

Keďže  $v \models \mathbf{T}(A \vee B)$ , tak  $v \models (A \vee B)$ , teda  $v \models A$  alebo  $v \models B$ .

Pretože ale  $v \models \mathbf{F} A$ , tak  $v \not\models A$ . Takže  $v \models B$ .

- Preto stále dokážeme lemu K1 (2.78):

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

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

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

Z nej dokážeme lemu K2 a vetu o korektnosti

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

### VI.4 Nové pravidlá vo všeobecnosti

**Definícia 2.89** (Tablové pravidlo a jeho korektnosť). Nech  $n$  a  $k$  sú prirodzené čísla,  $n \geq 0$ ,  $k > 0$ , nech  $P_1^+, \dots, P_n^+, C_1^+, \dots, C_k^+$  sú označené formuly nad výrokovými premennými  $\{q_1, \dots, q_m\}$ .

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

$$R = \left\{ \frac{P_1^+_{[q_1|X_1, \dots, q_m|X_m]} \quad \dots \quad P_n^+_{[q_1|X_1, \dots, q_m|X_m]}}{C_1^+_{[q_1|X_1, \dots, q_m|X_m]} \quad \dots \quad C_k^+_{[q_1|X_1, \dots, q_m|X_m]}} \mid X_1, \dots, X_m \in \mathcal{E} \right\},$$

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

Prvky hornej  $n$ -tice nazývame *premisy*, prvky dolnej  $k$ -tice nazývame *závery*.

Každý prvok  $R$  nazývame *inštancia pravidla*  $R$ .

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

## VI.5 Nové pravidlá vo všeobecnosti

### Úprava definície 2.71

(...)

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

⋮

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

## 2.9. Rezolvencia vo výrokovej logike

### VI.6 Transitivity implikácie

Vráťme sa k neoznačeným formulám.

Je nasledujúce pravidlo korektné?

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

Nahradíme implikácie disjunkciami:

$$\frac{(\neg A \vee B) \quad (\neg B \vee C)}{(\neg A \vee C)}$$

## VI.7 Rezolvenca

Predchádzajúce pravidlo sa dá zovšeobecniť na ľubovoľné dvojice klauzúl:

**Definícia 2.90.** *Rezolvenčný princíp (rezolvenca, angl. resolution principle)* je pravidlo

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

pre ľubovoľnú výrokovú premennú  $p$

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

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

**Tvrdenie 2.91.** *Rezolvenca je korektné pravidlo, teda rezolventa je logickým dôsledkom množiny obsahujúcej obe premisy.*

## VI.8 Špeciálne prípady rezolvenencie

Viacero pravidiel sa dá chápať ako špeciálne prípady rezolvenencie:

$\frac{(\neg p \vee q) \quad (\neg q \vee r)}{(\neg p \vee r)}$	$\frac{(p \rightarrow q) \quad (q \rightarrow r)}{(p \rightarrow r)}$	(tranzitivita $\rightarrow$ )
$\frac{(\neg p \vee \ell) \quad p}{\ell}$	$\frac{(p \rightarrow \ell) \quad p}{\ell}$	(modus ponens)
$\frac{(\neg p \vee q) \quad \neg q}{\neg p}$	$\frac{(p \rightarrow q) \quad \neg q}{\neg p}$	(modus tolens)

- Rezolvenca s jednotkovou klauzulou skráti druhú klauzulu:

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

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

- Ak rezolvenca odvodí **prázdnu klauzulu**

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

premisy **nie sú súčasne splniteľné**

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

$$\frac{(\neg p \vee q) \quad (p \vee \neg q)}{(q \vee \neg q)} \quad \frac{(\neg p \vee q) \quad (p \vee \neg q)}{(\neg p \vee p)} \quad \frac{(\neg p \vee q) \quad (p \vee \neg q)}{\square}$$

Prečo?

Lebo  $\{(\neg p \vee q), (p \vee \neg q)\}$  je splniteľná

$(v_1 = \{p \mapsto t, q \mapsto t\}, v_2 = \{p \mapsto f, q \mapsto f\})$ ,

ale  $\square$  je nesplniteľná

- Opakovaným aplikovaním rezolvenzie môžeme odvodzovať ďalšie dôsledky

*Príklad 2.92.* Z množiny  $S = \{(\neg p \vee r), (\neg q \vee r), (p \vee q)\}$  odvodíme  $(r \vee r)$ :

- (1)  $(\neg p \vee r)$  predpoklad z  $S$
- (2)  $(\neg q \vee r)$  predpoklad z  $S$
- (3)  $(p \vee q)$  predpoklad z  $S$
- (4)  $(r \vee q)$  rezolventa (1) a (3)
- (5)  $(r \vee r)$  rezolventa (2) a (4)

- Klausula  $(r \vee r)$  je evidentne ekvivalentná s  $r$ ;  
 $r$  sa ale z množiny  $S$  iba rezolvenciou odvodíť nedá
- Preto potrebujeme ešte *pravidlo idempotencie*:

$$\frac{(k_1 \vee \dots \vee \ell \vee \dots \vee \ell \vee \dots \vee k_n)}{(k_1 \vee \ell \vee \dots \vee k_n)}$$

#### VI.12 Rezolvenčné odvodenie a zamietnutie

**Definícia 2.93.** *Rezolvenčné odvodenie* z množiny klauzúl  $S$  je každá (aj nekonečná) postupnosť klauzúl  $C_1, C_2, \dots, C_n, \dots$ , ktorej každý člen  $C_i$  je:

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

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

**Definícia 2.94.** Množinu klauzúl budeme nazývať aj *klauzálna teória*.

#### VI.13 Korektnosť a úplnosť rezolvenčie

**Veta 2.95** (Korektnosť rezolvenčie). *Nech  $S$  je množina klauzúl. Ak existuje zamietnutie  $S$ , tak  $S$  je nespĺniteľná.*

**Veta 2.96** (Úplnosť rezolvenčie). *Nech  $S$  je množina klauzúl. Ak  $S$  je nespĺniteľná, tak existuje zamietnutie  $S$ .*

## 2.10. Späť k dôkazom o vyplývaní

VI.14 Konzultácie a termín pre 6. sadu úloh

---

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

využívajte **konzultačné hodiny**:

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

- Riešenie **6. sady úloh** odovzdajte

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

VI.15 Uvažovanie o vyplývaní

---

Cvičenie 2.97 (Sada úloh 3, úloha 3. Zbierka: úloha 2.4.6.). Nech  $X$  a  $Y$  sú ľubovoľné výrokové formuly, nech  $T$  je ľubovoľná výroková teória.

Dokážte alebo vyvráťte:

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

**Riešenie 2.97 (c).** Zoberme ľubovoľnú teóriu  $T$  a formulu  $X$  také, že  $T \models \neg X$ . Aby tvrdenie platilo:

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

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

- Zoberme  $T = \{(p \wedge \neg p)\}$  a  $X = p$ .
- Pre ľubovoľné ohodnotenie  $v$  platí  $v \models T$ , teda platia aj implikácie:  
i. ak  $v \models T$ , tak  $v \models \neg X$ ,                      ii. ak  $v \models T$ , tak  $v \models X$ ,  
lebo ich *antecedenty* sú nepravdivé.
- Ich *zovšeobecnením* dostávame:    i.  $T \models \neg X$     a    ii.  $T \models X$ .

**Riešenie 2.97 (d).** Zoberme ľubovoľnú teóriu  $T$  a formulu  $X$  také, že  $T \not\models X$ .

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

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

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

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

**Riešenie 2.97** (e, smer  $\Rightarrow$ ). Zoberme ľubovoľnú teóriu  $T$  a formuly  $X$  a  $Y$  také, že  $T \models (X \rightarrow Y)$ , teda

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

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

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

Zoberme teda ľubovoľné ohodnotenie  $v$ .

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

Vlastnosť (\*) teda platí aj v tomto prípade.

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



**Riešenie 2.97** (e, smer  $\Leftarrow$ ). Zoberme ľubovoľnú teóriu  $T$  a formuly  $X$  a  $Y$  také, že  $T \cup \{X\} \models Y$ , teda

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

Aby tvrdenie (e $\Leftarrow$ ) platilo, musí  $T \models (X \rightarrow Y)$ , teda

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

Zoberme teda ľubovoľné ohodnotenie  $v$ .

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

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

### Používanie pojmov *spĺnenie* a *vyplývanie*

- |   |  |
|---|--|
| ✓ ohodnotenie $v$ spĺňa formulu $X$       | ✓ z teórie $T$ vyplýva formula $X$               |
| ✓ formula $X$ je splnená v ohodnotení $v$ | ✓ formula $X$ vyplýva z teórie $T$               |
| ✓ $v \models X$                           | ✓ formula $X$ je (logickým) dôsledkom teórie $T$ |
| ✗ formula $X$ spĺňa ohodnotenie $v$       | ✓ teória $T$ má (logický) dôsledok $X$           |
| ✓ ohodnotenie $v$ spĺňa teóriu $T$        | ✓ $T \models X$                                  |
| ✓ teória $T$ je splnená v ohodnotení $v$  | ✗ z ohodnotenia $v$ vyplýva...                   |
| ✓ $v \models T$                           | ✗ z formuly $X$ vyplýva teória $T$               |
| ✗ teória $T$ spĺňa ohodnotenie $v$        |  |

## Ignorovanie pojmov a ich definícií

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

## Definície pojmov a ich negovanie

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

## Skríženie pojmov splnenia a vyplývania

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

## Skoky v uvažovaní veľké a nezdôvodnené

⚠ Ak  $T \models (X \rightarrow Y)$ , tak  $T \not\models X$  alebo  $T \models Y$ .

➡ Ak  $T \not\models X$  alebo  $T \models Y$ , tak  $T \models (X \rightarrow Y)$ .

➡ Ak  $v \not\models T$ , tak  $T$  je nespĺniteľná.

