

Prednášky z Matematiky (4) — Logiky pre informatikov

Ján Kľuka, Jozef Šiška

Letný semester 2018/2019

Obsah

I. O logike a tomto kurze	
Syntax výrokovej logiky	4
1. Úvod	4
1.1. O logike	4
1.2. O kurze	12
2. Výroková logika	13
2.1. Opakovanie: Výroková logika v prirodzenom jazyku	13
2.2. Syntax	14
II. Sémantika výrokovej logiky	20
2.3. Sémantika	26
2.4. Tautológia, (ne)splniteľnosť, falzifikovateľnosť	31
III. Vyplyvanie a ekvivalencia	37
2.5. Vyplyvanie	38

2.6. Ekvivalencia	42
2.6.1. Ekvivalentné úpravy	44
2.6.2. Konjunktívna a disjunktívna normálna forma	48
IV. CNF	
Hilbertovský kalkul	50
2.7. Logické kalkuly	55
2.8. Hilbertovský kalkul	57
V. Tablový kalkul a jeho korektnosť	62
2.9. Tablový kalkul	63
2.9.1. Korektnosť	71
VI. Korektnosť a úplnosť tablového kalkulu	72
2.9.2. Tablový dôkaz splniteľnosti	74
VII. Úplnosť tabiel	
Korektné pravidlá	
Výroková rezolvenca	77
2.9.3. Hintikkova lema	77
2.9.4. Úplnosť	78
2.9.5. Nové korektné pravidlá	79
2.10. Výroková rezolvenca	81
VIII. SAT solver a algoritmus DPLL	
Syntax relačnej logiky prvého rádu	85
2.11. Problém výrokovologickej splniteľnosti (SAT)	85
2.11.1. Naivný backtracking	86
2.11.2. Optimalizácia backtrackingu	88
2.11.3. DPLL	92

3. Logika prvého rádu	94
3.1. Syntax relačnej logiky prvého rádu	94
3.2. Formalizácia	101
3.2.1. Jednoduchá formalizácia	101
3.2.2. Základné idiómy	102
3.2.3. Nutné a postačujúce podmienky	103
3.2.4. Idiómy s rovnosťou	105
 IX. Definície predikátov.	
Sémantika relačnej logiky prvého rádu	107
3.2.5. Definície predikátov	109
3.3. Sémantika	111

I. prednáška

O logike a tomto kurze

Syntax výrokovkej logiky

18. februára 2019

1. Úvod

1.1. O logike

I.1 Čo je logika

- Logika je vedná disciplína, ktorá študuje formy usudzovania
 - filozofická, matematická, informatická, výpočtová
- Tri dôležité predmety záujmu:
 - Jazyk** zápis pozorovaní, definície pojmov, formulovanie teórií
 - Syntax* pravidlá zápisu tvrdení
 - Sémantika* význam tvrdení
 - Usudzovanie (inferencia)** odvodenie nových dôsledkov z doterajších poznatkov
 - Dôkaz** presvedčenie ostatných o správnosti záverov usudzovania

I.2 Poznatky a teórie

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

Príklad 1.1 (Party time!). Máme troch nových známych — Kim, Jima a Sarah.

Organizujeme párty a chceme na ňu pozvať niektorých z nich.

Od spoločných kamarátov sme sa ale dozvedeli o ich požiadavkách:

P1: Sarah nepôjde na párty, ak pôjde Kim.

P2: Jim pôjde na párty, len ak pôjde Kim.

P3: Sarah nepôjde bez Jima.

I.3 Možné stavy sveta a modely

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

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

⊭ stavy, v ktorých je nepravdivé.

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

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

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

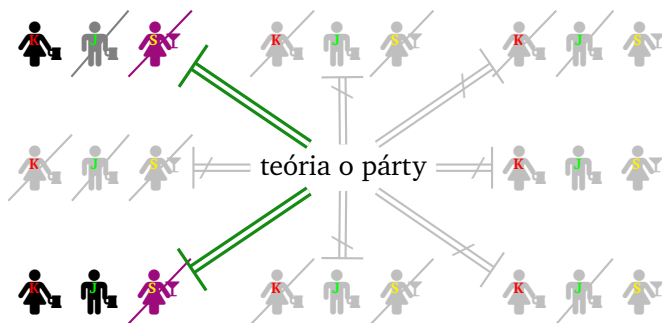


I.4 Logické dôsledky

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

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

Sarah nepôjde na párty.



I.5 Logické usudzovanie

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

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

Predpokladajme, že na párty pôjde Jim.

Teda podľa (P2) pôjde aj Kim.

Teda podľa (P1) nepôjde Sarah.

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

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

I.6 Usudzovacie pravidlá

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

Ak pôjde Jim, tak pôjde Kim.

Pôjde Jim.

Pôjde Kim.

Ak je dilítium dekryštalizované,
tak antihmota neprúdi.

Dilítium je dekryštalizované.

Antihmota neprúdi.

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

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

I.7 Korektné usudzovacie pravidlá a dedukcia

Korektné pravidlo odvodí z pravdivých premís pravdivý záver

Príklad 1.5. Pravidlo modus ponens

$$\begin{array}{l} \text{Ak } A, \text{ tak } B. \\ A. \\ \hline B. \end{array}$$

je korektné.

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

Dedukcia je usudzovanie, pri ktorom sa používajú iba korektné pravidlá

I.8 Nededuktívne pravidlá

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

Indukcia — zovšeobecnenie:

Videl som tisíc havranov.

Žiaden nebol inej farby ako čiernej.

Všetky havrany sú čierne.

Platí aj pre biele bicykle?

Abdukcia — odvodzovanie možných príčin z následkov:

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

Batéria je vybitá.

Čo ak nám kuna
prehrýzla káble?

Usudzovanie na základe analógie (podobnosti)

Venuša má atmosféru, podobne ako Zem.
Na Zemi sa prejavuje skleníkový efekt.

Na Venuši sa prejavuje skleníkový efekt.

A čo: Atmosféra
Zeme je dýchateľná?

I.9 Nededuktívne pravidlá

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

I.10 Ťažkosti s prirodzeným jazykom

Prirodzený jazyk je problematický:

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

Vlastníci bytov a nebytových priestorov v dome prijímajú rozhodnutia na schôdzi vlastníkov dvojtretinovou väčšinou hlasov všetkých vlastníkov bytov a nebytových priestorov v dome, ak hlasujú o zmluve o úvere a o každom dodatku k nej, o zmluve o zabezpečení úveru a o každom dodatku k nej, o zmluve o nájme a kúpe veci, ktorú vlastníci bytov a nebytových priestorov v dome užívajú s právom jej kúpy po uplynutí dojednaného času užívania a o každom dodatku k nej, o zmluve o vstavbe alebo nadstavbe a o každom dodatku k nim, o zmene účelu užívania spoločných častí domu a spoločných zariadení domu a o zmene formy výkonu správy; ak sa rozhoduje o nadstavbe alebo o vstavbe v podkroví alebo povale, vyžaduje sa zároveň súhlas všetkých vlastníkov bytov a nebytových priestorov v dome na najvyššom poschodí. — *Zákon č. 182/1993 Z. z. SR v znení neskorších predpisov*

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

I.11 Formálne jazyky

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

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

I.12 Formalizácia poznatkov

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

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

- Stretli ste sa už aj s formálnym jazykom výrokovej logiky

Príklad 1.6. Sformalizujme náš pártý príklad:

P0: Nieкто z trojice Kim, Jim, Sarah pôjde na párty.

P1: Sarah nepôjde na párty, ak pôjde Kim.

P2: Jim pôjde na párty, len ak pôjde Kim.

P3: Sarah nepôjde bez Jima.

I.13 Kalkuly — formalizácia usudzovania

- Pre mnohé logiky sú známe **kalkuly** — množiny usudzovacích pravidiel, ktoré sú **korektné** — odvodzujú iba logické dôsledky **úplné** — umožňujú odvodiť všetky logické dôsledky
- Kalkuly existujú aj v iných častiach matematiky
 - na počítanie s číslami, zlomkami (násobilka, aritmetika),
 - riešenie lineárnych rovníc (kalkul lineárnej algebry),
 - derivovanie, integrovanie, riešenie diferenciálnych rovníc (kalkul matematickej analýzy)

...

Poznáte už aj jeden logický kalkul — ekvivalentné úpravy

Sú korektné, ale nie vždy úplné

I.14 Výpočtová logika — automatizácia usudzovania

- Základná idea **výpočtovej logiky**:
 - Napíšeme program, ktorý systematicky aplikuje pravidlá logického kalkulu, kým neodvodí želaný dôsledok, alebo nevyčerpá všetky možnosti (nie vždy je ich konečne veľa!)

- Skutočnosť je komplikovanejšia, ale existuje množstvo automatických usudzovacích systémov
- *Jeden z prienikov informatiky a logiky*

I.15 Výpočtová logika — aplikácie

- Overovanie, dopĺňanie, hľadanie dôkazov matematických viet
- Špecifikácia a verifikácia hardvérových obvodov, programov, komunikačných protokolov
 - Špecifikácia a verifikácia programov (3. ročník)
 - Formálne metódy tvorby softvéru (magisterský)
- Logické programovanie
 - Programovacie paradigmy (3. ročník)
 - Výpočtová logika (magisterský)
 - Logické programovanie ASP (magisterský)
- Databázy — odvodzovanie neuložených faktov, optimalizácia dopytov
 - Deduktívne databázy (3. ročník)
- Sémantický web a integrácia dát z rôznych zdrojov
 - Reprezentácia znalostí a inferencia (magisterský)
 - Ontológie a znalostné inžinierstvo (magisterský)
- Analýza zákonov, regulácií, zmlúv

I.16

Spomeňte si I.1

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

- | | |
|------------------------|-----------------|
| A. premisou, | C. záverom, |
| B. logickým dôsledkom, | D. implikáciou. |

Spomeňte si I.2

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

Spomeňte si I.3

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

- | | | |
|-------------------|------------------|----------------|
| A. abdukcia, | C. formalizácia, | E. indukcia, |
| B. interpretácia, | D. dedukcia, | F. inferencia. |

1.2. O tomto kurze

I.17 Čím sa budeme zaoberať v tomto kurze

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

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

Prakticky • Vyjadrovaním problémov v jazyku logiky

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

Filozoficky • Zamýšľanými a nezamýšľanými okolnosťami platnosti tvr-
dení

- Obmedzeniami vyjadrovania a usudzovania

2. Výroková logika

2.1. Opakovanie: Výroková logika v prirodzenom jazyku

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

Príklady 2.1.

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

Negatívne príklady

- Toto je čudné.
- Píšte všetci modrým perom!
- Prečo je obloha modrá?

Výrokom priradujeme *pravdivostné hodnoty*

Operácie s výrokmi – *logické spojky*

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

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

Negatívny príklad

Spojku „pretože“ nepovažujeme za *logickú* spojku.