### VI.23 Problémy v dôkazoch (4)

#### ➡ Neuvedenie si toho, čo treba dokázať

Rozoberú sa možnosti vyplývajúce z predpokladov, ale nezistí sa, či platí požadovaný záver

#### ➡ Uvažovanie v kruhu

Použitie toho, čo máme dokázať, na zdôvodnenie nejakého kroku

#### ⚠ Snaha uvažovať **naraz o všetkých modeloch/ohodnoteniach**

- ✔ 1. Vyslovte jasne, akú vlastnosť majú mať všetky ohodnotenia
- 2. **Zoberte jedno ohodnotenie, o ktorom nič nepredpokladáte („ľubovoľné“)**
- 3. **Overte**, či má za každých okolností požadovanú vlastnosť
- 4. **Zovšeobecňte**, že požadovanú vlastnosť majú všetky ohodnotenia

#### ⚠ Snaha uvažovať **súbežne o viacerých možnostiach**

- ✔ **Uvažujte prípady postupne a oddelene, vyčerpajte všetky možnosti**

### VI.24 Problémy v dôkazoch (5)

#### Uvažovanie o formulách a teóriách, akoby to boli výrokové premenné

- Ohodnotenie  $v$  priradzuje  $t$  alebo  $f$  iba výrokovej premennej  
( $v(p) = t$ ,  $v(p) = f$ ,  ~~$v(X) = t$~~ ,  ~~$v(X \wedge Y) = t$~~ ,  ~~$v(T) = t$~~ )

- Formula  $X$  je v ohodnotení  $v$  splnená ( $v \models X$ ) alebo nesplnená ( $v \not\models X$ )
- Teória  $T$  je v ohodnotení  $v$  splnená ( $v \models T$ ) alebo nesplnená ( $v \not\models T$ )

## VII. prednáška

# SAT solver a algoritmus DPLL. Syntax relačnej logiky prvého rádu

9. apríla 2018

### 2.11. Problém výrokovologickej splniteľnosti (SAT)

#### VII.1 Problém SAT

---

- *Problémom výrokovologickej splniteľnosti (SAT)* je problém určenia toho, či je daná množina výrokových formúl splniteľná
- Zvyčajne sa redukuje na problém splniteľnosti množiny klauzúl (teda formuly v CNF)
- *SAT solver* je program, ktorý rieši problém SAT

*Príklad 2.98.* Je množina klauzúl  $S$  splniteľná?

$$S = \{(a \vee b), (a \vee \neg b), (\neg a \vee b), (\neg a \vee \neg b \vee \neg c), (\neg a \vee c)\}$$

#### VII.2 Tabuľková metóda

---

- Tabuľkovou metódou skúmame *všetky* ohodnotenia výrokových premenných
- Preskúmanie ohodnotení trvá  $O(s2^N)$  krokov, kde  $N$  je počet premenných a  $s$  je súčet veľkostí klauzúl
  - ▶  $2^N$  ohodnotení, pre každé treba zistiť, či sú všetky klauzuly splnené
- Celú tabuľku si pamätáme (píšeme na papier)

- Tabuľka zaberá priestor  $O(k2^N)$ , kde  $k$  je počet klauzúl
- Tabuľka slúži aj ako dôkaz nespľniteľnosti

### 2.11.1. Naivný backtracking

#### VII.3 Naivný backtracking v Pythone

---

```
#!/usr/bin/env python3
class Sat(object):
    def __init__(self, n, clauses):
        self.n, self.clauses, self.solution = n, clauses, None
    def checkClause(self, e, c):
        return any( ( e[abs(lit)] if lit > 0 else not e[abs(lit)] )
                    for lit in c )
    def check(self, e):
        return all( self.checkClause(e, cl) for cl in self.clauses )
    def solve(self, i, e):
        if i >= self.n:
            if self.check(e):
                self.solution = e
                return True
            return False
        for v in [True, False]:
            e[i] = v
            if self.solve(i+1, e):
                return True
        return False
```

Sat(20, [[]]).solve(0, {})

Čas:  $O(s2^N)$ , priestor:  $O(s+N)$ ;

$N$  — počet premenných,

$s$  — súčet veľkostí klauzúl

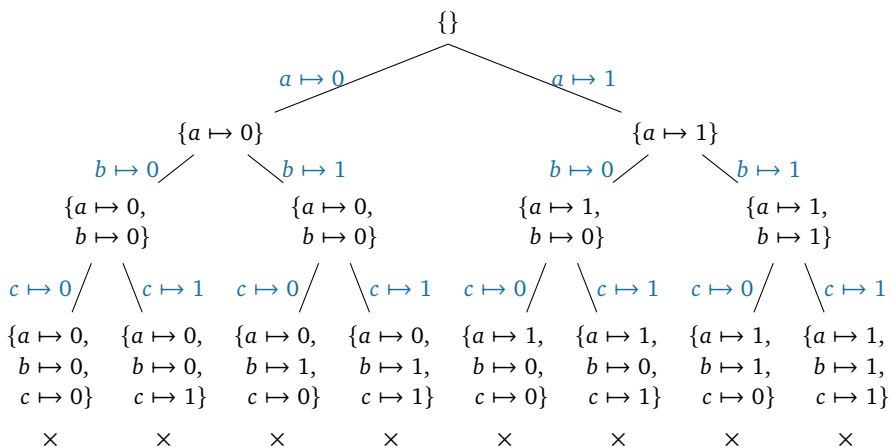
#### VII.4 Strom prehľadávania ohodnotení

---

$S = \{(a \vee b), (a \vee \neg b), (\neg a \vee b), (\neg a \vee \neg b \vee \neg c), (\neg a \vee c)\}$

$\times: v \models S$

$f := 0, t := 1$



## VII.5 Naivné C++

```
#include <iostream>
int N = 10; bool e[50];
bool check() {
    return false; // kontrola splnenia všetkých klauzúl
}
bool solve1(int i) {
    if (i >= N) {
        if (check())
            return true;
        return false;
    }
    e[i] = false;
    if (solve1(i+1)) return true;
    e[i] = true;
    return solve1(i+1);
}
int main(int argc, char *argv[]) {
    N=atoi(argv[1]);
    std::cout << "N=" << N << std::endl;
    solve1(0);
    return 0;
}
```

```

#include <iostream>
int N = 10;
bool check2(unsigned long long e) {
    return false; // kontrola splnenia všetkých klauzúl
}
bool solve2() {
    unsigned long long e, m = 1ULL << N;
    for (e=0; e < m ; ++e) {
        if (check2(e))
            return true;
    }
    return false;
}
int main(int argc, char *argv[]) {
    N=atoi(argv[1]);
    std::cout << "N=" << N << std::endl;
    solve2();
    return 0;
}

```

Čas prehľadávania stromu ohodnotení v závislosti od počtu literálov

Riešenie	10	20	30	35
python	0m0.028s	0m0.877s	14m49.221s	> 7h
cpp1	0m0.001s	0m0.012s	0m11.085s	5m07.995s
cpp2	0m0.001s	0m0.008s	0m03.441s	1m50.086s

### 2.11.2. Optimalizácia backtrackingu

- Každý uzol prehľadávaného stromu ohodnotení je *čiastočné ohodnotenie*
- Ohodnotenie v uzle je *rozšírením* ohodnotenia v rodičovi

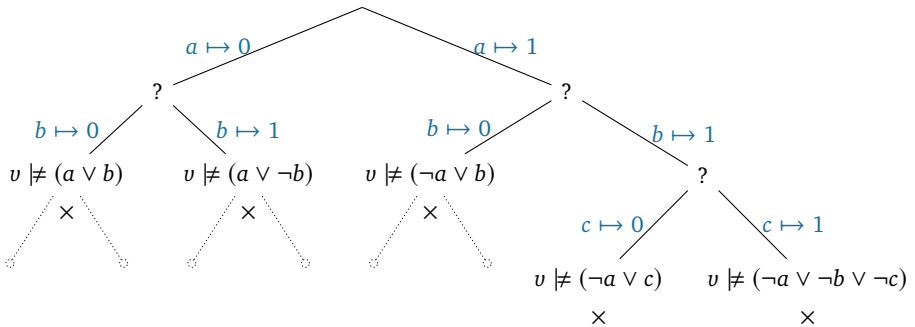


- Niektoré klauzuly sa dajú vyhodnotiť aj v čiastočnom ohodnotení
  - Napríklad v čiastočnom ohodnotení  $v = \{a \mapsto 0, b \mapsto 1\}$  vieme určiť splnenie  $(a \vee b)$ ,  $(a \vee \neg b)$ ,  $(\neg a \vee b)$  z našej  $S$
- Ak je niektorá nesplnená, môžeme „backtracknúť“ — zastaviť prehľadávanie vetvy a vrátiť sa o úroveň vyššie

#### VII.9 Prehľadávanie s priebežným vyhodnocovaním

$S = \{(a \vee b), (a \vee \neg b), (\neg a \vee b), (\neg a \vee \neg b \vee \neg c), (\neg a \vee c)\}$

$\times: v \not\models S$



#### VII.10 Zjednodušenie množiny klauzúl podľa literálu

Nech  $v$  je čiastočné ohodnotenie, v ktorom  $v(a) = 1$ .

Čo vieme o splnení klauzúl z  $S$  každým rozšírením  $v'$  ohodnotenia  $v$ ?