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

I.21 (Meta) matematika výrokovej logiky

- Stredoškolský prístup príliš **neoddeľuje** samotný *jazyk* výrokovej logiky od jeho *významu* a vlastne ani jednu stránku nedefinuje jasne
- V tomto kurze sa budeme snažiť byť **presní**
 - ▶ *Zdanlivo* budeme o jednoduchých veciach hovoriť zložito
- Pojmy z výrokovej logiky budeme **definovať matematicky**
 - ▶ ako množiny, postupnosti, funkcie, atď. ←-- Matematika (1), (3)
- Na praktických cvičeniach veľa pojmov **zadefinujete programátorsky**
 - ▶ ako reťazce, slovníky, triedy a ich metódy ←-- Programovanie (1), (2)
- Budeme sa pokúšať **dokazovať** ich vlastnosti
- Budeme teda hovoriť *o formálnej logike* pomocou matematiky, ktorá je ale sama postavená na *logike v prirodzenom jazyku*
- Matematickej logike sa preto hovorí aj *meta* matematika, matematika *o* logike (a v konečnom dôsledku aj o matematike)

2.2. Syntax výrokovej logiky

I.22 Syntax výrokovej logiky

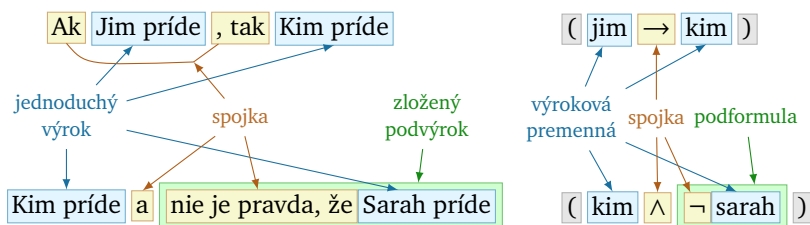
- Syntax sú pravidlá budovania viet v jazyku

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

I.23 Syntax výrokovej logiky

Aké tvrdenia chceme zapisovať vo výrokovej logike?

- Jednoduché výroky, ktorých štruktúra nás nebude zaujímať
 - „Miro sa nachádza v F1“, „Kim príde“
 Ich formálnu verziu nazveme **výrokové premenné**
- Zložené výroky, tvorené podvýrokmi a spojkou:



Ich formálnu verziu nazveme **formuly**

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

Tieto základné prvky nazveme **symbols**

Definícia 2.3. Symbolmi jazyka výrokovkej logiky sú:

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

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

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

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

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

Je o čosi všeobecnejší ako pojem znak.

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

Dohoda

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

Výrokové premenné formalizujú jednoduché výroky.

- Povedzme, že máme množinu výrokových premenných $\mathcal{V} = \{\text{kim, jim, sarah}\}$
- Ako môžu vyzeráť formuly vybudované nad touto množinou?

- Samotné premenné, napr. sarah.
 - Negácie premenných, napr. \neg sarah.
 - Premenné alebo aj ich negácie spojené spojkou, napr. $(\neg\text{kim} \vee \text{sarah})$.
 - Ale negovať a spájať spojkami môžeme aj zložitejšie formuly, napr. $(\neg(\text{kim} \wedge \text{sarah}) \rightarrow (\neg\text{kim} \vee \neg\text{sarah}))$.
- Ako presne popíšeme, čo je formula?

Induktívnou definíciou:

1. Povieme, čo sú základné formuly, ktoré sa nedajú rozdeliť na menšie formuly.
 - Podobne ako 0 pri matematickej indukcii
2. Opíšeme, ako sa z jednoduchších formúl skladajú zložitejšie.
 - Podobne ako indukčný krok pri matematickej indukcii

I.27 Výrokové formuly

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

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

Dohoda

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

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

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

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

Definícia 2.8. *Vytvárajúcou postupnosťou* nad množinou výrokových premenných \mathcal{V} je ľubovoľná konečná postupnosť postupností symbolov, ktorej každý člen

- je výroková premenná z \mathcal{V} , alebo
- má tvar $\neg A$, pričom A je niektorý predchádzajúci člen postupnosti, alebo
- má jeden z tvarov $(A \wedge B)$, $(A \vee B)$, $(A \rightarrow B)$, kde A a B sú niektoré predchádzajúce členy postupnosti.

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

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

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

II. prednáška

Sémantika výrokovej logiky

25. februára 2019

II.1

Spomeňte si II.1

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

- | | |
|---|-----------------------------------|
| A. $(p \vee \neg q \vee \neg r)$, | C. $\neg(\neg(\neg p))$, |
| B. $(p \wedge \neg(q \rightarrow r))$, | D. $(p \leftrightarrow \neg q)$. |

II.2 Ekvivalencia

Dohoda

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

II.3 Jednoznačnosť rozkladu formúl výrokovej logiky

Čo keby sme zadefinovali „formuly“ takto?

Definícia „formúl“



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

- 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 Problémy s vytvárajúcou postupnosťou

Vytvárajúca postupnosť popisuje konštrukciu formuly podľa definície formúl:

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

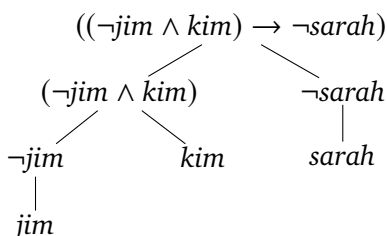
ale

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

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

II.6 Vytvárajúci strom

Konštrukciu si ale vieme predstaviť ako *strom*:



Takéto stromy voláme *vytvárajúce*.

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

II.7 Vytvárajúci strom formuly

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

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

Uvažujme formulu:

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

- Ako nazveme formuly, z ktorých vznikla?

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

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

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

- Ako tieto pojmy presne zadefinujeme?

Definícia 2.13 (Priama podformula).

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

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

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

II.10 Meranie syntaktickej zložitosti formúl

Miera zložitosti/veľkosti formuly:

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

Lepšiu mieru nazývame *stupeň formuly*

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

II.11 Meranie syntaktickej zložitosti formúl

Ako stupeň zadefinujeme?

Podobne ako sme zadefinovali formuly — induktívne:

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

II.12 Stupeň formuly

Definícia 2.16 (Stupeň formuly).

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

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

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

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

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

II.13 Indukcia na stupeň formuly

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

báza indukcie: každá formula stupňa 0 má vlastnosť P ,

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

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

II.14 Množina výrokových premenných formuly

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

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

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

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

Spomeňte si II.2

Je nasledujúce tvrdenie pravdivé? Odpovedzte áno/nie.

Vďaka jednoznačnosti rozkladu má každá formula práve jednu priamu podformulu.

Spomeňte si II.3

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

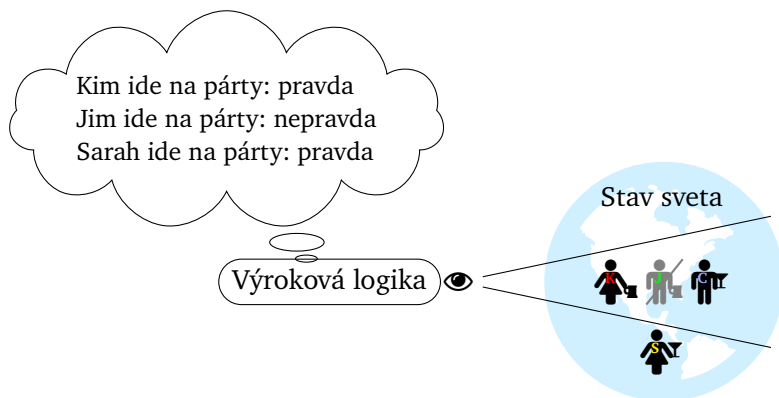
- priame podformuly,
- podformuly,
- vytvárajúci strom.

Spomeňte si II.4

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

2.3. Sémantika výrokovej logiky

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



II.18 Predstava výrokovej logiky o svete

Výroková logika vníma svet *veľmi zjednodušene*.

Zaujíma ju iba

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

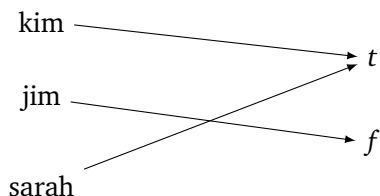
II.19 Formalizácia výrokového pohľadu na svet

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

II.20 Ohodnotenie výrokových premenných

Definícia 2.19. Nech (t, f) je usporiadaná dvojica *pravdivostných hodnôt*, $t \neq f$, pričom hodnota t predstavuje pravdu a f nepravdu.

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



Výroková premenná p je *pravdivá* pri ohodnotení v , ak $v(p) = t$.
 Výroková premenná p je *nepravdivá* pri ohodnotení v , ak $v(p) = f$.

II.21 Ohodnotenie výrokových premenných

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

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

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

Pondelkové ráno pred týždňom opisuje ohodnotenie v_2 , kde okrem iného

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

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

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

Prečo „okrem iného“?

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

II.22 Splňanie výrokových formúl

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

Príklad 2.21. Nech v_3 je ohodnotenie množiny $\mathcal{V} = \{a, \dots, z\}^+$, také že

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

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

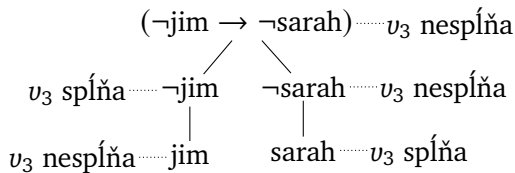
Zoberieme vytvárajúcu postupnosť, prejdeme ju zľava doprava:

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

Príklad 2.21 (pokračovanie).

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

Iná možnosť je použiť vytvárajúci strom:



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

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

- Veľmi podobne vieme zadať splnenie matematicky.

Definícia 2.22. Nech \mathcal{V} je množina výrokových premenných. Nech v je ohodnotenie množiny \mathcal{V} . Pre všetky výrokové premenné p z \mathcal{V} a všetky formuly A, B nad \mathcal{V} definujeme:

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

Dohoda

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

Definícia 2.22 (symbolicky). Nech \mathcal{V} je množina výrokových premenných. Nech v je ohodnotenie množiny \mathcal{V} . Pre všetky výrokové premenné p z \mathcal{V} a všetky formuly A, B nad \mathcal{V} definujeme:

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

Vzťah \models je súčasťou programovacích jazykov – vyhodnocovanie boolovských výrazov

Príklad 2.23. Nech v_3 je ohodnotenie množiny $\mathcal{V} = \{a, \dots, z\}^+$, také že

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

Zistíme, ktoré z formúl

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

ohodnotenie v_3 spĺňa a ktoré nespĺňa.

$\text{deg}(X)$	$v_3 \models X$	$v_3 \not\models X$
0	kim, sarah	jim
1	$\neg \text{jim}, (\text{kim} \vee \text{jim}), (\text{jim} \rightarrow \text{kim})$	$\neg \text{sarah}$
2	$((\text{kim} \vee \text{jim}) \vee \text{sarah})$	$(\text{kim} \rightarrow \neg \text{sarah})$
3		$(\neg \text{jim} \rightarrow \neg \text{sarah})$

2.4. Tautológie, (ne)splniteľnosť, falzifikovateľnosť

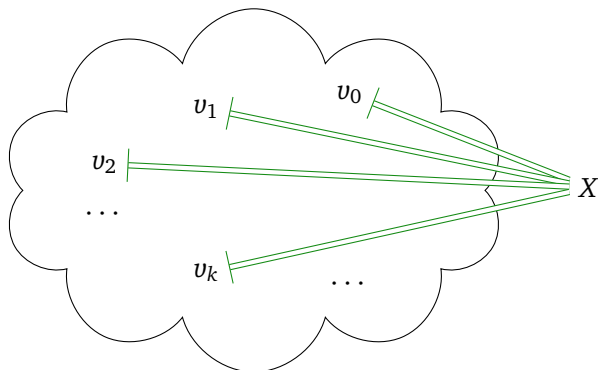
- Predchádzajúca definícia a príklad:
spĺňanie **mnohých formúl jedným ohodnotením** (stavom sveta)
- Obráťme perspektívu:
spĺňanie **jednej formuly mnohými ohodnoteniami**
- Ktoré stavy sveta vyhovujú podmienke vyjadrenej formulou?

Dohoda

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

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

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



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

II.31 Tautológia — testovanie

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

II.32 Tautológia — testovanie

Tvrdenie 2.25. *Splnenie výrokovej formuly pri ohodnotení výrokových premenných závisí iba od ohodnotenia konečného počtu výrokových premenných, ktoré sa v nej vyskytujú.*

Presnejšie:

Pre každú formulu X a všetky ohodnotenia v_1 a v_2 , ktoré zhodujú na množine $\text{vars}(X)$ výrokových premenných vyskytujúcich sa v X , platí $v_1 \models X$ vtt $v_2 \models X$.

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

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

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

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

Pretože všetky skúmané ohodnotenia spĺňajú X , je X tautológiou.

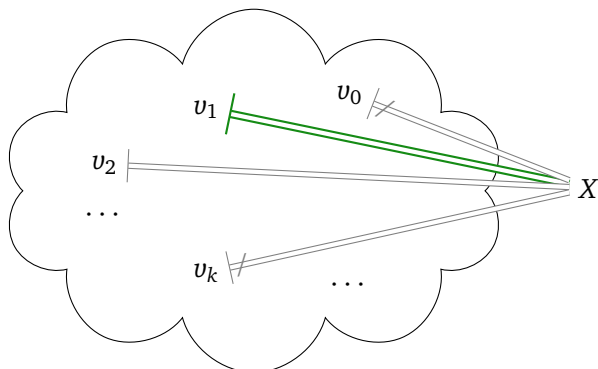
Dôkaz. Indukciou na stupeň formuly X .

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

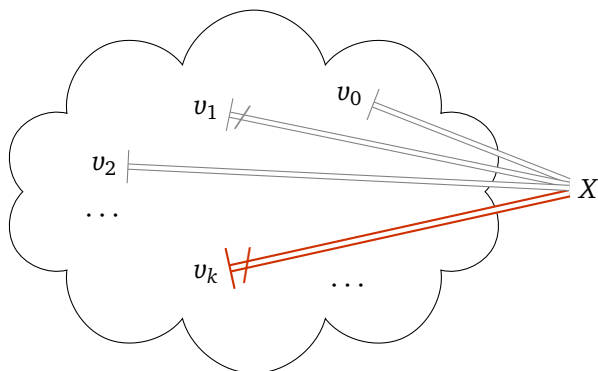
Krok: Nech X je stupňa $n > 0$ a tvrdenie platí pre všetky formuly stupňa nižšieho ako n (indukčný predpoklad). Zoberme ľubovoľné ohodnotenia v_1 a v_2 , ktoré sa zhodujú na premenných v X . Podľa definície stupňa a jednoznačnosti rozkladu nastáva práve jeden z prípadov:

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

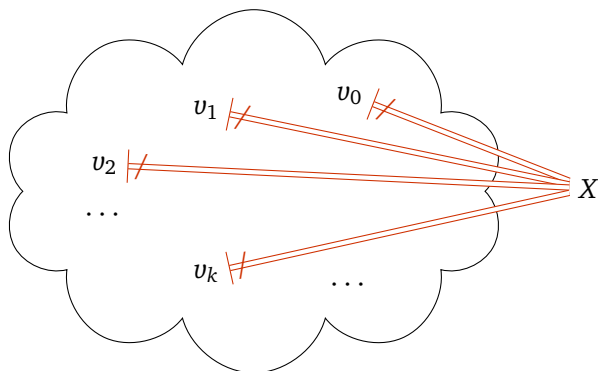
□



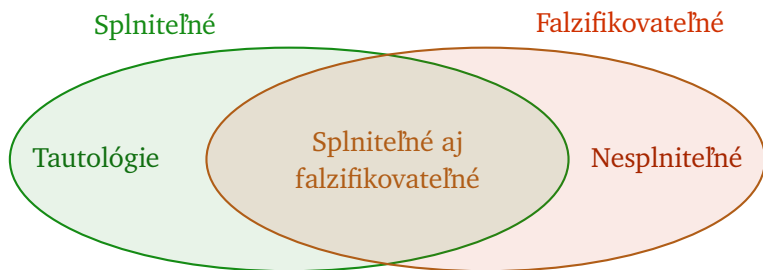
Definícia 2.27. Formulu X nazveme *splniteľnou* vtt **nejaké** ohodnotenie výrokových premenných **spĺňa** X (teda **existuje** také ohodnotenie výrokových premenných v , že $v \models X$).



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



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



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

Obrázok podľa [Papadimitriou, 1994]

Zamyslite sa II.5

Ak formula *nie* je falzifikovateľná, je:

A. splniteľná,

B. nesplniteľná,

C. tautológia.

III. prednáška

Vyplývanie a ekvivalencia

4. marca 2019

III.1 Tautológie a (ne)splniteľnosť

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

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

(\Leftarrow) Opačne, nech $\neg X$ je nespĺniteľná. To znamená, že pri každom ohodnotení výrokových premenných je $\neg X$ nespĺnená. Podľa definície spĺňania je teda X pri každom ohodnotení splnená, a teda je tautológia. \square

III.2 Teórie

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

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

Dohoda

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

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

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

Pojem splňania sa jednoducho rozšíri na teórie.

Definícia 2.33. Nech T je teória, nech v je ohodnotenie výrokových premených. Ohodnotenie v *spĺňa teóriu* T (skrátene $v \models T$) vtt v spĺňa každú formulu X z množiny T . Spĺňajúce ohodnotenie nazývame *modelom* teórie T .

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

Tvrdenie 2.35. *Splnenie teórie T pri ohodnotení výrokových premenných závisí iba od ohodnotenia výrokových premenných, ktoré sa vyskytujú vo formulách v T .*

Presná formulácia je podobná ako pri splňaní formúl. Dôkaz sporom, lebo množina formúl môže byť nekonečná.

2.5. Výrokovologické vyplývanie

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

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

Teória je *nesplniteľná* vtt nie je splniteľná.

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

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

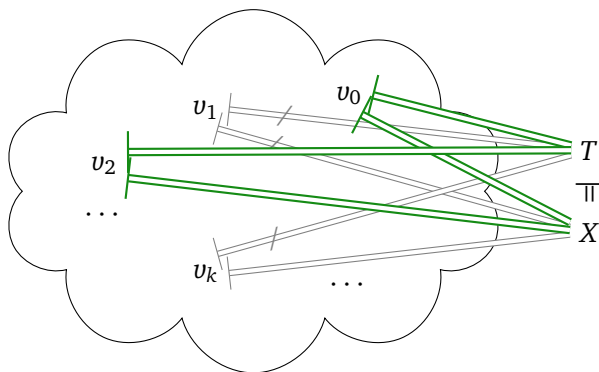
- Aký je účel teórií? Kedy je teória užitočná?
 - Keď z nej dokážeme *odvodiť* (uvažovaním alebo počítaním) *doteraz neznáme skutočnosti* (teda nezapísané v teórii), ktoré platia vo všetkých stavoch sveta spĺňajúcich teóriu.

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

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

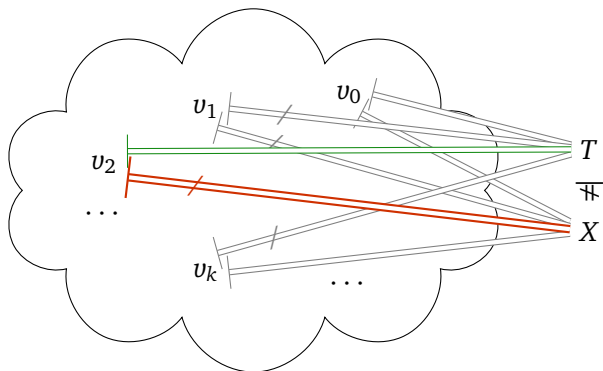
Ktorá ďalšia formula vyplýva z T_{party} ?

III.6 Výrokovologické vyplývanie



Definícia 2.39 (Výrokovologické vyplývanie). Z teórie T výrokovologicky vyplýva formula X (tiež X je výrokovologickým dôsledkom T , 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_{party} ?

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

III.8 Vyplývanie a (ne)splniteľnosť

Použitie SAT solvera na rozhodovanie vyplývania je založené na:

Tvrdenie 2.41. *Formula X výrokologicky vyplýva z teórie T vtt množina $T \cup \{\neg X\}$ je nespĺniteľná.*

Prečo je to tak?

III.9 Vyplývanie a (ne)splniteľnosť – dôkaz

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

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

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

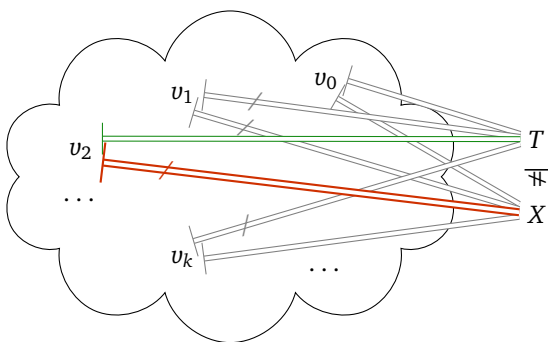
V oboch prípadoch v nespĺňa $T \cup \{\neg X\}$. Pretože v bolo ľubovoľné, môžeme zovšeobecniť, že žiadne v nespĺňa $T \cup \{\neg X\}$, teda $T \cup \{\neg X\}$ je nespĺniteľná.

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

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

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

Je aj jej negácia nezávislá od T_{party} ?



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

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

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

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

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

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

a) $T \cup \{A\} \models B$ vtt $T \models (A \rightarrow B)$.

b) $\{\} \models A$ vtt A je tautológia ($\models A$).

c) Nasledujúce tvrdenia sú ekvivalentné:

- i. $\{A_1, A_2, \dots, A_n\} \models B$
- ii. $\{((\dots(A_1 \wedge A_2) \wedge \dots) \wedge A_n)\} \models B$
- iii. $\{\} \models ((\dots(A_1 \wedge A_2) \wedge \dots) \wedge A_n \rightarrow B)$
- iv. $\models (((\dots(A_1 \wedge A_2) \wedge \dots) \wedge A_n) \rightarrow B)$

III.13 Hlasujte

Spomeňte si III.1

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

Pravda alebo nepravda?

2.6. Ekvivalencia formúl

III.14 Ekvivalencia formúl

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

Definícia 2.46. Dve formuly X a Y sú (výrokovologicky) ekvivalentné ($X \Leftrightarrow Y$) vtt

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

III.15 Ekvivalencia formúl a skratka \leftrightarrow

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

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

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

Ako súvisí ekvivalencia formúl s vyplývaním?

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

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

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

Dôkaz $\{Y\} \models X$ je podobný.

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

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

Tvrdenie 2.49 (Tranzitivita ekvivalencie). *Nech X , Y a Z sú formuly.*

*Ak X je ekvivalentná s Y a Y je ekvivalentná so Z ,
tak X je ekvivalentná so Z .*

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

je tautológia“

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

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

Dôkaz. Nech X, Y a Z sú formuly. Nech X je ekvivalentná s Y a Y je ekvivalentná so Z . Nech v je ľubovoľné ohodnotenie.

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

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

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

2.6.1. Ekvivalentné úpravy

III.18 Ekvivalentné úpravy

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

Príklad 2.50 (Nahradenie podformuly ekvivalentnou).

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

$$\Downarrow$$

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

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

III.19 Pravidlá ekvivalentných úprav

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

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

$$\Downarrow \qquad \qquad \Downarrow$$

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

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

Oba druhy dosadení pri ekvivalentných úpravách sú *substitúcie*

Definícia 2.52 (Substitúcia). Nech X , A , B sú formuly.