- $v'$  určite splní každú klauzulu obsahujúcu literál  $a$ 
  - $\{a \mapsto 1, \dots\} \models (a \vee b)$
  - $\{a \mapsto 1, \dots\} \models (a \vee \neg b)$

Tieto klauzuly sú pre zistenie splniteľnosti vo všetkých  $v'$  *nepodstatné*, môžeme ich vynechať

- $v'$  splní klauzulu  $(\ell_1 \vee \dots \vee \neg a \vee \dots \vee \ell_n)$  obsahujúcu  $\neg a$   
vtt  $v'$  splní *zjednodušenú* klauzulu  $(\ell_1 \vee \dots \vee \dots \vee \ell_n)$

- $\{a \mapsto 1, \dots\} \models (\neg a \vee \neg b \vee \neg c)$  vtt  $\{a \mapsto 1, \dots\} \models (\neg b \vee \neg c)$
- Mimochodom,  $(\neg b \vee \neg c)$  je rezolventa  $a$  a  $(\neg a \vee \neg b \vee \neg c)$

Stačia nám zjednodušené klauzuly

#### VII.11 Zjednodušenie množiny klauzúl podľa literálu

Množinu klauzúl

$$S = \{ (a \vee b), (a \vee \neg b), (\neg a \vee b), (\neg a \vee \neg b \vee \neg c), (\neg a \vee c) \}$$

teda môžeme zjednodušiť podľa  $a$  na

$$S|_a = \{ b, (\neg b \vee \neg c), c \}.$$

Analogicky môžeme  $S$  zjednodušiť podľa  $\neg a$  na

$$S|_{\neg a} = \{ b, \neg b \}.$$

#### VII.12 Zjednodušenie množiny klauzúl podľa literálu

**Definícia 2.99.** Nech  $p$  je výroková premenná.

Komplementom literálu  $p$  je  $\neg p$ . Komplementom literálu  $\neg p$  je  $p$ .

Komplement literálu  $\ell$  označujeme  $\bar{\ell}$ .

**Definícia 2.100.** Nech  $\ell$  je literál a  $S$  je množina klauzúl. Potom definujeme

$$S|_{\ell} = \{ (\ell_1 \vee \dots \vee \ell_n) \mid (\ell_1 \vee \dots \vee \bar{\ell} \vee \dots \vee \ell_n) \in S \} \cup \{ C \mid C \in S, \vee C \text{ sa nevyskytuje } \ell \text{ ani } \bar{\ell} \}.$$

**Tvrdenie 2.101.** Nech  $\ell$  je literál a  $S$  je množina klauzúl.

Potom  $S \cup \{\ell\}$  je splniteľná vtt  $S|_{\ell}$  je splniteľná.

#### VII.13 Propagácia jednotkových klauzúl

- Zjednodušením množiny klauzúl sa môže značne zmenšiť priestor spĺňajúcich ohodnotení
- Napríklad zjednodušením  $T = \{(a \vee \neg b), (a \vee b \vee c)\}$  podľa  $\neg a$  dostaneme  $T' := T|_{\neg a} = \{\neg b, (b \vee c)\}$
- $T'$  obsahuje jednotkovú klauzulu (unit clause alebo iba unit)  $\neg b$

- Preto  $T'$  spĺňajú iba ohodnotenia  $v$ , v ktorých  $v(b) = 0$
- Pre také ohodnotenia môžeme  $T'$  ďalej zjednodušiť podľa  $\neg b$ :  
 $T'' := T'|_{\neg b} = \{c\}$
- $T''$  môžu splniť iba ohodnotenia  $v$ , v ktorých  $v(c) = 1$
- Pre také ohodnotenia môžeme  $T''$  ďalej zjednodušiť podľa  $c$ :  
 $T''' := T''|_c = \{\}$
- $T'''$  je prázdna, teda je splniteľná

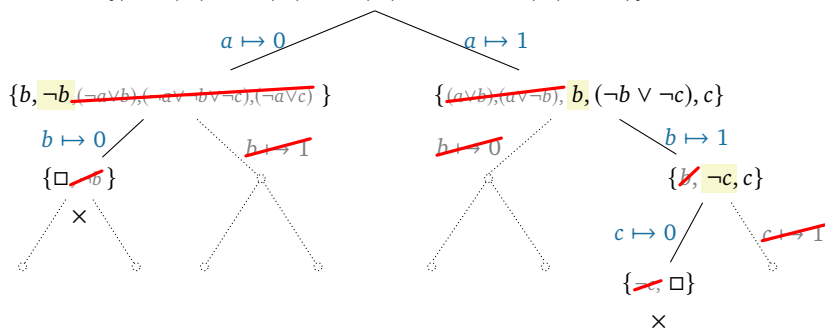
Propagácia jednotkových klauzúl (unit propagation) je proces opakovaného rozširovania ohodnotení podľa jednotkových klauzúl a zjednodušovania

#### VII.14 Propagácia jednotkových klauzúl

**Dôsledok 2.102.** *Nech  $\ell$  je literál a  $S$  je množina klauzúl obsahujúca jednotkovú klauzulu  $\ell$  ( $\ell \in S$ ). Potom  $S$  je splniteľná vtt  $S|_{\ell}$  je splniteľná.*

#### VII.15 Prehľadávanie so zjednodušovaním klauzúla unit propagation

$\{(a \vee b), (a \vee \neg b), (\neg a \vee b), (\neg a \vee \neg b \vee \neg c), (\neg a \vee c)\}$



- Všimnime si literál  $u$  v množine klauzúl:

$$T = \{(\neg a \vee \neg b \vee c), (\neg a \vee u), (\neg b \vee u), a, b, \neg c\}$$

- Literál  $u$  je *nezmiešaný* (angl. *pure*) v  $T$ :  
 $u$  sa vyskytuje v  $T$ , ale jeho komplement  $\neg u$  sa tam nevyskytuje
- Vynechajme z  $T$  všetky klauzuly obsahujúce  $u$ :

$$T' := T|_u = \{(\neg a \vee \neg b \vee c), a, b, \neg c\}$$

- Ak nájdeme ohodnotenie  $v \models T'$ ,  
tak  $v_0 := v(u \mapsto 0)$  aj  $v_1 := v(u \mapsto 1)$  sú modelmi  $T'$   
a  $v_1$  je navyše modelom  $T$ , teda  $T$  je splniteľná
- Ak je  $T'$  nesplniteľná,  
tak je nesplniteľná každá jej nadmnožina, teda aj  $T$

Takže: Z hľadiska splniteľnosti sú klauzuly obsahujúce  $u$  nepodstatné,  
stačí uvažovať  $T|_u$

Analogická úvaha sa dá aplikovať aj na  $\neg u$  a jeho komplement  $u$

**Definícia 2.103.** Nech  $\ell$  je literál a  $S$  je množina klauzúl.

Literál  $\ell$  je *nezmiešaný* (*pure*) v  $S$  vtt  $\ell$  sa vyskytuje v niektorej klauzule z  $S$ ,  
ale jeho komplement  $\bar{\ell}$  sa nevyskytuje v žiadnej klauzule z  $S$ .

**Tvrdenie 2.104.** Nech  $\ell$  je literál a  $S$  je množina klauzúl.

Ak  $\ell$  je *nezmiešaný* v  $S$ , tak  $S$  je splniteľná vtt  $S|_{\ell}$  je splniteľná.

### 2.11.3. DPLL

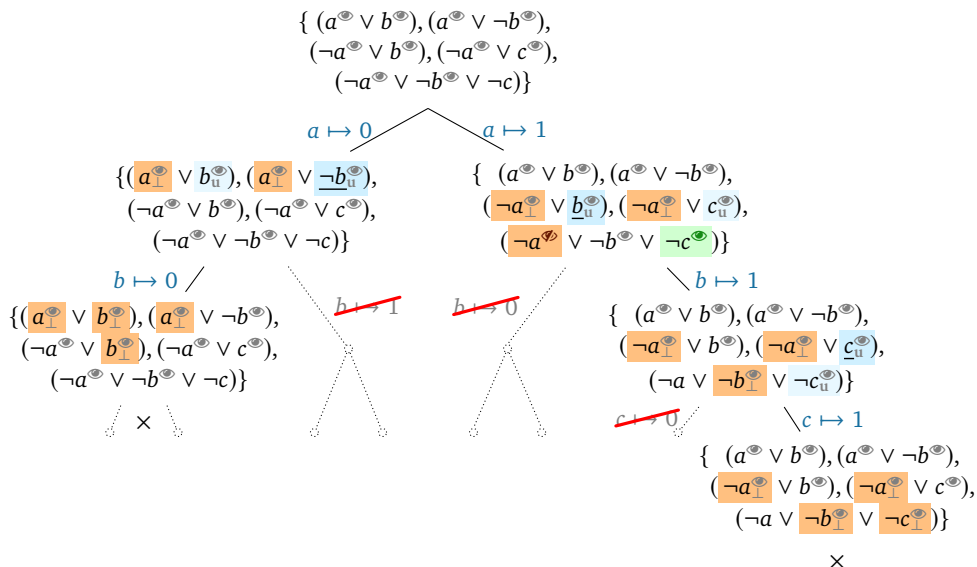
Algoritmus 2.105 (Davis and Putnam [1960], Davis et al. [1962]).

```
1: function DPLL( $\Phi, e$ )
2:   if  $\Phi$  obsahuje prázdnu klauzulu then
3:     return False
4:   end if
5:   if  $e$  ohodnocuje všetky premenné then
6:     return True
7:   end if
8:   while existuje jednotková (unit) klauzula  $\ell$  vo  $\Phi$  do
9:      $\Phi, e \leftarrow \text{UNIT-PROPAGATE}(\ell, \Phi, e)$ 
10:  end while
11:  while existuje nezmiešaný (pure) literál  $\ell$  vo  $\Phi$  do
12:     $\Phi, e \leftarrow \text{PURE-LITERAL-ASSIGN}(\ell, \Phi, e)$ 
13:  end while
14:   $x \leftarrow \text{CHOOSE-BRANCH-LITERAL}(\Phi, e)$ 
15:  return DPLL( $\Phi|_x, e(x \mapsto T)$ ) or DPLL( $\Phi|_{\neg x}, e(x \mapsto F)$ )
16: end function
```

#### VII.19 Technika sledovaných literálov (watched literals)

Aby sme nemuseli zjednodušovať množinu klauzúl:

- Pre každú klauzulu máme 2 sledované literály.
- Sledovaný literál vždy musí byť *nenastavený* alebo *true*.
- Ak nejaký literál nastavíme na *true*: nič nemusíme robiť.
- Ak nejaký literál nastavíme na *false*: musíme nájsť iný. Ak iný nie je, práve sme vyrobili jednotkovú klauzulu (všetky literály okrem toho druhého sledovaného sú *false*).
- Ak backtrackujeme: nič nemusíme robiť (možno sa niektoré sledované literály stali *nenastavenými*).



### 3. Logika prvého rádu

#### 3.1. Syntax relačnej logiky prvého rádu

- Výroková logika *veľmi* zjednodušuje prirodzený jazyk:
  - skúma iba štruktúru tvrdení tvorenú spojками,
  - atomické výroky *nemajú štruktúru*
- Niekedy to neprekáža – konštatovanie globálneho stavu:
  - Prší.
  - Cesta je mokrá.
  - Je pondelok.

- Atomické výroky často hovoria o *vlastnostiach objektov*

- Jerry je myš domová.
- Hlohovský je minister.
- Logika je ľahká.

alebo *vzťahoch objektov*

- Dorothy je staršia ako George.
- Komorník je bohatší ako grófka Agáta.
- Hlohovský prijal úplatok 250 tisíc eur od Veseliča v roku 2013.

- Výroková logika vynucuje *samostatné výrokové premenné* pre rôzne kombinácie objektov, vlastností a vzťahov — neintuitívne, nepraktické
- Existujú ale iné logiky ako výroková
- *Logika prvého rádu* rozoznáva štruktúru atomických výrokov

- Jednoduché vety v prirodzených jazykoch sa delia na *podmetovú* a *prísudkovú* časť  
Hlohovský prijal úplatok 250 tisíc eur od Veseliča v roku 2013  
Prísudková časť sa ďalej delí na:

<i>prísudok</i>	<i>predmet</i>		<i>predmet</i>		<i>prísl. urč. času</i>
prijal	úplatok 250 tisíc eur	od	Veseliča	v	roku 2013

- Logika prvého rádu nerozoberá štruktúru atomických výrokov až tak podrobne

- *Atomické formuly* (jednoduché výroky) v logike prvého rádu:  
*predikátový\_symbol* (*argument*<sub>1</sub>, *argument*<sub>2</sub>, ..., *argument*<sub>n</sub>)

**Predikátový symbol** zodpovedá prísudku

alebo celej prísudkovej časti:

(je) minister, (je) starší (ako), prijal, <, ...

**Jeho argumenty** zodpovedajú podmetu, predmetu, ...

Úloha argumentu je daná *pozíciou*

(ako v programovacích jazykoch).

- Predikátový symbol má jednoznačne určenú *aritu* —  
očakávaný počet argumentov
- Vždy musí mať práve toľko argumentov, aká je jeho arita

*Dohoda 3.1.* Aritu budeme niekedy písať ako horný index symbolu  
(minister<sup>1</sup>, starší<sup>2</sup>, prijal<sup>4</sup>, <<sup>2</sup>).

**Unárny** predikátový symbol (teda s aritou 1)

zvyčajne predstavuje *vlastnosť*

minister<sup>1</sup>(*arg*<sub>1</sub>)    *arg*<sub>1</sub> je minister  
myš\_domová<sup>1</sup>(*arg*<sub>1</sub>)    *arg*<sub>1</sub> je myš domová  
ľahká<sup>1</sup>(*arg*<sub>1</sub>)    *arg*<sub>1</sub> je ľahká

**Binárny, ternárny, ...** predikátový symbol (s aritou 2, 3, ...)

predstavuje *vzťah*

starší<sup>2</sup>(*arg*<sub>1</sub>, *arg*<sub>2</sub>)                      *arg*<sub>1</sub> je starší ako *arg*<sub>2</sub>  
medzi<sup>3</sup>(*arg*<sub>1</sub>, *arg*<sub>2</sub>, *arg*<sub>3</sub>)              *arg*<sub>1</sub> sa nachádza  
    medzi *arg*<sub>2</sub> a *arg*<sub>3</sub>  
prijal<sup>4</sup>(*arg*<sub>1</sub>, *arg*<sub>2</sub>, *arg*<sub>3</sub>, *arg*<sub>4</sub>)        *arg*<sub>1</sub> prijal *arg*<sub>2</sub>  
    od *arg*<sub>3</sub> v čase *arg*<sub>4</sub>



- Predikátový symbol predstavuje vlastnosť alebo vzťah, ktorého *pravdivosť* pre dané argumenty sa dá určiť *jednoznačne*
  - Napríklad pravdivosť vzťahu *byť vyšší ako* sa dá určiť jednoznačne.
  - Naopak pravdivosť vlastnosti *byť vysoký* sa *nedá* určiť jednoznačne.
    - \* Takýmito neostrými vlastnosťami sa zaoberajú *fuzzy* logiky.
- Často zanedbávame detaily — pomocné slovesá, predložky, skloňovanie, rod, ...:  
 $\text{starší}^2(\text{arg}_1, \text{arg}_2) - \text{arg}_1$  je starší/staršia/staršie ako  $\text{arg}_2$

- V prirodzenom jazyku *vlastné mená* označujú konkrétne, známe objekty alebo ľudí.
- V logike prvého rádu konkrétne, pevne dané objekty alebo hodnoty označujeme *symbolmi konštánt*.
  - Dorothy, Hlohovský, Jerry, 0, 1, 2, ..., rok2013
- Môžu byť *argumentmi predikátových symbolov* v atomických formulách
  - $\text{minister}(\text{Hlohovský})$ ,  $\text{starší}(\text{Dorothy}, \text{George})$ ,  
 $\text{prijal}(\text{Hlohovský}, \text{úplatok}250000\text{€}, \text{Veselič}, \text{rok}2013)$
- Samé o sebe *nie sú formulami*, nemajú pravdivostnú hodnotu.
- Dva symboly konštánt môžu označovať ten istý objekt:
  - $\text{stvrty\_prezident\_SR}$  a  $\text{Andrej\_Kiska}$
- *Rovnostné atómy* — špeciálny druh atomických formúl:  
 $\text{stvrty\_prezident\_SR} \doteq \text{Andrej\_Kiska}$

- V logike prvého rádu môžeme atomické formuly *spájať výrokovými spojkami* rovnako ako vo výrokovej logike:
  - $((\text{matka}(\text{Dorothy}) \wedge \text{syn}(\text{George})) \rightarrow \text{starší}(\text{Dorothy}, \text{George}))$
  - $(\text{zomrel}(\text{Stephen\_Hawking}) \rightarrow \neg(\text{najznámejší\_žijúci\_fyzik} \doteq \text{Stephen\_Hawking}))$
  - $(\text{prijal}(\text{Hlohovský}, \text{úplatok}250000\text{€}, \text{Veselič}, \text{rok}2013) \rightarrow \neg\text{dôveryhodný}(\text{Hlohovský}))$
- Máme ale aj zaujímavejšie možnosti...

- Atomické formuly nemusia vyjadrovať iba vlastnosti *konkrétnych* objektov označených konštantami
- Argumentami predikátových symbolov môžu byť aj *symboly individuových premenných* (skrátene *premenné*)

*Dohoda 3.2.* Ako premenné budeme zvyčajne používať malé písmená z konca abecedy  $u, v, w, x, y, z$  s prípadnými dolnými indexmi.

- Zastupujú objekty zo sveta, o ktorých chceme vysloviť nejakú vlastnosť alebo vzťah, ale nemôžeme ich označiť konštantami
- Atomické formuly s premennými nazývame *otvorené*
  - $\text{starší}(x, \text{Dorothy}), \text{minister}(z_5)$

Nepredstavujú plnohodnotné výroky, ale *výrokové formy*

- Premenné a formuly s nimi nadobúdajú význam pomocou *kvantifikátorov*

- *Všeobecný kvantifikátor*  $\forall$  predstavuje zámena „každý“, „všetci“, „pre všetky“, ...
- *Viaže* premennú, ktorá za ním nasleduje
- Vyjadruje, že vlastnosť, ktorú nasledujúca formula opisuje pre viazanú premennú, majú *všetky objekty*
  - $\forall x \text{ starší}(x, \text{Dorothy})$  – každý je starší ako Dorothy
- Kvantifikovaná formula nemusí byť atomická:
  - $\forall x (\text{starší}(x, \text{Dorothy}) \vee \neg \text{starší}(\text{George}, x))$

- *Existenčný kvantifikátor* *exists* predstavuje frázy „niekto“, „niečo“, „aspoň jedno“, „existuje/je ... také, že ...“, ...
- Vyjadruje, že vlastnosť, ktorú nasledujúca formula opisuje pre viazanú premennú, má *aspoň jeden objekt*
  - $\exists x \text{ starší}(x, \text{George})$  – niekto je starší ako George
- Kvantifikovaná formula nemusí byť atomická:
  - $\exists x (\text{starší}(x, \text{George}) \wedge \text{starší}(\text{Virginia}, x))$
- Kvantifikovaná formula môže obsahovať ďalšie kvantifikátory:
  - $\exists x \forall y \text{ starší}(x, y)$
  - $\forall x (\exists y \exists u \exists z (\text{prijal}(x, u, y, z) \wedge \text{úplatok}(u)) \rightarrow \neg \text{dôveryhodný}(x))$

**Definícia 3.3.** Symbolmi jazyka  $\mathcal{L}$  relačnej logiky prvého rádu sú:

*symboly (individuových) premenných* z nejakej nekonečnej spočítateľnej množiny  $\mathcal{V}_{\mathcal{L}}$  (označujeme ich  $x, y, \dots$ );

*mimologické symboly*, ktorými sú

*symboly konštánt* z nejakej spočítateľnej množiny  $C_{\mathcal{L}}$  (označované  $a, b, \dots$ );

*predikátové symboly* z nejakej spočít. množiny  $\mathcal{P}_{\mathcal{L}}$  (ozn.  $P, R, \dots$ );

*logické symboly*:

*logické spojky*: unárna  $\neg$ , binárne  $\wedge, \vee, \rightarrow$ ,

*symbol rovnosti*  $\doteq$ ,

*kvantifikátory*: existenčný kvantifikátor  $\exists$  a všeobecný kvantifikátor  $\forall$ ;

*pomocné symboly*  $(, )$  a  $,$  (ľavá, pravá zátvorka a čiarka).