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

Substitúciu si vieme predstaviť ako cyklus prechádzajúci cez X :

Substitúcia ako cyklus

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

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

Substitúcia rekurzívne

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

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

Korektnosť ekvivalentných úprav vyjadrujú nasledujúce tvrdenia:

Tvrdenie 2.53 (Dosadenie do ekvivalentných formúl). *Nech A a B sú navzájom ekvivalentné formuly, p je výroková premenná a Y je formula. Potom formuly $A[p|Y]$ a $B[p|Y]$ sú ekvivalentné.*

Veta 2.54 (Ekvivalentné úpravy). *Nech X je formula, A a B sú ekvivalentné formuly. Potom formuly X a $X[A|B]$ sú tiež ekvivalentné.*

Obe tvrdenia o korektnosti sú dôsledkami nasledujúcej lemy:

Lema 2.55. *Nech X je výroková formula, p je výroková premenná, A je formula a v je ohodnotenie výrokových premenných. Potom $v \models X[p|A]$ vtt $v_{p|A} \models X$, kde $v_{p|A}$ je ohodnotenie, pre ktoré platí:*

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

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

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

Nasledujúce dvojice formúl sú ekvivalentné:

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

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

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

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

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

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

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

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

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

Veta 2.56 (Pokračovanie).

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

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

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

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

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

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

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

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

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

2.6.2. Konjunktívna a disjunktívna normálna forma

III.28 Konjunkcia a disjunkcia postupnosti formúl

Dohoda

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

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

III.29 Konjunktívny a disjunktívny normálny tvar

Definícia 2.57.

Literál je výroková premenná alebo negácia výrokovej premennej.

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

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

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

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

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

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

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

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

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

IV. prednáška

CNF

Hilbertovský kalkul

11. marca 2018

IV.1 Existencia DNF a CNF

Veta 2.59. 1. Ku každej formule X existuje ekvivalentná formula D v disjunktívnom normálnom tvare.

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

Dôkaz. 1. Zoberme všetky ohodnotenia v_1, \dots, v_n také, že $v_i \models X$ a $v_i(q) = f$ pre všetky premenné $q \notin \text{vars}(X)$. Pre každé v_i zostrojme formulu C_i ako konjunkciu obsahujúcu p , ak $v_i(p) = t$, alebo $\neg p$, ak $v_i(p) = f$, pre každú $p \in \text{vars}(X)$. Očividne formula $D = \bigvee_{1 \leq i \leq n} C_i$ je v DNF a je ekvivalentná s X (vymenúva všetky možnosti, kedy je X splnená).

2. K $\neg X$ teda existuje ekvivalentná formula D v DNF. Znegovaním D a aplikáciou de Morganových pravidiel dostaneme formulu C v CNF, ktorá je ekvivalentná s X . \square

IV.2 CNF — trochu lepší prístup

- Skúmanie všetkých ohodnotení nie je ideálny spôsob ako upraviť formulu do CNF — najmä keď má veľa premenných a jej splniteľnosť chceme rozhodnúť SAT solverom.
- Je nejaký lepší systematický postup?

- Všimnime si:

CNF je konjunkcia disjunkcií literálov — výrokových premenných alebo ich negácií

Teda:

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

IV.3 CNF — trochu lepší prístup — algoritmus

Algoritmus CNF

1. Nahradíme implikáciu disjunkciou:

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

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

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

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

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

4. Prezátvorkujeme na požadovaný tvar pomocou asociatívnych pravidiel.

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

Príklad 2.61.

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

IV.5 Prečo iba trochu lepší prístup?

Distribúcia \vee cez \wedge spôsobuje nárast formuly:

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

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

IV.6 Obmedzenie exponenciálneho rastu CNF

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

1. Zoberme nové výrokové premenné r_1, \dots, r_n, s
2. 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 $(s \wedge (s \leftrightarrow (r_1 \vee \dots \vee r_n))) \wedge (r_1 \leftrightarrow (p_1 \wedge q_1)) \wedge \dots \wedge (r_n \leftrightarrow (p_n \wedge q_n))$

Ekvivalentnými úpravami

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

IV.7 Cejtinova transformácia do CNF

Cejtinova transformácia (angl. Tseytin transformation)

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

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

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

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

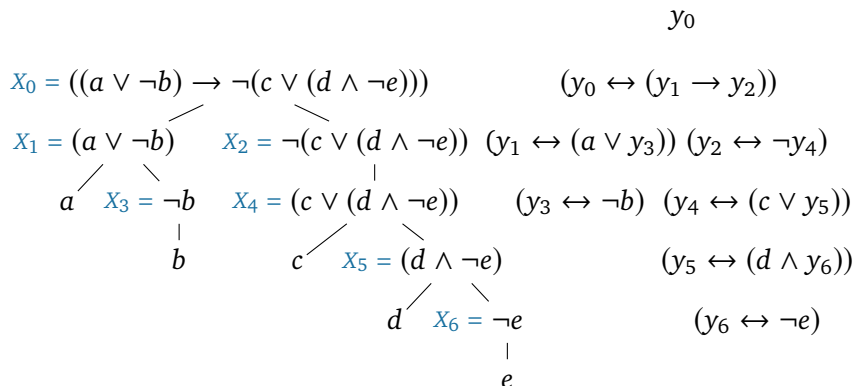
Pri úprave formuly do CNF pre SAT solver

- nepotrebuje zachovať ekvivalenciu
- stačí ekvisplniteľnosť

Cejtinova transformácia

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

Príklad 2.65.



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

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

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

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

2.7. Logické kalkuly

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

IV.13 Ekvivalencia syntakticky vs. sémanticky

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

IV.14 Kalkuly — dokazovanie vyplývania syntakticky

- Ak začneme nejakou formulou a budeme substituovať ekvivalentné podformuly, dostávame postupne rôzne formuly, ktoré sú ale stále ekvivalentné s pôvodnou formulou.
- Čo keby sme začali s tautológiou?
 - Dostávame stále tautológie.

- Logiku viac zaujíma vyplývanie ako ekvivalencia a tautológie
- Vyplývanie dôsledkov z teórií sme doteraz dokazovali sémanticky — vyšetrením všetkých ohodnotení.
- Na tento účel ale existujú aj syntaktické metódy — *kalkuly*.
- Ukážeme si tri kalkuly:
hilbertovský — klasický, lineárny, pomerne ťažkopádny
tablový — stromový, prirodzenejší
rezolvenciu — lineárny, strojový

2.8. Hilbertovský kalkul

IV.15 Hilbertovský kalkul — axiómy a pravidlo

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

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

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

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

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

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

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

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

a pravidla *modus ponens*:

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

pre všetky formuly A a B .

[Švejdar, 2002, §1.3]

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

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

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

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

[Švejdar, 2002, §1.3]

IV.17 Príklad dôkazu v hilbertovskom kalkule

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

(pre ľubovoľnú formulu X):

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

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

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

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

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

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

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

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

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

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

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

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

IV.19 Dokazovanie s vetou o dedukcii

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

(pre ľubovoľné formuly A, B a C).

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

Posledný dôkaz nájdeme veľmi ľahko:

$Y_1 = A$ predpoklad

$Y_2 = (A \rightarrow B)$ predpoklad

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

$Y_4 = (B \rightarrow C)$ predpoklad

$$Y_5 = C$$

(MP) pre Y_3, Y_4

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

IV.20 Dokazovanie s vetou o dedukcii

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

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

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

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

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

\vdots

dôkaz z príkladu 2.72

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

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

(MP) pre Y_1 a Y_n

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

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

IV.21 Korektnosť a úplnosť hilbertovského kalkulu

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

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

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

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

Ak S je množina výrokových formúl a ak

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

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

Úplnosť (angl. completeness) je komplikovanejšia.

Vyskúšajte si IV.1

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

V. prednáška

Tablový kalkul a jeho korektnosť

18. marca 2019

Logické kalkuly (opakovanie)

V.1 Logické kalkuly — vyplývanie syntakticky

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

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

Zvyčajne má dve zložky:

Axiómy alebo ich schémy — „základné pravdy“

Napríklad hilbertovské schémy axióm:

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

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

Napríklad jediné pravidlo hilbertovského kalkulu:

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

Kalkul je najužitočnejší, keď je súčasne

korektný (angl. sound):

dovoľuje odvodiť **iba** skutočne vyplývajúce formuly,

úplný (angl. complete):

umožňuje odvodiť **všetky** vyplývajúce formuly.

Hilbertovský kalkul je korektný aj úplný

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

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

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

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

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

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

2.9. Tablový kalkul

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

Podme na to sporom: Predpokladajme, že existuje také ohodnotenie v , že $v \models T'_{\text{party}}$, teda (1) $v \models (kim \rightarrow (jim \wedge \neg sarah))$ a (2) $v \models (eva \rightarrow kim)$, ale pritom (3) $v \not\models (sarah \rightarrow \neg eva)$.

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

Podľa (2) máme dve možnosti: (7) $v \models \text{eva}$ alebo (8) $v \models \text{kim}$. Možnosť (7) je v spore s (6).

Platí teda (8) a podľa (1) ďalej môžu nastať dva prípady: (9) $v \models \text{kim}$, ktorý je však v spore s (8), alebo (10) $v \models (\text{jim} \wedge \neg \text{sarah})$. V tom prípade (11) $v \models \text{jim}$ a (12) $v \models \neg \text{sarah}$, čiže (13) $v \models \text{sarah}$, čo je zase v spore s (4).

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

V.5 Tablová notácia pre dôkazy

Dôkaz stručne zapíšeme v tablovej (tabuľkovej) notácii:

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

V.6 Dôkaz vyplývania sporom v tablovej notácii

Príklad 2.76.

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

[†] Tento zápis nepoužívajte vo svojich riešeniach.

V.7 Definícia tablového kalkulu

Tablová notácia

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

Tablový kalkul — presne matematicky zadefinovaný formálny systém
Zadefinujeme:

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

Definícia 2.77. Nech X je formula výrokovej logiky.

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

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

- v *spĺňa* $\mathbf{T}X$ vtt v *spĺňa* X ;
- v *spĺňa* $\mathbf{F}X$ vtt v *nespĺňa* X .

Dohoda

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

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

V.9 Spĺňanie a priame podformuly

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

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

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

Pozorovanie 2.79 — dobrý základ pre odvodzovacie pravidlá

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

Splnenie/nespĺnenie vyjadríme označenými formulami podľa def. 2.78

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

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

Definícia 2.80 (Jednotný zápis označených formúl typu α).

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

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

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

Potom v spĺňa α vtt v spĺňa α_1 a v spĺňa α_2 .

Definícia 2.82 (Jednotný zápis označených formúl typu β).

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

β	β_1	β_2
$\mathbf{F}(X \wedge Y)$	$\mathbf{F} X$	$\mathbf{F} Y$
$\mathbf{T}(X \vee Y)$	$\mathbf{T} X$	$\mathbf{T} Y$
$\mathbf{T}(X \rightarrow Y)$	$\mathbf{F} X$	$\mathbf{T} Y$

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

Potom v spĺňa β vtt v spĺňa β_1 alebo v spĺňa β_2 .

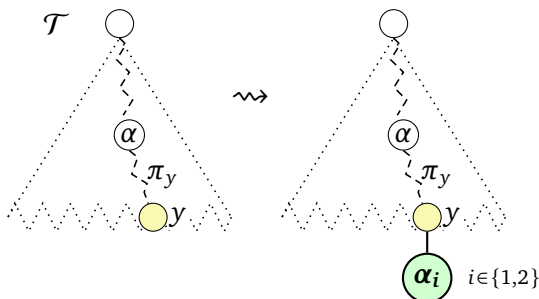
Akú štruktúru má dôkaz zapísaný v tablovej notácii?