Množiny  $\mathcal{V}_{\mathcal{L}}, C_{\mathcal{L}}, \mathcal{P}_{\mathcal{L}}$  sú vzájomne disjunktné.

Logické a pomocné symboly sa nevyskytujú v symboloch z  $\mathcal{V}_{\mathcal{L}}, C_{\mathcal{L}}, \mathcal{P}_{\mathcal{L}}$ .

Každému symbolu  $P \in \mathcal{P}_{\mathcal{L}}$  je priradená arita  $\text{ar}(P) \in \mathbb{N}^+$ .

*Poznámka 3.4.* Symboly (konštánt, funkčné, predikátové) môžu byť nealfabetické  $(1, <, +)$ , či tvorené viacerými znakmi (Virginia, dcéra).

**Definícia 3.5** (Term). Nech  $\mathcal{L}$  je jazyk relačnej logiky prvého rádu.

Symboly premenných z  $\mathcal{V}_{\mathcal{L}}$  a konštánt z  $C_{\mathcal{L}}$  súhrnne nazývame *termy*.

**Definícia 3.6** (Atomické formuly). Nech  $\mathcal{L}$  je jazyk relačnej logiky prvého rádu.

*Rovnostný atóm* jazyka  $\mathcal{L}$  je každá postupnosť symbolov  $t_1 \doteq t_2$ ,  
kde  $t_1$  a  $t_2$  sú termy.

*Predikátový atóm* jazyka  $\mathcal{L}$  je každá postupnosť symbolov  $P(t_1, \dots, t_n)$ , kde  
 $P$  je predikátový symbol s aritou  $n$  a  $t_1, \dots, t_n$  sú termy.

*Atomickými formulami* (skrátene *atómami*) jazyka  $\mathcal{L}$   
súhrnne nazývame všetky rovnostné a predikátové atómy jazyka  $\mathcal{L}$ .

Množinu všetkých atómov jazyka  $\mathcal{L}$  označujeme  $\mathcal{A}_{\mathcal{L}}$ .

## VII.35 Formuly jazyka relačnej logiky prvého rádu

**Definícia 3.7.** Množina  $\mathcal{E}_{\mathcal{L}}$  všetkých *formúl* jazyka relačnej logiky prvého  
rádu  $\mathcal{L}$

je *najmenšia* množina postupností symbolov jazyka  $\mathcal{L}$ , pre ktorú platí:

- Všetky atomické formuly z  $\mathcal{A}_{\mathcal{L}}$  sú formulami z  $\mathcal{E}_{\mathcal{L}}$  (teda  $\mathcal{A}_{\mathcal{L}} \subseteq \mathcal{E}_{\mathcal{L}}$ ).
- Ak  $A$  je formula z  $\mathcal{E}_{\mathcal{L}}$ , tak aj  $\neg A$  je formula z  $\mathcal{E}_{\mathcal{L}}$  (*negácia*  $A$ ).
- Ak  $A$  a  $B$  sú formuly z  $\mathcal{E}_{\mathcal{L}}$ , tak aj  $(A \wedge B)$ ,  $(A \vee B)$ ,  $(A \rightarrow B)$   
sú formuly z  $\mathcal{E}_{\mathcal{L}}$  (*konjunkcia*, *disjunkcia*, *implikácia*  $A$  a  $B$ ).
- Ak  $x$  je individuová premenná a  $A$  je formula z  $\mathcal{E}_{\mathcal{L}}$ ,  
tak aj  $\exists x A$  a  $\forall x A$  sú formuly z  $\mathcal{E}_{\mathcal{L}}$   
(*existenčná* a *všeobecná kvantifikácia* formuly  $A$  vzhľadom na  $x$ ).

*Dohoda 3.8.* Formuly označujeme písmenami  $A, B, C, \dots$  s prípadnými in-  
dexmi.

$(A \leftrightarrow B)$  je skratka postupnosti symbolov  $((A \rightarrow B) \wedge (B \rightarrow A))$ .

## 3.2. Formalizácia v logike prvého rádu

### 3.2.1. Jednoduchá formalizácia

## VII.36 Jednoduchá formalizácia

*Príklad 3.9* (podľa Genesereth and Kao [2013]). Sformalizujme v jazyku logiky prvého rádu túto situáciu:

V byte bývajú 4 spolubývajúce: Aďa, Biba, Ciri a Dada. Niektoré sa kamarátia a niektoré sa nemajú rady, ale máme o tom iba tieto nepriame informácie:

1. Biba má rada Ciri alebo Dadu.
2. Aďa má rada všetkých, ktorých má rada Biba.
3. Ciri má rada každého, kto má rád ju.
4. Biba má rada niekoho, kto ju má rád.
5. Žiadna nemá rada seba samú.
6. Každá má rada niekoho.
7. Niekoho majú rady všetky.

### 3.2.2. Základné idiómy

#### VII.37 Základné idiómy: Obmedzená kvantifikácia

Niektoré slovné obraty a ich prvorádové formalizácie sú veľmi bežné, ale pre začiatočníka nie úplne priamočiare:

**Obmedzená kvantifikácia** je všeobecné alebo existenčné tvrdenie, ktoré sa vzťahuje iba na objekty s nejakou vlastnosťou:

- „Každý, kto má vlastnosť  $P$ , má vlastnosť  $Q$ .“ / „Každý  $P$  je  $Q$ .“:
  - $\forall x(P(x) \rightarrow Q(x))$
- „Nieкто, kto má vlastnosť  $P$ , má vlastnosť  $Q$ .“ / „Niektorý  $P$  je  $Q$ .“:
  - $\exists x(P(x) \wedge Q(x))$

**Neexistencia** je negované existenčné tvrdenie,  
v slovenčine sa často vyjadruje *dvojitým záporom*  
[negatívne zámeno (nikto/nič) a negatívne tvrdenie]:

**Jednoduchá vlastnosť** „Nikto nie je dokonalý“:

- S dôrazom na zámeno:  $\neg \exists x \text{ dokonalý}(x)$
- S dôrazom na negatívne tvrdenie:  $\forall x \neg \text{dokonalý}(x)$

**Viacero vlastností** „Žiaden/nijaký vegán nie je obézny“:

- S dôrazom na zámeno:
  - $\neg \exists x (\text{vegán}(x) \wedge \text{obézny}(x))$
- S dôrazom na negatívne tvrdenie:
  - $\forall x \neg (\text{vegán}(x) \wedge \text{obézny}(x))$
  - $\forall x (\neg \text{vegán}(x) \vee \neg \text{obézny}(x))$
  - $\forall x (\text{vegán}(x) \rightarrow \neg \text{obézny}(x))$

### Zamlčaná existencia

- každý vegán si kúpil tekvicu:
  - $\forall x (\text{vegán}(x) \rightarrow \exists y (\text{kúpil}(x, y) \wedge \text{tekvica}(y)))$
- žiadny vegán si nekúpil syr:
  - $\neg \exists x (\text{vegán}(x) \wedge \exists y (\text{kúpil}(x, y) \wedge \text{syr}(y)))$
  - $\forall x (\text{vegán}(x) \rightarrow \neg \exists y (\text{kúpil}(x, y) \wedge \text{syr}(y)))$
  - $\forall x (\text{vegán}(x) \rightarrow \forall y (\neg \text{kúpil}(x, y) \vee \neg \text{syr}(y)))$
  - $\forall x (\text{vegán}(x) \rightarrow \forall y (\text{kúpil}(x, y) \rightarrow \neg \text{syr}(y)))$

### Existencia v antecedente s odkazom v konzekvente

- ak je *niekto* vegán, tak *on* nie je obézny:
  - $\forall x (\text{vegán}(x) \rightarrow \neg \text{obézny}(x))$

### 3.2.3. Nutné a postačujúce podmienky

#### VII.40 Nutné a postačujúce podmienky

---

- Často sa vyskytujú tvrdenia typu:
  1. Vegán je každý, kto si kúpil karfiol.
  2. Vegán je iba ten, kto si kúpil tekvicu.
- Hlavná veta („Vegán je ...“) vyjadruje nejakú *vlastnosť*
- Vedľajšia veta („kto si ...“) vyjadruje *podmienku*, ktorá súvisí s touto vlastnosťou
- Aký je rozdiel medzi týmito podmienkami?

#### VII.41 Postačujúca podmienka

---

Prvé tvrdenie „Vegán je každý, kto si kúpil karfiol.“

- Hovorí, že na to, aby niekto bol vegánom, *stačí*, aby platila podmienka, že si kúpil karfiol
- Kúpenie si karfiolu je teda *postačujúcou* podmienkou vegánstva
- Ekvivalentne:  
„Pre každého platí, že je vegán, ak si kúpil karfiol.“  
„Pre každého platí, že ak si kúpil karfiol, tak je vegán.“
- Formalizácia je teda  $\forall x (\exists y (\text{kúpil}(x, y) \wedge \text{karfiol}(y)) \rightarrow \text{vegán}(x))$

#### VII.42 Nutná podmienka

---

Druhé tvrdenie „Vegán je iba ten, kto si kúpil tekvicu.“

- Hovorí, že na to, aby niekto bol vegánom, *nevyhnutne* preňho platí podmienka, že si kúpil tekvicu (keby si ju nekúpil, nebol by vegánom)
- Kúpenie si tekvice je teda *nutnou* podmienkou vegánstva



- Ekvivalentne:  
 „Pre každého platí, že je vegán, *iba* ak si kúpil tekvicu.“  
 „Pre každého platí, že ak si *nekúpil* tekvicu, tak *nie* je vegán.“  
 „Pre každého platí, že ak je vegán, tak si kúpil tekvicu.“
- Formalizácia je teda  $\forall x(\text{vegán}(x) \rightarrow \exists y(\text{kúpil}(x, y) \wedge \text{syr}(y)))$

### 3.2.4. Idiómy s rovnosťou

#### VII.43 Idiómy s rovnosťou: Enumerácia

---

##### Vymenovanie objektov s vlastnosťou

- V byte č. 14 bývajú Aďa, Biba, Ciri, Dada.
  - $(\text{býva}_v(\text{Aďa}, \text{byt14}) \wedge \dots \wedge \text{býva}_v(\text{Dada}, \text{byt14}))$

Ekvivalentne:

Každá z Aďa, Biba, Ciri, Dada býva v byte č. 14.