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

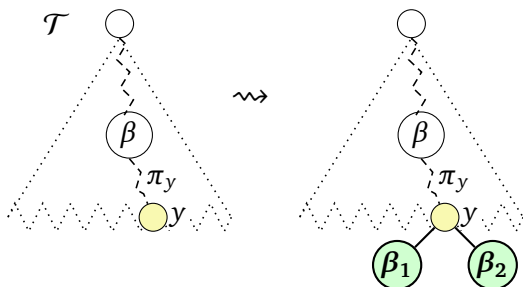
Nič iné nie je tablom pre S^+ .

V.16 Tablá a tablové pravidlá

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



α	α	α	α_1	α_2
α_1	α_2			
$T(X \wedge Y)$	$T X$	$T X$	$T X$	$T Y$
$F(X \vee Y)$	$F X$	$F X$	$F X$	$F Y$
$F(X \rightarrow Y)$	$T X$	$F Y$		
$T \neg X$	$F X$	$F X$		
$F \neg X$	$T X$	$T X$		



β	β	β_1	β_2
β_1	β_2		
$F(X \wedge Y)$	$F X$	$F X$	$F Y$
$T(X \vee Y)$	$T X$	$T X$	$T Y$
$T(X \rightarrow Y)$	$F X$	$T Y$	

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

V.17 Uzavretosť a otvorenosť vetvy a tabla

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

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

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

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

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

V.18

Spomeňte si V.1

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

2.9.1. Korektnosť

V.19 Korektnosť tablového kalkulu

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

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

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

VI. prednáška

Korektnosť a úplnosť tablového kalkulu

25. marca 2019

VI.1 Korektnosť — idea dôkazu

Aby sme dokázali korektnosť tabiel, dokážeme postupne dve lemy:

- (K1) Ak máme tablo pre splniteľnú množinu S^+ s aspoň jednou splniteľnou vetvou, tak každé jeho priame rozšírenie má tiež splniteľnú vetvu.
- (K2) Každé tablo pre splniteľnú množinu S^+ má aspoň jednu splniteľnú vetvu.

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

VI.2 Korektnosť — splnenie priameho rozšírenia tabla

Hodí sa nám pomocná definícia:

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

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

Lema 2.91 (K1). Nech S^+ je množina označených formúl, nech \mathcal{T} je tablo pre S^+

a nech v je ohodnotenie množiny výrokových premenných.

Ak v spĺňa S^+ a v spĺňa \mathcal{T} , tak v spĺňa aj každé priame rozšírenie \mathcal{T} .

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 π . Nech \mathcal{T}_1 je priame rozšírenie \mathcal{T} . Nastáva jeden z prípadov:

- \mathcal{T}_1 vzniklo z \mathcal{T} pravidlom α , pridaním nového dieťaťa z nejakému listu y v \mathcal{T} , pričom z obsahuje α_1 alebo α_2 pre nejakú formulu α na vetve π_y . Ak $\pi \neq \pi_y$, tak \mathcal{T}_1 obsahuje π a teda je splnené.
Ak $\pi = \pi_y$, tak v spĺňa aj α , pretože spĺňa π . Potom v musí spĺňať aj α_1 a α_2 . Spĺňa teda vetvu π_z v table \mathcal{T}_1 , ktorá rozširuje splnenú vetvu π o vrchol z obsahujúci splnenú ozn. formulu α_1 alebo α_2 . Preto v spĺňa tablo \mathcal{T}_1 .
- \mathcal{T}_1 vzniklo z \mathcal{T} pravidlom β , pridaním detí z_1 a z_2 nejakému listu y v \mathcal{T} , pričom z_1 obsahuje β_1 a z_2 obsahuje β_2 pre nejakú formulu β na vetve π_y . Ak $\pi \neq \pi_y$, tak \mathcal{T}_1 obsahuje π a teda je splnené.
Ak $\pi = \pi_y$, tak v spĺňa aj β , pretože spĺňa π . Potom ale v musí spĺňať aj β_1 alebo β_2 . Ak v spĺňa β_1 , tak spĺňa aj vetvu π_{z_1} v table \mathcal{T}_1 , a preto v spĺňa tablo \mathcal{T}_1 . Ak v spĺňa β_2 , spĺňa aj π_{z_2} , a teda aj \mathcal{T}_1 .
- \mathcal{T}_1 vzniklo z \mathcal{T} pravidlom S^+ , pridaním nového dieťaťa z nejakému listu y v \mathcal{T} , pričom z obsahuje formulu $X^+ \in S^+$. Ak $\pi \neq \pi_y$, tak \mathcal{T}_1 obsahuje π a teda je splnené.
Ak $\pi = \pi_y$, tak v spĺňa vetvu π_z v table \mathcal{T}_1 , pretože je rozšírením splnenej vetvy π o vrchol z obsahujúci splnenú formulu X (pretože $v \models S^+$). Preto v spĺňa tablo \mathcal{T}_1 . \square

Lema 2.92 (K2). *Nech S^+ je množina označených formúl, nech \mathcal{T} je tablo pre S^+*

a nech v je ohodnotenie.

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

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

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

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

VI.5 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 π v \mathcal{T} .

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

teda π obsahuje označené formuly $\mathbf{T}X$ a $\mathbf{F}X$ pre nejakú formulu X .

Ale $v \models \mathbf{T}X$ vtt $v \models X$ a $v \models \mathbf{F}X$ vtt $v \not\models X$, čo je spor. \square

2.9.2. Tablový dôkaz splniteľnosti

VI.6 Úplná vetva a tablo

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

Definícia 2.93 (Úplná vetva a úplné tablo). Nech S^+ je množina označených formúl a \mathcal{T} je tablo pre S^+ .

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

- pre každú označenú formulu α , ktorá sa vyskytuje na π , sa *obidve* označené formuly α_1 a α_2 vyskytujú na π ;
- pre každú označenú formulu β , ktorá sa vyskytuje na π , sa *aspoň jedna* z označených formúl β_1, β_2 vyskytuje na π ;

- každá $X^+ \in S^+$ sa vyskytuje na π .

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

Príklad 2.94. Vybudujme úplné tablo pre $\mathbf{F}X$, kde $X = (((p \vee r) \wedge (s \vee p)) \rightarrow (p \wedge (r \vee s)))$.

VI.7 Otvorené tablo a splniteľnosť

Nech tablové pravidlá v príklade použijeme v akomkoľvek,

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

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

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

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

Otázka. • Dá sa vždy nájsť úplné tablo?

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

VI.8 Existencia úplného tabla

Lema 2.95 (o existencii úplného tabla). *Nech S^+ je konečná množina označených formúl.*

Potom existuje úplné tablo pre S^+ .

Dôkaz. Vybudujme tablo \mathcal{T}_0 pre S^+ tak, že do koreňa vložíme niektorú formulu z S^+ a opakovaním spravidla S^+ postupne doplníme ostatné. Potom tablo postupne rozširujeme tak, že vyberieme ľubovoľný list y tabla \mathcal{T}_i , ktorého vetva π_y je otvorená a nie je úplná. Potom nastane aspoň jedna z možností:

- Na π_y sa nachádza nejaká formula α , ale nenachádza sa niektorá z formúl α_1 a α_2 .
- Na π_y sa nachádza nejaká formula β , ale nenachádza sa ani jedna z formúl β_1 a β_2 .

Ak platí prvá alebo obe možnosti, aplikujeme pravidlo α . Ak platí druhá možnosť, aplikujeme pravidlo β . 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

VII. prednáška

Úplnosť tabiel

Korektné pravidlá

Výroková rezolvenca

1. apríla 2019

2.9.3. Hintikkova lema

VII.1 Nadol nasýtené množiny a Hintikkova lemma

Definícia 2.96. 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 2.97. *Nech π je úplná otvorená vetva nejakého tabla \mathcal{T} . Potom množina všetkých formúl na π je nadol nasýtená.*

Lema 2.98 (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 korektné definované vďaka H_0 .

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

- v očividne spĺňa všetky označené výrokové premenné z S^+ .
- $X^+ \in S^+$ je buď α alebo β :
 - Ak X^+ je α , potom obidve $\alpha_1, \alpha_2 \in S^+ (H_1)$, sú nižšieho stupňa X^+ , a teda podľa indukčného predpokladu sú splnené pri v , preto v spĺňa aj α (podľa pozorovania 2.81).
 - Ak X^+ je β , potom aspoň jedna z β_1, β_2 je v $S^+ (H_2)$. Nech je to ktorákolvek, je nižšieho stupňa ako X^+ , teda podľa IP ju v spĺňa, a preto v spĺňa β (podľa pozorovania 2.83). \square

2.9.4. Úplnosť

VII.3 Úplnosť

Úplnosť kalkulu neformálne:

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

Veta 2.99 (o úplnosti). *Nech S^+ je konečná nesplniteľná množina označených formúl.*

Potom existuje uzavreté tablo pre S^+ .

Dôsledok 2.100. *Nech S je konečná teória a X je formula.*

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

Dôsledok 2.101. *Nech X je formula. Ak $\models X$, tak $\vdash X$.*

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

VII.4 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. \square

2.9.5. Nové korektné pravidlá

VII.5 Ingrediencie korektnosti a úplnosti tabiel

Všimnite si:

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

VII.6 Nové pravidlo

Čo sa stane, ak pridáme nové pravidlo, napríklad modus ponens:

$$\frac{\mathbf{T}(A \rightarrow B) \quad \mathbf{T} A}{\mathbf{T} B} \quad ? \quad (\text{MP})$$

Upravíme definíciu priameho rozšírenia:

Úprava definície 2.84

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

α : ...

\vdots

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

Korektnosť tabiel s (MP)

- Pri dôkaze lemy K1 (2.91)

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} .

využijeme

Tvrdenie 2.102 (Korektnosť pravidla (MP)). *Nech v je ľubovoľné ohodnotenie. Ak v spĺňa $\mathbf{T}(A \rightarrow B)$ a $\mathbf{T}A$, tak v spĺňa $\mathbf{T}B$.*

Dôkaz. Keďže $v \models \mathbf{T}(A \rightarrow B)$, tak $v \models (A \rightarrow B)$, teda $v \not\models A$ alebo $v \models B$.

Pretože ale $v \models \mathbf{T}A$, tak $v \models A$. Takže $v \models B$. □

- Dôkaz lemy K2 (2.92) a samotnej vety o korektnosti (2.87) — bez zmeny

Úplnosť — bez zmeny, úplné tablo vybudujú základné pravidlá

Definícia 2.103 (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 -tíc 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 súčasnou 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^+ .

Úprava definície 2.84

(...)

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

$$\vdots$$

R: Ak sa pre nejakú inštanciu pravidla R na vetve π_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^+ .

2.10. Rezolvenca vo výrokovkej logike

VII.10 Transitivity implicácie

Vráťme sa k neoznačeným formulám.

Je nasledujúce pravidlo korektné?

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

Nahradíme implikácie disjunkciami:

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

VII.11 Rezolvenca

Predchádzajúce pravidlo sa dá zovšeobecniť na ľubovoľné dvojice klauzúl:

Definícia 2.104. *Rezolvenčný princíp (rezolvencia, 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 2.105. *Rezolvencia je korektné pravidlo, teda rezolventa je logickým dôsledkom množiny obsahujúcej obe premisy.*

VII.12 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)

VII.13 Pozorovania o rezolvencii

- Rezolvencia 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 nespĺniteľná

- Opakovaným aplikovaním rezolvenzie môžeme odvodzovať ďalšie dôsledky

Príklad 2.106. 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)

- Klauzula $(r \vee r)$ je evidentne ekvivalentná s r ;
 r sa ale z množiny S iba rezolvenciou odvodíť nedá

- Preto potrebujeme ešte *pravidlo idempotencie*:

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

VII.16 Rezolvenčné odvodenie a zamietnutie

Definícia 2.107. *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 2.108. Množinu klauzúl budeme nazývať aj *klauzálna teória*.