- $\forall x((x \doteq \text{Aďa} \vee \dots \vee x \doteq \text{Dada}) \rightarrow \text{býva}_v(x, \text{byt14}))$
- V byte č. 14 bývajú *iba* Aďa, Biba, Ciri, Dada.  
 Každý, kto býva v byte č. 14, je jedna z Aďa, Biba, Ciri, Dada.
  - $\forall x(\text{býva}_v(x, \text{byt14}) \rightarrow (x \doteq \text{Aďa} \vee \dots \vee x \doteq \text{Dada}))$

#### VII.44 Idiómy s rovnosťou: Obmedzenia počtu

---

##### Aspoň $k$ :

- Jaro si kúpil aspoň dve tekvice.
- Existujú dve *navzájom rôzne* tekvice, ktoré si Jaro kúpil.
  - $\exists t_1 \exists t_2 (\neg t_1 \doteq t_2 \wedge \text{tekvica}(t_1) \wedge \text{tekvica}(t_2) \wedge \text{kúpil}(\text{Jaro}, t_1) \wedge \text{kúpil}(\text{Jaro}, t_2))$

##### Najviac jeden:

- Anka si kúpila najviac jednu tekvicu.
- Ekvivalentne: Anka si *nekúpila* aspoň dve tekvice.

- $\neg \exists t_1 \exists t_2 (\neg t_1 \doteq t_2 \wedge \text{tekvica}(t_1) \wedge \text{tekvica}(t_2) \wedge \text{kúpil}(\text{Anka}, t_1) \wedge \text{kúpil}(\text{Anka}, t_2))$
- $\forall t_1 \forall t_2 \neg (\neg t_1 \doteq t_2 \wedge \text{tekvica}(t_1) \wedge \text{tekvica}(t_2) \wedge \text{kúpil}(\text{Anka}, t_1) \wedge \text{kúpil}(\text{Anka}, t_2))$
- $\forall t_1 \forall t_2 (t_1 \doteq t_2 \vee \neg \text{tekvica}(t_1) \vee \neg \text{tekvica}(t_2) \vee \neg \text{kúpil}(\text{Anka}, t_1) \vee \neg \text{kúpil}(\text{Anka}, t_2))$
- $\forall t_1 \forall t_2 ((\text{tekvica}(t_1) \wedge \text{tekvica}(t_2) \wedge \text{kúpil}(\text{Anka}, t_1) \wedge \text{kúpil}(\text{Anka}, t_2)) \rightarrow t_1 \doteq t_2)$
- Teda ekvivalentne: Všetky tekvice, ktoré si Anka kúpila, sú rovnaké.

## VIII. prednáška

# Definície predikátov. Sémantika relačnej logiky prvého rádu

16. apríla 2018

### VIII.1 Formuly jazyka relačnej logiky prvého rádu

#### Otestujte sa VIII.1

Ktoré z nasledujúcich postupností symbolov sú formulami relačnej logiky prvého rádu, ak vhodne zvolíme jazyk?

- a)  $\forall x \text{ človek}(x) \wedge \text{žena}(\text{Eva})$
- b)  $\text{chytá}(\text{mačka}(\text{Muro}), \text{myš}(y))$
- c)  $(\neg \text{prší} \vee \exists x (\text{zmoknutý}(x)))$
- d)  $(\forall x \neg x \doteq \text{Eva} \rightarrow \neg \exists x x \doteq x)$

Ak postupnosť nie je formulou, ako sa dá správne vyjadriť pravdepodobne zamýšľaný význam?

*Riešenie.* a) **Nie** je formulou, chýbajú vonkajšie zátvorku. Formulou by bola  $(\forall x \text{ človek}(x) \wedge \text{žena}(\text{Eva}))$ . V jazyku, v ktorom  $\text{Eva} \in C_{\mathcal{L}}$  a  $\{\text{človek}^1, \text{žena}^1\} \subseteq \mathcal{P}_{\mathcal{L}}$ .

- b) **Nie** je formula, význam pravdepodobne správne vyjadruje formula:  $(\text{mačka}((\text{Muro}) \wedge \text{myš}(y)) \wedge \text{chytá}(\text{Muro}, y))$ .
- c) **Nie** je formula — ak by prší bol predikát, musel by mať argument; prší nemôže byť individuová konštanta, pretože tie nie sú formulami. Navyše priama podformula kvantifikácie je atomická, ktorá sa nezátvorkuje. Význam pravdepodobne správne vyjadruje formula:  $(\neg \text{prší}(\text{počasie}) \vee \exists x \text{zmoknutý}(x))$

- d) Je formulou v jazyku, v ktorom  $Eva \in C_{\mathcal{L}}$ . (Ak vás to prekvapuje, uveďte si, že priama podformula negácie a kvantifikácií sa nezátvorkuje. Samotný rovnostný atóm tiež nie je v zátvorkách.)

### 3.2.5. Definície predikátov

#### VIII.2 Pojmy

---

- V mnohých doménach sú zaujímavé komplikovanejšie kombinácie vlastností alebo vzťahov:
  - $x$  má spoločného rodiča s  $y$ :  

$$\exists z(\text{rodič}(z, x) \wedge \text{rodič}(z, y))$$
  - $x$  je živočích, ktorý konzumuje iba rastliny:  

$$(\text{živočích}(x) \wedge \forall y(\text{konzumuje}(x, y) \rightarrow \text{rastlina}(y)))$$
- Často sa vyskytujúce kombinácie vzťahov a vlastností je výhodné:
  - *pomenovať*
  - a jasne vyjadriť význam nového mena pomocou doteraz známych vlastností a vzťahov, teda *zadefinovať pojem*

#### VIII.3 Definície pojmov

---

**Definícia 3.10** (neformálna). *Definícia* je tvrdenie, ktoré vyjadruje význam pojmu.

*Explicitná definícia* (najčastejší druh definície) je ekvivalencia medzi pojmom a opisom jeho významu, v ktorom sa definovaný pojem sám nevyskytuje.

**Príklad 3.11.** •  $x$  je súrodencom  $y$  práve vtedy, keď  $x$  má spoločného rodiča s  $y$   

$$\forall x \forall y (\text{súrodenec}(x, y) \leftrightarrow \exists z(\text{rodič}(z, x) \wedge \text{rodič}(z, y)))$$

- $x$  je *bylinožravec* vtedy a len vtedy,  
keď  $x$  je živočích, ktorý konzumuje iba rastliny  

$$\forall x(\text{bylinožravec}(x) \leftrightarrow (\text{živočích}(x) \wedge \forall y(\text{konzumuje}(x, y) \rightarrow \text{rastlina}(y))))$$

#### VIII.4 Explicitná def. a nutná a postačujúca podmienka

Poznámka 3.12. Všimnite si:

- Definícia pojmu *súrodeneč* vyjadruje *nutnú aj postačujúcu* podmienku toho, aby medzi dvoma ľuďmi existoval súrodenecký vzťah
- Definícia pojmu *bylinožravec* vyjadruje *nutnú aj postačujúcu* podmienku toho, aby niečo bolo bylinožravcom

#### VIII.5 Použitie pojmov

Využitím definovaného pojmu

- skracujeme tvrdenia:
  - králiky sú bylinožravce:  

$$\forall x(\text{králik}(x) \rightarrow \text{bylinožravec}(x))$$
- jednoduchšie definujeme ďalšie pojmy:
  - $x$  je *sestrou*  $y$  práve vtedy, keď  $x$  je žena, ktorá je súrodencom  $y$ :  

$$\forall x \forall y (\text{sestra}(x, y) \leftrightarrow (\text{žena}(x) \wedge \text{súrodeneč}(x, y)))$$

#### Vyskúšajte si VIII.2

Zadefinujte pojem *teta* (chápaný ako vzťah dvoch ľudí) neformálne (v slovenčine) aj formálne (formulou logiky prvého rádu).