VII.17 Korektnosť a úplnosť rezolvenčie

Veta 2.109 (Korektnosť rezolvenčie). *Nech S je množina klauzúl. Ak existuje zamietnutie S , tak S je nespĺniteľná.*

Veta 2.110 (Úplnosť rezolvenčie). *Nech S je množina klauzúl. Ak S je nespĺniteľná, tak existuje zamietnutie S .*

VIII. prednáška

SAT solver a algoritmus DPLL

Syntax relačnej logiky prvého rádu

8. apríla 2019

2.11. Problém výrokovologickej splniteľnosti (SAT)

VIII.1 Problém SAT

Definícia 2.111 (Problém SAT). *Problémom výrokovologickej splniteľnosti (SAT) je problém určenia toho, či je daná množina výrokových formúl splniteľná*

- Zvyčajne sa redukuje na problém splniteľnosti *klauzálnej* teórie (teda formuly v CNF)
- *SAT solver* je program, ktorý rieši problém SAT

Príklad 2.112. Je množina klauzúl S splniteľná?

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

VIII.2 Tabuľková metóda

Tabuľková metóda:

- Skúma *všetky* ohodnotenia výrokových premenných
- Trvá $O(s2^N)$ krokov,
 - N je počet premenných a s je súčet veľkostí klauzúl
 - 2^N ohodnotení, pre každé treba zistiť, či sú všetky klauzuly splnené
- Zaberá priestor $O(k2^N)$

- k je počet klauzúl
 - Pamätáme si (píšeme na papier) celú tabuľku
- Tabuľka slúži aj ako dôkaz prípadnej nesplniteľnosti

2.11.1. Naivný backtracking

VIII.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,

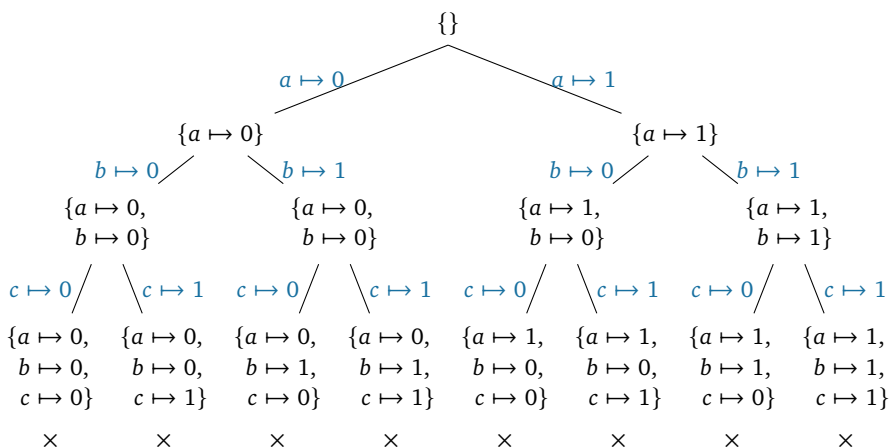
s – súčet veľkostí klauzúl

VIII.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 znamená $\not\models S$

$f := 0, t := 1$



VIII.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

Strom ohodnotení:

- List — ohodnotenie všetkých premenných
- Každý uzol — čiastočné ohodnotenie

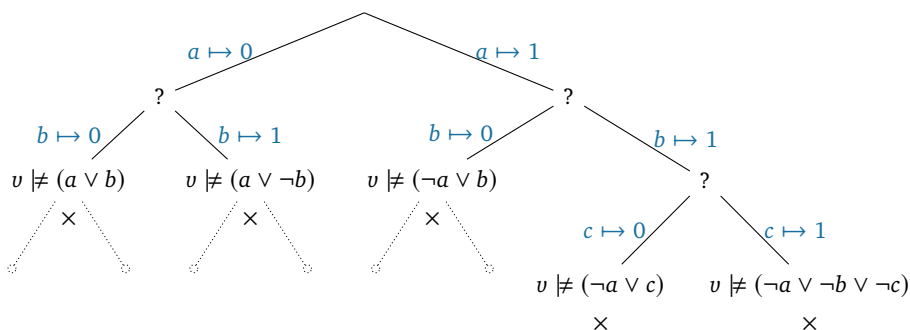
- Ohodnotenie v uzle je *rozšírením* ohodnotenia v rodičovi
- Niektoré klauzuly sa dajú vyhodnotiť aj v čiastočnom ohodnotení
 - V čiastočnom ohodnotení $v = \{a \mapsto 0, b \mapsto 1\}$ sa dá určiť splnenie $(a \vee b)$, $(a \vee \neg b)$, $(\neg a \vee b)$ z našej S
- Ak nájdeme nesplnenú, môžeme hneď „backtracknúť“ – zastaviť prehľadávanie vetvy a vrátiť sa o úroveň vyššie

VIII.9 Prehľadávanie s priebežným vyhodnocovaním

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

× znamená $v \not\models S$

? znamená zatiaľ žiadna nesplnená klauzula



VIII.10 Zjednodušenie množiny klauzúl podľa literálu

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

Každé rozšírenie v' ohodnotenia v :

- Splní klauzuly obsahujúce literál a
 - $\{a \mapsto 1, \dots\} \models (a \vee b)$
 - $\{a \mapsto 1, \dots\} \models (a \vee \neg b)$
- Splní klauzulu $(\ell_1 \vee \dots \vee \neg a \vee \dots \vee \ell_n)$ obsahujúcu $\neg a$ vtt 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 $(\neg a \vee \neg b \vee \neg c)$

Takže:

- Klausuly s a môžeme vynechať
- Klausuly s $\neg a$ môžeme zjednodušiť

VIII.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

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

VIII.12 Zjednodušenie množiny klauzúl podľa literálu

Definícia 2.113. Nech p je výroková premenná.

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

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

Definícia 2.114. Nech ℓ je literál a S je množina klauzúl. Potom definujeme

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

Tvrdenie 2.115. Nech ℓ je literál a S je množina klauzúl.

Potom množiny $S \cup \{\ell\}$ a $S|_{\ell}$ sú ekvivalentné.

VIII.13 Propagácia jednotkových klauzúl

Zjednodušenie množiny klauzúl \rightsquigarrow ľahšie hľadanie spĺňajúcich ohodnotení:

Nech $T = \{ (a \vee \neg b), (a \vee b \vee c) \}$, začnime zjednodušením podľa $\neg a$:

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

- $\neg b$ – jednotková klauzula (unit clause alebo iba unit)
- T' spĺňajú iba ohodnotenia v , kde $v(b) = 0$
- Takže T' zjednodušíme podľa $\neg b$

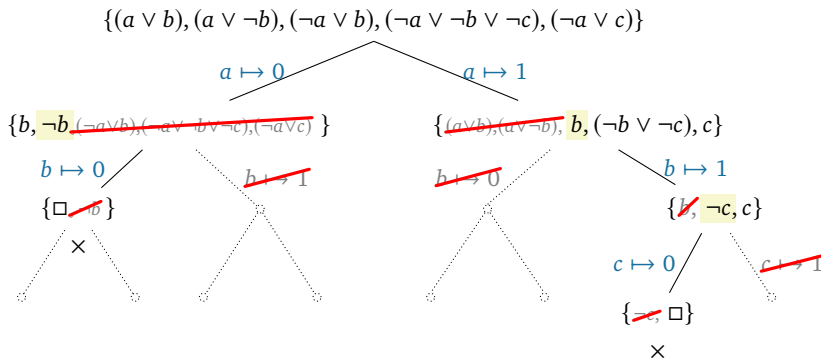
- $T'' := T'|_{\neg b} = \{c\}$
 - T'' spĺňajú iba ohodnotenia v , kde $v(c) = 1$
 - Takže T'' zjednodušíme podľa c

- $T''' := T''|_c = \{\}$

prázdna, triviálne splniteľná, podľa tvrdenia 2.115 je splniteľná aj T

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

VIII.14 Prehľadávanie so zjednodušovaním klauzula unit propagation



VIII.15 Eliminácia nezmiešaných literálov

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

Nech

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

- 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

Z hľadiska splniteľnosti sú klauzuly obsahujúce u nepodstatné.
Stačí uvažovať $T|_u$.

VIII.16 Eliminácia nezmiešaných literálov

Definícia 2.116. Nech ℓ je literál a S je množina klauzúl.

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

Tvrdenie 2.117. Nech ℓ je literál a S je množina klauzúl.

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

2.11.3. DPLL

Algoritmus 2.118 (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  $\text{DPLL}(\Phi|_x, e(x \mapsto T))$  or  $\text{DPLL}(\Phi|_{\neg x}, e(x \mapsto F))$ 
16: end function