*Riešenie.* Osoba  $x$  je *tetou*  $y$  vtedy a len vtedy, keď  $x$  je sestrou rodiča  $y$ .

$$\forall x \forall y (\text{teta}(x, y) \leftrightarrow \exists z (\text{sestra}(x, z) \wedge \text{rodič}(z, y)))$$

### 3.3. Sémantika relačnej logiky prvého rádu

#### VIII.6 Význam atomických formúl — výroková logika

---

Významom atomických formúl je pravdivostná hodnota

Vo výrokovej logike:

- Atomické formuly sú výrokové premenné — nemajú žiadnu štruktúru

starší\_Howard\_Virginia, otec\_George

- Význam im priamo priraduje ohodnotenie

$$v = \{\text{starší\_Howard\_Virginia} \mapsto f, \text{otec\_George} \mapsto t\}$$

- Rôzne ohodnotenia — rôzne stavy sveta

#### VIII.7 Význam atomických formúl — logika prvého rádu

---

Významom atomických formúl je pravdivostná hodnota

Logika prvého rádu:

- Atomické formuly majú štruktúru:  
predikátový symbol/rovnosť a jeho argumenty (termy)

minister(Hlohovský), starší(Dorothy,  $x$ ),  $x \doteq$  George,  
prijal(Hlohovský,  $u$ , Veselič, rok2013)

- Termy (symboly konštánt a *individuových* premenných)

Dorothy, George, Hlohovský, úplatok250000€, ...  $u$ ,  $x$ ,  
...

označujú objekty

- Predikátové symboly

minister<sup>1</sup>, starší<sup>1</sup>, prijal<sup>4</sup>

označujú vlastnosti alebo vzťahy objektov

- ❓ Aký matematický objekt predstavuje *vlastnosť* objektov?
- Množina, napríklad pre vlastnosť byť ministrom môžeme vytvoriť množinu všetkých objektov s touto vlastnosťou:  
 $\{ \text{👤Pšenová}, \text{👤Hlohovský}, \text{👤Zubáková}, \text{👤Žinčica}, \dots \}$
- ❓ Aký matematický objekt predstavuje *vzťah* niekoľkých objektov?
- Usporiadaná  $n$ -tica:  $(\text{👤Dorothy}, \text{👤George})$
- ❓ Aký matematický objekt predstavuje *mnoho vzťahov rovnakého druhu*?
- Množina usporiadaných  $n$ -tíc, napríklad pre vzťah byť starší  
 $\{ (\text{👤Dorothy}, \text{👤Virginia}), (\text{👤Howard}, \text{👤Virginia}), (\text{👤Dorothy}, \text{👤Howard}), (\text{👤Dorothy}, \text{👤George}), (\text{👤George}, \text{👤Virginia}) \}$
- ❓ Odkiaľ vyberáme objekty do týchto množín?
- Z množiny objektov existujúcich v časti sveta, ktorá nás zaujíma

## VIII.9 Význam mimologických symbolov

Aby sme dali význam symbolom nejakého jazyka  $\mathcal{L}$  logiky prvého rádu:

- Vyberieme *doménu*  $M$  — množinu objektov v časti sveta, ktorá nás zaujíma  

$$M = \{ \text{👤Pšenová}, \text{👤Hlohovský}, \text{👤Zubáková}, \text{👤Žinčica}, \dots, \text{👤Veselič}, \text{👤Petržlen}, \dots, \text{📅}_{50000}, \text{📅}_{250000}, \dots, \text{🚗}_{\text{HD}}, \dots, \text{📅}_{2012}, \text{📅}_{2013}, \dots \}$$
- Interpretujeme mimologické symboly v tejto doméne:  
**Symbole konštant** interpretujeme ako *objekty z domény*  

$$i(\text{Hlohovský}) = \text{👤Hlohovský}, \quad i(\text{rok2013}) = \text{📅}_{2013},$$

$$i(\text{minister\_vnútra}) = \text{👤Hlohovský}, \quad \dots$$

**Predikátové symboly** interpretujeme ako množiny prvkov domény

$$i(\text{minister}) = \{\text{Pšenová}, \text{Hlohovský}, \text{Zubáková}, \text{Žinčica}, \dots\}$$

alebo ich  $n$ -tíc

$$i(\text{prijal}) = \{(\text{Hlohovský}, 250000, \text{Veselič}, 2013), \\ (\text{Zubáková}, \text{HD}, \text{Petržlen}, 2012), \dots\}$$

v závislosti od arity symbolu

Dvojicu  $(M, i)$  nazveme *štruktúra* pre jazyk  $\mathcal{L}$

## VIII.10 Štruktúra

**Definícia 3.13.** Nech  $\mathcal{L}$  je jazyk relačnej logiky prvého rádu.

*Štruktúrou* pre jazyk  $\mathcal{L}$  nazývame dvojicu  $\mathcal{M} = (M, i)$ , kde

$M$  je neprázdna množina, *doména* štruktúry  $\mathcal{M}$ ;

$i$  je zobrazenie, *interpretačná funkcia* štruktúry  $\mathcal{M}$ , ktoré

- každému symbolu konštanty  $c$  jazyka  $\mathcal{L}$  priraduje prvok  $i(c) \in M$ ;
- každému predikátovému symbolu  $P$  jazyka  $\mathcal{L}$  s aritou  $n$  priraduje množinu  $i(P) \subseteq M^n$ .

*Dohoda 3.14.* Štruktúry označujeme veľkými písanými písmenami  $\mathcal{M}, \mathcal{N}, \dots$

Doménu označujeme rovnakým, ale tlačeným písmenom ako štruktúru.

## VIII.11 Štruktúry

- Štruktúr pre daný jazyk je nekonečne veľa
- Doména môže mať ľubovoľné prvky, môže byť nekonečná
- Interpretácia symbolov vôbec nemusí zodpovedať intuícii
- Štruktúra nedefinuje význam jednej zložky atomických forém – individuových premenných



**Definícia 3.15.** Nech  $\mathcal{M} = (M, i)$  je štruktúra pre jazyk  $\mathcal{L}$ .

Ohodnotenie (individuových) premenných je ľubovoľná funkcia  $e: \mathcal{V}_{\mathcal{L}} \rightarrow M$  (priraduje premenným prvky domény).

Zápisom  $e(x/v)$  označíme ohodnotenie individuových premenných, ktoré priraduje premennej  $x$  hodnotu  $v$  z domény  $M$

a všetkým ostatným premenným rovnakú hodnotu ako im priraduje  $e$ .

Majme  $\mathcal{V}_{\mathcal{L}} = \{x, y\}$  a doménu

$$M = \{\text{Andrea K.}, \text{Bibiána V.}, \text{Alena H.}, \text{Daniela L.}, \text{Edo S.}, \text{Fero Z.}\}$$

Ohodnotením (individuových) premenných je napríklad

$$e = \{x \mapsto \text{Bibiána V.}, y \mapsto \text{Daniela L.}\}$$

Potom

$$e(y/\text{Edo S.}) = \{x \mapsto \text{Bibiána V.}, y \mapsto \text{Edo S.}\}$$

**Definícia 3.16.** Nech  $\mathcal{M} = (M, i)$  je štruktúra,  $e$  je ohodnotenie premenných.

Hodnotou termu  $t$  v štruktúre  $\mathcal{M}$  pri ohodnotení premenných  $e$  je prvok  $t^{\mathcal{M}}[e]$  z  $M$  určený nasledovne:

- $t^{\mathcal{M}}[e] = e(x)$ , ak  $t$  je premenná  $x \in \mathcal{V}_{\mathcal{L}}$ ,
- $t^{\mathcal{M}}[e] = i(a)$ , ak  $t$  je konštanta  $a \in C_{\mathcal{L}}$ .

Konečne môžeme určiť význam atomickej formuly

- Zoberieme štruktúru  $\mathcal{M} = (M, i)$

$$M = \{ \text{♂Andrea K.}, \text{♂Bibiána V.}, \text{♂Alena H.}, \text{♂Daniela L.}, \text{♂Edo S.}, \text{♂Fero Z.} \}$$

$$i(\text{Ada}) = \text{♂Andrea K.}, \quad i(\text{Biba}) = \text{♂Bibiána V.},$$

$$i(\text{Ciri}) = \text{♂Alena G.}, \quad i(\text{Dada}) = \text{♂Daniela L.}$$

$$i(\text{má\_rada}) = \{ (\text{♂Andrea K.}, \text{♂Daniela L.}), (\text{♂Bibiána V.}, \text{♂Andrea K.}), \\ (\text{♂Bibiána V.}, \text{♂Edo S.}), (\text{♂Edo S.}, \text{♂Bibiána V.}) \}$$

a ohodnotenie premenných  $e = \{x \mapsto \text{♂Fero Z.}\}$

- Pre formulu  $\text{má\_rada}(\text{Biba}, x)$

1. vyhodnotíme termy vo formule:

$$\text{Biba}^{\mathcal{M}}[e] = i(\text{Biba}) = \text{♂Bibiána V.}, \quad x^{\mathcal{M}}[e] = e(x) = \text{♂Fero Z.}$$

2. zistíme, či  $(\text{♂Bibiána V.}, \text{♂Fero Z.}) \in i(\text{má\_rada})$  –  
v tomto prípade nie

- Takže štruktúra  $\mathcal{M}$  nespĺňa formulu  $\text{má\_rada}(\text{Biba}, x)$  pri ohodnotení  $e$

- Vyhodnotenie splnenia formuly s *výrokovými spojkami* v štruktúre pri ohodnotení si vieme ľahko predstaviť
- Ako vyhodnotíme splnenie formuly s *kvantifikátormi*?
- $\exists x \text{ má\_rada}(\text{Biba}, x)$ 
  1. Vyskúšame všetky ohodnotenia, ktoré postupne priradujú kvantifikovanej premennej jednotlivé prvky domény:

$m$	$\mathcal{M} \models \text{má\_rada}(\text{Biba}, x) [e(x/m)]$
Andrea K.	áno
Bibiána V.	nie
Alena H.	nie
Daniela L.	nie
Edo S.	áno
Fero Z.	nie

2.  $\mathcal{M} \models \exists x \text{ má\_rada}(\text{Biba}, x) [e]$  vtt **v aspoň jednom prípade**, teda pre aspoň jedno  $m \in M$ ,  $\mathcal{M} \models \text{má\_rada}(\text{Biba}, x) [e(x/m)]$

#### VIII.16 Splnenie všeobecne kvantifikovanej formuly

- Nech  $e = \{x \mapsto \text{Andrea K.}, y \mapsto \text{Daniela V.}\}$
- $\forall x \neg \text{má\_rada}(y, x)$

1. Vyskúšame všetky ohodnotenia, ktoré postupne priradujú kvantifikovanej premennej jednotlivé prvky domény:

$m$	$\mathcal{M} \models \neg \text{má\_rada}(y, x) [e(x/m)]$	$\mathcal{M} \models \text{má\_rada}(y, x) [e(x/m)]$
Andrea K.	áno	nie
Bibiána V.	áno	nie
Alena H.	áno	nie
Daniela L.	áno	nie
Edo S.	áno	nie
Fero Z.	áno	nie

2.  $\mathcal{M} \models \forall x \neg \text{má\_rada}(y, x) [e]$  vtt **vo všetkých prípadoch**, teda pre všetky  $m \in M$ ,  $\mathcal{M} \models \neg \text{má\_rada}(y, x) [e(x/m)]$

💡 Na pôvodnej hodnote  $e(x)$  nezáleží ani pri jednom kvantifikátore

#### VIII.17 Splnenie formuly v štruktúre

**Definícia 3.17.** Nech  $\mathcal{M} = (M, i)$  je štruktúra,  $e$  je ohodnotenie premenných.

Relácia štruktúra  $\mathcal{M}$  spĺňa formulu  $A$  pri ohodnotení  $e$  (skrátene  $\mathcal{M} \models A[e]$ ) má nasledovnú indukčnú definíciu:

- $\mathcal{M} \models t_1 \doteq t_2[e]$  vtt  $t_1^{\mathcal{M}}[e] = t_2^{\mathcal{M}}[e]$ ,
- $\mathcal{M} \models P(t_1, \dots, t_n)[e]$  vtt  $(t_1^{\mathcal{M}}[e], \dots, t_n^{\mathcal{M}}[e]) \in i(P)$ ,
- $\mathcal{M} \models \neg A[e]$  vtt  $\mathcal{M} \not\models A[e]$ ,
- $\mathcal{M} \models (A \wedge B)[e]$  vtt  $\mathcal{M} \models A[e]$  a zároveň  $\mathcal{M} \models B[e]$ ,
- $\mathcal{M} \models (A \vee B)[e]$  vtt  $\mathcal{M} \models A[e]$  alebo  $\mathcal{M} \models B[e]$ ,
- $\mathcal{M} \models (A \rightarrow B)[e]$  vtt  $\mathcal{M} \not\models A[e]$  alebo  $\mathcal{M} \models B[e]$ ,
- $\mathcal{M} \models \exists x A[e]$  vtt pre *nejaký* prvok  $m \in M$  máme  $\mathcal{M} \models A[e(x/m)]$ ,
- $\mathcal{M} \models \forall x A[e]$  vtt pre *každý* prvok  $m \in M$  máme  $\mathcal{M} \models A[e(x/m)]$ ,

pre všetky arity  $n > 0$ , všetky predikátové symboly  $P$  s aritou  $n$ , všetky termy  $t_1, t_2, \dots, t_n$ , všetky premenné  $x$  a všetky formuly  $A, B$ .

#### VIII.18 Splnenie množiny formúl

**Definícia 3.18.** Nech  $S$  je množina formúl jazyka  $\mathcal{L}$ , nech  $\mathcal{M}$  je štruktúra pre  $\mathcal{L}$ ,

nech  $e$  je ohodnotenie výrokových premenných.

Štruktúra  $\mathcal{M}$  spĺňa množinu  $S$  pri ohodnotení  $e$  (skrátene  $\mathcal{M} \models S[e]$ ) vtt pre všetky formuly  $X$  z  $S$  platí  $\mathcal{M} \models X[e]$ .

**Príklad 3.19.** Nájdime štruktúru a ohodnotenie, ktoré spĺňajú množinu  $S_{\text{spolubývajúce}} = \{A_1, \dots, A_6\}$  prvých 6 formúl o spolubývajúcich:

$$\begin{aligned} A_1 &= (\text{má\_rada}(\text{Biba}, \text{Ciri}) \vee \text{má\_rada}(\text{Biba}, \text{Dada})), \\ A_2 &= \forall x (\text{má\_rada}(\text{Biba}, x) \rightarrow \text{má\_rada}(\text{Ada}, x)), \\ A_3 &= \forall x (\text{má\_rada}(x, \text{Ciri}) \rightarrow \text{má\_rada}(\text{Ciri}, x)), \\ A_4 &= \exists x (\text{má\_rada}(x, \text{Biba}) \wedge \text{má\_rada}(\text{Biba}, x)), \\ A_5 &= \forall x \neg \text{má\_rada}(x, x), \quad A_6 = \forall x \exists y \text{má\_rada}(x, y) \end{aligned}$$

**Definícia 3.20.** Nech  $X$  je formula jazyka  $\mathcal{L}$  a nech  $S$  je množina formúl jazyka  $\mathcal{L}$ .

**Formula  $X$  je splniteľná** vtt aspoň jedna štruktúra  $\mathcal{M}$  pre  $\mathcal{L}$  spĺňa  $X$  pri aspoň jednom ohodnotení  $e$ .

**Množina formúl  $S$  je splniteľná** vtt aspoň jedna štruktúra  $\mathcal{M}$  pre  $\mathcal{L}$  spĺňa  $S$  pri aspoň jednom ohodnotení  $e$ .

**Formula  $X$  (množina formúl  $S$ ) je nesplniteľná** vtt nie je splniteľná.

*Príklad 3.21.* Dokážme, že množina všetkých 7 formúl o spolubývajúcich, teda  $S_{\text{spolubývajúce}} \cup \{\exists x \forall y \text{ má\_rada}(y, x)\}$ , je nesplniteľná.

**Definícia 3.22.** Nech  $X$  je formula v jazyku  $\mathcal{L}$ .

Formula  $X$  je *platná* (skrátene  $\models X$ ) vtt každá štruktúra  $\mathcal{M}$  pre  $\mathcal{L}$  spĺňa  $X$  pri každom ohodnotení  $e$ .

Platné formuly sú prvorádovou obdobou tautológií. Keď rovnaké atomické alebo kvantifikované podformuly nahradíme rovnakými výrokovými premenými), tak

- formula, z ktorej vznikne tautológia, je platná; ale
- *nie z každej platnej formuly vznikne tautológia.*

**Definícia 3.23.** Nech  $X$  je formula v jazyku  $\mathcal{L}$ , nech  $S$  je množina formúl v jazyku  $\mathcal{L}$ .

Formula  $X$  (*prvorádovo*) *vyplýva* z  $S$  (skrátene  $S \models X$ ) vtt pre každú štruktúru  $\mathcal{M}$  pre  $\mathcal{L}$  a každé ohodnotenie  $e$  platí, že ak  $\mathcal{M}$  spĺňa  $S$  pri  $e$ , tak  $\mathcal{M}$  spĺňa  $X$  pri  $e$ .

**Tvrdenie 3.24.** *Nech  $X$  je formula v jazyku  $\mathcal{L}$ .*

*Potom  $X$  je platná ( $\models X$ ) vtt*

*$X$  prvorádovo vyplýva z prázdnej množiny formúl ( $\{\} \models X$ ).*

**Tvrdenie 3.25.** *Nech  $X$  je formula a  $S$  je množina formúl v spoločnom jazyku  $\mathcal{L}$ .*

*Potom z  $S$  vyplýva  $X$  vtt  $S \cup \{\neg X\}$  je nespĺniteľná.*

**Cvičenie 3.26.** Dokážte (priamo či sporom) alebo vyvráťte (nájdením kontrapríkladu) nasledujúce tvrdenia:

- Nech  $T$  je ľubovoľná výroková teória,  
nech  $X$  a  $Y$  sú ľubovoľné výrokové formuly.  
Ak  $T \models (X \rightarrow Y)$ , tak  $T \models X$  alebo  $T \models Y$ .
- Nech  $T$  je ľubovoľná výroková teória,  
nech  $X$  a  $Y$  sú ľubovoľné výrokové formuly.  
Ak  $T \models X$  alebo  $T \models Y$ , tak  $T \models (X \rightarrow Y)$ .

**Riešenie.** a) Tvrdenie platí. Najjednoduchšie je dokázať ho sporom: Predpokladajme, že  $T \models (X \rightarrow Y)$  a zároveň  $T \models X$  a  $T \not\models Y$ . Z posledného predpokladu máme nejaké ohodnotenie  $v$  také, že  $v \models T$  a  $(*)$   $v \not\models Y$ . Keďže ale  $v \models T$ , z prvého predpokladu máme  $v \models (X \rightarrow Y)$ , teda  $v \models X$  alebo  $v \models Y$ . Druhá možnosť nenastáva podľa  $(*)$ . Takže  $v \models X$ , ale to je v spore s druhým predpokladom.

Priamy dôkaz je problematickejší, vyžaduje nie celkom zvyčajné zovšeobecnenie po rozbere prípadov.

b) Tvrdenie neplatí. Háčik je v tom, že  $T \models (X \rightarrow Y)$  musí podľa tvrdenia platiť aj keď iba  $T \models X$ , aj keď iba  $T \models Y$ . Práve v prvom prípade je problém.

Už pre  $T = \{\}$  môžeme zobrať  $X = p$  a  $Y = q$ . Ohodnotenie  $v = \{p \mapsto f, q \mapsto f\}$  spĺňa teóriu  $T$  a nespĺňa  $X$ , takže antecedent tvrdenia je pravdivý. Súčasne ale vieme nájsť ohodnotenie  $v = \{p \mapsto t, q \mapsto f\}$  ktoré spĺňa teóriu  $T$  a nespĺňa  $(X \rightarrow Y)$ . Tieto  $T, X, Y$  sú teda kontrapríkladom platnosti tvrdenia.

## Literatúra

- Martin Davis and Hillary Putnam. A computing procedure for quantification theory. *J. Assoc. Comput. Mach.*, 7:201–215, 1960.
- Martin Davis, George Logemann, and Donald Loveland. A machine program for theorem-proving. *Communications of the ACM*, 5(7):394–397, 1962.
- Michael Genesereth and Eric Kao. *Introduction to Logic*. Morgan & Claypool, 2013. ISBN 9781627052481.
- 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>.