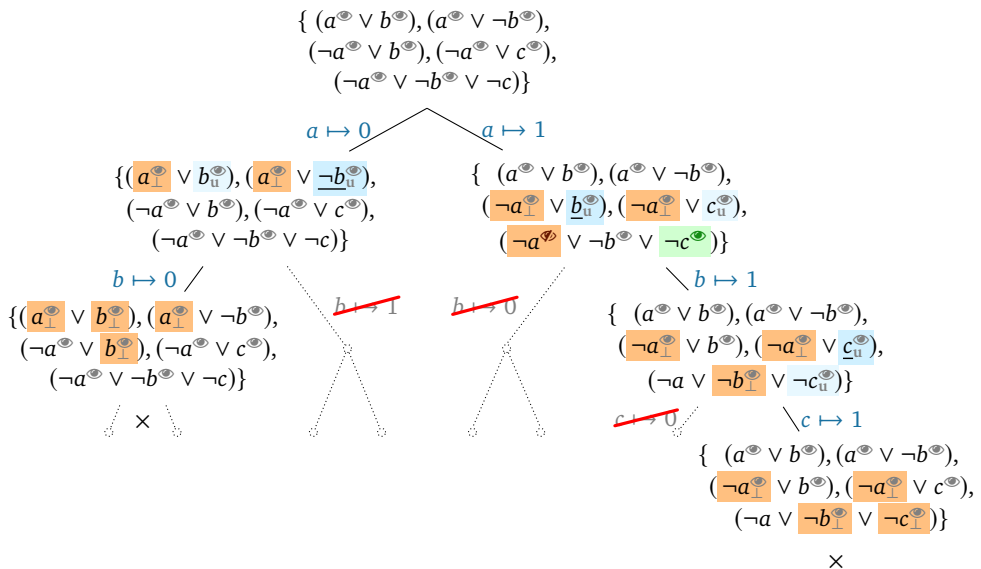
```

VIII.18 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*).

VIII.19 Prehľadávanie s unit propagation a sledovaním



3. Logika prvého rádu

3.1. Syntax relačnej logiky prvého rádu

VIII.20 Štruktúra jednoduchých viet

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

VIII.21 O čom hovoria atomické výroky?

- 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:
prísudok *predmet* *predmet* *prísl. urč. času*
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*₁, *argument*₂, ..., *argument*_n)
Predikátový symbol ~ prísudok (alebo celá prísudková časť):
(je) minister, (je) starší (ako), prijal, <, ...
Jeho argumenty ~ podmet, predmet, ...
Úloha je daná *pozíciou* (ako v prog. 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 (minister¹, starší², prijal⁴, <²).

Unárny predikátový symbol (teda s aritou 1)
zvyčajne predstavuje *vlastnosť*

minister¹(*arg*₁) *arg*₁ je minister
myš_domová¹(*arg*₁) *arg*₁ je myš domová
ľahká¹(*arg*₁) *arg*₁ je ľahká

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

$\text{starší}^2(\text{arg}_1, \text{arg}_2)$	arg_1 je starší ako arg_2
$\text{medzi}^3(\text{arg}_1, \text{arg}_2, \text{arg}_3)$	arg_1 sa nachádza medzi arg_2 a arg_3
$\text{prijal}^4(\text{arg}_1, \text{arg}_2, \text{arg}_3, \text{arg}_4)$	arg_1 prijal arg_2 od arg_3 v čase arg_4

VIII.25 Výber predikátových symbolov

- 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, ... :
 $\text{starší}^2(\text{arg}_1, \text{arg}_2)$ — arg_1 je starší/staršia/staršie ako arg_2

VIII.26 Konkrétne argumenty predikátov — konštanty

- V prirodzenom jazyku *vlastné mená* označujú konkrétne, známe objekty alebo ľudí.
- V logike prvého rádu konkrétne, pevne dané objekty alebo hodnoty označujeme *symbolmi konštant*.
 - 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:
 - stvrty_prezident_SR a Andrej_Kiska
- *Rovnostné atómy* – špeciálny druh atomických formúl:
 - stvrty_prezident_SR \doteq Andrej_Kiska

VIII.27 Výrokové spojky a atomické formuly

- 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...

VIII.28 Premenné a otvorené atomické formuly

- 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*

VIII.29 Všeobecný kvantifikátor

- *Všeobecný kvantifikátor* \forall predstavuje zámená „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:
 - $\forall x (\text{starší}(x, \text{Dorothy}) \vee \neg \text{starší}(\text{George}, x))$

VIII.30 Existenčný kvantifikátor

- *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:
 - $\exists x \forall y \text{ starší}(x, y)$
 - $\forall x (\exists y \exists u \exists z (\text{prijal}(x, u, y, z) \wedge \text{úplatok}(u)) \rightarrow \neg \text{dôveryhodný}(x))$

VIII.31 Symboly jazyka relačnej logiky prvého rádu

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, ktorými sú

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

symbol rovnosti \doteq ,

kvantifikátory: existenčný \exists a všeobecný \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* $\text{ar}(P) \in \mathbb{N}^+$.

VIII.32 Symboly jazyka relačnej logiky prvého rádu

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 $\mathcal{C}_{\mathcal{L}}$ 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 $\mathcal{A}_{\mathcal{L}}$.

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 indexmi.

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

3.2. Formalizácia v logike prvého rádu

3.2.1. Jednoduchá formalizácia

VIII.35 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.

VIII.36 Jednoduchá formalizácia

Riešenie. $\mathcal{V}_{\mathcal{L}} = \{x, y, z\}$, $\mathcal{C}_{\mathcal{L}} = \{\text{Aďa, Biba, Ciri, Dada}\}$, $\mathcal{P}_{\mathcal{L}} = \{r^2\}$
 $r(x, y)$ znamená „ x má rada y “

1. $(r(\text{Biba}, \text{Ciri}) \vee r(\text{Biba}, \text{Dada}))$
2. $\forall x(r(\text{Biba}, x) \rightarrow r(\text{Aďa}, x))$
3. $\forall x(r(x, \text{Ciri}) \rightarrow r(\text{Ciri}, x))$
4. $\exists x(r(x, \text{Biba}) \wedge r(\text{Biba}, x))$
5. $\neg \exists x r(x, x)$

$$6. \forall x \exists y r(x, y)$$

$$7. \exists x \forall y r(y, x)$$

3.2.2. Základné idiómy

VIII.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 .“
 - $\exists x(P(x) \wedge Q(x))$

VIII.38 Základné idiómy: Neexistencia

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:
 - $\forall x \neg (\text{vegán}(x) \wedge \text{obézny}(x))$

- $\forall x (\neg \text{vegán}(x) \vee \neg \text{obézny}(x))$
- $\forall x (\text{vegán}(x) \rightarrow \neg \text{obézny}(x))$

VIII.39 Základné idiómy: Zamlčaná a zdanlivá existencia

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:
 - „nie je obézny“ sa odvoláva na „niekto“
 - „niekto“ teraz nevyjadruje existenciu!
 - $\forall x (\text{vegán}(x) \rightarrow \neg \text{obézny}(x))$

3.2.3. Nutné a postačujúce podmienky

VIII.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?

VIII.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 $\forall x(\exists y(\text{kúpil}(x, y) \wedge \text{karfiol}(y)) \rightarrow \text{vegán}(x))$

VIII.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 $\forall x(\text{vegán}(x) \rightarrow \exists y(\text{kúpil}(x, y) \wedge \text{tekvica}(y)))$

3.2.4. Idiomy s rovnosťou

VIII.43 Idiomy 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.

 - $\forall x(\text{býva_v}(x, \text{byt14}) \rightarrow (x \doteq \text{Aďa} \vee \dots \vee x \doteq \text{Dada}))$

VIII.44 Idiomy 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.

IX. prednáška

Definície predikátov.

Sémantika relačnej logiky prvého rádu

15. apríla 2019

IX.1 Jednoznačnosť rozkladu formúl

Pre našu definíciu formúl platí:

Tvrdenie 3.10 (o jednoznačnosti rozkladu). *Pre každú formulu $X \in \mathcal{E}_{\mathcal{L}}$ v jazyku relačnej logiky prvého rádu \mathcal{L} platí práve jedna z nasledujúcich možností:*

- *Existuje práve jeden taký predikátový symbol $P \in \mathcal{P}_{\mathcal{L}}$ a práve jedna taká n -tica termov t_1, \dots, t_n z $\mathcal{V}_{\mathcal{L}} \cup \mathcal{C}_{\mathcal{L}}$, kde n je arita P , že $X = P(t_1, \dots, t_n)$.*
- *Existuje práve jedna dvojica termov t_1, t_2 z $\mathcal{V}_{\mathcal{L}} \cup \mathcal{C}_{\mathcal{L}}$ taká, že $X = t_1 \doteq t_2$.*
- *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 $X = (A \ b \ B)$.*
- *Existuje práve jedna formula $A \in \mathcal{E}$ a jedna individuová premenná $x \in \mathcal{V}_{\mathcal{L}}$ také, že $X = \forall x \ A$ alebo $X = \exists x \ A$.*

IX.2 Vytvárajúci strom relačnej prvorádovej formuly

Definícia 3.11. *Vytvárajúci strom T pre formulu X je binárny strom obsahujúci v každom vrchole formulu, pričom platí:*

- *v koreni T je formula X ,*

- ak vrchol obsahuje formulu v tvare $\neg A$, $\forall x A$, $\exists x A$, tak má práve jedno dieťa, ktoré obsahuje formulu A ,
- ak vrchol obsahuje formulu v tvare $(A b B)$, kde b je jedna z binárnych spojok, tak má dve deti, pričom ľavé dieťa obsahuje formulu A a pravé formulu B ,
- vrcholy obsahujúce atómy sú listami.

Príklad 3.12. Zostrojme vytvárajúci strom pre formulu $\forall x((\exists y R(x, y) \wedge \exists z R(y, z)) \rightarrow x \doteq y)$.

IX.3 Formuly jazyka relačnej logiky prvého rádu

Otestujte sa IX.1

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

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

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 $\{\text{človek}^1, \text{žena}^1\} \subseteq \mathcal{P}_{\mathcal{L}}$.

- Nie** je formula, význam pravdepodobne správne vyjadruje formula: $(\text{mačka}((\text{Muro}) \wedge \text{myš}(y)) \wedge \text{chytá}(\text{Muro}, y))$.
- 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

IX.4 Pojmy

- V mnohých doménach sú zaujímavé komplikovanejšie kombinácie vlastností alebo vzťahov:
 - x má spoločného rodiča s y , ale x je rôzne od y :

$$\exists z(\text{rodič}(z, x) \wedge \text{rodič}(z, y)) \wedge \neg x \doteq y$$
 - 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*

IX.5 Definície pojmov

Definícia 3.13 (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 3.14. • x je súrodencom y práve vtedy, keď x má spoločného rodiča s y , ale x je rôzne od y

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

- x je *bylinožravec* vtedy a len vtedy,
keď x je živočích, ktorý konzumuje iba rastliny
 $\forall x(\text{bylinožravec}(x) \leftrightarrow$
 $\quad (\text{živočích}(x) \wedge \forall y(\text{konzumuje}(x, y) \rightarrow \text{rastlina}(y))))$

IX.6 Explicitná def. a nutná a postačujúca podmienka

Poznámka 3.15. Všimnite si:

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

V prípade súrodencov to znamená:

- Pre každú dvojicu objektov x a y , ktoré označíme za súrodencov, **musí** existovať ich spoločný rodič a musia byť navzájom rôzne.
- Každé dva navzájom rôzne objekty x a y , ktoré majú spoločného rodiča, **musia** byť súrodenci.

Podobne pre iné definície.

IX.7 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 :
 $\forall x \forall y (\text{sestra}(x, y) \leftrightarrow (\text{žena}(x) \wedge \text{súrodenec}(x, y)))$

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

IX.8 Význam atomických formul – výroková logika

Významom atomických formlí je pravdivostná hodnota

Výroková logika:

- Atomické formuly sú výrokové premenné – nemajú žiadnu štruktúru

šstudent_Evka, zapísaný_Evka_LPI

- Význam im *priamo* priraduje ohodnotenie

$$v = \{\text{študent_Evka} \mapsto t, \quad \text{zapísaný_Evka_LPI} \mapsto f\}$$

- Rôzne ohodnotenia — rôzne stavy sveta

IX.9 Význam atomických formul — logika prvního řádu

Významom atomických formlí je pravdivostná hodnota

Logika *prvého* rádu:

- Atómicke fórmuly majú štruktúru:
predikátový symbol/rovnosť a jeho argumenty (termy)

$$\text{student}(\text{Evka}), \text{ zapísaný}(\text{Evka}, x), \quad x \doteq \text{LPI}, \\ \text{hodnotený}(\text{Ferdo}, \text{LPI}, C)$$

- *Termy* (symboly konštant a *individuových* premenných)

Evka, Ferko, LPI, A, ... u , x , ...

označujú objekty

- Predikátové symboly

študent¹, zapísaný², hodnotený³

označujú vlastnosti alebo vzťahy objektov

IX.10 Vlastnosti a vzťahy matematicky

Aký **matematický** objekt zodpovedá...

- vlastnosti objektov?
 - Množina objektov s vlastnosťou
 - $\{x \mid x \text{ je študent/-ka}\} = \{\text{♂}_{\text{Alica}}, \text{♂}_{\text{Bonifác}}, \text{♂}_{\text{Cyril}}, \text{♀}_{\text{Eva}}, \text{♂}_{\text{František}}, \dots\}$
- vzťahu niekoľkých objektov?
 - Usporiadaná n -tica
 - $(\text{♂}_{\text{Cyril}}, 1\text{-AIN-221}, 2.5)$
- všetkým vzťahom rovnakého druhu?
 - n -árna relácia (množina usporiadaných n -tíc)
 - $\{(\text{♂}_{\text{Alica}}, 1\text{-AIN-221}, 1.5), (\text{♂}_{\text{Alica}}, 1\text{-AIN-412}, 1), (\text{♂}_{\text{Bonifác}}, 1\text{-AIN-221}, 2), (\text{♂}_{\text{Cyril}}, 1\text{-AIN-221}, 2.5), (\text{♂}_{\text{Cyril}}, 1\text{-AIN-222}, 4), (\text{♂}_{\text{František}}, 1\text{-AIN-412}, 2)\}$

IX.11 Význam mimologických symbolov

Priradenie významu symbolom nejakého jazyka \mathcal{L} relačnej logiky 1. rádu:

1. Vyberieme doménu M —

množinu objektov v časti sveta, ktorá nás zaujíma

$$M = \{\text{♂}_{\text{Alica}}, \text{♂}_{\text{Bonifác}}, \text{♂}_{\text{Cyril}}, \text{♀}_{\text{Eva}}, \text{♂}_{\text{František}}, \dots, \text{♂}_{\text{Dr. Žinčica}}, \text{♀}_{\text{prof. Kováčová}}, 1\text{-AIN-221}, 1\text{-AIN-222}, 1\text{-AIN-412}, \dots, 1, \dots, 4, \dots\}$$

2. Interpretujeme mimologické symboly v tejto doméne:

symboly konštant ako objekty z domény

$$i(\text{Evka}) = \clubsuit_{\text{Evka}}, \quad i(\text{Ferdo}) = \heartsuit_{\text{František}}, \quad i(\text{LPI}) = 1\text{-AIN-412}, \\ i(\text{A}) = 1, \quad i(\text{B}) = 1.5, \quad i(\text{B}) = 2, \quad \dots, \quad i(\text{Fx}) = 4, \quad \dots$$

predikátové symboly podľa arity ako množiny prvkov domény

$$i(\text{študent}^1) = \{\clubsuit_{\text{Alica}}, \heartsuit_{\text{Bonifác}}, \spadesuit_{\text{Cyril}}, \clubsuit_{\text{Eva}}, \heartsuit_{\text{František}}, \dots\}$$

alebo ako množiny n -tíc prvkov domény

$$i(\text{hodnotený}^3) = \{(\clubsuit_{\text{Alica}}, 1\text{-AIN-221}, 1.5), (\clubsuit_{\text{Alica}}, 1\text{-AIN-412}, 1), \\ (\heartsuit_{\text{Bonifác}}, 1\text{-AIN-221}, 2), (\spadesuit_{\text{Cyril}}, 1\text{-AIN-221}, 2.5), \dots\}$$

Dvojica (M, i) – štruktúra pre jazyk \mathcal{L}

IX.12 Štruktúra

Definícia 3.16. Nech \mathcal{L} je jazyk relačnej logiky prvého rádu.

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

doména M štruktúry \mathcal{M} je ľubovoľná neprázdna množina;

interpretačná funkcia i štruktúry \mathcal{M} je zobrazenie, 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 3.17. Štruktúry označujeme veľkými písanými písmenami $\mathcal{M}, \mathcal{N}, \dots$

Doménu označujeme rovnakým, ale tlačným písmenom ako štruktúru.

IX.13 Štruktúra ako informatický objekt

















Štruktúru sme definovali pomocou matematických objektov.

Aký informatický objekt zodpovedá štruktúre?

Databáza:

- Predikátové symboly a ich arita \sim veľmi zjednodušená schéma DB

- Interpretácia predikátových symbolov ~ konkrétne tabuľky s dátami

$i(\text{študent}^1)$	$i(\text{zapísaný}^2)$		$i(\text{hodnotený}^3)$		
1	1	2	1	2	3
 Alica	 Eva	1-AIN-221	 Alica	1-AIN-221	1.5
 Bonifác	 Alica	1-AIN-221	 Alica	1-AIN-412	1
 Cyril	 Alica	1-AIN-412	 Bonifác	1-AIN-221	2
 Eva	 Bonifác	1-AIN-221	 Cyril	1-AIN-221	2.5
...	 Cyril	1-AIN-221	 Cyril	1-AIN-222	4
	 Cyril	1-AIN-222	 František	1-AIN-412	2
		

IX.14 Štruktúry — upozornenia

- Štruktúr pre daný jazyk je *nekonečne veľa*
- Doména štruktúry
 - môže mať ľubovoľné prvky
 - nijak *nesúvisí* s intuitívnym významom interpretovaného jazyka
Jazyk o vysokoškolských vzťahoch — číselná doména štruktúry
 - môže byť *nekonečná*
- Interpretácia symbolov konštánt:
 - Každý konstante je priradený objekt domény
 - Nie každý objekt domény musí byť priradený nejakej konstante
 - Rôznym konstantám môže byť priradený rovnaký objekt
- Interpretácie predikátových symbolov môžu byť *nekonečné*
- Štruktúra nedefinuje význam jednej zložky atomických formúl — individuových premenných

Definícia 3.18. Nech $\mathcal{M} = (M, i)$ je štruktúra pre jazyk \mathcal{L} .

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

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

a všetkým ostatným premenným rovnakú hodnotu ako im priraduje e .

Nech

$$\mathcal{V}_{\mathcal{L}} = \{x, y\} \quad M = \{\text{👤}_{\text{Alica}}, \text{👤}_{\text{Bonifác}}, \text{👤}_{\text{Cyril}}, \text{👤}_{\text{Eva}}, \text{👤}_{\text{František}}, 1, 1.5, \dots, 4\}.$$

Ohodnotením (indivíduových) premenných je napríklad

$$e = \{x \mapsto \text{👤}_{\text{Eva}}, y \mapsto \text{👤}_{\text{Bonifác}}\}$$

Potom

$$e(y/2.5) = \{x \mapsto \text{👤}_{\text{Eva}}, y \mapsto 2.5\}$$

Definícia 3.19. 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 $a \in C_{\mathcal{L}}$.

IX.17 Splnenie atomickej formuly v štruktúre

Určenie významu atomickej formuly, napr. zapísaný(Ferko, y), v danej štruktúre, napr. $\mathcal{M} = (M, i)$, kde

$$M = \{\text{Alica}, \text{Bonifác}, \text{Cyril}, \text{Eva}, \text{František}, 1, 1.5, \dots, 3, 4, 1\text{-AIN-221}, 1\text{-AIN-222}, 1\text{-AIN-412}\}$$

$$i(\text{Evka}) = \text{Eva},$$

$$i(\text{Ferko}) = \text{František},$$

$$i(\text{LPI}) = 1\text{-AIN-412}$$

$$i(\text{študent}) =$$

$$\{\text{Alica}, \text{Bonifác}, \text{Cyril}, \text{Eva}, \text{František}\}$$

$$i(\text{zapísaný}) =$$

$$\{(\text{Alica}, 1\text{-AIN-221}), (\text{Alica}, 1\text{-AIN-412}), (\text{Bonifác}, 1\text{-AIN-221}), (\text{Cyril}, 1\text{-AIN-221}), (\text{Cyril}, 1\text{-AIN-222}), (\text{Eva}, 1\text{-AIN-221})\}$$

a pri ohodnotení premenných, napr. $e = \{x \mapsto 1, y \mapsto 1\text{-AIN-221}\}$:

1. vyhodnotíme termy vo formule:

$$\text{Ferko}^{\mathcal{M}}[e] = i(\text{Ferko}) = \text{František}, \quad y^{\mathcal{M}}[e] = e(y) = 1\text{-AIN-221}$$

2. zistíme, či $(\text{František}, 1\text{-AIN-221}) \in i(\text{zapísaný})$:
v tomto prípade *nie*

Takže štruktúra \mathcal{M} nespĺňa formulu zapísaný(Ferko, y) pri ohodnotení e

IX.18 Splnenie existenčne kvantifikovanej formuly

- Vyhodnotenie splnenia formuly s výrokovými spojkami v štruktúre pri ohodnotení — rovnaké ako vo výrokovej logike
- Ako vyhodnotíme splnenie formuly s kvantifikátormi?

IX.19 Splnenie existenčne kvantifikovanej formuly

$\mathcal{M} \models \exists y \text{ zapísaný}(y, \text{LPI})[e]$?

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

m	$e(y/m)$	$\mathcal{M} \models \text{zapísaný}(y, \text{LPI})[e(y/m)]$
Alica	$\{x \mapsto 1, y \mapsto \text{Alica}\}$	áno
Bonifác	$\{x \mapsto 1, y \mapsto \text{Bonifác}\}$	nie
Cyril	$\{x \mapsto 1, y \mapsto \text{Cyril}\}$	nie
Eva	$\{x \mapsto 1, y \mapsto \text{Eva}\}$	nie
František	$\{x \mapsto 1, y \mapsto \text{František}\}$	nie
1	$\{x \mapsto 1, y \mapsto 1\}$	nie
...		
1-AIN-412	$\{x \mapsto 1, y \mapsto 1\text{-AIN-421}\}$	nie

2. $\mathcal{M} \models \exists y \text{ zapísaný}(y, \text{LPI})[e]$ vtt **pre aspoň jedno** $m \in M$ máme $\mathcal{M} \models \text{zapísaný}(y, \text{LPI})[e(y/m)]$;
pravá strana je **pravdivá** pre $m = \text{Alica}$ — *svedok*

IX.20 Splnenie všeobecne kvantifikovanej formuly

$\mathcal{M} \models \forall x (\text{študent}(x) \rightarrow \text{zapísaný}(x, y))[e]?$

Nech $A = \text{študent}(x)$, $B = \text{zapísaný}(x, y)$

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

m	$\mathcal{M} \models A[e(x/m)]$	$\mathcal{M} \models B[e(x/m)]$	$\mathcal{M} \models (A \rightarrow B)[e(x/m)]$
Alica	áno	áno	áno
Bonifác	áno	áno	áno
Cyril	áno	áno	áno
Eva	áno	áno	áno
František	áno	nie	nie
1	nie	nie	áno
...			
1-AIN-412	nie	nie	áno

2. $\mathcal{M} \models \forall x (\text{študent}(x) \rightarrow \text{zapísaný}(x, y))[e]$ vtt **pre všetky** $m \in M$ máme $\mathcal{M} \models (\text{študent}(x) \rightarrow \text{zapísaný}(x, y))[e(x/m)]$;
pravá strana je **nepravdivá** pre $m = \text{František}$ — *kontrapríklad*

Pri určovaní splnenia formuly $\forall x A$, $\exists x A$ v štruktúre \mathcal{M} pri ohodnotení e

- *Nezáleží* na pôvodnej hodnote $e(x)$ pre kvantifikovanú premennú x
- Hovoríme, že premenná x je *viazaná* kvantifikátorom
- Podobné ako formálny parameter funkcie v programovaní
- *Môže závisieť* na hodnote $e(y)$ premenných $y \neq x$

Definícia 3.20. 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 .

Definícia 3.21. 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 3.22. Nájdime štruktúru a ohodnotenie, ktoré spĺňajú množinu $S_{\text{spolubývajúce}} = \{A_1, \dots, A_6\}$ prvých 6 formúl o spolubývajúcich:

$$A_1 = (\text{má_rada}(\text{Biba}, \text{Ciri}) \vee \text{má_rada}(\text{Biba}, \text{Dada})),$$

$$A_2 = \forall x (\text{má_rada}(\text{Biba}, x) \rightarrow \text{má_rada}(\text{Ada}, x)),$$

$$A_3 = \forall x (\text{má_rada}(x, \text{Ciri}) \rightarrow \text{má_rada}(\text{Ciri}, x)),$$

$$A_4 = \exists x (\text{má_rada}(x, \text{Biba}) \wedge \text{má_rada}(\text{Biba}, x)),$$

$$A_5 = \forall x \neg \text{má_rada}(x, x), \quad A_6 = \forall x \exists y \text{má_rada}(x, y)$$

Definícia 3.23. 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 3.24. 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 3.25. 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 premennými, tak

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

Definícia 3.26. 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 3.27. 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 3.28. 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.

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>.